PureConnect®

2023 R3

Generated:

09-November-2023

Content last updated:

22-June-2020

See Change Log for summary of changes.

GENESYS™

Interaction Recorder Remote Content Service

Installation and Configuration Guide

Abstract

This document provides the installation and preliminary configuration procedures for Interaction Recorder Remote Content Service-an optional subsystem of Interaction Recorder-that retrieves recordings, stores them either locally or on another system, and retrieves recordings for playback or export.

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

Table of Contents

Interaction Recorder Remote Content Service Overview

In PureConnect, there are three phases to making a recording:

- Record, compress, and encrypt phase – All three of these actions are done simultaneously through Interaction Media Server or, in the case of screen recordings, on a personal computer.
- Storage phase – Moving the compressed and encrypted recording file to a location, such as a subsystem or a remote file server
- Database phase – Creating an entry in the Customer Interaction Center (CIC) database so that the recording is cataloged and identified to reside in a specific storage location

Interaction Recorder Remote Content Service facilitates the retrieval and storage of both audio and screen recordings in your PureConnect environment. This capability offloads those actions from the Interaction Recorder subsystem that resides on the CIC server thereby granting that server more processing and bandwidth resources for facilitating and handling interactions.

Record Interactions Without Interaction Recorder Remote Content Service

The following diagram displays the process of recording interactions without Interaction Recorder Remote Content Service:

Step	Description
1	CIC facilitates an interaction between a customer and an agent.
2	Interaction Media Server records, compresses, and encrypts the interaction.
3	After the interaction is complete, Interaction Recorder, by way of the CIC server, moves the recording from the Interaction Media Server to a remote storage location.
4	Interaction Recorder writes an entry to the database that identifies the recording and its location.

Record Interactions With Interaction Recorder Remote Content Service

The following diagram displays the process of recording interactions with Interaction Recorder Remote Content Service:

Step	Description
1	CIC facilitates an interaction between a customer and an agent.
2	Interaction Media Server records, compresses, and encrypts the interaction.
3	Based on *Selection Rules*, the CIC server selects an Interaction Recorder Remote Content Service server to move the recording to either itself or to a remote storage location.
4	The selected Interaction Recorder Remote Content Service instance moves the recording from its original recording location to its configured repository.
5	Interaction Recorder creates a database entry for the recording.

Interaction Recorder Remote Content Service Features

Following are the main features of Interaction Recorder Remote Content Service when used in your PureConnect environment.

Interaction Recorder Client playback

You use Interaction Recorder Client installed on a personal computer to play stored recordings.

The following diagram displays how an Interaction Recorder Client, on a personal computer, retrieves recordings from the PureConnect environment with Interaction Recorder Remote Content Service:
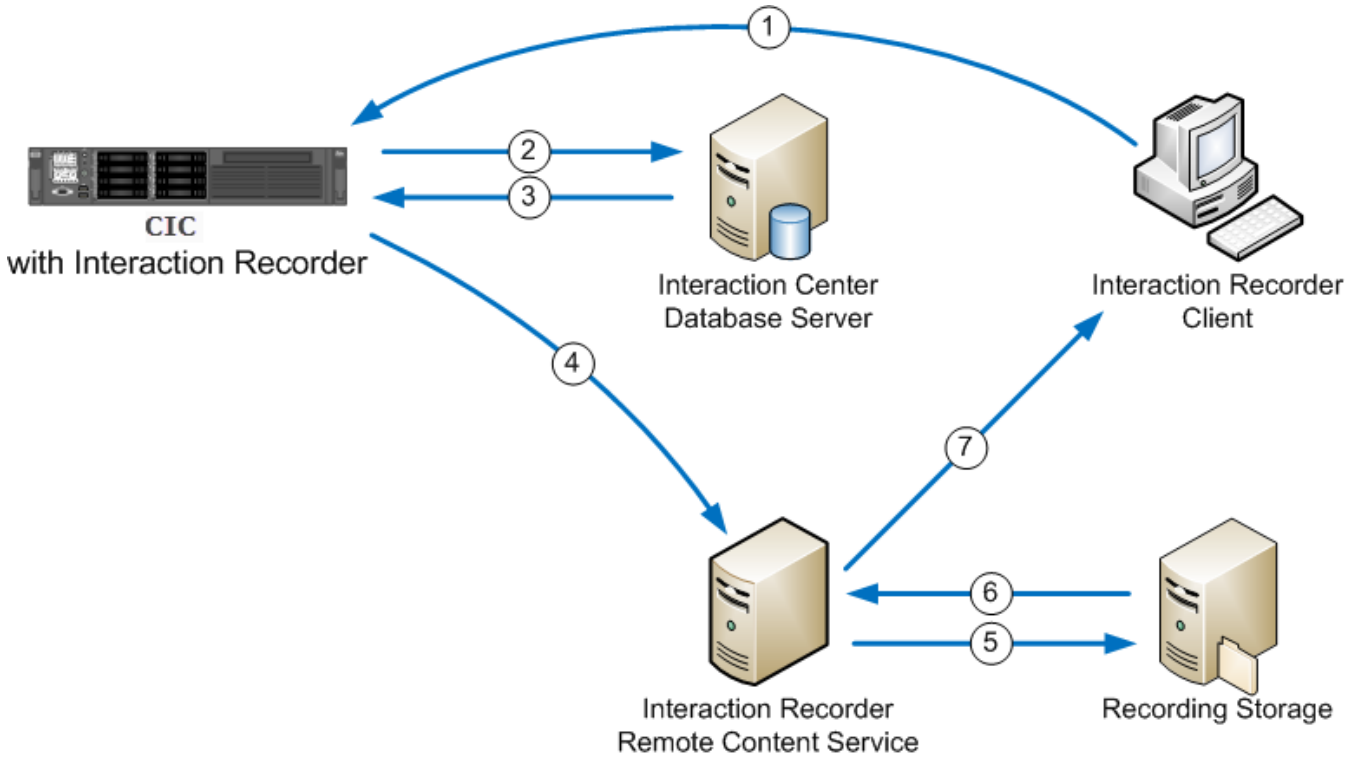

Step	Description
1	Interaction Recorder Client requests playback of a recording from Interaction Recorder on the CIC server.
2	Interaction Recorder looks up the specified recording in the database.
3	The CIC database sends information about the recording file to Interaction Recorder, including the file storage location.
4	Through a bidding process that includes consideration of latency and available storage space, the CIC server selects the best Interaction Recorder Remote Content Service instance to facilitate playback.
5	Interaction Recorder Remote Content Service requests the recording file from the storage server. If you do not have a storage server, the recording file is stored locally on the Interaction Recorder Remote Content Service server.
6	The recording file is retrieved by Interaction Recorder Remote Content Service.
7	The recording file is streamed to the associated telephone or temporarily copied, in encrypted form, to the personal computer.

Interaction Recorder Remote Content Service transmits recordings through an HTTP connection. By default, Interaction Recorder Remote Content Service uses port 8106 for these transfers. If Interaction Recorder Client is on a remote personal computer, ensure that your firewall has this port open so that Interaction Recorder Remote Content Service can send the recording to the remote personal computer.

Export recordings through Interaction Recorder Remote Content Service

Much like Interaction Recorder, Interaction Recorder Remote Content Service can export recordings through Interaction Recorder Client on a personal computer. It also verifies that the logged-on user has the appropriate rights to access the recordings. Exporting a recording through Interaction Recorder Client has no additional interface controls as locating and retrieving the recording is a system process involving Interaction Recorder, the CIC server, and, if available, Interaction Recorder Remote Content Service.

Using Interaction Recorder Remote Content Service in your environment alleviates the sending of recording files through the Interaction Recorder server as the files are decrypted and sent directly to Interaction Recorder Client by Interaction Recorder Remote Content Service using an HTTP connection. CIC selects the Interaction Recorder Remote Content Service to service the export through a bidding process that includes availability, network latency, and available storage space as factors.

Interaction Recorder Remote Content Service co-residence with Interaction Media Server

You can install and run Interaction Recorder Remote Content Service directly on an Interaction Media Server.

> **Important!**
> To support co-residence between Interaction Recorder Remote Content Service and Interaction Media Server, ensure that your Interaction Media Servers have enough available resources for Interaction Recorder Remote Content Service to function without creating resource shortages on the host. If your Interaction Media Server is doing keyword spotting (Interaction Analyzer), recording, and serving as the main conferencing system, you may be required to either upgrade your Interaction Media Server hardware or purchase more Interaction Media Servers.

Interaction Recorder Remote Content Service screen recordings

When screen activity of an agent is recorded during an interaction, the specific Interaction Recorder Remote Content Service server that the CIC server selects is based on the CIC location in which the agent's personal computer resides, not the CIC location of the call, such as the gateway, SIP line, or Interaction Media Server that services the interaction.

Send Recordings as e-mail attachments

Through Interaction Recorder Client, you can send one or more recordings as an e-mail attachment. Interaction Recorder Remote Content Service decrypts the recording and then attaches that recording to the e-mail, which is sent through PostOffice Server on the CIC server. Once the e-mail is sent, Interaction Recorder Remote Content Service removes the temporarily decoded recording to ensure that no one can access it.

Network Configurations for Interaction Recorder Remote Content Service

You can deploy Interaction Recorder Remote Content Service in your network environment in many ways. Various considerations, such as bandwidth usage, recording retrieval, and storage limitations can affect your deployment decisions.

Remote contact center with Interaction Recorder Remote Content Service

The following diagram displays how Interaction Recorder Remote Content Service reduces wide area network (WAN) bandwidth usage by keeping the recording data within the local area network (LAN) of the remote locations.
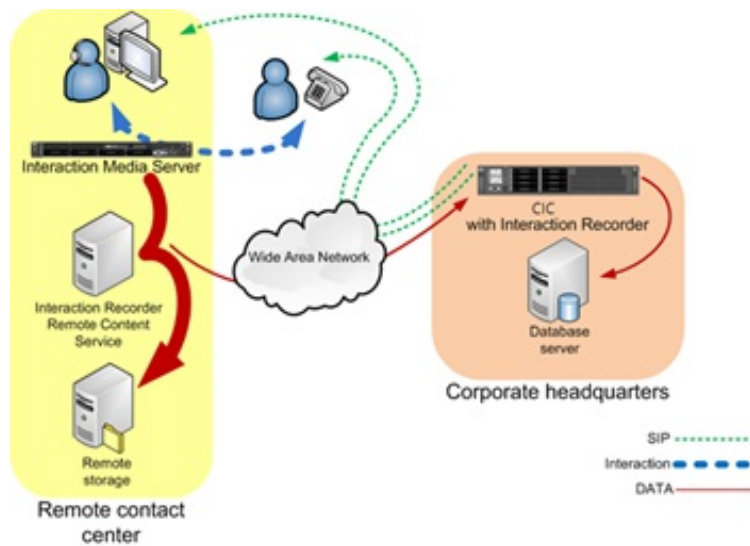
The following list provides the benefits for using Interaction Recorder Remote Content Service in this type of configuration:

- Only small Session Initiation Protocol (SIP) messages and data messages are sent through the WAN.
- The process of moving and storing large recording files is done only through the LAN of the remote contact center.
- You can review recordings at the remote contact center without requiring transmission of the recording through the Interaction Recorder server on the CIC Server.

Multiple Remote Contact Centers with Multiple Servers

The following diagram displays how having multiple Interaction Recorder Remote Content Service servers in multiple remote contact centers allow efficiency and redundancy regarding the storage of recordings in WAN configurations.
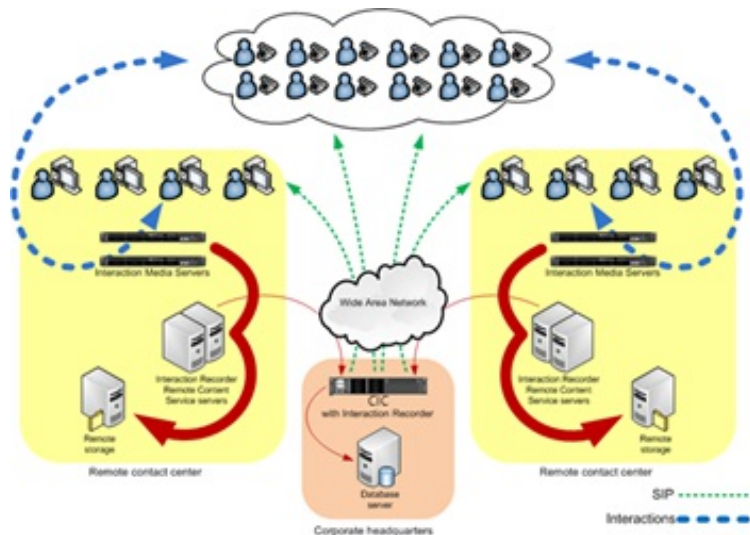
Following are the benefits for using Interaction Recorder Remote Content Service in this type of configuration:

- Interactions, such as call and screen activity, are recorded, compressed, encrypted, and stored in each remote contact center.
- The amount of data that is transmitted over the WAN is reduced.
- You can review recordings at the remote contact center without requiring transmission of the recording through the Interaction Recorder server on the CIC Server.
- Multiple Interaction Recorder Remote Content Service servers provide each remote contact center with redundancy and load balancing so that no recordings are missed because of server maintenance or unforseen hardware failures.

Note: If you ad an Interaction Recorder Remote Content Service instance to a set of existing instances, CIC stores more recordings on the new instance until it has a level similar to the existing instances.

Location Assignments and Server Selection Rules

Interaction Recorder Remote Content Service functions as an independent, non-location-based subsystem. As a result, you cannot assign Interaction Recorder Remote Content Service as a member of a logical location in Interaction Administrator. Instead, you can use Interaction Administrator to configure any Interaction Recorder Remote Content Service server to service one or more locations in which Interaction Media Server creates recordings.

To ensure that Interaction Recorder Remote Content Service removes the work of moving recordings from the CIC Server, it uses location assignments, server selection rules, and a subsequent bidding process, should multiple servers be available for the task.

For more information, see:
- Location Assignments
- Server Selection Rules

Location Assignments

Using Interaction Administrator, you can configure the locations that each Interaction Recorder Remote Content Service server covers. The locations that you enable for an Interaction Recorder Remote Content Service server indicate your preference for the locations that this server services. However, CIC, through the Server Selection Rules feature, can select an Interaction Recorder Remote Content Service server to move a recording, even if it is not configured with the applicable location as a preference.

Server Selection Rules

Similar to other CIC subsystems, Interaction Recorder Remote Content Service uses server selection rules. This feature allows you to configure the order in which the CIC Server searches for and selects an Interaction Recorder Remote Content Service server to move a recording from an Interaction Media Server.

By default, CIC locations are configured to use the **<Default Media Server Selection Rule>** selection rule to select an Interaction Recorder Remote Content Service server to move a recording.

You can create many selection rules in the Selection Rules container in Interaction Administrator. Afterwards, you can assign a selection rule to an individual location. Then, when a recording should be moved from an Interaction Media Server that is a member of that location, CIC uses the assigned selection rule to find an appropriate Interaction Recorder Remote Content Service instance that is active an has enough available storage space to move the recording.
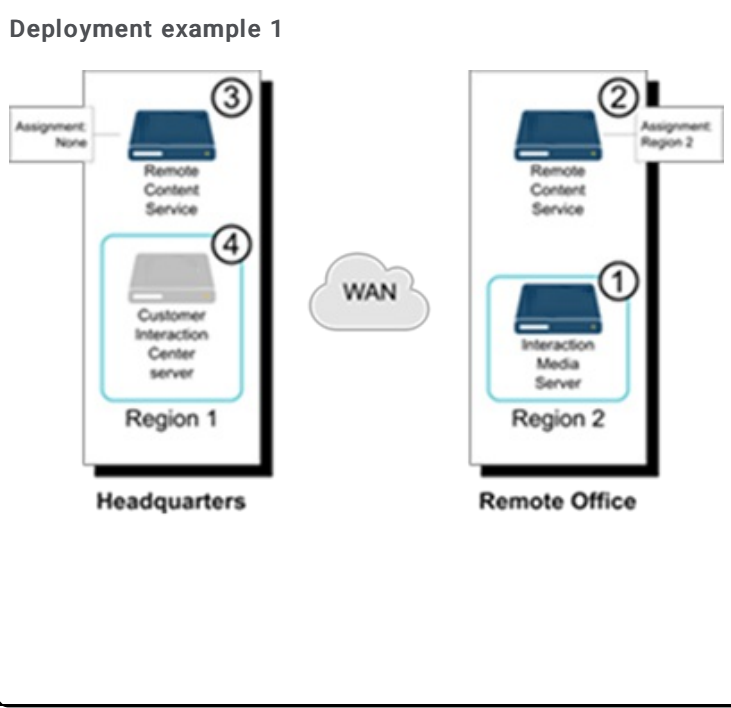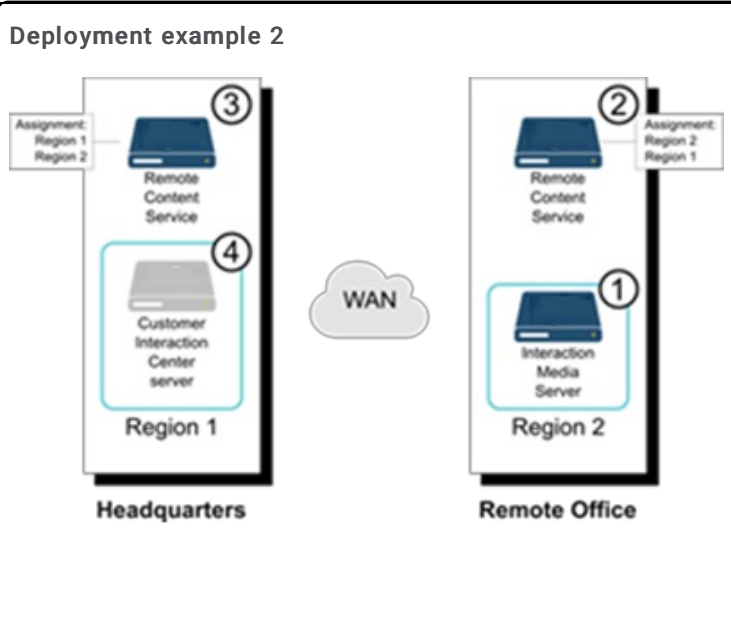
Selection rule location variables

A selection rule can contain defined locations or location variables. Defined locations are those that you have created through Interaction Administrator. Location variables represent relative locations that are involved in an Interaction.

CIC supports the following location variables for Interaction Recorder Remote Content Service in server selection rules.

Location Variable	Description
<This Location>	This variable represents the location that contains the Interaction Media Server that hosts the recording to be moved.
<IC Server Location>	This variable represents the location containing the CIC Server that controls the Interaction for which the recording was made. **Note**: The <IC Server Location> variable indicates only the locatin in which the CIC Server is assigned. It does not represent the CIC Server directly. Only if no Interaction Recorder Remote Content Service servers are available in any location specified in the selection rules does the CIC Server move a recording.
Any*	In each Selection Rules configuration, you can enable the Use any Location option. This option directs CIC to use an Interaction Recorder Remote Content Service in the network—and not in the exclusion list below the option—if it cannot find another server available in the previous locations.

Deployment examples

The following deployment examples can help you understand how you can use location assignments and selection rules with Interaction Recorder Remote Content Service.

Deployment example 1	Locations:
	- Region 1 - Region 2
	Selection rule: <This Location> <IC Server Location> **Do not use any other Locations** option enabled
	1. A recording is created on an Interaction Media Server in the Region 2 location. 2. The CIC Server locates all RCS servers assigned to Region 2 (<This Location>). If an RCS server is available, it moves the recording. 3. If no RCS servers are available and no others are found in the other locations, the CIC Server moves the recording. **Note:** The RCS server located at Headquarters is not assigned to service any locations and the **Use any Location** option is not set in the selection rule.

Deployment example 2	Locations:
	- Region 1 - Region 2
	Selection rule: <This Location> <IC Server Location> **Do not use any other Locations** option enabled
	1. A recording is created on an Interaction Media Server in the Region 2 location. 2. The CIC Server locates all RCS servers assigned to Region 2 (<This Location>). 3. Since there is more than one RCS server assigned to the location, CIC uses a load balancing process to select a server. 4. If no RCS servers are available, the CIC Server moves the recording.

Deployment example 3	Locations:
	• Region 1 • Region 2
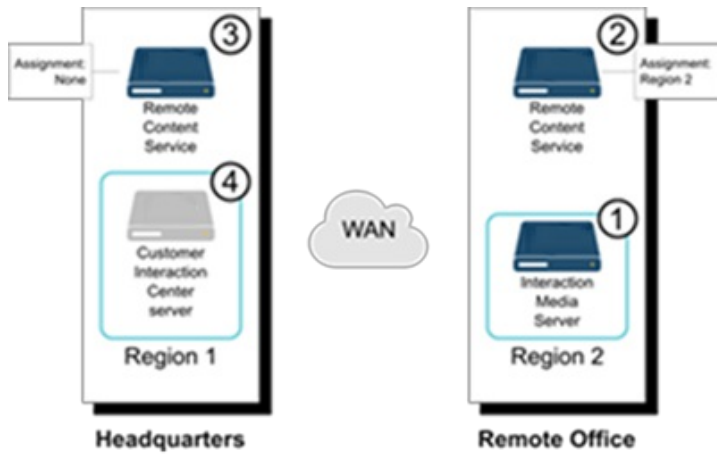
<table>
<tr><td colspan="2">

Selection rule:

<This Location>

<IC Server Location>
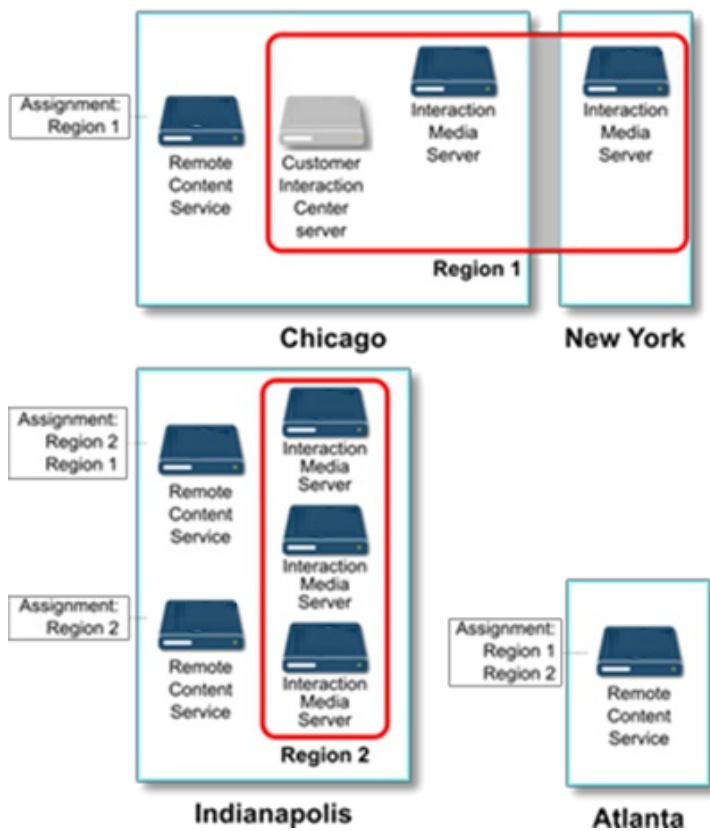
Use any Location option enabled
</td></tr>
</table>

1. A recording is created on an Interaction Media Server in the Region 2 location.
2. The CIC Server locates all RCS servers assigned to Region 2 (<This Location>).
3. The CIC Server attempts to locate all RCS servers assigned to Region 1 (<IC Server Location>).

   Note: The RCS server that is physically located at Headquarters is not assigned to a location and is not selected by the CIC Server for <IC Server Location>.
4. Finding no RCS servers assigned <IC Server Location>, the CIC Server, because of the **Use any Location** option, can select any RCS server that is registered and functional. At this step, the CIC Server selects the RCS server at Headquarters.

Deployment example 4	Locations:
	• Region 1 • Region 2

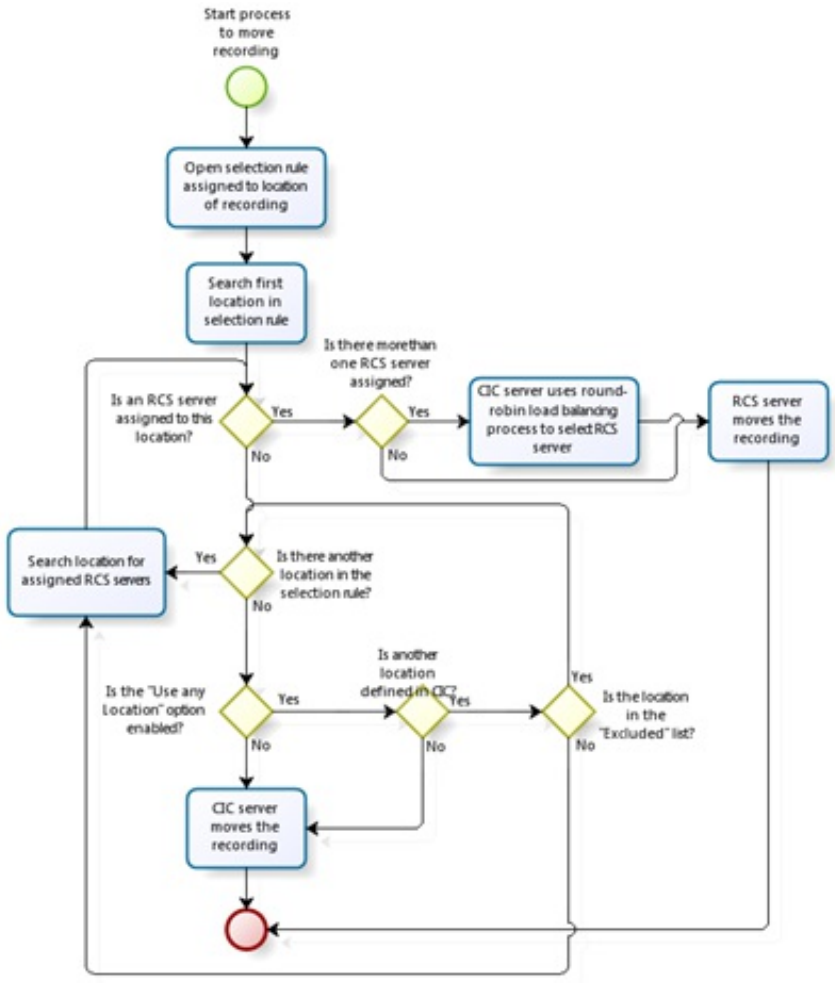**Selection rule:**

<This Location>

<IC Server Location>

Use any Location option enabled

This complex example displays how the combination of Location assignments and selection rules can result in a system where the selection of an RCS server by the CIC Server can become confusing and difficult to follow.

Even with only two logical locations defined in CIC, the combination of multiple location assignments to RCS servers, disparate geographic locations, and the **Use any Location** option creates a situation where any RCS server can move a recording.

However, even with this complex configuration, the resources of the CIC Server remain unburdened as an RCS server should always be available to move a recording.

Overall server selection process

Recording Retrieval Process

After Interaction Recorder Remote Content Service moves a recording, users may need to review or export the recording. CIC uses a different process for selecting which Interaction Recorder Remote Content Service to facilitate those types of retrievals.

For any recording retrieval where Interaction Recorder Remote Content Service is deployed, CIC creates a list of the existing locations, which have been defined in the Regionalization container of Interaction Administrator. From that list, CIC determines which Interaction Recorder Remote Content Service systems serve those locations.

> **Note**: CIC removes any Interaction Recorder Remote Content Service system that is inactive from the list of systems that can facilitate the retrieval of a recording.

If CIC locates more than one Interaction Recorder Remote Content Service system that can facilitate the recording retrieval, it then determines the values for several criteria, including network latency and available storage space, to select the optimal system.

Interaction Recorder Remote Content Service Installation

Interaction Recorder Remote Content Service Requirements

Following are the minimum requirements for installing and using Interaction Recorder Remote Content Service.

|	
Operating system	• Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2
CPU	Intel Xeon, 2.4 GHz
Media drive	DVD-ROM drive
Hard drive	• 346 MB of free space • 7200 rpm or higher
Memory	4 GB
Network Interface Card	Gigabit Ethernet
Software	• CIC 20*nn* R*n* on another server in the network • Interaction Media Server 20*nn* R*n* on another server in the network • Microsoft .NET Framework 3.0 or greater **Important!** Interaction Media Server and Interaction Recorder Remote Content Service must be on the same or newer version as the CIC server.The Interaction Recorder Remote Content Service and Media Servers can be on different versions as long as they are the same or newer than the CIC server.

Install Interaction Recorder Remote Content Service

Following are the prerequisites for installing Interaction Recorder Remote Content Service:
- If you are a PureConnect Cloud customer, you must first generate a certificate through the procedure specified in Regenerate Interaction Recorder Remote Content Service Certificates.
- If you apply an upgrade, you must upgrade Interaction Recorder Remote Content Service before you upgrade the CIC server. Interaction Recorder Remote Content Service is backwards compatible with CIC servers of previous version.

To install Interaction Recorder Remote Content Service
1. If you have not done so already:
   a. Download the CIC `.iso` file from the PureConnect product information site at the following URL address:
      https://my.inin.com/products/Pages/Downloads.aspx.
   b. Copy the `.iso` file to a non-CIC file server with a high bandwidth connection to the machines on which you will install Interaction Recorder Remote Content Service.
   c. Mount the `.iso` file and share the contents to make them accessible to the machines on which you will install Interaction Recorder Remote Content Service.
2. In the mounted `.iso` image, open the `\Installs\Off-ServerComponents` directory.
3. Copy the `IRRemoteContentService_20nnRn.msi` file to the machine on which to install Interaction Recorder Remote Content Service.
4. Run the `IRRemoteContentServer.msi` file.
5. If the **Security Warning** dialog box appears, click **Run**. The **Interaction Recorder Remote Content Service for CIC Setup** dialog box appears.
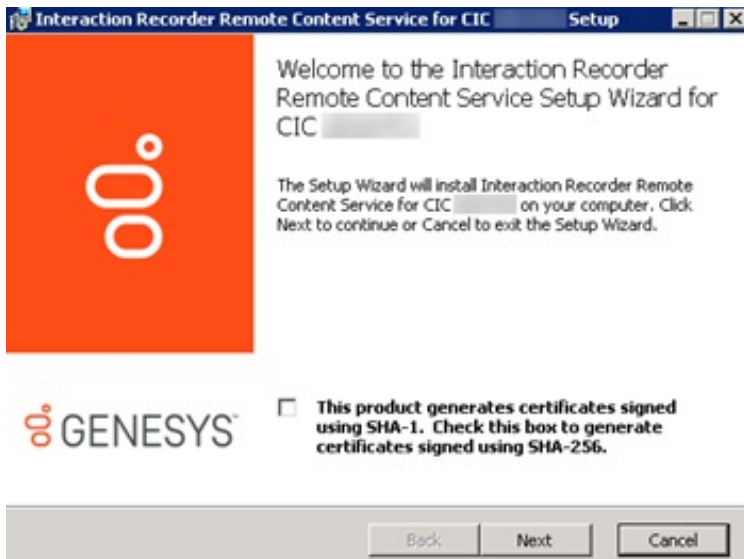
For a *new* installation (not an upgrade or patch), a check box for specifying the certificate signing method appears. For more information about SHA-1 and SHA-256, see:

- Certificate Digest in the *IC Setup Assistant Help*
- *PureConnect Security Features Technical Reference* (requires logon credentials)

6. Do one of the following:

- To generate certificates signed using SHA-1, leave the certificate signing method check box cleared.
- To generate certificates signed using SHA-256, select the certificate signing method check box.

7. Click **Next**. The **Custom Setup** dialog box appears.
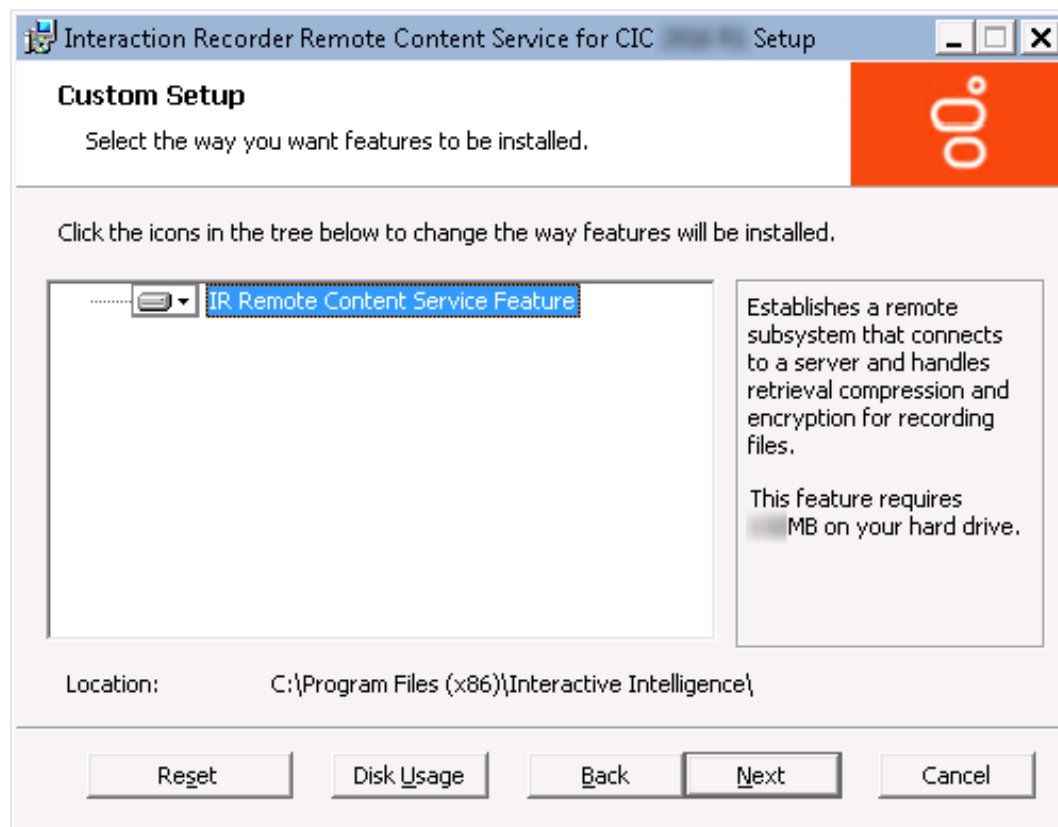
8. To choose a different installation location, click **Browse** and then select a different directory. Otherwise, click **Next**. The **IR Remote Content Service Connection** dialog box appears.
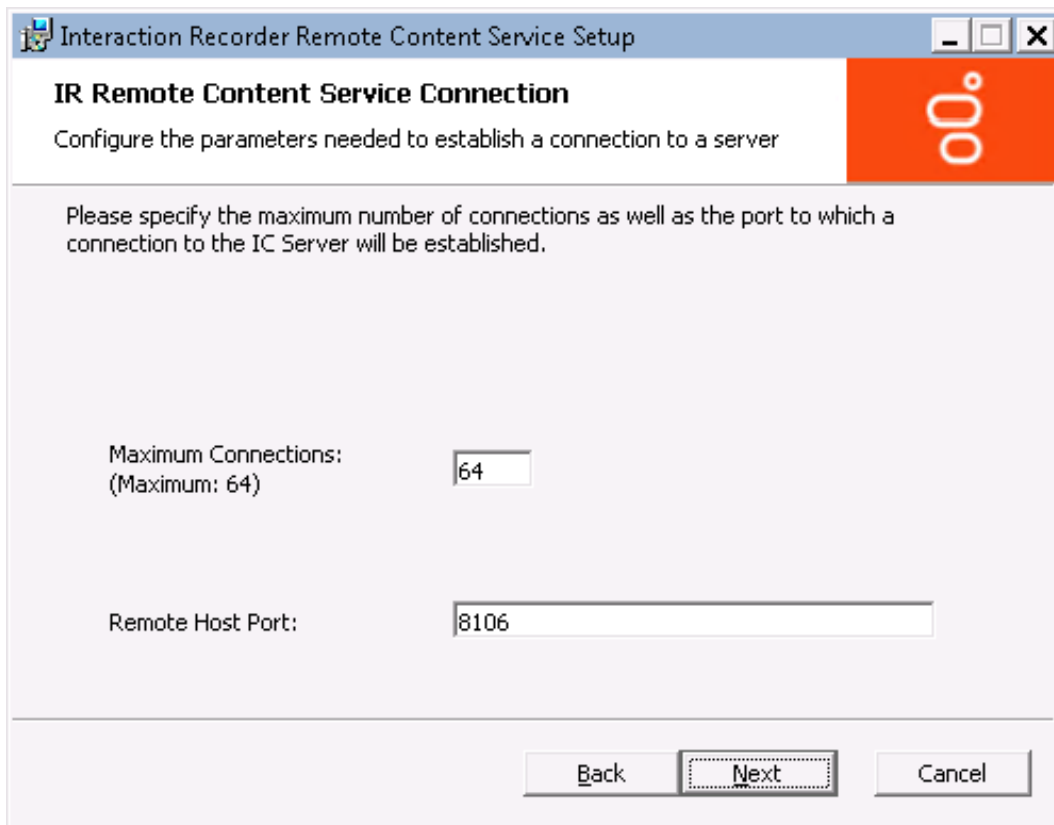
> **Notes:**
> - Ensure that the hard disk drive has enough free space to install the software. Click **Disk Usage** and, in the resulting dialog box, verify that you have at least 350 megabytes of free space.
> - By default, the PureConnect QoS driver installs silently and the install adds the certificate to the Trusted Publishers list. If your site has reasons to modify this default behavior, see KB article https://genesyspartner.force.com/customercare/pkb_Home?id= kA50B0000008R5H. Follow the instructions provided in the KB article to modify the QoS properties and run the install using Group Policy or other methods. You must have a user account on the PureConnect Customer Care website to view the article.

9. In the **Maximum Connections** box, type a value that corresponds to the number of simultaneous connections that can be made to Interaction Recorder Remote Content Service.

   Valid values range from 0 (zero) to 64.

   > **Important!**
   > Setting the value of the **Maximum Connections** box to a low number can severely limit the ability of Interaction Recorder Remote Content Service to service recordings. You must specify a value that adequately represents the predicted workload that this Interaction Recorder Remote Content Service instance is intended to support. If you need to later adjust this value, edit the configuration file. For more information, see Interaction Recorder Remote Content Service Configuration File.

10. In the **Remote Host Port** box, type the port number on this server for Interaction Recorder Remote Content Service to use for inbound communications from Interaction Recorder, Interaction Recorder Client, and Interaction Media Server.

    > **Important!**
    > Ensure that the port number is not in use by any other service or application.

11. Click **Next**. The **Please specify the IC Servers** dialog box appears.
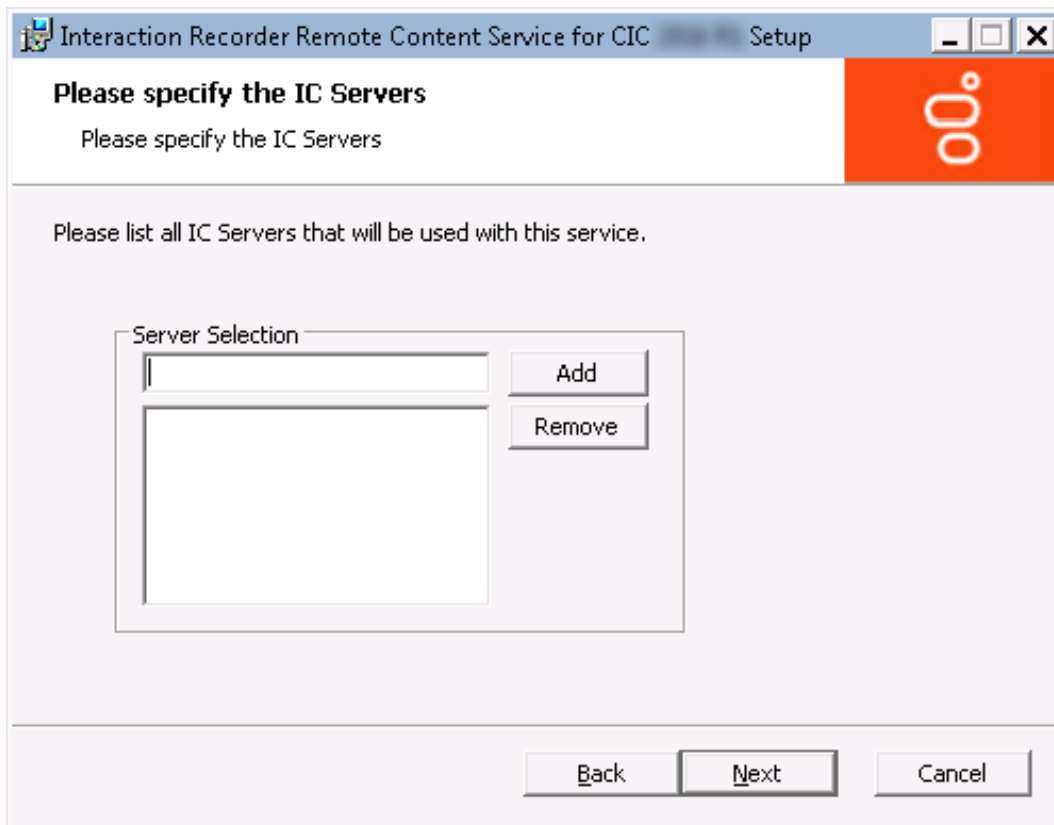
12. In the **Server Selection** box, type the fully-qualified domain name of the CIC server to communicate with Interaction Recorder Remote Content Service and then click **Add**.

    Genesys recommends that you do not use an IP address to specify the CIC server as it causes certificate authentication to fail.

    > **Note:**
    > If you have a fallback CIC server, type it in the **Server Selection** box.

    To remove an item, click it and then click **Remove**.

13. If necessary, repeat the previous step for other CIC servers that you want to connect with this Interaction Recorder Remote Content Service server. When finished adding CIC servers, click **Next**. The **Domain User Validation** dialog box appears.
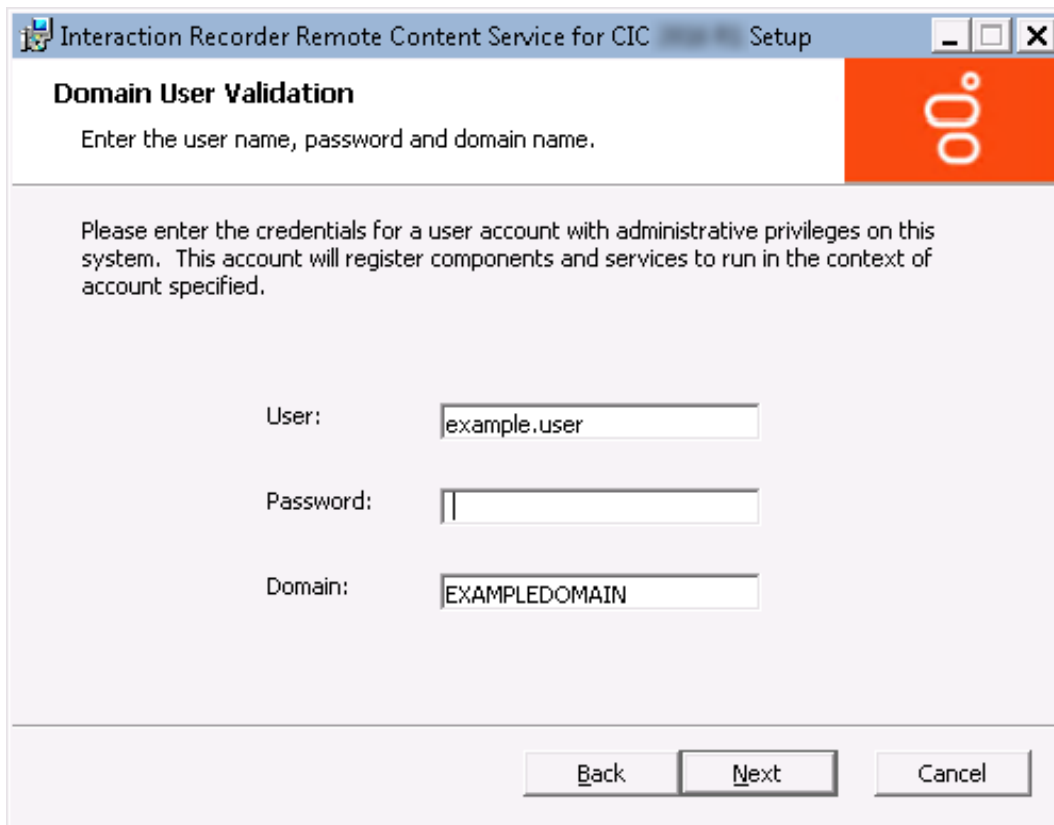
14. In the **Password** box, type the password of the logged in user and the click **Next**. The **Interaction Center Server and Credentials** dialog box appears.
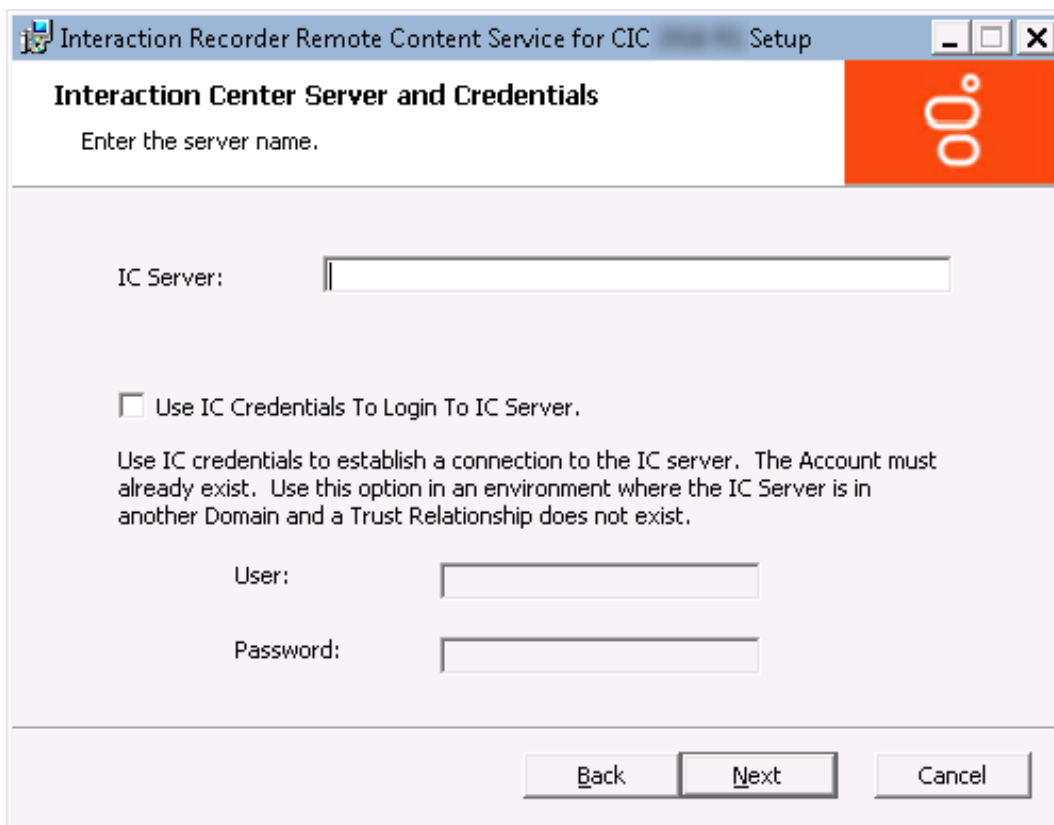
> **Important!**
> The user account that you used to log on to this server machine must be a member of the **Administrators** group and must be able to access the shared network resources of the Interaction Media Server. If the account is not able to access the recordings directory on Interaction Media Server, cancel the installation, log off, and log on with a user identity that can.

15. In the **IC Server** box, type the fully-qualified domain name for the main CIC server and then click **Next**. This step creates the necessary security certificates to that the systems can communicate.

    Genesys recommends that you do not use an IP address to specify the CIC server as it causes certificate authentication to fail.

16. If the CIC server resides in a different domain than the machine on which you are installing Interaction Recorder Remote Content Service, select the **Use IC Credentials To Login To IC Server** check box.

17. In the **User** and **Password** boxes, type the credentials of a defined CIC server administrator and then click **Next**. The **Ready to install Interaction Recorder Remote Content Service** dialog box appears.
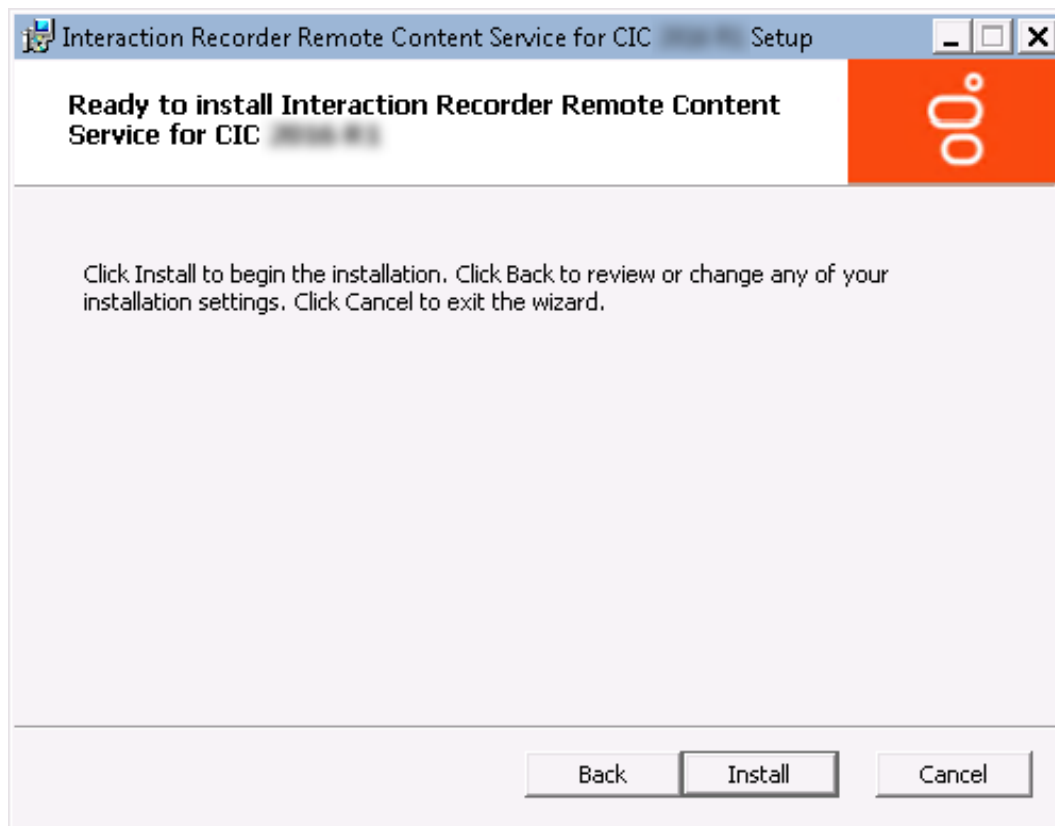

18. Click **Install**. The **Installing Interaction Recorder Remote Content Service** dialog box appears and provides the status of the installation process.

19. When the installation process is finished, click **Finish**.

Uninstall Interaction Recorder Remote Content Service

To uninstall Interaction Recorder Remote Content Service

1. Using an administrative user account, log on to the Windows host where you installed Interaction Recorder Remote Content Service.
2. Click **Start** > **Control Panel**.
3. In the **Control Panel** window, double-click **Programs and Features**. The **Uninstall or change a program** window appears.
4. In the list of programs, click **Interaction Recorder Remote Content Service**.
5. Click **Uninstall**.
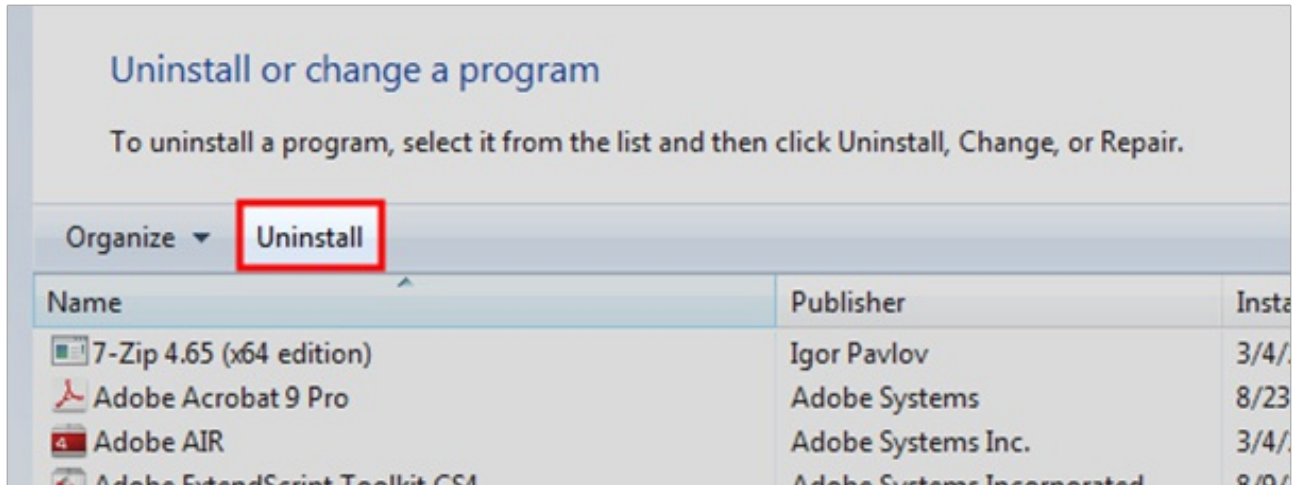
6. In the confirmation dialog box, click **Yes**.
7. Wait while Windows uninstalls Interaction Recorder Remote Content Service.

Configure Interaction Recorder Remote Content Service

Complete the following tasks to configure Interaction Recorder Remote Content Service:

- Trust the Interaction Recorder Remote Content Service Connection in Interaction Administrator
- Configure Interaction Recorder Remote Content Service Through Interaction Administrator
- Configure Interaction Recorder Remote Content Service Selection Rules
- Interaction Recorder Remote Content Service Configuration File
- Regenerate Interaction Recorder Remote Content Service Certificates
- Create an HTTPS Certificate Signed by a Certificate Authority for Viewing Playback

Trust the Interaction Recorder Remote Content Service Connection in Interaction Administrator

Interaction Recorder Remote Content Service generates a certificate automatically for connecting to a CIC server. However, you must use Interaction Administrator to trust that certificate before you can use Interaction Recorder Remote Content Service to move, store, and retrieve recordings.

To trust the Interaction Recorder Remote Content Service connection in Interaction Administrator

1. Open Interaction Administrator and, if necessary, log on as a CIC administrator.
2. In the navigation pane of the **Interaction Administrator** window, click **System Configuration**.
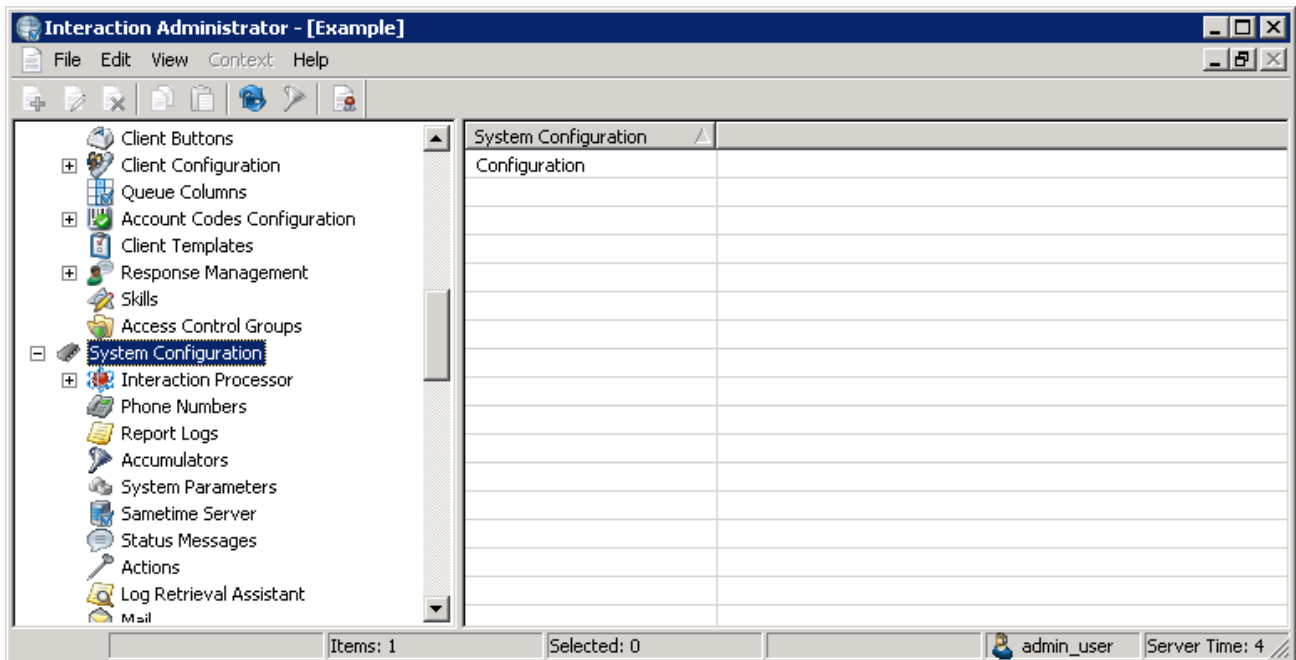
3. In the configuration pane, double-click the **Configuration** item. The **System Configuration** dialog box appears.

System Configuration

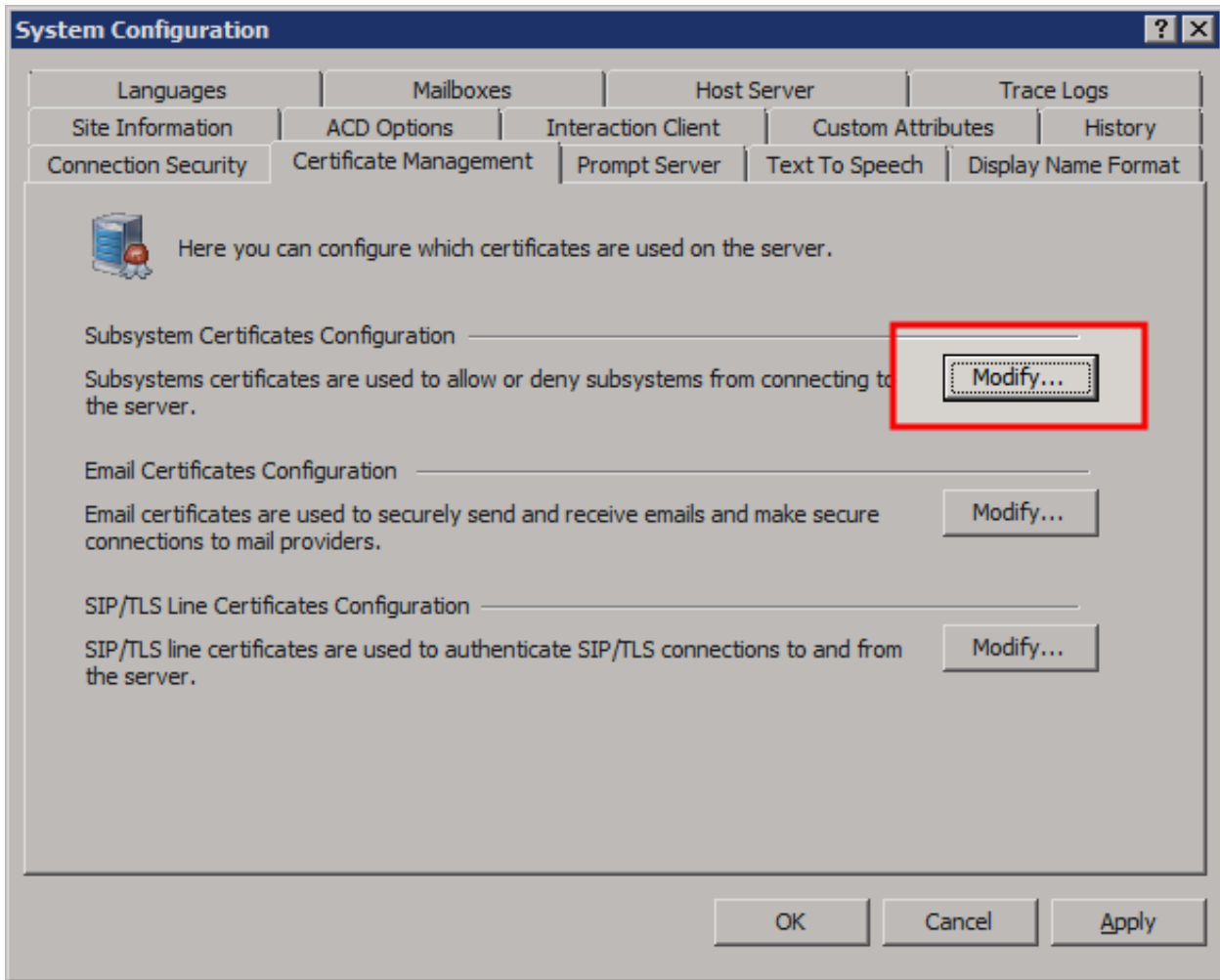| Languages	Mailboxes	Host Server	Trace Logs
Connection Security	Certificate Management	Prompt Server	Text To Speech	Display Name Format
Site Information	ACD Options	Interaction Client	Custom Attributes	History

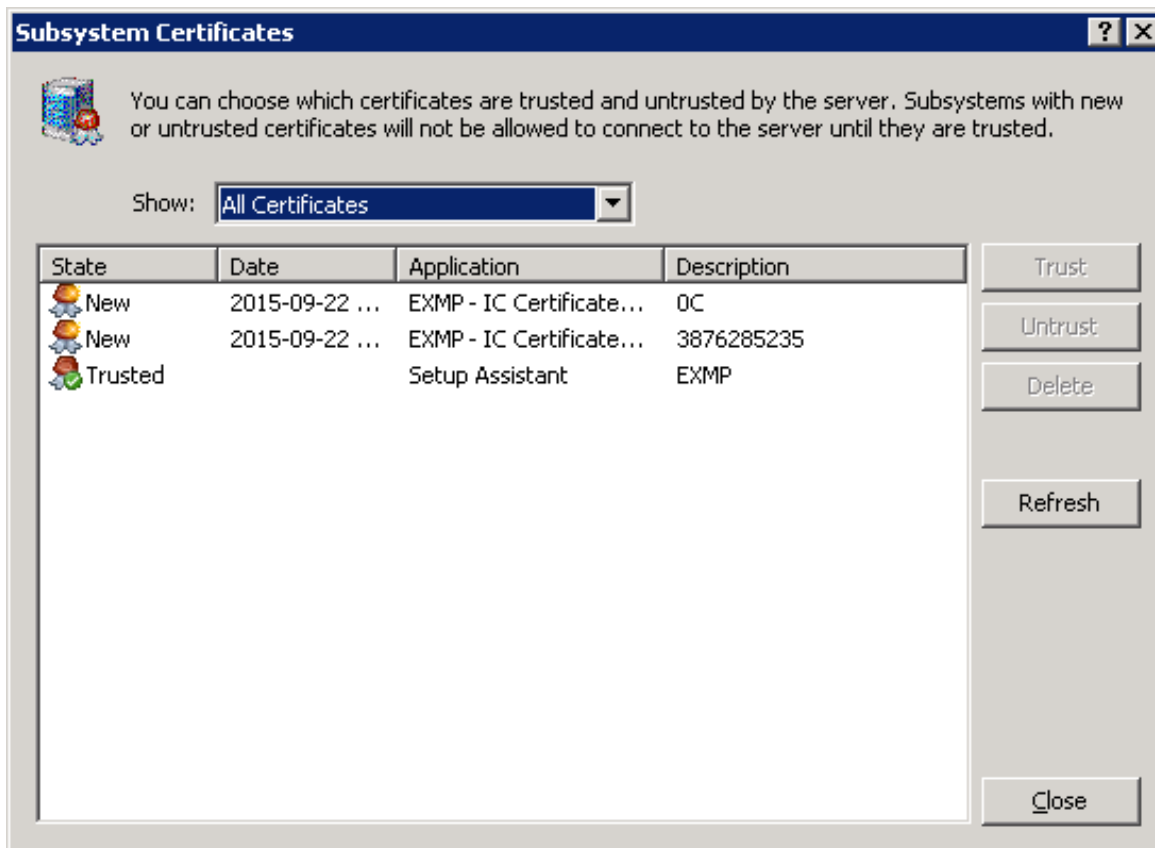Enter the name of your company, and an optional location name.

Organization Name: `OrganizationName`

Location Name: `Location 111`

[OK] [Cancel] [Apply]

4. Click the **Certificate Management** tab.

System Configuration

Languages	Mailboxes	Host Server	Trace Logs
Site Information	ACD Options	Interaction Client	Custom Attributes	History
Connection Security	Certificate Management	Prompt Server	Text To Speech	Display Name Format

Here you can configure which certificates are used on the server.

Subsystem Certificates Configuration

Subsystems certificates are used to allow or deny subsystems from connecting to the server.

[Modify...]

Email Certificates Configuration

Email certificates are used to securely send and receive emails and make secure connections to mail providers.

[Modify...]

SIP/TLS Line Certificates Configuration

SIP/TLS line certificates are used to authenticate SIP/TLS connections to and from the server.

[Modify...]

[OK]   [Cancel]   [Apply]

5. Under **Subsystem Certificates Configuration**, click **Modify**. The **Subsystem Certificates** dialog box appears with a **New** certificate from the Interaction Recorder Remote Content Service server.

6. Click the new certificate and then click **Trust**.
7. In the **Subsystem Certificates** dialog box, click **Close**.
8. In the **System Configuration** dialog box, click **OK**. The certificate for Interaction Recorder Remote Content Service is now trusted and the two servers can communicate securely.
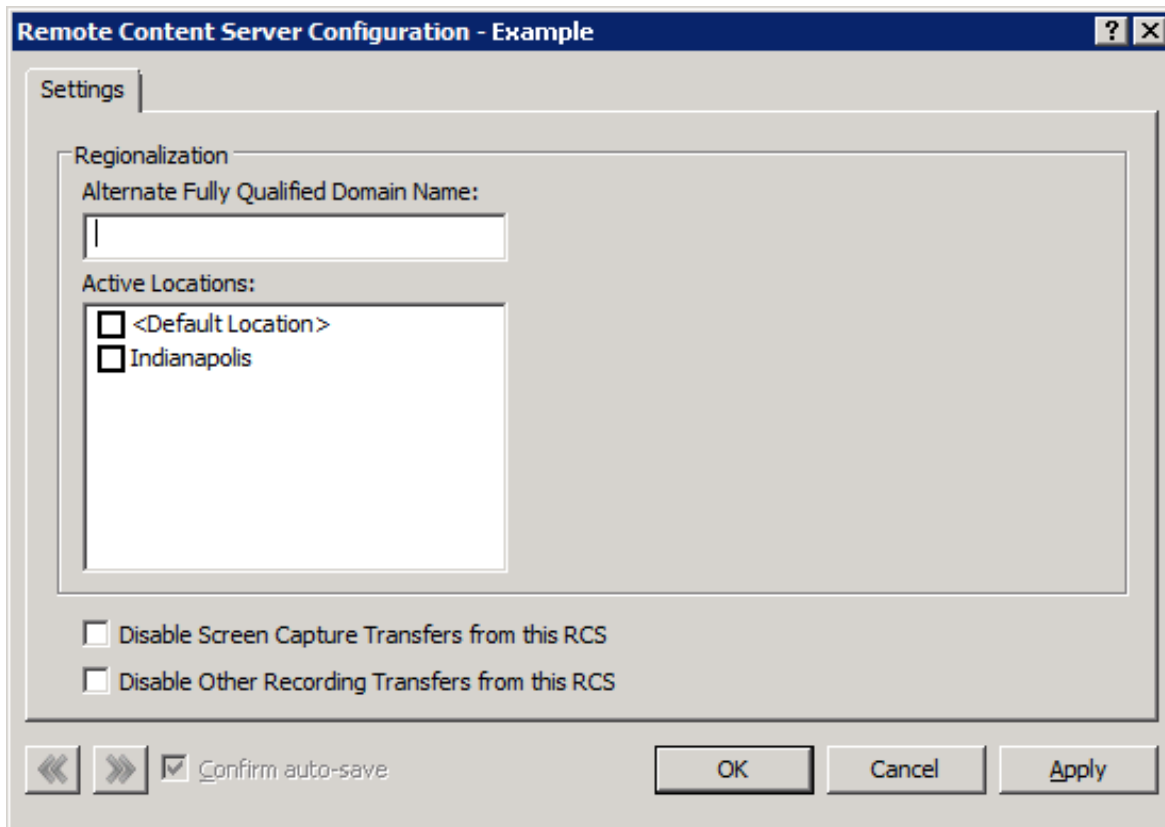
Configure Interaction Recorder Remote Content Service Through Interaction Administrator

To configure Interaction Recorder Remote Content Service through Interaction Administrator

1. Open Interaction Administrator and log on as an administrative user.
2. In the navigation pane, expand the **Interaction Recorder** container.
3. In the **Interaction Recorder** tree, click the **Remote Content Server** object.

    ⊟ 📷 Interaction Recorder
         📷 Policy Editor
         📷 Screen Recording
         📷 Remote Content Server
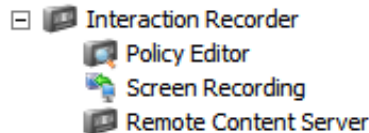
4. In the details pane, double-click the entry for the Interaction Recorder Remote Content Service instance that you want to configure. The **Remote Content Server Configuration** dialog box for the selected server appears.

Alternate Fully Qualified: If you are using PureConnect Cloud, specify a replacement fully-qualified domain name (FQDN) for this Interaction Recorder Remote Content Service server in your domain. In a PureConnect Cloud environment, this feature allows Interaction Recorder to retrieve and play the recording from this Interaction Recorder Remote Content Service server.

Active Locations: If selected, you want the Interaction Recorder Remote Content Service server to move recordings from Interaction Media Servers for that region.

Disable Screen Capture Transfers from this RCS: If selected, you want to prevent this Interaction Recorder Remote Content Service instance from transferring screen recordings from the computers on which they are recorded.

Disable Other Recording Transfer from this RCS: If selected, you want to prevent this Interaction Recorder Remote Content Service instance from transferring any recordings—other than screen recordings—from the servers on which they are recorded.

> **Note:**
> CIC uses only those Interaction Recorder Remote Content Service instances listed as **Active**. However, you can configure any listed instance, regardless of its state.

5. To view or adjust the configuration for another defined Interaction Recorder Remote Content Service server, click << or >>.
6. To have Interaction Administrator save your configuration settings automatically as you cycle through Remote Content Service servers, select the **Confirm auto-save** check box.
7. When finished, click **OK**.

Configure Interaction Recorder Remote Content Service Selection Rules

The Selection Rules feature of Interaction Administrator enables you to create lists or prioritized locations that the CIC server uses when selecting a subsystem server, such as Interaction Media Server or Interaction Recorder Remote Content Service, for a specific operation.

> **Important!** If you modify an existing Selection Rules configuration, it affects all locations that currently use that configuration. Before you modify the configuration, Genesys recommends that you validate how the proposed modifications can affect each location that uses the configuration.

To configure Interaction Recorder Remote Content Service Selection Rules

1. On the CIC server or a remote personal computer, open Interaction Administrator. The **Interaction Administrator** window appears.

   > **Note:**
   > To add or modify Selection Rules configurations, your CIC user account must have the **Administrator Access** permission for the configurations. Those configurations are in the **Selection Rules** section of the **Administrator Access** dialog box in Interaction Administrator. For more information, see "Administrator Access" in the *Interaction Administrator Help* at https://help.genesys.com/cic/mergedProjects/wh_ia/desktop/interaction_administrator_help.htm.

2. In the navigation pane under the object that represents your CIC server, expand the **Regionalization** container.

3. Under the **Regionalization** container, click the **Selection Rules** object.
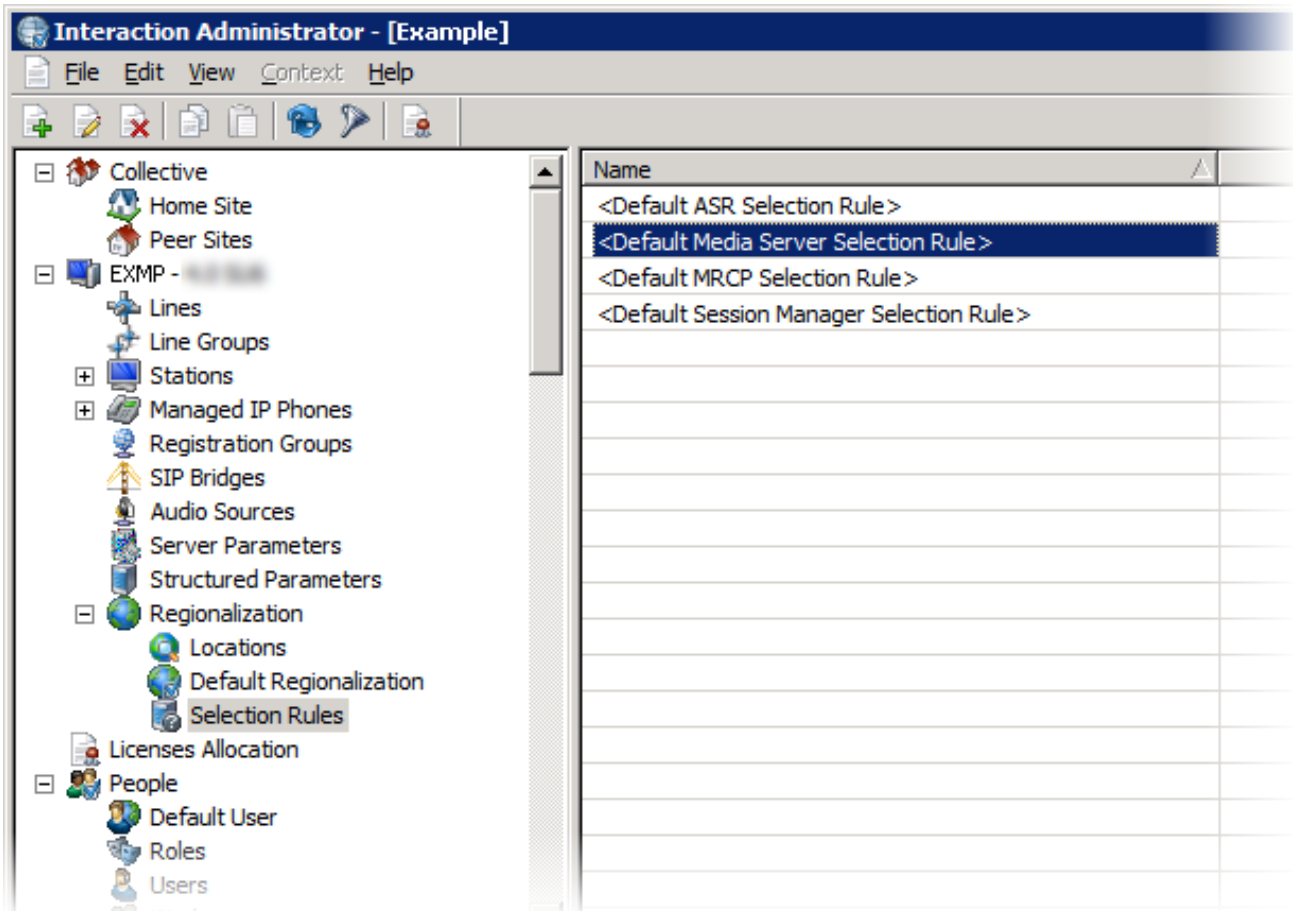
4. Do one of the following:
   - To create a Selection Rules configuration, do the following:
     a. Right-click an empty area in the right pane and click **New** from the resulting shortcut menu.
     b. In the **Entry Name** dialog box, type a unique name for the new Selection Rules configuration and then click **OK**.
   - To modify an existing Selection Rules configuration, double-click the Selection Rules entry in the configuration pane.

   The **Selection Rule Configuration** dialog box appears.
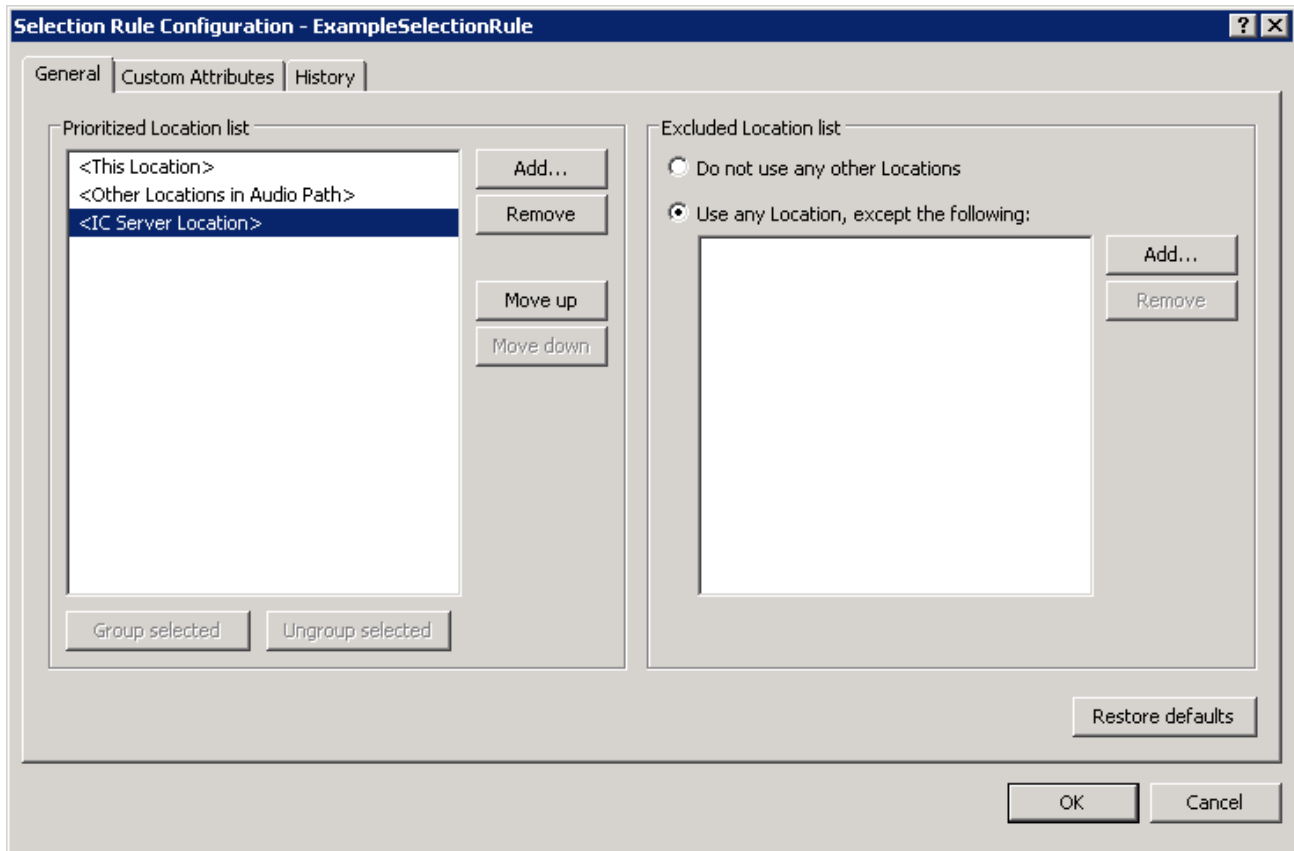
Prioritized Location list

> **Add:** Adds a static or variable location to the **Prioritized Location list** box..
>
> **Remove:** Removes a selected location.
>
> **Move up:** Moves a selected location to a higher position in the list.
>
> **Move down:** Moves a selected location to a lower position in the list.
>
> **Group selected:** Assigns selected locations to a group that provides load balancing.
>
> **Ungroup selected:** Removes selected locations from an existing group.

Excluded Location list

> **Do not use any other Locations:** If selected, restricts CIC from selecting locations not listed in the **Prioritized Location list** box.
>
> **Use any Location, except the following:** If selected, allows CIC to select any available location after it cannot locate an available Interaction Recorder Remote Content Service server assigned to the location in the **Prioritized Location list** box. CIC excludes locations specified in the **Excluded Location list** box.
>
> **Add:** Adds a location to the **Excluded Location list** box.
>
> **Remove:** Removes the selected location from the **Excluded Location list** box.
>
> **Restore defaults:** Resets the configuration to the default settings.

Tip: To select multiple locations, press and hold the **Ctrl** key while clicking each location.

5. On the **General** tab, modify the Selection Rules configuration and then click **OK**.

Interaction Recorder Remote Content Service Configuration File

During the installation of Interaction Recorder Remote Content Service, you specified the port that it uses and the maximum number of simultaneous connections. To change these values, edit the configuration file.

> **Note:**
> If you edit the configuration file, restart Interaction Recorder Remote Content Service for the changes to take effect.

The name of the Interaction Recorder Remote Content Service configuration file is `ircontentserverconfig.xml`. It is in the directory that contains the service binary files on the server running Interaction Recorder Remote Content Service.

The following example provides the default contents of the configuration file.

```
<IRContentServerConfig>
<HttpPort>8106</HttpPort>


 <HttpPort>8107</HttpsPort>
<MaxConnections>64</MaxConnections>


 <ICServers>


 <ICServer>


 <HostName>CICServerA</HostName>


 </ICServer>


 <ICServer>


 <HostName>CICServerB</HostName>


 </ICServer>


 </ICServers>
</IRContentServerConfig>
```

The configuration file specifies the following information:

- `<HttpPort>` - The port through which a HyperText Transfer Protocol (HTTP) connection is made
- `<MaxConnections>` - The maximum number of simultaneous connections to this Interaction Recorder Remote Content Service server allowed. This number represents the maximum number of simultaneous recording playbacks that this server allows.

  > **Note:**
  > While the installation program allows you to specify a maximum of 16 connections, you can specify larger values for the `<MaxConnections>` entry, such as 32 and 64.

- `<BidExpirationTime>` – The maximum number of seconds allowed to pass from the time Interaction Recorder Remote Content Service receives a bid request to the time it sends a bid response. If the waiting time for a bid exceeds the number of seconds, the Interaction Recorder Remote Content Service does not continue processing the bid request. Valid entries are between 15 and 45 seconds. The default of 0 indicates no wait time limit.

Regenerate Interaction Recorder Remote Content Service Certificates

The installation program creates a security certificate for this Interaction Recorder Remote Content Service server. However, if you change the server's domain, you may need to regenerate this security certificate manually so that this server can communicate with the CIC server.

To manually regenerate a certificate for this server

1. On the Interaction Recorder Remote Content Service server, open a command prompt window.
2. In the command prompt window, open the directory where you installed Interaction Recorder Remote Content Service. The default installation location is one of the following paths, depending on your operating system:
   - `C:\Program Files\Interactive Intelligence\IRRemoteContentService\`
   - `C:\Program Files (x86)\Interactive Intelligence\IRRemoteContentService\`
3. Run the following command:
   `gensslcertsu.exe –r CIC_Server_Name CIC_User_Name CIC_User_Password -f`
   The parameters for this command are:
   - *CIC_Server_Name* – Name of the CIC server on which you are generating the certificate.
   - *CIC_User_Name* – CIC administrator's user name.
   - *CIC_User_Password* – CIC administrator's password.

   Note:
   You must specify these variables correctly for this command to be successful.

   The CIC server creates a certificate for all remote subsystems and adds the Interaction Recorder Remote Content Service instance.
4. In the **Services** window, restart the **ININ Remote Content Service** service.
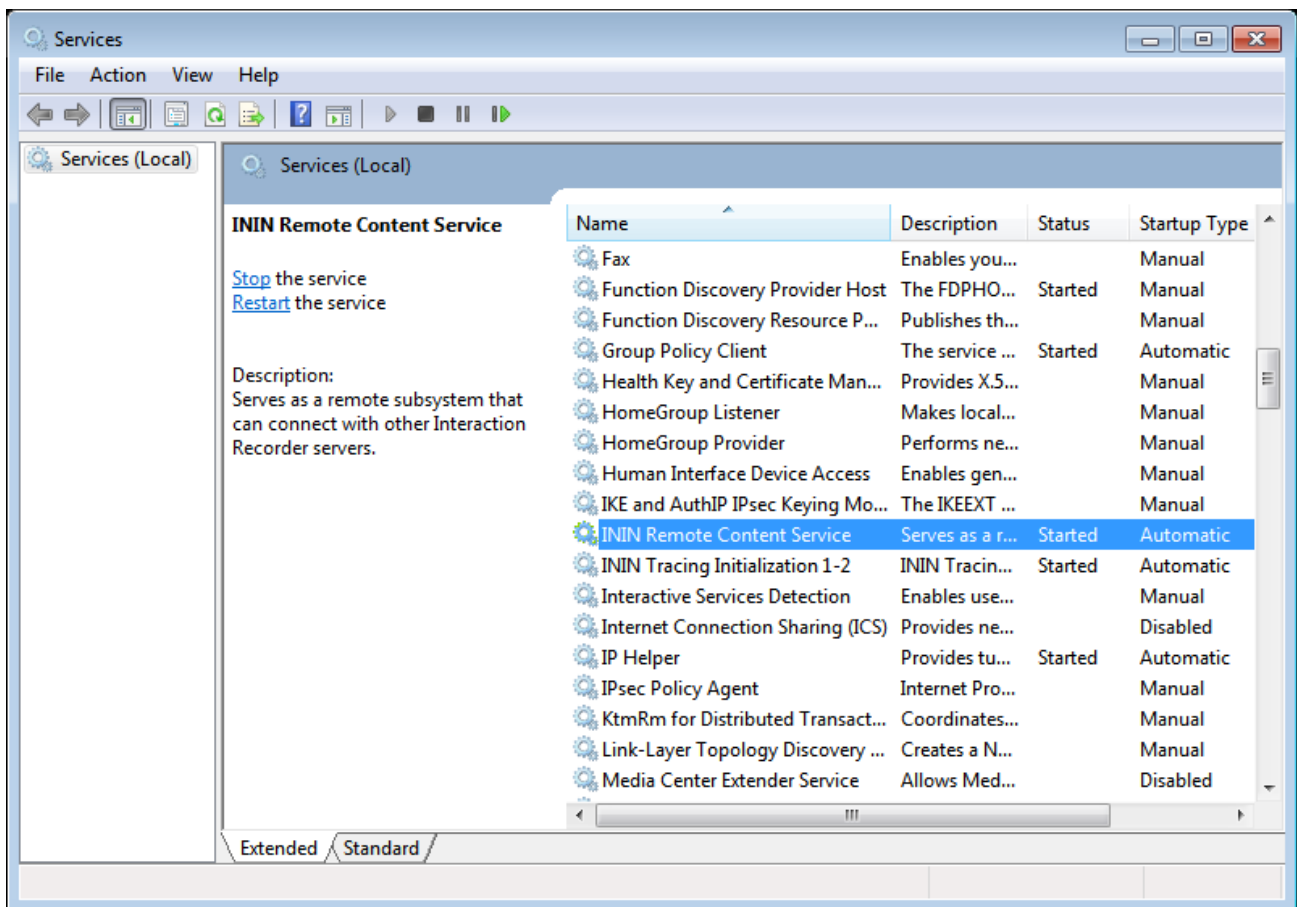
   Tip:
   Press **Win key+ R** to display the **Run** dialog box, type `services.msc` in the **Open** box, and then click **OK** to display the **Services** window.

5. Using the Interaction Administrator application, log on and connect to the CIC server.
6. In the navigation pane, click the **System Configuration** object.
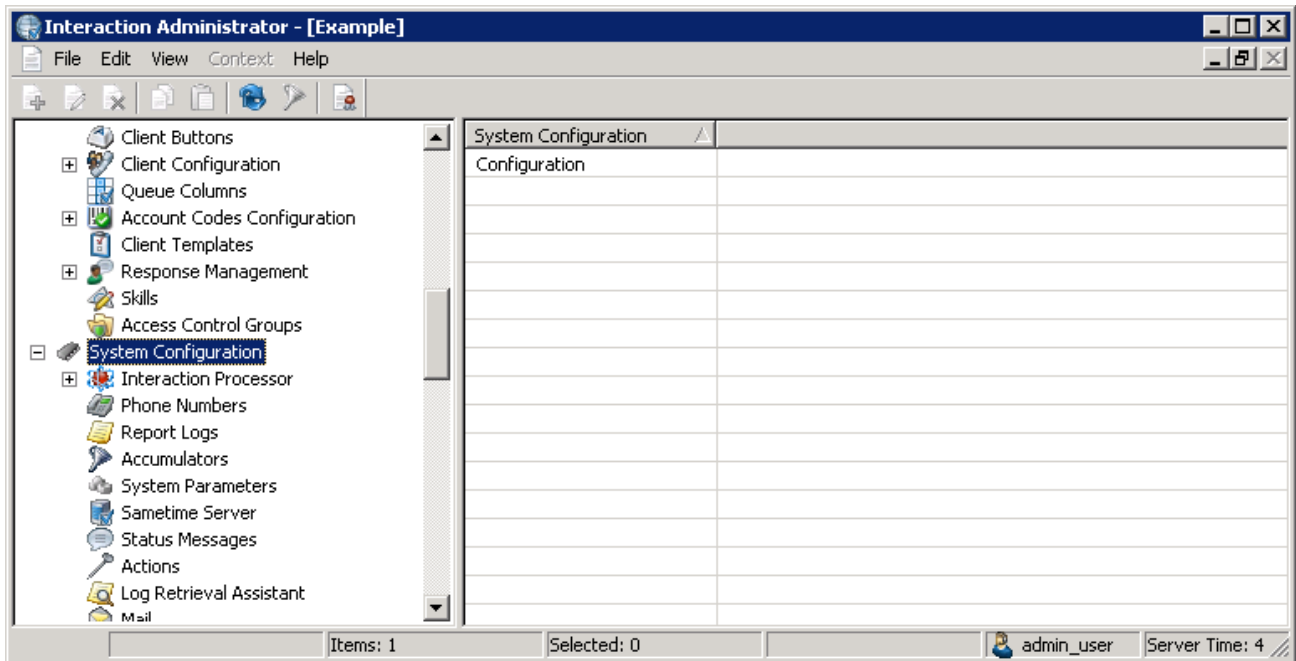
7. In the configuration pane, double-click the **Configuration** item. The **System Configuration** dialog box appears.
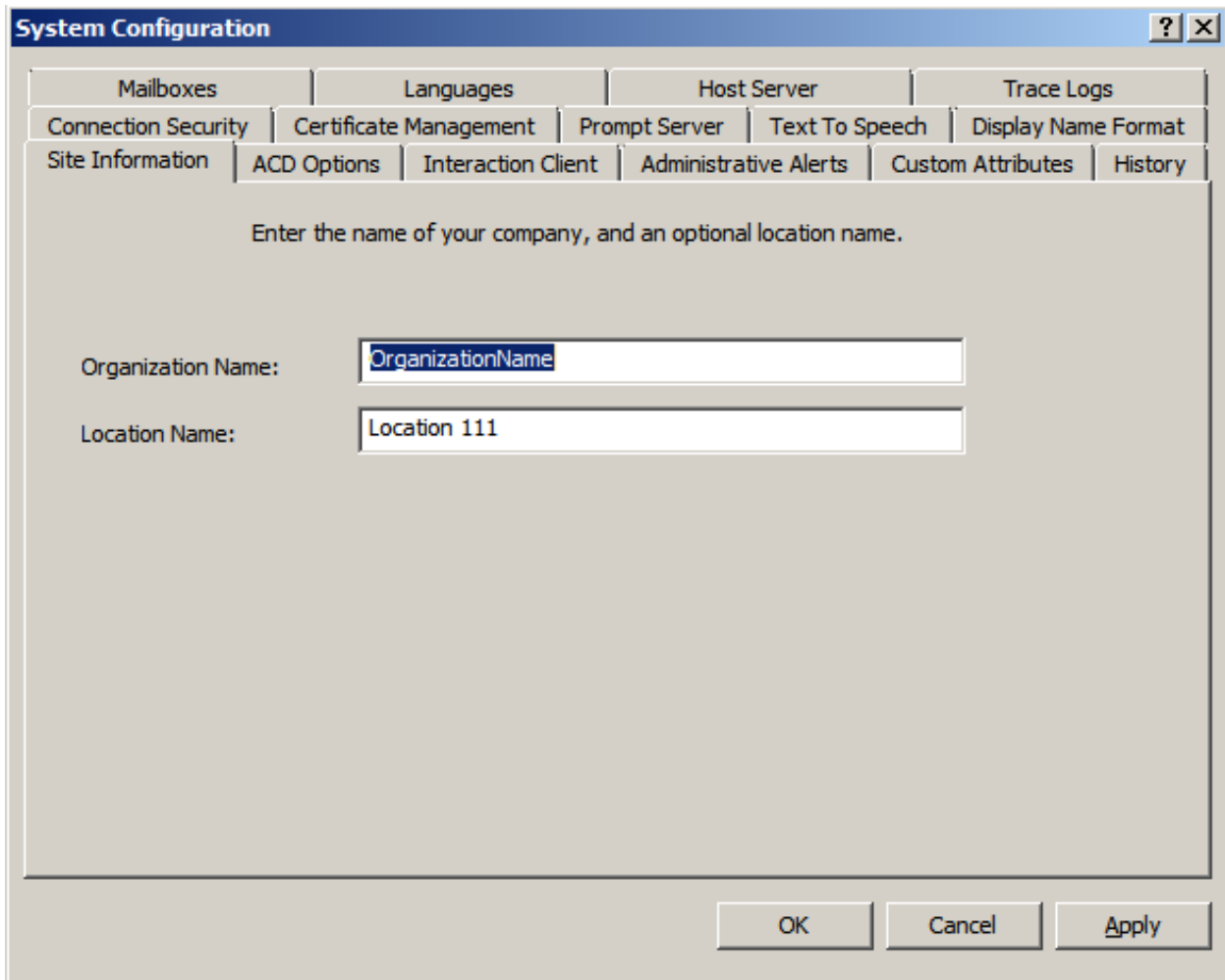
8. Click the **Certificate Management** tab.
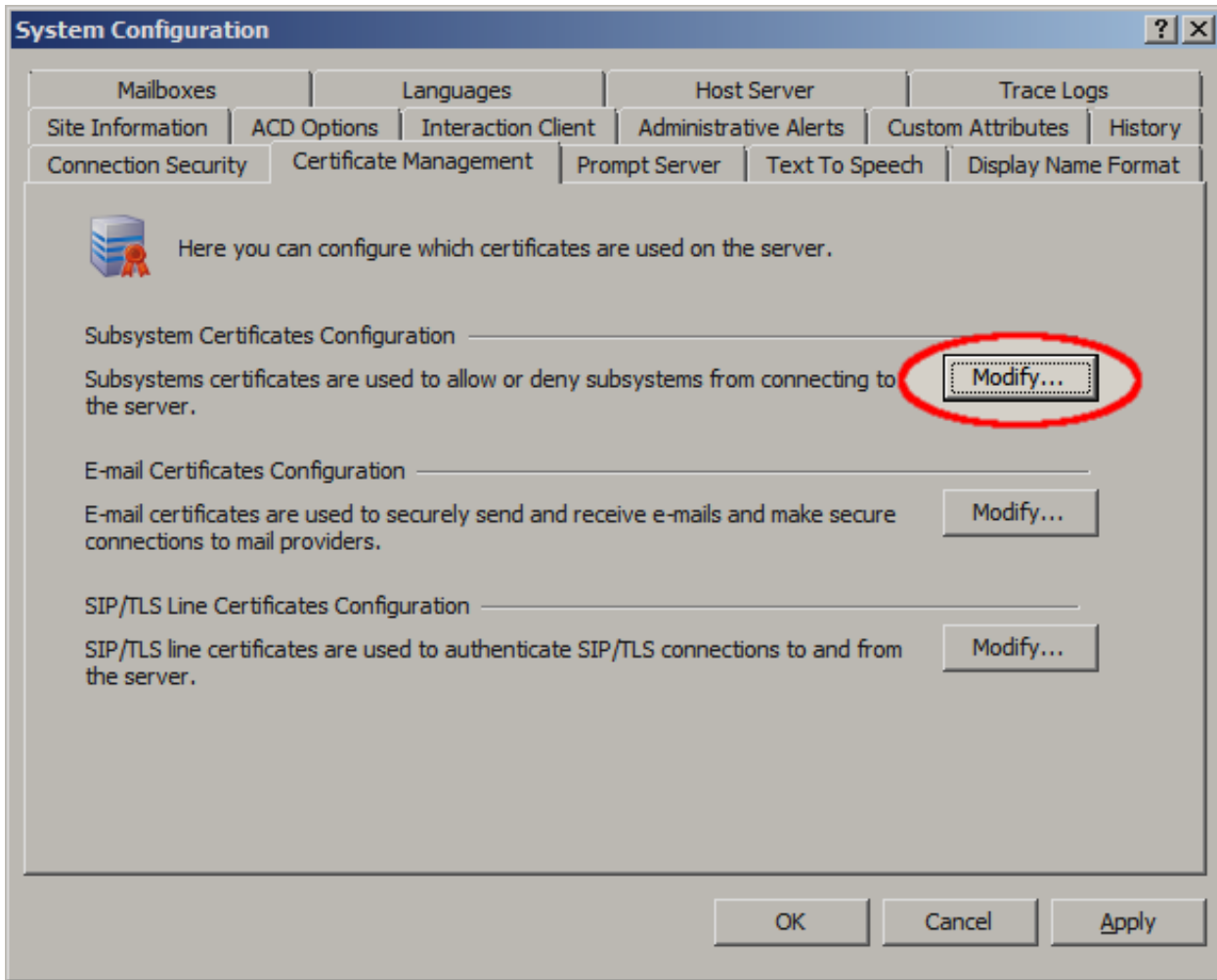
9. Under **Subsystem Certificates Configuration**, click **Modify**. The **Subsystem Certificates** dialog box appears with a **New** certificate from the Interaction Recorder Remote Content Service server.

Subsystem Certificates

You can choose which certificates are trusted and untrusted by the server. Subsystems with new or untrusted certificates will not be allowed to connect to the server until they are trusted.

Show: All Certificates

State	Date	Application	Description
New	2015-09-22 ...	EXMP - IC Certificate...	0C
New	2015-09-22 ...	EXMP - IC Certificate...	3876285235
Trusted		Setup Assistant	EXMP

Trust
Untrust
Delete
Refresh
Close
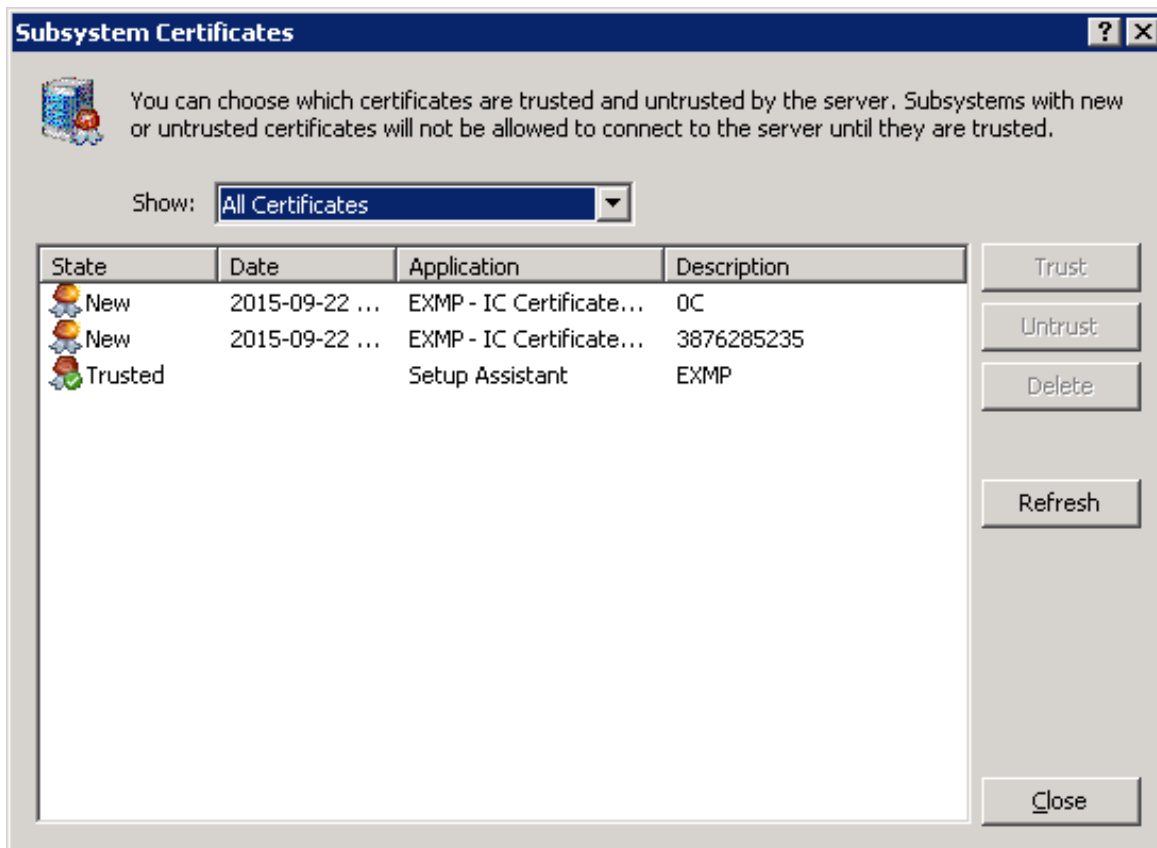
10. Click the new certificate and then click **Trust**. The certificate for Interaction Recorder Remote Content Service is now trusted and the two servers can communicate securely.

Create an HTTPS Certificate Signed by a Certificate Authority for Viewing Playback Recordings

To use Interaction Recorder Remote Content Service to serve content for recording playback in the My Quality Results view in Interaction Connect, ensure that the proper certificates are in place. If you do not use HTTPS and traffic only passes inside an intranet, the following recommendation does not apply. However, for safety, we recommend using HTTPS. When Interaction Connect uses HTTPS, the My Quality Results view requires Interaction Recorder Remote Content Service to pass playback information over HTTPS. To avoid certificate warnings in the web browser running Interaction Connect, use an HTTPS certificate signed by a third-party certificate authority (CA) for each Interaction Recorder Remote Content Service server.

The following instructions assume that you installed the Interaction Recorder Remote Content Service servers and connected them to the CIC server.

> **Notes:**
> - All certificates being generated need to use SHA-256.
> - You must regenerate Interaction Recorder Remote Content Service Certificates while doing these steps.
> - If certificates used SHA-1 previously, restart the RCS Server (not just the ININ Remote Content Service) to ensure that the old certificates clear out of cache properly.
> - After the reboot, ensure that the workstations using Interaction Connect have the FQDN_TrustedCertificate.cer (for example, RCS.Genesys.net_TrustedCertificate.cer) from the RCS in the HTTPS directory installed.
> - Install the certificate on the Local Machine under the Trusted Root Certification Authorities.

Generate a certificate signing request

Generating a certificate signing request creates a certificate signing request file and a private key file. You send the certificate signing request file to a CA for signing. Save the private key file. Otherwise, you must regenerate the signing request and request that the CA sign the certificate again. Use the GenSSLCertsU.exe command-line utility to generate the certificate signing request.

To generate a certificate signing request

From the Interaction Recorder Remote Content Service server, run the following command on the command line:

> **GenSSLCertsU.exe -g HTTPS**

> **Note**: If you issued a signing request already, run the command **GenSSLCertsU.exe -g HTTPS -f** to back up the existing certificate signing requests and generate a new one.

For more information, see "Generating Certificates Manually with GenSSLCertsU" in the *PureConnect Security Features Technical Reference* at https://help.genesys.com/pureconnect/secure/download.aspx?path=/Service%20Updates/doc/pureconnect/Security_Features_TR.pdf. You must have the appropriate logon credentials to view this document.

Import a signed certificate

After the CA signs the certificate, import the certificate for use in the Interaction Recorder Remote Content Service. Ensure that the private key file from the previous step, the signed certificate from the CA, and the Chain of Trust CA certificate exist in a known place on the Interaction Recorder Remote Content Service server.

> **Important!**
> The HTTPS certificate signed by a CA must use x509 in PEM format. The Chain of Trust certificate must use PEM format.

To import a signed certificate

From the Interaction Recorder Remote Content Service server, run the following command on the command line:

> **GenSSLCertsU.exe -i HTTPS <signed certificate file path> <private key file path> <Chain of Trust certificate file path> -f**

> **Note**: **-f** is required to back up any existing HTTPS certificate (for example, installation creates an HTTPS certificate automatically) before you import the new certificate.

Troubleshooting Interaction Recorder Remote Content Service

Following are solutions and answers regarding specific problems with Interaction Recorder Remote Content Service.

Recordings are not being processed

Ensure that the following conditions are met:

- Interaction Recorder Remote Content Service is listed as a trusted source on the CIC server.
- One or more Interaction Recorder Remote Content Service instances are active. Confirm this state through the **Interaction Recorder** > **Remote Content Server** object in Interaction Administrator.
- Each instance of Interaction Recorder Remote Content Service is configured to support enough connections. Edit the configuration file to change the allowed number of connections. For more information, see Interaction Recorder Remote Content Service Configuration File.
- The network resource or local directory for recording storage specified in the retention policy exists.
- The user ID that Interaction Recorder Remote Content Service uses to access the recording storage location has the proper permissions.
- The following Interaction Media Server properties are set to existing directories or network locations: **ResourceBaseUriLocal**

Recording playback processed by Interaction Recorder Remote Content Service servers in wrong regions

If you are playing recordings and an Interaction Recorder Remote Content Service in another location is selected over an Interaction Recorder Remote Content Service instance in the same location where the recording is stored, ensure that the following conditions are met.

- The network connection to the Interaction Recorder Remote Content Service server is not burdened by other traffic.
- The Interaction Recorder Remote Content Service is started on the server.
- The Interaction Recorder Remote Content Service server has a trusted certificate on the CIC server.
- In Interaction Administrator, the intended Interaction Recorder Remote Control Service instance is indicated as **Active**.
- Each instance of Interaction Recorder Remote Content Service is configured to support enough connections. If necessary, edit the configuration file and increase the allowed number of connections. For more information about the configuration file, see Interaction Recorder Remote Content Service Configuration File.
- The Interaction Recorder Remote Control Service that you want to playback recordings in a specific region must have access permissions and network access to the storage location of the recording.

Change Log

The following table lists the changes to the *Interaction Recorder Remote Content Service Installation and Configuration Guide* since its initial release.

Date	Changes
04-November-2011	Initial release
06-March-2012	IC-93830 - The Interaction Recorder 4.0 Remote Content Service documentation needs to discuss screen recordings
19-March-2012	IC-85502 - Correct documentation errors
30-September-2013	IC-111478 - Add procedure for trusting the Interaction Recorder Remote Content Service certificate through Interaction Administration during initial configuration
21-March-2014	- IC-112785 - Corrected installation procedure to prompt only for fully-qualified domain name when specifying an Interaction Center server - IC-114319 - Added content to support new feature for CaaS customers to use an alternative fully-qualified domain name for retrieving and playing recordings through Interaction Recorder - Added content for new feature to disable transfer of screen recordings from Interaction Media Server - Updated copyright and trademark page
23-May-2014	DP-357 - Recorder Reliability - Remote Content Server Functionality Work (Server selection rules)
01-August-2014	- Added corrections and clarification to content regarding Server Selection Rules feature - Miscellaneous edits for clarification and organization
14-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 Interactive Intelligence Product Information site URLs, and copyright and trademark information.
26-January-2015	- Updated legal page - Added content for exporting recordings as e-mail attachments
10-April-2015	Updated formatting for new corporate standards
02-October-2015	- Updated images to reflect new corporate branding - IC-131736 - Updated content to reflect maximum maxconnection setting change from 16 to 64
22-March-2018	Rebranded to Genesys.
26-April-2018	Updated requirements. Added topic "Create an HTTPS certificate signed by a certificate authority for viewing playback recordings".
04-October-2018	Update KB link in Install Interaction Recorder Remote Content Service section.
30-April-2019	Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section...".
07-October-2019	Adding information about the certificate signing method check box that appears for new installations.
01-April-2020	Changed path to *Security Features Technical Reference* in Create an HTTPS Certificate Signed by a Certificate Authority for Viewing Playback.
22-June-2020	Added notes to Create an HTTPS Certificate Signed by a Certificate Authority for Viewing Playback.

OpenSSL Copyright

LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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