Interaction Gateway®

Administrator's Guide

Interactive Intelligence Customer Interaction Center® (CIC)

Version 2016

Last updated November 16, 2015

(See Change Log for summary of changes.)

Abstract

This document provides essential information for initial installation and configuration of your Interaction Gateway software product on the Interaction Edge platform. For the latest version of this document, see the Interaction Edge product information site: https://my.inin.com/products/edge/Pages/Documentation.aspx

Interactive Intelligence, Inc.
7601 Interactive Way
Indianapolis, Indiana 46278
Telephone/Fax (317) 872-3000
www.ININ.com

Copyright and Trademark Information

Interactive Intelligence, Inc.

7601 Interactive Way

Indianapolis, Indiana 46278

Telephone/Fax (317) 872-3000

www.ININ.com

Table of Contents

Overview of Interaction Gateway

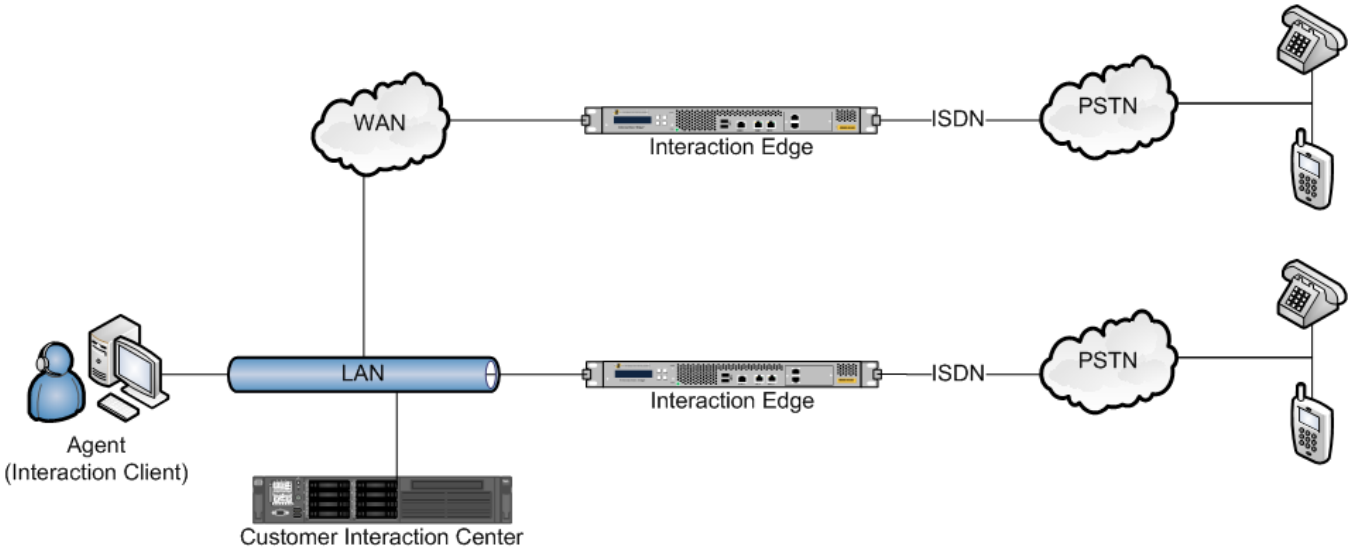
This section contains the following introductory topics about the Interaction Gateway software. You should become familiar with these topics before you configure the software.

Introduction to Interaction Gateway

Interaction Gateway is a software application that, along with the Interaction Edge™ appliance, enables voice and data traffic to be sent over the same network, including IP fax transmissions through the T.38 protocol. It connects T1/E1/ISDN/CAS spans from the telephone company (PSTN) or service provider to the corporate LAN. Along with serving as a general telephony gateway, Interaction Edge and Interaction Gateway enable SIP stations, which are defined in the Customer Interaction Center (CIC) server, to talk to telephones outside of the contact center by using voice over IP (VoIP).

The Interaction Gateway software transcodes audio between CIC VoIP stations and the PSTN to Real-time Transport Protocol (RTP) or Secure RTP (SRTP) audio streams. It manages SIP control messages with the CIC server or other devices, optionally offering SIP security through TLS. It uses one IP address for both SIP messaging and for RTP/SRTP audio streams.

A single Interaction Edge and Interaction Gateway system can be deployed with one or more CIC servers. Alternatively, a single CIC server can route calls through multiple Interaction Gateways. See the following diagram for an example of a multiple CIC server telephony environment with Interaction Edge and Interaction Gateway:



Interaction Edge and Interaction Gateway are particularly well-suited for use with Interaction Dialer, a powerful outbound dialing application suite that supports high throughput for hundreds of agents for each server, but it can also be used with other CIC systems and IP PBXs. Interaction Gateway enables each agent to use a SIP-enabled device, such as IP telephones, soft phones, and Interaction SIP Station, from any location. The CIC server can perform outbound dialing through Interaction Gateway with accurate call analysis from Interaction Media Server to make the results of a dialing campaign highly successful.

The Interaction Gateway software supports three standard voice codecs for audio transmission:

- G.711a-law
- G.711μ-law
- G.729ab

Interaction Gateway feature summary

- **International protocols** – Interaction Gateway supports the following TDM protocols:

Supported T1 protocols	Supported E1 protocols
• ISDN T1 PRI — NI2, National ISDN-2 — 5ESS, AT&T — 4ESS, AT&T — DMS 100 PRI, Nortel — DMS 100 ISDN, Nortel — QSIG, ECMS 142/143 — INS, INS-1500 • CAS — Wink start — Immediate start	• ISDN E1 PRI — Euro-ISDN, ETS 300 — QSIG, ECMS 142/143

Note:

QSIG support currently consists of basic call control only, which supports all messaging used to set up, disconnect, and tear down voice audio calls. It does not currently support all features of extended call control, which covers non-call control messages, such as INFO messages. The current version does support user-to-user information (UUI). It does not currently support message waiting indicators (MWI), redirecting transfers, path replacements, and other non-call messaging features.

- **Fax relay support** - T.30 is the standard for fax transmission on the PSTN. T.38 is the standard for fax transmission through packets on the Internet or a data network. Fax relay is the process of translating T.30 fax signals into T.38 fax packets and the reverse. This process allows faxes to be received from and sent to the PSTN by a SIP-based IC system (or other SIP-based fax endpoint).

Note:

Interaction Gateway does not support the V.8, V.33, or V.34 fax standards.

- **Web-based interface** – Interaction Gateway has a web user interface that you use to monitor and configure the system.
- **Secure connections and support for secure audio** – All user connections to the Interaction Gateway web interface use the secure HTTPS protocol for all HTTP sessions as they require a certificate exchange. In addition, you can optionally configure Interaction Gateway to use TLS and SRTP for secure (encrypted) audio streams. Enabling this level of security requires configuration of the Interaction Gateway **Spans** page as well as related systems, including the Customer Interaction Center server, Interaction Media Server, and Interaction SIP Proxy server.
- **SNMP support** – Interaction Gateway enables you to configure call thresholds and call dispositions for generating Simple Network Management Protocol (SNMP) trap messages.
- **Support for standardized D-Channel trace format**– Using a third-party protocol trace viewing application, such as WireShark, you can view D-Channel network transmissions from Interaction Gateway to help with any diagnostic tasks that you choose to do.

- **Improved performance tracing** – You can now set the amount of performance detail of the host system that you want Interaction Gateway to record to the `ININLOG` log file.
- **Simulate Call enhancements** – When you use the Simulate Call feature, you can now have Interaction Gateway actually place the call to the specified destination through the assigned route. For more information, see Simulate a call through the new call route.
- **Support for restricted numbers** – The new system parameter, **`restrictedCallingNumber`**, enables you to allow or block (use *Anonymous*) calls from ISDN to SIP where the ISDN setup message marks the call as *Presentation Restricted*. For more information, see Configure Interaction Gateway to restrict calling party number for ISDN connections.
- **Outbound ANI override** – This feature enables you to override the ANI string for outbound calls. You can specify the ANI string through the page for call properties, which you access through the **Settings-Call Routes** page. For more information about this feature, see the "Call Properties" topic in *Interaction Gateway Help.*
- **Channel group sort order** – This feature on the **Settings-Channel Groups** modification page enables you to display the assigned channels in a channel group as Interaction Gateway selects them according to the specified Hunt Selection Method. For more information about this feature, see the "Channel Groups Table" topic in *Interaction Gateway Help*.
- **Downloadable configuration file** – A new hyperlink on the **Settings-Import/Export** page enables you to download the Interaction Gateway configuration file to a remote computer or storage location.

For more Interaction Gateway information

In addition to the printed version of this book, you can find a `.PDF` file in the documentation library that is installed on a Customer Interaction Center server. Additional information is available in Help, updates, and other related information in the following locations.

Interaction Gateway Help

In the Interaction Gateway web interface, click the **Help** icon in the upper right corner of the page to display *Interaction Gateway Help*.

In the contents pane on the left, select the section or page of the web interface you want to learn about. For example, *Interaction Gateway Help* contains useful examples and detailed instructions for defining call routes through Interaction Gateway.

Subsequent Interaction Edge updates may modify the content in *Interaction Gateway Help*.

Interaction Edge Installation and Configuration Guide

Interaction Edge Installation and Configuration Guide, which is available for download on the Interaction Edge webpage on the Interactive Intelligence product information website (http://my.inin.com/products/edge/Pages/Documentation.aspx), provides concepts and procedures for the appliance on which Interaction Gateway is hosted.

Interaction Edge Help

The Interaction Edge web interface has a Help system that can provide additional information on subjects related to Interaction Gateway, such as resource usage and SNMP configuration.

Interactive Intelligence product information website

The Interaction Edge product information website contains updates along with other resources related to usage of Interaction Edge and Interaction Gateway.

The Interactive Intelligence website requires you to log on with a user name and password. If you do not have an Interactive Intelligence account, contact your reseller or Interactive Intelligence sales representative.

The Interaction Edge product information website is available through the following Uniform Resource Locator (URL) address:

https://my.inin.com/products

Newsgroups

Visit the Interaction Gateway forum at http://community.inin.com/ to share ideas and gather information regarding Interaction Edge and Interaction Gateway. The Interactive Intelligence Interactive Community is a free and public service provided by Interactive Intelligence to promote an online community devoted to the sharing of ideas and information regarding Interactive Intelligence products. Opinions expressed on the Interactive Community are not those of Interactive Intelligence, and Interactive Intelligence accepts no legal responsibility for their veracity or nature.

Feedback

Submit product feedback and suggestions for Interaction Edge and Interaction Gateway at http://ideas.inin.com. Select the **Hardware** link to review the ideas of others in the community for Interaction Edge and use **Post Idea** to submit your own.

Setup Interaction Gateway

This section provides the requirements and procedures for configuring Interaction Gateway. It contains the following topics:

Compatibility requirements for Customer Interaction Center interoperability

This version of Interaction Gateway is a general purpose telephony gateway and does not require Customer Interaction Center (CIC). However, if you use Interaction Gateway in a CIC network, consider the following requirements:

Interaction Gateway with Customer Interaction Center

- This version of Interaction Gateway is compatible with CIC 2015 R1 and later.
- This version of Interaction Gateway is compatible with CIC 4.0 and all Service Updates.
- This version of Interaction Gateway is compatible with CIC 3.0 and all Service Updates for the processing of SIP-based calls.
- For call analysis, Interaction Gateway requires a minimum of Interaction Media Server 3.0 SU8 in the audio path and CIC 3.0 SU8.

  Note:

  This version of Interaction Gateway does not provide an independent call analysis feature. For information about configuring call analysis on CIC 3.0 SU8 or later, see Create a SIP Line in CIC 3.0 SU8 or later.

- To use Interaction Media Server 4.0 or 20*nn* R*n*, either hosted on the Interaction Edge appliance or on a separate server, you must use CIC 3.0 SU12 or later, CIC 4.0, or CIC 20*nn* R*n*.

Interaction Gateway with Interaction Dialer

This version of Interaction Gateway is compatible with Interaction Dialer 3.0, 4.0, and 20*nn* R*n*. Interaction Dialer 3.0 is supported only on CIC 3.0. Interaction Dialer 4.0 is supported only on CIC 4.0. Interaction Dialer 20*nn* R*n* requires the same version on the CIC server.

Note:

Interactive Intelligence recommends that you apply the latest updates to your version of Interaction Dialer to ensure the best compatibility and performance.

Log on to Interaction Gateway

Note:

Before you can log on to Interaction Gateway, the Interaction Edge appliance must be installed and operational. For more information about installing and configuring the Interaction Edge appliance, see *Interaction Edge Installation and Configuration Guide*.

To log on to Interaction Gateway, do the following steps:

1. At the Interaction Edge appliance, press and hold the upper left LCD panel button to display the currently-configured IPv4 address.

2. On a remote computer, open a web browser and navigate to the IPv4 address that the Interaction Edge appliance displayed in the LCD panel.

   Tip:

   If you want to connect directly to the Interaction Gateway interface without going through the Interaction Edge interface, use your web browser to navigate to the direct IPv4 address and port number of the Interaction Gateway system, such as http://*<IPv4 address>*:8082 or https://*<IPv4 address>*:444.

   You may be presented a page that notifies you that the certificate on the web page is not trusted on your computer. If this occurs, select the appropriate option to continue to the website.

   Note:

   If you want to bypass the certificate warning for subsequent login attempts, add this certificate to the trusted root store of your PC. See the help system for your specific browser to learn more about installing certificates from trusted sources.

   You are presented with an Interaction Edge dialog box prompting you for a user name and password.

3. Enter the administrator user name and password and press the **Enter** key.

   Note:

   The default administrator user name and password are `admin` and `1234`.

   The user interface of Interaction Edge is displayed.

4. In the table at the bottom of the page, locate the Interaction Gateway service and select the associated **Configure** hyperlink.

   You are prompted to enter the administrator user name and password.

5. Enter the administrator user name and password and press the **Enter** key.

   The Interaction Gateway user interface is displayed.

Interaction Gateway web interface

The Interaction Gateway web interface is comprised of two different areas: **Status** and **Settings**.

For detailed information about the controls on these pages, select the **Help** icon in the upper right corner of the page.

Interaction Gateway Status pages

This area of the Interaction Gateway web interface displays information about the current state of Interaction Gateway, its processes, and any current communications. The **Status** area contains the following pages:

- **Spans** – This page displays a summary of the current state of each span along with the SIP span status on the connected Network Interface Card (NIC). It also offers an optional historical view of span status by day and an active view of channels in use.
- **Reporting** – This page displays graphs of call activity per Span, SIP Protocol, Channel, Day, Hour, and Type of Call for Interaction Gateway.
- **Admin Log** – This page displays the Interaction Gateway administrative log data in a configurable table format.
- **About** – This page displays a summary of product and file version information, machine name, IP address, and other information.

Interaction Gateway Settings pages

This area of the Interaction Gateway web interface enables you to configure the software for your telephony network environment. The **Settings** area contains the following pages:

- **Call Routes** – This page enables you to configure routing rules and properties for inbound and outbound calls. It also enables you test changes with the simulator interface.
- **Channel Groups** – This page enables you to configure groups of channels used for outbound dialing.
- **Spans** – This page is a summary of the state of each span and enables you to progress further into the details of each span. It also enables you to configure the SIP (NIC) Span status.
- **Media** – This page enables you to configure fax and RTP audio settings.
- **Alerts** – This page enables you to configure Simple Network Management Protocol (SNMP) trap options specific to Interaction Gateway. For more information about configuring these SNMP options, see *Interaction Gateway Help*. For configuring all other SNMP options and connectivity, see *Interaction Edge Help*.
- **Certificates** – This page enables you to configure active TLS certificates, trusted certificate authorities, and certificate signing requests.
- **Access List** – This page enables you to configure access control lists of devices by IP address and configures protocols that can be allowed or denied access to Interaction Gateway.
- **Import / Export** – This page enables you to save and modify the Interaction Gateway configuration file.
- **Administration** – This page enables you to configure the user names and passwords for the administrator account, the restricted account, and the FTP account. It also offers diagnostic tools and controls to set tracing levels.

Initial Interaction Gateway configuration

To configure Interaction Gateway, do the following tasks:

Note:

For more information about the controls on each interface, select the **Help** icon in the Interaction Gateway web interface. You can also use the Interactive Intelligence product information website for additional information (http://my.inin.com/products).

Change the administrator user name and password

Caution!

Write down and remember these credentials. There is no master user and password.

Note:

You use this administrator account to log on to both the Interaction Edge and Interaction Gateway interfaces. For more information about administrator accounts on the Interaction Edge appliance, see *Interaction Edge Installation and Configuration Guide*.

1. Log on to Interaction Gateway using the default administrator credentials:
   - User name: **admin**
   - Password: **1234**

   The **Status-Spans** page is displayed.
2. In the upper right corner of the page, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.
3. On the left side of the page, select the **Administration** tab.

   The **Settings-Administration** page is displayed.
4. Under the **Gateway Web Administrator Account** heading in the **User Name** box, enter a string of characters as the identifier of this account.
5. In the **New Password** box, enter a new password for the administrator account.
6. In the **Confirm New Password** box, re-enter the new password.
7. Select the **Apply** button.

   When you select the **Apply** button, Interaction Gateway disconnects your current session. You can then log on again with the new administrator user name and password that you provided in this procedure.

Change all TDM spans for E1

> **Important!**
>
> Do not do this procedure if you use T1 TDM spans.

1. Open a web browser and log on to the Interaction Gateway web interface.
2. In the upper right corner, select the **Settings** icon.
3. On the left side of the page, select the **Administration** tab.
4. In the **TDM Network Type** list box, select **E1**.
5. Select the **Apply** button.

   Interaction Gateway restarts. This restart may take up to five minutes to complete. When the LCD panel displays **Interaction Edge** again, you are ready to log on to the web interface and continue.

   You have successfully changed the span from T1 to E1.

Configure Interaction Gateway TDM spans

This topic provides the procedure for configuring the Time Division Multiplexer (TDM) spans on Interaction Gateway.

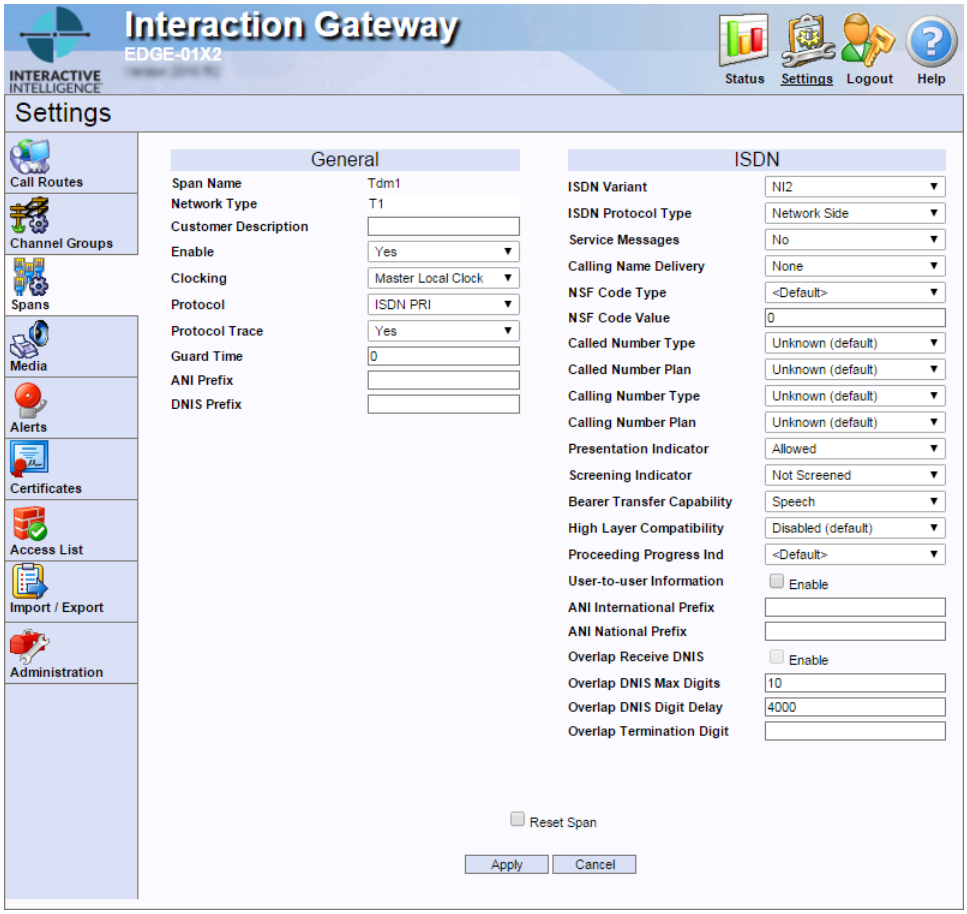
1. Log on to Interaction Gateway with the administrator user name and password.

   The **Status-Spans** page is displayed.
2. In the upper right corner, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.
3. On the left side of the page, select the **Spans** tab.

   The **Settings-Spans** page is displayed.
4. For any TDM span, select the associated **Modify** button on the far right side of the row.

   The following page is displayed:



5. In the appropriate controls, enter the necessary information for this TDM span.

> **Tip:**
>
> Your service provider should supply you with these settings, except for the **Customer Description** and the **Enable** controls, which you can modify freely. You and the provider must determine which protocol and feature settings are to be enabled when the circuits are ordered. If you need assistance in determining the protocols or features that you need in your environment, contact Interactive Intelligence Support.

> **Note:**
>
> You can find descriptions of each control on this page in *Interaction Gateway Help*. Select the **Help** icon in the upper right corner of the page.

6. After you have supplied the settings in the appropriate controls, enable the **Reset Span** check box and select the **Apply** button.

   The selected TDM span is reset and goes into an active state with the settings that you specified.

7. Repeat this procedure for each remaining TDM spans.

Configure the Interaction Gateway SIP span

This topic provides the procedure for configuring the Session Initiation Protocol (SIP) span on Interaction Gateway.

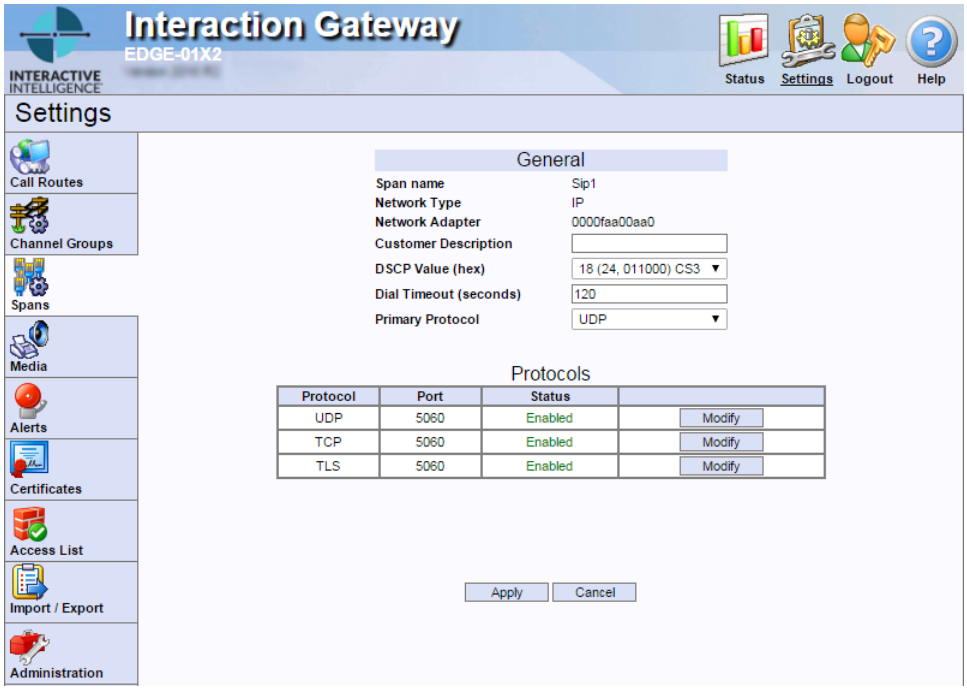
1. Log on to Interaction Gateway with the administrator user name and password.

   The **Status-Spans** page is displayed.
2. In the top-right corner, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.
3. On the left side of the page, select the **Spans** tab.

   The **Settings-Spans** page is displayed.
4. At the bottom of the page, select the **Modify** button that is associated with the **Sip1** span.

   The following page is displayed:

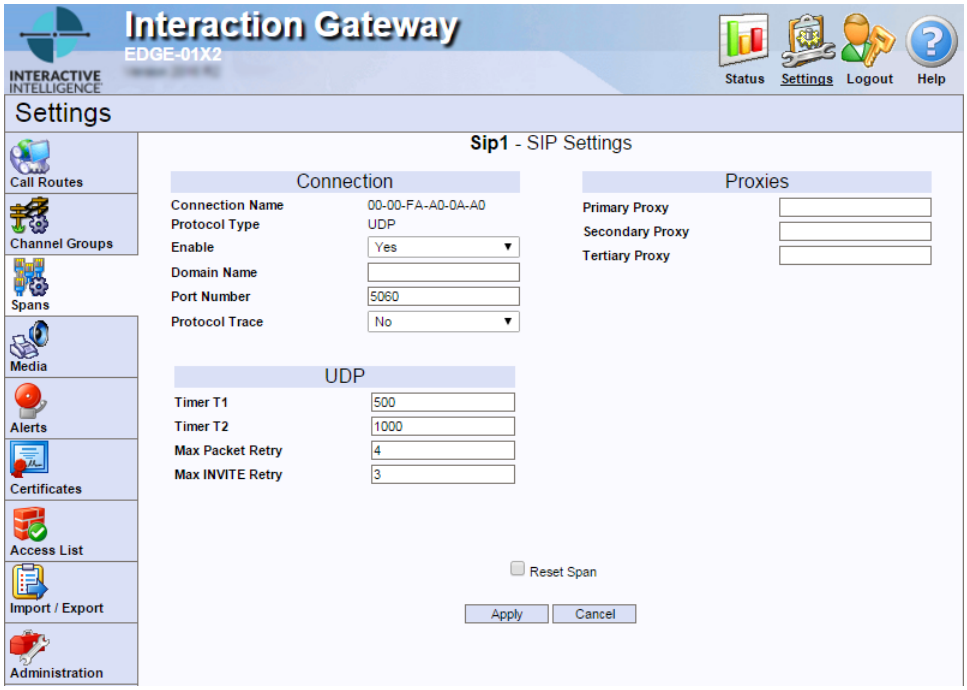


5. In the appropriate controls in the **General** section, enter the necessary information for this SIP span.

   Note:

   You can find descriptions of each control on this page in *Interaction Gateway Help*. Select the **Help** icon in the upper right corner of the page.
6. For one of the protocols (UDP, TCP, TLS), select the associated **Modify** button.

   A page resembling the following image is displayed:



7. In the **Connection** and **Proxies** areas, enter the necessary settings for the displayed controls.

> **Important!**
>
> Interaction Gateway does not currently use *stateful awareness* to determine if SIP proxies are available for SIP message processing. Interactive Intelligence recommends that you specify the IP address of an Interaction SIP Proxy server in the **Primary Proxy** box for this transport layer protocol. Enter any Customer Interaction Center servers in the **Secondary Proxy** and **Tertiary Proxy** boxes. Using this method, Interaction SIP Proxy, which uses stateful awareness, can direct SIP messages from Interaction Gateway to an available receiver for call processing.
>
> For more information about troubleshooting dropped carrier calls and how it can be related to the availability of SIP proxies, see the Incoming calls are failing topic.

> **Important!**
>
> The following list provides the default SIP ports for when Interaction Edge hosts Interaction Gateway and Interaction SIP Proxy:
>
> Interaction Gateway: TCP/UDP 5060; TLS 5061
>
> Interaction SIP Proxy: TCP/UDP 5058; TLS 5059

8. Below the **Connections** and **Proxies** area, enter the necessary settings for the displayed controls in the area specific for the specified protocol.
9. After you have finished entering the settings, enable the **Reset Span** check box and select the **Apply** button.

   The SIP span is reset and the affected protocol is enabled.
10. Repeat this procedure for the remaining SIP protocols.

Important!

If you want to use TLS for secure communications between devices, you must first install the TLS certificate before you can enable the TLS protocol on Interaction Gateway.

Install Interaction Gateway certificates

If you plan to use TLS and SRTP for secure communication with other SIP-enabled devices, you must first install the appropriate TLS certificate on the **Certificates** page in the Interaction Gateway web interface before you enable the TLS protocol of the SIP span on the **Spans** page.

Generate the Interaction Gateway TLS certificate

This procedure directs you to install certificates on Interaction Gateway so that it operates with other TLS enabled nodes in your communication network.

1. Create a TLS certificate by doing the following steps:
   a. Open a web browser and log in to the Interaction Gateway web interface.
   b. In the upper right corner, select the **Settings** icon.
   c. On the left side of the page, select the **Certificates** tab.

      The **Settings-Certificates** page is displayed.
   d. In the **Certificate Signing Request (CSR)** area, enter the following information:
      - **Organization** – Enter a name such as that of your company. For example, **XYZ Company**.
      - **Organization Unit** – Enter a name such as that of your department. For example, **Operations Department**.
      - **Common Name** – Enter a name such as to how the department is referred. For example, **Operations third floor**.
   e. Select the **Generate** button.

      The CSR window displays the certificate, as shown in the following example:

```
----BEGIN CERTIFICATE REQUEST-----

MIIBnzCCAQgCADBgMR0wGwYDVQQKExRBY21lIERvZ2Zvb2QgQ29tcGFueTEWMBQGA1UECxMNVGFzdGluZyBEZX
B0LjEnMCUGA1UEAxMeQWNtZSBEb2dmb29kIFRhc3RlcnMgbG9jYWwgOTExMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQChiiig6C3Tvxdl0en09tEDVp/A0+oTRkG5tofexY2mpFjJFG/6ktye634mDEe1ftM98QnJsydOMO
UoNatTdrD79ktbzQ8Dqbz5C5d+OM2bJHfM86x/VBozTmSgsWW/GucGRWE9Gma7okcbiCeR4oPbMK1EnXlKbr7Z
XTK/jVsx5QIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAk3cBSi24ikG2R69oYcI5rxZyK5Zl4lcOGCaBG40V/A
pWaANGvMqR5pI8EEvwhXzM6N7omSUr2mu51a8cNmm/GfRa4XLNdWDfe8R59NF9Rs/8qu2pcSLtZlxuLIer+cRK
65Biil3d+oZ7jOwwgpwLLDjB+2ixtvv8VcpN3aWuo=

-----END CERTIFICATE REQUEST-----
```

2. After you have generated the certificate, you must submit this certificate to a Certificate Authority for validation and signing before you can use it in Interaction Gateway. Some well-known, global Certificate Authority organizations are Verisign, Thawte, Entrust, and CAcert. After the Certificate Authority validates and signs the request, it sends back the new TLS certificate with the file extension of `.CER`.

Note:

If you are using Customer Interaction Center in your telephony environment, it has the ability to sign certificates without using a Certificate Authority. For more information, see *Interaction Administrator Help*.

Important!

Certificates are time-sensitive. If the time setting on the generating device is not synchronized with the device that is signing the certificate, then authorization may fail. To avoid this problem, ensure that the time settings of both devices are the same before continuing with the request.

Install the Trusted Authority (Root) Certificate on Interaction Gateway

This topic contains the procedure for installing Trusted (verified and signed) Authority Certificates, also known as Root Certificates, on Interaction Gateway. These certificates authenticate incoming SIP/TLS connection requests.

Important!

You must first generate the Certificate Signing Request, submit it to a Certificate Authority, and receive back the `.CER` certificate file before you can do this procedure.
Additionally, Interaction Gateway expects all submitted certificates to be in Privacy Enhanced Mail (PEM) base64 encoded format.

Typically, you install public Root Certificates from other TLS-capable servers and nodes that communicate with Interaction Gateway. These servers and nodes include other Interactive Intelligence products in your telephony network, such as Customer Interaction Center and Interaction SIP Proxy.

To install a Trusted Authority Certificate on Interaction Gateway, do the following steps:

1. Save the Trusted Authority Certificate on the hard disk drive of the personal computer that you use to access the Interaction Gateway web interface.
2. Open a web browser and log on to the Interaction Gateway web interface.
3. In the upper right corner, select the **Settings** icon.
4. On the left side of the page, select the **Certificates** tab.

   The **Settings-Certificates** page is displayed.
5. Locate the **Trusted Certificate Authorities** section in the middle of the page.
6. Select the **Browse** button to the right of the **Upload Certificate** box.
7. In the resulting dialog box, select the verified and signed certificate file on the hard disk drive of the personal computer.
8. Select the **Upload** button.

   The Trusted Authority Certificate is uploaded to Interaction Gateway and saved for future use with SIP/TLS connection requests.

Install the TLS Certificate on Interaction Gateway

1. Save the Certificate Signing Request (CSR) that you created in Generate the Interaction Gateway TLS certificate on the hard disk drive of the personal computer that you use to log on to the Interaction Gateway web interface.
2. Open a web browser and log on to the Interaction Gateway web interface.
3. In the top right corner, select the **Settings** icon.
4. On the left side of the page, select the **Certificates** tab.
5. On the **Settings-Certificates** page, locate the **Active TLS Certificate** area at the top of the page.
6. Select the **Browse** button that is located to the right of the **Import Certificate** box.
7. Locate and select the CSR on the hard disk of the personal computer.

8. Select the **Import** button.

   Interaction Gateway validates the CSR against the Trusted Authority Certificate that you uploaded in Install the Trusted Authority (Root) Certificate on Interaction Gateway.

> **Important!**
>
> After the Interaction Gateway validates the certificate, you must enable or reset the SIP TLS span before it takes effect. This action can cause a brief communication outage if the TLS span is currently active.

Edit the channel groups for Interaction Gateway

Channel groups enable you to assign specific TDM and SIP channels to logical groups, which you can then use in call routes. Through this feature, you can determine which channels are used for specific destination telephone numbers, such as reserving channels for long-distance dialing, local dialing, internal calls, company officers, or departments.

The following table provides an example of a small organization with four channel groups using one T1 TDM span:

Channel Group	Assigned TDM channels
Long Distance	1-16
Local	17-20
Toll Free	21,22
Chief Executive Officer	23

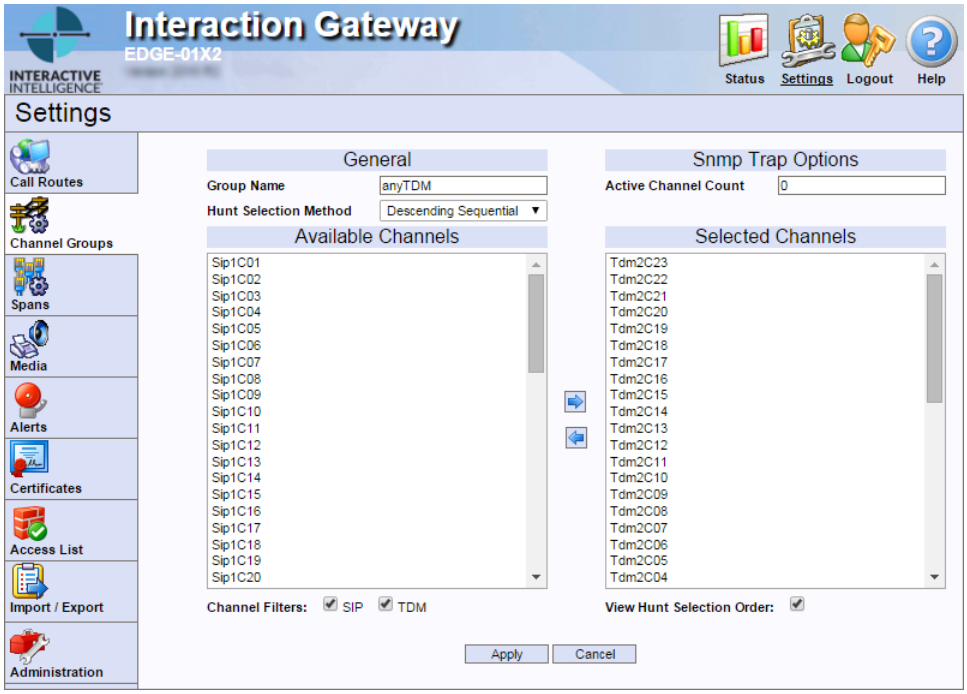
> **Note:**
>
> When you first add a TDM span to Interaction Gateway, all of the channels in that span are added to the **anyTDM** group.

To edit the channels that are assigned to a channel group, do the following steps:

1. Open a web browser and log on to the Interaction Gateway interface.
2. In the upper right corner of the web interface, select the **Settings** icon.
3. On the left side of the page, select the **Channel Groups** tab.

   The **Settings-Channel Groups** page is displayed.
4. Select a **Group Name** hyperlink to modify the list of selected channels. For example, select the **anyTDM** group hyperlink.

The following page is displayed.



Note:

A channel can be a member of multiple channel groups.

5. Depending on your need, do one of the following actions:
   - If you want to remove channels from this group, select one or more channels in the **Selected Channels** list and select the left arrow button.
   - If you want to add channels to this group, select one or more channels in the **Available Channels** list and select the right arrow button.

Tip:

You can select multiple channels in a list by using the **Shift** or **Ctrl** keys when you left-click a second item.

The selected channels are moved to the appropriate list.

6. After you have configured the channel group with the necessary channels, select the **Apply** button to save your changes and put them into service.

Note:

For more information about the controls on this page, see *Interaction Gateway Help*.

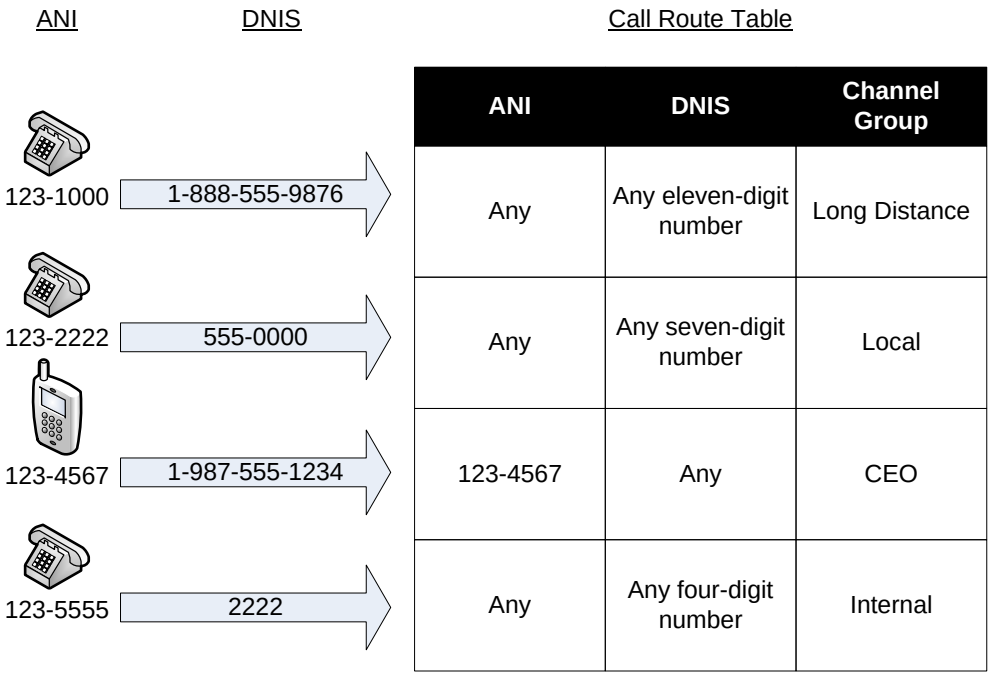
Modify the Interaction Gateway call route table

This section contains reference and procedural information regarding call route tables in Interaction Gateway.

Interaction Gateway call route table overview

A call route determines which channel group will handle a specific call, based on the dialed or originating telephone number. Multiple call routes comprise the *call route table*, which can route any dialed or originating telephone number in your organization.

The following image provides a simple example of a call route table and how it matches telephone numbers to route a call through a specific channel group.



ANI	DNIS	Channel Group
Any	Any eleven-digit number	Long Distance
Any	Any seven-digit number	Local
123-4567	Any	CEO
Any	Any four-digit number	Internal

To match telephone numbers, Interaction Gateway uses regular expressions as a pattern-matching language. This enables you to have one call route that covers multiple telephone numbers. For more information about regular expressions and how you can create them in Interaction Gateway, see *Interaction Gateway Help*.

Add a call route table entry in Interaction Gateway

1. Open a web browser and log on to the Interaction Gateway web interface.
2. In the upper right corner, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.
3. At the bottom of the **Call Routes** table, select the **Add Route** button.

   A new row is added to the bottom of the table.
4. Enter the appropriate regular expression for the following columns:
   - **ANI / From Address Matches**
   - **DNIS / To Address Matches**
   - **Route To Address**

> **Note:**
>
> The **Route To Address** field is case-sensitive. Use only lowercase characters.

5. In the **Channel Group** list for this new row, select the channel group to which you want these calls to use.
6. If you have not created any properties previously, leave the **Properties** list box with the **<default>** setting.
7. At the bottom of the page, select the **Apply** button.
8. Continue with the next procedure, Simulate a call through the new call route.

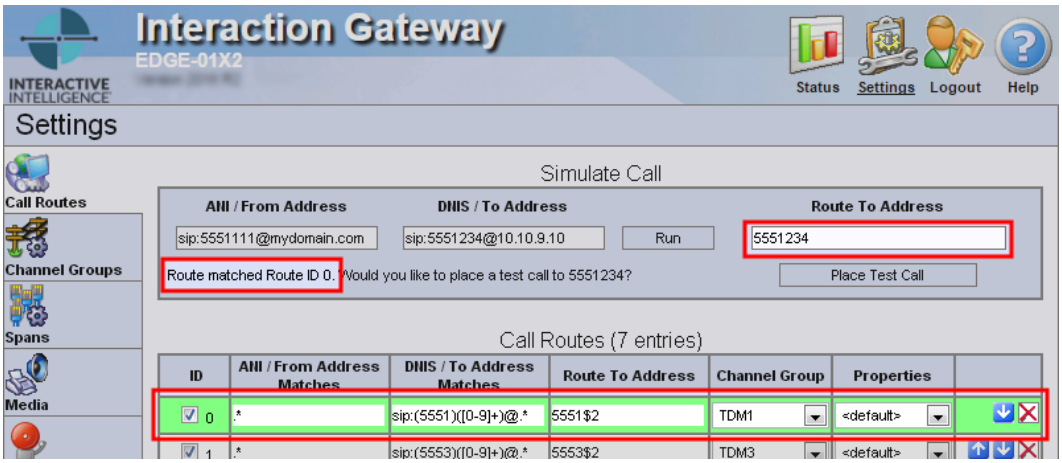
Simulate a call through the new call route

1. At the top of the page in the **Simulate Call** area, enter the calling telephone number in the **ANI / From Address** box.
2. Enter the destination telephone number in the **DNIS / To Address** box.
3. Select the **Run** button.

   If a match is found in the call routes, the following events occur:

   - The **Route To Address** box is filled with the configured routing address.
   - A status message is displayed.
   - The selected call route is highlighted in green.
   - A message and a **Place Test Call** button are displayed.

   If no call routes match the call, the **Route To Address** box displays **No Route Match!**

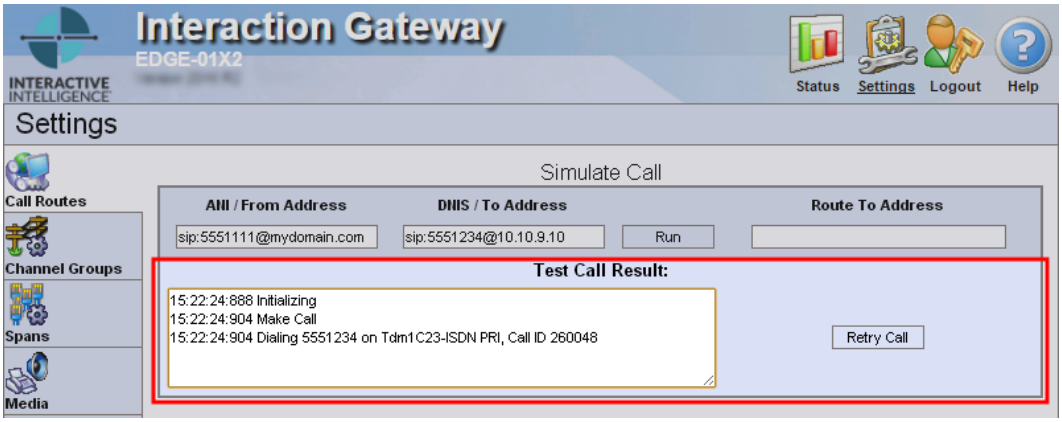


Tip:

You can disable a call route by removing the check mark next to the ID number of the route.

4. If you want Interaction Gateway to actually place a call to the address or telephone number specified in the **DNIS / To Address** box, select the **Place Test Call** button.

   A box with progress messages is displayed.



Interaction Gateway places a call to the specified destination. If the call fails, a cause code is displayed.

Add call properties for a call route

For each call route that you configure on the **Settings-Call Routes** page, you can assign independent call properties. These call properties enable you to override the call properties that Interaction Gateway derives from span settings and other areas.

To configure the properties for calls that match a call route, do the following steps:

1. Open a web browser and log on to the Interaction Gateway web interface.
2. In the upper right corner, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.
3. In the **Call Routes** table, select the **Modify** button at the bottom of the **Properties** column.

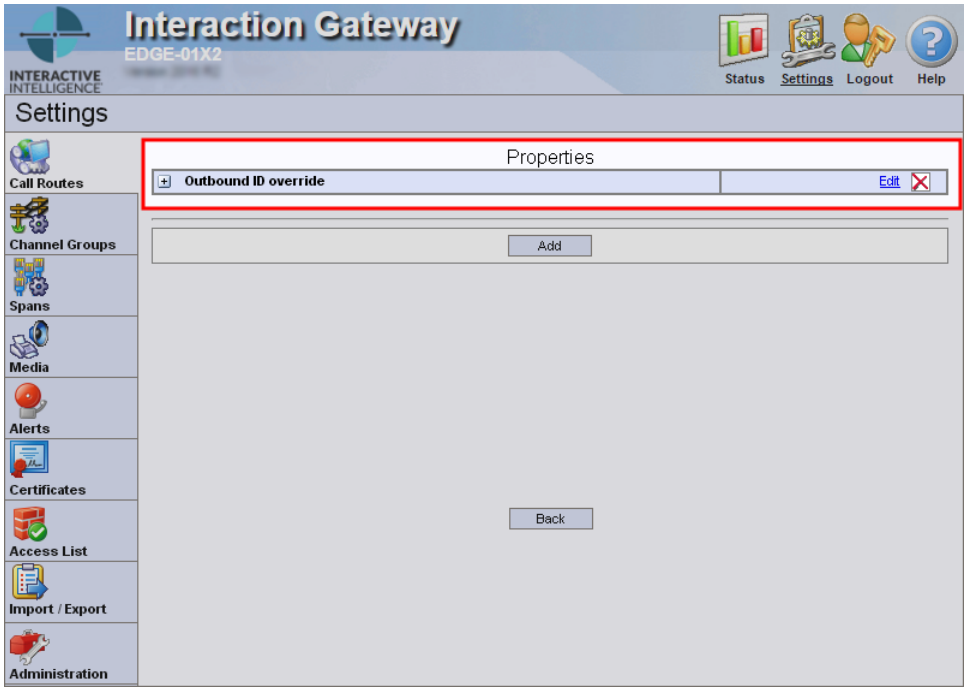
   If you have not defined call properties previously, only an **Add** button is displayed on the page.
4. Select the **Add** button.

   A page of configurable call properties is displayed.
5. In the **Property Name** box, enter a unique, identifiable name for this set of call properties.

   A value in the **Property Name** box is required.
6. Using the available controls, set the values for the call properties as necessary.

   For information about each call property, see *Interaction Gateway Help*.
7. When you are finished modifying this set of call properties, select the **Add** button.

   The name of the set of call properties is displayed in a list.



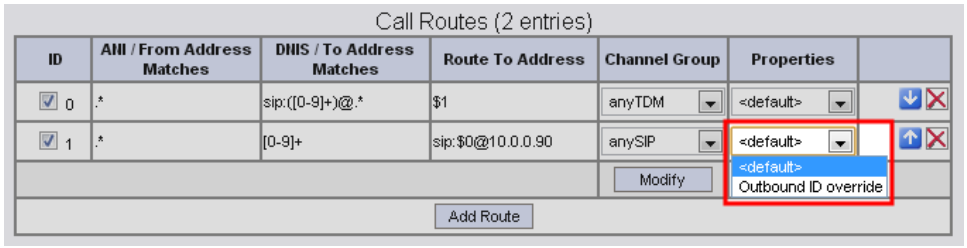
Tip:

Click the button to the left of any call property set to view the values it contains.

8. At the bottom of the page, select the **Back** button.

   The **Settings-Call Routes** page is displayed.

9. Click the **Properties** list box for a call route to select the new call property set.



10. At the bottom of the page, select the **Apply** button.

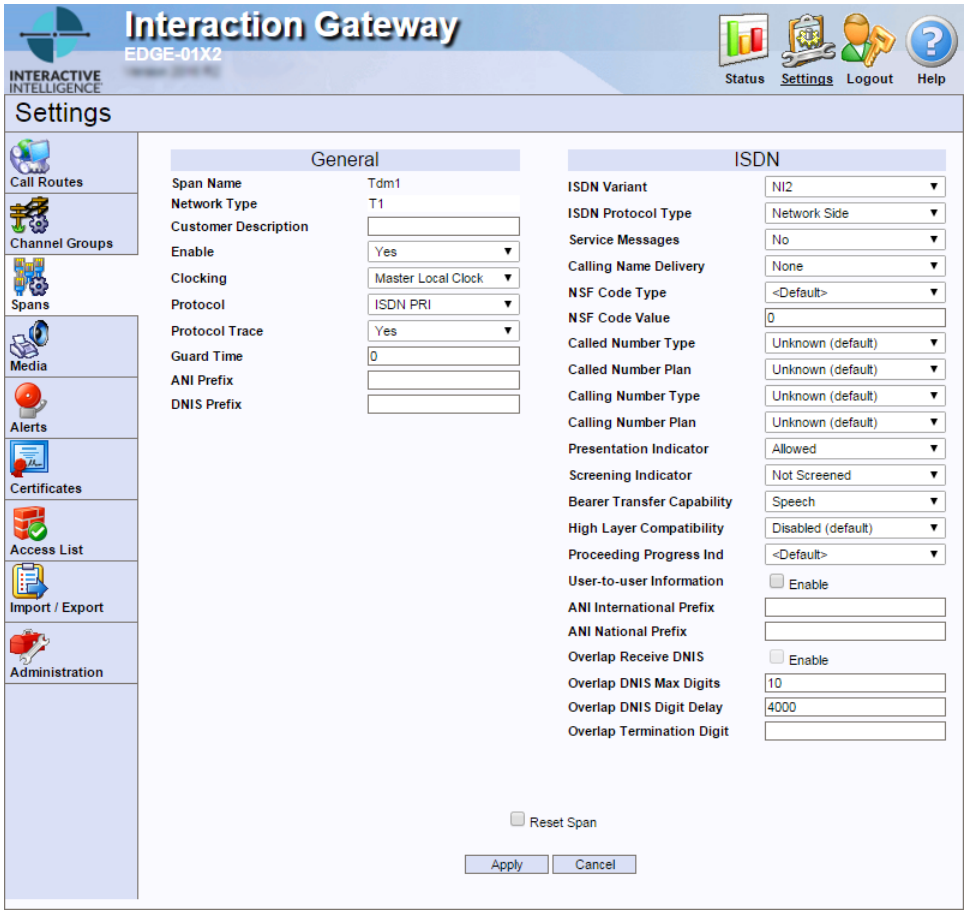
Set span clocking

Note:

By default, span clocks are set to **Normal**. This setting serves most TELCO circuits. Do not do this procedure unless it is required for a specific configuration, such as TDM spans connected to slave systems (PBX) that require a master clock from a TELCO circuit or loopback testing situations.

1. In the web interface, select the **Settings** icon in the upper right corner of the page.
2. On the left side of the page, select the **Spans** tab.
3. On the resulting page, select the TDM span for which you want to configure the clocking source.

   The settings for the selected span are displayed.



4. In the **Clocking** list box, select the appropriate clocking option:

   - **Normal** – The span receives its clocking from the connected TELCO circuit. This is the default setting and the only valid option to use for live TELCO circuits.

     Important!

     All TELCO circuits that are connected to the Interaction Edge appliance and are configured for the **Normal** setting must have synchronized clocks. TELCO circuit clocks that are not synchronized can result in poor audio quality and failed fax transmissions. In some infrequent instances, TELCO circuit clocks from different providers may not be synchronized. If a TELCO circuit provider cannot guarantee synchronized clocking with other TELCO circuit providers, you should use separate Interaction Edge appliances for the circuits from each TELCO provider.

   - **Master** – The span derives its clocking from Span 1. Use this selection when you have Span 1 configured in **Normal** mode and it is connected to a live TELCO circuit while other spans are connected to systems, such as PBX systems, that demand to be a slave entity of the circuit connection.
   - **Master Local Clock** – This span derives its own clocking from an internal hardware oscillator to synchronize devices that are connected to this span. You should use this selection only when performing *loopback* tests and not connected to a TELCO circuit.
   - **CO Loopback** – This span mirrors clocking and data to the central office (CO). This is a test-only mode selection. Interaction Gateway call functionality is not available with this selection and circuits will not provide a **Ready** status on the **Status** page.

5. Select the **Apply** button at the bottom of the page.

Migrate Generation 2 configuration to current version

If you have an Interaction Gateway Generation 2 appliance, you can migrate your configuration for spans, call routes, channel groups, and SNMP configurations to the current version of Interaction Gateway on the Interaction Edge appliance.

1. From a remote computer, log on to the Interaction Gateway Generation 2 FTP server with an FTP client program.

   Use the FTP user name and password that you configured through the Interaction Gateway Generation 2 web interface. The default FTP user name and password are `iguser` and `FetchL0gs`.

   > **Note:**
   >
   > The `FetchL0gs` password is case sensitive with a `0` (zero) instead of an `O` in L0gs.

2. Download the following configuration files from the Interaction Gateway Generation 2 appliance:

   - `SpanConfig.xml`
   - `ChannelGroupsConfig.xml`
   - `CallRoutesConfig.xml`
   - `SnmpConfig.xml`

3. Log on to Interaction Edge with an FTP client program.

   > **Note:**
   >
   > The default user name and password are `iguser` and `FetchL0gs`.

4. Using the FTP client program, upload the configuration files to the `Configurations` folder.

5. On the remote computer, open a web browser and navigate to the URL address of the current version of Interaction Gateway.

   > **Note:**
   >
   > The URL address of Interaction Gateway is the same as Interaction Edge except that it uses port 444. Specify the URL address as follows: `https://<IP_address>:444`

   The web browser displays the **Authentication Required** dialog box.

6. Enter the administrator user name and password, and then select the **OK** button.

   > **Note:**
   >
   > The default user name and password is `admin` and `1234`.

   The **Status-Spans** page is displayed.

7. In the upper right corner of the page, select the **Settings** icon.

8. On the left side of the page, select the **Import/Export** tab.

9. In the **Select Source File** list box of the **Import Stored Configuration** area, select a file in the following list in order.

   a. `SpanConfig.xml` – **Spans** check box

   b. `ChannelGroupsConfig.xml` – **Channel Groups** check box

   c. `CallRoutesConfig.xml` – **Call Routes** check box

   d. `SnmpConfig.xml` – **SNMP** check box

> **Note:**
>
> The **System** check box is for the importing of configuration files for the current version of Interaction Gateway.

10. For each configuration file, you must select check box that indicates what options you are importing. The previous step indicates the necessary check box with the bold font.

> **Tip:**
>
> To enable all options in the **Configuration Import Options** group, enable the **Select All Config Options** check box.

11. Select the **Import** button.
12. Repeat this procedure for each configuration file.

    The configuration from the file is imported into Interaction Gateway.

> **Important!**
>
> The **Trap Options for Call Disposition** section of the **SNMP** page is not updated through the import of the `SnmpConfig.xml` file. This is due to significant format changes from the Generation 2 configuration file syntax. You must manually configure this section to match your Generation 2 configuration.

Additional Interaction Gateway configuration tasks

This section contains the following topics:

Configure SNMP on Interaction Gateway

Use the **Settings-Snmp** page of the Interaction Edge web interface to define Simple Network Management Protocol (SNMP) connections to management systems and permissions.

For Interaction Gateway, use the **Settings-Alerts** tab to configure specific SNMP trap options for call thresholds and call dispositions.

For more information about configuring thresholds and call dispositions for SNMP trap messages, see *Interaction Gateway Help*.

Configure Interaction Gateway fax support

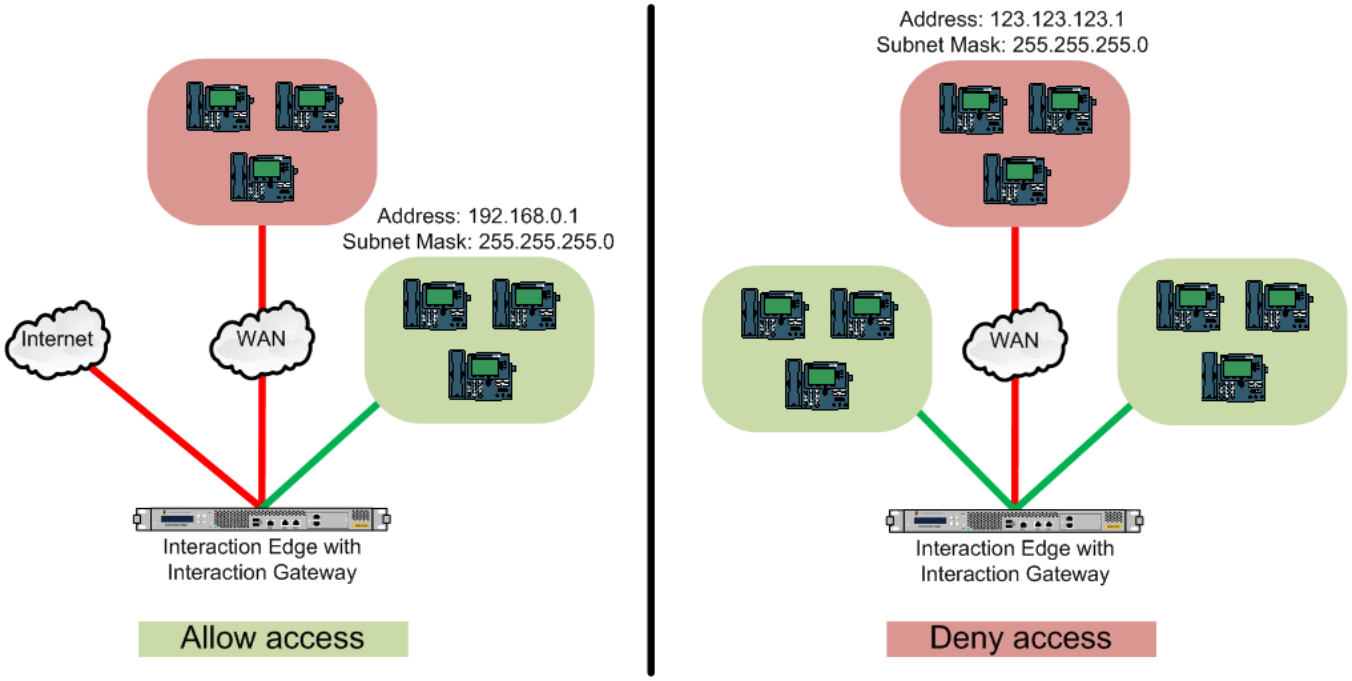
Use the **Settings-Media** page of the Interaction Gateway web interface to configure fax settings.

For more information about the controls for configuring fax support, see *Interaction Gateway Help*.

Control SIP message processing for IP addresses

Access List feature

The **Access List** page enables you to configure Interaction Gateway to allow or deny processing of SIP messages from defined IP addresses, as displayed in the following example:



When you define an entry on the **Access List** page, the combination of the IP address and subnet mask enables you to specify a single IP address or a range of IP addresses in that entry. You also define which SIP transport layer protocols (UDP, TCP, and TLS) are affected for SIP messages to and from the defined IP address.

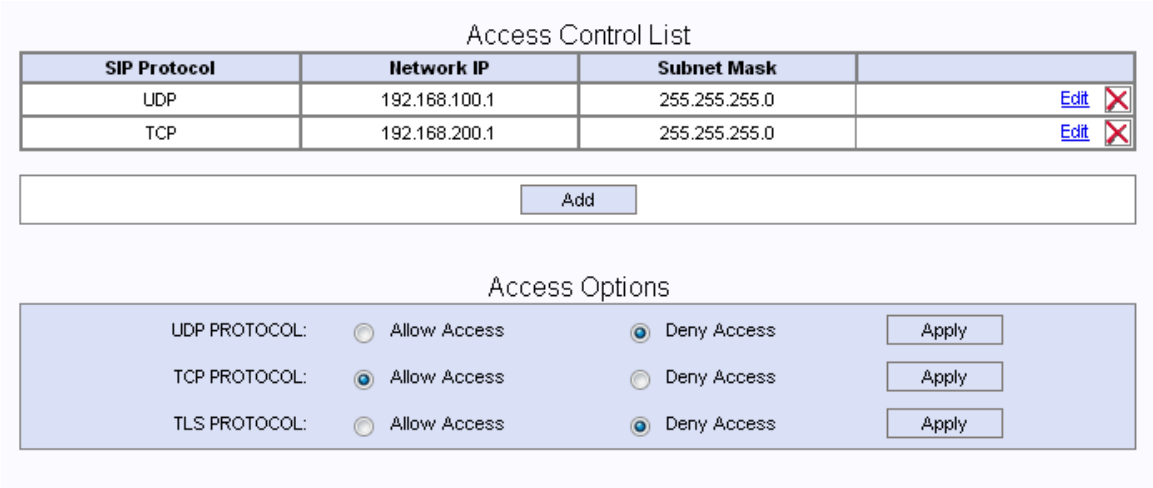
Before you create entries on the **Access List** page, you must first decide on the access method Interaction Gateway will use for each SIP transport layer protocol:

- Allow – Interaction Gateway processes SIP messages on the specified transport layer protocols for IP addresses that match entries in the table.
- Deny – Interaction Gateway processes SIP messages on the specified transport layer protocols for IP addresses that do not match entries in the table.

Important!

If you do not define any entries on the **Access List** page, ensure that the **Deny Access** option is applied. If you select and apply the **Allow Access** option and do not define entries in the **Access Control List** table, Interaction Gateway denies all SIP messages on the associated transport layer protocol for any IP address.

The following image displays the **Access List** page with example entries:



The following table describes how Interaction Gateway interprets the example entries in the **Access Control List** table with the selections in the **Access Options** area:

Protocol	IP address	Access
UDP	192.168.100.1 through 192.168.100.254	Denied
	All other IP addresses	Allowed
TCP	192.168.200.1 through 192.168.200.254	Allowed
	All other IP addresses	Denied
TLS	Any IP address	Allowed

Add an Access List entry

1. Log on to Interaction Gateway with the administrator user name and password.

   The **Status-Spans** page is displayed.

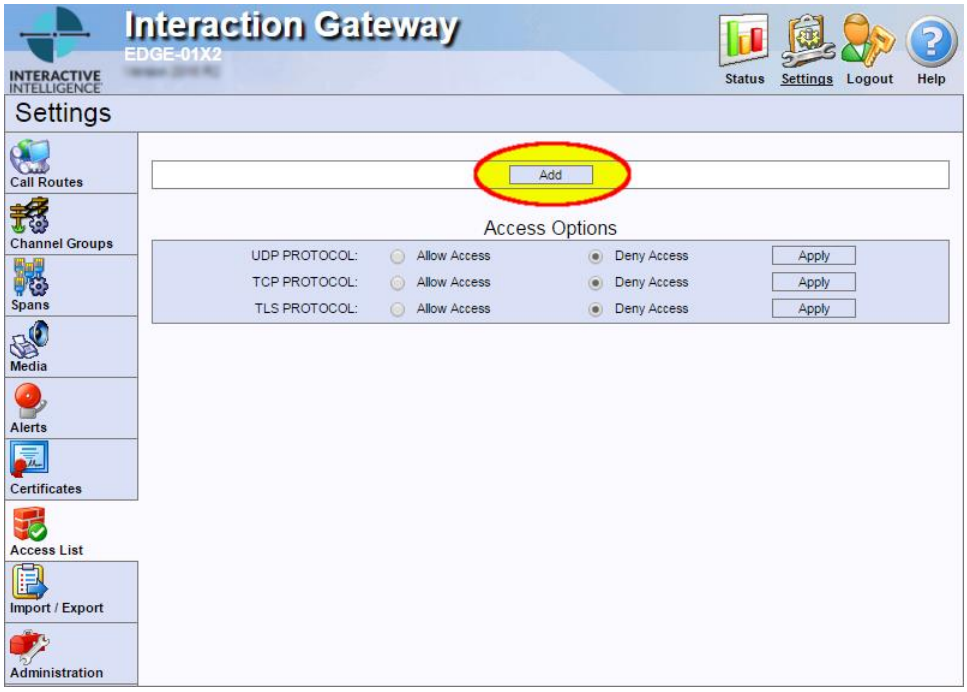
2. In the upper right corner, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.

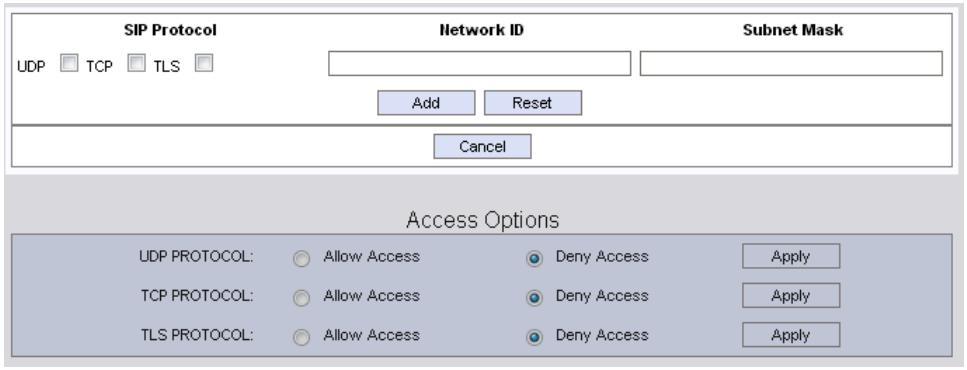
3. On the left side of the page, select the **Access List** tab.

   The **Settings-Access List** page is displayed.

4. Select the **Add** button.



   A row of controls is displayed.



5. Use the controls to define this entry.

   For descriptions of each control, see *Interaction Gateway Help*.

6. After you have entered the necessary information, select the **Add** button.

   The entry is added to the **Access Control List** table.

7. In the **Access Options** area, select either the **Allow Access** or **Deny Access** option for each transport layer protocol.

> **Note:**
> After you select an access option for a transport layer protocol, you must select the **Apply** button located to the right of the **Deny Access** option.

The selected access options are applied for all entries in the **Access Control List** table for the specified SIP type.

Protocol Trace files

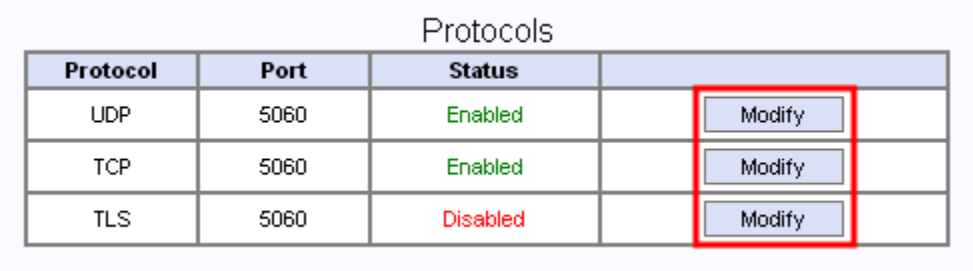
Interaction Gateway can record all processed network packets for a specific communication session in a packet capture (PCAP) file. You can analyze PCAP files to troubleshoot problems in SIP or other network communications. To analyze a PCAP file, you must first download the file to a remote computer through an FTP connection with Interaction Edge. You can then use a third-party software application to view the PCAP file.

Configure a span to create Protocol Trace files

1. In the upper right corner of the Interaction Gateway interface, select the **Settings** icon.
2. On the left side of the page, select the **Spans** tab.

   The **Settings-Spans** page is displayed.
3. On the **Settings-Spans** page, select the span for which you want Interaction Gateway to create protocol trace files.

   The configuration page for the selected span is displayed.
4. If you selected a TDM span, select **Yes** in the **Protocol Trace** list box and proceed to step 6. Otherwise, proceed to the next step.
5. For a SIP span, do the following steps:
   a. In the **Protocols** area, select the **Modify** button that is associated with the protocol for which you want to create protocol trace files.



   The configuration page for the selected SIP protocol is displayed.
   b. In the **Protocol Trace** list box, select **Yes**.
6. At the bottom of the page, select the **Apply** button.

> **Note:**
> Enabling the protocol trace feature applies only to the selected span. To create protocol trace files for all communications, you must repeat this procedure for all spans.

Delete Protocol Trace Files

Interaction Gateway deletes protocol trace files that are older than seven days. However, if you are doing extensive troubleshooting of multiple spans, you may want to delete protocol trace files before Interaction Gateway automatically deletes them.

1. In the upper right corner of the Interaction Gateway interface, select the **Settings** icon.
2. On the left side of the page, select the **Spans** icon.
3. On the Settings-**Spans** page, select the **Protocol Trace File Management** hyperlink.
4. In the **Capture Trace File Names** list, select one or more protocol trace files that you want to delete.

> **Tip:**
>
> To select multiple, individual files, hold down the **Ctrl** key and click each additional file name that you want to delete. To select a consecutive range of files, click a file name, hold down the **Shift** key, and select the last file name that you want to delete.

5. Select the **Delete** button.

> **Caution!**
>
> You cannot recover deleted protocol trace files. Ensure that you have selected the appropriate files before you select the **Delete** button. Selecting the **Cancel** button does not restore deleted files.

6. Select the **Cancel** button to return to the **Settings-Spans** page.

ISDN cause code and SIP response custom mappings

Overview

Both ISDN and SIP communications use numeric codes to represent specific events, which include expected results and unexpected errors. Interaction Gateway uses default mappings between ISDN cause codes and SIP responses. These default mappings equate a numeric value for one communication method to a numeric value for the other method. For example, a SIP response of 0 (zero), by default, is mapped to the ISDN cause code of 16. This mapping is reciprocated in the mapping of ISDN cause code 16 to the SIP response of 0 (zero).

Interaction Gateway enables you to override the default mappings with custom mappings. For example, consider the following default mapping:

SIP response	ISDN cause code
400 – Bad Request	99 - Information Element Nonexistent Or Not Implemented

Using custom mappings, you can change the mappings, for both SIP to ISDN and ISDN to SIP, to return a different numeric value:

SIP response	ISDN cause code
404 – Not Found (User not found)	99 – Information Element Nonexistent Or Not Implemented

The following rules apply to custom mappings:

- You can create only one custom mapping for a single numeric value.

- You can create custom mappings for multiple numeric codes in one communication method to a single numeric code in the other communication method.

  The following table provides examples of default mappings that use these rules:

SIP to ISDN mapping		ISDN to SIP mapping	
SIP response	**ISDN cause code**	**ISDN cause code**	**SIP response**
400	127	5	400
~~400~~	~~5~~	7	400
~~400~~	~~7~~	8	400
~~400~~	~~8~~	9	400

Note:

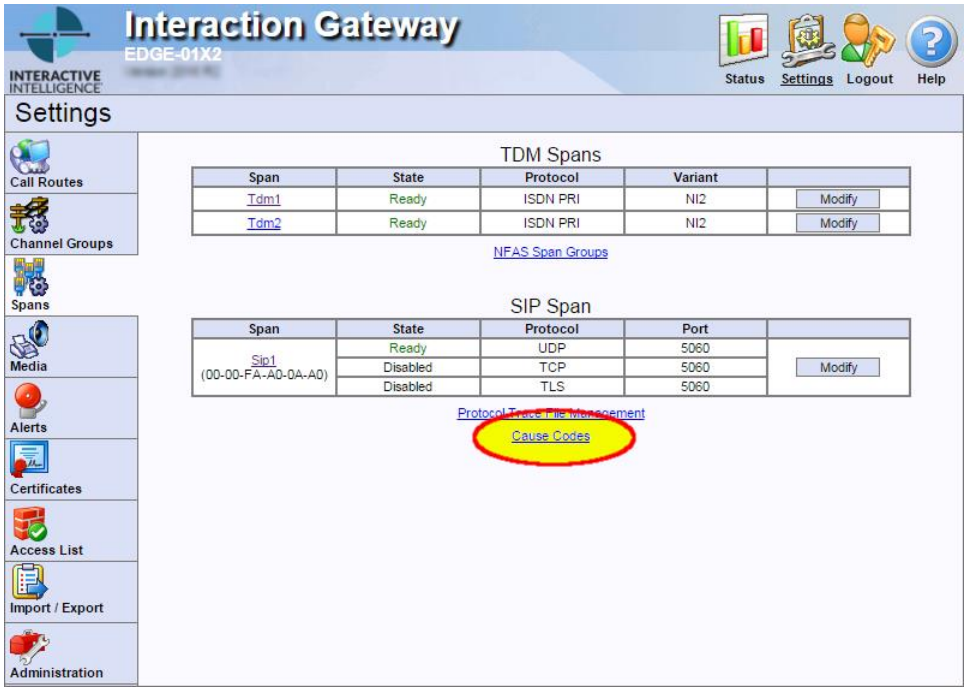
Interaction Gateway applies all custom mappings across all ISDN TDM and SIP spans.

You access the cause code mappings interface by selecting the **Cause Codes** hyperlink on the **Settings-Spans** page.

Create a custom mapping

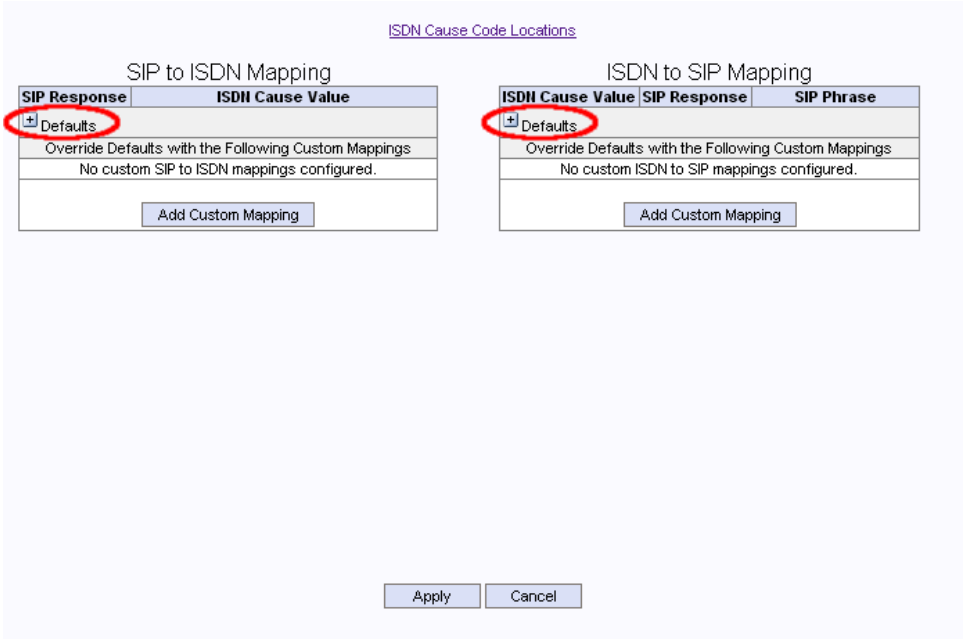
1. In the web interface, select the **Settings** icon in the upper right corner of the page.
2. On the left side of the page, select the **Spans** tab.

   The **Settings-Spans** page is displayed.



3. Select the **Cause Codes** hyperlink.

The page for mapping cause codes is displayed.

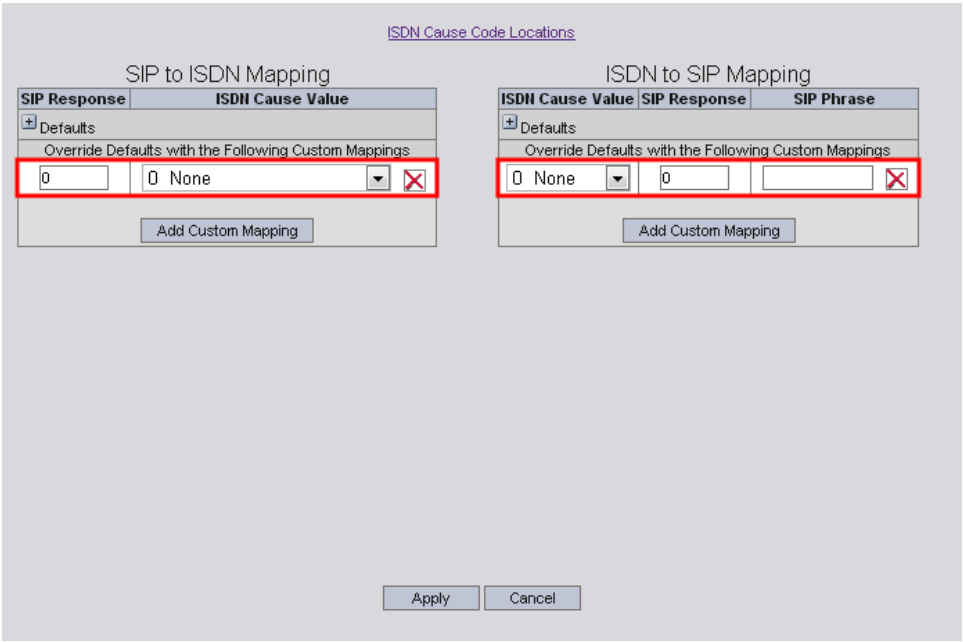


Note:

To view the default mappings, select the **Defaults** button for each mapping table.

4. To add a custom mapping, select the **Add Custom Mapping** button at the bottom of the appropriate mapping table.

   A row of controls is displayed.



   The controls are associated with the headings at the top of each mapping table.

   For more information about each control, see "Cause Code Mappings" in *Interaction Gateway Help*.

5. Using the available controls, enter the necessary information for this custom mapping.

> **Note:**
>
> If you want to abandon entering a custom mapping, either select the **Cancel** button to clear any information and return to the **Settings-Spans** page or select the Delete button (**X**) on the right side of the row of controls.

6. After you have entered the information, select the **Apply** button.

   Interaction Gateway saves this custom mapping to the configuration and displays a result message. When you select the **OK** button for the results message, the **Settings-Spans** page is displayed.

ISDN cause code locations

The ISDN Cause Code Locations feature enables you to set one specific location for a single ISDN cause code value. The location identifies the network entity that issued the specified ISDN cause code. Some carriers require you to submit a specific location with ISDN cause codes, which you can do with this feature. ISDN cause code locations apply to all ISDN TDM spans defined in Interaction Gateway. If you specify a location other than **Default** for an ISDN cause code, Interaction Gateway always returns that specified location.

Access the ISDN Cause Code Locations Page

1. In the upper right corner of the Interaction Gateway web interface, select the **Settings** icon.

   The **Settings-Call Routes** page is displayed.

2. On the left side of the page, select the **Spans** tab.

   The **Settings-Spans** page is displayed.

3. At the bottom of the page, select the **Cause Codes** hyperlink.

4. At the top of the resulting page, select the **ISDN Cause Code Locations** hyperlink.

For information about the controls you use to configure ISDN Cause Code Locations, see *Interaction Gateway Help*.

Configure Interaction Gateway to restrict calling party number for ISDN connections

You can block the telephone number of a calling party on an ISDN inbound call that has the `Presentation Restricted` setup message.

1. Log on to Interaction Gateway.

2. In the upper right corner, select the **Settings** icon.

3. On the left side of the page, select the **Administration** tab.

4. In the **System Parameters** section of the resulting page, enter the following text into the left blank box:

   `restrictedCallingNumber`

5. In the right blank box, enter **`Block`**.

6. At the bottom of the page, select the **Apply** button.

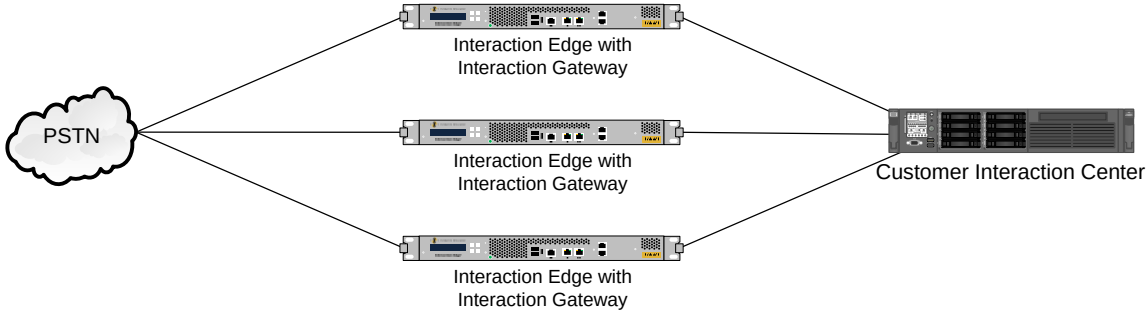
Configure Customer Interaction Center for Interaction Gateway

This section provides information about configuring Customer Interaction Center (CIC) for use with Interaction Gateway.

CIC manages SIP communications for entities that you define through Interaction Administrator. These entities include Interaction Gateway. There are multiple methods in which you can configure CIC for interoperability with Interaction Gateway. You can select one of the following methods for sending SIP calls from CIC through Interaction Gateway:

Create a SIP line for each Interaction Gateway system

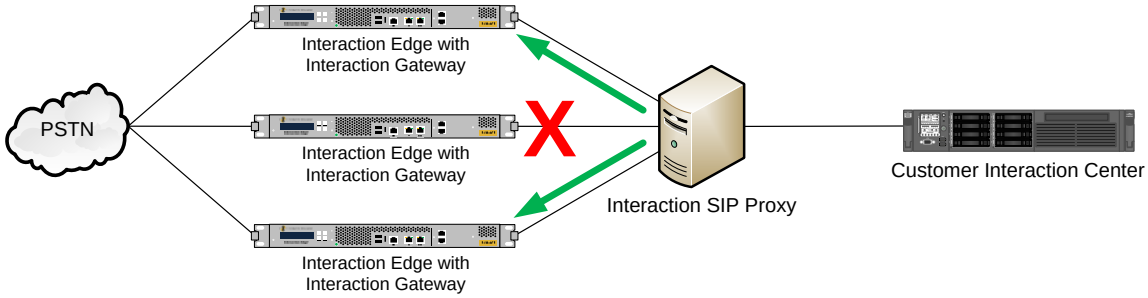
You can create a SIP line for each Interaction Gateway system. You can organize these SIP lines into a *line group* and configure that line group to use a *round-robin* method of call distribution for selecting a SIP line to service a call. Use this line group in your CIC dial plan to direct outbound calls.



One disadvantage of this method is that if an Interaction Gateway system is unavailable, CIC is not aware of the problem and continues to send SIP calls to that Interaction Gateway system.

Create a SIP line for Interaction SIP Proxy

You can create a SIP line and configure it to deliver SIP calls to an Interaction SIP Proxy server. You can then configure that Interaction SIP Proxy server to distribute calls to multiple Interaction Gateway systems. You can also provide additional call routing options through Interaction SIP Proxy.



Interaction SIP Proxy can monitor the status of SIP communications with a defined destination, such as Interaction Gateway. If an Interaction Gateway system becomes unavailable, Interaction SIP Proxy puts the unresponsive destination on probation for a period of time. During this period of time, Interaction SIP Proxy

does not send new SIP calls to that destination. This method ensures that you do not lose outbound SIP calls through unavailable Interaction Gateway systems.

You can further define SIP lines through the **Regionalization** container in Interaction Administrator, including supported codecs.

Create a SIP Line for a Interaction Gateway system or Interaction SIP Proxy server

1. Open Interaction Administrator.
2. In the navigation pane on the left side of the window, select the **Lines** container.
3. In the pane on the right side of the window, right click an open area and select **New** from the resulting shortcut menu.

   The **Line Configuration** dialog box is displayed.
4. Depending on your release of Customer Interaction Center (CIC) and any applied updates, configure the SIP line to conform to the settings:
   - Create a SIP Line in CIC 3.0 GA through SU8
   - Create a SIP Line in CIC 3.0 SU8 or later
   - Create a SIP Line in CIC 4.0 GA through SU1
   - Create a SIP Line in CIC 4.0 SU2 or later, or CIC 20nn Rn

For more information about creating a SIP line and descriptions of all controls, see *Interaction Administrator Help*.

Create a SIP Line in CIC 3.0 GA through SU8

Tab/Page	Control	Description
SIP Line Configuration tab/**Line** page	**Active** check box	Enable this check box to activate this SIP line after you finish creating it. **Tip:** You can use this check box to deactivate this SIP line and remove Interaction Gateway from service for the Customer Interaction Center server.
	Phone Number box	Enter a telephone number to use as the `From` header in outbound SIP calls.
	Domain Name box	Enter a DNS name to use as the host portion for SIP addresses. **Note:** If you are using Interaction Dialer and it selects this SIP line for a call, the Interaction Dialer configuration overrides the entry in the **Domain Name** box.
	Call Analysis Type list box	This version of Interaction Gateway does not support call analysis for these update levels of Customer Interaction Center 3.0.
SIP Line Configuration tab/**Session** page	**Disable Delayed Media** check box (GA)	Enable this check box. If this check box is disabled, callers cannot hear pre-connect audio, such as special information tones (SIT).
	Media Timing list box (SU1 or later)	Select the **Normal** item. If you select the **Delayed** item, callers cannot hear pre-connect audio, such as special information tones (SIT).
	ASR Enabled check box	If you are using Interaction Dialer, enable this check box. Otherwise, leave this check box disabled.
SIP Line Configuration tab/**Proxy** page	**Prioritized list of Proxy IP addresses** list box	Select the **Add** button, enter the IP address of the Interaction Edge appliance, and select the **OK** button. The default port number is 5060. This configuration causes Customer Interaction Center to send all calls on this SIP line directly to Interaction Gateway. If you are using a separate Interaction SIP Proxy server in your Customer Interaction Center network, you can instead enter its IP address.

		Note: If you direct this SIP line to an Interaction SIP Proxy server, you must configure the call routes on Interaction SIP Proxy server to send calls to the IP address of the Interaction Edge appliance.

Create a SIP Line in CIC 3.0 SU8 or later

Tab/Page	Control	Description
SIP Line Configuration tab/**Line** page	**Active** check box	Enable this check box to activate this SIP line after you finish creating it. **Tip:** You can use this check box to deactivate this SIP line and remove Interaction Gateway from service for the Customer Interaction Center server.
	Domain Name box	Enter a DNS name to use as the host portion for SIP addresses. **Note:** If you are using Interaction Dialer and it selects this SIP line for a call, the Interaction Dialer configuration overrides the entry in the **Domain Name** box.
	Call Analysis Type list box	To use call analysis, select **Internal to Interaction Gateway**. This selection requires Interaction Media Server in your Customer Interaction Center network.
SIP Line Configuration tab/**Session** page	**Media Timing** list box	Select the **Normal** item. If you select the **Delayed** item, callers cannot hear pre-connect audio, such as special information tones (SIT).
	ASR Enabled check box	If you are using Interaction Dialer, enable this check box. Otherwise, leave this check box disabled.
SIP Line Configuration tab/**Proxy** page	**Prioritized list of Proxy IP addresses** list box	Select the **Add** button, enter the IP address of the Interaction Edge appliance, and select the **OK** button. The default port number is 5060. This configuration causes Customer Interaction Center to send all calls on this SIP line directly to Interaction Gateway. If you are using a separate Interaction SIP Proxy server in your Customer Interaction Center network, you can instead enter its IP address. **Note:** If you direct this SIP line to an Interaction SIP Proxy server, you must configure the call routes on Interaction SIP Proxy server to send calls to the IP address of the Interaction Edge appliance.

Create a SIP Line in CIC 4.0 GA through SU1

Tab/Page	Control	Description
SIP Line Configuration tab/**Line** page	**Active** check box	Enable this check box to activate this SIP line after you finish creating it. **Tip:** You can use this check box to deactivate this SIP line and remove Interaction Gateway from service for the Customer Interaction Center server.
	Domain Name box	Enter a DNS name to use as the host portion for SIP addresses. **Note:** If you are using Interaction Dialer and it selects this SIP line for a call, the Interaction Dialer configuration overrides the entry in the **Domain Name** box.
	Call Analysis Type list box	To use call analysis, select **Internal (Media Server) to Interaction Gateway**. This selection requires Interaction Media Server 4.0 or 20*nn* R*n* in your Customer Interaction Center network. This setting differs from the **Internal (Media Server)** setting in that it directs Interaction Gateway to handle line signaling for audio in the most optimal manner for call analysis performance. **Important!** The **Interaction Gateway** item in the **Call Analysis Type** list box applies only to Interaction Gateway Generation 2 and not this version of Interaction Gateway.
SIP Line Configuration tab/**Session** page	**Media Timing** list box	Select the **Normal** item. If you select the **Delayed** item, callers cannot hear pre-connect audio, such as special information tones (SIT).
	ASR Enabled check box	If you are using Interaction Dialer, enable this check box. Otherwise, leave this check box disabled.
SIP Line Configuration tab/**Proxy** page	**Prioritized list of Proxy addresses** list box	Select the **Add** button, enter the IP address of the Interaction Edge appliance, and select the **OK** button. The default port number is 5060. This configuration causes Customer Interaction Center to send all calls on this SIP line directly to Interaction Gateway. If you are using a separate Interaction SIP Proxy server in your Customer Interaction Center network, you can instead enter its IP address.

		Note: If you direct this SIP line to an Interaction SIP Proxy server, you must configure the call routes on Interaction SIP Proxy server to send calls to the IP address of the Interaction Edge appliance.

Create a SIP Line in CIC 4.0 SU2 or later, or CIC 20*nn* R*n*

Tab/Page	Control	Description
SIP Line Configuration tab/**Line** page	**Active** check box	Enable this check box to activate this SIP line after you finish creating it. **Tip:** You can use this check box to deactivate this SIP line and remove Interaction Gateway from service for the Customer Interaction Center server.
	Line Usage list box	Select **General Purpose**.
	Domain Name box	Enter a DNS name to use as the host portion for SIP addresses. **Note:** If you are using Interaction Dialer and it selects this SIP line for a call, the Interaction Dialer configuration overrides the entry in the **Domain Name** box.
	Call Analysis Type list box	To use call analysis, select **Media Server to Interaction Gateway**. This selection requires Interaction Media Server 4.0 SU2 or later, or Interaction Media Server 20*nn* R*n* in your Customer Interaction Center network. This setting differs from the **Media Server** setting in that it directs Interaction Gateway to handle line signaling for audio in the most optimal manner for call analysis performance. **Important!** The **Interaction Gateway** item in the **Call Analysis Type** list box applies only to Interaction Gateway Generation 2 and not this version of Interaction Gateway.
SIP Line Configuration tab/**Session** page	**Media Timing** list box	Select the **Normal** item. If you select the **Delayed** item, callers cannot hear pre-connect audio, such as special information tones (SIT).
	ASR Enabled check box	If you are using Interaction Dialer, enable this check box. Otherwise, leave this check box disabled.
SIP Line Configuration tab/**Proxy** page	**Prioritized list of Proxy addresses** list box	Select the **Add** button, enter the IP address of the Interaction Edge appliance, and select the **OK** button. The default port number is 5060. This configuration causes Customer Interaction Center to send all calls on this SIP line directly to Interaction Gateway. If you are using a separate Interaction SIP Proxy server in your Customer

		Interaction Center network, you can instead enter its IP address. **Note:** If you direct this SIP line to an Interaction SIP Proxy server, you must configure the call routes on Interaction SIP Proxy server to send calls to the IP address of the Interaction Edge appliance.

Interaction Gateway updates

Interactive Intelligence provides Interaction Edge updates that include the latest release of Interaction Gateway software. For more information about these updates, see *Interaction Edge Installation and Configuration Guide* and the *Interaction Edge Updates* whitepaper on the Interaction Edge product information website.

Caution!

Applying an Interaction Edge update to the General Availability (GA) version of Interaction Edge erases all Interaction SIP Proxy and Interaction Media Server SNMP configuration settings. You must record these SNMP settings for both products and manually enter them in the new Interaction Edge **SNMP** page to restore the prior SNMP functionality for these products.

Information gathering and troubleshooting

This section explains items that Interactive Intelligence technical support personnel need to diagnose potential problems with your Interaction Gateway system.

View Admin Log

The Admin Log feature enables you to review many different types of events for Interaction Gateway.

> **Note:**
>
> Interaction Gateway does not automatically delete Admin Log entries. To remove all Admin Log entries, select the **Clear Log** button.

1. In the upper right corner of the Interaction Gateway interface, select the **Status** icon.
2. On the left side of the page, select the **Admin Log** tab.

   The Admin Log page is displayed.
3. Use the controls on the page to configure which events are displayed on this page.

   For more information about the controls on this page, see *Interaction Gateway Help*.

Enable diagnostic recordings

If you have problems with call connections and audio for PSTN carriers, do the following procedures in this section to create diagnostic recordings. After you have configured these settings and replicated the problems, contact Interactive Intelligence technical support and supply the diagnostic recordings for analysis.

Enable span protocol tracing

1. In the upper right corner of the Interaction Gateway interface, select the **Settings** icon.
2. On the left side of the page, select the **Spans** tab.
3. Set the **Protocol Trace** list box to **Yes**.
4. At the bottom of the page, select the **Apply** button.

Activate diagnostic audio captures

1. In the upper right corner of the Interaction Gateway interface, select the **Settings** icon.
2. On the left side of the page, select the **Administration** tab.
3. In the **Audio Capture Count** box in the **Diagnostics** section, enter `20`.
4. At the bottom of the page, select the **Apply** button.

> **Note:**
>
> Diagnostic audio captures are erased after 7 days. Additionally, Interaction Gateway will not record diagnostic audio captures if the available internal storage space is insufficient.

Gather log and trace files

If issues develop that suggest a problem in Interaction Gateway, Interactive Intelligence technical support staff will likely request log and trace files from the Interaction Gateway software, Interaction Edge appliance, and any related Interactive Intelligence systems. The following lists summarize files that are generally needed to troubleshoot Interaction Gateway problems.

Interaction Edge and Interaction Gateway files:

The following files are located in the `\Logs` directory:

- AdminLog.csv
- CallLog.csv
- IGateway.ininlog
- SIPEngine-IG.ininlog

The following files are located in date-specific directories under the \Logs directory:

- D-Channel trace log files

  These files are named Tdm*x*_*yyyyyy*.pcap where *x* represents the TDM span number and *yyyyyy* represents the time that logging was started. For example, Tdm1_072412.pcap indicates the D-channel trace on span 1 was started at 7:24:12 AM.

- SIP protocol trace files

  These log files contain packet capture (PCAP) information. They are named Sip*XXX*_*yyyyyy*.pcap, where the *XXX* represents the protocol configured for tracing (UDP, TCP, or TLS) and *yyyyyy* represents the time the tracing started. For example, Sip1UDP_072412.pcap indicates the SIP tracing on UDP traffic started at 7:24:12 AM.

Customer Interaction Center server files:

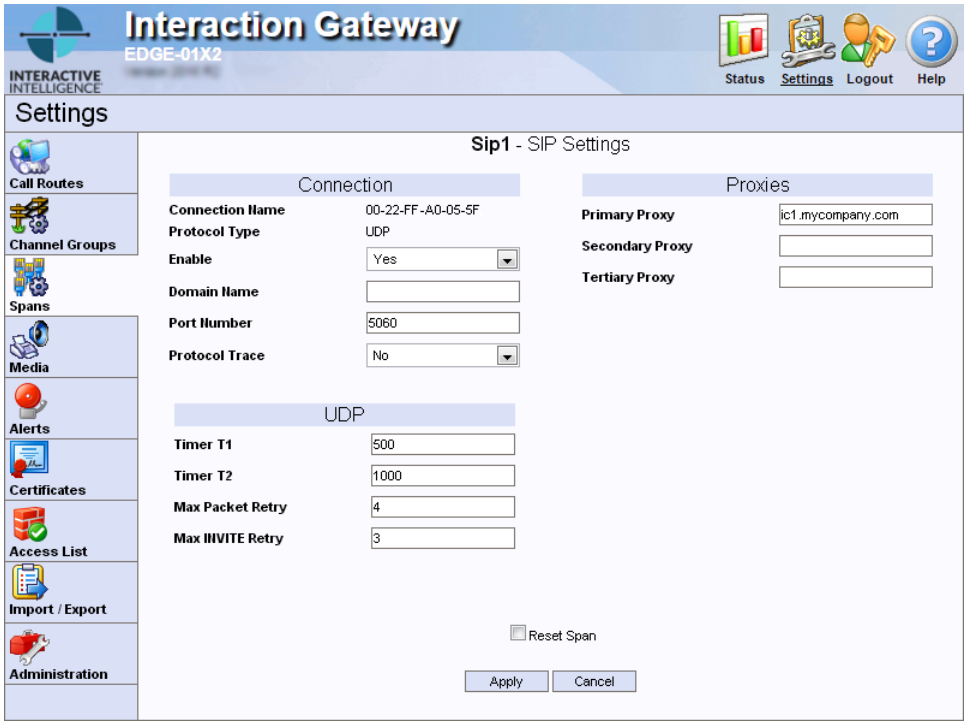
- TsServer.ininlog and SIPEngine.ininlog from the appropriate days.

Incoming calls are failing

When Interaction Gateway receives incoming calls from carriers, it establishes the Voice over IP (VoIP) portion of the call through Session Initiation Protocol (SIP) messages to a SIP receiver, such as a Customer Interaction Center server or Interaction SIP Proxy. The SIP receiver can then connect the call with a SIP endpoint, such as an IP telephone. If the SIP receiver does not respond within a certain period of time, the carrier may drop the call when its connection timer expires.

The problem of dropped calls by the carrier can result if the SIP receiver is not reachable because of a network outage or if the SIP receiver cannot respond quickly as can happen with system outages or overtaxed systems.

Interaction Gateway does not currently monitor the state of SIP receivers that you define in the **Proxies** section of the protocol settings page for a SIP span. As a result, Interaction Gateway will attempt to establish SIP calls through the SIP receiver specified in the **Primary Proxy** box until the connection timer expires and the configured number of reattempts is executed, even if the SIP receiver is unavailable. Only when the connection timers expire and the number of reattempts is executed will Interaction Gateway attempt to connect the call to the SIP receiver specified in the **Secondary Proxy** box. If the accumulated time that Interaction Gateway accrues while attempting to connect the call exceeds the connection timers from the carrier, the carrier will drop the call.



To correct this problem, you can use an Interaction SIP Proxy server as the **Primary Proxy**. Interaction SIP Proxy monitors the availability of SIP receivers and will route SIP messages to only those systems that are available.

If you do not have an Interaction SIP Proxy server, you can decrease the number of milliseconds in the timer controls in the same protocol setting page of the SIP span:

Protocol	Settings
UDP	Decrease the number of milliseconds that Interaction Gateway waits for a response or before reattempting connection in the **Timer T1** and **Timer T2** boxes. You can also lower the number of attempts that Interaction Gateway sends to a SIP receiver through the **Max Packet Retry** and **Max INVITE Retry** boxes. These decreases in time and attempts can enable Interaction Gateway to attempt establishing the SIP call with the SIP receivers specified in the **Secondary Proxy** and **Tertiary Proxy** boxes before the carrier drops the call.
TCP/TLS	Decrease the number of milliseconds that Interaction Gateway waits for a response in the **Connect Time** box.

For more information about the controls on the protocol settings page for a SIP span, see *Interaction Gateway Help*.

Important!

You should not modify the timers or retry controls for the SIP span unless directed to do so by an Interactive Intelligence Support representative. All network environments have many variables that affect latency, accumulated time, discarded packets, and so on. Improper settings can cause all subsequent call connection attempts to fail.

Tip:

Before you modify the timers or retry controls for the SIP span, contact your carrier to determine the amount of time that it allows to pass before it abandons the call attempt. Use this amount of time to determine the values that you set for the timers and retry attempts in the protocol settings of the SIP span. Ensure that you do not lower the values to a point where responses from the SIP receivers are ignored. If you change the timer values and the number of retry attempts, Interactive Intelligence recommends that you first test these settings in a non-production environment to ensure that you do not impact business operations.

Change Log

The following changes have been made to this document since release:

Date	Change
May 1, 2012	Initial Release
October 19, 2012	Service Update 1
May 21, 2013	Service Update 2
December 17, 2013	Service Update 3
August 28, 2014	Updated documentation to reflect changes required in the transition from version 4.0 SU# to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to Interactive Intelligence Product Information site URLs, and copyright and trademark information.
March 10, 2015	• Updated "Copyright and Trademark Information" page • Updated content to reflect change in versioning paradigm • Updated content to reflect new terminology and methods for updates • Updated screen shots to reflect new UI labels and controls • Added admonishment that specifies the default SIP ports used by Interaction Gateway and Interaction SIP Proxy, if hosted on Interaction Edge
November, 16, 2015	• Corporate rebranding

Index