



**PureConnect®**

**2018 R5**

Generated:

12-November-2018

Content last updated:

26-April-2018

See [Change Log](#) for summary of changes.



# 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/cic>.

For copyright and trademark information, see [https://help.genesys.com/cic/desktop/copyright\\_and\\_trademark\\_information.htm](https://help.genesys.com/cic/desktop/copyright_and_trademark_information.htm).

# Table of Contents

Table of Contents	2
Interaction Recorder Remote Content Service overview	3
Record interactions without Interaction Recorder Remote Content Service	4
Record interactions with Interaction Recorder Remote Content Service	5
Interaction Recorder Remote Content Service features	6
Interaction Recorder Client playback	6
Export recordings through Interaction Recorder Remote Content Service	7
Interaction Recorder Remote Content Service co-residence with Interaction Media Server	7
Interaction Recorder Remote Content Service screen recordings	7
Sending Recordings as e-mail attachments	7
Network Configurations	8
Remote contact center with Interaction Recorder Remote Content Service	8
Multiple Remote Contact Centers with Multiple Servers	9
Location assignments and Server Selection Rules	9
Location assignments	10
Server selection rules	10
Selection rule location variables	10
Deployment examples	10
Overall server selection process	13
Recording retrieval process	14
Interaction Recorder Remote Content Service installation	15
Interaction Recorder Remote Content Service prerequisites	15
Interaction Recorder Remote Content Service requirements	15
Install Interaction Recorder Remote Content Service	15
Uninstall Interaction Recorder Remote Content Service	22
Configure Interaction Recorder Remote Content Service	23
Trust the Interaction Recorder Remote Content Service connection in Interaction Administrator	23
Configure Interaction Recorder Remote Content Service through Interaction Administrator	26
Configure Interaction Recorder Remote Content Service selection rules	27
Interaction Recorder Remote Content Service configuration file	30
Regenerate Interaction Recorder Remote Content Service certificates	30
Create an HTTPS certificate signed by a certificate authority for viewing playback recordings	35
Generate a certificate signing request	35
Import a signed certificate for use in Interaction Recorder Remote Content Service	35
Troubleshooting Interaction Recorder Remote Content Service	36
Recordings are not being processed	36
Recording playback processed by Interaction Recorder Remote Content Service servers in wrong regions	36
Change Log	37
OpenSSL Copyright	38
Copyright and Trademark Information	40

# Interaction Recorder Remote Content Service overview

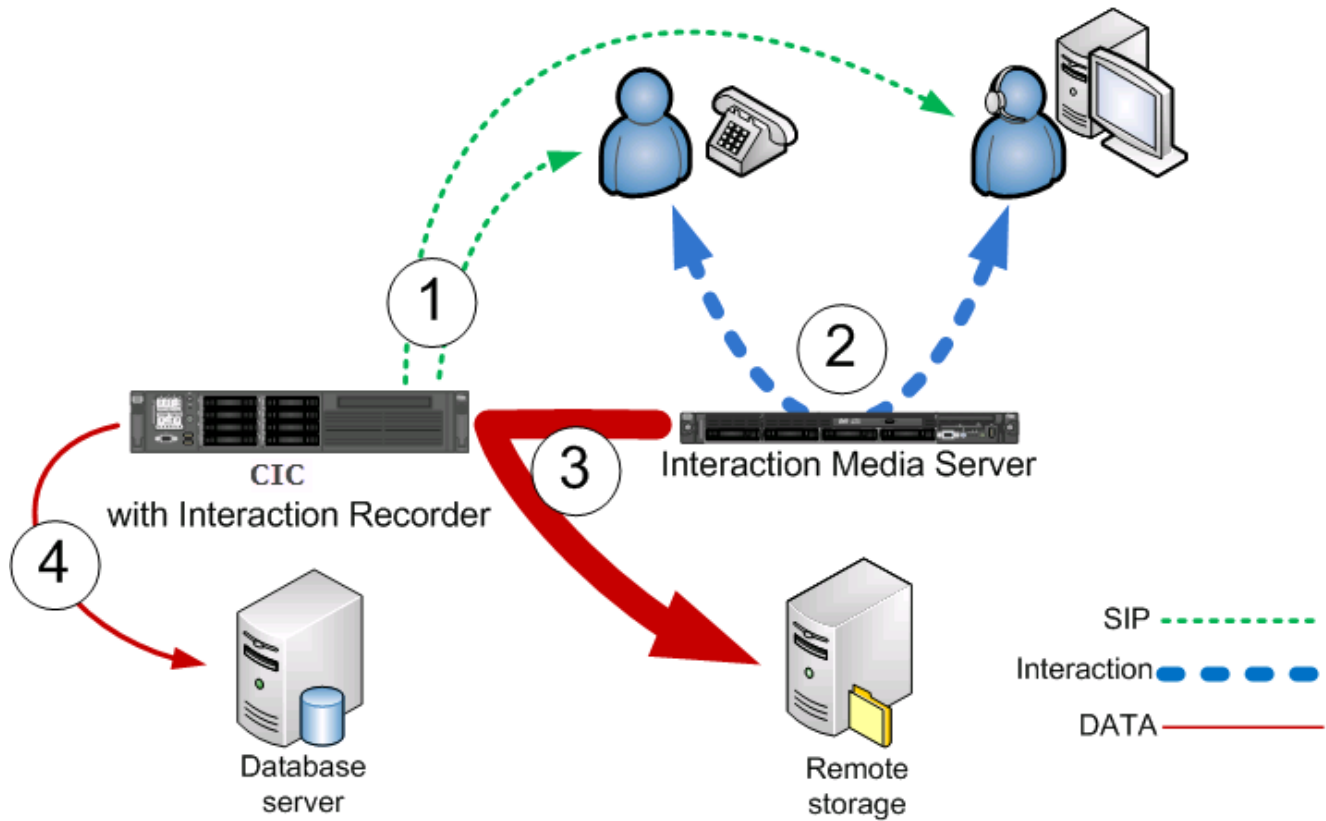
In PureConnect, there are three phases to making a recording:

- 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 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 Customer Interaction Center server thereby granting that server more processing and bandwidth resources for facilitating and handling interactions.

# Record interactions without Interaction Recorder Remote Content Service

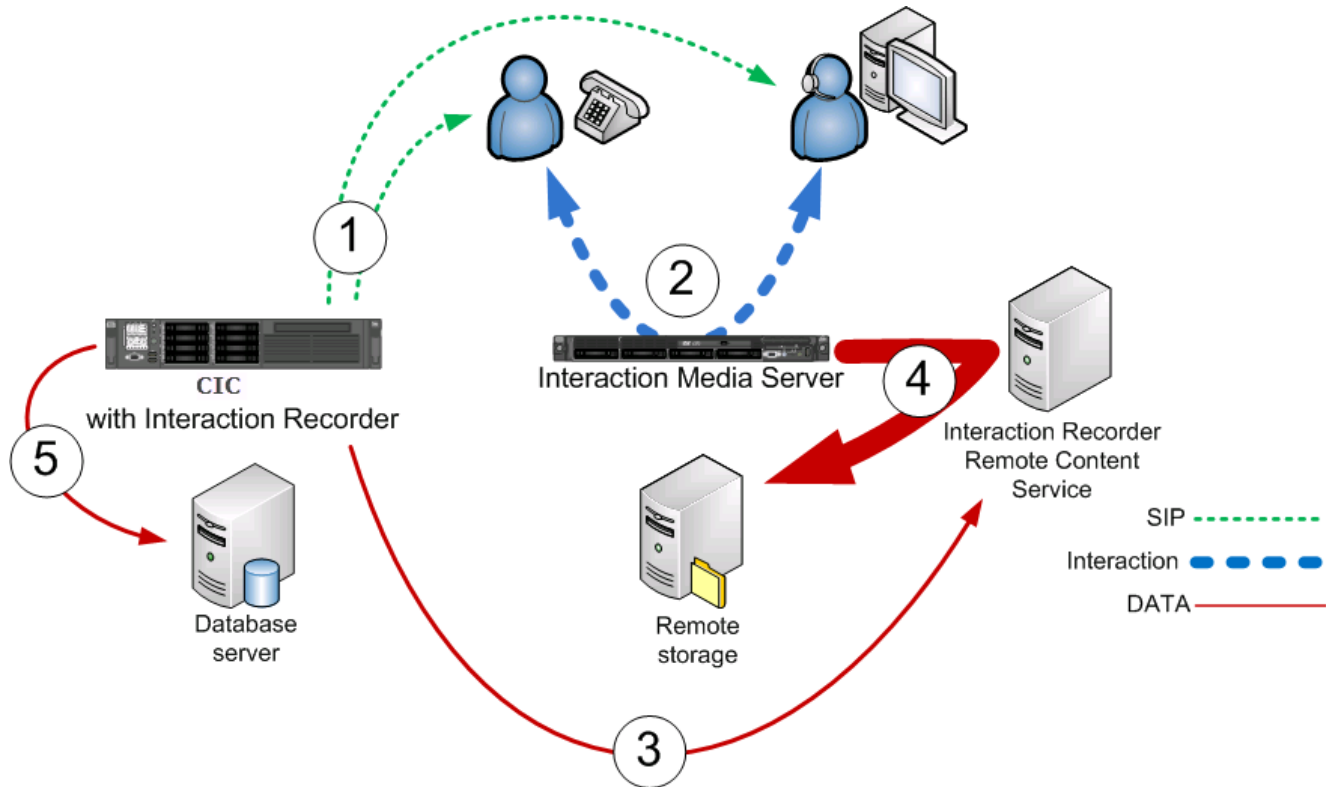
The following diagram displays the process of recording interactions without Interaction Recorder Remote Content Service:



Step	Description
1	Customer Interaction Center 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 Customer Interaction Center 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	Customer Interaction Center facilitates an interaction between a customer and an agent.
2	Interaction Media Server records, compresses, and encrypts the interaction.
3	Based on <i>Selection Rules</i> , the Customer Interaction Center 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.

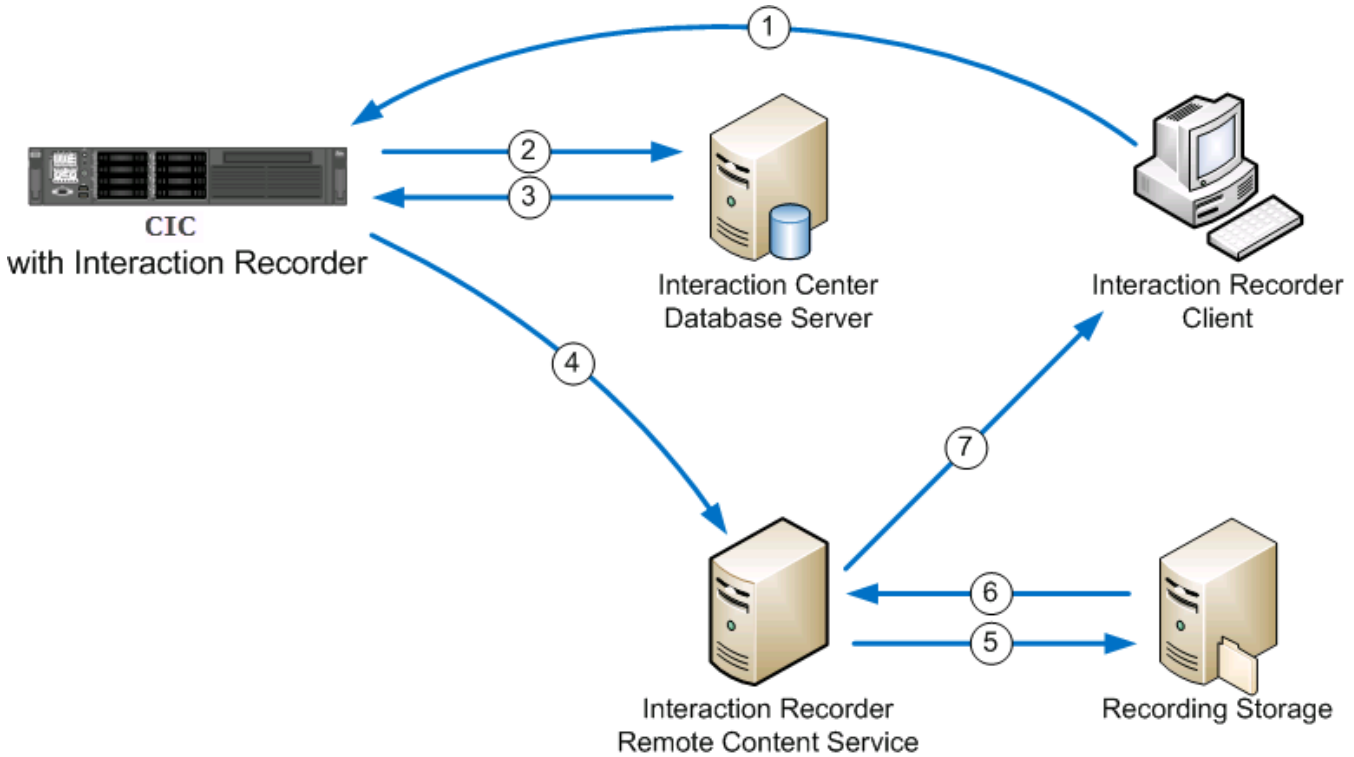
# Interaction Recorder Remote Content Service features

This topic provides 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 Customer Interaction Center server.
2	Interaction Recorder looks up the specified recording in the database.
3	The Customer Interaction Center 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 Customer Interaction Center 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 Customer Interaction Center 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. Customer Interaction Center 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 Customer Interaction Center 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.

## Sending Recordings as e-mail attachments

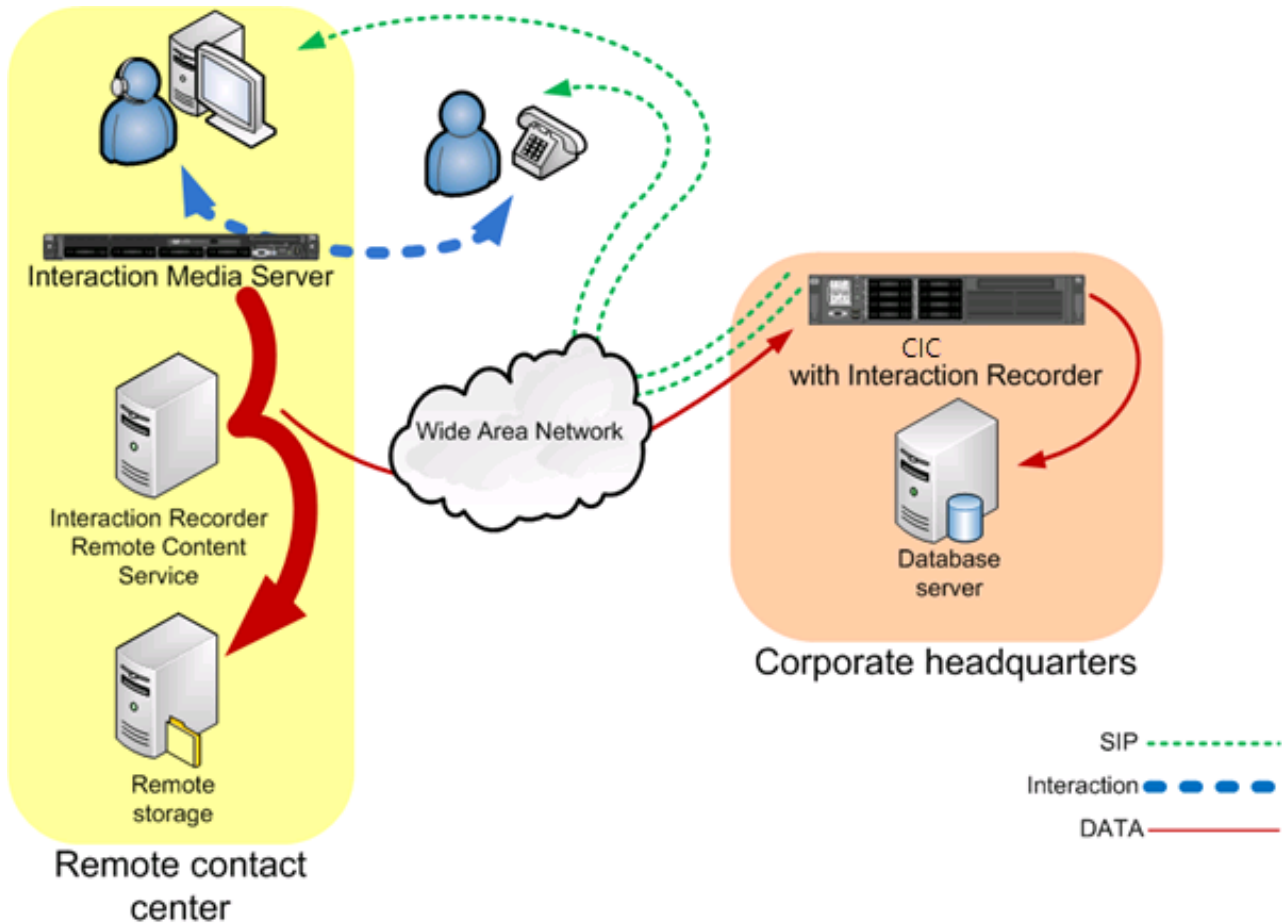
Through Interaction Recorder Client, you can send one or more recordings as an e-mail attachment. Interaction Recorder Remote Content Service decrypts the recording and then attaches that recording to the e-mail, which is sent through PostOffice Server on the Customer Interaction Center server. Once 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

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.



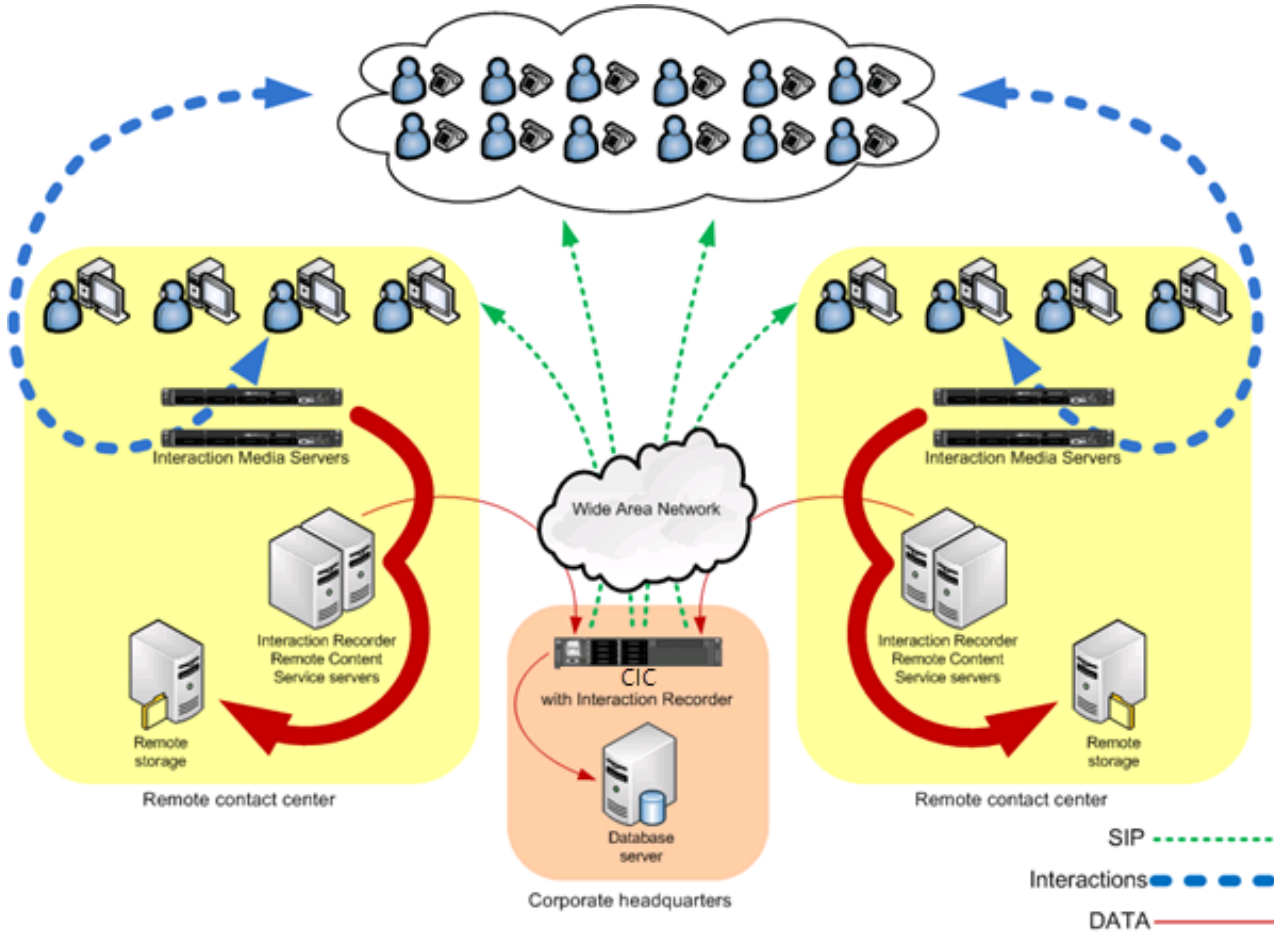
The following list provides the benefits for using Interaction Recorder Remote Content Service in this type of configuration:

- 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 unforeseen hardware failures.

**Note:** If you add 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 on 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.

---

## 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 and 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.

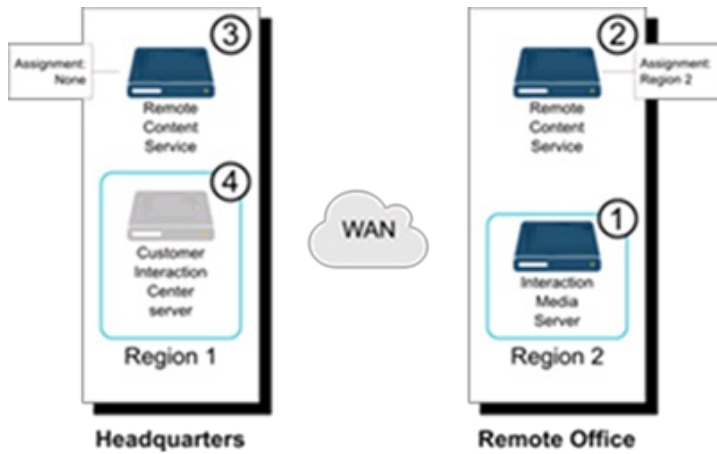
CIC supports the following location variables for Interaction Recorder Remote Content Service in server selection rules.

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. <b>Note:</b> The <IC Server Location> variable indicates only the location 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:

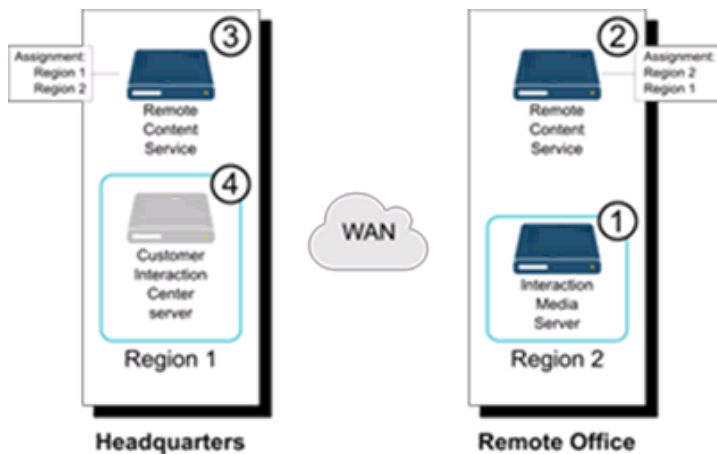
<This Location>  
<IC Server Location>

**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

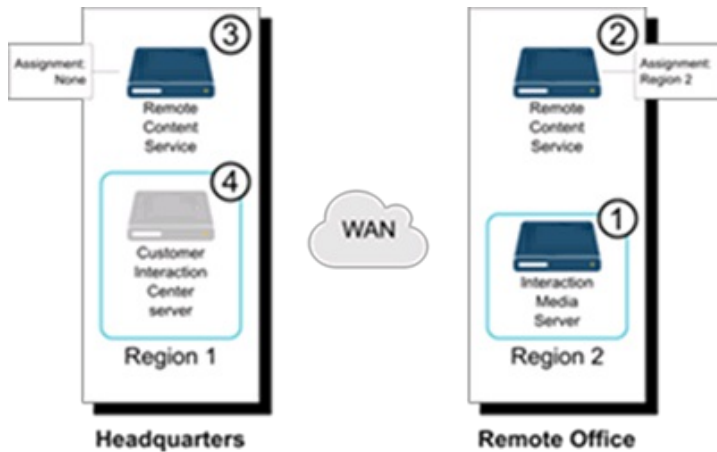
#### Selection rule:

<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

Selection rule:

<This Location>  
<IC Server Location>

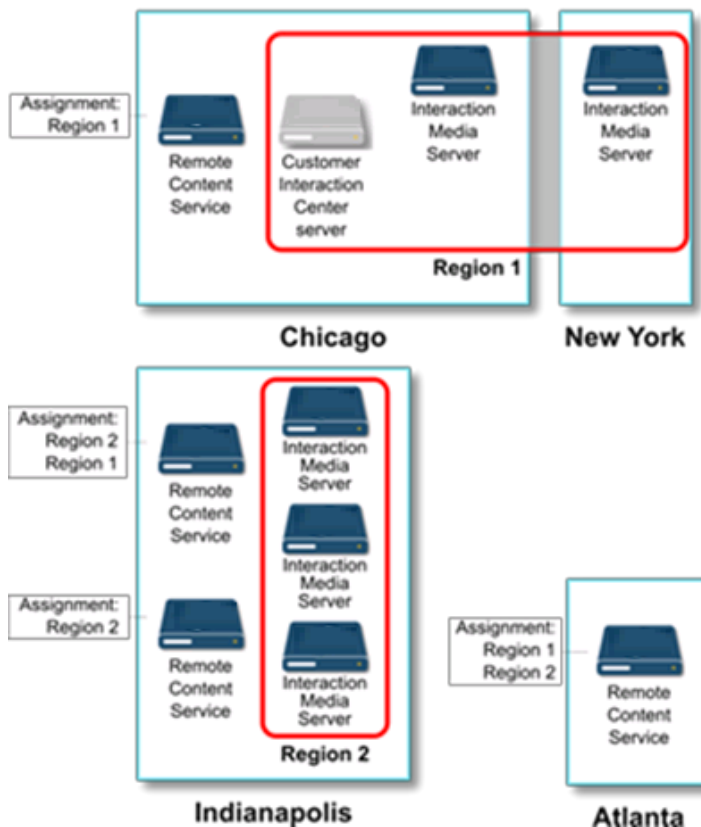
**Use any Location** option enabled

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. 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>

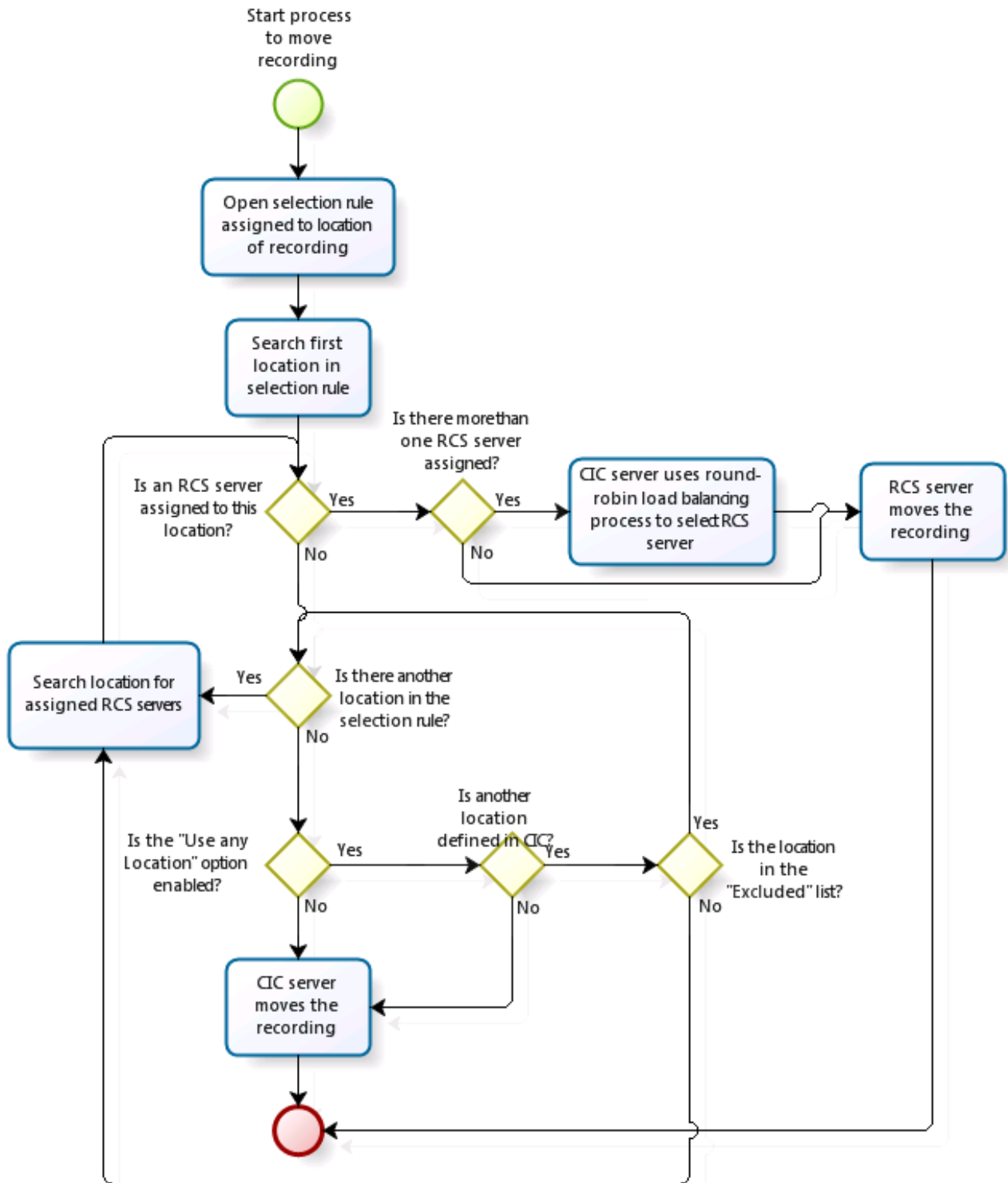
**Use any Location** option enabled

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

This section contains the prerequisites, requirements, and the procedures for installing and uninstalling Interaction Recorder Remote Content Service.

## Interaction Recorder Remote Content Service prerequisites

The following list provides 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 Customer Interaction Center server. Interaction Recorder Remote Content Service is backwards compatible with Customer Interaction Center servers of previous version.

## Interaction Recorder Remote Content Service requirements

The following list provides the minimum requirements for installing and using Interaction Recorder Remote Content Service:

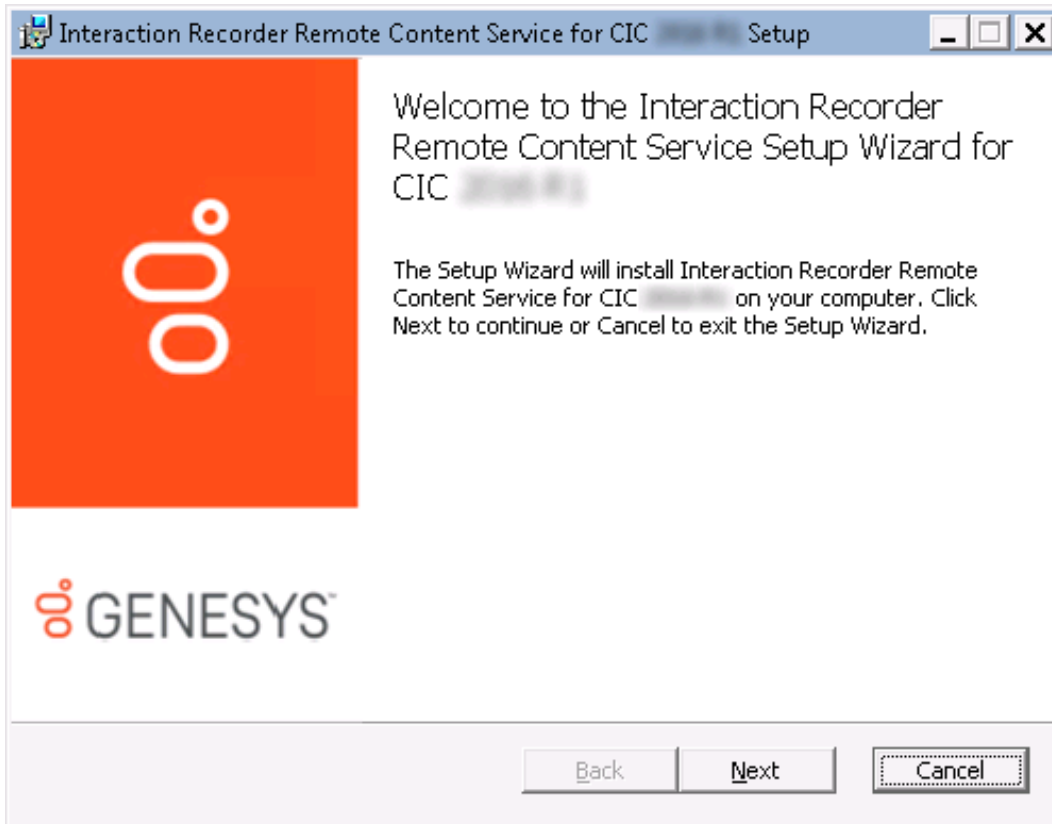
Operating system	<ul style="list-style-type: none"><li>• Microsoft Windows Server 2016</li><li>• Microsoft Windows Server 2012 R2</li></ul>
CPU	Intel Xeon, 2.4 GHz
Media drive	DVD-ROM drive
Hard drive	<ul style="list-style-type: none"><li>• 346 MB of free space</li><li>• 7200 rpm or higher</li></ul>
Memory	4 GB
Network Interface Card	Gigabit Ethernet
Software	<ul style="list-style-type: none"><li>• Customer Interaction Center 20nn Rn on another server in the network</li><li>• Interaction Media Server 20nn Rn on another server in the network</li><li>• Microsoft .NET Framework 3.0 or greater</li></ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"><b>Important!</b> 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.</div>

## 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-Customer Interaction Center 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, navigate to the `\Installs\Off-ServerComponents` directory.
3. Copy the `IRRemoteContentService_20nnRn.msi` file to the machine on which you will install Interaction Recorder Remote Content Service.
4. Execute the `IRRemoteContentServer.msi` file.

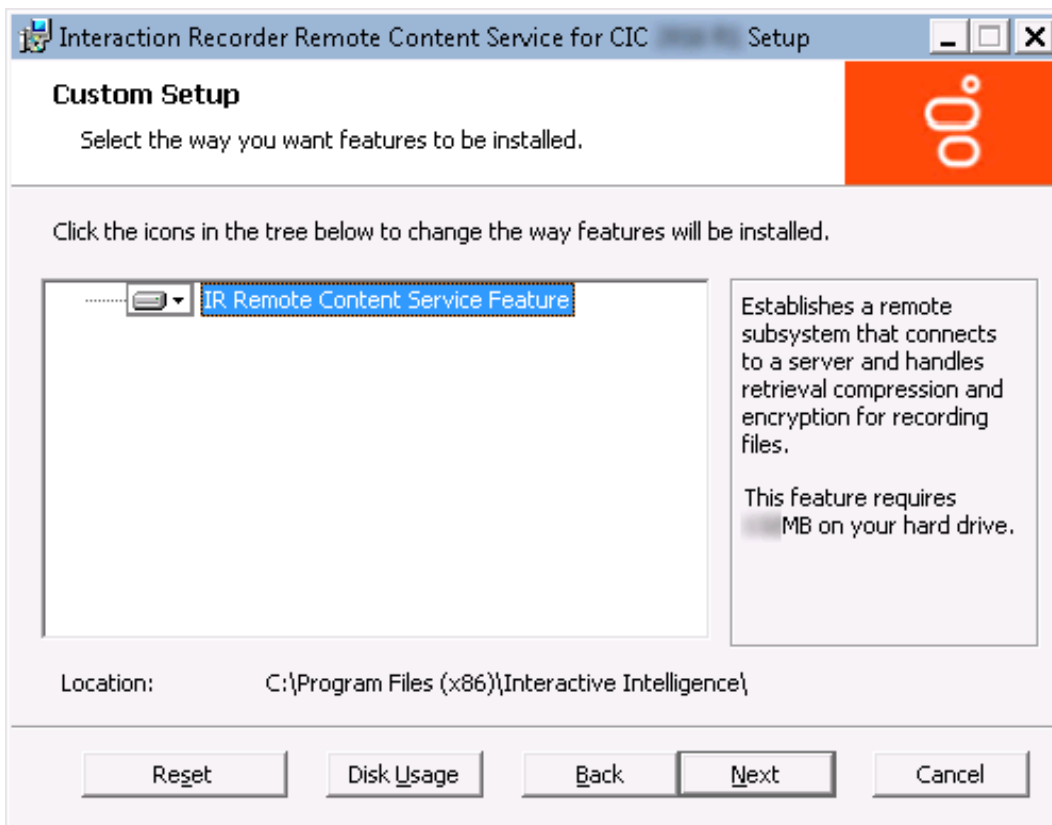
5. Depending on your security settings, you may receive **Security Warning** dialog box. If this dialog box is displayed, select the **Run** button.

The **Interaction Recorder Remote Content Service for CIC Setup** dialog box appears.



6. Select the **Next** button.

The **Custom Setup** dialog box appears.





- If you want to choose a different installation location, select the **Browse** button and select a different directory. If not, select the **Next** button.

**Note:**

You must ensure that the hard disk drive has enough free space to install the software. Select the **Disk Usage** button and, in the resulting dialog box, verify that you have at least 350 megabytes of free space.

**Note:**

By default, the PureConnect QoS driver will be silently installed and the certificate will be added to the Trusted Publishers list. If your site has reasons to modify this default behavior, see KB article [Q131006915300479](#) and follow the instructions provided 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.

The **IR Remote Content Service Connection** dialog box appears.

Interaction Recorder Remote Content Service Setup

### IR Remote Content Service Connection

Configure the parameters needed to establish a connection to a server

Please specify the maximum number of connections as well as the port to which a connection to the IC Server will be established.

Maximum Connections:  
(Maximum: 64)

Remote Host Port:

Back Next Cancel

- In the **Maximum Connections** text box, enter 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](#).

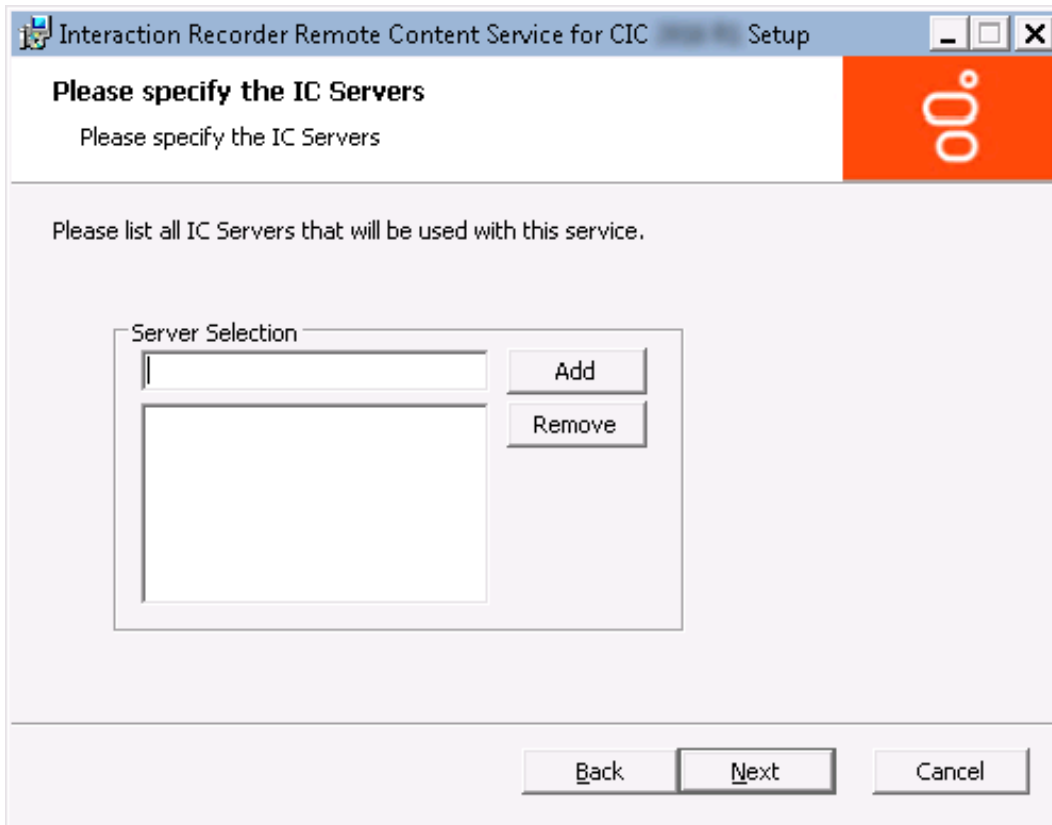
- In the **Remote Host Port** text box, enter the port number on this server that Interaction Recorder Remote Content Service will use for inbound communications from Interaction Recorder, Interaction Recorder Client, and Interaction Media Server.

**Important!**

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

- Select the **Next** button.

The **Please specify the IC Servers** dialog box appears.



11. In the **Server Selection** text box, enter the fully-qualified domain name of a Customer Interaction Center server that will communicate with Interaction Recorder Remote Content Service and then select the **Add** button.  
Genesys recommends that you do not use an IP address to specify the Customer Interaction Center server as it will cause certificate authentication to fail.

**Note:**

If you have a fallback Customer Interaction Center server, you should also enter it in the **Server Selection** field.

If you add an erroneous entry, highlight that entry and select the **Remove** button.

12. If necessary, repeat the previous step for any additional Customer Interaction Center servers that you want to connect with this Interaction Recorder Remote Content Service server. When you have finished adding Customer Interaction Center servers, select the **Next** button.

The **Domain User Validation** dialog box appears.

Interaction Recorder Remote Content Service for CIC Setup

### Domain User Validation

Enter the user name, password and domain name.

Please enter the credentials for a user account with administrative privileges on this system. This account will register components and services to run in the context of account specified.

User:

Password:

Domain:

13. In the **Password** text box, enter the password of the currently logged in user and select the **Next** button.

**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.

The **Interaction Center Server and Credentials** dialog box appears.

Interaction Recorder Remote Content Service for CIC Setup

### Interaction Center Server and Credentials

Enter the server name.

IC Server:

Use IC Credentials To Login To IC Server.

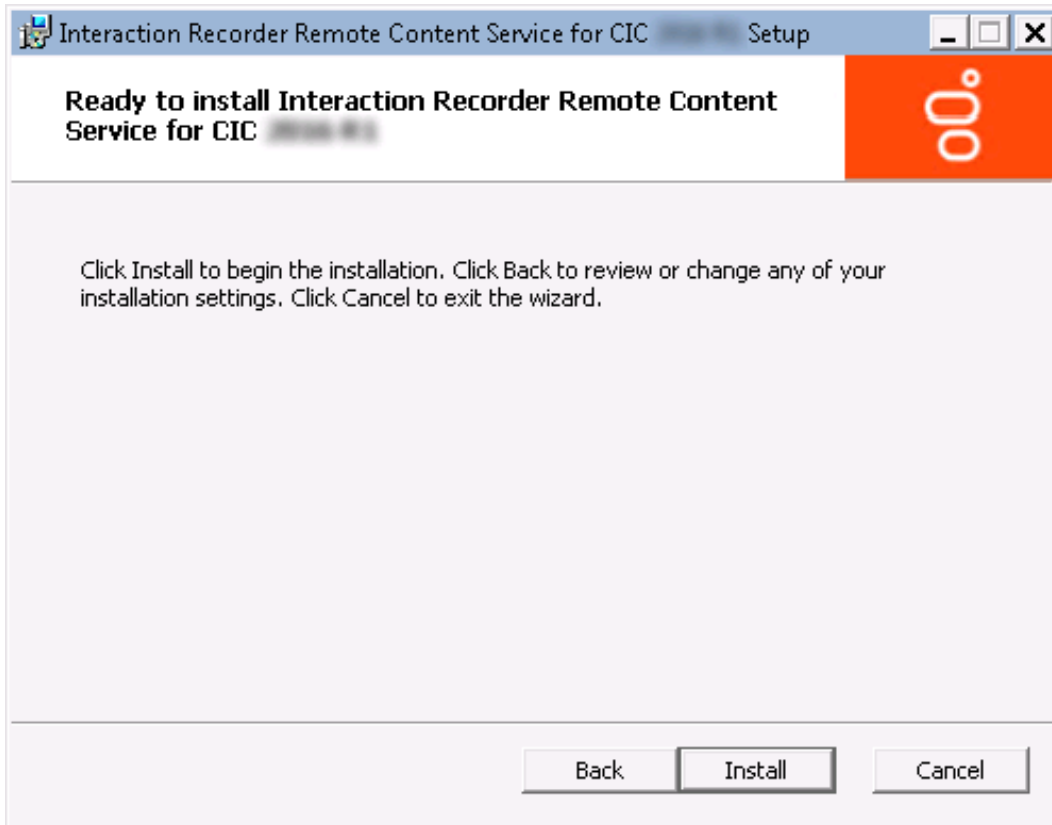
Use IC credentials to establish a connection to the IC server. The Account must already exist. Use this option in an environment where the IC Server is in another Domain and a Trust Relationship does not exist.

User:

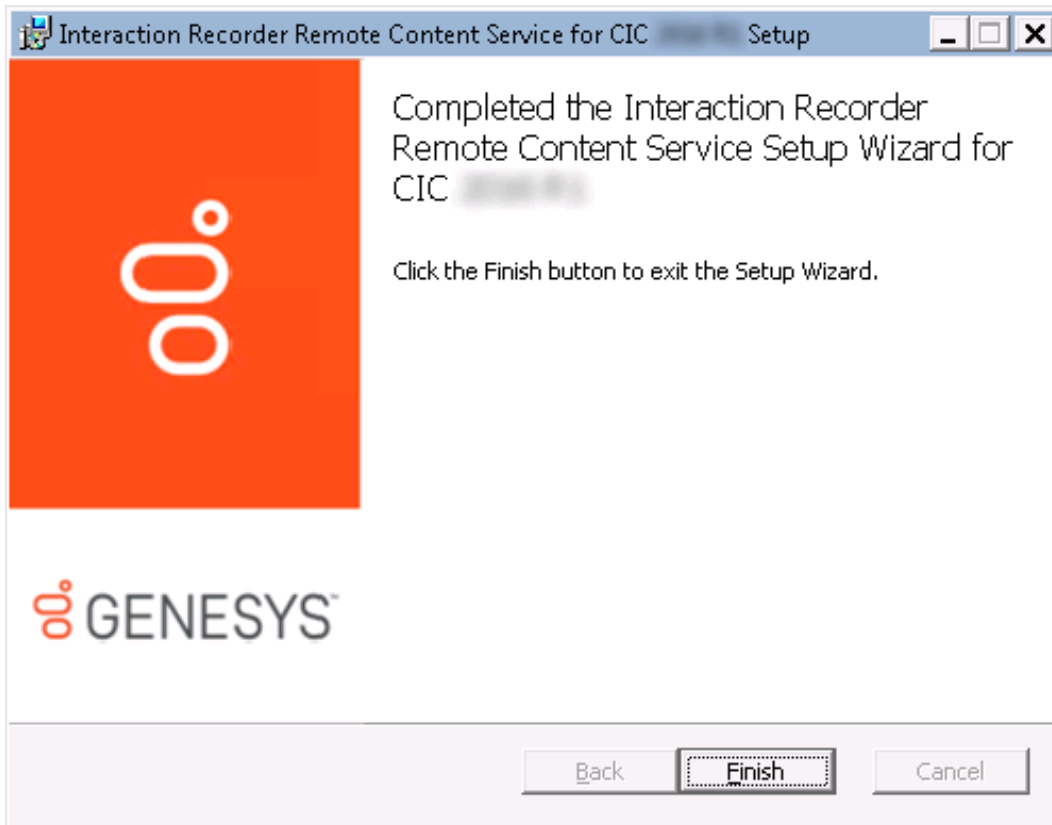
Password:

14. In the **IC Server** text box, enter the fully-qualified domain name for the main Customer Interaction Center server and then select the **Next** button.  
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 Customer Interaction Center server as it will cause certificate authentication to fail.
15. If the Customer Interaction Center server resides in a different domain than the machine on which you are installing Interaction Recorder Remote Content Service, place a check mark in the **Use IC Credentials To Login To IC Server** check box.
16. In the **User** and **Password** text boxes, supply the credentials of a defined Customer Interaction Center server administrator.
17. Select the **Next** button.

The **Ready to install Interaction Recorder Remote Content Service** dialog box appears.



18. Select the **Install** button.  
The **Installing Interaction Recorder Remote Content Service** dialog box appears and provides the status of the installation process. When the installation process is finished, the following dialog box appears:



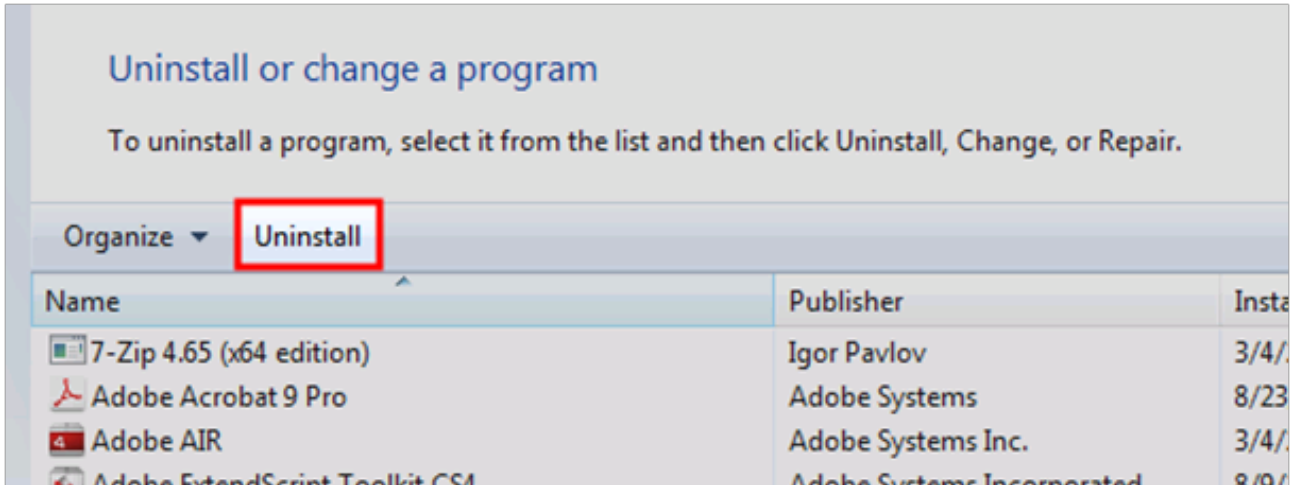
19. Select the **Finish** button.

You have successfully completed the installation of Interaction Recorder Remote Content Service.

## Uninstall Interaction Recorder Remote Content Service

If you need to uninstall Interaction Recorder Remote Content Service, do the following steps:

1. Using an administrative user account, log on to the Windows host where Interaction Recorder Remote Content Service is installed.
2. Select **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, locate **Interaction Recorder Remote Content Service** and select it with a single click.
5. Select the **Uninstall** link at the top of the list.



A **Programs and Features** message box is displayed, which asks you if you want to uninstall Interaction Recorder Remote Content Service.

6. In the message box, select the **Yes** button.
7. Wait while Windows uninstalls Interaction Recorder Remote Content Service.

Interaction Recorder Remote Content Service is removed from your system.

# Configure Interaction Recorder Remote Content Service

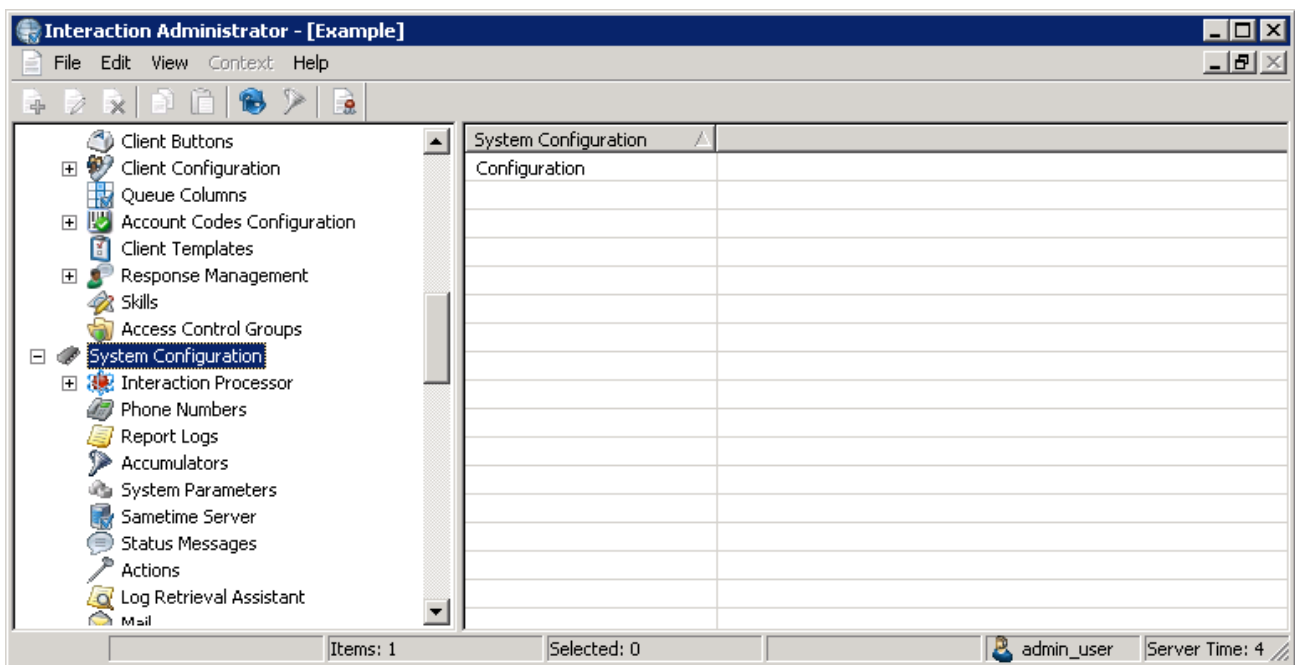
This section contains information about the configuration of Interaction Recorder Remote Content Service and presents the following topics:

- [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](#)

## Trust the Interaction Recorder Remote Content Service connection in Interaction Administrator

Interaction Recorder Remote Content Service generates a certificate automatically for connecting to a Customer Interaction Center 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.

1. Open Interaction Administrator and, if necessary, log on as a Customer Interaction Center administrator user.
2. In the left pane of the **Interaction Administrator** window, select the **System Configuration** object with a single click.



3. In the right pane, double-click the **Configuration** item.  
The **System Configuration** dialog box appears.

**System Configuration** [?] [X]

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.

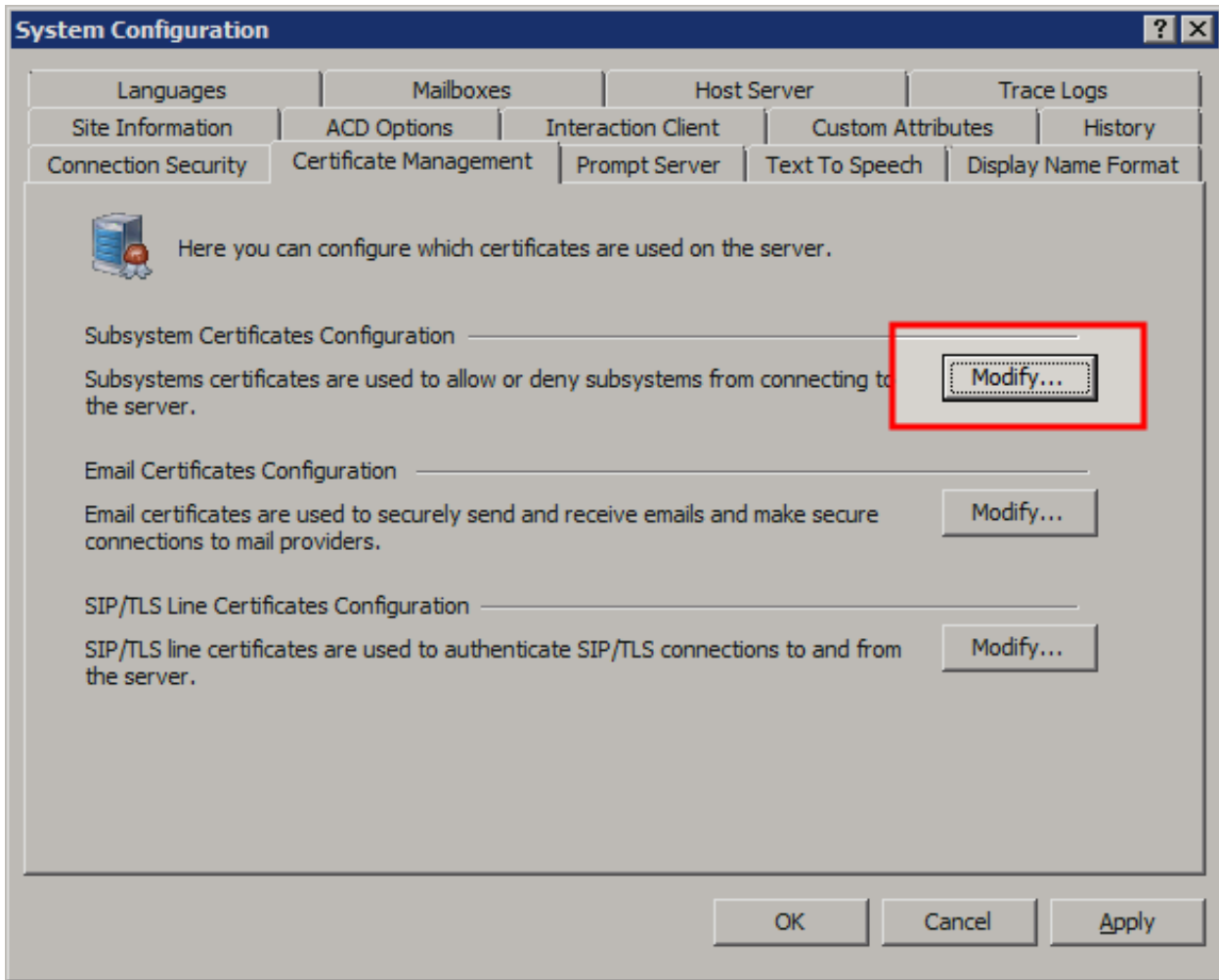
Organization Name:

Location Name:

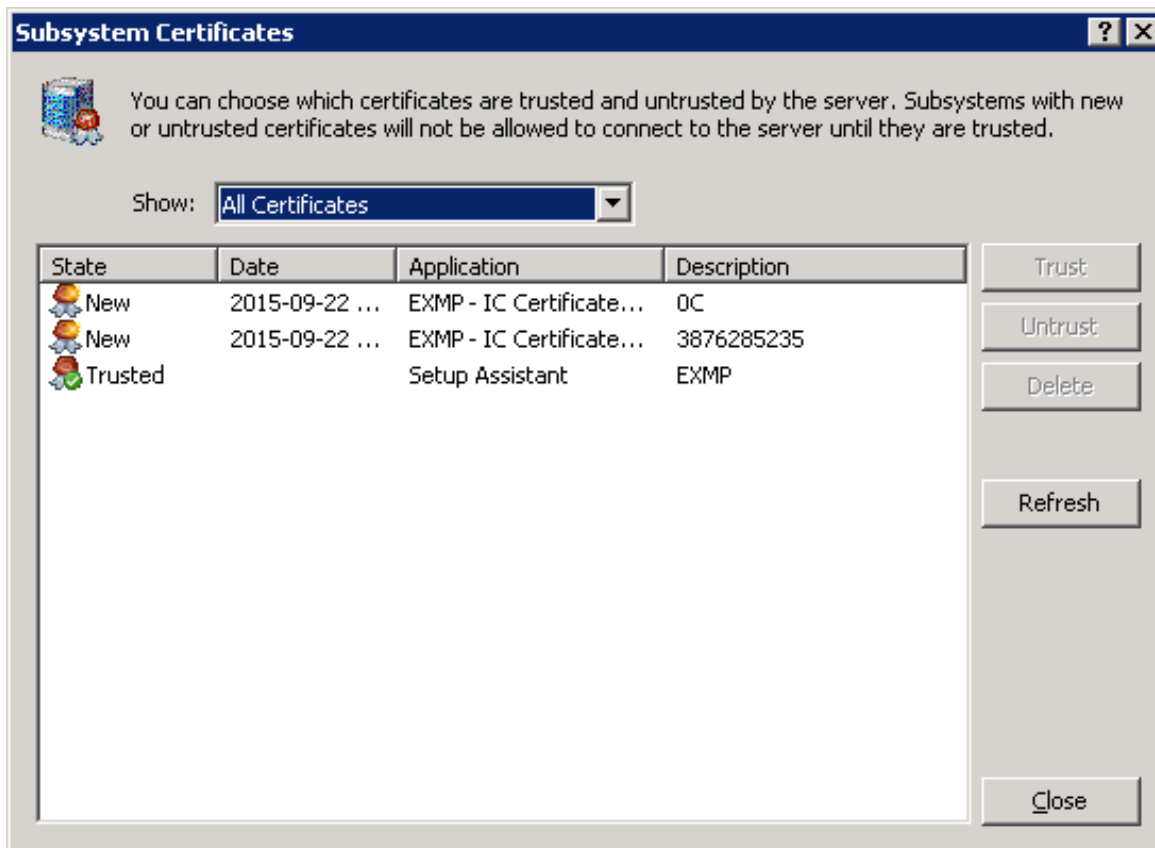
OK Cancel Apply

4. Select the **Certificate Management** tab.
5. Under **Subsystem Certificates Configuration**, select the **Modify** button.





The **Subsystem Certificates** dialog box appears with a **New** certificate from the Interaction Recorder Remote Content Service server.

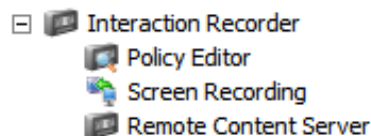


6. Select the new certificate and select the **Trust** button.
7. In the **Subsystem Certificates** dialog box, select the **Close** button.
8. In the **System Configuration** dialog box, select the **OK** button.

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

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

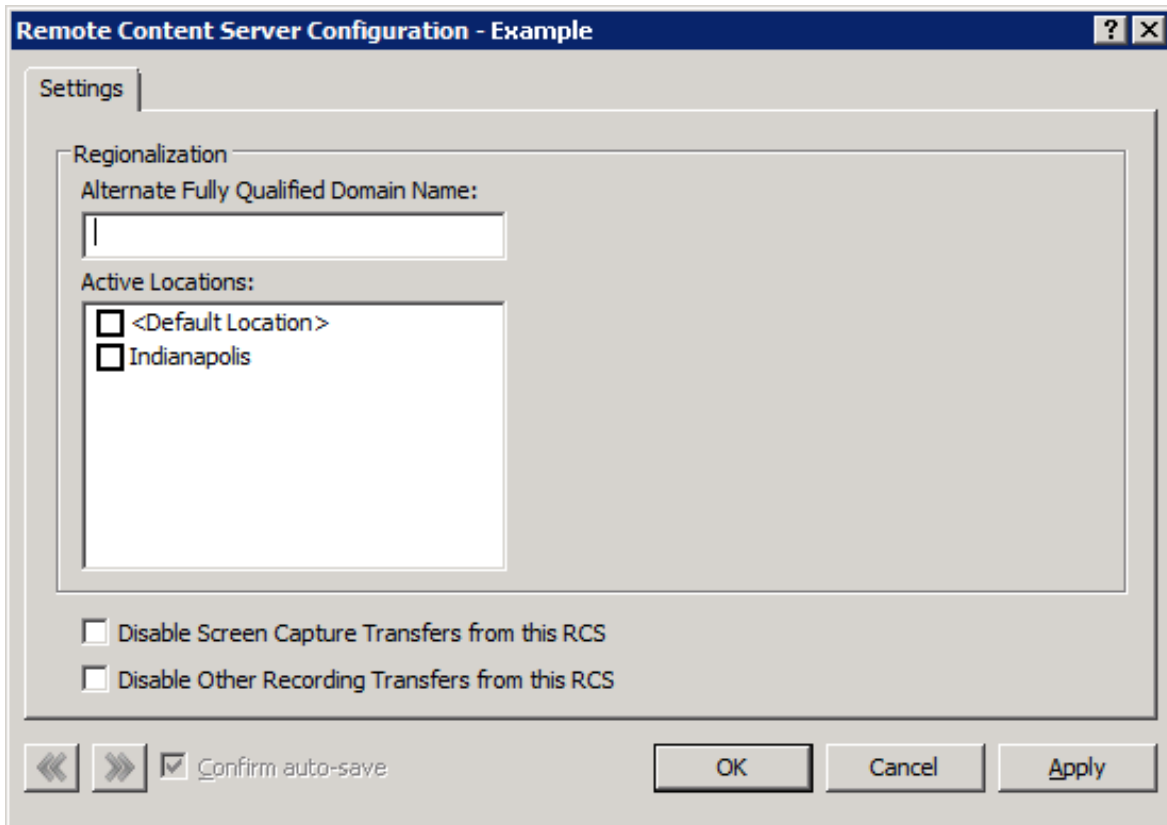


4. In the details pane on the right side, double-click the entry for the Interaction Recorder Remote Content Service instance that you want to configure.

### Note:

Customer Interaction Center uses only those Interaction Recorder Remote Content Service instances that are listed as **Active**. However, you can configure any listed instance, regardless of its state.

The **Remote Content Server Configuration** dialog box for the selected server appears.



The **Remote Content Server Configuration** dialog box contains the following fields:

<b>Alternate Fully Qualified</b>	If you are using PureConnect Cloud, enter 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 enables Interaction Recorder to retrieve and play the recording from this Interaction Recorder Remote Content Service server.
<b>Active Locations</b>	Using the appropriate check box, enable the regions for which you want this Interaction Recorder Remote Content Service server to move recordings from Interaction Media Servers.
<b>Disable Screen Capture Transfers from this RCS</b>	Enable this check box if you want to prevent this Interaction Recorder Remote Content Service instance from transferring screen recordings from the computers on which they are recorded.
<b>Disable Other Recording Transfer from this RCS</b>	Enable this check box if 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.

- If you want to view or adjust the configuration for another defined Interaction Recorder Remote Content Service server, use the << and >> buttons in the lower left corner.
- If you want Interaction Administrator to automatically save your configuration settings as you cycle through Remote Content Service servers, place a check mark in the **Confirm auto-save** check box.
- When you finish configuring one or more Interaction Recorder Remote Content Service servers, select the **OK** button to save the configuration and return to Interaction Administrator.

## 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 Customer Interaction Center server uses when selecting a subsystem server, such as Interaction Media Server or Interaction Recorder Remote Content Service, for a specific operation.

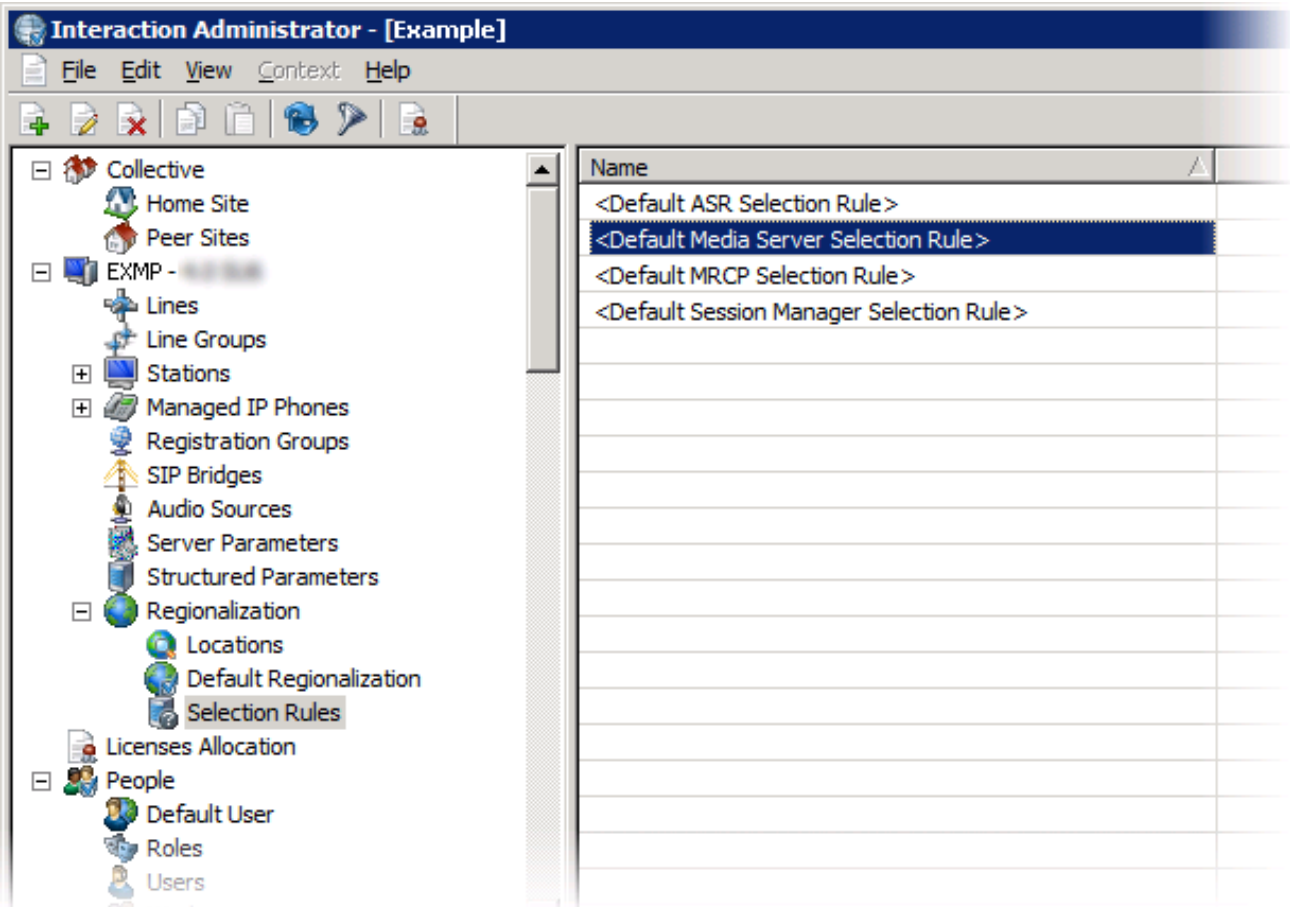
**Important!** If you modify an existing Selection Rules configuration, it affects all locations that currently use that configuration. Before you modify the configuration, Genesys recommends that you validate how the proposed modifications can affect each location that uses the configuration.

- On the Customer Interaction Center server or a remote personal computer, open Interaction Administrator. The **Interaction Administrator** window appears.

**Note:**

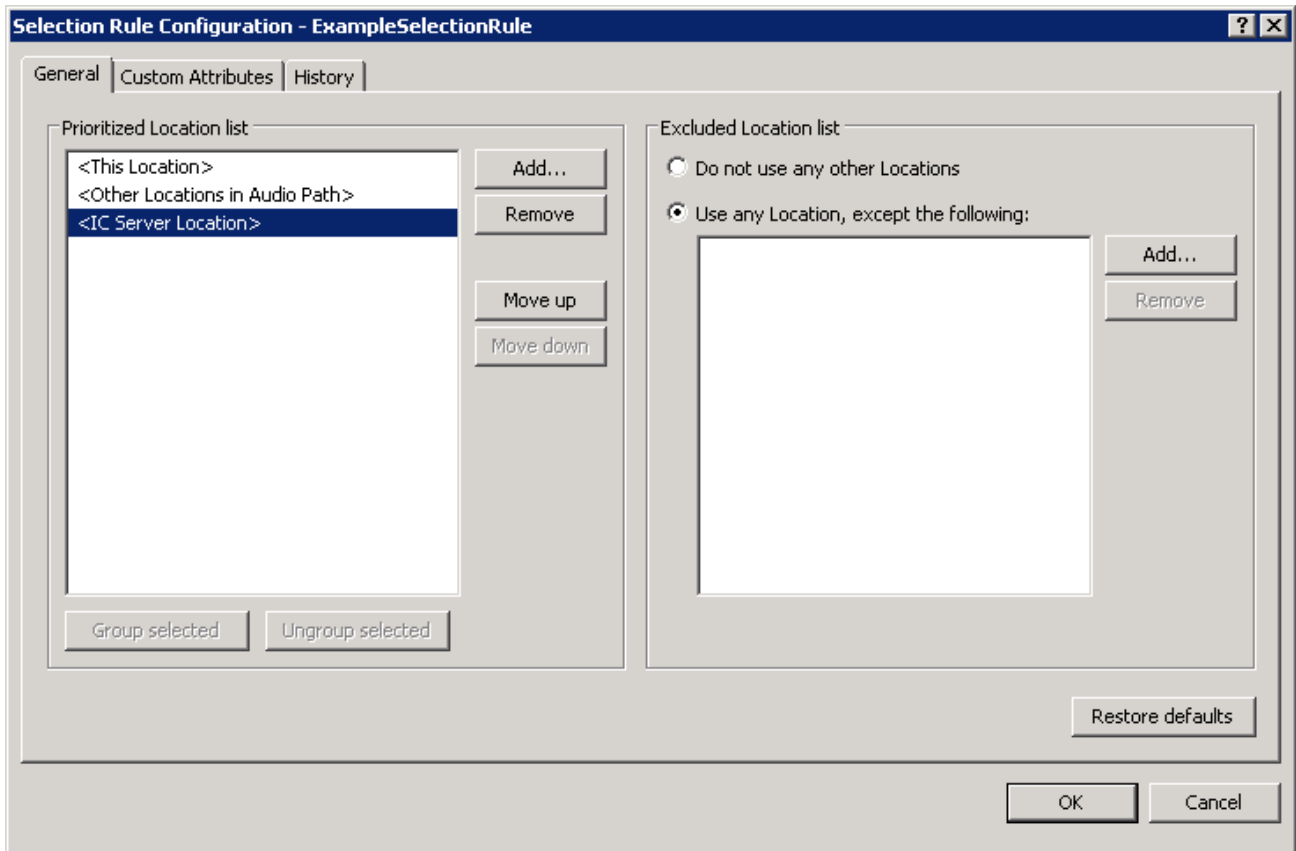
To add or modify Selection Rules configurations, your Customer Interaction Center user account must have the **Administrator Access** permission for the configurations. Those configurations are listed in the **Selection Rules** section of the **Administrator Access** dialog box in Interaction Administrator. For more information, see "Administrator Access" in *Interaction Administrator Help*.

2. In the left pane of the **Interaction Administrator** window, under the object that represents your Customer Interaction Center server, expand the **Regionalization** container.
3. Under the **Regionalization** container, click the **Selection Rules** object.



4. Do one of the following steps:
  - o If you want to create a Selection Rules configuration, do the following steps:
    - a. Right-click an empty area in the right pane and select **New** from the resulting shortcut menu.
    - b. In the resulting **Entry Name** dialog box, enter a unique name for the new Selection Rules configuration and click **OK**.
  - o If you want to modify an existing Selection Rules configuration, double-click the Selection Rules configuration entry in the right pane.

Interaction Administrator displays the **Selection Rule Configuration** dialog box.



5. On the **General** tab, use the following controls to modify the Selection Rules configuration:

Prioritized Location list	
<b>Add</b>	Click this button to add a static or variable location to the <b>Prioritized Location list</b> box.
<b>Remove</b>	Click this button to remove the selected location from the <b>Prioritized Location list</b> box.
<b>Move up</b>	Click this button to move the selected location to higher position in the <b>Prioritized Location list</b> box.
<b>Move down</b>	Click this button to move the selected location to a lower position in the <b>Prioritized Location list</b> box.
<b>Group selected</b>	Click this button to assign the selected locations to a group that provides load balancing. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <b>Tip:</b>            To select multiple locations, press and hold the <b>Ctrl</b> key while clicking each location in the box.         </div>
<b>Ungroup selected</b>	Click this button to remove the selected location from an existing group.
Excluded Location list	
<b>Do not use any other Locations</b>	Click this option to restrict Customer Interaction Center from selecting any other location than those locations specified in the <b>Prioritized Location list</b> box.
<b>Use any Location, except the following</b>	Click this option to allow Customer Interaction Center to select any available location after it cannot locate an available Interaction Recorder Remote Content Service server assigned to the location in the <b>Prioritized Location list</b> box. Customer Interaction Center excludes any location specified in the <b>Excluded Location list</b> box.
<b>Add</b>	Click this button to add a location to the <b>Excluded Location list</b> box.
<b>Remove</b>	Click this button to remove the selected location from the <b>Excluded Location list</b> box.
<b>Restore defaults</b>	Click this button to reset this configuration to the default settings.

6. When finished, click **OK** to save the new Selection Rules configuration.

## 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. If you need to change these values, you must manually edit the configuration file.

**Note:**

If you edit the configuration file, you must restart Interaction Recorder Remote Content Service for the changes to take effect.

The Interaction Recorder Remote Content Service configuration file is named `ircontentserverconfig.xml`. It is located 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 that can be made to this Interaction Recorder Remote Content Service server. This number represents the maximum number of simultaneous recording playbacks that this server will allow.

**Note:**

While the installation program allows you to specify a maximum of 16 connections, you can enter 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 with 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 automatically creates a security certificate for this Interaction Recorder Remote Content Service server. However, if you change the domain in which the server is located, you may need to manually regenerate this security certificate so that this server can communicate with the Customer Interaction Center server.

To manually regenerate a certificate for this server, do the following steps:

1. On the Interaction Recorder Remote Content Service server, open a command prompt window.
2. In the command prompt window, navigate to 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. Execute the following command:

```
gensslcertsu.exe -r CIC_Server_Name CIC_User_Name CIC_User_Password -f
```

The parameters for this command are defined as follows:

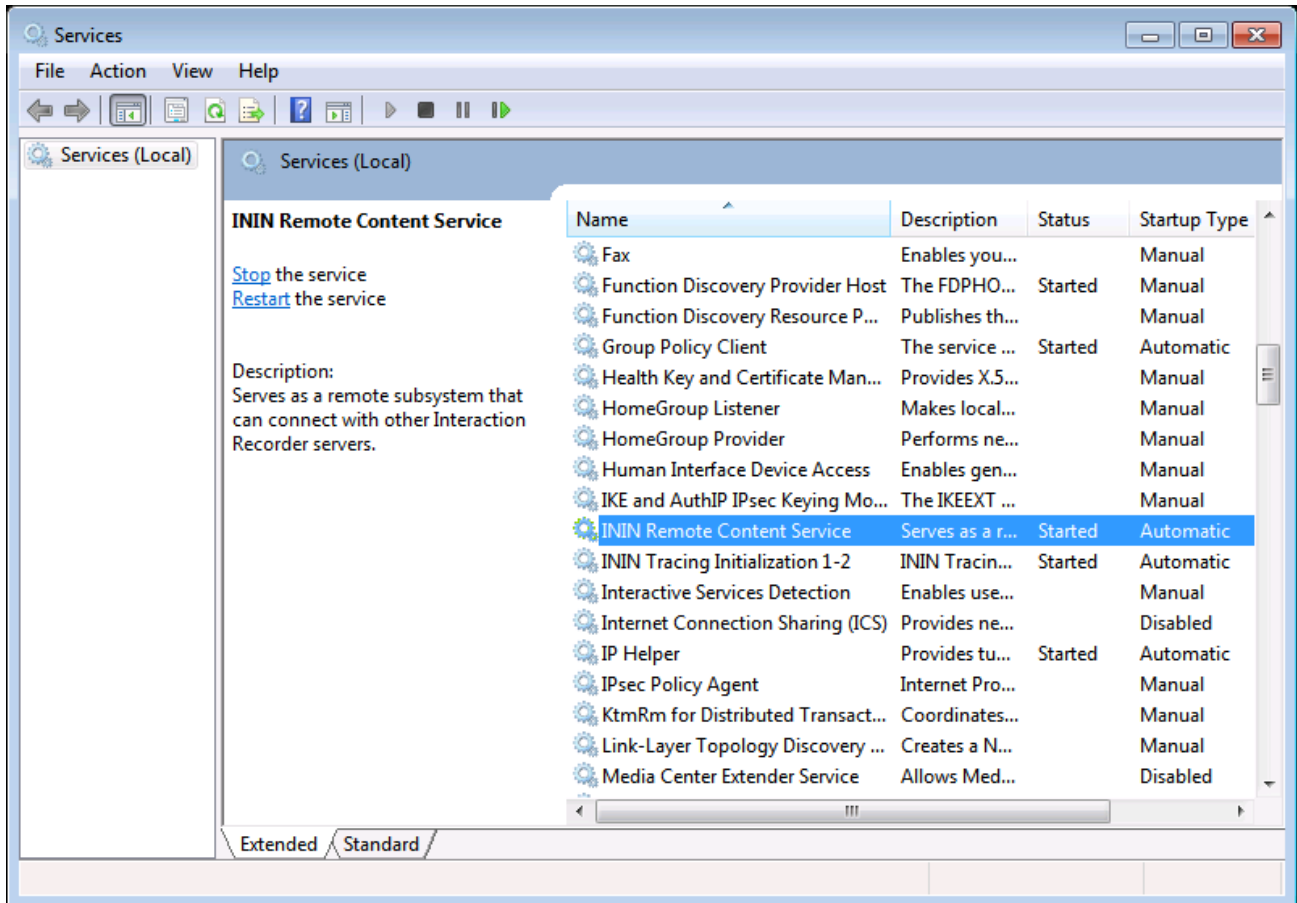
- *CIC\_Server\_Name* – The name of the Customer Interaction Center server on which you are generating the certificate
- *CIC\_User\_Name* – The user name of a Customer Interaction Center administrator
- *CIC\_User\_Password* – The password associated with the specified Customer Interaction Center administrator

**Note:**

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

The Customer Interaction Center server creates a certificate for all remote subsystems and adds the Interaction Recorder Remote Content Service instance.

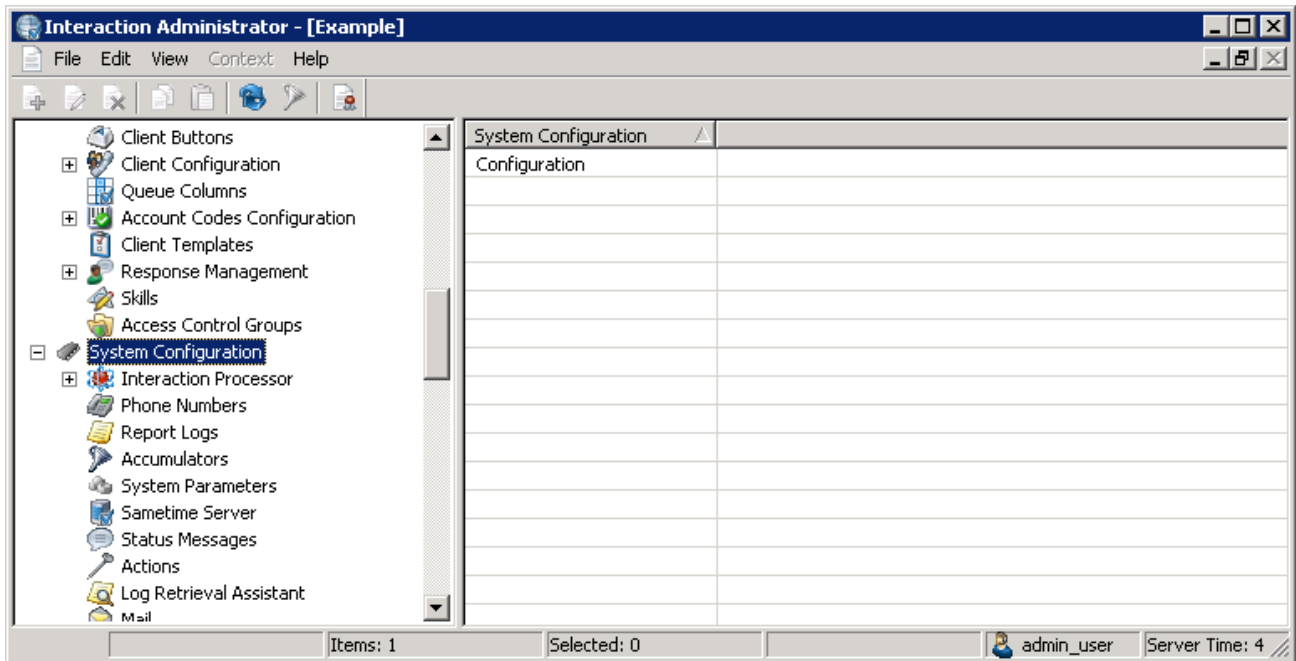
4. Using the **Services** window, restart the **ININ Remote Content Service** service.



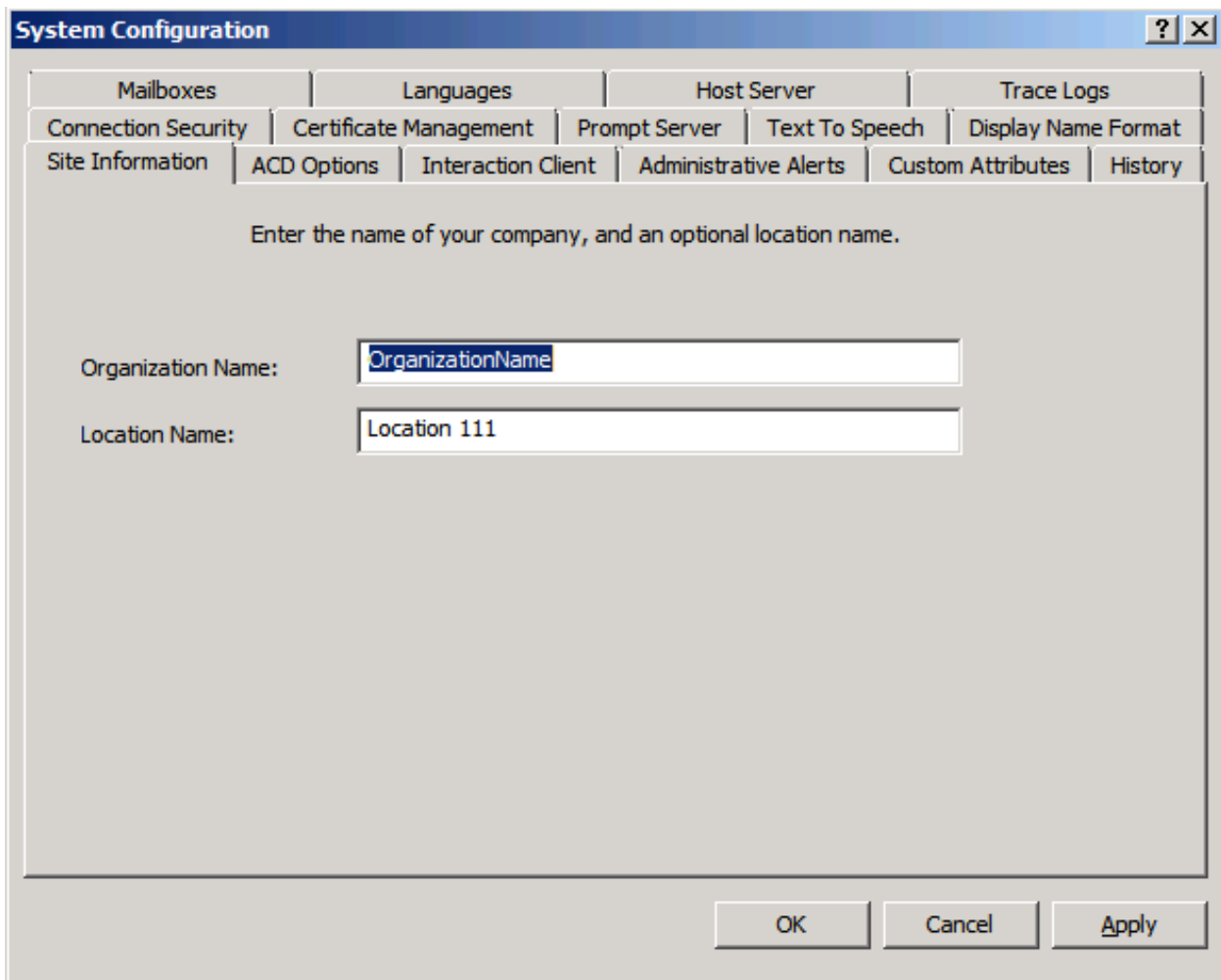
**Tip:**

Press **Win key+ R** to display the **Run** dialog box, enter `services.msc` in the **Open** box, and select **OK** to quickly display the **Services** window.

5. Using the Interaction Administrator application, log on and connect to the Customer Interaction Center server.
6. In the left pane, highlight the **System Configuration** object with a single click.

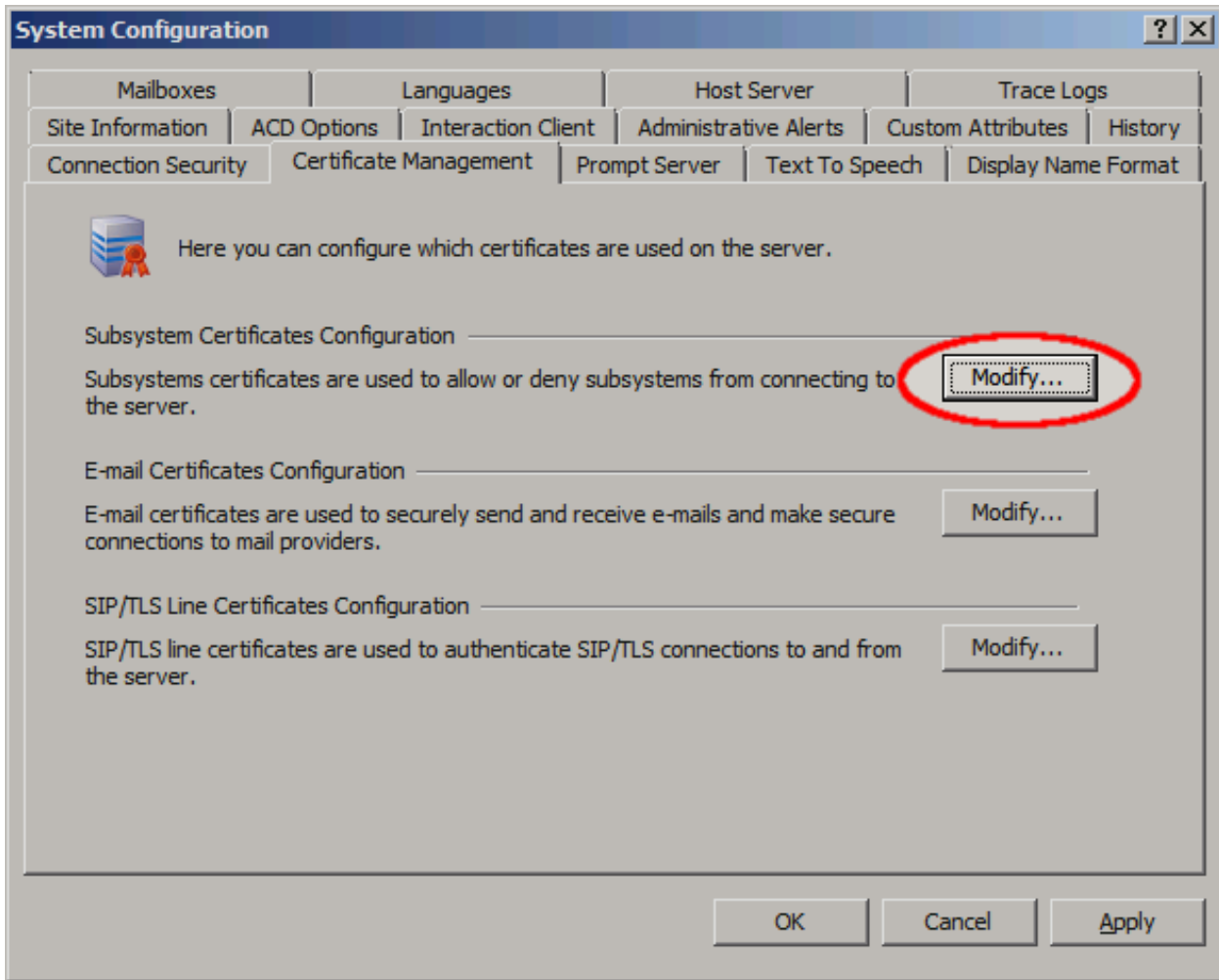


- In the right pane, double-click the **Configuration** item.  
The **System Configuration** dialog box appears.

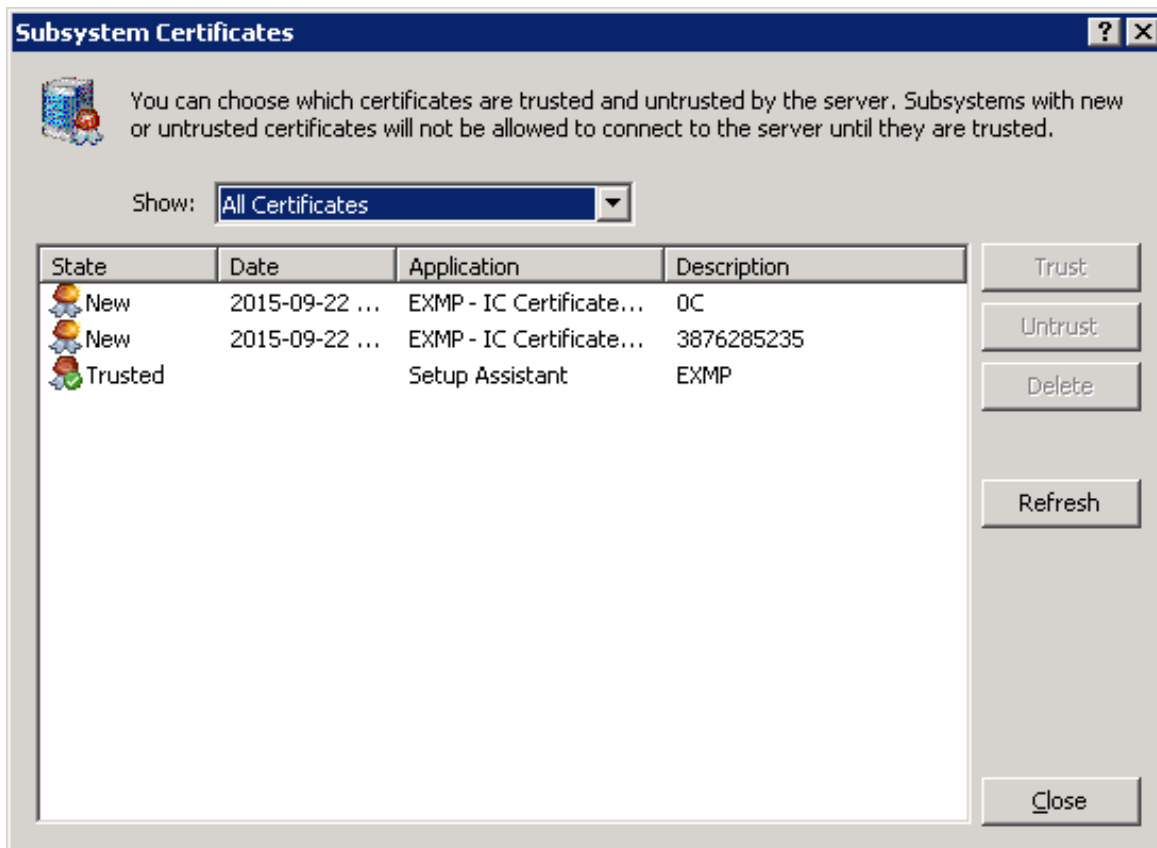


- Select the **Certificate Management** tab.
- Under **Subsystem Certificates Configuration**, select the **Modify** button.





The **Subsystem Certificates** dialog box appears with a **New** certificate from the Interaction Recorder Remote Content Service server.



10. Highlight the new certificate and select the **Trust** button.

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 to create an HTTPS certificate signed by a CA assume that the Interaction Recorder Remote Content Service servers are installed and connected to the CIC server. The instructions include:

- Generate a certificate signing request.
- Import a signed certificate for use in Interaction Recorder Remote Content Service server.

---

### 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. From the Interaction Recorder Remote Content Service server execute the following command on the command line:

#### GenSSLCertsU.exe -g HTTPS

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

For more information, refer to the “Generating Certificates Manually with GenSSLCertsU” section in the *PureConnect Security Features Technical Reference* in the PureConnect Documentation Library.

---

### Import a signed certificate for use in Interaction Recorder Remote Content Service

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.

From the Interaction Recorder Remote Content Service server, execute 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 automatically creates an HTTPS certificate) before you import the new certificate.

# Troubleshooting Interaction Recorder Remote Content Service

This section provides 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 Customer Interaction Center 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 Customer Interaction Center 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

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	<ul style="list-style-type: none"> <li>• IC-112785 - Corrected installation procedure to prompt only for fully-qualified domain name when specifying an Interaction Center server</li> <li>• 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</li> <li>• Added content for new feature to disable transfer of screen recordings from Interaction Media Server</li> <li>• Updated copyright and trademark page</li> </ul>
23-May-2014	DP-357 - Recorder Reliability - Remote Content Server Functionality Work (Server selection rules)
01-August-2014	<ul style="list-style-type: none"> <li>• Added corrections and clarification to content regarding Server Selection Rules feature</li> <li>• Miscellaneous edits for clarification and organization</li> </ul>
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	<ul style="list-style-type: none"> <li>• Updated legal page</li> <li>• Added content for exporting recordings as e-mail attachments</li> </ul>
10-April-2015	Updated formatting for new corporate standards
02-October-2015	<ul style="list-style-type: none"> <li>• Updated images to reflect new corporate branding</li> <li>• IC-131736 - Updated content to reflect maximum maxconnection setting change from 16 to 64</li> </ul>
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".

# OpenSSL Copyright

## NOTICE

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

Copyright © 1998-2011 The OpenSSL Project. All rights reserved.

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

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

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

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

### Original SSLeay License

Copyright © 1995-1998 Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:  
"This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))."

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF

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

The 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].

# Copyright and Trademark Information

*Interactive Intelligence, Interactive Intelligence Customer Interaction Center, Interaction Administrator, Interaction Attendant, Interaction Client, Interaction Designer, Interaction Tracker, Interaction Recorder, Interaction Mobile Office, Interaction Center Platform, Interaction Monitor, Interaction Optimizer, and the "Spirograph" logo design* are registered trademarks of Genesys Telecommunications Laboratories, Inc. *Customer Interaction Center, EIC, Interaction Fax Viewer, Interaction Server, ION, Interaction Voicemail Player, Interactive Update, Interaction Supervisor, Interaction Migrator, and Interaction Screen Recorder* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©1997-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Dialer and Interaction Scripter* are registered trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2000-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Messaging Interaction Center and MIC* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2001-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Director* is a registered trademark of Genesys Telecommunications Laboratories, Inc. *e-FAQ Knowledge Manager and Interaction Marquee* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2002-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Conference* is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2004-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction SIP Proxy and Interaction EasyScripter* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2005-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Gateway* is a registered trademark of Genesys Telecommunications Laboratories, Inc. *Interaction Media Server* is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2006-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Desktop* is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2007-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Process Automation, Deliberately Innovative, Interaction Feedback, and Interaction SIP Station* are registered trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2009-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Analyzer* is a registered trademark of Genesys Telecommunications Laboratories, Inc. *Interaction Web Portal and IPA* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2010-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Spotability* is a trademark of Genesys Telecommunications Laboratories, Inc. ©2011-2018. All rights reserved.

*Interaction Edge, CaaS Quick Spin, Interactive Intelligence Marketplace, Interaction SIP Bridge, and Interaction Mobilizer* are registered trademarks of Genesys Telecommunications Laboratories, Inc. *Interactive Intelligence Communications as a Service<sup>SM</sup>* and *Interactive Intelligence CaaS<sup>SM</sup>* are trademarks or service marks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2012-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Speech Recognition and Interaction Quality Manager* are registered trademarks of Genesys Telecommunications Laboratories, Inc. *Bay Bridge Decisions and Interaction Script Builder* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2013-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interaction Collector* is a registered trademark of Genesys Telecommunications Laboratories, Inc. *Interaction Decisions* is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2013-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

*Interactive Intelligence Bridge Server and Interaction Connect* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2014-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

The veryPDF product is ©2000-2018 veryPDF, Inc. All rights reserved.

This product includes software licensed under the Common Development and Distribution License (6/24/2009). We hereby agree to indemnify the Initial Developer and every Contributor of the software licensed under the Common Development and Distribution License (6/24/2009) for any liability incurred by the Initial Developer or such Contributor as a result of any such terms we offer. The source code for the included software may be found at <http://wpflocalization.codeplex.com>.

A database is incorporated in this software which is derived from a database licensed from Hexasoft Development Sdn. Bhd. ("HDSB"). All software and technologies used by HDSB are the properties of HDSB or its software suppliers and are protected by Malaysian and international copyright laws. No warranty is provided that the Databases are free of defects, or fit for a particular purpose. HDSB shall not be liable for any damages suffered by the Licensee or any third party resulting from use of the Databases.



Other brand and/or product names referenced in this document are the trademarks or registered trademarks of their respective companies.

DISCLAIMER

GENESYS TELECOMMUNICATIONS LABORATORIES (GENESYS) HAS NO RESPONSIBILITY UNDER WARRANTY, INDEMNIFICATION OR OTHERWISE, FOR MODIFICATION OR CUSTOMIZATION OF ANY GENESYS SOFTWARE BY GENESYS, CUSTOMER OR ANY THIRD PARTY EVEN IF SUCH CUSTOMIZATION AND/OR MODIFICATION IS DONE USING GENESYS TOOLS, TRAINING OR METHODS DOCUMENTED BY GENESYS.

Genesys Telecommunications Laboratories, Inc.  
2001 Junipero Serra Boulevard  
Daly City, CA 94014  
Telephone/Fax (844) 274-5992  
[www.genesys.com](http://www.genesys.com)