PureConnect®

2023 R2

Generated:

30-May-2023

Content last updated:

8-February-2021

See Change Log for summary of changes.

GENESYS™

Short Message Services

Technical Reference

Abstract

This document describes how to set up and configure CIC to send, receive, and route messages using the Short Message Service (SMS) protocol.

For the latest version of this document, see the PureConnect Documentation Library at: http://help.genesys.com/pureconnect.

Table of Contents

Overview of SMS in CIC

This section covers:
- [How CIC supports SMS](#)
- [Understanding and choosing SMS Brokers](#)
- [Recover of SMS Interactions in Switchover](#)

SMS stands for *Short Message Service*. SMS allows users to exchange text messages between cell phones, e-mail accounts, and CIC user accounts. SMS messages can be up to 160 characters long when Latin alphabets are used. When non-Latin alphabets such as Arabic or Chinese are used, SMS messages are limited to 70 characters.

SMS operates over voice networks and uses available voice bandwidth to send messages. In Europe and Asia, SMS messages are usually sent over the *Global System for Mobile Communications* (GSM). GSM is a system for analog voice with modulated digital capabilities built in. SMS messages in the USA are sent over CDMA (*Code Division Multiple Access*), which transmits digital information as a radio signal. *General Packet Radio Service* (GPRS) is gaining popularity as it is faster and packet-driven instead of time-driven.

SMS Setup and Licensing

Customer Interaction Center includes SMS features by default. You do not need to install SMS features separately. To use them, make sure your server license provides SMS services by checking for `I3_FEATURE_SMS` in Interaction Administrator License Management as well as I3_FEATURE_WEB_SERVICES to allow for inbound SMS routing as a chat. Customers with an Intermediate Server license will need to upgrade to the Advanced Server license which contains this feature.

You must also:
- Contract with an SMS broker to route SMS messages to and from your CIC server.
- Use HTTP or HTTPS to connect with your chosen SMS broker.

How CIC supports SMS

Customer Interaction Center provides an integrated SMS Server subsystem that connects with external *SMS brokers* to exchange messages. The SMS Server subsystem arbitrates between SMS brokers and internal CIC subsystems, such as ACD Server, Reporting, and Recorder. When a CIC user sends an SMS message to a cellphone, the CIC server forwards the message to an SMS broker, which sends it on to the cellphone. When a cellphone user sends an SMS message to the phone number of the SMS broker, the broker pushes the message to the CIC server. The CIC server then converts the SMS message to a specialized SMS object and routes it to the agent (see figure).
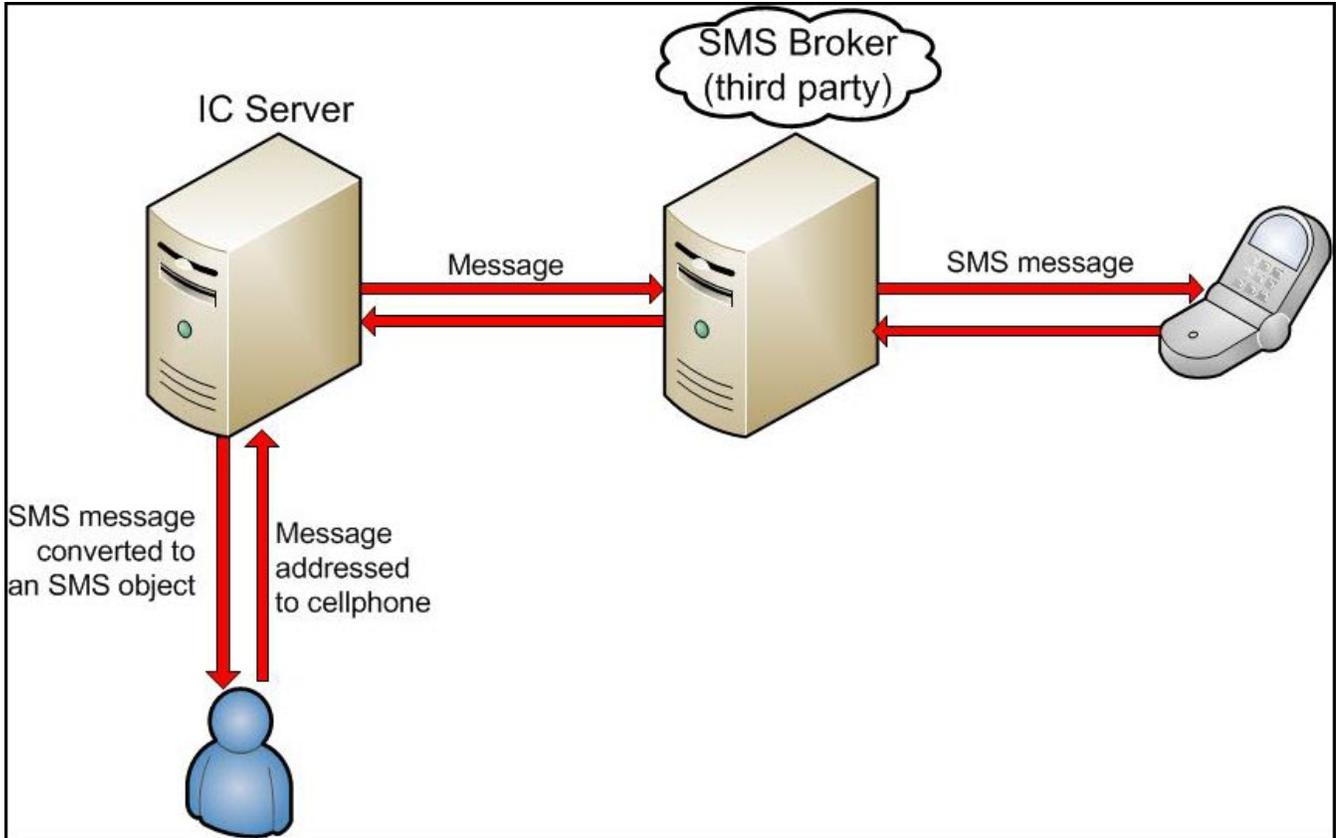
Understanding and choosing SMS Brokers

An SMS broker is a company that routes SMS messages to cell phone providers and collects SMS messages from cell phones. To do this, SMS brokers maintain hardware at the premises of cell phone providers, called Short Message Service Centers (SMS-Cs).

CIC comes with a choice of certified CIC brokers that provide all the long and short codes necessary to send and receive SMS messages. Genesys already supports the SMS brokers listed in the Broker Configuration dialog box in Interaction Administrator. These listed brokers have unique characteristics and are the best in the SMS marketplace in both price and functionality.

You can add other brokers, but you need to perform broker integration work for each new broker. To add a broker, the administrator creates an XML document defining how CIC exchanges data with the broker. For help, call the Genesys Professional Services Organization. Otherwise just select an SMS broker listed in CIC.

The CIC server connects to the selected SMS Broker, sending messages and receiving messages and status reports. When selecting an SMS broker for your Use Case consider these broker functions:

- Does the broker cover all the geographic areas that you need? This factor is sometimes important if your operations are international.
- Does the broker support "transaction atomicity" so that you can (if needed) track each message individually?
- Does the broker support alphanumeric source addresses that contain characters as well as digits?
- Does the broker support delivery receipts?
- Are delivery receipts sent to the device?
- Does the broker support multiple languages?
- Does the broker allow multiple recipients in a single request?
- Does the broker authenticate messages, based on IP address or other factors?
- Does the broker provide shared short codes or Free-To-End-User short codes?
- Does the broker provide special long codes or 800 number long codes?

The SMS world is a federally-regulated communication channel and as such SMS can be complicated and difficult to navigate. Check with Genesys or our partners to make sure that your customer's Use Case requires and uses the proper type of long code or short code. There are many variations of long and short codes. But, with the help of Genesys, you can make sure that your SMS requirements are met. We can also provide SMS configuration help and updates to SMS as they become available.

Recovery of SMS Interactions in Switchover

Previously, following a switchover, SMS users had to reconnect and wait for an agent. Starting with CIC 2016 R4, the Interaction Recovery Service subsystem recovers SMS interactions with a transition that is almost seamless. Once switchover occurs, the WebProcessor subsystem prepares the mirrored interactions.

To enable recovery of SMS interactions, set the SMS Interaction Recovery Enabled server parameter to 1. For this parameter to take effect, you must restart the Web Processor on both the primary and backup servers in a switchover pair. For more information, see the *Automated Switchover System Technical Reference*.

Configure Web Service Parameters

You can use web service parameters to disconnect completed SMS chat interactions automatically. You can also use custom web service parameter attributes to configure automatic replies.

- Set Web Services Parameters to Disconnect Chats
- Set Custom Attributes for Web Services Parameters

Set Web Services Parameters to Disconnect Chats

By default, agents must manually disconnect each SMS Chat interaction. To disconnect completed SMS Chat interactions automatically, in Interaction Administrator, navigate to **Web Services** > **Web Services Parameters** container. Create these new parameters and set their values:
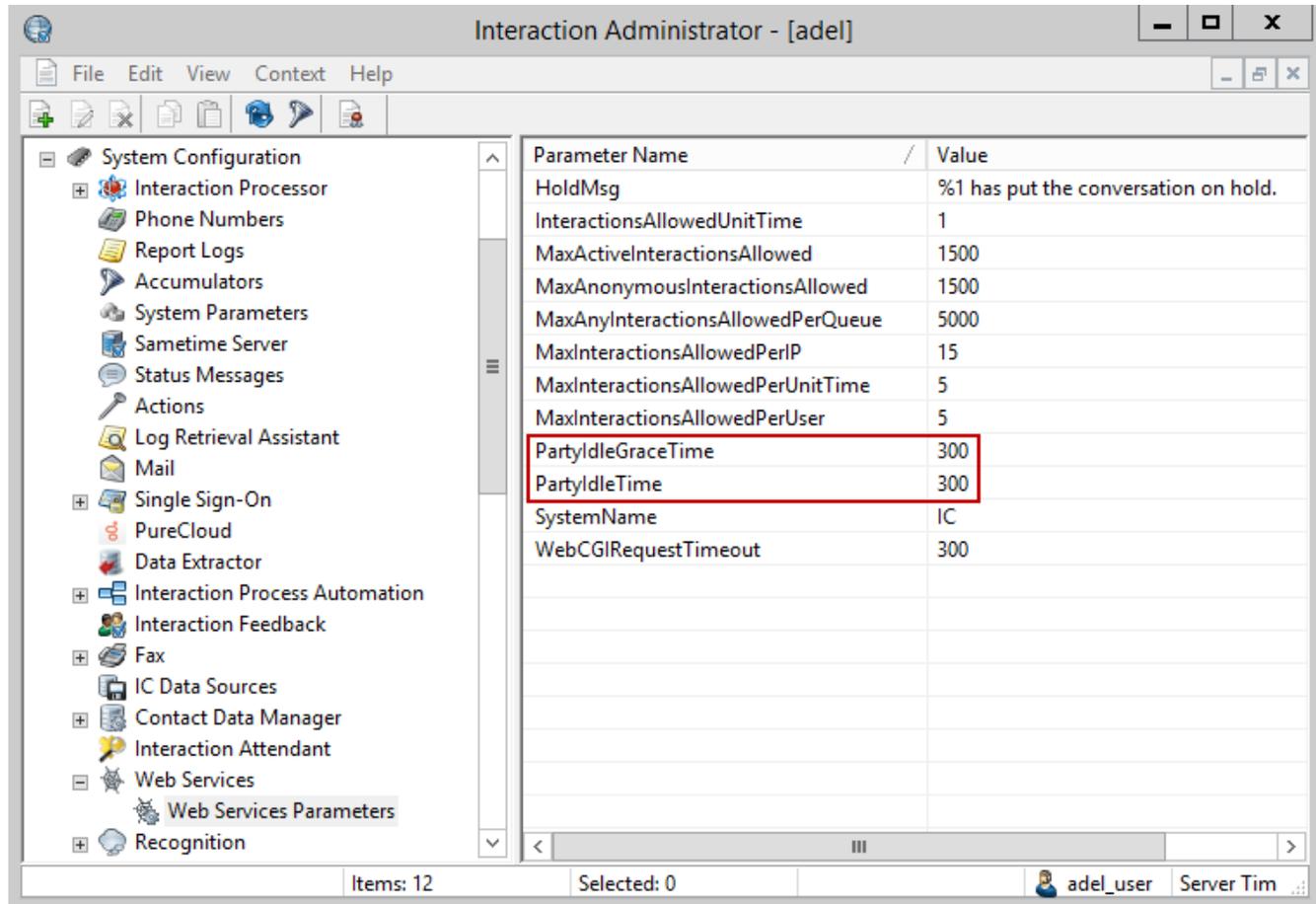
EnableIdleTimeout:

Set the value to **1** to enable the timeout

PartyIdleTime:

Set to a value such as 300. This parameter sets a completed interaction to an idle state after the specified number of seconds.

PartyIdleGraceTime:

Set to a value such as 300. This parameter disconnects an interaction after it has been idle for the specified number of seconds.

> **Note:**
> These parameters affect all chat interactions, not just SMS chat interactions. You can set custom attributes for **Settings: Chat** and **Settings: SMS** which override these global settings. For more information, see Set Custom Attributes for Web Services Parameters.

Set Custom Attributes for Web Services Parameters

Custom attributes determine the automatic replies that the CIC server sends for notification purposes, such wait time in a queue or position in a queue.

If you create custom attributes, you can set Web Services parameters for them:

1. Open a command window and navigate to the following directory:

   `\I3\IC\Server\`

   By default, this path is `C:\I3\IC\Server\`.

2. Shut down Interaction Administrator if it is running.

   > Note:
   > Interaction Administrator cannot be running when you do the next step.

3. Run the following command:

   `SendCustomNotification.exe Set IWeb Strings`

   > **Note:**
   > If you defined any parameters manually for SMS or Chat, this command overwrites them for SMS and Chats.

4. After the command prompt reappears, exit from the command window.

5. Start Interaction Administrator and navigate to the **System Configuration** > **Web Services | Web Services Parameters** container.

6. Double-click Settings: SMS.

   Interaction Administrator displays the **Web Services Parameter Configuration - Settings:SMS** dialog. On the **Custom Attributes** tab (see figure), you can add, enable, or disable custom attributes. Those attributes can include custom text notifications to users who send SMS messages to the CIC server.

   > Note:
   > Custom attributes for the **Settings: SMS** parameter override the timeout settings for all chat interactions set by the corresponding Web Services parameters. Custom attributes for Settings: SMS affect SMS chats only. The syntax for these attributes is:
   >
   > `CUSTOM::OPTION:EnableIdleTimeout`
   > `CUSTOM::OPTION:PartyIdleTime`
   > `CUSTOM::OPTION:PartyIdleGraceTime`
   > The `IdleWarningMessage` and `IdleDisconnectMessage` messages are sent only for web chat interactions. They are not sent for SMS chats.

Configure SMS

SMS configuration settings control the operation of the SMS server. The SMS server arbitrates between external SMS brokers and internal CIC subsystems, such as the ACD server, reporting, and Interaction Recorder.

This section covers:
- SMS Configuration Dialog
- Configure Inbound Routing
- Configure Outbound Routing
- Configure SMS Purge Data setting
- Configure SMS Custom Attributes
- Document SMS Configuration History

SMS Configuration Dialog

The CIC administrator configures the SMS server subsystem in Interaction Administrator. The SMS Configuration dialog is available under the System Configuration container.
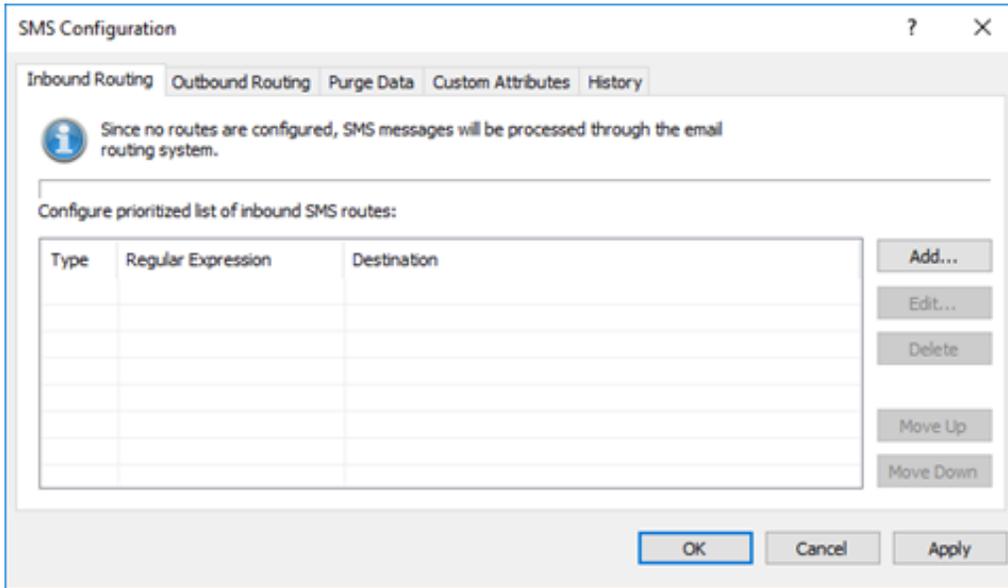
As in other Interaction Administrator configuration dialogs:

Add:

Display a configuration dialog for a new route.

Edit:

Displays the Inbound Route Configuration dialog to edit the selected route.

Delete:

Deletes the selected route.

> **Note:**
> You cannot delete the default route.

Move Up / Move Down buttons:

Move the selected route up or down in the priority list.

OK:

Saves your input and closes the dialog box.

Cancel:

Closes the dialog box without saving your input.

Apply:

Applies your input immediately but does not close the dialog box. Use this button if you wish to change settings on the other tabs.

Configure Inbound Routing

Configure a prioritized list of inbound SMS routes. If you do not configure any inbound routes, messages travel through the email message routing system. If you configure one or more inbound routes, you must also configure a default inbound route.
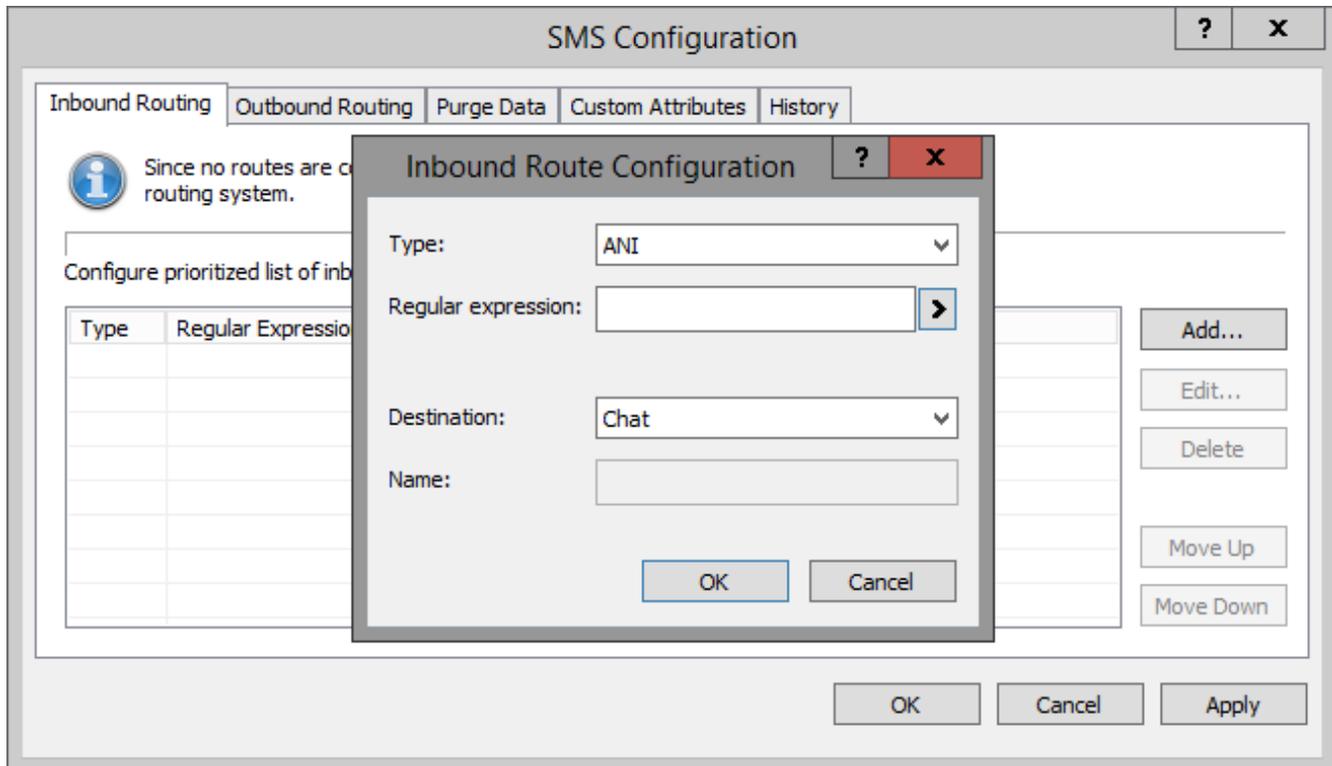
1. In Interaction Administrator, navigate to System Configuration > SMS and click **Configuration** in the SMS container's list view window (right pane).
2. Select the **Inbound Routing** tab.
3. Select a **Type** of route to indicate where the filter operates.

    ANI

    > Sender's mobile number

    Body

    > SMS message text

    DNIS

    > Dialed number

4. Use a **Regular expression** to define a filter that selects which inbound interactions take this route.

    For example, if the regular expression is `317.*` then the CIC server routes all messages from mobile numbers (ANI) whose first three numbers are **317** to the specified destination.

5. Select a **Destination** for the inbound SMS message.

    This specifies where to route the interactions selected by filter.

    Chat

    > The SMS object is routed as a Chat interaction.
    >
    > > **Note:**
    > > If you select **Chat** destination, navigate to the **System Configuration** > **Phone Numbers** container. Double-click **Configuration**. On the **DID/DNIS** tab, add the phone number that cell phone users call for this route. The number is the short code from the broker. The chat destination option does not allow SMS interactions to persist through switchover with the `Chat Interaction Recovery Enabled` server parameter. However, you can enable recovery of SMS interactions by setting the SMS Interaction Recovery Enabled server parameter to `1`. For more information, see *Automated Switchover System Technical Reference*.

    Handler

    > A handler processes the SMS object.

> **Note:**
> If you select Handler, you must also modify the **CustomSMSRoutingToHandler** handler to route correctly. It works the same as Interaction Attendant subroutine calls.

Queue

The SMS object goes to a user queue or via ACD to a workgroup queue. You are prompted to select a queue.

6. In **Name**, do one of the following:
    - If the Destination is **Handler**, enter the name of the handler.
    - If the Destination is **Queue**, select the user or workgroup queue name.
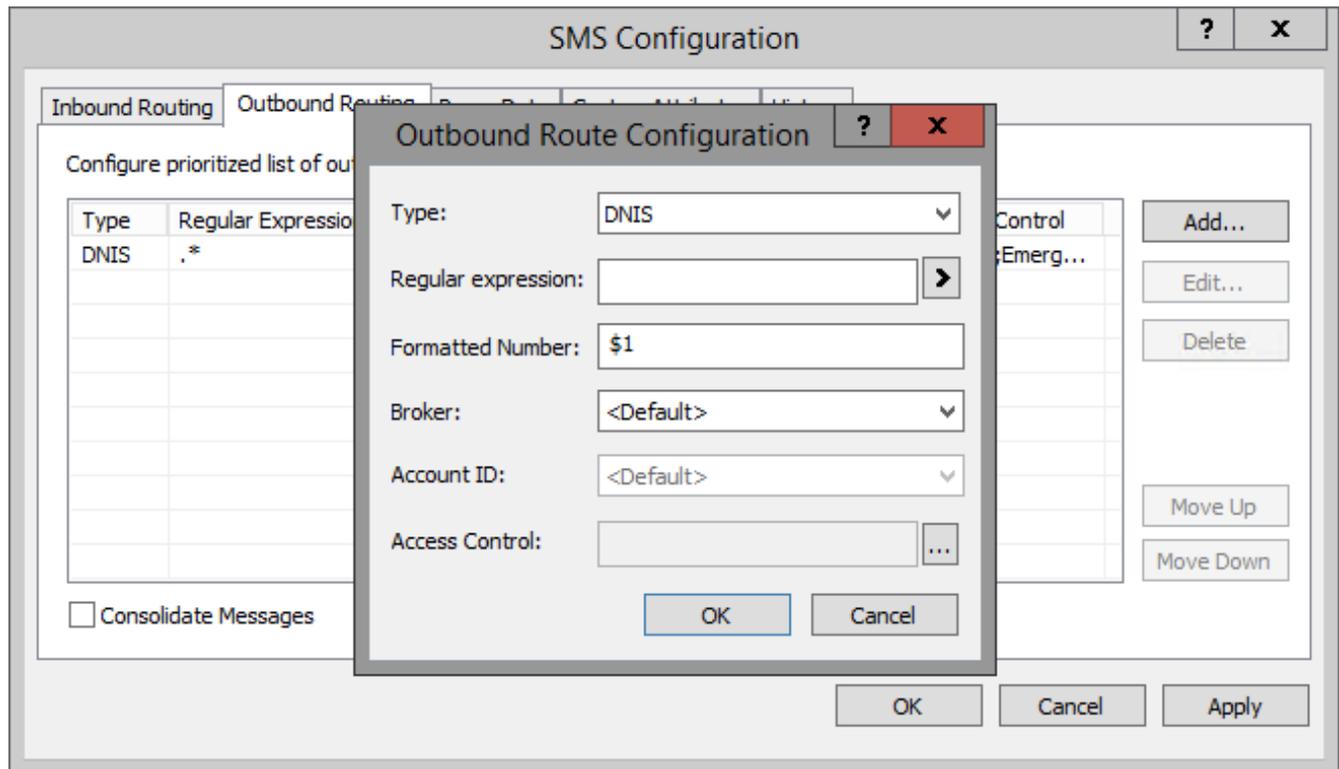
> **Note:**
> If the destination is **Chat**, this field is unavailable.

7. Click **OK**.

Configure Outbound Routing

Configure an ordered set of rules for routing outbound SMS messages through CIC. SMS uses the highest ranking matching route in the list. Based on regular expression matching of DNIS, CIC sends outbound directed SMS messages to a broker using the proper destination number formatting. The routes are defined by type, regular expression, formatted number, broker and account ID.

1. Skip **Type.** Currently, **DNIS** is the only option.
2. Use a **Regular expression** to define a filter that selects which outbound interactions take this route.

   > **Note:**
   > The Regular expression must match the part (described in the **Type**) of the SMS message to send the message to its destination. It also provides the pattern matches for the formatted number.

3. Specify the destination number. Enter the **Formatted Number** that that CIC uses as the outbound dial number for the SMS message. All characters are valid. Regular expression pattern replacements are denoted this way:
   - Use $ for regular expression pattern replacements.
   - Use $0 for the input expression as a whole.
   - Use $1 for the first grouped match, and so on.
4. Select a **Broker** to deliver the SMS message.
5. Select the **Account ID** at the selected broker to use for the SMS message.
6. In **Access Control**, select the phone number classifications for the selected outbound SMS route.

   > **Note:**
   > You must select at least one phone number classification for the outbound SMS route. If you do not select a phone number classification, or do not select a call classification that provides the correct access permissions, then agents and workgroups using this SMS route see an error message when they try to send SMS messages. You manage the available call classifications as part of your regional dial plans.

7. Click **OK**.
8. Optionally, in the **Outbound Routing** tab, select **Consolidate Messages** to automatically combine short messages. If a new message comes in and another message is waiting to be sent, it can be added to the waiting message if the combined length is less than the SMS maximum length of 160 characters.

Configure SMS Purge Data setting

Use this tab to configure when old SMS data is purged from the database. In the **Purge data older than** box, type a number greater than 1.
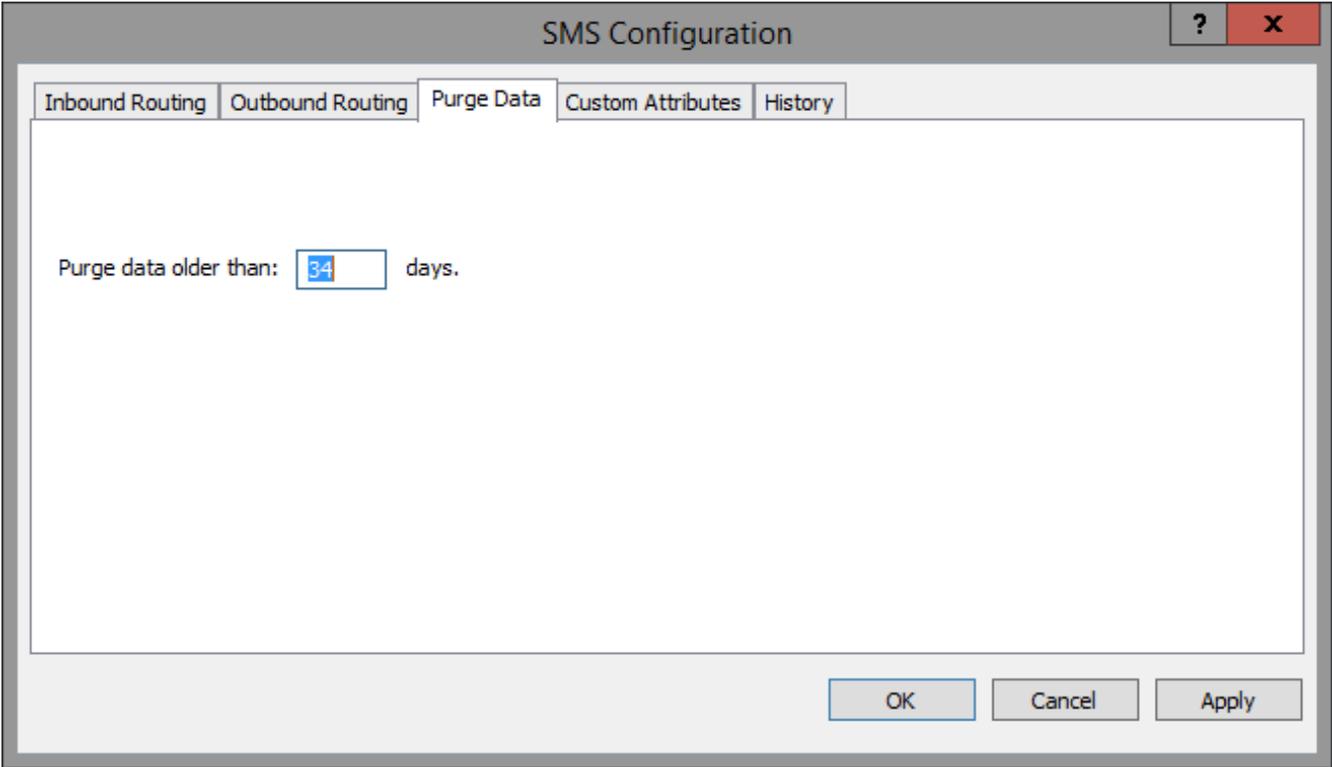
Configure SMS Custom Attributes

Custom attributes enable you to reference your own variables and setting through the IceLib interface. You manage custom attributes in the same way as you do for any other IA feature. For more information, see the topic Custom Attributes in the Interaction Administrator help.

Document SMS Configuration History

In the same manner as any other IA configuration feature, you can use the History page to manually document configuration changes and when they occurred.
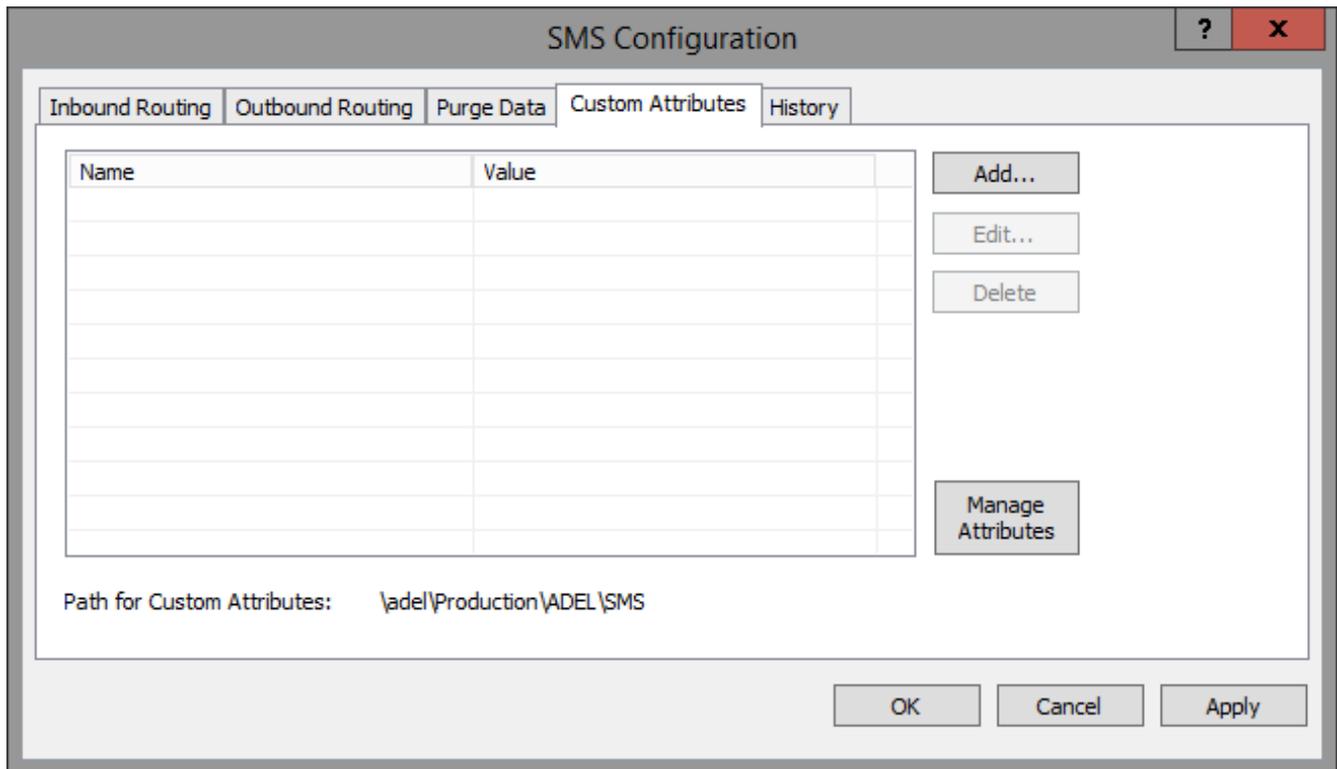
SMS Configuration	? X

Inbound Routing | Outbound Routing | Purge Data | Custom Attributes | **History**

Enter notes about configuration settings and changes.

Last Modified: `3/19/2018 2:16:24 PM`   Date Created: `3/12/2018 10:00:37 AM`

Notes

[OK]   [Cancel]   [Apply]

Configure SMS Brokers

CIC includes a default HTTP broker, but you can configure any number of SMS HTTP brokers.

This section includes:

International Outbound SMS Messages

In CIC 2018 R1 and later releases, PureConnect supports receiving all domestic and international inbound SMS and also international outbound messages via the Genesys SMS broker. This international outbound message support is to any nation that receives international SMS when those messages include the country code. You supply the country code as part of the phone number in the **Local Address** for the **Broker Account**.

HTTP-based SMS Brokers

CIC 4.0 SU4 added support and configuration options for multiple HTTP-based SMS brokers as the preferred SMS interface. By the time of CIC 4.0 SU6, CIC no longer supported the SMS Gateway-based interface, but the configuration options remained in Interaction Administrator. Starting in CIC 2017 R2, the SMS Gateway configuration options were removed from Interaction Administrator and anyone still using the SMS Gateway interface needs to move to the HTTP-based SMS interface.

You configure Broker settings in the **Broker Configuration dialog box**. There are several tabs, on each tab you can use any of these controls.

OK:

Saves your input and closes the dialog box.

Cancel:

Closes the dialog box without saving your input.

Apply:

Applies your input immediately but does not close the dialog box. Use this button if you wish to change settings on the other tabs.
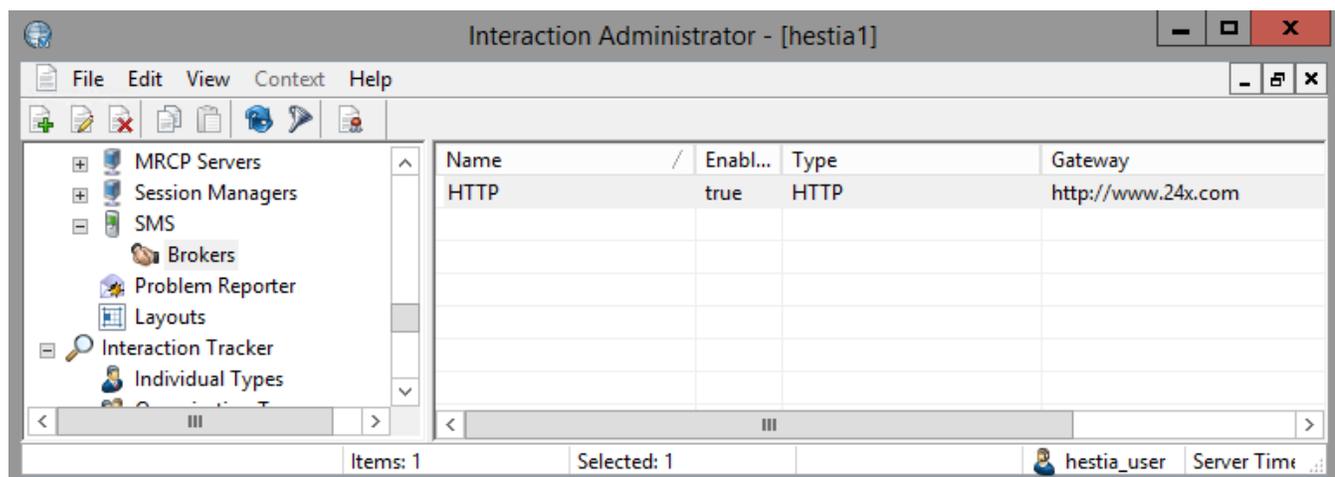
Configure HTTP Broker Settings

You can modify the default HTTP broker settings or right-click and create a new set of Broker settings.

1. In Interaction Administrator, navigate to **System Configuration** > **SMS** > **Brokers**. Right-click and modify existing settings or create a new Broker configuration.
2. In the **Configuration** tab, do one of the following:
   - Select **Enable** to enable the broker configuration for Message Originated (MO) and Message Terminated (MT) processing.
   - Clear the **Enable** check box to disable MO and MT processing.
3. Select the desired Broker from the list.

   > **Note:**
   > If the broker is not one of the preconfigured brokers, you or an SMS administrator must create and install an XML file to define the broker. Contact the Genesys Professional Services Organization for assistance in creating this file.

4. From the **Profile** list, select the specific configuration profile to use for SMS messages. Many brokers offer only one profile.
5. **Encryption**: Choose basic encryption or no encryption.

   > **Note:**
   > Select **HTTPS (Basic)** if you are using SSL. If you select this, you must use HTTPS for both inbound and outbound messages. For more information, see Using SSL.

Configure Broker Accounts

You can configure multiple accounts registered to the same broker. These accounts use the same broker interface and communication ports. You can add new accounts, edit existing accounts, or delete an account.

Broker Configuration - HTTP

Tabs: Proxy | Custom Attributes | History | Configuration | Accounts | Message Originated | Message Terminated

Configure list of active accounts for this broker:

Account ID: 24x

Account dialog:
- Account ID: 24x
- Local Address: 5559999
- Login:
- Password:
- Confirm Password:

Buttons: Add... | Edit... | Delete | Associate...

OK | Cancel

☑ Confirm auto-save

OK | Cancel | Apply

---

1. In the **Accounts** tab of the **Broker Configuration** dialog box, add or edit an active broker account.
2. In **Account ID**, enter the account ID that the broker uses for your SMS messages.

> **Note:**
> The value you specify must be unique among all other account IDs on this broker. If a broker provider does not provide or use an account ID, then choose an arbitrary account identification.

3. In **Local Address**, enter the phone number for the account.

> **Note:**
> This setting is optional, but if you do specify a number, it must be unique among the other local addresses on this account.

The local address serves two purposes:

   ○ CIC populates it on an outbound message if the broker profile requires its specification.

   > **Note:**
   > **Genesys Broker Outbound messages**: If you are configuring the **Genesys SMS broker** for outbound **international** SMS messages, you must include the **country code** as part of this phone number. The Genesys Broker uses the country code to route the message to the appropriate carrier.

   ○ CIC populates it on inbound messages to create a pairing between the external party and an internal account. If the broker does not provide a local address on incoming messages, CIC uses this value for the message's local address.

4. In **Login**, enter the User ID for logging on to this account.

> **Note:**
> You can leave **Login** and **Password** blank, if the broker does not require account validation.

5. In **Password**, enter the Password for the account. In **Confirm Password**, repeat the password entry.
6. Click **OK**.
7. Optionally, in the **Accounts** tab, select a broker and click **Associate**. In the **Outbound SMS Workgroup and User Associations** dialog box, select **Workgroups and Users** to associate with this Broker Account.

Note:
This enables agents to choose which number appears when they send an SMS message, either their personal number or the number associated with their workgroup.
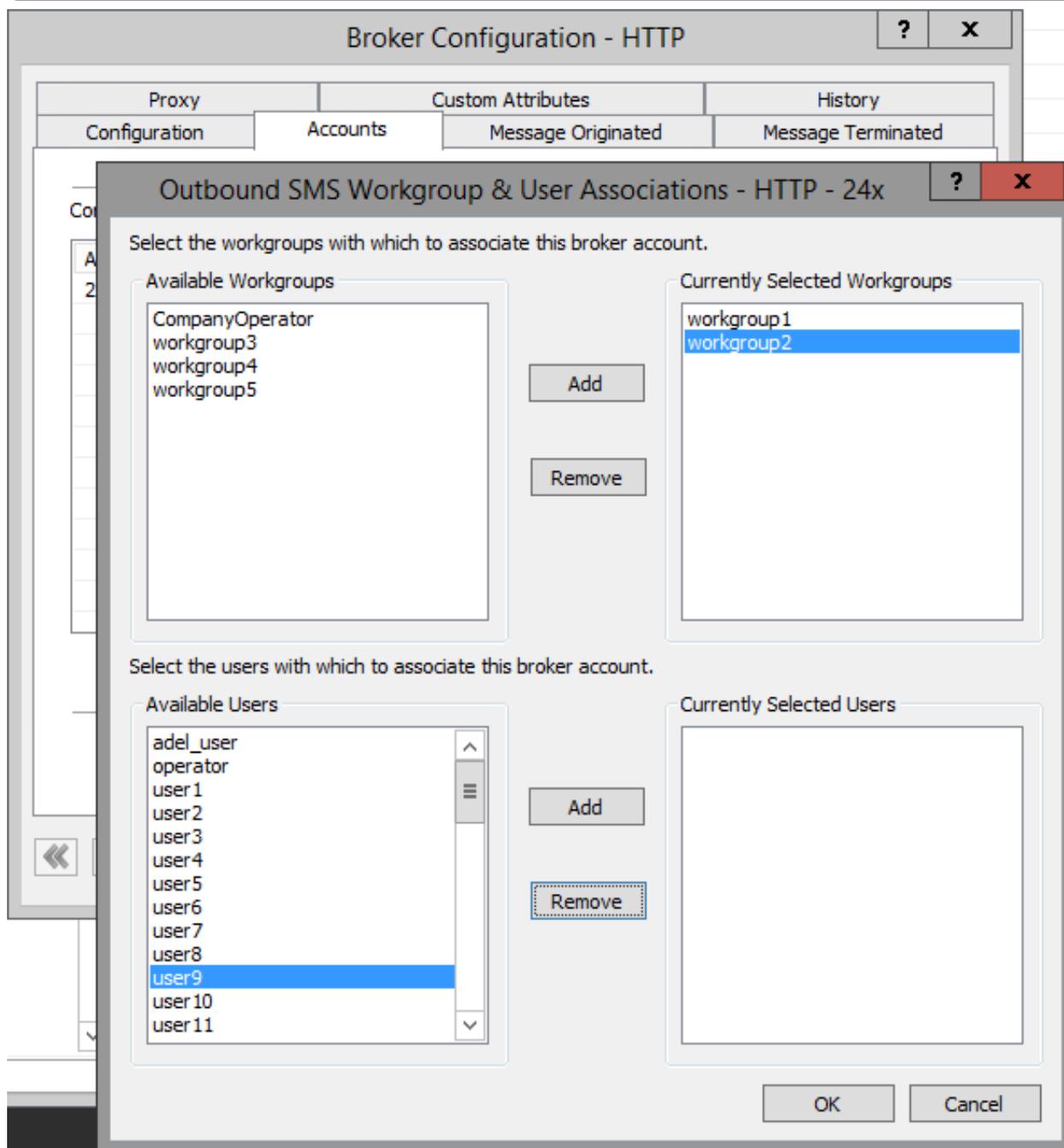
8. To save your input and close the dialog box, click **OK**.

Configure Broker Message Originated settings

A Mobile Origination (MO) message is an inbound SMS message that comes from a cellphone. Use this tab to configure settings when polling for new messages and receiving new messages.

1. In the **Message Originated** tab, do one of the following:
   - Select **Enable** to enable the MO functionality.
   - Clear the **Enable** check box to disable MO functionality.

   > **Note:**
   > If the two check boxes conflict, the **Enable** check box on the **Configuration** tab takes priority.

2. In **Incoming HTTP Port**, enter the number of the IP port to which the SMS broker sends incoming inbound HTTP requests (SMS messages).

   > **Note:**
   > Provide the port number to the Broker. Do not share this port with any other application on the CIC server, and make sure it is accessible by the public network.

3. In **Incoming Path**, type the path with which an incoming request's URL is compared and validated.

   This determines that a request should be processed by this broker configuration. It must be unique for each broker.

   > **Note:**
   > If this broker shares an incoming HTTP port with other brokers on this CIC server, make sure that the Incoming Path and Delivery Receipt URL values are unique among all brokers that share this port.
   > When ordering a service from an SMS provider, you must provide the information on this page. Typically, the information should be in the form of a URL that the provider can send messages to. This URL is composed of `http://<IC server IP>:< HTTP Port><Path>`, so for example, `http://172.10.10.10:8080/MyBroker/IncomingSMS`.

4. In **Delivery Receipt URL**, enter the path where the broker pushes incoming delivery receipt notifications for outbound messages.

   Most brokers support delivery receipts in one of the following ways:
   - The delivery receipt URL is set in the broker account configuration, for example through the broker's web portal.
   - The delivery receipt URL is passed by CIC with each outbound message. In this case, you must go to the Message Terminated tab and specify a value for the ExternalDeliveryStatusURI option.

Configure Broker Message Terminated settings

A mobile terminated message (MT) is an outbound SMS message that goes to a cell phone. This is the only type of message that can be used by handlers. Use this tab to configure settings used when CIC sends SMS messages.

1. In the **Message Terminated** tab, do one of the following:
   - Select **Enable** to enable the MT functionality.
   - Clear the **Enable** check box to disable MT functionality.

   Note:
   If the two check boxes conflict, the **Enable** check box on the **Configuration** tab takes priority.

2. In **Gateway**, type the destination of the HTTP or HTTPS request to reach the broker.

   Note:
   To create the complete URL before sending the request, CIC combines this destination with a service path by the application. For some brokers the default gateway may be sufficient, however some brokers require a URL with a unique identifier. The default gateway is http://www.24x.com.

3. In **Outgoing Path**, type the path against which an outgoing URL should be validated.

   By default, the field contains the outgoing path from the broker file; however, you can override this value.

> **Note:**
> Both inbound and outbound messages must use either HTTPS or HTTP. For more information about using SSL, see the PureCloud for CIC Administration Guide in the PureConnect Documentation Library.

4. In **Timeout**, type the duration in seconds for outbound HTTP or HTTPS requests to connect before CIC treats the request as failed.

   The default is 60 seconds.

5. To send internationalized phone numbers to SMS brokers, select **Internationalize Telephone Numbers**. Internationalized phone numbers are formatted as `FQTN (+CCdddddddd)`.

6. In **Message Parsing,** configure how messages should be handled if they exceed the size limit.

   An SMS message has a limit of either 70 characters or 160 characters, depending on the character encoding.

   Note:

   Do not alter any MT message that exceeds the SMS limit.

   Split:

   Split an MT message that exceeds the SMS limit into multiple messages.

   Truncate:

   Truncate a message that exceeds the SMS limit. Send only the characters that fit within the limit.

7. In **Options**, specify a **Name** and a **Value** for a configuration option specific to this broker.

   Options are values that are required by some brokers and are too specialized for CIC to consider as a general configuration option. The broker configuration predefines the Names as empty values. You can specify a value for a name by double-clicking on the name, and add or modify the value. Some brokers may fail SMS messages if you do not populate the information with correct values.

> **Note:**
> If the **ExternalDeliveryStatusURI** option appears, then you must specify a value for it in order to receive delivery receipts for SMS messages. This option contains the external URL that receives delivery receipts for SMS messages:
> If the CIC server is directly connected to the Internet, the external URL is typically http://<CIC server IP>:<HTTP Port><Delivery Receipt URL>.
> If the CIC server is behind a reverse proxy or other device, the external URL may be different.
> For more information, see the description of the **Delivery Receipt URL** box in **Configure Broker Message Originated** settings.

Configure Broker Proxy settings

Use this tab to configure the HTTP broker proxy settings if you use a proxy between the CIC server and the HTTP broker endpoint, for example, a corporate HTTP proxy. You set the login and password credentials on the HTTP broker as the `Proxy-Authorization` tag using basic scheme authentication.

1. In the **Proxy** tab, in the **Address** field, type the address of the proxy server.
2. In **Login**, type the User ID (user name) for the account on the proxy server.
3. In **Password**, type the password for the account to use when logging on to the proxy server.
4. In **Confirm Password**, type the password again.
5. In **Encryption**, select **SSL** to enable encryption or select **None**.

Configure Broker Custom Attributes

Custom attributes enable you to reference your own variables and setting through the IceLib interface. You manage custom attributes in the same way as you do for any other IA feature. For more information, see the topic Custom Attributes in the Interaction Administrator help.

Document Broker Configuration History

In the same manner as any other IA configuration feature, you can use the History page to manually document configuration changes and when they occurred.

Configure a New Broker

You configure a new broker in the same way as you configure one of the default brokers. First, however, your SMS administrator creates an XML file defining values and parameters the new broker needs. This administrator places the XML file in `i3\ic\resources\i3sms\` and then restarts the SMS server.

> **Note:**
> For help creating an XML broker file, contact Genesys Professional Services.

To configure a new broker:
1. Verify that your SMS administrator created and installed the XML file for the broker.
2. In the **SMS | Brokers** container of Interaction Administrator, right-click a blank area and click **New**.
3. In the **Entry Name** dialog (see figure), type the broker name and click **OK**.
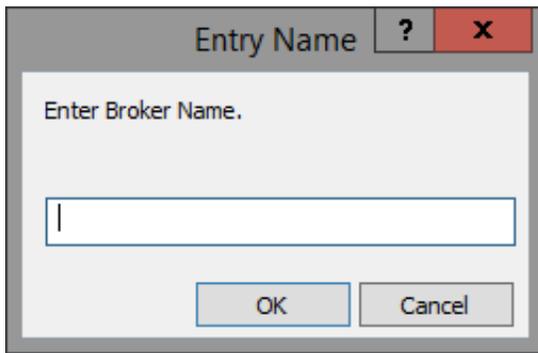
4. On the **Configuration** tab of the **Broker** dialog, expand the **Broker** list and select the new broker.
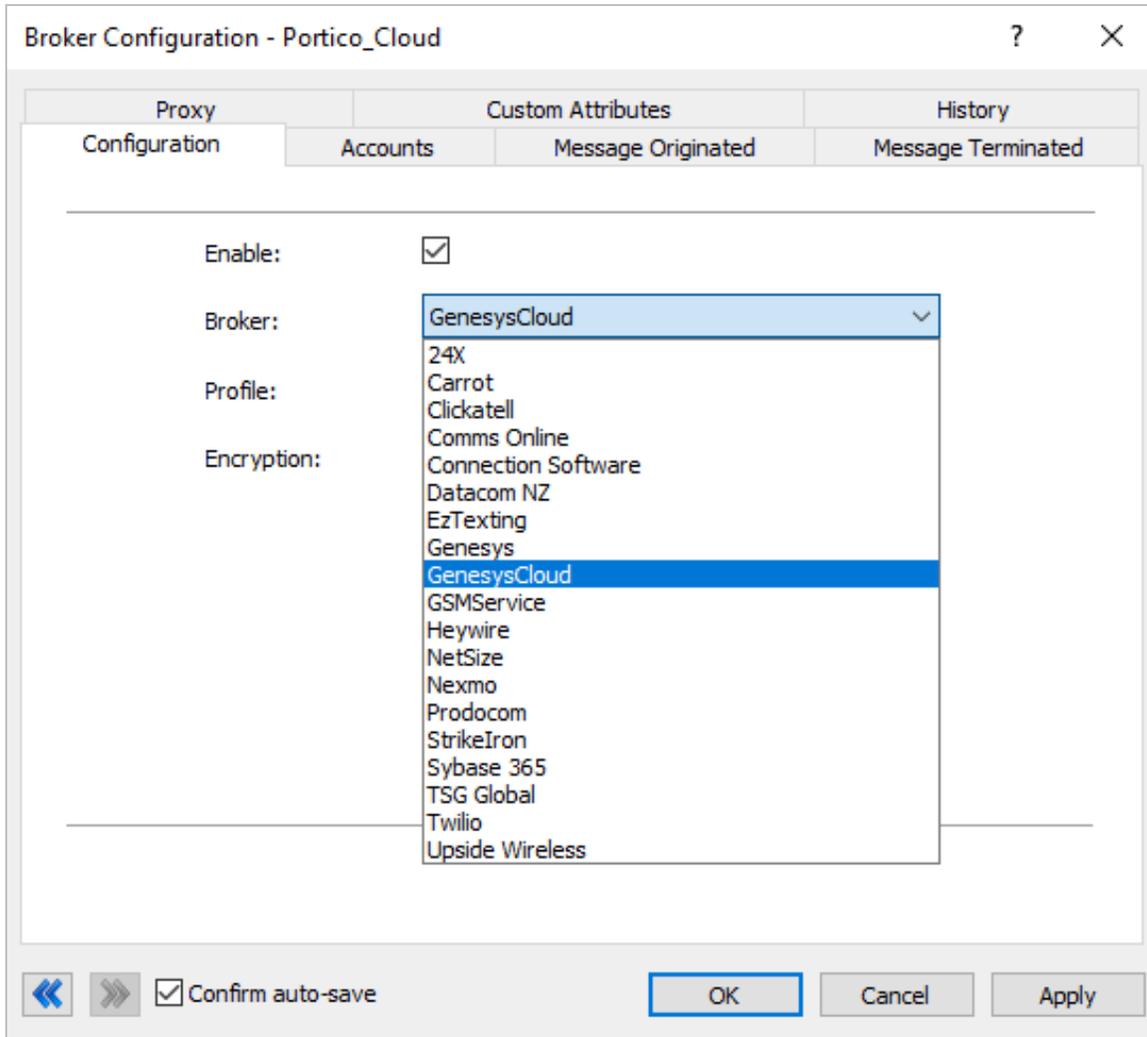
5. Configure the broker in the same way as you configure a default broker. See Configure SMS Brokers.

Using SSL

SSL (HTTPS) works with brokers for both MO (inbound SMS) and MT (outbound SMS). One specific caveat is that both MO and MT from the CIC server can use either HTTP or HTTPS, but you must use the **same for both.**

Typically, SMS brokers use HTTPS for their side of the service so MO (inbound) also has to use HTTPS. It is simple to do HTTPS from the reverse proxy to the CIC server (trusting the IC HTTPS certificate authority at the reverse proxy). From there, one can do HTTP from the broker to the reverse proxy. For best security, it should be HTTPS all the way. (The broker must trust the CA for the certificate used at the reverse proxy).

This section documents at a high level the requirements for using end to end SSL when consuming SMS services in PureConnect environments via the Genesys SMS broker service.

- URL
- FQDN
- SSL Certificate

Most SMS broker services (service) can provide SSL encryption on inbound SMS messages that are PUSHed to PureConnect (endpoint). The service can also receive SSL encrypted outbound SMS message requests from the endpoint. When configured together the service and endpoint use SSL encryption for both inbound and outbound SMS messages at all times.

URL

The primary consumption method for most customers is inbound SMS messaging. In this scenario, the endpoint acts as an HTTP server that is capable of receiving POST messages from the service. The service is configured with a URL value that corresponds to the endpoint which is the target for each inbound message. A proper URL consists of an FQDN portion and an action portion.

Example: https://webportal.xyzcorp.com/SMSGenesys

The FQDN portion is `webportal.xyzcorp.com` and the action portion is `/SMSGenesys`. In this case, SSL is requested when the `https://` connection method is specified. The connection method and action portion are trivial and are easily specified. The FQDN portion requires additional action on the part of the endpoint custodian.

See also Using SSL.

FQDN

An FQDN must be publicly resolvable. The endpoint custodian must formally register its entire value with either their own publicly accessible DNS infrastructure or a known DNS hosting provider. In the example above, `webportal.xyzcorp.com` was registered with the endpoint custodian's corporate public DNS servers. After the FQDN is registered with a public DNS server or multiple servers, the public IP must be formally associated with the FQDN. Only after this process is completed will inbound SMS messages encrypted with SSL be possible.

See also Using SSL.

SSL Certificate

Once an FQDN is registered and associated, the endpoint custodian must purchase an SSL certificate from one of the main public Certificate Authorities (CA). The endpoint custodian cannot use a self-signed certificate without breaking SSL negotiations with the service. The certificate can be a named or wildcard certificate.

In case of the example above a certificate for `webportal.xyzcorp.com` or `*.xyzcorp.com` from Thawte, Digicert, or Verisign would be more than sufficient. The endpoint custodian's budget determines the duration and type of certificate that they purchase. Once the certificate is purchased, it must be applied to the endpoint(s). Generally, it is easiest to use a reverse proxy between the service and endpoint(s) and apply the certificate there for simpler administration. If any one piece of the valid URL is missing then SSL negotiations between the service and the endpoint will fail.

In the case of outbound SMS messages from the endpoint to the service, the same principals apply. However, the service typically has already configured and registered their SSL certificates and FQDNs so there is nothing needed on the part of the endpoint custodian.

See also Using SSL.

SMS Reverse Proxy Setup

For switchover, load balancing, and so on, it may be necessary to use a reverse proxy for SMS. Proper setup and configuration of the reverse proxy is required to get this to work with our product.

Prerequisites

First install the proper roles and extensions:
- Install the IIS role on a valid Windows Server machine.
- Install the Application Request Routing (ARR) extension.
- Install the URL Rewrite extension.

Then proceed to:
- IIS Configuration
- Server Farm and Switchover Considerations

IIS Configuration

Reverse Proxy- Proxy Type
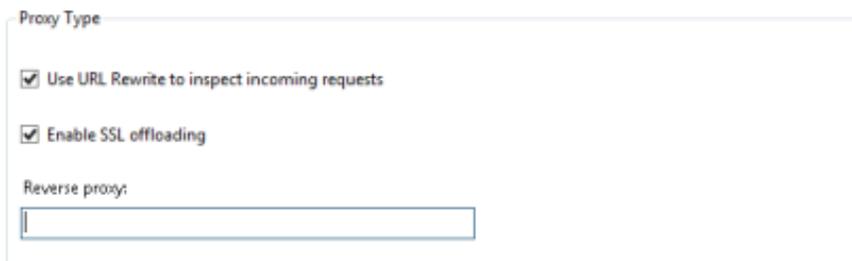
After installing the roles and extensions, configure the reverse proxy.
1. To open the IIS Manager, in the **Run** dialog box, run the command `inetmgr`.
2. Select the server name (on the left-pane) and open the **Application Request Routing Cache** node.
3. Select the **Server Proxy settings…** link for the ARR.
4. On the proxy settings, select the **Use URL Rewrite to inspect incoming requests** checkbox.
5. Additionally, select the **Enable SSL offloading** checkbox.
6. Finally, in the **Reverse proxy** text box, add the CIC server's IP address.
7. Apply the changes.

Reverse Proxy- URL Rewrite

After configuring the reverse proxy and ARR, configure the URL Rewrite to manipulate the incoming requests.

1. Navigate back to the IIS Manager home screen.
2. Open the **URL Rewrite** extension node.
3. By default there should be at least one inbound route because we added an IP address when we configured the proxy, open that existing route (ARR_server_proxy).
4. In the **Action** section, change **Rewrite URL** to the following:
   `https://<IP ADDRESS OF CIC server>/receivesms.php{R:0}`

   > **Note:**
   > In the example in this section, the URL is unique to EzTexting. If you use another broker, change `/receivesms.php` to the broker's incoming patch as defined in Interaction Administrator. If the CIC server is receiving on a port different than port 80 or 443, you must define the port here as well. For example, `https://IPAddress:8191/receiveTexts.php{R:0}`.

5. Apply the changes.

Reverse Proxy - CIC Server's certificate

If you are using HTTPS, you need to trust the CIC Server's certificate on the Reverse Proxy. The SMS Server uses the Server certificate to secure the connection. The Server certificate is signed by the CIC Certificate Authority certificate, and the CIC Certificate Authority certificate is signed by the Server Group certificate. The Server Group certificate is self-signed. Both the CIC Certificate Authority certificate and the Server Group certificate need to be in the certificate store on the reverse proxy. The CIC Certificate Authority could go in either the Trusted Root Certificate Authorities store, or more appropriately the Intermediate Certificate Authorities store. The Server Group certificate should go in the Trusted Root Certificate Authorities store.

The following steps explain how to do that:

> **Note:**
> It is not a requirement that you use HTTPS between the web server and the CIC server.

1. Copy the CIC Server's ServerGroup certificate to the Reverse Proxy.
2. Open **mmc.exe** and add the "Certificates" snap-in.

   > **Note:**
   > Ensure you add this for the computer account.

3. Expand the **Trusted Root Certification Authorities** and select the **Certificates** container.
4. Right-click in that container and select **All Tasks | Import**.
5. Follow the on-screen instruction and import the ServerGroup certificate.

   Result: The Reverse Proxy can now connect to the CIC server and it can forward requests from the broker to the CIC server.

   > **Note:**
   > Configuring the URL Rewrite address to use HTTPS does not mean only incoming HTTPS messages will be accepted. Technically speaking, SSL is first stripped off incoming HTTPS packets from an SMS Broker. URL Rewrite then negotiates SSL with the CIC server and encapsulates the HTTP (previously HTTPS) message. In other words, regular HTTP messages from the SMS Broker can be sent to the reverse proxy while HTTPS is configured.

Reverse Proxy - Default Web Site HTTPS Binding
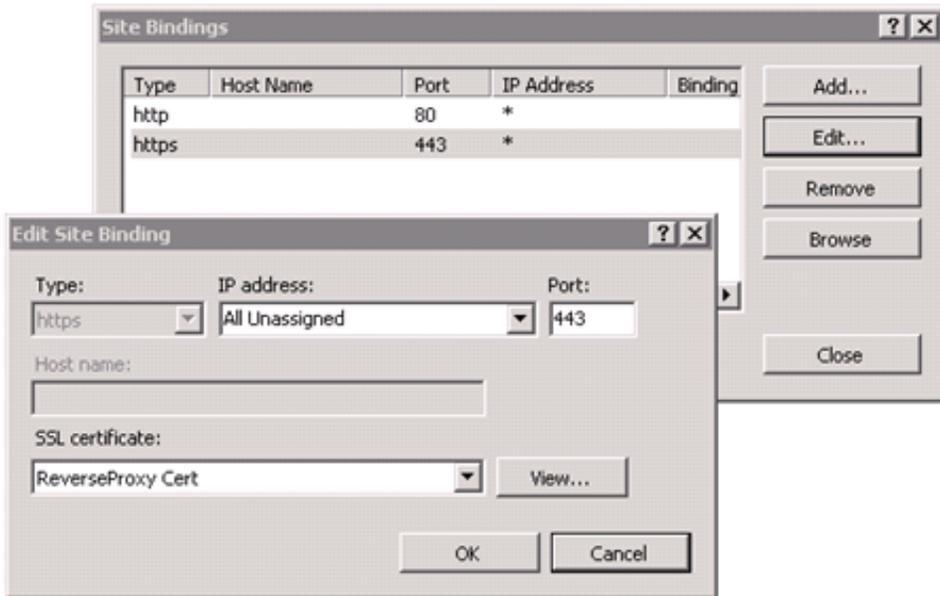
In addition to configuring HTTPS between the reverse proxy and CIC server, inbound HTTPS must also be accepted. The following steps outline how to create a self-signed certificate and bind port 443 to the default website (created automatically during previous steps).

1. To open the IIS Manager, in the **Run** dialog box, run the command `inetmgr`.
2. Select the server name (left-most pane) and double-click **Server Certificates**.
3. In the right-hand pane, select **Create Self-Signed Certificate**.
4. Enter a name and select **OK**.
5. Expand the **Sites** folder (left-most pane) and select the site titled **Default Web Site**.
6. In the right-most pane, click **Bindings**.
7. To add a new binding, set the following values:

Type	https
IP Address	**All Unassigned**
Port	**443**
SSL Certificate	**<Cert Name from step 4>**

Result: The reverse proxy will now accept both HTTP and HTTPS traffic from SMS Brokers. You can verify this by navigating to `https://<Public_IP_of_Reverse_Proxy>`.

> **Note:**
> For inbound SMS to work properly, the SMS Broker must import the self-signed SSL certificate. If the broker won't do this, you must purchase and configure a signed certificate from a certificate authority (CA) to replace the self-signed certificate.

Server Farm and Switchover Considerations

In addition to the standard reverse proxy configurations, some installations use a switchover CIC server pair. To route interactions if the primary server goes down, the reverse proxy must know what the two servers are in this switchover pair. The following section describes how to configure the reverse proxy to connect to the switchover pair.

URL Rewrite with Server Farm
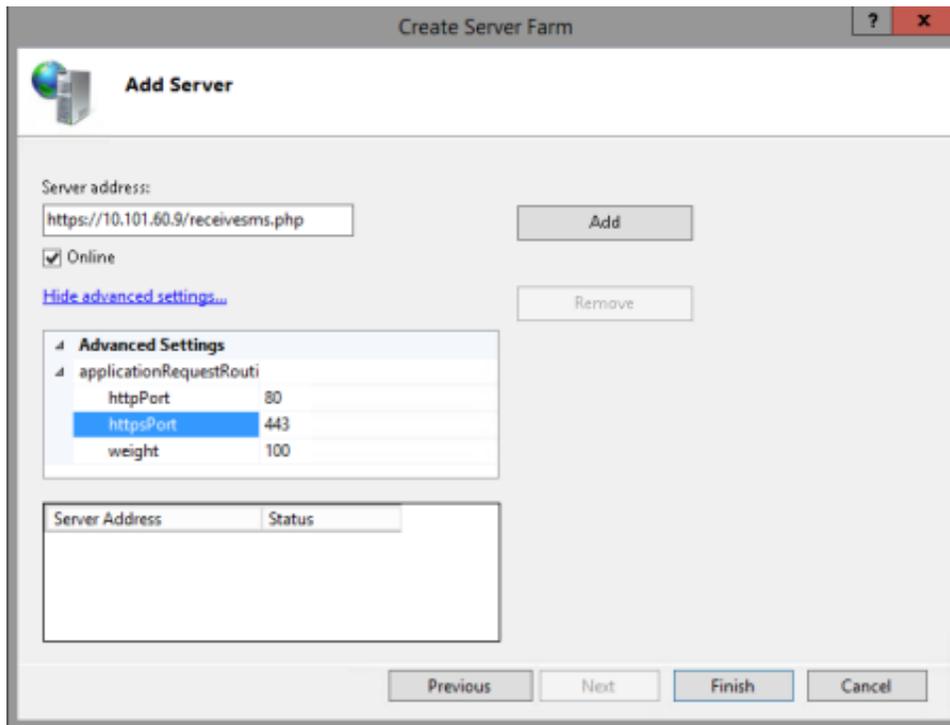
First, create a Server Farm to point to both servers.

1. To open the IIS Manager, in the **Run** dialog box, run the command `inetmgr`.
2. Right-click the **Server Farms** section and select **Create Server Farm**.
3. Enter a name for the server farm and select **Next**.
4. Add the corresponding IP addresses for the two CIC servers.
5. If the SMS broker does not use port 80 or port 443, click **Advanced Settings** and change the port number.
6. Select **Finish** and make sure the system creates a URL rewrite for the server farm.

   Result: There is a new URL rewrite that uses the server farm as the server we are going to send it to, as in the following example:

Health Test for Server Farm

The URL now routes to the specific server in question now, but there is no check to determine if ServerA or ServerB is the primary. To get around this, use a health check that points to the SMS path. The SMSServer will respond to the HTTP request (however there will be no SMS created since the information will be incorrect).

To set up the health check:

1. Select the container for the server farm that was created.
2. The features for that farm will be displayed, double-click **Health Test**.
3. Input the SMS URL to send the Health Test to.

   > **Note:**
   > See the screenshot for an example for a specific broker. Use the appropriate URL for your SMS broker.
   > Starting in IC 4.0 SU6, adding the parameter `healthcheckignore=1` to the end of the URL suppresses certain error messages in logging that occur when SMSServer receives an invalid URL for an SMS.

4. Click **Apply**.

Verification for Health Test

This option attempts to send a *fake* SMS message to the SMS server. However, the SMS server sends a response back indicating that it is alive. The **Verify URL Test** button can be selected in order to determine if the URL is working. Here is an example of what you should see:

Verify URL Test

Results:

Server Address	Result	Details
10.101.24.50	Fail	Cannot connect to the server. The HTTP status code is 0 ...
10.101.60.9	Pass	Pass

Close
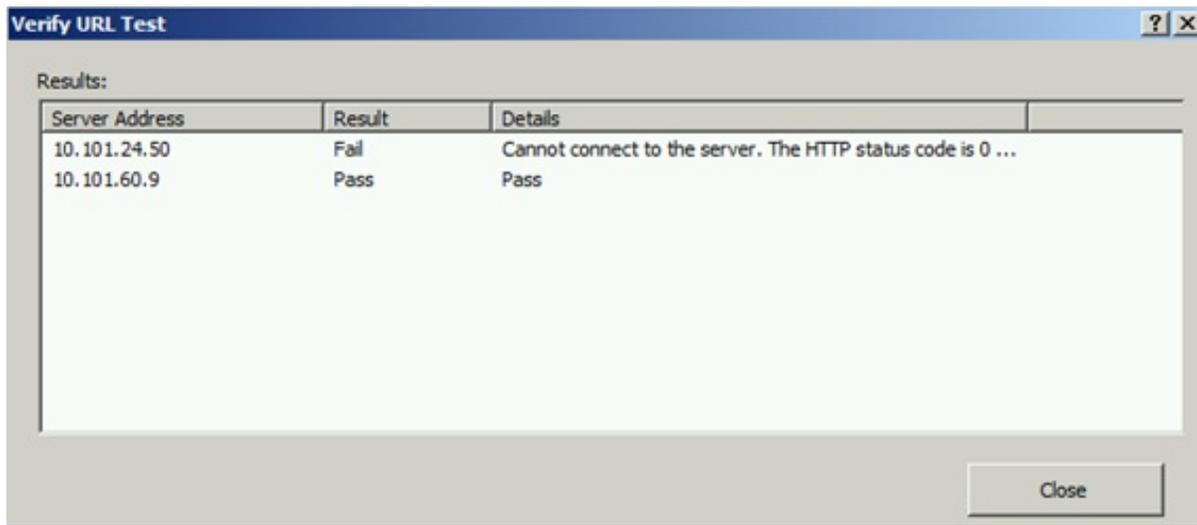
In this example, this URL test indicates that 10.101.60.9 is the active server in the switchover pair and 10.101.24.50 is the backup server. Any HTTP messages sent to this server are redirected to the 10.101.60.9 server and not the backup.

Change Log

Date	Changes
30-March-2011	Created beta release version of this document.
02-August-2011	On title page and in "Installing the SMS Feature," changed the e-mail address for contacting the Beta program.
03-November-2011	Updated for IC 4.0 SMS beta release.
20-March-2012	Updated beta information because only HTTP-based SMS is still in beta.
15-August-2013	Updated for IC 4.0 Service Update 4 with new dialogs, new brokers, setting Web Services parameters, and the ability to define additional brokers. Updated SMS Gateway material and moved it to an appendix.
19-August-2013	Made cosmetic alteration in figure and added HTTP as an option.
26-August-2013	Added notes that users cannot delete the default routes.
25-March-2014	Removed Appendix on SMS Gateway.
08-August-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 Product Information site URLs, and copyright and trademark information.
13-January-2015	Added information to configuration sections that the chat destination option does not support resilience.
15-July-2015	Updated cover page with new logo. Removed incorrect information about types of routing allowed in the outbound routing tab.
21-October-2015	• Added info about outgoing path, internationalize phone numbers, and message parsing to "Message Terminated Tab." • Added information about consolidate messages option in "Outbound Routing Tab." • Updated screenshots.
19-February-2016	Added note to contact PSO if help creating a broker file is needed.
04-April-2016	• Added information about Delivery Receipt URL to "Message Originated Tab." • Added information about SMS Recovery to "Recovery of SMS Interactions in Switchover." • Added "Associate Workgroups and Users." • Updated broker list screenshot.
28-June-2016	Added SMS Reverse Proxy Setup section.
11-November-2016	Added Note about the deprecated gateway configuration interface. Fixed missing Outbound Route image, updated copyright page, and other minor cleanup.
28-February-2017	Updated screen capture in Broker Configuration Dialog: HTTP to remove deprecated gateway configuration.
01-August-2017	Added Using SSL section, with references from the Configuration Tab and Message Terminated Tab sections.
19-Janurary-2018	Rebranded this document to apply Genesys lexicon.
02-February-2018	Converted to HTML format.
07-March-2018	Added International Outbound SMS Messages section to Configure SMS Brokers.
14-June-2018	Review and revision of entire document.
29-October-2018	Updated Installing the SMS Feature. I3_FEATURE_WEB_SERVICES license is required to allow for inbound SMS routing as a chat.
11-February-2019	Added step 4. Click Apply. to Health Test for Server Farm.

07-May-2019	Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section..." For more details, see CICDOC-184.
24-September-2019	Added note to the Set Web Services Parameters to Disconnect Chats topic and Set Web Services Parameters to Disconnect Chats topics point out the custom attributes for **Setting: SMS** which can override timeout settings for all chat interactions.
29-June-2020	Fixed typo in Configure a New Broker topic.
21-October-2020	Added to note in Set Custom Attributes for Web Services Parameters topic: The IdleWarningMessage and IdleDisconnectMessage messages are sent only for web chat interactions. They are not sent for SMS chats.
8-February-2021	Updated Broker_GenesysCloud image in Configure a New Broker topic.