# Cisco TelePresence ISDN Gateway Version 2.2

## Online Help (Printable Format)

D14872.01

January 2013

# Contents

# Introduction

This document contains the text of the online help for the Cisco TelePresence ISDN Gateway web user interface. It is provided so that the help text can be viewed or printed as a single document.

See the online help for details of software licenses that relate to this product.

# Setting up the gateway

This section describes how to set up the Cisco TelePresence ISDN Gateway ready to make calls.

# Getting started with the gateway

## Before you begin

1. Make sure that the physical setup of the ISDN gateway is complete in accordance with the accompanying *Getting Started Guide*.
2. Check that your endpoints and the MCU are correctly configured to operate with the ISDN gateway.

## Setup summary

Before you can make calls you must configure the following ISDN gateway elements through the application web interface:

1. ISDN interfaces
2. ISDN ports
3. Dial plan

## Setup process

1. **Log in**
   Use your browser to navigate to the IP address of the ISDN gateway. Click **Log in** and enter the username '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 your installation. *E1* is typically used in the UK and mainland Europe, *T1* in North America, and *J1* in Japan.
   c. You may need to set values in the **ISDN advanced settings** section. Only change these settings if you know of a specific requirement to do so.
   d. Click **Apply changes**.
   e. Depending on the changes, you may need to restart the ISDN gateway before the changes will take effect. The ISDN gateway will prompt you if this is the case (to restart, go to **Settings > Shutdown** and click **Shut down ISDN GW**).
3. **Configure ISDN ports**
   Go to **Settings > ISDN ports**. For each port specify the following settings (the other settings can be left unchanged unless you have specific requirements):
   a. Set low and high channels:
      - If you have a fully-populated PRI (the norm) set **Low channel** to '1' for all network types and **High channel** to *Max*.
      - 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. The search can start from the high channel and work down, or vice versa. Your ISDN provider can advise which scheme to use, although the choice is not critical.
   c. Click **Apply changes**.
4. **Configure the dial plan**

The default behavior of the gateway is to reject all calls, and you must create a dial plan to allow (permitted) calls to be placed. The simplest configuration is a dial plan that connects any IP to ISDN call routed to the gateway, to the number that the caller has dialed (using any free enabled port), and connects any ISDN to IP call to the MCU auto attendant. To create this dial plan, do the following:

a. Go to **Dial plan > IP to ISDN** and click **Add rule**.
b. Type a name for the rule. (The **UID** field is auto-populated later with a unique identifier for the rule.)
c. For **Condition**, set **Called number matches** to *Any*.
d. For **Action**, select **Place call** and set **Call this number** to *Original*. Leave other values unchanged.
e. 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. Type a name for the rule.
h. For **Condition**, set **Called number matches** to *Any*.
i. For **Action**, select **Place call**; then set **Call this number** to *Custom* and enter the IP address of the MCU. Leave other values unchanged.
j. Click **Add rule** to add the rule to the dial plan.

## Related topics

- Making calls with the gateway [p.11]
- Understanding the dial plan [p.115]

# Making calls with the gateway

The ISDN gateway allows users with ISDN endpoints to place calls to users with IP endpoints, and users with IP endpoints to place calls to users with ISDN endpoints.

Setup information is provided in Getting started with the gateway [p.9] and in the *Getting Started Guide*. In summary, calls can be placed through the gateway once the ISDN gateway and associated devices such as the MCU have been configured and an appropriate dial plan is in place.

When configured correctly the gateway is transparent to users, who will need minimal assistance to place calls through it. However, cost is a potential training consideration for users making ISDN calls. 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 (see Understanding the dial plan [p.115]).

## ISDN to IP calls

If you configure the dial plan as in Getting started with the gateway [p.9], endpoints that call the phone number of the gateway are forwarded to the auto attendant of the MCU (after the call is completely established). From here users can use the Far End Camera Controls (FECC) of their endpoints 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 they are calling. However, if the call will be placed via an MCU, the ISDN 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, which matches all numbers and calls out to a single phone number.

If you want users to be able to call any number, set up the ISDN gateway as an 'H.323 gateway' on your MCU and direct calls to ISDN numbers via that. Or if you use a gatekeeper on your IP network, you can register a prefix with which users may prefix the ISDN number they want to call (similar to dialing '9' for an external line on a phone system).

### Related topics

- Getting started with the gateway [p.9]
- Understanding the dial plan [p.115]

# Using the gateway for voice-only calls

The ISDN gateway can be used to forward voice-only IP calls to the ISDN network (the PSTN) and to forward voice-only ISDN calls from the PSTN to IP telephones on the IP network.

## Configuration methods

You can configure the ISDN gateway to forward voice-only calls globally or through the dial plan configuration.

- **Globally** The gateway can be configured as entirely voice-only with all calls restricted to voice. Or it can be configured as partially voice-only with incoming ISDN video calls allowed and outgoing ISDN calls restricted to voice, or vice versa.
- **Dial plan configuration** The dial plan can be configured to allow certain calls (ingoing and outgoing) as video calls, and to restrict other specific calls to voice only.

### IP to ISDN calls

Many IP endpoints do not allow callers to specify the type of call being made. So a caller may want to make a telephone call (that is, voice only) but be unable to specify it as such. To overcome this problem, for IP data calls the ISDN gateway can extract the voice part of the call and forward it to the ISDN network as a voice-only call.

If the gateway receives an incoming IP to ISDN video call and the global call settings require voice only (maximum call rate is *Telephone*), the video call is not necessarily dropped. The gateway will only reject the call if the dial plan also requires voice only (the **Condition** for all matching rules specifies **Incoming call type** as *H.323-Telephone only*). In other cases the incoming video call will be forwarded as a voice call.

If the IP endpoint does allow the call type to be specified, an incoming 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.

In the ISDN to IP case, an incoming video call will be rejected if either of the following applies:

- The global call settings require voice only (maximum call rate is *Telephone*), or
- The video call is rejected by the dial plan (the **Condition** for all matching rules specifies **Incoming call type** as *Telephone only*).

## Configuring global settings

1. Go to **Settings > ISDN**.
2. To restrict incoming ISDN calls to voice-only calls, set the **Max incoming ISDN call rate** to *Telephone*. To restrict outgoing ISDN calls to voice-only calls, set the **Max outgoing ISDN call rate** to *Telephone*.
3. Complete the other ISDN settings as per your requirements (for details see Configuring general ISDN settings [p.55]).

**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.

# Configuring the dial plan

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 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 does not need to enter the DTMF codes manually on the telephone keypad and can have the call re-routed automatically using the ISDN gateway dial plan. An example of how to specify DTMF tones after a telephone call connects is provided in Example dial plan rules [p.139].

## 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 gateway itself work out which number to call based on dial plan rules.

Whichever method you use, you must configure an appropriate dial plan rule that specifies the **Call type** (for the **Action**) as *Telephone* or has the **Fall back to telephone** checkbox enabled. Then the call will be established correctly.

## Related topics

- Getting started with the gateway [p.9]
- Configuring general ISDN settings [p.55]
- Understanding the dial plan [p.115]
- Configuring dial plan rules [p.127]
- Example dial plan rules [p.139]

# Using the web interface

This section describes how to sign in to the Cisco TelePresence ISDN Gateway web interface and how to use the auto attendant.

# Logging in to the web interface

You need a user account configured on the ISDN gateway in order to log in to its web interface. Your user account has an associated username (user ID) and password, and a set of user privileges which determine your access to the various features in the interface.

To log in to the web interface:

1. In a web browser, enter the host name or IP address of the ISDN gateway.
2. Click **Log in** and enter your assigned **Username** and **Password** (if any).
3. Click **OK**.
   The **Home** page appears.

## Related topics

- Problems logging in [p.16]

# Problems logging in

The **Access denied** page indicates that you have been unable to log in to the ISDN gateway web interface, or have been denied access, for one of the following reasons:

| Message | Explanation |
|---|---|
| Invalid username/password | The username or password was typed incorrectly.<br>If advanced account security mode is enabled for the ISDN gateway and an incorrect username or password is typed three times consecutively, an *admin* account will be disabled for 30 minutes. Other accounts will be disabled indefinitely or until an administrator re-enables the account. |
| No free sessions | The maximum number of sessions allowed simultaneously on the ISDN gateway has been exceeded. |
| This user has been disabled | The user account in question has been disabled. |
| Your IP address does not match that of the browser cookie you supplied | Try deleting your cookies and then log in again. |
| You do not have access rights to view this page | You do not have the necessary privileges to view the page. |
| Page expired | The **Change password** page can expire if the ISDN gateway suspects that the user who asked to change password, may not be the user who is actually submitting the change password request. (This may happen if you use a new browser tab to submit the request.) |

## Disabled accounts (incorrect password entry)

If advanced account security mode is enabled, the ISDN gateway will disable your user account if you enter an incorrect password three times consecutively. Admin accounts are disabled for 30 minutes. Other accounts are disabled indefinitely or until an administrator re-enables the account from the **Users** page.

### Related topics

- Configuring security settings [p.77]
- Managing user accounts [p.148]

# Using the auto attendant

If your administrator has set up calls to be directed to the auto attendant on the ISDN gateway, you can use the auto attendant to enter the number you want to call directly from your endpoint. The auto attendant will prompt you to enter the number.

If you call from an IP endpoint, enter a phone number. If you call from an ISDN endpoint, enter an IP address—you can optionally enter an extension number or phone number after the IP address.

## Dialing from the auto attendant

You can use the following keys or buttons to dial from the auto attendant:

| Key/button | Description |
|---|---|
| 0 to 9 | Standard digits. |
| * (asterisk or star) | Interpreted as a dot for ISDN to IP calls. |
| ** | Interpreted as an ! (exclamation mark) and used as an extension separator for ISDN to IP calls. |
| # (hash) | Indicates that the number is complete and to start dialing. If you omit the #, the ISDN gateway automatically starts dialing after 30 seconds. |

If you do not enter any numbers and leave the auto attendant idle, the ISDN gateway hangs up the call after 60 seconds.

## Calling a specific extension

To call a specific extension, separate the number/address from the extension by typing an exclamation mark (!). For example, to call an MCU with IP address "10.2.1.33" and join a conference numbered "00000", you need to enter 10.2.1.33 ! 00000. To do this you type `10*2*1*33 ** 00000#`

## 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.

# Updating your user profile

You can make some changes to your user profile, as described in the table below. To do this, go to **User profile**.

**Note:** If you are logged in as administrator the **User profile** tab is not available and you need to use the **Users** tab instead.

| Field | Field description |
|---|---|
| **Current password** | Type your current password. |
| **Password** | Type your new password. Unless the ISDN gateway is in advanced security mode there are no set criteria for password selection.<br>In advanced security mode, passwords are subject to the following criteria and rules:<br>■ At least fifteen characters.<br>■ At least two uppercase alphabetic characters.<br>■ At least two lowercase alphabetic characters.<br>■ At least two numeric characters.<br>■ At least two non-alphanumeric (special) characters.<br>■ Not more than two consecutive repeating characters (two repeating characters are allowed but three are not).<br>■ The password must be different from the previous 10 passwords used with the associated user account.<br>■ The password will expire if it is not changed within 60 days.<br>■ Except for users with administrator privileges, the password may not be changed more than once in 24 hours. |
| **Re-enter password** | Verify your new password. |

# Changing your password

To change your password, go to the **Home** page and click **Change password**.

## Standard mode

Unless the ISDN gateway is in advanced security mode there are no set criteria for password selection.

## Advanced security mode

If the ISDN gateway is in advanced security mode, passwords are subject to the following criteria and rules:

- 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 (two repeating characters are allowed but three are not).
- The password must be different from the previous 10 passwords used with the associated user account.
- The password will expire if it is not changed within 60 days.
- Except for users with administrator privileges, the password may not be changed more than once in 24 hours.

### Expired passwords

This applies only in advanced security mode. If you log in with a correct but expired password the ISDN gateway prompts you to change the password. If you choose not to change it, you are allowed two more login attempts to change the password. If you do not change it on those two attempts, your account is disabled.

# System status

This section describes how to display system status information for the Cisco TelePresence ISDN Gateway.

# Displaying general status

The **General** status page (**Status > General**) provides an overview of the current status of the ISDN gateway:

| Field | Description |
|---|---|
| **System status** | |
| **Model** | The specific ISDN gateway model. |
| **Serial number** | The unique serial number of the ISDN gateway. |
| **Software version** | The installed software version. (This information is needed when speaking to Cisco customer support.) |
| **Build** | The build version of installed software. (This information is needed when speaking to Cisco customer support.) |
| **Uptime** | 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 (see Displaying and resetting system time [p.75] for details). |
| **System log** | |
| ■ User requested shutdown<br>■ User requested upgrade<br>■ 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.<br>The log will also display "unknown" if there has been an unexpected reboot or power failure, which you should report to Cisco customer support if it happens repeatedly. |
| **Diagnostic information** | |
| **Download diagnostic information** | If requested by Cisco customer support, click **Download diagnostic information** to save a set of diagnostic files. |

## Related topics

- Displaying ISDN port status [p.23]
- Displaying hardware health status [p.24]

- Displaying and resetting system time [p.75]
- Upgrading and backing up or restoring the ISDN gateway [p.99]
- Shutting down and restarting the ISDN gateway [p.98]

# Displaying ISDN port status

The **ISDN** status page (**Status > ISDN**) provides an overview of the current status of the ISDN ports on the ISDN gateway. The following information is displayed for each physical port:

| Field | Description |
|---|---|
| **Port** | The port number. |
| **State** | Whether or not the port is enabled. A port may be disabled because the port is not applicable, or not licensed, or has been explicitly disabled (see Configuring ISDN ports [p.62]).<br>For ISDN gateway 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.<br>The layer 2 field is not present in leased line mode. |
| **Type** | The interface type configured for this port (to change the interface type, see Configuring general ISDN settings [p.55]). |

## Related topics

- Displaying general status [p.21]
- Displaying hardware health status [p.24]
- Configuring general ISDN settings [p.55]
- Configuring ISDN ports [p.62]

# Displaying hardware health status

The **Health** status page (**Status > Health**) provides information about the ISDN gateway hardware components. Both the current health status and the worst health status seen since the last restart are displayed:

| Field | Description |
|---|---|
| **Fans**<br>**Voltages**<br>**RTC battery** | Possible states are:<br>■ *OK* – component is functioning properly<br>■ *Out of spec* – check with your support provider—the component might require service |
| **Temperature** | Possible states are:<br>■ *OK* – temperature of the ISDN gateway is within the appropriate range<br>■ *Out of spec* – check the ambient temperature (should be less than 34 degrees Celsius) and that the air vents are not blocked<br>■ *Critical* – temperature of the ISDN gateway is too high. An error message also appears in the event log to indicate that the system will shutdown in 60 seconds if the condition persists |

If **Worst status seen** is *Out of spec*, but **Current status** is *OK*, we recommend that you monitor the status regularly to verify that it was only a temporary condition.

To reset the status values, click **Clear**.

## Related topics

- Displaying general status [p.21]

# Managing security warnings

The **Security** status page (**Status > Security**) displays any active security warnings for the ISDN gateway.

To acknowledge a security warning, select the warning and click **Acknowledge selected**. To fix a security issue, click on the **Action** link for the associated warning message. When you fix a security issue, the warning disappears from the **Security** status page and is logged to the Audit log.

**Note:** Rebooting the ISDN gateway causes all warnings to be reset. Any previously acknowledged warnings must be re-acknowledged.

The following information is displayed in security warnings:

| Field | Description |
|---|---|
| **Warning** | Text of the security warning. |
| **State** | ■ *New* The warning has been raised by the ISDN gateway but has not yet been acknowledged. New warnings also appear on the **Home** page.<br>■ *Acknowledged* The warning has been acknowledged (but not yet fixed). Acknowledged warnings do not appear on the **Home** page. |
| **Action** | Each security warning has a corresponding action to fix the security issue. Usually this is a link to the relevant configuration page, where you can make the necessary changes. |

## Related topics

- Configuring security settings [p.77]
- Working with the audit log [p.166]
- Understanding security warnings [p.80]
- Displaying ISDN port status [p.23]
- Displaying hardware health status [p.24]

# Network settings

This section describes how to configure network settings for the Cisco TelePresence ISDN Gateway, including IP routes and services, and SNMP and DNS values.

# Configuring network settings

To configure network settings for the ISDN gateway, or to check network status, go to **Network > Port A** or **Network > Port B**. The ISDN gateway has two Ethernet interfaces (Port A and Port B). Because the configuration pages for the two interfaces are similar, they are described together here and differences are noted where appropriate.

Port A and Port B can be configured to be allocated an 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.

## IP configuration

These settings determine the IP configuration for the appropriate Ethernet port of the ISDN gateway. When you finish making any changes, click **Update IP configuration**.

| Field | Field description |
|---|---|
| **IPv4 configuration** | |
| **IP configuration** | Specifies whether the port should be configured manually or automatically. If set to *Manual* the gateway uses the IP address values that you specify in the **Manual configuration** fields below. If set to *Automatic via DHCP* the gateway obtains its own IP address for this port automatically via DHCP and ignores any manual settings. |
| `Manual configuration` | |
| **IP address** | The dot-separated IPv4 address for this port, for example 192.168.4.45. |
| **Subnet mask** | The subnet mask required for the IP address you want 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 *Manual* the gateway uses the IP address values that you specify in the **Manual configuration** fields below. If set to *Automatic via SLAAC/DHCPv6* the gateway obtains an IP address for the port automatically and ignores any manual settings. 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). |
| `Manual configuration` | |
| **IPv6 address** | The hexadecimal colon-separated global IPv6 address for this port. For example, [2001:db8:168:4::45]. IPv6 addresses must be enclosed in square brackets [ ]. |
| **Prefix length** | The decimal prefix length value for the global IPv6 address for this port. In the example IPv6 address above, the prefix length is 64. |
| **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 (obtained via DHCP or configured manually), 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. When you finish making any changes, click **Update Ethernet configuration**.

| Field | Field description | Usage tips |
|---|---|---|
| **Ethernet settings** | Specify whether you want this port to negotiate its Ethernet settings automatically with the device to which it is connected, or to use the values you specify in the **Manual** configuration fields below. | The settings here *must* match the settings for the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both must be 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.<br>You only need to select this option if you have chosen *Manual* Ethernet settings, as described above. |
| **Duplex** | Identifies the connection duplex mode:<br>■ *Full duplex*<br>Both devices can send data to each other at the same time<br>■ *Half duplex*<br>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.<br>You only need to select this option if you selected *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:** | These fields display further statistics for this port.<br>■ Multicast packets sent<br>■ Multicast packets received<br>■ Total bytes sent<br>■ Total bytes received<br>■ Receive queue drops<br>■ Collisions<br>■ Transmit errors<br>■ 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

These address assignment preferences are applied for IPv6 addressing, based on the ICMPv6 Router Advertisements received when port configuration is set to *Automatic*:

| *RA flags | | | Preferred address |
|---|---|---|---|
| **a** | **o** | **m** | |
| **0** | **0** | **0** | Stateful DHCPv6 |

| | | | |
|---|---|---|---|
| **1** | **0** | **0** | SLAAC |
| **0** | 1 | 0 | Stateful DHCPv6 |
| **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

## Related topics

- Configuring network settings [p.27]
- Configuring IP routes [p.33]
- Configuring IP services [p.36]
- Configuring DNS settings [p.31]
- Configuring SNMP settings [p.39]
- Upgrading and backing up or restoring the ISDN gateway [p.99]

# Configuring DNS settings

To configure DNS settings for the ISDN gateway, go to **Network > DNS**. The settings are described below. If you make any changes, click **Update DNS configuration** when you finish.

| Field | Field description | Usage tips |
|---|---|---|
| **DNS configuration** | Select how you want the ISDN gateway to get its name server address.<br>For example, if you select *Via Port A DHCPv6* the gateway will automatically get a name server address using DHCP over the IPv6 network connected to Ethernet port A. (Port A must be configured to use DHCP.)<br>If you select *Manual*, you must provide a name server address. You may also want to provide a secondary name server or domain name (DNS suffix). | If the DHCP server on your network does not supply DNS configuration information, then the gateway will have no ability to look up names.<br>For IPv6 the Router Advertisement packets determine whether or not DHCPv6 is used.<br>The ISDN gateway does not allow automatic configuration for the name server address if a static IP address is set on the selected interface (see Configuring network settings [p.27]). |
| **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. | Required if you select the *Manual* name server preference. |
| **Secondary name server** | Identifies an optional second name server. | The ISDN gateway queries the secondary DNS server only if the first server is unavailable. If the first server is available but returns that it does not know an address, the secondary DNS server is not 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.<br>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 look up *endpoint.cisco.com*. |

## DNS status

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

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

## Related topics

- Configuring network settings [p.27]
- Configuring IP routes [p.33]
- Configuring IP services [p.36]

# Configuring IP routes

To configure IP routes for the ISDN gateway, go to **Network > Routes**. You may set up one or more routes to control how IP traffic flows in to and out of the ISDN gateway. It is important that these routes are created correctly, or you may be unable to make calls or access the web interface.

## Port preferences

If both Ethernet ports are enabled you need to specify which port should be used in certain particular circumstances. Make the appropriate selections as described in the table and then 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).<br>It only makes sense to have precisely one default gateway, even if different default gateways 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.<br>Selecting Port B as the default gateway preference and 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).<br>As in the IPv4 case, it only makes sense to have precisely one default gateway, even if different default gateways 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.<br>Selecting Port B as the default gateway preference and 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 networks to which the ISDN gateway is connected.

### Adding IP routes

To add a new route, enter the appropriate details as described in the table and then click **Add IP route**. If the route already exists, or aliases (overlaps) an existing route, you are 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.<br>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.<br>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 can select *Port A*, *Port B*, or *gateway*. If you select *gateway*, specify the IP address of the gateway to which you want packets directed.<br>If you select *Port A*, matching packets will be routed to the default gateway for Port A (see Configuring network settings).<br>If you select *Port B*, matching packets will be routed to the default gateway for Port B. If Ethernet Port B is disabled, the option to route packets to Port B is also disabled. |

## Viewing and deleting existing IP routes

Configured routes are listed below the **Add IP route** section. These details are shown per route:

- 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 that are not covered by manually configured routes will be routed according to this route.

Manually configured routes may be deleted by checking the appropriate check box and clicking **Delete selected**.

## Packets are not re-routed from disabled ports

If you disable a port, be aware that any packets that attempt to route to that port will be discarded. The gateway does not re-route them to an alternative port. This applies whether the packets are routed to the port manually (through a specific route configuration) or automatically (no specific route is configured and the port in question is defined as the default gateway). You should take care to avoid this situation.

# Current routes table

The **Current routes** table shows the current default gateway and name servers for Ethernet Port A and Port B. These fields cannot be changed and are provided for reference.

## Related topics

- Configuring network settings [p.27]
- Configuring IP services [p.36]
- Configuring SNMP settings [p.39]
- Upgrading and backing up or restoring the ISDN gateway [p.99]

# Configuring IP services

To configure IP services for the ISDN gateway, go to **Network > Services**. The settings are described below. If you make any changes, click **Apply changes** when you finish.

## Introduction

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 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 ISDN gateway does not allow IP to IP calls (calls between Ethernet ports).

To prevent accidental lock-outs you cannot disable the service that is currently being used to administer the ISDN gateway. So for example, if you configure the gateway over HTTP and come in on Port A, the option to disable the HTTP service for Port A is not available in the interface.

As well as controlling the Ethernet interfaces over which a service operates, administrators can also specify the port number on which that service is provided. If you change the port number for a service (usually there is no need to do this) make sure that the new value does not clash with the port number used by any other service.

### IPv4 and IPv6 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 what is enabled for the port. When specifying settings, use the appropriate column for the required addressing scheme.

### SNMP traps

By default SNMP traps are sent to port UDP port 162 (on the destination network management station). This is configurable, as described in Configuring SNMP settings [p.39].

## Services settings

**Note:** If a port is disabled, these settings are unavailable for that port.

| Field | Field description | Usage tips |
|---|---|---|
| **TCP service** | | |
| **HTTP** | 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.<br>If you require advanced security for the ISDN gateway, disable web access. |

| | | |
|---|---|---|
| **HTTPS** | 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 and backing up or restoring the ISDN gateway [p.99].<br>By default, the ISDN gateway has its own SSL certificate and private key. You can upload a new private key and certificate if required (see Configuring SSL certificates [p.43]).<br>This field cannot be disabled if the device is configured to require certificate-based logins (*Require client certificate login* option is enabled for HTTPS on the **Network > SSL certificates** page). |
| **Incoming H.323** | Enable/disable the ability to receive incoming calls to the ISDN gateway using H.323 or change the port used for this service. | Disabling this option will not prevent outgoing calls to H.323 devices being made by the ISDN gateway. |
| **SIP (TCP)** | Enable/disable the listening service for SIP in respect of incoming calls using SIP over TCP, or change the port used for this service. | Disabling this option will prevent incoming calls using SIP over TCP. |
| **Encrypted SIP (TLS)** | Enable/disable the listening service for SIP in respect of incoming encrypted calls using SIP over TLS, or change the port used for this service. | Disabling this option will prevent incoming calls using SIP over TLS. |
| **FTP** | Enable/disable FTP access on the specified interface or change the port used for this service. | FTP can be used to upload and download ISDN gateway configuration.<br>You should consider disabling FTP access on any port that is outside your organization's firewall.<br>If you require advanced security for the ISDN gateway, disable FTP access. |
| **UDP service** | | |
| **SNMP** | Enable/disable the receiving of the SNMP protocol on this port or change the port used for this service. | By default SNMP traps are sent to port UDP port 162 (on the destination network management station). This is configurable, as described in Configuring SNMP settings [p.39].<br>If you require advanced security for the ISDN gateway, disable the SNMP service. |
| **SIP (UDP)** | Enable/disable the listening service for SIP in respect of incoming and outgoing calls using SIP over UDP, or change the port used for this service. | Disabling this option will prevent calls using SIP over UDP. |

| | |
|---|---|
| **H.323 gatekeeper** | Enable/disable access to the built-in H.323 gatekeeper or change the port used for the built-in H.323 gatekeeper. |

# Reverting to factory defaults

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

## Related topics

- Configuring network settings [p.27]
- Configuring IP routes [p.33]
- Configuring SNMP settings [p.39]
- Configuring SSL certificates [p.43]

# Configuring SNMP settings

To configure SNMP monitoring for the ISDN gateway, go to **Network > SNMP**. The settings are described below. If you make any changes, click **Update SNMP settings** when you finish.

- The ISDN gateway sends out an SNMP trap when the device is shut down or started up.
- The 'system uptime' that appears in the trap is the time since SNMP was initialized on the ISDN gateway (and therefore differs from the **Uptime** reported by 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 TelePresence ISDN GW*. |
| **Location** | Location that appears in the system MIB. | Optional.<br>This setting is useful where you have more than one ISDN gateway. The default setting is *Unknown*. |
| **Contact** | Contact details that appear in the system MIB. | Optional.<br>Can be used 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. The default setting is *Unknown*. |
| **Description** | Description that appears in the system MIB. | Optional.<br>Can be used to provide more information on the ISDN gateway. The default setting is *Cisco TelePresence ISDN GW nnnn* where *nnnn* indicates the model number of the ISDN gateway. |

# Configured trap receivers

| Field | Field description | Usage tips |
|---|---|---|
| **Enable traps** | Check this check box to enable the ISDN gateway to send traps. | If this check box is unchecked then no traps will be sent. |
| **Enable authentication failure trap** | Check this check box to enable authentication failure traps. | If this check box is checked, authentication failure traps will be generated and sent to the trap receivers when someone tries to read or write a MIB value with an incorrect community string.<br>You can check this check box only if **Enable traps** above is also checked. |
| **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. | All traps sent by the ISDN gateway are SNMP v1. You can configure trap receivers or 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. | **CAUTION:** SNMP community strings are not secure and are sent in plain text across the network. We recommend that you change the community strings before you enable SNMP, as the defaults are well known. |
| **RW community** | Community string/password that gives read/write access to all trap information. | **CAUTION:** SNMP community strings are not secure and are sent in plain text across the network. We recommend that you change the community strings before you enable SNMP, as the defaults are well known. |
| **Trap community** | Community string/password that is sent with all traps. | Some trap receivers can filter on the trap community value. |

## Related topics

- Configuring network settings [p.27]
- Configuring IP routes [p.33]
- Configuring IP services [p.36]

# Configuring QoS settings

Quality of Service (QoS) settings are defined on the **Network > QoS** page to set priorities for outbound traffic from the ISDN gateway. They are specified as 6-bit binary values (tags) in the *Type of Service* header field for IPv4 or the *Traffic Class* header field for IPv6, and can be interpreted by networks as Type of Service (ToS) or Differentiated Services (DiffServ).

QoS tags are supported for every IP packet type transmitted by the ISDN gateway: media (audio, video, and telephony), signaling, and administration.

**CAUTION:** We advise you not to alter QoS settings unless you have specific requirements to do so.

## QoS tags

| Field (tag) | Defines priority for... |
|---|---|
| **Audio** | Audio data packets, including RTP and RTCP streams. |
| **Video** | Video data packets, including FECC, BFCP, RTP, and RTCP streams. |
| **Telephony** | Audio data packets in ISDN telephone (speech-only) calls.<br>Note that a non-telephone ISDN call that contains only audio (for whatever reason) is considered to be **Audio**. |
| **Signaling** | H.225, H.245, and SIP signaling packets. |
| **OA&M** | Administration packets, including HTTP, HTTPS, FTP, DNS, syslog, OCSP, and NTP traffic. |

Any traffic that is not covered by one of these categories is tagged as **OA&M**.

### ToS configuration

ToS uses six out of a possible eight bits. The ISDN gateway allows you to set bits 0 to 5, and places 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.

ToS configuration represents a tradeoff between precedence, delay, throughput, and reliability. Ensure that you maintain a balance when prioritizing packets, so that other packets on the network are not subject to undue delay (so 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 places zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

## Default values

These are the default QoS settings on the ISDN gateway:

- *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 DiffServ, this means expedited forwarding.
- *Video 100010*
  - For ToS, this means IP precedence is set to 4 giving quite high priority (but not 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).
- *Telephony 000000*
- *Signaling 000000*
- *Admin 000000*

To revert to default values, click **Reset to default**.

## More information

For more information about QoS, including ToS and DiffServ values, see the relevant RFCs on the Internet Engineering Task Force web site www.ietf.org:

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

## Related topic

- Configuring network settings [p.27]

# Configuring SSL certificates

To manage certificates, HTTPS and SIP trust stores, and optionally to configure OCSP (Online Certificate Status Protocol), go to **Network > SSL certificates**. The ISDN gateway supports certificate-based user authentication over HTTPS, using mutual TLS authentication between certificates on the user (client) side and certificates in the HTTPS trust store on the ISDN gateway. The client must present a valid certificate that has been signed by a trusted certificate authority. Attempts to log in with a revoked certificate are recorded in the **Audit log**.

Optionally the SSL certificate settings can also be used to allow or enforce certificate-based login in place of standard, password-based login (see Client certificate security below).

## Prerequisites

All certificates and trust stores uploaded to the ISDN gateway must be in PEM format (Base64 encoded).

HTTPS access to the web user interface requires the following options:

- The *Secure management (HTTPS)* or *Encryption* feature key must be installed on the ISDN gateway.
- HTTPS must be enabled on the **Network > Services** page.

**CAUTION:** A local certificate and private key is pre-installed on the ISDN gateway and is used by default for HTTPS access. As all ISDN gateways have identical default certificates and keys, to ensure security we recommend that you upload your organization's own certificate and private key (see below).

## Managing certificates and trust stores

To upload or delete certificates and trust stores on the ISDN gateway, go to **Network > SSL certificates**.

### Uploading a custom local certificate and key

1. Go to the **Local certificate configuration** section.
2. Click **Browse** for the **Certificate** field to navigate to the certificate *.pem* file.
3. Click **Browse** for the **Private key** field to navigate to the private key file that accompanies your certificate.
   You must upload the certificate and its key simultaneously.
4. In the **Private key encryption password** field, type the relevant password.
5. Click **Upload certificate and key**.
6. Restart the ISDN gateway.

### Deleting a custom local certificate

1. Go to the **Local certificate** section.
2. Click **Delete custom certificate and key**.

### Uploading a trust store

1. Go to the appropriate trust store configuration section (**SIP trust store** or **HTTPS trust store**) and click **Browse** to navigate to the trust store *.pem* file.

2. Click **Upload trust store**.
   The new trust store will replace the existing one.

**Deleting a trust store**

1. Go to the appropriate trust store configuration section.
2. Click **Delete trust store**.

# Configuring SIP verification

You can configure the ISDN gateway to secure incoming and outgoing SIP calls using TLS. The ISDN gateway uses its SIP trust store to verify the certificate presented by the remote end of a SIP TLS connection.

## SIP client certificate identity requirements

When inspecting the client certificate as part of the SIP TLS handshake, the ISDN gateway looks for either an IP address or a domain identifier for the remote party in the URI and DNS fields of the certificate's subject alternative name (**subjectAltName**) extension. If the **subjectAltName** is not present, the ISDN gateway looks for either an IP address or a domain identifier in the certificate's **Common Name** (CN) field.

You should ensure that the certificates presented by your SIP entities to the ISDN gateway contain both the SIP URI and the IP address of the entity.

## ISDN gateway certificate identity requirements

The remote party must similarly be able to verify the ISDN gateway's local certificate against its trust store, so the local certificate for the ISDN gateway must also be generated according to the guidelines above.

**Note:** If you require TLS on non-proxied SIP calls from the ISDN gateway, the ISDN gateway's local certificate must identify the ISDN gateway by its IP address. This requirement arises because the remote endpoint will be establishing TLS connections directly to the ISDN gateway, which provides its IP address as its identity.

1. Go to **Network > SSL certificates**.
2. Navigate to the **SIP trust store** section.
3. Select an option for the **Verification settings** field (for details see the Certificate settings table below).
4. Click **Apply changes**.

# Configuring HTTPS verification

You can configure certificate-based authentication for users logging in to the web interface and for applications interacting with the API. You can also configure whether the ISDN gateway should verify server certificates, presented by an OCSP server or by feedback receivers, before allowing these connections.

**CAUTION:** If you specify certificate-based authentication as *required* for the ISDN gateway it is possible inadvertently to block *all* login access (including administrators) to the application. If you want to require certificate-based authentication for the first time, or move to it from an existing lower level of authentication, we strongly recommend that you first review the option descriptions below and then follow the process in Transitioning to certificate-based security [p.50].

**CAUTION:** Also be aware that if you transition from solely password-based authentication to *any* level of certificate authentication (including the "lower" levels that permit but do not require certificates) it is possible inadvertently to block all login access to the application. This can happen if HTTP is disabled or HTTP to HTTPS redirection is enabled. In such cases a certificate that is trusted by the ISDN gateway must be presented by the client side (typically you the administrator) in order to log in. If no such client certificate exists then no one can log in.

### Configuring client certificate security

1. Go to **Network > SSL certificates**.
2. Navigate to the **HTTPS trust store** section.
3. Select an option for the **Client certificate security** field (for details see the Certificate settings table below).
4. Click **Apply changes**.

### Configuring server certificate security

1. Go to **Network > SSL certificates**.
2. Navigate to the **HTTPS trust store** section.
3. Select an option for the **Sever certificate security** field (for details see the Certificate settings table below).
4. Click **Apply changes**.

## OCSP support

You can optionally configure an external OCSP server, which the ISDN gateway will use to check the revocation status of client certificates presented with incoming connection requests (OCSP configuration settings are described below).

**Note:** For chained certificates the OCSP check is performed only against the leaf certificate.

The ISDN gateway supports SHA-1 hashing for OCSP.

If the response from the OCSP server is anything other than '*good*' (that is, the client certificate is invalid, revoked, unknown, timed out, or in some other error condition) the ISDN gateway rejects the associated connection request. Once a connection is established no further OCSP checking takes place. So if a certificate is revoked during an active session, that session will continue.

**CAUTION:** If you enable OCSP checking for the ISDN gateway it is possible inadvertently to block *all* login access (including administrators) to the application. If you want to enable OCSP checking, we strongly recommend that you first review the option descriptions below and then follow the process in Transitioning to certificate-based security [p.50].

# Certificate settings

The following fields are available on the **Network > SSL certificates** page. If you make any changes, click **Apply changes** when you finish—make sure you select the correct **Apply changes** button for the section(s) you change.

**CAUTION:** If you specify certificate-based authentication as *required* for the ISDN gateway it is possible inadvertently to block *all* login access (including administrators) to the application. If you want to require certificate-based authentication for the first time, or move to it from an existing lower level of authentication, we strongly recommend that you first review the option descriptions below and then follow the process in Transitioning to certificate-based security [p.50].

**CAUTION:** Also be aware that if you transition from solely password-based authentication to *any* level of certificate authentication (including the "lower" levels that permit but do not require certificates) it is possible inadvertently to block all login access to the application. This can happen if HTTP is disabled or HTTP to HTTPS redirection is enabled. In such cases a certificate that is trusted by the ISDN gateway must be presented by the client side (typically you the administrator) in order to log in. If no such client certificate exists then no one can log in.

| Field | Description |
|---|---|
| **Local certificate** | |
| **Subject** | The business to which the certificate has been issued:<br>■ **C** Country where the business is registered<br>■ **ST** State or province where the business is located<br>■ **L** Locality or city where the business is located<br>■ **O** Legal name of the business<br>■ **OU** Organizational unit or department<br>■ **CN** Certificate common name, or the domain name |
| **Issuer** | The issuer of the certificate. Where the certificate has been self-issued, these details are the same as for **Subject**. |
| **Issued** | Date on which the certificate was issued. |
| **Expires** | Date on which the certificate will expire. |
| **Private key** | Your web browser uses the SSL certificate 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.> |
| **Certificate** | Click **Browse** to navigate to the certificate file. |
| **Private key** | Click **Browse** to navigate to the private key file that accompanies the certificate. |
| **Private key encryption password** | If the private key is stored in encrypted format, you must enter the password in order to upload it. |

| SIP trust store | |
|---|---|
| **Subject, Issuer, Issued, Expires** | Details of the trust store certificate (similar to the Local certificate [p.46] details above). |
| **Trust store** | This trust store is optionally used to authenticate incoming and outgoing SIP calls. You can upload a trust store of certificates that the ISDN gateway can use to verify certificates presented by the remote end of a SIP TLS connection in order to be sure of their identity. Trust store files must be in *.pem* format. |
| **Verification settings** | Determines the circumstances in which the remote certificate must be verified with the SIP TLS trust store:<br>■ *No verification*: All outgoing connections are permitted, even if the remote end does not present a valid and trusted certificate (remote end always trusted).<br>■ *Outgoing calls only*: Outgoing SIP TLS connections are only permitted if the remote end has a trusted certificate.<br>■ *Outgoing and incoming calls*: Outgoing and incoming SIP TLS connections are only permitted if the remote end has a trusted certificate. |

| HTTPS trust store | |
|---|---|
| **Subject, Issuer, Issued,Expires** | Details of the trust store certificate (similar to the Local certificate [p.46] details above). |
| **Trust store** | This trust store is optionally used to authenticate user logins, API messages and feedback messages, and to validate OCSP requests over HTTPS. You can upload a trust store of certificates that the ISDN gateway can use to verify certificates presented by the remote end of an HTTPS connection in order to be sure of their identity. Trust store files must be in *.pem* format. |

| | |
|---|---|
| **Client certificate security** | This setting determines the circumstances in which the remote certificate must be verified with the HTTPS trust store. It can also be used to allow or enforce certificate-based login in place of standard, password-based login.<br>■ *Not required*: The default setting. No client-side authentication is required. All incoming connections are permitted, even if the remote end does not present a valid and trusted certificate (remote end always trusted). Password-based login is the sole authentication mechanism over all user interface connection methods — HTTPS, HTTP, FTP,and console (serial port).<br>■ *Verify certificate*: Incoming HTTPS connections are only permitted if the remote end has a trusted certificate. Password-based login is *also* required over HTTPS. Password-based login is allowed as normal over HTTP, FTP, and console connections.<br>■ *Certificate-based authentication allowed*: Incoming HTTPS connections are only permitted if the remote end has a trusted certificate. Certificate-based login is allowed over HTTPS and the common name in the certificate is presented as the login username (only the first common name is used and any others are ignored; common names with more than 64 characters are not supported.) If the common name matches a username configured on the ISDN gateway the user is allowed access with the privileges associated with that username. If the common name does not match a username then password-based login is required. Password-based login is allowed as normal over HTTP, FTP, and console connections.<br>■ *Certificate-based authentication required*: Incoming HTTPS connections are only permitted if the remote end has a trusted certificate. Certificate-based login is required over HTTPS *and* all other connection types. If the common name from the certificate does not match a configured username the login attempt is rejected. Password-based login is not allowed over HTTP, FTP, and console connections.<br>The *Certificate-based authentication required* option bypasses the login screen altogether, so for HTTP, FTP, and console connections the effect is to disable user access to most functions (no certificate is available for login). Users will be able to access any functions that do not require a login (for example, unless your configuration requires an administrator login for console access, console users will be able to access console commands).<br>The ISDN gateway requires every user account to have a password defined, even if *Require client certificate login* is enabled. And if the ISDN gateway is running in advanced account security mode, a new password must be defined every 60 days. Users are not prompted to change their passwords when logged in using certificate-based authentication. The password will expire, but they will not be asked to change it as long as they are logged in using a certificate.<br>For the purpose of any timed access restrictions that exist on user accounts (typically password change intervals and inactive account expiry rules) any log in using a certificate is treated as a standard password-based login and will reset the timer accordingly.<br>For information about how these options affect the API interface, see the *Cisco TelePresence ISDN Gateway Remote Management API Reference Guide*. |
| **Server certificate security** | Determines whether a trusted certificate is required from the remote server (feedback receiver) for HTTPS feedback messages and OCSP requests to be permitted. |

### Online certificate status protocol (OCSP)

| | |
|---|---|
| **Certificates to check** | To enable OCSP-based checking of HTTPS client certificate revocation status, select *HTTPS client certificates*. |

| | |
|---|---|
| **OCSP server** | Enter the URL of the external OCSP server.<br>■ If the default port allocation is sufficient (port 80 for HTTP and port 443 for HTTPS) use one of these formats, as appropriate: *http://example.com*; *https://example.com*; *http://example.com/examplepath*; *https://example.com/examplepath*<br>■ To send to a non-standard port number (port 88 is used in the examples here) use one of these formats, as appropriate: *http://example.com:88*; *https://example.com:88*; *http://example.com:88/examplepath*; *https://example.com:88/examplepath* |
| **Require nonce** | Determines whether OCSP queries must include a nonce extension (to prevent replay attacks).<br>■ If enabled, the ISDN gateway includes a nonce in each OCSP request, and requires the nonce to be returned in the corresponding response. If the nonce is not returned, the associated connection request is rejected.<br>■ If disabled, note that the ISDN gateway does not send a nonce at all. |
| **Maximum clock skew of OCSP server** | Specifies the maximum acceptable time (in seconds) for clock skew in OCSP responses. In this context the skew is the divergence between the respective system clocks on the ISDN gateway and on the OCSP server. If the skew exceeds this setting, then the OCSP responses may be treated as invalid. |
| **Maximum age of OCSP server records** | Specifies the maximum acceptable age (in days) for certificates. The certificate age is derived from the response field '*thisUpdate*' which indicates when the returned status was last known to be correct. How this value is determined depends on the OCSP server configuration (often it is the last time the server was updated with a new Certificate Revocation List).<br>The ISDN gateway rejects any response where the value of '*thisUpdate*' is later in the past than the time derived by counting back from current time by the number of days specified here (after accounting for clock skew). |

## Related topics

- Configuring security settings [p.77]
- Configuring IP services [p.36]
- Transitioning to certificate-based security [p.50]

# Transitioning to certificate-based security

Certificate-based security methods carry a risk of inadvertently blocking all login access to the ISDN gateway. (If problems occur with the client certificate or the trust store, you will need to fall back to HTTP. If you cannot fall back—because HTTP is disabled or because HTTP to HTTPS redirection is set—then all access methods will be blocked.) To avoid this we strongly recommend that you follow the corresponding procedure below when implementing certificate-based security options:

- Enabling client certificates and certificate login (HTTPS connections) [p.50]
- Enabling OCSP checking [p.51]
- Requiring certificate-only login (all connections) [p.51]

## Enabling client certificates and certificate login (HTTPS connections)

To transition access handling for HTTPS connections from standard, password-based access to required client certificate validation and optionally to allow certificate-based login, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the ISDN gateway (**Network > SSL certificates**) and that the web browser(s) to be used to access the ISDN gateway are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and disable **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
   a. Navigate to the **HTTPS trust store** section.
   b. Set **Client certificate security** to *Verify certificate* (to have client certificate validation but no certificate login) or *Certificate-based authentication allowed* (to have client certificate validation and to allow certificate-based login).
   c. Click **Apply changes**.
5. Now test that you are able to log in to the ISDN gateway over an HTTPS connection.
   a. First verify that you can log in using the standard password login mechanism.
   b. If you specified *Certificate-based authentication allowed* in the previous step, also verify that certificate-based login is working as expected. This step is recommended, although strictly not essential as *Certificate-based authentication allowed* mode still allows password login if certificate login fails.

**Note:** Provided that this procedure is successful, you can now disable HTTP (**Network > Services**) or enable redirection from HTTP to HTTPS (**Settings > Security**) if either are required by your configuration.

# Enabling OCSP checking

**CAUTION:** The ISDN gateway will only perform OCSP checking if client certificate security mode is enabled. To do this go to **Network > SSL certificates** and set the **Client certificate security** option. When you first enable OCSP checking, set **Client certificate security** to one of the 'lesser' modes (*Verify certificate* or *Certificate-based authentication allowed*). If you want to set it to *Certificate-based authentication required*, only do so after you have completed the procedure for Requiring certificate-only login (all connections) [p.51] and you are certain that OCSP checking is working correctly.

To enable OCSP checking for the ISDN gateway, do the following:

1. Ensure that an appropriate HTTPS trust store has been installed on the ISDN gateway (**Network > SSL certificates**).
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS**. This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
   a. Navigate to the **Online certificate status protocol (OCSP)** section.
   b. Set **Certificate to check** to *HTTPS client certificates*.
   c. Enter the URL of the external OCSP server and set any options you require.
   d. Click **Apply changes**.
5. Now test that you are able to log in to the ISDN gateway over an HTTPS connection. Only proceed to the next step if you can successfully log in.
6. Do one of the following, as appropriate for your configuration:
   - Go to **Network > Services** and disable HTTP.
   - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

# Requiring certificate-only login (all connections)

To transition from password-based authentication to required certificate-based authentication for *all* connection types, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the ISDN gateway (**Network > SSL certificates**) and that the web browser(s) to be used to access the ISDN gateway are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**:
   a. Navigate to the **HTTPS trust store** section.
   b. Set **Client certificate security** to *Certificate-based authentication allowed*.
   Do NOT set **Client certificate security** to *Certificate-based authentication required* yet.
   c. Click **Apply changes**.
5. Now test that you are able to log in to the ISDN gateway over an HTTPS connection *using a certificate*. Only proceed to the next step if you can successfully log in with a certificate.
6. Assuming the previous step succeeded, go to the **Client certificate security** option again and this time set it to *Certificate-based authentication required*.

7. Click **Apply changes** and confirm at the prompt.
   It is now not possible to log in over HTTP. To log in over HTTPS requires a valid client certificate signed by a certificate authority, which matches the HTTPS trust store on the ISDN gateway.
8. Do one of the following, as appropriate for your configuration:
   - Go to **Network > Services** and disable HTTP.
   - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

## Related topics

- Configuring SSL certificates [p.43]
- Configuring security settings [p.77]
- Configuring IP services [p.36]

# Testing network connectivity

You can use the **Network connectivity** page to troubleshoot network issues between the ISDN gateway and a remote video conferencing device. On this page you can ping another device from the ISDN gateway 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. In the case of a hostname, the IP address to which it has been resolved will be displayed.

To test connectivity with a remote device:

1. Go to **Network > Connectivity**.
2. In the text box, enter the IP address or hostname of the target device.
3. Click **Test connectivity**.

## Test results

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). For IPv4 connections the TTL (Time To Live) value on the echo reply is also shown. For IPv6 connections the hop limit is shown.

For each intermediate host (typically routers) on the route between the ISDN gateway and the remote device, the IP address of the host and the time taken to receive a response from that host is shown.

## Non-responses or unrecognized responses

Not all devices will respond to the messages sent by the ISDN gateway to analyze the route. Routing entries for non-responding devices are shown as <*unknown*>. Some devices are known to send invalid ICMP response packets (for example, with invalid ICMP checksums). These responses are not recognized by the ISDN gateway and therefore these hosts' entries are also shown as <*unknown*>.

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

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

### Related topics

- Configuring network settings [p.27]

# Configuration

This section describes how to perform configuration tasks for the Cisco TelePresence ISDN Gateway, such as specifying system settings and resetting the system time.

# Configuring general ISDN settings

To configure global settings for the ISDN gateway, such as ISDN network type and options, and allowed call features, go to **Settings > ISDN**. The settings are described below. If you make any changes, click **Apply changes** when you finish.

**Note:** This page contains device-wide settings. Some ISDN configuration is done on a port-by-port basis from the **Settings > ISDN ports** page (see Configuring ISDN ports [p.62]).

# Basic settings

| Field | Field description | Usage tips |
|---|---|---|
| **ISDN interface type** | The ISDN network type to which the ISDN gateway is connected. Select *E1*, *T1 (USA and Canada)*, or *J1 (Japan)* as appropriate. | E1 is typically used in the UK and mainland Europe; T1 in the U.S. and Canada; and J1 in Japan. Refer to your ISDN network provider if unsure which interface type to select.<br>The ISDN gateway may need to be restarted for changes of this setting to take effect. |
| **ISDN switch type** | If the **ISDN interface type** is *T1* or *J1*, select the appropriate **ISDN switch type** for the ISDN switch to which the ISDN gateway is connected:<br>■ *National ISDN*: default switch type for use with the ISDN gateway<br>■ *4ESS*: an AT&T custom switching protocol<br>■ *DMS-100*: a custom protocol used with Nortel network infrastructure in T1 networks | This field only applies to ISDN gateway models that end with a 1, for example the 3201 or 8321.<br>This setting has no effect when the ISDN gateway is in leased line mode. |
| **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.<br>If you select or deselect **Leased line mode**, you must restart the ISDN gateway. |
| **Compatibility** | Select the appropriate settings. | ■ By default the *Send "sending complete"* option is enabled, and the ISDN gateway will send a message to the network when it finishes sending the dial string. Some networks require this but others do not. Leave this setting enabled, but if you find that outbound calls fail (and inbound calls succeed), then try disabling it.<br>■ Select the *Legacy capabilities* option if you experience difficulties connecting your older endpoints to the ISDN gateway. When enabled, the ISDN gateway will detect when one of those endpoints is being called and will send a reduced capability set. |

| | | |
|---|---|---|
| **Send calling number to ISDN network** | Select the appropriate setting. Many networks ignore this field; others disallow it and the call will fail if it is set; and in some networks the call will work only if the calling number is forwarded and the DN is set exactly right. You may need to experiment to identify the appropriate setting for your configuration.<br><br>**Note:** If the calling number exceeds certain length limits, the gateway truncates the number before forwarding it. For E1 networks the maximum number length that will be forwarded is 21 characters. For T1 networks the maximum depends on the switch type, and is 21 for National, 15 for 4ESS, and 13 for DMS-100. | ■ Select *Always* if you want all IP to ISDN calls to forward the calling number where available. (For 4ESS switch configurations—which forbid non-numeric calling numbers—this setting has the same effect as *Only if numeric* below. For DMS-100 configurations, this setting also has the same effect as *Only if numeric*, except that asterisk/star (*) or pound/hash (#) symbols are accepted as numeric.)<br>■ Select *Only if numeric* to forward the calling number only if it is numeric. In this context the gateway does not accept asterisk/star (*) or pound/hash (#) symbols as numeric. If the calling number includes anything other than digits 0-9 it will not be forwarded.<br>■ Select *Never* if IP to ISDN calls should never forward the calling 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.<br><br>This setting also allows you to use the ISDN gateway as a PSTN to voice-over-IP gateway (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 phones. | This setting specifies the maximum bandwidth for an incoming ISDN call. The dial plan cannot override this value with a higher maximum bandwidth, although you can use the dial plan to impose a lower bandwidth for particular calls. (Also, the calling ISDN endpoint may elect to establish a call at a lower bandwidth.)<br><br>If you select *Telephone*, the ISDN gateway forwards ISDN voice calls as voice-only IP calls. ISDN video calls are rejected. For details, see Using the gateway for voice-only calls [p.12]. |
| **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 kbps, and the corresponding number of ISDN B-channels required.<br><br>This setting also allows you to use the ISDN gateway as a voice-over-IP to PSTN gateway (as a voice-only gateway, rather than a video-conferencing gateway). In this case, set the call rate to *Telephone*. Voice calls from IP phones can then be placed to regular PSTN phones. | This setting specifies the maximum bandwidth for an outgoing ISDN call. The dial plan cannot override this value with a higher maximum bandwidth, although you can use the dial plan to impose a lower bandwidth for particular calls. (Also, the calling ISDN endpoint may elect to establish a call at a lower bandwidth.)<br><br>If you select *Telephone*, the ISDN gateway forwards IP calls (voice or video) as voice-only ISDN calls. For details, see Using the gateway for voice-only calls [p.12]. |
| **Maximum call duration** | Limits the length of all calls unless you select *no time limit*. | You may want 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.<br>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.<br>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.<br>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.<br>If *Require layer 2* is selected, then layer 2 must be up before calls are allowed. (This was the default behavior in earlier software versions.) |

# ISDN advanced settings

| Field | Field description | Usage tips |
|---|---|---|
| **Advertise out-of-band DTMF (telephone and auto attendant)** | Enable this setting if you want the gateway to advertise out-of-band DTMF capability to IP if the ISDN side is a telephone call. Received out-of-band tones will be converted and sent over ISDN as in-band tones.<br>If enabled, the gateway also advertises out-of-band DTMF for all calls to the (IP side) auto attendant. This includes video calls—although received out-of-band tones are only converted to in-band in the case of telephone calls. | The gateway does not advertise out-of-band DTMF for video calls (except as described for calls to the auto attendant). |
| **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 or International.<br>In such cases select this setting to set the TON for outgoing ISDN calls to National or International as required. For International you must also specify the **International prefix** (see below). | If this setting is selected, an outgoing ISDN call has a National TON or International TON depending on whether the beginning of the dialed number matches the value specified in the **International prefix** setting. If a match exists the call is International; otherwise the call is National.<br>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.<br>If no value is specified for **International prefix**, no called number will match the international prefix and all calls will have a National TON. |
| **International prefix** | This setting only applies if **Specify national/international type of number** is selected. Use it 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** | This setting only applies if the **ISDN interface type** is *E1*. It controls whether ISDN signaling 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.<br>The ISDN gateway may need restarting for changes to this setting to take effect. |
| **T1 ESF enabled** | This setting only applies if the **ISDN interface type** is *T1*. It controls whether ISDN signaling 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.<br>The ISDN gateway may need restarting for changes to this setting to take effect. |
| **Send channel ID in Q.931,**<br>**Line length,**<br>**Line impedance,**<br>**Line coding,**<br>**Transmit pulse shape,**<br>**National bits (Sa4..Sa8)** | Do not change these settings unless advised to do so by Cisco customer support, or you are an experienced ISDN administrator. | Not all settings apply to all networks. For example, the **National bits** setting is relevant only for E1 networks. |
| **Video NSF**<br>**Telephone NSF** | These settings 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).<br>Do not change these settings unless advised to do so by Cisco customer support, or 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 want to restrict the choices available.<br>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 an 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 want to restrict the choices available.<br>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 an MCU or IP VCR, consider disabling the codec on that device instead.<br>*H.263* also encompasses H.263+. |
| **Content video codecs allowed** | Restricts the choice of content codecs that endpoints calling through the ISDN gateway may select. Content allows a separate presentation stream alongside the video stream. | IP and ISDN endpoints between themselves negotiate which content codecs to use during a call. Use these options if you want to restrict the choices available.<br>**Note:** The ISDN gateway does not advertise content at bandwidths of 128 kbps or lower. We recommend a total call bandwidth of at least 384 kbps for a video call with content.<br>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 an 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. |

## Related topics

- Configuring ISDN ports settings
- Shutting down the ISDN gateway

# Configuring ISDN ports

The options available for configuring ISDN ports differ depending on whether or not the ISDN gateway is in leased line mode:

- Configuring ISDN ports [p.62] (non-leased line mode)
- Configuring ISDN ports in leased line mode [p.65]

## Configuring ISDN ports

To configure ISDN gateway ports to the requirements of your ISDN network, go to **Settings > ISDN ports**. The settings are described below. If you make any changes, click **Apply changes** when you finish. You can configure multiple ports at once.

If the ISDN gateway is running in leased line mode, see instead Configuring ISDN ports in leased line mode [p.65].

**Note:** This page contains port-level settings. Some ISDN configuration is done on a device-wide basis from the **Settings > ISDN** page (see Configuring general ISDN settings [p.55]).

## ISDN 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.<br>When the ISDN gateway has received that number of dialed digits, it will connect the call immediately.<br>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.<br>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.<br>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.<br>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.<br>This calling party number can then be used by an IP participant to return a call to the ISDN participant.<br>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.<br>This calling party number can then be used by an IP participant to return a call to the ISDN participant.<br>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.<br>Refer to your ISDN network provider if you are unsure which value to use. |
| **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).<br>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.<br>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.<br>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.<br>This setting is only visible when the ISDN gateway is configured to use T1 as the **ISDN interface type** in **Settings > ISDN**.<br>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 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.<br>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 gateway 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. |

### Related topics

- Configuring general ISDN settings [p.55]
- Displaying ISDN port status [p.23]

# Configuring ISDN ports in leased line mode

These settings (**Settings > ISDN ports**) affect the per-port ISDN configuration of the ISDN gateway in leased line mode and are used to enable the ports and to configure leased line groups.

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

The settings are described below. After making any changes, click **Apply changes**. You must restart the ISDN gateway for 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 up to 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 must be in contiguous blocks and may not span PRIs.<br>The B-channels configured for this group on the ISDN gateway must match exactly the groups configured on the leased line to which it is connected.<br>For each PRI you can use B-channels 1-31 in E1 mode and 1-24 in T1 mode, except in the case of Cisco TelePresence ISDN GW MSE 8310 and 3200 Series devices, for which the limits are 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 field to 0 (zero) means that the leased line group is not used. |

### Related topics

- Configuring general ISDN settings [p.55]

# Configuring an H.323 gatekeeper

For convenience this topic is repeated here from the earlier section about configuration.

You can configure the ISDN gateway to use a gatekeeper, which can make it easier for users to make calls using directory numbers rather than needing 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 (see Configuring the built-in gatekeeper [p.110]).

To access gatekeeper settings, go to **Settings > H.323**. The settings are described below. If you make any changes, click **Apply Changes** when you finish.

# H.323 gatekeeper settings

| Field | Field description | Usage tips |
|---|---|---|
| **H.323 gatekeeper usage** | Enables the ISDN gateway to use an H.323 gatekeeper for registration of numeric identifiers. | Choose from:<br>■ *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.<br>■ *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.<br>■ *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 as a host name or an IP address.<br>This field will have no effect if **H.323 Gatekeeper usage** is set to *Disabled*.<br>The gatekeeper can be the built-in gatekeeper enabled on the **Gatekeeper** page (see Configuring the built-in gatekeeper [p.110]) 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 standalone Cisco gatekeeper. | Either *gateway* or *gateway (Cisco GK compatible)*. |
| **Ethernet port association** | For all incoming calls, and for outgoing calls dialed by IP address rather than by E.164 phone number or H.323 ID, the gatekeeper will be used to validate the call only if the network interface over which the call is made is selected here. | The check boxes available depend on which interfaces are enabled.<br>In the case of an incoming call to an address in the format <*numeric ID*>@<*domain*> the admission query used to validate the connection will be stripped to <*numeric ID*>. |

| | | |
|---|---|---|
| **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. |
| **Use password** | If the configured gatekeeper required password authentication from registrants, select *Use password* and type the password. | 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. | Optional. If set, users who dial a number beginning with any of the prefixes will have their call directed to the ISDN gateway.<br>Registering several prefixes allows you to create IP to ISDN rules that use different prefixes in certain circumstances, such as for different call rates.<br>This field has 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 selects where to place calls.<br>Also enter the **Threshold** above which messages will be sent to the gatekeeper. The threshold is the percentage of available B-channels in use. An 'available' port has at least layer 1 up and the channel is not in use as a D-channel/reserved channel. For example, if the threshold is 80%, the ISDN gateway informs the gatekeeper that it is busy when 80% of its available B-channels are in use.<br>You can use this feature in two scenarios:<br>■ 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 informs the gatekeeper when it is unavailable. Gatekeepers that support this functionality will favor ISDN gateways in the available state when choosing where to place new calls<br>■ Where there is only one ISDN gateway, and you want to limit the use of the gateway by IP calls. This ensures there will always be some capacity for calls from the ISDN network<br>When selected, the ISDN gateway informs the gatekeeper when it is unavailable (when all 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.<br>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.<br>For example, when one ISDN gateway sends the gatekeeper a message indicating that it is not available, the gatekeeper attempts to use a different ISDN gateway for new calls. |

| | | |
|---|---|---|
| **Deregister from gatekeeper if no ISDN link** | If you select this option the gatekeeper does not forward calls to the ISDN gateway if the gateway is not in a state to receive them. 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. | All PRIs must be down for deregistration. Deregistration will not occur when the gateway is fully loaded with active calls. |

# Current 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. | The status can be one of the following:<br>■ *name resolved to <IP address>*: the ISDN gateway has successfully validated the IP address of the gatekeeper.<br>■ *not in use*: no gatekeeper is in use<br>■ *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.<br>■ *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.<br>■ *failed to resolve gatekeeper name*: the ISDN gateway could not find the IP address of the gatekeeper.<br>■ *registered with <IP address>*: the ISDN gateway has successfully registered to 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 alternate gatekeepers and if the ISDN gateway loses contact with the configured gatekeeper, the ISDN gateway will attempt to register with each of the alternate gatekeepers in turn. If none respond, the ISDN gateway reports that the registration has failed.<br>If the ISDN gateway successfully registers with an alternate gatekeeper, the following will apply:<br>■ The **H.323 gatekeeper status** indicates that registration is with an alternate.<br>■ The list of alternates received from the new gatekeeper replaces the previous list.<br>■ The ISDN gateway will only revert to the original gatekeeper if the alternate fails, and either the original gatekeeper is configured as an alternate on the current gatekeeper's list of alternates or there is no response from any of these alternates.<br>If the ISDN gateway registers with an alternate gatekeeper that does not itself supply a list of alternates, the ISDN gateway retains the original list and if it loses contact with the current gatekeeper, each one is attempted from the top again. |
| **Resource availability status** | Indicates whether the gatekeeper is configured to send resource availability indications and (if so) the current resource availability status of the ISDN gateway. | The possible statuses are:<br>■ *resources available*<br>■ *resources unavailable*<br>■ *<indications not configured>* |
| **Number of active registrations** | This number refers to the H.323 ID and dial plan prefixes. It also shows whether these registrations are pending (in progress, but not fully registered) or active (fully registered). | |
| **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, see the settings table above. |
| **Dial plan prefixes** | Displays the dial plan prefixes that the ISDN gateway has registered with the gatekeeper. | For more information about prefixes, see the settings table above. |

## Related topics

- Configuring the built-in gatekeeper [p.110]

# Configuring SIP settings

To access SIP settings for outgoing calls from the ISDN gateway, go to **Settings > SIP**. The settings are described below. If you make any changes, click **Apply changes** when you finish.

## SIP call settings

| Field | Description |
|---|---|
| **Outbound address** | The hostname or IP address of the SIP proxy/trunk. Square brackets are mandatory for IPv6 addresses. |
| **Outbound domain** | The default domain to apply to outgoing SIP calls in cases where the dialed address does not contain an @ symbol. It will be applied both to direct calls and to calls via a proxy/trunk. (Dial plan rules will fail validation if the called number of a SIP non-trunk call does not contain an @ symbol.)<br>If no value is specified, the outbound address value is used as the outbound domain. |
| **Outgoing transport** | The protocol to be used for call control messages for outgoing call connections. Select the protocol used by your SIP devices.<br>To use encrypted SIP, select TLS. For TLS, you must have the **Encryption** feature key (or the **Secure management** feature key) installed and TLS must be enabled on the **Network > Services** page. Using TLS for call setup is not sufficient for the call to be considered encrypted for the purpose of participating in a conference which requires encryption. Where encryption is required in the conference configuration, a SIP call must use SRTP.<br>The ISDN gateway can accept connections on TCP, UDP, and TLS providing those services are enabled on **Network > Services**. |

# Advanced SIP implementation

The ISDN gateway implements SIP as defined in RFC 3261. Any product wanting to establish SIP calls with the ISDN gateway should implement INVITE, ACK, BYE, and CANCEL messages along with responses from 1xx to 6xx.

For video Fast Update Requests, the ISDN gateway supports a type that involves sending an INFO message with an XML body. This only applies to video endpoints, but these endpoints should be able to reply correctly to INFO requests whether or not they understand them as Fast Update Requests.

# Configuring encryption settings

To access encryption settings for the ISDN gateway, go to **Settings > Encryption**. If you make any changes, click **Apply changes** when you finish.

To use encryption, the Encryption feature key must be present on the ISDN gateway (installing feature keys is described in Upgrading and backing up or restoring the ISDN gateway [p.99]).

You can configure the ISDN gateway to encrypt connections to and from H.323 and SIP endpoints.

- When encryption is in use to and from H.323 endpoints, the ISDN gateway encrypts audio, video, and content media, using Advanced Encryption Standard (AES). It does not encrypt control or authentication information.
- When encryption is in use to and from SIP endpoints, the ISDN gateway encrypts audio, video, and content media using Secure Real-time Transport Protocol (SRTP). Encryption for SIP calls requires the ISDN gateway to use Transport Layer Security (TLS) for SIP messaging.

## Encryption options available

You can do the following:

- 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 IP leg if a SIP endpoint can use SRTP 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 the appropriate endpoints can use encryption. If encryption is required on either leg of the call but the appropriate endpoint cannot use it, the call is disconnected.
- Configure each dial plan rule to use transparent encryption. When transparent encryption is used, the ISDN gateway will simulate point-to-point encryption. It sets the encryption state (enabled/disabled) for the outgoing call to the state used on the received call (that is, attempts to match the outgoing call encryption state to the incoming state).

## Using encryption with SIP

With SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDES). SDES exchanges keys in clear text, so it is a good idea to use SRTP in conjunction with a secure transport for call control messages—accordingly the ISDN gateway allows encryption for SIP calls only if TLS is used for call setup. If the ISDN gateway is not configured to use TLS, then calls that require encryption (to or from the gateway) will fail.

**Note:** TLS calls to or from the ISDN gateway can be made with unencrypted RTP if encryption is disabled or optional for the appropriate dial plan rule (and the far end endpoint).

To configure the ISDN gateway to use SRTP to encrypt media in calls that are set up using TLS:

1. You must have the encryption feature key installed.
2. Go to **Settings > Encryption** and set the **IP encryption status** to *Enabled*.

3. Go to **Settings > SIP** and set **Outgoing transport** to *TLS*. To allow the ISDN gateway to accept incoming TLS calls, go to **Network > Services** and ensure that **Encrypted SIP (TLS)** is selected.

# Encryption settings

| Field | Field description | Usage tips |
|---|---|---|
| **IP encryption status** | Whether or not the ISDN gateway is able to use encryption on the IP leg of a call. | 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.<br>If you disable encryption here but leave it as *Required* in a dial plan rule, all calls using that rule will be rejected. |
| **ISDN encryption status** | Whether or not the ISDN gateway is able to use encryption on the ISDN leg of a call. | 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, optional, or disabled when using that dial plan.<br>If you disable encryption here but leave it as *Required* in a dial plan rule, all calls using that rule will be rejected. |

# Related topic

- Configuring dial plan rules [p.127]

# Displaying and resetting system time

To access time settings for the ISDN gateway, go to **Settings > Time**. The system date and time can be set manually or using the Network Time Protocol (NTP) settings described below. The ISDN gateway re-synchronizes with the NTP server every hour.

## System time

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

## NTP settings

If you change NTP settings, click **Update NTP settings** when you finish.

- If a firewall exists between the ISDN gateway and the NTP server, you should configure the firewall to allow NTP traffic to UDP port 123.
- If the NTP server is local to Port A or Port B, the ISDN gateway automatically uses the appropriate port to communicate with the NTP server.
- If the NTP server is not local, the ISDN gateway uses the port configured as the default gateway to communicate with the NTP server, unless a specific IP route to the network/IP address of the NTP server is defined (**Network > Routes** page).

| Field | Field description | Usage tips |
|---|---|---|
| **Enable NTP** | If selected, use of the NTP protocol is Enabled on the ISDN gateway. | |
| **UTC offset** | The offset from the time zone that you are in from Coordinated Universal Time (UTC). UTC is in broad terms equivalent to Greenwich Mean Time. The offset allows you to set a local time appropriate to the geographic location of the gateway and to adjust for daylight saving. | The offset can be -12:59 to 14:59 hours and can be set in the format hh:mm (or -hh:mm for negative offsets) to specify locations that vary from UTC in half hours. For example, the offset for Rangoon — which is six and a half hours ahead of UTC — is 6:30. You do not need to enter the minutes for whole hours, so an offset of one hour is 1.<br>You must update the offset manually when the clocks go backwards or forwards. The 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.

## Related topics

- Configuring IP routes [p.33]

# Configuring security settings

To configure security settings for the ISDN gateway, go to **Settings > Security**.



## Hashing passwords

By default the ISDN gateway hashes user passwords before storing them in the **configuration.xml** file. Passwords are stored as hash sums and are not stored anywhere on the ISDN gateway in plain text.

## Security settings

If you make any changes, click **Update security settings** when you finish.

| Field | Field description |
|---|---|
| **Advanced account security mode** | **Important!** If you decide to enable advanced account security mode, you should first implement the recommendations below in Usage recommendations for advanced account security [p.78].<br>Advanced account security has the following features:<br>■ All current passwords (created when the ISDN gateway was not in advanced account security mode) will be expired and must be changed by the users when they next log in.<br>■ The ISDN gateway will demand that passwords fulfil certain criteria (using a mixture of alphanumeric and non-alphanumeric characters) and will apply certain rules on expiring and changing passwords.<br>■ The ISDN gateway will disable a user account after three consecutive incorrect password entry attempts. Administrator accounts are disabled for 30 minutes; other accounts are disabled indefinitely or until re-enabled by an administrator.<br>■ The ISDN gateway will disable any non-administrator account that is inactive for 30 days. Administrators can re-enable the account from the **User** page.<br>■ From the **User** page, administrators can also change the password for any user account, or enforce a password change by the user, or lock the password to prohibit password changes except by an administrator. |
| **Redirect HTTP requests to HTTPS** | Enable this option to have HTTP requests to the ISDN gateway automatically redirected to HTTPS. The option is unavailable if either HTTP or HTTPS access is disabled on the **Network > Services** page. |
| **Idle web session timeout** | The timeout setting for idle web sessions, which can be set to a value between 1 minute and 60 minutes. If a web session expires, the user must log in again.<br>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, from the **Settings > User interface** page. |

# Serial console settings

If you make any changes, click **Update console settings** when you finish.

| Field | Field description |
|---|---|
| **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 console input during startup** | Enable this option for enhanced serial port security. |
| **Require administrator login** | Enable 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 device (or with access to your terminal server) can potentially enter commands on the serial console. |
| **Idle serial console session timeout** | If you enable **Require administrator login**, you can configure a session timeout period for idle console sessions. The timeout value can be between 1 minute and 60 minutes.<br>The administrator must log in again if a console session expires. |

# Usage recommendations for advanced account security

If you decide to enable advanced account security mode, we recommend that you first do the following:

- Back up your configuration.
  The ISDN gateway gives the option to create a backup file when it asks for confirmation of the advanced account security request.
- Rename the default administrator account.
  This is especially important where the ISDN gateway is connected to the public Internet, because security attacks 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 possible for innocent attempts to log into the ISDN gateway to cause the account to be locked out for 30 minutes.
- Create several accounts with administrator privileges.
  This ensures that if an administrator account is locked out, you have another account through which to access the ISDN gateway.
- Create dedicated administrator accounts for each API application (if any) that accesses the ISDN gateway.

## Password format and usage

In advanced account security mode, user passwords are subject to the following rules on format and usage:

- 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 (two repeating characters are allowed but three are not).
- The password must be different from the previous 10 passwords used with the associated user account.
- The password will expire if it is not changed within 60 days.
- Except for users with administrator privileges, the password may not be changed more than once in 24 hours.

**Note:** If the ISDN gateway is configured to require certificate-based login only (*Require client certificate login* is enabled for HTTPS on the **Network > SSL certificates** page) every user account still requires a password to be defined, and the rules on password format and usage, including changing within 60 days, still apply.

## Expired passwords

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

## Related topics

- Managing security warnings [p.25]
- Understanding security warnings [p.80]
- Managing user accounts [p.148]
- Configuring SSL certificates [p.43]

# Understanding security warnings

Security warnings identify potential weaknesses in the security of the ISDN gateway configuration. Depending on your deployment, some warnings might not be relevant to your organization (for example, enabling HTTP may not be a security issue if the ISDN gateway is inside a secure network).

These are the warnings that may appear, and the relevant actions to fix them:

| Warning | Action | Explanation |
|---|---|---|
| **Advanced password security is disabled** | Enable **advanced account security mode** in security settings | If advanced account security mode is not enabled, passwords are stored in plain text in the configuration file **configuration.xml** and are therefore insecure.<br>To enable advanced account security mode, go to **Settings > Security** and select *Advanced account 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 stops event messages appearing on the console. |
| **Require administrator login to console is disabled** | Enable require administrator login in serial console settings | You must log in using an admin account to access serial console commands, in this way the serial console will be more secure.<br>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 *list only* privileges. Users who log in as *guest* can only view information about active calls and port status.<br>Disabling the *guest* account makes the ISDN gateway more secure. To do this, go to **Users > User list** and select **Guest**. Then 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.<br>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 easily to discover usernames and passwords.<br>To disable FTP, go to **Network > Services** and deselect **FTP** . |
| **Unsecured HTTP service is enabled** | Disable HTTP in network TCP services | Information sent using HTTP is unsecured and not encrypted.<br>To disable HTTP, go to **Network > Services** and deselect **HTTP**. We recommend that you enable **HTTPS**. |

| | | |
|---|---|---|
| **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 easily to discover usernames and passwords.<br>To disable SNMP, go to **Network > Services** and deselect **SNMP**. |
| **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 on an idle ISDN gateway a session will never time out.<br>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**.<br>For more information on the audit log, refer to Working with the audit log [p.166]. |
| **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.<br>For more information on the audit log, see Working with the audit log [p.166]. |
| **Audit logs hash check failed, audit system integrity compromised** | Check the 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.<br>For more information on the audit log, see Working with the audit log [p.166]. |
| **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.<br>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.<br>To enable encryption, go to **Settings > Encryption** and select *Enabled* for **IP encryption status** and **ISDN encryption status**. |
| **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. If the log is nearing either limit, 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.<br>To do this, go to **Logs > Audit log** and click **Download as XML**. When the download completes, click **Delete *X* to *Y***. This removes from the log all records in the range *X* to *Y*. If necessary, repeat against further ranges until you are satisfied you have freed up sufficient space in the log. |

| | | |
|---|---|---|
| **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. If the log is nearing either limit, 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.<br>To do this, go to **Logs > Audit log** and click **Download as XML**. When the download completes, click **Delete *X* to *Y***. This removes from the log all records in the range *X* to *Y*. If necessary, repeat against further ranges until you are satisfied you have freed up sufficient space in the log. |
| **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** is not enabled, the serial console is not protected during application startup. This means users will have access to debug services in the operating system.<br>To enable this option, go to **Settings > Security** and select **Disable serial input during startup**. |

## Related topics

- Managing security warnings [p.25]
- Configuring security settings [p.77]
- Working with the audit log [p.166]

# User interface

The topics in this section describe how you can customize the Cisco TelePresence ISDN Gateway user interface.

# User interface customization basics

The following customization options for the ISDN gateway web user interface are available to administrators, from the **Settings > User interface** page:

- You can configure header, footer, and message banner text, and the auto-refresh function for web pages. See Managing user interface functions [p.87].
- You can record and upload customized voice prompts that use a different language, wording, or accent from the supplied default prompts. See Creating customized voice prompts [p.94] and Managing customization files [p.90].
- For certain languages you can apply a Cisco 'localization package' to translate the web interface text fields, and in some cases also the voice prompts, from the default U.S. English into one of the available package languages. See Managing localization packages [p.89].

The supplied default voice prompts are in English, spoken in an American, female accent. The following default prompts can be customized:

| Filename | Default wording |
|---|---|
| `voice_prompt_connecting` | Thank you. I'll connect you now |
| `voice_prompt_enter_number` | Please enter the number you want to dial followed by the hash key |
| `voice_prompt_please_hold` | Please hold and an auto attendant will be available shortly |
| `voice_prompt_welcome_<product_name>` | Hello |

## How customizations are organized

Customized elements (voice prompts or web interface text fields) can exist in either or both of the following formats:

- As customization files created locally by your own organization. These can be standalone files or optionally bundled into customization packages for convenient distribution or upload. Generally they contain customized voice prompts only.
- As part of one of the overall localization packages supplied by Cisco for certain languages (accessed via the FTP site at http://ftp.tandberg.com/pub/software/language_packs/codian/). Depending on the package these may contain localized web interface text fields only, or customized voice prompts as well.

Customization packages and localization packages are not the same thing. Customization packages are typically created by your own organization and contain specific, customized voice prompts. Localization packages are supplied by Cisco, may contain both web interface text files and voice prompts, and apply globally to all customizable files.

Three possible customization levels exist on the ISDN gateway:

- Factory default files (U.S. English)
- Localization packages

- Customization files (standalone or bundled in a customization package)

Where an element has both a customization file and a localization package version, the customization file takes precedence. For each customizable element, the ISDN gateway applies the following precedence scheme when selecting which file to use:

1. If an active customization file exists, that file is used.
2. If no active customization file exists, but a localized package is enabled (and the corresponding file exists in the package), the file from that package is used.
3. If no active customization file exists and no localization package is enabled, the default U.S. English file is used.

### Using customization packages

Customization packages are useful for managing customization files and for simplifying the upload process if customized files are to be applied to more than one ISDN gateway. Rather than uploading each file individually to every device, you can create a customization package containing all the customized files from the first ISDN gateway.

A customization package does not have to include a complete set of files. If a particular customized file is not included in the package, then any existing customized prompts or interface elements are left unchanged. This means that you can optionally use multiple packages to build up customization sets.

## Applying customizations

When you apply a localization package the change is global. Each element for which a localized file exists in the package will be affected (except files for which an active customized version already exists, which will not be overwritten).

In contrast, customization files can be applied on a file by file basis. When you apply a new customization file the following actions occur:

- If a customization already exists in the form of a specific customization file, the existing file is overwritten by the new one and deleted from the system.
- If a customization already exists as part of a localization package, the new file is used in its place but the existing file is not deleted from the system.
- Any existing customization files for other elements remain untouched.

**Note:** If you apply a localization package, you are still able subsequently to upload and download individual customized files on a file by file basis.

## How customization options interact

This is how the customization options on the **Settings > User interface** page interact for customized voice prompts (similar principles apply to customized text fields):

- If **Use localization** is checked and **Use customized voice prompts** is unchecked, the application uses whatever voice prompt files are in the localization package.
- If **Use localization** is unchecked and **Use customized voice prompts** is checked, the application uses the individually uploaded voice prompt customization files.

- If **Use localization** and **Use customized voice prompts** are both checked, the application again uses the individually uploaded voice prompt customization files. Custom-made files override any voice prompt files in the localization package.

# Managing user interface functions

To work with configurable web user interface settings for the ISDN gateway, go to **Settings > User interface**. (To change the auto attendant banner, go to **Settings > Auto attendant**.)

## Text entry

The ISDN gateway allows you to type using any character set when entering text into the web interface. However some browsers and FTP clients do not support Unicode characters.

## Controlling auto-refresh

You can set the ISDN gateway to auto-refresh its web status pages (listed below).

- **Status > General**
- **Status > ISDN**
- **Status > Health**
- **ISDN > ISDN calls**
- **ISDN > ISDN ports**
- **ISDN > ISDN calls > Call details**

**CAUTION:** Web pages that auto-refresh will keep a web session active indefinitely, which means that an administrator login will never timeout. This may be considered a security weakness.

1. Go to **Settings > User interface**.
2. In the **Status page auto-refresh interval** field, choose a time interval for the page auto-refresh function, or choose *No auto-refresh* to turn it off.
3. Click **Apply changes**.

## Configuring message banners

You can optionally configure a message banner to appear on the Login page and/or the Home page of the ISDN gateway:

1. Go to **Settings > User interface**.
2. In the **Welcome messages** section, enter a message title and the message text in the **Login message** area and/or the **Home page message** area. For each banner you can specify up to 1600 characters in the message body and up to 100 characters in the message title.
3. Click **Apply changes**.

To revert to the supplied default messages, click **Use default welcome message**.

# Adding headers and footers

You can optionally configure header and footer text, with up to 100 characters each. The headers and footers will display on each page of the web user interface (except the help):

1. Go to **Settings > User interface**.
2. In the **Header and footer messages** section, enter the required text for the header and/or footer.
3. Click **Apply changes**.

Changes to headers or footers are recorded in the **Event log** and the **Audit log**.

# Managing localization packages

To work with localization packages for the ISDN gateway, go to **Settings > User interface**.

When you apply a localization package the change is global. Each element for which a localized file exists in the package will be affected (except files for which an active customized version already exists, which will not be overwritten).

## Checking localization status

To see whether or not the ISDN gateway is currently localized (that is, has a localization package applied), go to **Settings > User interface**. If the unit is localized, the **Use localization package** check box will be checked.

## Applying a localization package

**CAUTION:** Any existing localization package on the ISDN gateway will be overwritten immediately by the new one.

1. If you have not already done so, download the required localization package to your computer from the FTP site at http://ftp.tandberg.com/pub/software/language_packs/codian/.
2. Log in to the ISDN gateway as administrator.
3. Go to **Settings > User interface**.
4. In the **Upload customization package** section, click **Browse** and navigate to the target *.package* file on your computer.
5. Click **Upload package** and wait for the upload to complete.
6. To apply the uploaded package, navigate to the **Select customization** section of the **User interface** page and select **Use localization package**.

## Reverting to factory defaults

The default file set for the web user interface (text, voice prompts, and help pages) cannot be deleted. If your configuration uses a localization package or other customization, you can return to the U.S. English default settings at any time:

1. Go to **Settings > User interface**.
2. Navigate to the **Select customization** section.
3. Uncheck the **Use localization package** check box.
4. If the **Use customized voice prompts** or **Enable customized files** check boxes are displayed, make sure that they are also unchecked.
5. Optional step. If customized voice prompts or text messages are listed in the interface and you are sure that you will not want to use them again, you can delete them from the system.

# Managing customization files

To work with customization files for the ISDN gateway, go to **Settings > User interface**.

## Displaying available prompts

Each voice prompt exists as a .wav file (for example, *voice_prompt_connecting.wav*). Voice prompt files may be the supplied factory defaults or customized versions that have been subsequently uploaded (either individually or as part of a package). To list the voice prompts that are currently available on the system:

1. Go to **Settings > User interface**.
2. Scroll to the **Installed voice prompts** section.
3. In the **Voice prompts** table, if necessary click the **show file details** toggle to expand the file list. An asterisk is displayed next to the **Voice prompts** table name if one or more customized prompts exist.

The expanded list displays the filenames of each available prompt. For any *customized* prompts, the file length and the modification date (when it was uploaded) is displayed together with additional information denoted by the following symbols:

| This symbol... | Indicates that the customization file... |
|---|---|
| ** (two asterisks) | Can be uploaded or downloaded individually. |
| * (one asterisk) | Is supplied by Cisco customer support and cannot be uploaded or downloaded individually. |
| + (plus sign) | Is part of a localization package supplied by Cisco. |

## Uploading and enabling customized prompts

You can upload customized voice prompts to the ISDN gateway in two ways:

- One by one as individual files.
- In a single operation as a customization package.

Customization packages are useful for managing customization files and for simplifying the upload process if the files are to be applied to more than one ISDN gateway. Rather than uploading each file individually to every device, you can create a customization package containing all the customized files from the first ISDN gateway.

A customization package does not have to include a complete set of files. If a customization file is not included in the package for a particular prompt, then any existing customization file for that prompt will be left unchanged. This means that you can optionally use multiple packages to build up customization sets.

### Uploading individual customization files

Before you begin, be aware that:

- Any customization file that already exists for the prompt will be replaced immediately when you upload the new file.

- Assuming that **Use customized voice prompts** is already selected, the ISDN gateway will start using the new file immediately.

To upload a customization file:

1. Go to **Settings > User interface**.
2. Scroll to the **Installed voice prompts** section.
3. Click the **show files details** toggle to open the file list.
4. In the voice prompts list, locate the voice prompt that you want to customize.
5. For that voice prompt, click **upload**. The **upload** button is on the far right of the screen (do not use the **Upload package** button higher up the screen, which is only relevant if you are uploading a bundled customization package).
6. In the **Upload details** page, click **Browse** and locate the customization file on your computer.
7. Click **Upload customization**.
   When the upload completes a confirmation page displays the size of the uploaded file. If the upload fails, check that the file matches the required format before contacting your support representative. Information about voice prompt formats is provided in Creating customized voice prompts [p.94].
8. If the **Use customized voice prompts** option in the **Select customization** section is not already selected then you need to select it to enable the new customization.

## Uploading a customization package

Before you begin, be aware that:

- Any existing customization files on the ISDN gateway that correspond with the files contained in the customization package, will be replaced immediately by the new versions.
- Assuming that **Use customized voice prompts** is already selected, the ISDN gateway will start using the new files immediately.

To upload a customization package:

1. Go to **Settings > User interface**.
2. Scroll to the **Upload customization package** section.
3. Click **Browse...** and locate the *.package* file on your computer.
4. Click **Upload package** and wait for the upload to complete.
5. If the **Use customized voice prompts** option in the **Select customization** section is not already selected then you need to select it to enable the new customizations uploaded in the package.

# Downloading customized prompts

You can download individual customization prompts that exist on the ISDN gateway, which is useful if you want to review the contents or format of a prompt. You cannot download the default voice prompt set or any prompts that were uploaded as part of a package.

To download a voice prompt:

1. Go to **Settings > User interface**.
2. Scroll to the **Installed voice prompts** section.

3. Click the **show files details** toggle to open the **Voice prompts** file list so you can see what customizations are installed.
4. Locate the voice prompt file that you want to download.
5. Right-click **download** and choose **Save Target As** (or the equivalent operation for your web browser). The file will be downloaded to your computer.

# Deleting customized prompts

You cannot delete the supplied default voice prompts, but you can delete customized voice prompts, either individually or globally. (Note that you can revert to the supplied default set at any time without needing to delete any customized prompts.)

To delete a customized voice prompt:

1. Go to **Settings > User interface**.
2. Scroll to the **Installed voice prompts** section.
3. Locate the voice prompt file that you want to delete.
4. Check the check box to the left of the voice prompt.
5. Click **Delete selected** to remove the voice prompt.

When you delete a customized prompt, the ISDN gateway immediately reverts to the relevant default prompt (regardless of whether you have enabled **Use customized voice prompts** at the top of the page).

To delete *all* customized prompts:

1. Go to **Settings > User interface**.
2. Scroll to the **Installed voice prompts** section.
3. Click **Delete all**.

# Creating a customization package (optional)

A customization package can only contain customized voice prompts that have been previously uploaded *as separate files* onto the ISDN gateway. The package will include all such customized voice prompts that are currently uploaded. Prompts that have been uploaded as part of another package will also be included.

To create a customization package:

1. Go to **Settings > User interface**.
2. Scroll to the **Installed voice prompts** section.
3. Optional step. Click the **show files details** toggle to open the **Voice prompts** file list so you can see what customizations are installed.
4. Click the **Download package** button (located just below the **Voice prompts** file list).
   The customization package will be downloaded to your computer.
   The **Download package** button is dimmed if no qualifying voice prompts exist on the system.

# Reverting to the factory defaults

If your configuration uses customized voice prompts, you can revert to the supplied default prompts at any time:

1. Go to **Settings > User interface**.
2. In the **Select customization** section, uncheck the **Use customized voice prompts** check box
3. If the ISDN gateway currently has a localization package applied, uncheck the **Use localization package** check box.
4. Optional step. If customized voice prompts and/or text messages are listed in the interface and you are sure that you will not want to use them again, you can delete them from the system.
5. Click **Apply changes**.

The default prompts are applied immediately (it may take a few seconds before everyone who is connected to the ISDN gateway can hear them).

# Creating customized voice prompts

This topic describes how to create customized voice prompts, to change the language, wording, or accent of the supplied default prompts.

The supplied default voice prompts are in English, spoken in an American, female accent. The following default prompts can be customized:

| Filename | Default wording |
|---|---|
| `voice_prompt_connecting` | Thank you. I'll connect you now |
| `voice_prompt_enter_number` | Please enter the number you want to dial followed by the hash key |
| `voice_prompt_please_hold` | Please hold and an auto attendant will be available shortly |
| `voice_prompt_welcome_<product_name>` | Hello |

## Step 1. Create the prompts

### Recording format

For each customized voice prompt that you need, create a Microsoft WAVE (.wav) file. We recommend the following file settings:

- 16 kHz (16000 Hz) sample rate
- 16-bit resolution
- Mono (mono is the ideal but if you are unable to make mono recordings the ISDN gateway can convert stereo)
- Uncompressed
- Maximum 10 seconds length

If you upload a file that is not in the format given here, the upload may fail or the prompt may sound distorted. Use an audio editing package to make any conversions required.

### Overall recording length limit

As well as the 10-second limit per prompt, an overall limit of four minutes applies for the full set of prompts. It must take no more than 240 seconds to play all the samples back-to-back.

### Optimizing recording quality

As well as the recording format recommendations above, many other factors can impact the quality of voice prompt recordings. These are some points to consider:

- Minimize background noise such as road traffic and noise from fans and other equipment. Background noise in recordings will be very apparent when played back on the ISDN gateway.

- If possible, record all voice prompts in one session. This ensures the voice and background conditions remain constant and that the voice sounds similar from prompt to prompt.
- Try to keep the volume of the recorded voice as consistent as possible across all prompts. The best recordings are achieved by speaking sufficiently loudly for the voice to be recorded loudly compared to any residual background noise, but not so loudly that the voice sounds distorted when played back.

## Step 2. Upload and enable the prompts

When you finish creating new prompts, you need to upload and enable them on the ISDN gateway. Optionally you can also create a customization package for distribution to other ISDN gateways. These tasks are explained in Managing customization files [p.90].

# Managing the auto attendant

The ISDN gateway auto attendant can support up to 20 concurrent connections.

## How queued calls are handled

If all auto attendant connections are busy, incoming calls to the auto attendant are queued until a connection becomes available. Queued calls are handled as follows:

- ISDN video calls are prioritized over other call types.
- IP calls are kept in the alerting state.
- ISDN video calls are connected to a hold prompt (an audio message is played to the caller and the auto attendant banner is displayed).
- ISDN voice-only calls are kept in the altering state.

## Customizing the auto attendant banner

You can optionally upload a custom banner for the auto attendant, in the following file format:

| | |
|---|---|
| File type | GIF, JPEG, or Windows BMP |
| Maximum file size | 90 KB |
| Maximum pixel dimension | 352 x 64 |

**To upload a banner**

1. Make sure the custom banner file is available on your computer hard drive.
2. Go to **Settings > Auto attendant**.
3. In the **Banner upload** area, click **Browse...** to locate and select the required banner file.
4. If the banner is smaller than 352 x 64 pixels so the background is visible, optionally enter RGB color model values to specify the background color.
5. Click **Upload image**.

**To activate a banner**

1. Go to **Settings > Auto attendant**.
2. In the **Auto attendant banner** area, select the banner you want to use.
3. Click **Update** to activate the banner.

**To remove a banner**

1. Go to **Settings > Auto attendant**.
2. Select the banner to be removed (you cannot remove the supplied default).
3. Click **Remove banner**.

# Maintenance

This section describes how to shutdown and restart the Cisco TelePresence ISDN Gateway, and how to perform backups and software upgrades.

# Shutting down and restarting the ISDN gateway

Sometimes you will need to shut down the ISDN gateway, generally to restart as part of an upgrade. You should also shut down the 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 the **Shut down ISDN GW** button.
   The button changes to **Confirm ISDN GW shutdown**.
3. Click **Confirm ISDN GW shutdown** to confirm your shutdown request.
4. The gateway begins to shut down.
   When the shutdown is complete, the button changes to **Restart ISDN GW**.
5. Click **Restart ISDN GW** to restart the gateway.

## Related topics

- Upgrading and backing up or restoring the ISDN gateway [p.99]

# Upgrading and backing up or restoring the ISDN gateway

To back up (or subsequently restore) the ISDN gateway configuration, or to upgrade the software, go to **Settings > Upgrade**.

## Before you begin

**CAUTION:** You **must** back up your configuration before you upgrade the software. Some software upgrades (and downgrades) render the configuration incompatible with previous software versions, which means that without a backup you will be unable to revert to the former software should you need to. Remember the administrator user name and password for the backup file in case you need to use it later.

**CAUTION:** If you use Call Detail Records (CDRs) for billing, auditing or other purposes, you **must** download and save the current CDR data. Some software upgrades (or downgrades) delete existing CDR data.

**CAUTION:** We recommend that you back up the audit logs. Some software upgrades (or downgrades) delete existing audit data.

The software upgrade process requires a hardware restart. Make sure that the device is not in use, or warn any active users who may be affected by the loss of service.

Have the following items available before you start:

- The new software image file.
- The current software image file (in case you need to reverse the upgrade).
- Your configuration backup XML file.
- The administrator user name and password for the configuration backup file.
- If applicable, make sure that the CDR data has been downloaded and saved.

## Upgrading the main software image

The main 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** of the main software image to verify the currently installed version.
3. Log on to the support pages on cisco.com 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 **4-port ISDN-IP gateway software upgrade status** field or in the 8-port equivalent.
11. Shut down and restart the ISDN gateway (see Shutting down and restarting the ISDN gateway [p.98]).

# Upgrading the loader software image

**CAUTION:** You should only upgrade the loader software image under the guidance of Cisco customer support.

Upgrades for the loader software image are not available as frequently as for the main software image. If you are asked by Cisco technical support to upgrade the loader software image, follow these steps:

1. Go to **Settings > Upgrade**.
2. Check the **Current version** of the loader software 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. Shut down and restart the ISDN gateway (see Shutting down and restarting the ISDN gateway [p.98]).

# Backing up and restoring the configuration

The **Back up and restore** area of the **Upgrade** page is used to back up and restore the ISDN gateway configuration from the web interface. You can revert the ISDN gateway to a previously backed up configuration. You can also "clone" one device 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 subsequently restore the configuration, locate a previously-saved **configuration.xml** file and click **Restore backup file**.

**Note:** You can also back up and restore the ISDN gateway configuration using FTP (see Backing up and restoring the configuration using FTP).

## Controlling which settings are overwritten on restore

When restoring a configuration file to the ISDN gateway you can use the **Network settings** and **User settings** overwrite options to control which parts of the configuration are overwritten. By default both options are disabled and existing network and user settings will be preserved (except QoS settings, which are always overwritten).

### Network settings

If you enable **Network settings**, the existing network configuration is overwritten by the equivalent settings

in the restored file. The network configuration includes all network settings *and* the **Redirect HTTP requests to HTTPS** option on the **Settings > Security** page (this option is visible in the user interface only if an encryption or secure management (HTTPS) feature key is present).

**CAUTION:** Typically you should only enable **Network settings** to restore from a file backed up from the same ISDN gateway, or to replace an out-of-service device. If network settings are copied from a different, active, ISDN gateway and there is a clash (such as both are now configured to use the same fixed IP address) then one or both devices may become unreachable via IP.

If you disable **Network settings**, the network configuration is left unchanged by the restore—*except* the QoS settings (**Network > QoS**), which are always overwritten regardless of this option.

### User settings

If you enable **User settings**, all current user accounts and passwords *and* the **Advanced account security mode** and **Idle web session timeout** options on the **Settings > Security** page are overwritten by the equivalent settings in the restored file. If no user account exists in the restored file that corresponds to your current login, you will need to log in again after the file has been uploaded.

**CAUTION:** Remember that in this context, network settings include **Redirect HTTP requests to HTTPS** and user settings include **Advanced account security mode** and **Idle web session timeout** (all three options are configured on the **Settings > Security** page).

## Summary of overwrite controls

| | Status | Overwrites these elements ... |
|---|---|---|
| Network settings | Enabled | All network settings (including QoS settings)<br>Redirect HTTP requests to HTTPS option (**Settings > Security**) |
| | Disabled | QoS settings only |
| User settings | Enabled | User accounts and passwords<br>Advanced account security mode option (**Settings > Security**)<br>Idle web session timeout option (**Settings > Security**) |
| | Disabled | Nothing overwritten |

# Activating features or activating the ISDN gateway

The **Feature management** area of the **Upgrade** page is used to activate features, and in some cases to activate the device itself.

The ISDN gateway requires activation before most of its features can be used. New ISDN gateway are generally supplied pre-activated. If you have a device that is not pre-activated, or have upgraded to a newer firmware version, or are enabling a new feature, you may need to contact your supplier to obtain an appropriate activation code (you will need the gateway serial number). If the gateway has not been activated, the banner at the top of the web interface shows a prominent warning; in every other respect the web interface looks and behaves normally.

Regardless of whether you are activating the gateway or enabling an advanced feature, the process is the same:

1. Check the **Activated features** 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**. If the activation is successful, the browser window refreshes and lists the newly activated item and its activation code.
   If the activation code is not valid, you are prompted to re-try.
4. We recommend that you record the activation code in case you need to re-enter it in future.

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

**Note:** You can remove some feature keys by clicking the **remove** link next to the feature key in this page.

## Time-limited and expired activation codes

Activation codes may be time limited, in which case the expiry date is displayed.

If the feature has already expired, a warning is displayed. Expired activation codes are still listed, but the corresponding feature will not be activated.

## Related topics

- Backing up and restoring using FTP [p.103]

# Backing up and restoring using FTP

This topic describes how to backup or restore the configuration of the ISDN gateway using FTP. To back up and restore the configuration through the web interface, see instead Upgrading and backing up or restoring the ISDN gateway [p.99].

## Backing up via FTP

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

The backup process is now complete.

## Restoring 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 prompted, enter the username and password you use to log in to the ISDN gateway web interface as an administrator.
4. Upload the required **configuration.xml** file to the ISDN gateway, overwriting the existing file on the ISDN gateway.
5. If the restored configuration file contains changes to the ISDN port settings, you need to restart the gateway (go to **Settings > Shutdown**).

The restore process is now complete.

## To transfer a configuration

The same process can be used to transfer a configuration from one ISDN gateway to another *of the same model number*. Before doing this, be sure to keep a copy of the original feature keys from the ISDN gateway for which you are replacing the configuration. 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 device was configured with a static address, you will need to reconfigure the IP address on any other devices on which you have used the configuration file.

# Gatekeeper

This section describes gatekeeper management tasks for the Cisco TelePresence ISDN Gateway. You can register the ISDN gateway with an external gatekeeper or you can enable its own built-in gatekeeper.

# Configuring an H.323 gatekeeper

For convenience this topic is repeated here from the earlier section about configuration.

You can configure the ISDN gateway to use a gatekeeper, which can make it easier for users to make calls using directory numbers rather than needing 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 (see Configuring the built-in gatekeeper [p.110]).

To access gatekeeper settings, go to **Settings > H.323**. The settings are described below. If you make any changes, click **Apply Changes** when you finish.

# H.323 gatekeeper settings

| Field | Field description | Usage tips |
|---|---|---|
| **H.323 gatekeeper usage** | Enables the ISDN gateway to use an H.323 gatekeeper for registration of numeric identifiers. | Choose from:<br>■ *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.<br>■ *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.<br>■ *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 as a host name or an IP address.<br>This field will have no effect if **H.323 Gatekeeper usage** is set to *Disabled*.<br>The gatekeeper can be the built-in gatekeeper enabled on the **Gatekeeper** page (see Configuring the built-in gatekeeper [p.110]) 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 standalone Cisco gatekeeper. | Either *gateway* or *gateway (Cisco GK compatible)*. |
| **Ethernet port association** | For all incoming calls, and for outgoing calls dialed by IP address rather than by E.164 phone number or H.323 ID, the gatekeeper will be used to validate the call only if the network interface over which the call is made is selected here. | The check boxes available depend on which interfaces are enabled.<br>In the case of an incoming call to an address in the format <*numeric ID*>@<*domain*> the admission query used to validate the connection will be stripped to <*numeric ID*>. |

| | | |
|---|---|---|
| **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. |
| **Use password** | If the configured gatekeeper required password authentication from registrants, select *Use password* and type the password. | 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. | Optional. If set, users who dial a number beginning with any of the prefixes will have their call directed to the ISDN gateway.<br>Registering several prefixes allows you to create IP to ISDN rules that use different prefixes in certain circumstances, such as for different call rates.<br>This field has 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 selects where to place calls.<br>Also enter the **Threshold** above which messages will be sent to the gatekeeper. The threshold is the percentage of available B-channels in use. An 'available' port has at least layer 1 up and the channel is not in use as a D-channel/reserved channel. For example, if the threshold is 80%, the ISDN gateway informs the gatekeeper that it is busy when 80% of its available B-channels are in use.<br>You can use this feature in two scenarios:<br>■ 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 informs the gatekeeper when it is unavailable. Gatekeepers that support this functionality will favor ISDN gateways in the available state when choosing where to place new calls<br>■ Where there is only one ISDN gateway, and you want to limit the use of the gateway by IP calls. This ensures there will always be some capacity for calls from the ISDN network<br>When selected, the ISDN gateway informs the gatekeeper when it is unavailable (when all 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.<br>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.<br>For example, when one ISDN gateway sends the gatekeeper a message indicating that it is not available, the gatekeeper attempts to use a different ISDN gateway for new calls. |

| | | |
|---|---|---|
| **Deregister from gatekeeper if no ISDN link** | If you select this option the gatekeeper does not forward calls to the ISDN gateway if the gateway is not in a state to receive them. 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. | All PRIs must be down for deregistration. Deregistration will not occur when the gateway is fully loaded with active calls. |

# Current 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. | The status can be one of the following:<br>■ *name resolved to <IP address>*: the ISDN gateway has successfully validated the IP address of the gatekeeper.<br>■ *not in use*: no gatekeeper is in use<br>■ *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.<br>■ *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.<br>■ *failed to resolve gatekeeper name*: the ISDN gateway could not find the IP address of the gatekeeper.<br>■ *registered with <IP address>*: the ISDN gateway has successfully registered to 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 alternate gatekeepers and if the ISDN gateway loses contact with the configured gatekeeper, the ISDN gateway will attempt to register with each of the alternate gatekeepers in turn. If none respond, the ISDN gateway reports that the registration has failed.<br>If the ISDN gateway successfully registers with an alternate gatekeeper, the following will apply:<br>■ The **H.323 gatekeeper status** indicates that registration is with an alternate.<br>■ The list of alternates received from the new gatekeeper replaces the previous list.<br>■ The ISDN gateway will only revert to the original gatekeeper if the alternate fails, and either the original gatekeeper is configured as an alternate on the current gatekeeper's list of alternates or there is no response from any of these alternates.<br>If the ISDN gateway registers with an alternate gatekeeper that does not itself supply a list of alternates, the ISDN gateway retains the original list and if it loses contact with the current gatekeeper, each one is attempted from the top again. |
| **Resource availability status** | Indicates whether the gatekeeper is configured to send resource availability indications and (if so) the current resource availability status of the ISDN gateway. | The possible statuses are:<br>■ *resources available*<br>■ *resources unavailable*<br>■ *<indications not configured>* |
| **Number of active registrations** | This number refers to the H.323 ID and dial plan prefixes. It also shows whether these registrations are pending (in progress, but not fully registered) or active (fully registered). | |
| **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, see the settings table above. |
| **Dial plan prefixes** | Displays the dial plan prefixes that the ISDN gateway has registered with the gatekeeper. | For more information about prefixes, see the settings table above. |

## Related topics

- Configuring the built-in gatekeeper [p.110]

# Configuring the built-in gatekeeper

The ISDN gateway contains a built-in gatekeeper with which devices can register multiple IDs. The IDs can be numbers, prefixes, or H.323 IDs. 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, in which case the ISDN gateway counts as one registered device.

## Enabling 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 (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 first opening the port, an error message displays.)

### Configuring neighboring gatekeepers

You can optionally configure the built-in gatekeeper with up to two neighboring gatekeepers. Then if the built-in gatekeeper receives an Admission Request (ARQ) to resolve an ID to an IP address, and that ID is not currently registered with it, the built-in gatekeeper will forward the request to its neighbor gatekeeper(s) as a Location Request (LRQ). The built-in gatekeeper then uses 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 about unknown IDs to its neighbors.
- Reply to LRQs from other gatekeepers.
- Accept Location Confirm (LCF) messages from non-neighboring gatekeepers.

## Built-in gatekeeper settings

Use 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 or hostname of the neighboring gatekeeper (or <*host*>:<*port number*> to specify a port other than the default—1719—on the neighboring gatekeeper).<br>Repeat if you want to configure a second neighbor. | 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 neighbors. Choose from the options:<br>■ *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.<br>■ *Enabled, using local return address*: The ISDN gateway will put, in the LRQ, its own address as the return address for the LCF.<br>■ *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.<br>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).<br>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 from which this registration was made. | 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 those devices), check 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. | |

## Related topics

- Configuring IP services [p.36]
- Configuring an H.323 gatekeeper [p.105]

# Dial plan

This section describes how to set up and manage the dial plan on the Cisco TelePresence ISDN Gateway.

# Understanding the dial plan

The dial plan is a set of rules which control how the ISDN gateway routes calls between IP and ISDN networks. When an incoming call request arrives the gateway uses the dial plan to determine how to handle the outgoing part of the call. For example, the dial plan might direct certain ISDN calls to a specific conference on an MCU, or require a particular bandwidth for IP to ISDN calls.

The dial plan has two parts:

- IP to ISDN
- ISDN to IP

The incoming part of a connection into the gateway determines which dial plan is used. For incoming requests from an IP endpoint, the IP to ISDN dial plan is used. For incoming requests from an ISDN endpoint, the ISDN to IP dial plan is used.

**Note:** The two dial plans behave similarly and the online help only distinguishes between them where differences exist.

## Dial plan rules

Each rule in the dial plan comprises the following elements:

- **Rule name**
  Assigned when you create the rule.
- **Condition**
  Every rule must have a condition, which if matched by an incoming call request causes the rule to be invoked. Conditions can define any combination of called number, calling number, incoming protocol, and incoming call type.
- **Action**
  Every rule must have an action to perform if the rule is invoked. The action can be to place the call (to the original dialed number or to a specified number or address), reject the call, or enter the auto attendant.
- **Options**
  Additional settings can be applied to the action. For example, to specify encryption and bandwidth requirements, or to manipulate the caller's number before it is forwarded to the ISDN or IP network.
- **Codecs**
  Each rule also has an associated set of allowed codecs.

Each rule also has a system-generated unique ID, used to identify the rule in the **Audit log**.

### How dial plan rules are applied

1. When the gateway receives an incoming call request, it checks the appropriate dial plan (IP to ISDN or ISDN to IP) and compares the request against the condition of *each* rule in the dial plan until a match is found.
2. If a match is found, the action in the matching rule is used to determine what should be done next. No further rules are checked.
3. If no matching rule condition is found for the call request (or the dial plan contains no rules) the call is rejected.

## Rule ordering

Rules are always checked in top-to-bottom order against each incoming call. This means the dial plan can be designed to handle specific calling cases first, then general calls if no specific cases match. For example, this dial plan calls a particular endpoint if a request is received for a specific number (6056 in this case) and connects all other incoming requests to an operator:

| Rule order | Condition | Action (Place call) |
|---|---|---|
| 1 | **Called number matches** set to *6056* | **Call this number** set to *Original* |
| 2 | **Called number matches** set to *Any* | **Call this number** set to *1000* |

# Leased line mode

The dial plan options differ if the gateway is in leased line mode. See Configuring dial plan rules in leased line mode [p.133].

## Related topics

- Managing the dial plan [p.125]
- Displaying and testing the dial plan [p.124]
- Configuring dial plan rules [p.127]
- Example dial plan rules [p.139]
- Dial plan syntax [p.120]
- Making calls with the gateway [p.11]

# How call number matching works

Call number matching is key to dial plan management and controls how dial plan rules are invoked:

1. A typical dial plan rule is defined with a call number to be matched.
2. If the corresponding element of an incoming call matches that number, the rule will be invoked.
3. If the incoming call does not match then the next rule in the dial plan is checked in sequence, and so on until a match is found.
4. If no match is found in the dial plan the call is rejected.

Matching can be specified against either or both of:

- The **destination number** the caller is trying to reach.
  This is called number matching, set in the **Called number matches** condition for the rule.
- The **originating number** the caller is calling from.
  This is calling number matching, set in the **Calling number matches** condition for the rule.

## Using special characters

The number to be matched can be defined as follows:

- As a specific number that you simply type in the interface.
- Using special characters—similar to regular expressions—to derive the number.

Special characters can be applied to any combination of digits 0-9 and to all or part of the called number/calling number. They can be used to denote asterisk/star and pound/hash dialing keys, to repeat or match particular digits, and to include (substitute) portions of the incoming called or calling digits. For details see Dial plan syntax [p.120].

## How the gateway handles alphanumeric numbers

The ISDN gateway gateway algorithms for call number matching require call numbers to be numeric only. The gateway manages call numbers as follows:

- Numbers that are all numeric are used unchanged.
- For alphanumeric numbers in the format <*numeric ID*>@<*domain*> (and only that format) the gateway removes the '@domain.com' part and uses just the numeric part.
- For numbers in any other alphanumeric format the gateway treats the entire string as null.

These rules apply to called numbers and calling numbers, and to number matching (incoming leg of the call) and number forwarding (outgoing leg). The only exception is the calling number, which by default is forwarded unchanged to the outgoing leg. The table summarizes how the gateway modifies alphanumeric call numbers:

| Dial plan operation | Modified? |
|---|---|
| Called number — matching the incoming number | Yes |
| Called number — forwarding the outgoing number | Yes |
| Calling number — matching the incoming number | Yes |
| Calling number — forwarding the outgoing number | No |

**Note:** If you want to remove alphanumerics from the forwarded calling number, use the standard (D*) and $n substitution characters in the dial plan, adjusted to fit the required case. For example, **Condition** as *Calling number matches* set to *Custom (D*)* and **Action** as *Use calling number* set to *Custom $1*.

# Examples of call number handling

The tables here illustrate how particular called number and calling number formats are handled in the dial plan, including:

- The value (which may be null) that the gateway uses to search for a dial plan match.
- Whether that value will match to *Any*, *None*, or *Custom* conditions (a sample value is assumed for *Custom*).
- The value (which may be null) that is forwarded for use in the outgoing call leg.
- How the forwarded value will compare in its *Original* state as derived by the gateway, and in a *Custom* state as derived by dial plan manipulation (a sample value is assumed for *Custom*).

## Called numbers

| Called number | Value to match | Any | None | Custom '123' | Value to forward | Original | Custom '888$A' |
|---|---|---|---|---|---|---|---|
| 123 | 123 | Yes | - | Yes | 123 | 123 | 888123 |
| 123dev | Null | Yes | Yes | - | Null | Null | 888 |
| 123@test.com | 123 | Yes | - | Yes | 123 | 123 | 888123 |
| 123dev@test.com | Null | Yes | Yes | - | Null | Null | 888 |

## Calling numbers

| Calling number | Value to match | Any | None | Custom '123' | Value to forward | Original | Custom '888$A' |
|---|---|---|---|---|---|---|---|
| 123 | 123 | Yes | - | Yes | 123 | 123 | 888123 |
| 123dev | Null | Yes | Yes | - | 123dev | 123dev | 888123dev |
| 123@test.com | 123 | Yes | - | Yes | 123@test.com | 123@test.com | 888123@test.com |
| 123dev@test.com | Null | Yes | Yes | - | 123dev@test.com | 123dev@test.com | 888123dev@test.com |

# How the called number is determined

In SIP calls the called number is always presented in a standard format (whether numeric or alphanumeric). In H.323 calls the endpoints can signal a called number in multiple formats. For the IP to ISDN dial plan it is useful (particularly in the case of H.323) to know how the ISDN gateway analyses the incoming called number to determine the called number value to be passed to the dial plan, as listed below:

Numeric values in this context may contain digits 0-9, commas, and the # and * dialing symbols.

- [H.323 only] If the Q.931 called party field is present and is numeric, that value is always used.
- [H.323 only] If the dialed digits field is present in the destination address, that value is used.

Technically, the endpoint request can contain multiple instances of address fields. If multiple dialed digits fields are present in the destination address, only the first dialed digits field is used and any other instances are ignored.

- If any SIP URI or H.323 ID or H.323 URL ID fields are present which are a numeric string or a numeric prefix followed by an @ symbol (for example, *12345@test.com*) the numeric part of the first such field is used, but the alphabetic part is discarded. So *12345@test.com* in an H.323 ID field, results in called number *12345*. (This is significant for dial plan management, as incoming alphanumeric IDs will be treated as matching rules that require digit-only numbers.)
- Any SIP URI or H.323 ID or H.323 URL ID that has alphabetic characters before an @ symbol is ignored and treated as a null value.
- Any SIP URI or H.323 ID or H.323 URL ID that is exclusively alphabetic is also ignored and treated as a null value.
- If no acceptable value is found, the called number will be null.

## Related topics

- Configuring dial plan rules [p.127]
- Understanding the dial plan [p.115]
- Dial plan syntax [p.120]
- Managing the dial plan [p.125]
- Example dial plan rules [p.139]
- Displaying and testing the dial plan [p.124]

# Dial plan syntax

Call numbers in both the condition and action settings for dial plan rules can be defined as a specific number or expressed as a pattern using special characters.

## Syntax for conditions

This syntax can be used to define values for **Called number matches** and **Calling number matches** in rule conditions:

| Syntax | Purpose | Examples |
|---|---|---|
| Numbers 0 to 9 | Specifies digits to be matched. | To match calls to "001234", type **001234**<br>The condition will match that and only that number. |
| S | Denotes an asterisk/star symbol (*) | To match calls to "**1234", type **SS1234**<br>The condition will match that and only that number. |
| P | Denotes a pound/hash symbol (#) | To match calls to "#1234", type **P1234**<br>The condition will match that and only that number. |
| D | Matches any digit and/or the * and # symbols (wildcard character). | To match any number that starts "623" followed by exactly two more digits, type **623DD**<br>The condition will match "62300", "62323", "62355", "62399" "623*#", and so on, but not "623" or "623233". |
| ? | Matches once or zero times (repeat character).<br>Useful with the **D** wildcard if the expected number length is unknown. | To match one 6 or no 6s, type **6?**<br>The expression: **67800D?** will match "67800" and "678004" but not "67800666". |
| + | Matches once or more times (repeat character). | To match at least one 5, but possibly more, type **5+** |
| * | Matches zero or more times (repeat character).<br>Useful with the **D** wildcard. For example, **D*** means match any digit, any number of times. | To match any number that starts "01", has any amount of digits in the middle, and ends with "5", type **01 D* 5** |
| () | Indicates substitution groups.<br>To include any of the incoming called digits into the outgoing called number, enclose each substitution group in parentheses.<br>To include the complete number, there is no need to enclose the whole expression in parentheses. | To match any number that starts "678", followed by a number of other digits, and to have the final digits form part of the called number, type **678 (D*)**<br>This will match "6780000", "678123", "6789999", and so on. It will not match "775000". |

| | | |
|---|---|---|
| () | [This option only applies if your configuration is in leased line mode.]<br>Indicates substitution groups in leased-line mode.<br>To substitute 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 parentheses.<br>To include the complete number, there is no need to enclose the whole expression in parentheses. | For an incoming number that starts "678", followed by two digits, where you want to use the penultimate digit as the outgoing port number and the final digit as the outgoing leased line group, type **`678 (D)(D)`**. This will match incoming called digits "67812".<br>For an incoming number that starts "987", followed by the port number, the leased line group number, and a TCS-4 extension of four or more digits, type **`987(D)(D)(DDDD+)`**. This will match incoming digits "987235678" and "98733456789.<br>See also Example dial plan rules in leased line mode [p.145]. |

# Syntax for actions

This syntax can be used to define a value for **Call this number** in rule actions:

| Syntax | Description | Examples |
|---|---|---|
| Letters and numbers for address | To call a specific number, type the number required. Or for ISDN to IP calls you can specify an IP address, hostname, H.323 ID, or H.323 URI. (In configurations that use a gatekeeper, calls to an H.323 URI are supported only if the gatekeeper itself supports URI dialing.)<br>IPv6 addresses must be enclosed in brackets [ ]. | To specify that when this rule is invoked, the MCU with hostname "my_mcu" is called, type **`my_mcu`**<br>Or suppose the domain "test.com" has an H.323 SRV (service) record set up. To call the H.323 video endpoint with URI "example.person@test.com", type **`example.person@test.com`**. (Information about domain (DNS) SRV records is available in RFC 2782.) |
| ! | [ISDN to IP] To call a specific extension, separate the IP address or hostname from the extension by typing an exclamation mark (!).<br>You cannot use the ! extension separator with H.323 IDs. | 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 digits from the incoming called number in the outgoing number, use one or more of the following substitutions:<br>*$A* — substitutes the entire incoming called number.<br>*$B* — substitutes the entire calling number.<br>*$1* to *$9* — substitutes the digits enclosed in the *n*th set of parentheses of the condition.<br>To specify a dollar sign as part of an actual SIP or H.323 address string rather than as an expression, type two dollar symbols in succession ($$). They will be interpreted as a single dollar in the string. | Say you want all calls that match condition "55 (DDDD)" to call the MCU "my_mcu" and join the conference with an identifier that matches "(DDDD)". To do this, type **`my_mcu ! 00 $1`**<br>Any incoming call to "551234" will attempt to join the conference with numeric identifier "001234" on "my_mcu".<br>If the substitution creates an empty number, the call is rejected. In this example, an incoming call to 55 will result in an empty substitution. |
| ! | [IP to ISDN] For video calls, this delimiter is used in an "ISDN bridge between IP islands" when you want to use TCS-4 extensions. In this case use the ! before the 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 [p.139]. |
| ! | [IP to ISDN ] For telephone calls, this delimiter is used where there is a number to dial which must be followed by DTMF tones. It allows you to configure the dial plan to start sending DTMF tones after a telephone call has connected. | This delimiter is useful to manage call routing in the case of calls through the ISDN gateway to a device which may be behind another gateway that only supports DTMF. The caller does not need to enter DTMF codes manually on the phone keypad and the call can be re-routed automatically using the ISDN gateway dial plan. To do this, in the settings for *Call this number*, type the number to call, followed by an exclamation mark (!) and then the DTMF extension. |
| , | [IP to ISDN] 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 if more than one set of DTMF tones must be entered. For example, an automated operator system that requires the caller to choose a menu option, and then transfers the call to an audio conferencing system, which in turn requires the caller to enter a conference ID. |

## Related topics

- Configuring dial plan rules [p.127]
- How call number matching works [p.117]
- Example dial plan rules [p.139]
- Displaying and testing the dial plan [p.124]

- Making calls with the gateway [p.11]
- Using the gateway for voice-only calls [p.12]

# Displaying and testing the dial plan

Go to **Dial plan > IP to ISDN** or **Dial plan > ISDN to IP** as required. The dial plan rules are listed with a summary of the settings for each rule. An asterisk against a rule indicates that it has recently been moved in the list.

The dial plan test facility can be used to see how the set of rules configured for the dial plan acts on a particular number:

1. In the **IP to ISDN** dial plan or **ISDN to IP** dial plan as appropriate, go to the **Test dial plan** section.
2. [IP to ISDN only] For **Incoming protocol**, select a protocol type to be applied for the test of the incoming part of the call.
3. In **Called number**, enter the outgoing destination number to test against the dial plan.
   This represents the number a caller is trying to reach.
4. In **Calling number**, enter the incoming calling number to test against the dial plan.
   This represents the incoming originating number for a caller.
5. For **Call type**, select whether the call should be tested as a video or telephone call.
6. Click **Test number**.

The **Test Result** section displays the number tested, the rule that the condition matched, the outcome (whether the call was rejected or the number that has been dialed in response), and the bandwidth.

**CAUTION:** The test facility does not take into account the device-wide settings for your local configuration. A successful result only indicates that the dial plan is valid; it does not mean that the dial plan will necessarily work with the actual configuration of the ISDN gateway.

## Related topics

- Configuring dial plan rules [p.127]
- Making calls with the gateway [p.11]
- Example dial plan rules [p.139]
- Dial plan syntax [p.120]
- Using the auto attendant [p.17]

# Managing the dial plan

Go to **Dial plan > IP to ISDN** or **Dial plan > ISDN to IP** as required.

## Changing the rule order

You can change the order of rules by using drag-and-drop or the up / down links to move rules around in the dial plan list.

## Adding, modifying and deleting rules

### Adding a dial plan rule

1. In the dial plan list, do one of the following:
   a. Click **Add rule**.
   b. Or to create a new rule by copying, open an existing rule and use **Copy rule**.
2. Type a name in the **Rule name** field.
   Leave the **UID** field blank. The ISDN gateway auto-populates this field with a unique ID for the rule.
3. Complete the relevant settings for the dial plan rules (see the tables below for guidance).
   a. Select at least one **Condition** and define any associated settings.
   b. Select an **Action** and define its associated settings.
   c. Set any options you want (such as bandwidth or encryption requirements).
   d. Optionally specify the **Codecs allowed** for this rule. In the case of the *Custom codecs choices* option, select or deselect the individual codecs as required.
4. Click **Add rule** again to confirm the new rule.

### Updating an existing rule

1. In the dial plan list, click the relevant rule name to open the rule.
2. Modify the details as required.
3. Click **Update rule**.

### Creating a new rule from an existing one

1. In the dial plan list, click the relevant rule name to open the rule.
2. Click **Copy rule**.
   A new rule is created with the existing parameters.
3. Modify the settings for the new rule as required (see the tables below).
4. Click **Add rule**.

### Deleting rules

1. In the dial plan list, select one or more rules as required.
2. Click **Delete selected rules**.

## Related topics

- Configuring dial plan rules [p.127]
- Displaying and testing the dial plan [p.124]
- Example dial plan rules [p.139]
- Understanding the dial plan [p.115]
- How call number matching works [p.117]
- Dial plan syntax [p.120]

# Configuring dial plan rules

To work with dial plan rules, go to **Dial plan > IP to ISDN** or **Dial plan > ISDN to IP** as required. If the ISDN gateway is in leased line mode, see instead Configuring dial plan rules in leased line mode [p.133].

Settings for dial plan rules are grouped as follows:

- Condition settings [p.127]
- Action settings [p.128]
- Options (advanced settings) [p.130]
- Codec settings [p.132]

Some settings apply only to the **IP to ISDN** or **ISDN to IP** dial plan respectively, or are context specific. These settings are available in the user interface only if you are working in the relevant dial plan and context (for example, if you select H.323 then SIP-related settings are unavailable).

## Condition settings

These settings specify the condition for the dial plan rule, which must be matched before the rule will be applied to a call. Rules are typically defined to match against the called number (outgoing number) but you can also match against the incoming calling number, and the incoming call protocol and call type.

| Condition | Description |
|---|---|
| **Incoming protocol** | [IP to ISDN only] Specifies a protocol (*Any*, *H.323*, or *SIP*) that the incoming call must match for this rule to be applied to the call. |
| **Incoming call type** | Specifies a call type that the incoming call must match for this rule to be applied to the call. Allowed values are *Any*, *Video only*, *H.323-Telephone only* for IP to ISDN; or *Any*, *Video only*, *Telephone only* for ISDN to IP. |

| | |
|---|---|
| **Called number matches** | Specifies a value that the called number must match for this rule to be applied to the call (the called number is the number the caller is trying to reach):<br>*Any* — matches any incoming call (even if the called number is unknown or unavailable). If this rule is used, it should usually be relatively low in the dial plan list to match numbers that are not recognized by more specific rules higher in the list.<br>*None* — for ISDN calls this condition matches when the called number is unknown or unavailable; for IP calls it matches when the caller uses the IP address or hostname of the ISDN gateway.<br>*Custom* — matches to the number that you specify in the adjoining text field. The custom number can be defined as:<br>■ A specific number that you simply enter directly in the field. For example, to match calls to "001234", type `001234`. The condition will match that and only that number.<br>■ A derived number obtained by manipulating the called number in accordance with a sequence of digits and special characters that you enter in this field. Special characters can be used in any combination to denote asterisk/star and pound/hash dialing keys, to repeat or to match particular digits, and to include — substitute — portions of the incoming called digits. Special characters are detailed in How call number matching works [p.117].<br>**CAUTION:** If the called number is alphanumeric in the form <*numeric ID*>@<*domain*>, only the numeric ID before the @ symbol is checked against the dial plan. The gateway ignores the remainder of the number. For example, with an H.323 ID of *12345@test.com*, the '12345' part is checked but the '@test.com' part is ignored. So any alphanumeric called numbers of this type (H.323 IDs, H.323 URL IDs, or SIP URIs with a numeric prefix before the @) are treated as all-digit values when the gateway checks them for a dial plan match. It follows that **such numbers will match any dial plan rules that require digit-only numbers**, and assuming any other conditions are met the gateway will place the outgoing call. |
| **Calling number matches** | The settings here are identical to **Called number matches**, but apply to the originating caller's number (incoming part of the call) rather than to the outgoing called number that the caller is trying to reach. You can define the condition to match to a custom number, or to any number or none. As with **Called number matches** the custom number can be a specific number or derived by manipulating the calling number (see How call number matching works [p.117]).<br>**CAUTION:** If the calling number is alphanumeric in the form <*numeric ID*>@<*domain*>, only the numeric ID is checked against the dial plan. The gateway ignores the remainder of the number. For example, with an H.323 ID of *12345@test.com*, the '12345' part is checked but the '@test.com' part is ignored. So any calling numbers of this type (including alphanumeric H.323 IDs / H.323 URL IDs / SIP URIs with a numeric prefix) are treated as all-digit values when the gateway checks them for a dial plan match. It follows that **such numbers will match any dial plan rules that require digit-only numbers**, and assuming any other conditions are met the gateway will place the outgoing call. |

# Action settings

These settings specify the action to be applied to the outgoing part of any call that matches the rule conditions.

| Action | Description |
|---|---|

| | |
|---|---|
| **Action** | Specifies how the outgoing part of the call should be handled if this rule is invoked.<br>*Reject the call* — the call will be terminated and the outgoing part of the call will not be established.<br>*Enter the auto attendant* — the call will be connected to the auto attendant. The ISDN gateway applies the dial plan to numbers dialed in the auto attendant. You can optionally specify the protocol and call type to use (see below).<br>*Enter the auto attendant + TCS-4* — the call will enter the auto attendant and send 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, but it may display briefly with the TCS-4 extension shown. You can optionally specify the protocol and call type to use (see below). For more information about using TCS-4 see Example dial plan rules [p.139].<br>*Place call* — the outgoing part of the call will be placed to the number you specify, in accordance with any other settings or options that you define for this action. |
| **Protocol** | [ISDN to IP only] Specifies whether the outgoing part of the call should use H.323 or SIP. |
| **Call type** | Specifies the call type for the outgoing part of the call.<br>**Note:** In the IP to ISDN dial plan these settings are overriden if the device-wide **Max outgoing ISDN call rate** field is set to *Telephone* (**Settings > ISDN** page). In such cases the outgoing part is always placed as a telephone call.<br>*Use incoming call type* — sets the call type to match that for the incoming call.<br>*Telephone* — sets the call type for a speech-only phone call.<br>*Video using BONDING* — sets the call type for a typical video call (the default option).<br>*Video using H.221 aggregation (legacy)* [IP to ISDN only] — only select this call type if your deployment has legacy ISDN endpoints that need this feature. |

| | |
|---|---|
| **Call this number** | Specifies the number to use for the outgoing part of the call if this rule is invoked. For IP to ISDN rules only digits and the asterisk/star (*) and pound/hash (#) symbols are permitted. For ISDN to IP rules the number string can include alphanumerics.<br>*Original* — the call will be placed to the original called number. For example, an incoming ISDN call to "54321" will result in an outgoing call placed over IP to "54321".<br>*Custom* — the call will be placed to the number you define here, which can be defined as any combination of the following:<br>■ To specify a particular number, enter the number directly in the field as any combination of digits and * or # symbols.<br>■ For ISDN to IP rules you can specify an IP address, hostname, H.323 ID, H.323 URI, or SIP URI. Enclose IPv6 addresses in brackets [ ].<br>Example 1: To call the MCU with hostname "my_mcu", type **`my_mcu`**.<br>Example 2: Assume the domain "cisco.com" has an H.323 service (SRV) record set up. To call an H.323 endpoint in that domain with URI "example.person@cisco.com", type **`example.person@cisco.com`**<br>■ To call a specific extension, separate the IP address or hostname from the extension with an exclamation mark (!). For 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**. The ! separator cannot be used after an H.323 ID or SIP URI.<br>■ To include any digits from the incoming called number or calling number in the outgoing number, specify a substitution. Substitutions are specified by the dollar sign ($) followed by an index:<br>○ $A substitutes the entire incoming called number in the case of all-numeric values. In the case of alphanumeric values the gateway modifies the numbers during the dial plan matching, and for called numbers the *modified* value is substituted here, *not* the original number. Depending on the original alphanumerics format the modified value may be all-numeric or null (for details see How call number matching works [p.117]).<br>○ $B substitutes the entire original calling number (you could also select the **Use calling number** option below to do this).<br>○ $1, $2, $3 ... through to $9 substitutes the digits enclosed in the relevant set of parentheses of the condition.<br>Example 1: Assume that for calls which match the condition "55 (DDDD)" you want to set an action to call the MCU named "my_mcu" and join the call to the conference with an identifier that matches "(DDDD)". To do this you would type **`my_mcu ! 00 $1`**. The outcome is that an incoming call to "551234" (for example) will attempt to join a conference with numeric identifier "001234" on the MCU named "my_mcu".<br>Example 2: Assume an IP to ISDN dial plan rule, for calls which match the condition (D*)P(D*). You set an action to call **`$1!$2`**. This will match any numbers which contain a pound/hash symbol (#). The number before the pound/hash symbol will be used for the phone number and the number after the symbol will be used as the TCS-4 extension.<br>A further example of using TCS-4 is given in Example dial plan rules [p.139]. |
| **Call these numbers** | [IP to ISDN only] This setting is available if you select the *Video using H.221 aggregation (legacy)* call type. Take care to enter the correct number of phone numbers. For example, if you select 3 x 64 kbps as the call bandwidth, you must enter three numbers here.<br>You can use the same substitution methods as described above for **Call this number**. |

# Options (advanced settings)

These optional settings can be used to modify the basic action for the rule.

| Option | Description |
|---|---|
| **Use calling number** | Use this option to manipulate or replace the originating caller's number before it is forwarded to the IP or ISDN side (typically to provide a simplified callback mechanism or to supply calling party identification where the caller ID is absent). For ISDN to IP rules the string can include alphanumerics. For IP to ISDN rules only digits are permitted — although if the original calling number is alphanumeric, it can be passed on by substitution as described below.<br>*Original* — uses the caller's number as is with no changes.<br>*Custom* — derives a new number in accordance with the settings you enter here.<br>■ To append digits to the original number, type the digits.<br>■ For ISDN to IP rules, you can append an IP address, hostname, H.323 URI, or SIP URI. Enclose IPv6 addresses in brackets [ ].<br>■ To include all or some of the original caller number digits in the forwarded number, use one or more dollar ($) substitutions:<br>○ **$B** substitutes the entire original calling number.<br>○ $A substitutes the entire incoming called number in the case of all-numeric values. In the case of alphanumeric values the gateway modifies the numbers during the dial plan matching, and for called numbers the *modified* value is substituted here, *not* the original number. Depending on the original alphanumerics format the modified value may be all-numeric or null (for details see How call number matching works [p.117]).<br>○ **$1**, **$2**, **$3** ... through to **$9** substitutes the digits enclosed in the relevant set of parentheses of the associated condition. |
| **Outgoing transport** | For SIP calls, if you don't want to use the global SIP proxy/trunk setting on the **Settings > SIP** page, you can explicitly select a transport protocol (TCP, UDP, or TLS) for outgoing call control. The selected protocol must be enabled on the **Network > Services** page. |
| **Restrict (56k)** | Only enable this option if your network requires it. When enabled, for calls that match this rule the ISDN gateway makes the outgoing ISDN call in restricted 56k mode. (If the endpoint only supports 64k, the ISDN gateway drops the call.) |
| **Fall back to telephone** | [IP to ISDN only] Enable this option to have the ISDN gateway retry a failed outgoing video call as a telephone call, in the case of the following disconnect cause codes:<br>■ *0x41* Bearer capability not implemented<br>■ *0x58* Incompatible destination<br>Fallback only occurs on call setup. It is not attempted after a second channel connects. |
| **Maximum call bandwidth** | You can select a maximum bandwidth for the call. If no value is selected this setting defaults to the maximum ISDN call rate for the device (**Settings > ISDN** page). The maximum bandwidth available to a call is ultimately limited to the global value, regardless of any higher value specified here. |

| | |
|---|---|
| **Encryption settings** | Use these options to enable transparent encryption, or to specify encryption separately as optional or required for the IP leg and the ISDN leg of the call respectively. For the ISDN leg you can explicitly disable encryption. |
| | **Use transparent encryption** When selected, the ISDN gateway will simulate point-to-point encryption. It sets the encryption state (enabled/disabled) used on the received call as that to be used on the outgoing call (that is, it attempts 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 on both sides of the ISDN gateway but then the incoming call stops being encrypted for some reason. In such cases the outgoing part of the call will also drop encryption and both callers will know that the call is no longer encrypted. |
| | **IP encryption / ISDN encryption** Select *Required* in the appropriate checkboxes if you always want the IP and/or ISDN part of a call to be encrypted. Or select *Optional* if encryption is only to be used to endpoints that support it. For the ISDN leg you can select *Disable* to explicitly disallow encryption for the ISDN part of the call.<br>Encryption must also be enabled globally on the **Settings > Encryption** page.<br>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 guaranteed. If *Optional* is selected and the endpoint supports encryption, then a call may start even before encryption can be guaranteed — but will use encryption as soon as possible subsequently. |
| **Place call on** | [IP to ISDN only] Use this option if you want to specify the ISDN port(s) on which the outgoing part of the call may be placed. They will be used in the port search order specified on the **Settings > ISDN** page. |
| **Receive call on** | [ISDN to IP only] Use this option if you want to specify the port(s) to advertise to the calling endpoint. These ports may be used to complete subsequent calls from the calling end. They will be used in the port search order specified on the **Settings > ISDN** page. |

# Codec settings

| Field | Description |
|---|---|
| **Codecs allowed** | We recommend leaving this option to the default setting, unless you need to change it to fix connection problems with older endpoints when certain codecs are enabled (that is, even though the endpoint supports the codecs in question). If you need to change this setting, select one of the following options:<br>■ *Custom codec choices* to specify manually which of the codecs allowed at device level are allowed for this rule.<br>■ *Safe codec choices* to limit the codecs allowed for this rule to G.711 and H.261 video only. |

## Related topics

- Displaying and testing the dial plan [p.124]
- Managing the dial plan [p.125]
- How call number matching works [p.117]
- Dial plan syntax [p.120]
- Example dial plan rules [p.139]
- Understanding the dial plan [p.115]

# Configuring dial plan rules in leased line mode

To work with dial plan rules when the ISDN gateway is in leased line mode, go to **Dial plan > IP to ISDN** or **Dial plan > ISDN to IP** as required and follow the instructions below. The options differ from standard settings, as the absence of a D-channel means that no number is sent over the leased line call.

Settings for dial plan rules are grouped as follows:

- Condition settings [p.133]
- Action settings [p.135]
- Options (advanced settings) [p.136]
- Codec settings [p.138]

Some settings apply only to the **IP to ISDN** or **ISDN to IP** dial plan respectively, or are context specific. These settings are available in the user interface only if you are working in the relevant dial plan and context. For example, if you select H.323 then SIP-related settings are unavailable.

## Condition settings

These settings specify the condition for the dial plan rule, which must be matched before the rule will be applied to a call.

| Condition | Description |
|---|---|
| **Incoming protocol** | [IP to ISDN only] Specifies a protocol (*Any*, *H.323*, or *SIP*) that the incoming call must match for this rule to be applied to the call. |
| **Incoming call type** | [IP to ISDN only] Specifies a call type that the incoming call must match for this rule to be applied to the call. Allowed values are *Any*, *Video only*, or *H.323-Telephone only*. |

| | |
|---|---|
| **Called number matches** | [IP to ISDN only] Specifies a value that the called number must match for this rule to be applied to the call (the called number is the number the caller is trying to reach):<br>*Any* — matches any incoming call (even if the called number is unknown or unavailable). If this rule is used, it should usually be relatively low in the dial plan list to match numbers that are not recognized by more specific rules higher in the list.<br>*None* — [IP to ISDN only] this condition matches when the caller uses the IP address or hostname of the ISDN gateway.<br>*Custom* — matches to the number that you specify in the adjoining text field. The custom number can be defined as:<br>■ A specific number that you simply enter directly in the field. For example, to match calls to "001234", type **`001234`**. The condition will match that and only that number.<br>■ A derived number obtained by manipulating the called number in accordance with a sequence of digits and special characters that you enter in this field. Special characters can be used in any combination to denote star and pound/hash dialing keys, to repeat or to match particular digits, and to include (substitute) portions of the incoming called digits (for details see How call number matching works [p.117]).You can also use substitution groups to include any of the incoming called digits as the port number, leased line group, and optional TCS-4 extension for the outgoing call.<br>**CAUTION:** If the called number is alphanumeric in the form <*numeric ID*>@<*domain*>, only the numeric ID before the @ symbol is checked against the dial plan. The gateway ignores the remainder of the number. For example, with an H.323 ID of *12345@test.com*, the '12345' part is checked but the '@test.com' part is ignored. So any alphanumeric called numbers of this type (H.323 IDs, H.323 URL IDs, or SIP URIs with a numeric prefix before the @) are treated as all-digit values when the gateway checks them for a dial plan match. It follows that **such numbers will match any dial plan rules that require digit-only numbers**, and assuming any other conditions are met the gateway will place the outgoing call. |
| **Calling number matches** | [IP to ISDN only] The settings here are identical to **Called number matches**, but apply to the originating caller's number (incoming part of the call) rather than to the (outgoing) called number that the caller is trying to reach. You can define the condition to match to a custom number, or to any number or none. As with **Called number matches** the custom number can be a specific number or derived by manipulating the calling number (for details see How call number matching works [p.117]).<br>**CAUTION:** If the calling number is alphanumeric in the form <*numeric ID*>@<*domain*>, only the numeric ID is checked against the dial plan. The gateway ignores the remainder of the number. For example, with an H.323 ID of *12345@test.com*, the '12345' part is checked but the '@test.com' part is ignored. So any calling numbers of this type (including alphanumeric H.323 IDs / H.323 URL IDs / SIP URIs with a numeric prefix) are treated as all-digit values when the gateway checks them for a dial plan match. It follows that **such numbers will match any dial plan rules that require digit-only numbers**, and assuming any other conditions are met the gateway will place the outgoing call. |
| **Match calls incoming on port** | This condition matches calls that arrive on the specified port. |
| **Leased line group** | This condition matches calls that use the specified leased line group. |

# Action settings

These settings specify the action to be applied to the outgoing part of any call that matches the rule conditions.

| Action | Description |
|---|---|
| **Action** | Specifies how the outgoing part of the call should be handled if this rule is invoked.<br>*Reject the call* — the call will be terminated and the outgoing part of the call will not be established.<br>*Enter the auto attendant* [ISDN to IP only] — the call will be connected to the auto attendant. The ISDN gateway applies the dial plan to numbers dialed in the auto attendant. You can optionally specify the protocol and call type to use (see below).<br>*Enter the auto attendant + TCS-4* [ISDN to IP only] — the call will enter the auto attendant and send 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, but it may display briefly with the TCS-4 extension shown. You can optionally specify the protocol and call type to use, as described below. For more information about using TCS-4 see Example dial plan rules in leased line mode [p.145].<br>*Place call* [ISDN to IP only] — the outgoing part of the call will be placed to the number you specify, in accordance with any other settings or options that you define for this action. |
| **Call port** | [IP to ISDN only] Specifies a port number for the outgoing ISDN call. You can specify digits or use substitution groups from the **Called number matches** setting for the associated condition. |
| **Leased line group** | [IP to ISDN only] Specifies a leased line group for the outgoing ISDN call. You can specify digits or use substitution groups from the **Called number matches** setting for the associated condition. |
| **Protocol** | [ISDN to IP only] Specifies whether the outgoing part of the call should use H.323 or SIP. |

**Call this number**

Specifies the number to use for the outgoing part of the call if this rule is invoked. For IP to ISDN rules only digits and the asterisk/star (*) and pound/hash (#) symbols are permitted. For ISDN to IP rules the number string can include alphanumerics.

*Original* — the call will be placed to the original called number. For example, an incoming ISDN call to "54321" will result in an outgoing call placed over IP to "54321".

*Custom* — the call will be placed to the number you define here, which can be defined as any combination of the following:

- To specify a particular number, enter the number directly in the field as any combination of digits and * or # symbols.
- For ISDN to IP rules you can specify an IP address, hostname, H.323 ID, H.323 URI, or SIP URI. Enclose IPv6 addresses in brackets [ ].

  Example 1: To call the MCU with hostname "my_mcu", type **`my_mcu`**.

  Example 2: Assume the domain "cisco.com" has an H.323 service (SRV) record set up. To call an H.323 endpoint in that domain with URI "example.person@cisco.com", type **`example.person@cisco.com`**
- To call a specific extension, separate the IP address or hostname from the extension with an exclamation mark (!). For 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**. The ! separator cannot be used after an H.323 ID or SIP URI.
- To include any digits from the incoming called number or calling number in the outgoing number, specify a substitution. Substitutions are specified by the dollar sign ($) followed by an index:
  - For IP to ISDN rules, $A substitutes the entire incoming called number in the case of all-numeric values. In the case of alphanumeric values the gateway modifies the numbers during the dial plan matching, and for called numbers the *modified* value is substituted here, *not* the original number. Depending on the original alphanumerics format the modified value may be all-numeric or null (for details see How call number matching works [p.117]).
  - For IP to ISDN rules, $B substitutes the entire original calling number (you could also select the **Use calling number** option below to do this).
  - For IP to ISDN rules, $1, $2, $3 ... through to $9 substitute the digits enclosed in the relevant set of parentheses of the associated condition. For ISDN to IP rules, $1 and $2 substitute the port and group respectively and the other dollar substitutions do not apply.

  Example 1: Assume that for calls which match the condition "55 (DDDD)" you want to set an action to call the MCU named "my_mcu" and join the call to the conference with an identifier that matches "(DDDD)". To do this you would type **`my_mcu ! 00 $1`**. The outcome is that an incoming call to "551234" (for example) will attempt to join a conference with numeric identifier "001234" on the MCU named "my_mcu".

  Example 2: Assume an IP to ISDN dial plan rule, for calls which match the condition (D*)P(D*). You set an action to call **`$1!$2`**. This will match any numbers which contain a pound/hash symbol (#). The number before the pound/hash symbol will be used for the phone number and the number after the symbol will be used as the TCS-4 extension.

# Options (advanced settings)

These optional settings can be used to modify the basic action for the rule.

| Option | Description |
|---|---|

| | |
|---|---|
| **Use calling number** | Use this option to manipulate or replace the originating caller's number before it is forwarded to the IP or ISDN side (typically to provide a simplified callback mechanism or to supply calling party identification where the caller ID is absent). For ISDN to IP rules the string can include alphanumerics. For IP to ISDN rules only digits are permitted — although if the original calling number is alphanumeric, it can be passed on by substitution as described below.<br>*Original* — uses the caller's number as is with no changes.<br>*Custom* — uses the caller's number to derive a new number in accordance with the settings you enter here.<br>■ You can append digits to the original number by typing them directly into the field.<br>■ For ISDN to IP rules, you can append an IP address or hostname. An IPv6 address must be enclosed in brackets [ ].<br>■ To include digits from the caller's number in the outgoing number, specify a substitution. Substitutions are specified by the dollar sign ($) followed by an index:<br>○ For IP to ISDN rules, $B substitutes the entire original calling number.<br>○ For IP to ISDN rules, $A substitutes the entire incoming called number in the case of all-numeric values. In the case of alphanumeric values the gateway modifies the numbers during the dial plan matching, and for called numbers the *modified* value is substituted here, *not* the original number. Depending on the original alphanumerics format the modified value may be all-numeric or null (for details see How call number matching works [p.117]).<br>○ For IP to ISDN rules, $1, $2, $3 ... through to $9 substitute the digits enclosed in the relevant set of parentheses of the associated condition. For ISDN to IP rules, $1 and $2 substitute the port and group respectively and the other dollar substitutions do not apply. |
| **Outgoing transport** | For SIP calls, if you don't want to use the global SIP proxy/trunk setting (**Settings > SIP** page), you can explicitly select a transport protocol (TCP, UDP, or TLS) for outgoing call control. The selected protocol must be enabled on the **Network > Services** page. |
| **TCS-4 extension digits (optional)** | Specify any TCS-4 extension to be used for calls that match this rule. You can type the extension or specify a substitution group to use digits from the original called number as the TCS-4 extension. For example, if you specify `99(D+)` for **Called number matches**, and `$1` for the TCS-4 extension, then a call to 991234 will use "1234" as the TCS-4 extension. |
| **Restrict (56k)** | Only enable this setting if your network requires it. When enabled, for calls that match this rule the ISDN gateway makes the outgoing ISDN call in restricted 56k mode. (If the endpoint only supports 64k, the ISDN gateway drops the call.) |

| | |
|---|---|
| **Encryption settings** | You can use these settings to enable transparent encryption, or to specify encryption separately as optional or required for the IP leg and the ISDN leg of the call respectively. For the ISDN leg you can also explicitly disable encryption. |
| | **Use transparent encryption** When selected, the ISDN gateway will simulate point-to-point encryption. It sets the encryption state (enabled/disabled) used on the received call as that to be used on the outgoing call (that is, it attempts 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 on both sides of the ISDN gateway but then the incoming call stops being encrypted for some reason. In such cases the outgoing part of the call will also drop encryption and both callers will know that the call is no longer encrypted. |
| | **IP encryption / ISDN encryption** Select *Required* in the appropriate checkboxes if you always want the IP and/or ISDN part of a call to be encrypted. Or select *Optional* if encryption is only to be used to endpoints that support it. For the ISDN leg you can select *Disable* to explicitly disallow encryption for the ISDN part of the call.<br>Encryption must also be enabled globally in the **Settings > Encryption** page.<br>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 guaranteed. If *Optional* is selected and the endpoint supports encryption, then a call may start even before encryption can be guaranteed — but will use encryption as soon as possible subsequently. |

# Codec settings

| Field | Description |
|---|---|
| **Codecs allowed** | We recommend leaving this option to the default setting, unless you need to change it to fix connection problems with older endpoints when certain codecs are enabled (that is, even though the endpoint supports the codecs in question). If you need to change this setting, select one of the following options:<br>■ *Custom codec choices* to specify manually which of the codecs allowed at device level are allowed for this rule.<br>■ *Safe codec choices* to limit the codecs allowed for this rule to G.711 and H.261 video only. |

## Related topics

- Displaying and testing the dial plan [p.124]
- Managing the dial plan [p.125]
- How call number matching works [p.117]
- Dial plan syntax [p.120]
- Example dial plan rules in leased line mode [p.145]

# Example dial plan rules

This topic provides examples of how to configure dial plan rules.

## Allocating bandwidth for IP to ISDN calls

You can use rules to limit bandwidth for calls to particular numbers or to allocate more bandwidth to priority calls. For example, to allocate maximum bandwidth to calls to the chief executive, set a **Condition** that matches calls to the relevant number, set the **Action** to call with the original called number, and set the **Maximum call bandwidth** to the highest available value.

As cost is an issue with calls to the ISDN network, you may want to provide users with a list of prefixes they can use to control the bandwidth for their calls. This example gives some rules 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. In the absence of any further rules, any calls that do not match the listed conditions will be rejected (the default behavior of the dial plan).

| # | Condition | Action | Call type | Bandwidth | Description |
|---|---|---|---|---|---|
| 0 | Called number matches `552 (D*)` | Call this number `$1` | Video using BONDING | 128 kbps | This rule allocates 128 kbps (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. So 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 using BONDING | 192 kbps | This rule allocates 192 kbps (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. So 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 using BONDING | 512 kbps | This rule allocates 512 kbps (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. So an incoming call to "5585678" will cause an outgoing call allocated with eight channels to be placed to "5678". |

## Allocating bandwidth for ISDN to IP calls

This example limits the bandwidth available for incoming ISDN calls, which can be useful to limit the network resources available to individual calls.

| # | Condition | Action | Call type | Bandwidth | Description |
|---|---|---|---|---|---|
| 0 | Called number matches "Any" | Call this number (Original) | Video using BONDING | 384 kbps | This rule forwards all calls to the dialed number, with a bandwidth of 384 kbps. |

## Forwarding ISDN calls to an operator or a conference

This example **ISDN to IP** dial plan 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.

| # | Condition | Action | Call type | Bandwidth | Description |
|---|---|---|---|---|---|
| 0 | Called number matches `D+ 0000` | Call this number `10.2.1.10` | Video using BONDING | 384 kbps | 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 using BONDING | 384 kbps | 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 the `D` wildcard matches the * and # symbols 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

This **IP to ISDN** dial plan specifies how IP telephone calls (voice-only calls) will be forwarded to the ISDN network. Some IP endpoints do not allow users to specify the call type, so the example shows how users can dial a prefix to denote a telephone call rather than a video and voice call. It also shows how to use the dial plan to specify DTMF tones to be dialed after the call has been answered.

| # | 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. So 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.<br>In this example, the audio bridge will answer the call. After a two second pause the gateway sends the DTMF tones for the conference ID (555). These are the digits that follow the exclamation mark (!) delimiter (the delimiter 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 gateway sends the PIN (888). The audio bridge requires a caller to press pound/hash after the ID and the PIN, and these are represented with 'P'. |
| 2 | Called number matches "Any" | Call this number (Original) | Video using BONDING | 128 kbps | 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 a simplified callback mechanism

These dial plan rules provide an easy method for users who miss an incoming call to call back the originating caller. This example assumes that an H.323 endpoint "333" tries to call an ISDN endpoint "222". The gateway has ISDN address "051" and H.323 prefix "054".

In the **IP to ISDN** dial plan, set up this rule:

| # | Condition | Action | Use calling number |
|---|---|---|---|
| | Called number matches `054(D*)`<br>Calling number matches / Incoming protocol / Incoming call type "Any" | Call this number `$1` | `051 $B` |

In the **ISDN to IP** dial plan, set up this rule:

| # | Condition | Action | Use calling number | Protocol |
|---|---|---|---|---|
| | Called number matches `051(D*)`<br>Calling number matches / Incoming call type "Any" | Call this number `$1` | `054 $B` | H.323 |

The destination number requested by the H.323 endpoint arrives at the gateway as "054222". The gateway will call 222 as 051333 (**Use calling number** = `051 $B`). This means that the user at ISDN endpoint 222 can simply press **Redial** to call 051333 as 222, which will route to the gateway. The gateway will transform this into a call from 054222 to 333 (the original calling H.323 endpoint). If the H.323 endpoint user presses **Redial** their original call will be retried.

# Creating a calling party ID from the calling number

In the relevant dial plan (this example assumes **ISDN to IP**), set up the following rule:

| # | Condition | Action | Use calling number | Protocol |
|---|---|---|---|---|
| | Called number matches / Calling number matches / Incoming call type "Any" | Call this number `[2001:DB8:0:ABCD::1]` | `$A` | H.323 |

Assume for this example that an ISDN call to 333444 comes into the gateway. The gateway will transform the outgoing part of the call into an H.323 call to IPv6 address “2001:DB8:0:ABCD::1” and forward number “333444” as the calling party ID.

# Setting up dial plan rules for TCS-4

The TCS-4 protocol provides a mechanism to signal an extension number after an H.320 call has been established. It only applies to H.320 video calls. By using a TCS-4 extension to pass the extra digits to the gateway, users can dial from a predefined endpoint phone list instead of entering the extension using DTMF in the auto attendant.

## ISDN to IP calls

The **ISDN to IP** dial plan supports *Enter the auto attendant + TCS-4* as an **Action**. 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 so that the auto-attendant is not displayed, although it may be visible briefly with the TCS-4 extension shown.

The table explains how to send a TCS-4 extension from certain endpoints. For other endpoints please refer to the endpoint user documentation for assistance.

| Endpoint type | Method |
|---|---|
| Cisco TelePresence (ISDN-capable) | Dial the ISDN number followed by an * and then enter the TCS-4 extension.<br>Example: If the TCS-4 dial plan incoming number match is 1234 and the required TCS-4 extension is 5678, dial `1234*5678` from the endpoint. The gateway will connect to the TCS-4 dial plan and dial out 5678 from the auto attendant with no need to enter the extension via DTMF. |
| Polycom | Replace the * with ## |
| LifeSize | Replace the * with # |
| Sony | Replace the * with # |

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). From ISDN-capable Cisco TelePresence endpoints, it is also possible to send an IP address as a TCS-4 extension.

## IP > ISDN > ISDN > IP calls

When using TCS-4 in an "ISDN bridge between IP islands" configuration (two IP endpoints/MCUs communicate traversing an ISDN link), two ISDN gateways are required. The first gateway (for the IP to ISDN conversion) cannot do TCS-4 because TCS-4 functionality only works in the ISDN to IP direction. However, the second 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 gateway needs to forward a number to the second gateway in the same format as a TCS-4 request received from any other ISDN endpoint. So even though the first gateway does not perform TCS-4 extension dialing, it should be set up so that it can call out with a number that is the same as sending a TCS-4 request to the second gateway. This functionality is implemented for the **IP to ISDN** dial plan 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.

For the purposes of this example, assume the following:

- The dial plan call-in number match for the first gateway is 123.
- The TCS-4 dial plan call-in number match for the second gateway 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 # symbol to indicate that this is the TCS-4 extension. The first gateway strips the 123 portion from this number and sends the rest of the number 456789 to the second gateway in such a format that the second gateway understands that the 456 portion is the dial plan match number and the 789 is the TCS-4 extension. The second gateway then dials the TCS-4 extension using its TCS-4 dial plan.

To set up the first gateway to send a number string that matches a TCS-4 request, use the ! delimiter. This splits the **Call this number** field, so that the part before the ! is the ISDN number to call, and the remaining portion after the ! is the extension address to respond to a TCS-4 request. In the **Call this number** field, enter <*ISDN number of second GW*>!<*TCS-4 extension used by second GW*>.

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

| Condition | Action |
|---|---|
| Called number matches `123(D*)#(D*)` | Call this 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 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 gateway, which will receive it as a TCS-4 request, assuming that the second gateway has this **ISDN to IP** dial plan:

| Condition | Action |
|---|---|
| Called number matches `456` | 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 dial plan rule you must use *, #, or ## to separate the ISDN number and the TCS-4 extension depending on the ISDN endpoint manufacturer. When dialing from the IP endpoint to the first ISDN

gateway, you can use either * or # irrespective of the endpoint type. So if you dial 123456#789 from the IP endpoint, you could also dial 123456*789. In the latter case, change the **Called number matches** setting for the first gateway from `123(D*)P(D*)` to `123(D*)S(D*)` (where `S` denotes *).

### Limitations

It is not possible to send alphanumeric characters as a TCS-4 extension from the IP side. You cannot dial 123456*MCU or 123456#MCU from an IP endpoint. This is because the extension number (after the * or # symbol) 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.

## Related topics

- Example dial plan rules in leased line mode [p.145]
- Understanding the dial plan [p.115]
- Configuring dial plan rules [p.127]
- Displaying and testing the dial plan [p.124]
- Dial plan syntax [p.120]
- Making calls with the gateway [p.11]
- Using the gateway for voice-only calls [p.12]

# Example dial plan rules in leased line mode

This topic provides examples of how to configure dial plan rules if the ISDN gateway is in leased line mode.

## ISDN to IP dial plan

This **ISDN to IP** dial plan forwards certain calls from the ISDN network to an auto attendant on the MCU. It allows for some calls to arrive with a TCS-4 extension and has a catch-all rule to forward all other calls to an operator.

| # | 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 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". | 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

| # | 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 number that begins 98 and has five digits or more. 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 ISDN port 2 using leased line group 3, will be answered by an operator. |

# Users

This section describes how to manage user configuration data on the Cisco TelePresence ISDN Gateway.

# Displaying the user list

The **User list** page (go to **Users**) provides summary information about the user accounts configured on the ISDN gateway.

| Field | Field description |
|---|---|
| **User ID** | The username the user needs to access the web interface of the ISDN gateway. Click on a name for more details. |
| **Name** | Currently this setting cannot be configured. |
| **Privilege** | The access privileges associated with the user. |

## Deleting users

To delete a user, select the relevant user(s) and click **Delete selected users**. You cannot delete the *admin* and *guest* users.

### Related topics

- Managing user accounts [p.148]
- System defined users [p.151]

# Managing user accounts

Some user accounts are pre-defined on the ISDN gateway. Administrators can add or modify other user accounts from the **Users** page.

## Adding or modifying users

To add a user account:

1. Click **Add new user**.
2. Complete the relevant settings for the user (see User settings [p.149]).
3. Click **Add user** to confirm.

To modify user account settings:

1. Select the relevant user.
2. Complete the relevant settings for the user (see User settings [p.149]).
3. Click **Update user settings** to confirm.

To delete user accounts:

1. Select the relevant user(s).
2. Click **Delete selected users**.
   The *admin* and *guest* user accounts cannot be deleted.

# User settings

| Field | Field description | Usage tips |
|---|---|---|
| **User ID** | Identifies the login name that the user will use to access the ISDN gateway web interface. | User IDs (also known as usernames) can contain up to 64 characters. You can enter text in any character set, but note that some browsers and FTP clients do not support Unicode.<br>The following user IDs are reserved and cannot be added:<br>■ admin<br>■ guest<br>■ invalid<br>■ system<br>■ unknown |
| **Password** | Required password (if any). | This option is only active when adding a new user. To change an existing user's password, click **Update password** instead. You can enter text in any character set, but note that some browsers and FTP clients do not support Unicode.<br>If the ISDN gateway is not using advanced account security mode, any password can be used.<br>In advanced account security mode, passwords must match the following criteria:<br>■ At least fifteen characters.<br>■ At least two uppercase alphabetic characters.<br>■ At least two lowercase alphabetic characters.<br>■ At least two numeric characters.<br>■ At least two non-alphanumeric (special) characters.<br>■ Not more than two consecutive repeating characters (two repeating characters are allowed but three are not).<br>■ The password must be different from the previous 10 passwords used with the associated user account.<br>■ The password will expire if it is not changed within 60 days.<br>■ Except for users with administrator privileges, the password may not be changed more than once in 24 hours.<br>Every user account must have a password defined, even if the ISDN gateway is configured to require certificate-based login only (*Require client certificate login* is enabled for HTTPS on the **Network > SSL certificates** page). |
| **Re-enter password** | Verifies the required password. | |
| **Disable user account** | Disables a user account or re-enables a previously disabled account. | You cannot disable the system-created *admin* account.<br>The system-created *guest* account is disabled by default. If you enable it, the ISDN gateway generates a security warning.<br>In advanced account security mode, a non-*admin* account expires after 30 days inactivity (the ISDN gateway disables it). |

| | | |
|---|---|---|
| **Lock password** | Prevents the user from changing their password. | This option is useful if you want multiple users to use the same user ID. The system-defined *guest* account has *Lock password* enabled by default. |
| **Force user to change password on next login** | Forces the user to change their password when they next attempt to log in to the ISDN gateway.<br>Not available if *Lock password* is selected. | For new accounts this option is enabled by default. The option is cleared automatically when a user changes their password. |
| **Privilege level** | The access privileges to be granted to this user. | ■ Users with *administrator* privileges can change any ISDN gateway configuration, and view all status information.<br>■ Users with *list only* privileges can only view basic details about active calls. (The system-defined *guest* account is fixed with *list only*.)<br>■ All users can view the online help. |

## Related topics

- Displaying the user list [p.147]
- Configuring security settings [p.77]
- Logging in to the web interface [p.15]
- Problems logging in [p.16]
- Configuring SSL certificates [p.43]

# System defined users

The ISDN gateway is pre-configured with two user accounts:

- *admin*
- *guest*

The following table describes the settings for these user accounts (some settings can be modified):

| User ID | Description | Usage tips |
|---|---|---|
| admin | 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.<br>For security reasons, we recommend that you change this to require a password. (If you configure the ISDN gateway with advanced account security mode, a password is required.) | After logging into the ISDN gateway for the first time, you can change the User ID and password for this account. The privilege level is fixed at *administrator*, which allows all pages to be seen and all configurable settings to be updated. |
| guest | The ISDN gateway must have at least one configured user with access privileges below *administrator*. The fixed User ID for this user is *guest*. By default no password is required.<br>If you configure the ISDN gateway with advanced account security mode, the *guest* account requires a password (which must match secure password criteria). | You cannot change the User ID for the *guest* account. You can add a password. |

## Related topics

- Logging in to the web interface [p.15]
- Displaying the user list [p.147]
- Managing user accounts [p.148]
- Configuring security settings [p.77]

# Calls and ports

This section describes how to display call and port status information on the Cisco TelePresence ISDN Gateway.

# Displaying the ISDN calls list

To display the ISDN calls list, go to **ISDN > ISDN calls**. The list displays active and completed calls on the ISDN gateway together with their basic settings.

From the calls list you can:

- Disconnect active calls
- Delete completed calls from the list
- Display details about active calls

## Information in the calls list

- Active calls are calls that are taking place now. The active calls list shows all calls that are currently taking place.
- 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.
- The maximum number of calls that can take place simultaneously is constrained by the ISDN bandwidth available to the ISDN gateway.

The following fields are displayed in the ISDN calls list. To see detailed information about an active call, click **more**.

| Field | Field Description |
|---|---|
| **Type** | The type of call, which will either be *IP to ISDN* or *ISDN to IP*. |
| **Participants** | The participants in the call. IP participants are listed by IP address, E164 number, H.323 ID, or SIP URI. ISDN participants are listed by Calling Party Number, or "<*none*>" if your ISDN network does not supply this information. |
| **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**.

# Displaying detailed call information

To view details about an active call, go to **ISDN > ISDN Calls** and click **more** for the relevant call. The **Call details** page is displayed, with information for the ISDN and IP side of the call respectively, grouped into participant, audio, and video statistics:

| | |
|---|---|
| **Participant details** | |
| **Name** | The name the caller provided when the call was initiated. |
| **E.164** | The telephone number of the participant. |
| **Call type** | The participant call type. Either *H.320* (ISDN caller) or *H.323*or *SIP* (IP caller). |
| **FECC** | Whether or not Far-End Camera Control has been established. |
| **Started at** | For IP to ISDN calls, the time at which the call was received by the ISDN gateway. For ISDN to IP calls, the time at which all the channels comprising the call connected and bonded. |
| **Progress** | The status of the call, which will be one of:<br>■ *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.<br>■ *Calling out*: the ISDN gateway is trying to make contact with the other side of the call.<br>■ *Connected*: the call is in progress between and IP and ISDN endpoints.<br>■ *Dying*: Displayed briefly while a call is terminated, either by one of the participants or via the web interface. |
| **Channel bonding map** | [ISDN participants only] The ISDN channels in use for this call. |
| **Encryption** | Whether encryption is active and if so, whether all or only some media channels are encrypted. |
| **Channel rate** | [ISDN participants only] Whether or not restricted 56 k 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 64 kbps. |
| **Video and extended video** | |
| **Receive stream** | |
| **Negotiated received bandwidth** | The negotiated bit rate available for the endpoint to send video, or H.239 content video in the case of extended video. This value represents the maximum amount of video traffic, or content video traffic in the case of extended video, that the remote endpoint will send to the ISDN gateway. It may send less data (for example if the gateway requests a lower rate) but it should not send more. |
| **Measured received bandwidth** | The most-recently measured actual bit rate. |

| | |
|---|---|
| **Received capabilities** | |
| **Forwarded capabilities** | |
| **Audio** | |
| **Receive stream** | |
| **Receive address** | |
| **Transmit address** | |
| **Packets received** | |
| **Packet errors** | Packets that are corrupt or can't be decrypted due to header errors, or are in some other error state. Note that a packet error also causes the **Packets dropped** counter to be incremented. |
| **Packets discarded** | Packets discarded by the ISDN gateway, due to buffering issues. |
| **Packets dropped** | Packets lost due to errors on the network (missing sequence numbers). |
| **Packets sent** | |
| **Jitter** | |
| **Received capabilities** | |
| **Forwarded capabilities** | |

# Displaying ISDN port use

Go to **ISDN > ISDN ports** to display link status and channel activity information for the ISDN ports. If the ISDN gateway is running in leased line mode, see instead Displaying ISDN port use in leased line mode [p.158].

## Link status

Link status information is shown for both layer 1 (physical) and layer 2 (D-channel). This information is also available from the **Status > ISDN** page.

## Channel activity

For each ISDN port, the following information is displayed per channel:

| Field | Field description |
|---|---|
| **#** | ISDN channel number. |
| **Activity** | Indicates whether or not the channel is currently active:<br>■ *inactive* if the channel is not in use.<br>■ *active (data)* if a voice and video call is using the channel.<br>■ *active (voice)* if an audio-only call is using the channel. |
| **Direction** | If the channel is active, indicates the call direction:<br>■ *inbound* for calls to the ISDN endpoint.<br>■ *outbound* for calls from the ISDN endpoint. |
| **Calling party** | The identity of the endpoint that initiated the call. Depending on the information supplied by the endpoint, this will be:<br>■ For outbound IP to ISDN calls, the name of the device, the telephone number, or "ISDN gateway".<br>■ For inbound ISDN to IP calls, the telephone number of the endpoint that made the call. |
| **Called party** | The number dialed by the calling party. |

## Activating the D-channel

An **Activate D-channel now** button is available for any port for which layer 1 is up and layer 2 (D-channel) is down.

In reality you are unlikely to need to activate a D-channel manually, as the ISDN gateway periodically attempts auto-activation. But if you do need to bring up a D-channel manually, you can do so by clicking this button.

**Note:** D-channel activation is a two-way handshaking operation that depends on a response from the ISDN switch. If the switch does not respond, the activation will fail.

The **Activate D-channel now** button is disabled for ports where either layer 1 and layer 2 are both up, or layer 1 and layer 2 are both down.

# Displaying ISDN port use in leased line mode

Go to **ISDN > ISDN ports** to display link status and channel activity information for the ISDN ports.

## Link status

Link status information is shown for layer 1. This information is also available from the **Status > ISDN** page.

## Channel activity

For each ISDN port, the following information is displayed per channel:

| Field | Field Description |
|---|---|
| **#** | The ISDN channel number. |
| **Activity** | Indicates whether or not the channel is currently active:<br>■ *inactive* if the channel is not in use.<br>■ *active (data)* if a voice and video call is using the channel.<br>■ *active (voice)* if an audio-only call is using the channel. |
| **Direction** | If the channel is active, indicates the call direction:<br>■ *inbound* for calls to the ISDN endpoint.<br>■ *outbound* for calls from the ISDN endpoint. |
| **Calling party** | The identity of the endpoint that initiated the call. Depending on the information supplied by the endpoint, this will be:<br>■ For outbound IP to ISDN calls, the name of the device, the telephone number, or "ISDN gateway".<br>■ For inbound ISDN to IP calls, the port number on which the call is coming in and the leased line group that the call is using (in the format *<port number> * <group number>*). |

**Note:** In leased line mode, the **Activate D-channel now** button is dimmed.

# Logs

This section describes how to view and manage log data for the Cisco TelePresence ISDN Gateway.

# Working with the event log

The last 2000 status messages generated by the ISDN gateway are displayed in the **Event log** page (**Logs > Event log**). Most messages are provided for information, although *Warnings* or *Errors* may also be displayed. If you experience a specific problem with the operation or performance of the ISDN gateway, Cisco customer support can assist you in collecting and interpreting log entries.

You can do the following from the **Event log** page:

- Sort the events display by clicking the column headers.
- Jump through the displayed log in steps of 100 events by clicking the page numbers.
- Download the log as text (click **Download as text**).
- 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.
- Empty the log (click **Clear log**).

To filter the entries displayed in the log, see Filtering event log entries [p.160].

To change the logging level recorded in the log (only do this under guidance from Cisco customer support), see Changing the event logging level [p.161].

# Filtering event log entries

To modify the event display filter to view a subset of the event log or to highlight particular log entries, go to **Logs > Event display filter**. The filter works on stored entries and does not affect which events are actually captured in the log.

## Text filtering

1. Enter a **Filter string** to display only the stored events which contain that string.
2. Enter a **Highlight string** if you want that string to be highlighted in the log display.
3. Click **Update display**.
   The ISDN gateway displays the filtered and/or highlighted log entries.

## Display levels

There are many sub-systems of the ISDN gateway, which can all log events. You can modify the level of detail that you want to see — for each sub-system or for all of them.

For example, if you are interested in SIP errors only:

1. Scroll to the bottom of the page where you can see the **Set all to:** drop-down list.
2. Select *None* from the drop-down list.
3. Click **Set all to:**.
   The display level changes to *None* for all sub-systems.
4. Select *Errors only* from the drop-down list next to the SIP sub-system.
5. Click **Update settings**.
   The ISDN gateway displays SIP errors only.

# Changing the event logging level

The event capture filter defines which events the ISDN gateway will keep in the log. By default this filter is configured to capture *Errors, warnings and information* from all the ISDN gateway sub-systems.

If requested to do so by Cisco customer support, it is possible to change the level of detail collected in the traces. To do this, go to the **Event capture filter** page and change the settings in accordance with the guidance from your support representative.

**CAUTION:** Modifying the event logging level can impair ISDN gateway performance. Do not modify these settings unless asked to do so by Cisco customer support.

# 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**. The available settings are described in this topic.

## 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 ISDN gateway on the Syslog host. Choose from the following options:<br>■ *0 - kernel messages*<br>■ *1 - user-level messages*<br>■ *2 - mail system*<br>■ *3 - system daemons*<br>■ *4 - security/authorization messages (see Note 1)*<br>■ *5 - messages generated internally by syslog*<br>■ *6 - line printer subsystem*<br>■ *7 - network news subsystem*<br>■ *8 - UUCP subsystem*<br>■ *9 - clock daemon (see Note 2)*<br>■ *10 - security/authorization messages (see Note 1)*<br>■ *11 - FTP daemon*<br>■ *12 - NTP subsystem*<br>■ *13 - log audit (see Note 1)*<br>■ *14 - log alert (see Note 1)*<br>■ *15 - clock daemon (see Note 2)*<br>■ *16 - local use 0 (local0)*<br>■ *17 - local use 1 (local1)*<br>■ *18 - local use 2 (local2)*<br>■ *19 - local use 3 (local3)*<br>■ *20 - local use 4 (local4)*<br>■ *21 - local use 5 (local5)*<br>■ *22 - local use 6 (local6)*<br>■ *23 - local use 7 (local7)* | Choose a value that you will remember as being the ISDN gateway.<br>**Note:** Various operating system daemons and processes have been found to use Facilities 4, 10, 13, and 14 for security/authorization, audit, and alert messages which seem to be similar.<br>Various operating systems have been found to use both Facilities 9 and 15 for clock (cron/at) messages.<br>Processes and daemons that have not been explicitly assigned a Facility value may use any of the "local use" facilities (16 to 21) or the "user-level" facility (1). We recommend that you select these values. |

# 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 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)

## Related topics

- Working with the event log [p.160]

# Working with Call Detail Records

To work with the Call Detail Records (CDR) log, go to **Logs > CDR log**. The ISDN gateway can display up to 20 pages of CDRs. However, the ISDN gateway is not intended to provide long-term storage of CDRs and if you wish to retain them, you must download and store the records elsewhere.

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

## Customizing the display

The CDR log can contain a lot of information. You can use the **Status and display** settings to control and filter the log:

| Field | Field description | Usage tips |
|---|---|---|
| **Current status** | Indicates whether CDR logging is enabled or disabled. Use (**Enable CDR permanent storage** / **Disable CDR permanent storage**) to change status.<br>If you enable logging, the ISDN gateway writes the CDRs to the compact flash card.<br>If you disable logging, CDRs are still generated but are not written to compact flash. | Enabling or disabling CDR logging has immediate effect. There is no need to click **Update display**.<br>Ensure that a compact flash card is available. |
| **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* shows the greatest amount of detail for all messages, regardless of which other options are selected. |

## Information available

The CDR log list shows some or all of the stored records, depending on any filtering and display settings specified. Click on a column heading to sort by that field. These fields are displayed in the CDR log list:

| Field | Field description | Usage tips |
|---|---|---|
| **# (record number)** | Unique index number for this record. | |
| **Time** | The time the record was created. | Records are created as different connection events occur. The time the record was created is the time that the event occurred.<br>Incoming CDR log requests are stored with the local time stamp (not UTC).<br>Changing the time (either by changing the system time or via an NTP update) causes new events in the CDR log to show the new time. No change will be made to existing logged CDR events. |

| | | |
|---|---|---|
| **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 record type, and brief details if available. | The display settings allow you to display more extensive details for different record types.<br>The **filter string** allows you to select for display only records where a particular word or string occurs. |

# Downloading the log

The CDR log includes all stored CDRs, 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.

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

- To download the entire CDR log, click **Download as XML**.
- To download just a range of records, click **Download *X* to *Y* as XML**. If a large number of logged CDRs exist, it may take several seconds to download and display them. The range of records that you can download to the web interface works in groups. Therefore you may see **Download *X* to *Y* as XML** and *Y* does not increase even though the log is filling up. When a pre-defined threshold is reached, then *Y* will increase.
- The web interface displays a maximum of 20 pages. If the log includes more records than can be displayed, the more recent ones are displayed. So you may see **Download *X* to *Y* as XML** where *X* keeps increasing when the page is refreshed.

# Clearing the log

The delete button is greyed out until the log holds a certain number of records.

To clear the CDR log, click **Delete X to Y**. This permanently removes CDR records in the range *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, say you delete log entries numbered 0-399. In this case the 400th log entry will appear as the first entry in this page, even if you download the entire log. The download button will show that you can download 400-*nnn*, where *nnn* is the maximum number of log entries. The delete button will be greyed out again, because it is only available when a certain number of records are in the log.

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

## Related topics

- Working with the event log [p.160]
- Displaying and resetting system time [p.75]
- Understanding security warnings [p.80]

# Working with the audit log

To work with the audit log, go to **Logs > Audit log**.

If the audit log is enabled, all user actions on the ISDN gateway that might compromise security for the device or the network are recorded. This includes changes to network and security settings, dial plan additions or deletions, and any changes to the audit log itself. As well as the web interface, it covers actions made through the serial console, API, FTP, and (Cisco TelePresence ISDN GW MSE devices only) the supervisor blade.

**Note:** By default the audit log is disabled.

## Enabling the audit log

1. Go to **Logs** > **Audit log**.
2. Click **Enable auditing**.

## Information in the audit log

Each log entry has a severity classification (Error, Severe Warning, Warning, Info, or Status Warning) and indicates which module has caused the entry, as follows:

| | |
|---|---|
| Web | Configuration changes made through the web interface. |
| Serial | Configuration changes made through the serial console. |
| API | Configuration changes made through the API. |
| Supervisor | Configuration changes made through the Supervisor blade (Cisco TelePresence ISDN GW MSE devices only). |
| System | Audit messages from the ISDN gateway. |
| FTP | Audit messages that record requests made to the ISDN gateway over FTP. |

## About audit log messages

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 present. You can view only the last 2000 messages through the web interface, but you can download all stored audit messages (up to the 100,000) as XML.

You can delete audit messages, except the most recent 400 audit messages. The delete action will be audited in a new audit message.

You cannot send the audit log to a syslog server.

# Logging H.323 or SIP messages

The **H.323/SIP log** page records every H.323 and SIP message received by or transmitted from the ISDN gateway.

The H.323/SIP log is disabled by default because the volume of messages affects performance, but Cisco customer support may ask you to enable it to assist in troubleshooting.

Click **Enable H323/SIP logging** to start recording these protocol messages. You can also download the log as an XML file for further processing or to send to support (click **Download as XML**).

To avoid impacting future device performance, when you are satisfied that the issue is resolved, you should disable H.323/SIP logging and then clear the log (click **Clear log**).

# Feedback receivers

The ISDN gateway publishes feedback events so that any receivers listening to it can take action when something changes. To see information about any configured feedback receivers, go to **Logs > Feedback receivers**—the table below describes the information available.

If necessary you can clear all configured receivers by clicking **Delete all**. You cannot undo this action.

| Field | Field description | Usage tips |
|---|---|---|
| **Index** | The position of the receiver in the list. | |
| **Receiver URI** | The fully qualified URI of the receiver. | The receiver may be a software application, for example Cisco TelePresence Management Suite, that can respond to the feedback events with an appropriate API call to retrieve the list of changes from the feedback source. |
| **Source identifier** | A string that the source will provide to the receiver when it is queried or when it publishes feedback events. | This string is optional and defaults to the MAC address of Ethernet port A on the ISDN gateway. |
| **Notification events subscribed to** | The list of source feedback events that the receiver is subscribing to. | The receiver can subscribe to some or all of the feedback events published by the source. By default, the receiver subscribes to all such feedback events. |