



PureConnect®

2020 R2

Generated:

05-May-2020

Content last updated:

17-July-2019

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



Session Manager

Development Application Note

Abstract

This document created and maintained by Genesys developers, contains technical information useful to PureConnect Customer Care and partners.

Note:

This document is intended to supplement the official product documentation. Before referring to this document, check the official product documentation at <https://help.genesys.com/cic>.

This document contains information about Session Manager as relates to your CIC server.

This document is a work in progress.

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.

Table of Contents

Table of Contents	2
Session Manager Architecture	4
Single Customer Interaction Center Server	5
Customer Interaction Center Server Switchover Pair	6
Off-Server Session Manager Machines	7
WAN-Switchover with Off-Server Session Manager Machines	8
Session Manager Discovery and Selection	10
Client Application Logon Host Value	10
Session Manager Instance Discovery	11
Client Application Selection of Session Manager Instances	12
Client Application Selection with Regionalization and Selection Rules	13
DNS Host Name Resolution	13
DNS host name resolution example	14
Session Manager Sizing	15
Sizing Calculation	15
Sizing Calculation with Regionalization	18
On-Server Session Manager Installation and System Requirements	19
Hardware and Network Requirements for On-Server Session Managers	19
Encryption Key Management for On-Server Session Managers	19
Off-Server Session Manager Installation	20
Hardware Requirements for Off-Server Session Managers	20
Virtualization	20
Running Additional Software on a Server Hosting Off-Server Session Manager	21
Third-Party Software	21
Other PureConnect Software	21
Anti-Virus Software	21
Network Requirements for Off-Server Session Managers	22
QoS Driver Installation	22
Installing Off-Server Session Manager	22
Encryption Key Management for Off-Server Session Managers	23
Certificates for Off-Server Session Manager	23
Trust Off-Server Session Manager Certificate	23
Session Manager Certificates for non-WAN-Switchover Pair	24
Custom Authority Certificates	24
Applying Updates to Off-Server Session Manager Machines	27
Automatic Process	27
Manual Process	27
24x7 Environments	27
Session Manager Configuration and Monitoring	28
Configuring Session Manager Instances	28
Retiring a Session Manager Instance	29
Setting Session Manager Identity	30
Use Regionalization with Selection Rules	31
Specify Switchover Behavior	32
Configure Session Manager Selection Rules	32
Configure a Session Manager's Accept Connections Status	34
Restrict Company Directories	34
Specify an Alternate Directory for Transfers	35
Configure High and Low Watermarks for Client Application Logons	36
View Session Manager Connections in Interaction Supervisor	36
View Connection Information for Interaction Desktop	38
Manage the Off-Server Session Manager	39
Windows Default Behavior with Authentication and Delegation	40
IceLib Outgoing Bandwidth Limiting	40
Configuration	40
High Priority Messages	41
Medium Priority Messages	41
Memory Safe Guard	42
Changing CIC Time Zone	42
Connecting IceLib Applications over the Internet	43
Reverse Proxy Requirements	43

Monitor Session Manager instances	47
Session Manager Command-Line Arguments	48
Server Parameters	49
Required Ports	50
Change Log	51

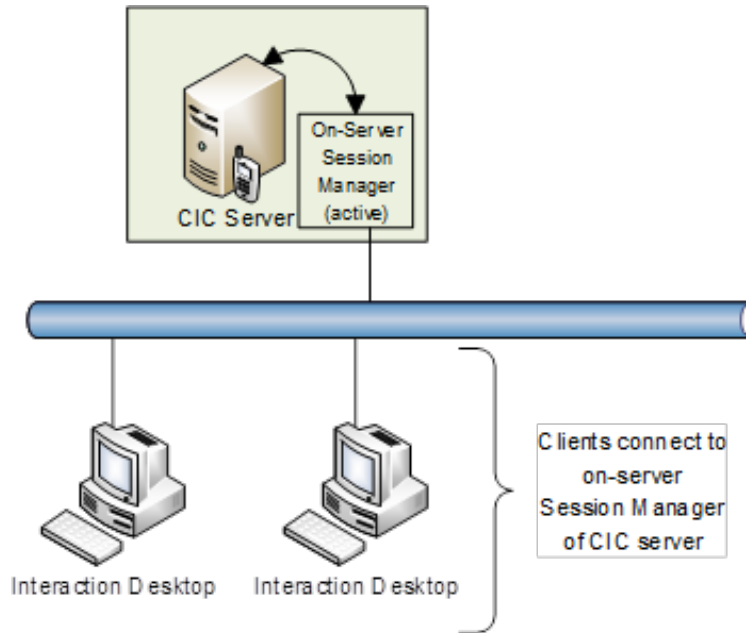
Session Manager Architecture

Session Manager is a Customer Interaction Center (CIC) server subsystem that is designed to interact with client applications written with IceLib. It provides a layer of business logic, security, and caching that enables commonly shared behavior between client applications. In larger environments one or more Session Manager instances can be installed on “off-server” machines to off-load CPU and memory utilization that could potentially affect the performance of the CIC server if run on the same physical machine. For more information, see Section [3 Session Manager Sizing](#).

In the various diagrams of Session Manager system architectures that follow, any reference to “Interaction Desktop” can be thought of as any IceLib-based application. The Interaction Desktop is a canonical example of one of those applications.

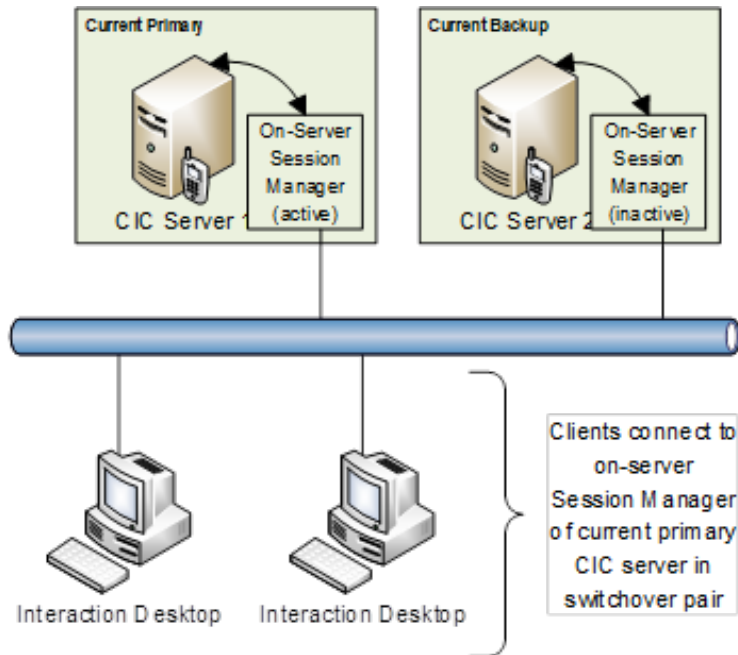
Single Customer Interaction Center Server

In a single CIC server environment, a single instance of Session Manager runs directly on the CIC server. Interaction Desktop instances connect via a standard network configuration directly to the CIC server via this one instance of Session Manager. When the client application logs in, it specifies the CIC server name as the remote host.



Customer Interaction Center Server Switchover Pair

In a switchover pair, each CIC server (primary and backup) is running its own individual instance of Session Manager. Interaction Desktop instances connect via a standard network configuration directly to the primary CIC server. When the client connects to the primary CIC server, Session Manager returns information about the Session Manager instances on the primary and backup CIC servers to the client. If the client connects to the backup CIC server, Session Manager running on the backup server rejects this connection and return information about both Session Manager instances with the primary Session Manager indicated as the first choice for the client connection.



Off-Server Session Manager Machines

In larger implementations, it may be necessary to off-load the CPU and memory usage of Session Manager from the CIC server to dedicated servers on the network. Multiple factors are used to determine the optimal configuration. For example, considering the number of user applications running on the system, a determination can be made whether an off-server Session Manager implementation is advantageous or required.

In this configuration, the off-server Session Manager instances remain connected to the active CIC server in the switchover pair, regardless of which CIC server is active. For more information about configuration options related to switchover, see [Configuring Session Manager Instances](#).

In order to support allowing initial client logon attempts to receive the other Session Manager instances, it is desirable to run Session Manager on the CIC server locally as well, even in an off-server Session Manager implementation. For more information, see [Session Manager Discovery and Selection](#).

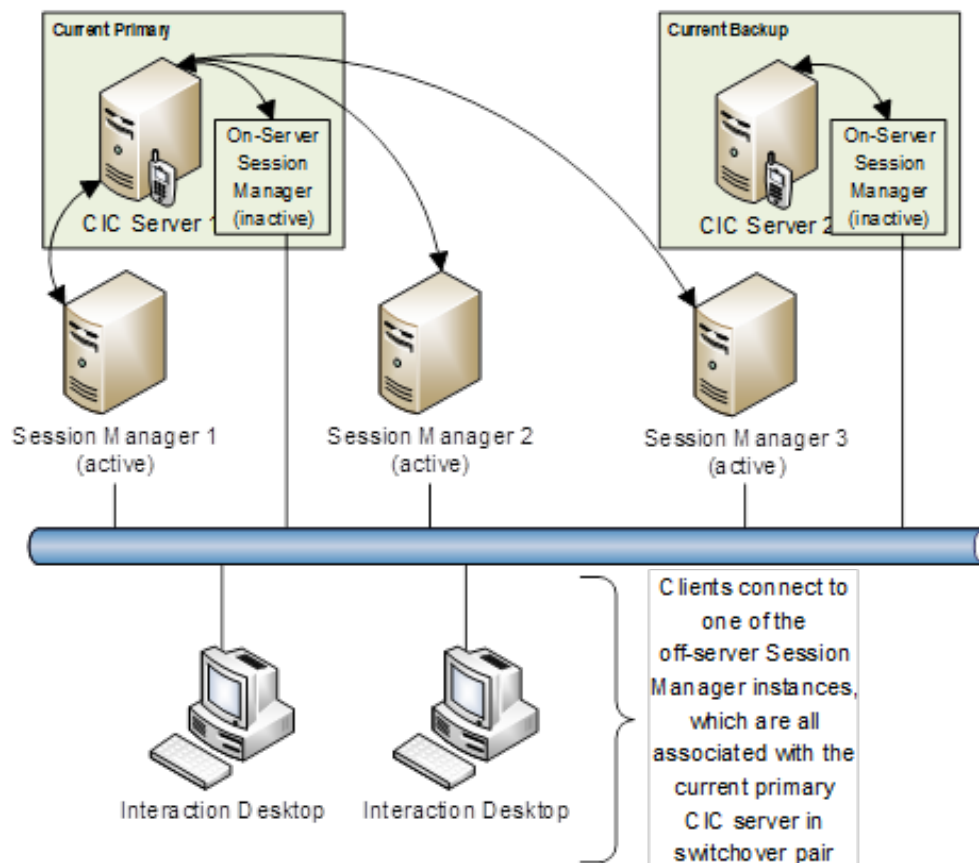
Interaction Desktop instances connect to the Session Manager server via a standard TCP/IP network. Regardless of the state of the Session Manager the client connects to (whether it is on-server or off-server and connected to the primary or backup Customer Interaction Center server), the Session Manager always responds with the list of available alternate Session Manager machines. In the case below, the list includes five Session Managers—all three off-server Session Managers—as well as the two Session Managers running locally on the CIC servers.

If the client initially connects to an on-server Session Manager, the connection is rejected after the list of alternate servers has been provided. The client then attempts to reconnect to one of the listed alternate servers, preferring off-server Session Managers over on-server Session Managers.

If the client initially connects to an off-server Session Manager, the connection succeeds.

Once the client has cached the list of alternate servers, any future connection attempts by the client prefer off-server Session Managers, even when a new instance of the client process is being started.

For more information about hardware requirements and installation of an off-server Session Manager, see [Off-Server Session Manager Installation](#).



WAN-Switchover with Off-Server Session Manager Machines

In some larger implementations, the CIC servers in a switchover pair might be located in separate data centers to provide greater resiliency if an incident occurs at one data center. A WAN connection typically separates these data centers, resulting in higher latency between the CIC servers than would occur in a typical co-located LAN-based CIC server switchover pair. This WAN-based switchover configuration is termed *WAN-switchover* and results in another Session Manager Architecture option.

In CIC 3.0, off-server Session Managers remained connected to the same CIC server when a switchover occurred to avoid connections to CIC over a high-latency WAN connection. Recent CIC testing indicates that the bandwidth utilization between CIC and Session Manager is much less than the bandwidth between Session Manager and the clients so, in the current release of CIC, the default switchover behavior for off-server Session Managers is always to connect to the primary CIC server. Customers are still allowed to use the subsystem mode (WAN switchover mode) for reasons other than what we tested. So in the current release of CIC, we still support running off-server Session Manager in subsystem mode.

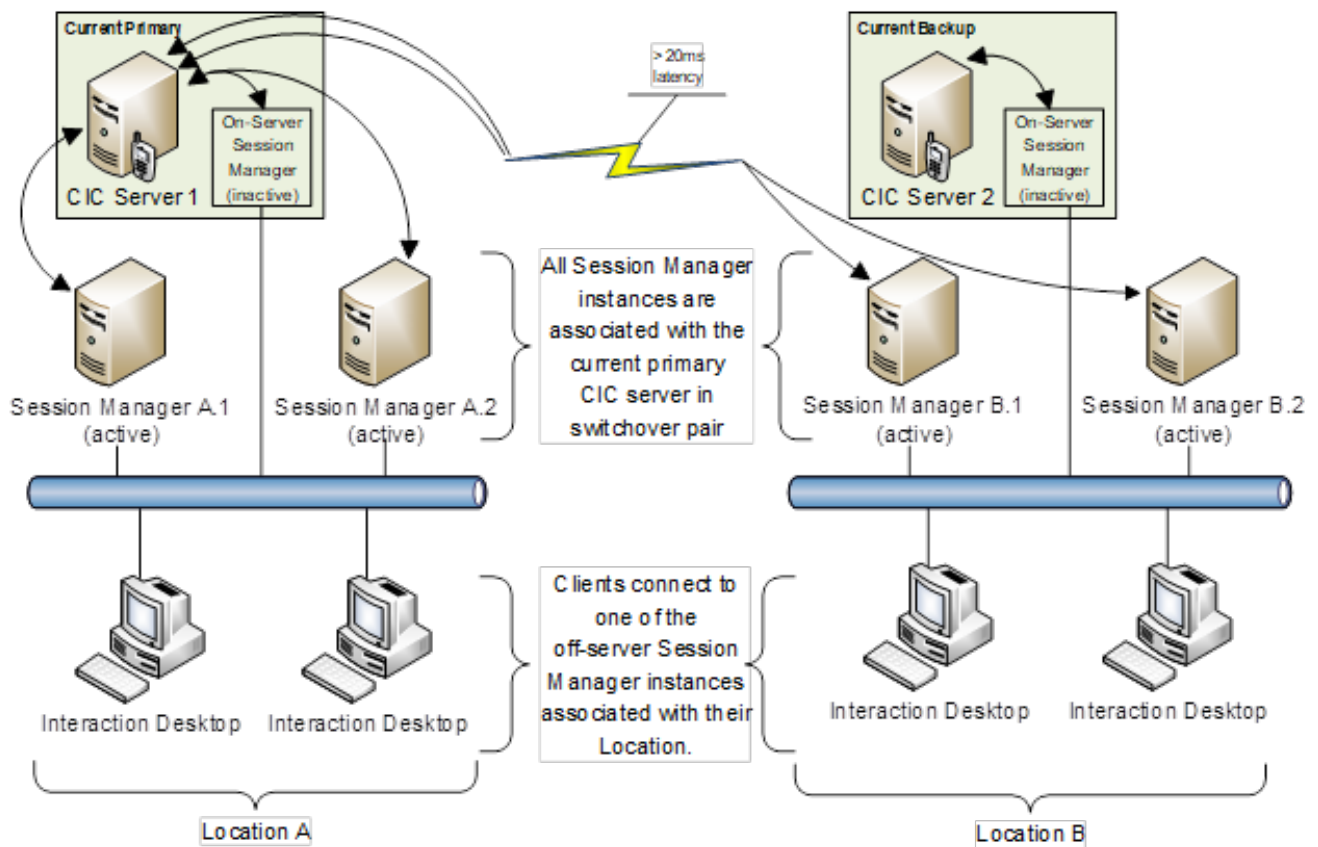
In a WAN-switchover configuration, it is ideal that client connections to a Session Manager over a high-latency WAN connection are minimized. The off-server Session Managers can be assigned to a CIC location to match the location of the on-server Session Manager, or they can use any other configured location. When a client makes a connection, Session Manager returns information about all on-server and off-server Session Managers on that CIC configuration including the location assignment for each. In the case below, the list would include all four off-server Session Managers as well as the two Session Managers running locally on the CIC servers.

The list of Session Managers is ordered as follows: first by the off-server Session Managers assigned to the same Location entry as the station, then by the off-server Session Managers assigned to the same Location entry as the user, any other off-server Session Managers, the primary CIC server, and finally the backup CIC server. If none of the off-server Session Managers are available, the client uses the IP address (or addresses) of the "Host" value specified in the client to attempt to discover and connect to Session Manager.

Matching the Location entries of users or stations to the same Location entry configured for an off-server Session Manager is a strategy that administrators can use to ensure that clients connect to Session Manager over a low-latency connection. For more information about configuring Session Manager for switchover, see [Configuring Session Manager Instances](#).

Once the client has cached the list of alternate servers, any future connection attempts by the client prefer off-server Session Managers, even when a new instance of the client process is being started.

For more information on the process of discovering and selecting a Session Manager, see [Session Manager Discovery and Selection](#).



Session Manager Discovery and Selection

Session Manager-based client applications, such as the Interaction Desktop, connect to the CIC server via a Session Manager instance. There are several aspects to consider, including what server a client application specifies to log on to, how a client application discovers the available Session Manager instances, and how a client application selects which Session Manager instance to connect to. Each of these considerations is described in the following sections.

- [Client Application Logon Host Value](#)
- [Session Manager Instance Discovery](#)
- [Client Application Selection of Session Manager Instances](#)
- [DNS Host Name Resolution](#)

Client Application Logon Host Value

At application logon, a single Session Manager instance can be specified. In client application logon dialogs, the value is often referred to as the *host*.

Typically, *host* is an auto-populated value, which matches the one specified when the application was installed. The value can be changed and might be communicated to users via an e-mail, a system administrator might configure the value, or an automated mechanism that runs the installation on the machine might configure the value.

Some client applications support a silent logon mode where the user is not offered a logon dialog. In these cases, a *host* value might be used from the installation values or from persisted or shared values from other client application logon attempts.

For deployments involving a single Customer Interaction Center server (that is, no switchover), the host value specified for logon should be the network name of the CIC server, even if off-server Session Manager instances are part of the deployment.

For deployments involving an Customer Interaction Center server switchover pair, the host value specified for logon should be the network name of the CIC server, even if off-server Session Manager instances are part of the deployment. For more information about configuring DNS to discover the host names of the switchover pair, see [DNS Host Name Resolution](#).

Session Manager Instance Discovery

For CIC server switchover pairs, there are two CIC servers that are each running an on-server Session Manager instance. For larger deployments, multiple off-server Session Manager instances are also typically installed. In order to make good decisions at each logon attempt, client applications are able to “discover” these various Session Manager instances.

Information about all instances of Session Manager is located in Directory Services and can be configured using Interaction Administrator. For more information about configuring Session Manager, see [Configuring Session Manager Instances](#). Upon startup of CIC, the on-server Session Manager enters its registration information into Directory Services. In a switchover configuration, on-server Session Manager running on the backup server communicates its information to the on-server Session Manager on the primary server and on-server Session Manager running on the primary server registers the backup Session Manager into Directory Services. In an off-server Session Manager configuration, the off-server Session Manager also enters its registration information into Directory Services upon startup. When clients connect, Session Manager returns the Session Manager configuration as an “alternate server list” so that the client can cache this list for subsequent connection attempts.

For CIC server switchover pairs, if a client application attempts to log on to the current backup server in the CIC server switchover pair, the backup server rejects the logon attempt and the client application is provided with the configured Session Manager instances to consider for further connection attempts. Automatic detection of the available Session Manager instances by Session Manager on the backup CIC server is a feature that allows initial client application logon attempts to discover other Session Manager instances. This occurs even in cases where the client application was configured at installation to connect to a CIC server which is no longer available for connection.

If a client application attempts to log on to the current primary server in the CIC server switchover pair when there are available off-server Session Manager instances, then the Session Manager instance running on the CIC server itself rejects the logon attempt. As part of the rejected logon attempt, the client application is provided with the configured Session Manager instances to consider for further connection attempts. If switchover is not involved, if a client application attempts to connect to the only Customer Interaction Center server, the same reject behavior occurs. This feature allows initial client application logon attempts to receive the other Session Manager instances.

CIC 3.0 had an issue where on-server Session Manager would incorrectly accept connections if off-server Session Managers took slightly longer to come up after a switchover or restart event. On-server Session Manager would stop accepting connections when it identified that off-server Session Managers became available. However, the connections that are accepted until that point are not moved to the off-server Session Managers. In subsequent CIC releases, this situation would happen only once, before any off-server Session Managers are configured. In this instance, *configured* means that off-server Session Manager is installed, certificates are generated and marked as **Trusted** in Interaction Administrator, and Interaction Administrator displays off-server Session Manager in the **Session Manager** container. After this process is completed, on-server Session Manager recognizes that there is at least one off-server Session Manager configured and no longer accepts client connections.

If a larger deployment includes off-server Session Manager instances, but they are not currently available (due to maintenance or a failure), and the on-server Session Manager instance is not explicitly configured to accept connections, then the on-server Session Manager instance does not accept client application logon attempts. There are two ways to make the on-server Session Manager instance accept connections:

- In the **Session Managers** container in Interaction Administrator, you can configure the on-server Session Manager instance to explicitly accept connections regardless of the existence of other configured Session Manager instances. For more information, see [Configure a Session Manager's Accept Connections Status](#).
- If the on-server Session Manager instance is not explicitly configured to accept connections, the only way to make it accept connections is by removing the non-functional off-server Session Manager instances from the **Session Managers** container in Interaction Administrator. See [Retiring a Session Manager Instance](#).

In a CIC server switchover pair without off-server deployment, only the Session Manager instance on the current primary Customer Interaction Center server accepts connections.

In a deployment with off-server Session Managers that are not currently available, the Session Manager instance only accepts client application logon attempts up until the point that the CIC server reports that it has become loaded, based on factors such as a round-trip “ping” time to the Notifier subsystem. At that point, or when off-server Session Manager instances become available again, the client application logon attempts are rejected, with the other Session Manager instances being provided as usual. See [Configure High and Low Watermarks for Client Application Logons](#) for more information.

For larger deployments, off-server Session Manager instances are typically installed. In these scenarios, the discovery process allows client application logon attempts to the on-server Session Manager instance (or instances) to be provided with the entire network of Session Manager instances for the CIC server (or switchover pair) in question.

Client Application Selection of Session Manager Instances

Once client applications have received the entire list of Session Manager instances, this information is persisted and used for the next logon attempt.

The subsequent logon attempt might immediately follow a rejected on-server logon attempt. Or, it might have been days or weeks since the last logon attempt, with various off-server or on-server Session Manager instances now down for maintenance, or with a CIC server switchover event having occurred. When a client application logon is requested, the state of the Session Manager network is not known, but the client application must make good decisions anyway.

The client application starts by loading its cached data containing the last-known configuration of Session Managers in the CIC configuration. This list includes information about whether each is an on-server or off-server instance as well as location information.

When the client eventually makes a successful connection, it receives the current list of Session Manager instances. The client then erases the previously persisted list and the new list obtained from Session Manager is persisted. Essentially, the list is valid only until the next successful logon. This approach was new in CIC 4.0.

Client Application Selection with Regionalization and Selection Rules

When the IceLib-based application is attempting to connect, it sorts the Session Manager instances into groupings based on the configured Selection Rule for the user's location. The user's location is determined first by the user's station's configured location, and if that is not set, the user's configured location is used. The Selection Rule for the user's location is then used to prioritize these groupings, and if there is no Selection Rule defined in that location, then the **<Default Session Manager Selection Rule>** is used. These groupings are always considered in the order shown in the following list:

1. Any Session Manager instances in locations that have been blacklisted by the Selection Rule are not included.
2. Session Manager instances that are in locations that are prioritized by the Selection Rule will be grouped and prioritized according to the priority that is set in the Selection Rule. Both off-server and on-server Session Manager instances will be included in these groups.
3. If other (non-prioritized and non-blacklisted) locations are not allowed by the Selection Rule, then no other Session Manager instances will be included.
4. If other locations are allowed by the Selection Rule, the next grouping is **other off-server Session Managers**.
5. If other locations are allowed by the Selection Rule, the next grouping is **other on-server Session Managers**.
6. The final grouping is the **raw IP address (or addresses) of the Host entry used to connect**. If the host is a DNS alias that is configured to resolve to multiple addresses, the final grouping can be multiple IP addresses. See [DNS Host Name Resolution](#), for more information about DNS aliases. This entry will always be present, whether the Selection Rule allows for other locations or not.

Note:

If there are multiple Session Manager instances in a given grouping, then their order is randomized within that grouping, to spread the load of connection attempts.

In an initial connection attempt, an IceLib-based application first attempts to connect to the hostname entered in the logon dialog. If the Session Manager on that server rejects the logon attempt, a list of available Session Managers and the Selection Rules are provided to the IceLib-based application to continue the logon process. Then, the application attempts a connection using all Session Manager groupings, in order, until a successful connection is made, or until all attempts have failed. The application only makes a single attempt to connect to a given Session Manager instance. Since IceLib will attempt to connect to whatever Session Manager is entered as the hostname in the logon dialog on the very first attempt, that Session Manager will enforce Selection Rules for that session enough to ensure that Session Manager is not in an excluded location for that session's Selection Rule.

When automatically reconnecting an IceLib-based application, the application makes several attempts to connect to only the top Selection Rule priority grouping (if the grouping is non-empty), without any attempt to connect to Session Managers in the other groupings. Then, if the reconnect attempt is still not successful after those attempts, the application tries to connect using the full list of groupings, the same as an initial connection attempt.

If the client application encounters a logon failure it stops attempting other Session Manager instances and immediately reports the issue to the user, rather than futilely continuing to attempt the other Session Manager instances. Examples of logon failures are an invalid CIC User password, invalid Windows User authentication, or an invalid CIC Station.

For more information on how to configure Session Manager instances for regionalization, see [Use Regionalization with Selection Rules](#).

For more information on how to configure Session Manager Selection Rules, see [Configure Session Manager Selection Rules](#).

For more information about sizing an installation that is using regionalization, see [Sizing Calculation with Regionalization](#).

DNS Host Name Resolution

For Customer Interaction Center server switchover pairs, a useful practice is to configure DNS Host Name Resolution (A records for IPv4 addresses and AAAA records for IPv6 addresses) to create an alias that represents both CIC servers in the pair. Creating a DNS host name alias simplifies deployment by allowing users to log on to their client applications using a single *Host* value that represents both servers in the CIC server switchover pair.

Having a DNS host name alias also guarantees that the initial client application logon attempt by a user discovers an appropriate Session Manager instance, even if the specified CIC server switchover pair machine is unavailable. If an individual server in the pair is specified and it happens to be unavailable, then the initial logon fails because the Session Manager is unable to accept the connection or to provide the other configured Session Manager instances to consider for further connection attempts.

DNS host name resolution example

A switchover pair consists of CIC servers:

- ExampleCIC1
- ExampleCIC2

The DNS host name alias might be called ExampleCIC which represents both of the actual physical servers in the pair. The DNS host name allows client applications to log on with ExampleCIC as their Host, at which time they are provided with the configured Session Manager instances to consider for connecting (even the first time before any discovery has occurred).

IceLib based applications (as directed by Session Manager) will use the network name of the CIC server when the application intends to download a resource such as Status Icons or Response Management files. In some cases, a regular network name may not be discoverable from the computer that is running the IceLib application. So, overriding with a discoverable network name might be the only option to allow access to the HTTPS resource to download. Set the server parameter, **SM HTTPS URL Base Map**, in such cases. For more information about the SM HTTPS URL Base Map server parameter, see Section [9 Server Parameters](#).

Session Manager Sizing

A given Session Manager instance allows large numbers of simultaneous client application connections. Each client application connection takes up a certain number of server resources such as CPU load, memory utilization, or network bandwidth.

Different types of client applications require different resources, such as CPU, memory, network bandwidth, and so on. For example, Interaction Supervisor requires different resources than the Interaction Desktop. Even different usages in the same client application type require different server resources, putting different loads on the Session Manager server. For example, a business user running the Interaction Desktop with the Company Directory and monitoring their own My Interactions tab, requires X resources, depending on how many people are in the Company Directory, how many interactions they receive, and other various factors. Consider a call center agent who has the Company Directory and a Workgroup Directory up, monitoring their My Interactions tab, as well as a workgroup Queue Statistics tab. That application usage could require vastly different resources than the application of a business user, depending on call volume, number of workgroups, and a vast number of additional variables.

Because of the impact of various client features on the performance requirements of Session Manager, there are certain guidelines for determining how many simultaneous user connections are appropriate for a given on-server or off-server Session Manager instance. By extension, this calculation also determines how many Session Manager instances are necessary for a given site.

Additionally, if regionalization is being used then the sizing calculation should be determined for each individual location. For more information, see [Section 3.2 Sizing Calculation with Regionalization](#).

Sizing Calculation

To estimate the appropriate number of servers needed, use the assumptions in Table 1 to establish a comparable set of values. As described in [Session Manager Sizing](#), different types of client applications require different resources. As such, take individual variations from these example usages into account when determining an estimated sizing.

Table 1 User Categories for Sizing

User Category	Description
Business Users	Interaction Desktops loading Company Directory and one additional directory that is a subset of the Company Directory; moderate call volume (less than 20% of users on phone at one time).
Call Center Agents	Interaction Desktops loading Company Directory, one additional directory, Workgroup Queue Statistics; less than 20% of users monitoring one ACD queue; heavy call volume (approximately 100% users on phone or in follow-up; approximately one call in queue for each agent on phone). Genesys performed sizing estimates with an assumed ratio of 10:1 for call center agents to supervisors. So, for example, if there are 1000 call center agents, the sizing is modeled based on an assumption of an additional 100 supervisor users as well. See Table 2 for additional details about how those Supervisor users were tested. Note: Queue monitoring is designed for IT, Management, and Team Lead personnel and not intended for all agents. If all agents must monitor ACD queues, scalability is reduced and Genesys recommends that you consult Sales Engineers for proper Session Manager sizing.

Table 2 Additional Details for Call Center Agents Scenario

Additional information	Scenario details
Supervisor clients configuration	• 1 workgroup queue with default supervisor queue attributes. Change to a different queue every 5-10 minutes • 200 Agent statistics: ◦ 20 Agents with 10 statistics each ◦ The 10 statistics are the same for all agents however, each supervisor will monitor different stats randomly chosen from current period and current shift. ◦ Watch all statistics on one workgroup. Change to different workgroup every 5-10 minutes. • One workgroup directory watch with user status. Change to different workgroup every 5-10 minutes. • 161 Alerts per supervisor • One Time In Status alert with On Call Status from 30-60 seconds on one workgroup • 100 Agent Statistic Alerts (20 agents X 5 stats X 1 range), non-time based • 60 Workgroup Statistic Alerts (3 workgroups X 10 stats X 2 ranges) ◦ Approximately ten time-based and 50 non-time-based alerts ◦ Send client memo to workgroup members on six of the statistics
Additional scenario details	• 25 workgroups, 100 active members each, one workgroup per user • 20 CPS (All inbound ACD), recorded, with a max of 3800-4000 calls • On Call status and Follow Up enabled in the workgroups • Exchange 2010, Outlook Client 2010, Oracle 11gR2

Further, example scaling estimates were created based on tests performed with a particular set of hardware, as described in Table 3. Take into account individual variations from this example when determining an estimated sizing.

Table 3 Hardware Used for Sizing Estimates

Scalability Test Configuration					
Function	Enterprise / Business Users			Call Center Agents	
CIC server	CPU	Intel Xeon X5670 • Dual 6-Core Hyperthreaded (24 Core) • 2.93GHz		CPU	Intel Xeon X5570 • Dual Quad-Core Hyperthreaded (16 Core) • 2.93GHz
	RAM	24GB		RAM	12GB
Off-Server Session Manager	CPU	Intel Xeon E5620 • Quad-Core Hyperthreaded (8 Core) • 2.40GHz		CPU	Intel Xeon E5620 • Quad-Core Hyperthreaded (8 Core) • 2.40GHz
	RAM	6GB		RAM	6GB

The maximum load per Session Manager instance is shown in Table 4 in which the values indicate maximums where only one type of user exists at a site. However, actual installations have a mixture of business users and call center agents, resulting in a maximum load somewhere between the two values (see Table 5 for an explanation of how to calculate sizing with a mixture of user types). The maximum values refer to designing for the specified number of simultaneous users. If there are more users than the maximum for a Session Manager running on the CIC server, then the design must include sufficient off-server Session Manager machines to support all users. This guidance is because the on-server Session Manager instance does not accept connections if there are configured off-server Session Manager machines. For more information, see [Configuring Session Manager Instances](#).

Table 4 Maximum Load per Session Manager

User Category	Session Manager (CIC Server)	Off-Server Session Manager	Total in Tested Scenario, Across All Off-Server Session Managers
Approximate maximum business users	5,000	5,000	10,000
Approximate maximum call center agents	2,500* (+ 250 supervisors)	2,500* (+ 250 supervisors)	4,000* (+ 400 supervisors)
	*Sizing estimates were performed with an assumed ratio of 10 to 1 for call center agents to supervisors. So, for example, if there are 2500 call center agents, the sizing is modeled based on an assumption of an additional 250 supervisor users as well.		

When designing a large site for N+1 redundancy, the following equation can be used to determine the number of off-server Session Manager machines that are needed. The +1 adds an off-server Session Manager instance to provide resiliency for when another off-server Session Manager machine fails or is taken offline for maintenance. In addition, the +1 machine also aids in spreading the resource load while all the off-server Session Managers are functional.

Table 5 Sizing Calculation

Value	Definition
Number of off-server Session Manager Machines	$\text{Ceiling} \left(\left(\frac{B_{total}}{B_{max}} \right) + \left(\frac{A_{total}}{A_{max}} \right) \right) + 1$ Note: <i>Ceiling</i> refers to rounding up to the next whole number.
B_{total}	Total number of simultaneously logged in business users.
A_{total}	Total number of simultaneously logged in call center agents.
B_{max}	Maximum number of simultaneous business users per off-server Session Manager machine. This value is 5000, as per Table 4.
A_{max}	Maximum number of simultaneous call center agents per off-server Session Manager machine. This value is 2500, as per Table 4.

Sizing Calculation with Regionalization

If regionalization is being used, Off-Server Session Manager instances will be associated with each Location entry from which users will connect. For more information, see [Use Regionalization with Selection Rules](#). In this scenario, the sizing calculation described in [Sizing Calculation](#) should be performed separately for each location.

For instance, consider an installation that uses regionalization with multiple locations configured across the WAN and with the following user characteristics:

- Location: Primary site
 - Business users = 2000
 - Call center agents = 1000
- Location: Satellite office
 - Business users = 500
 - Call center agents = 100
- Total across all locations
 - Business users = 2500
 - Call center agents = 1100

If we consider the total number of users across all Location entries, using the equation from [Table 5](#), we would determine that only two off-server Session Managers are needed to support the total number of users. It might seem sensible to then associate one off-server Session Manager with each Location entry.

However, if we consider the Primary Site on its own, using the equation from [Table 5](#), we find that it should be associated with two off-server Session Managers. Similarly, if we consider the satellite office on its own, we find that it should be associated with two off-server Session Managers. Essentially, by applying the equation separately for each Location entry, what we find is that each location has its own $N + 1$ protection for an off-server Session Manager being unavailable to service the users at that location.

If only the total number of users were considered for the equation, and therefore a single off-server Session Manager was deployed at the satellite office location, then if that off-server Session Manager were to become unavailable (for example due to a hardware issue or during maintenance), then the users at the satellite office would have to fall back and connect across the WAN to the off-server Session Manager at the primary site. This is not ideal and introduces additional bandwidth concerns.

On-Server Session Manager Installation and System Requirements

The CIC installation process automatically installs Session Manager on the CIC server. For more information, see the *PureConnect Installation and Configuration Guide*. This section describes installation-related topics for Session Manager when running on the CIC server.

- [Hardware and Network Requirements for On-Server Session Managers](#)
- [Encryption Key Management for On-Server Session Managers](#)

Hardware and Network Requirements for On-Server Session Managers

The CIC server hardware and network requirements include the needs of on-server Session Manager and are documented separately from this application note.

Specifically, Session Manager listens on port 3952 for incoming requests. Interaction Desktop and other IceLib-based applications connect to Session Manager on this port. Every server that is running Session Manager must have permissions to open port 3952, including the CIC server (or servers in a switchover pair). Every computer that is running an IceLib-based client application must be able to access port 3952 of all Session Managers that they are allowed to connect to.

Some file transfers between IceLib and the server utilize the HTTPS protocol via port 8019. Every server that is running Session Manager must have permissions to open port 8019, including the CIC server (or servers). Every computer that is running an IceLib-based client application must be able to access port 8019 of all Session Managers that they are allowed to connect to, as well as port 8019 of the CIC server (or servers).

For IceLib based applications connecting over the internet, either port 8952 or port 8951 need to be opened on a server running Session Manager (including the CIC server or servers) for WebSocket connections between the application and Session Manager. Ports 8952 or 8951 must not be publicly available over the internet. Instead, a publicly available reverse proxy must be in place which would direct traffic to the appropriate Session Manager server. For more information, see Section [7.11 Connecting IceLib Applications over the Internet](#).

IceLib based applications (as directed by Session Manager) will use the network name of the CIC server when the application intends to download a resource such as Status Icons or Response Management files. In some cases, a regular network name may not be discoverable from the computer that is running the IceLib application. So overriding with a discoverable network name might be the only option to allow access to the HTTPS resource to download. A server parameter, SM HTTPS URL Base Map, should be set in such cases. For more information about this server parameter, see section [9 Server Parameters](#).

Encryption Key Management for On-Server Session Managers

Starting in 4.0, Session Manager no longer utilizes public/private keys for its communication encryption between the server and the client socket connection. The encryption has been improved from the AES RSA-type that was used in CIC 3.0 to a more secure solution using TLS v1.

Session Manager uses the Subsystem Remote Client certificate generated by the installer to secure data transmission between clients and Session Manager. TLS certificates contain the server name, the trusted certificate authority (CA), and the public key data of the server. For more information about certificates in Session Manager, see [Certificates for Off-Server Session Manager](#).

The default certificate authority signs the certificate used between Session Manager and clients, using private keys stored on the CIC server. For security and/or regulatory requirements, some customers require certificates signed by a custom certificate authority (such as VeriSign). CIC provides the capability to import root certificates signed by custom certificate authorities for signing certificates used by Session Manager. For more information about using certificates signed by another certification authority (CA), see [Custom Authority Certificates](#).

Off-Server Session Manager Installation

The off-server Session Manager install is available on the CIC 4.0 ISO image. This section describes installation-related topics for Session Manager when running on a separate machine from the CIC server.

- [Hardware Requirements for Off-Server Session Managers](#)
- [Running Additional Software on a Server Hosting Off-Server Session Manager](#)
- [Network Requirements for Off-Server Session Managers](#)
- [QoS Driver Installation](#)
- [Installing Off-Server Session Manager](#)
- [Encryption Key Management for Off-Server Session Managers](#)
- [Certificates for Off-Server Session Manager](#)
- [Custom Authority Certificates](#)

Hardware Requirements for Off-Server Session Managers

See the Testlab website at <http://testlab.genesys.com> for information about supported hardware for off-server Session Manager. For this website, an off-server Session Manager is considered an **Interaction Application Server**.

Virtualization

CIC 4.0 and later releases support virtualization of the CIC environment. For the latest information, see *CIC Virtualization Technical Reference* in the PureConnect Documentation Library.

Running Additional Software on a Server Hosting Off-Server Session Manager

Running other software on an off-server Session Manager machine can have a negative impact on the performance and/or stability of Session Manager. Therefore, only use a server that is hosting an off-server Session Manager for that purpose.

Third-Party Software

Avoid installation of third-party applications on a server hosting an off-server Session Manager, or carefully evaluate if the software is required.

Other PureConnect Software

No other PureConnect applications can be installed on the server but you can install plug-ins on off-server Session Manager instances for communication with other CIC products:

- Interaction Dialer

The Interaction Dialer plug-in for off-server Session Manager enables Interaction Dialer to communicate with Session Manager. For the procedure to install the Interaction Dialer plug-in for Session Manager, see "Install Dialer Plug-ins for IC Session Manager Server" in *Interaction Dialer Installation and Configuration Guide*.

- Interaction Conference

The Interaction Conference plug-in for off-server Session Manager enables Interaction Conference to communicate with Session Manager. For the procedure to install the Interaction Conference plug-in for Session Manager, see "Optionally install Session Manager IConference plug-ins on off-host Session Manager servers" in *Interaction Conference Administrator's Guide*.

Anti-Virus Software

Genesys has verified that McAfee VirusScan and Symantec AntiVirus software can be installed on PureConnect platform servers, including an off-server Session Manager server, as part of a system-wide anti-virus strategy. See the Testlab website at <http://testlab.genesys.com> for the latest supported versions of McAfee VirusScan and Symantec AntiVirus.

Note the following requirements and recommendations:

- Run a scan of all disks during off-peak hours, once per day, or at least once per week. Synchronize this effort with other backup tasks that are typically run daily.
- Disable active scanning while running installs or applying service updates to the server. Active scanning locks files and causes excessive disk I/O and high CPU utilization, which can result in system slowdowns or failure.

If active scanning is a requirement, do not enable it during business hours, especially if the server is under a high CPU load. If running active scanning is required, refer to the "Anti-virus requirements and Best Practices" section in the *PureConnect Installation and Configuration Guide* for a list of configuration changes to make.

- If Genesys suspects the anti-virus software is causing any issues, a support engineer might ask you to remove the software for troubleshooting purposes.

Network Requirements for Off-Server Session Managers

Off-server Session Manager connects to the Notifier subsystem running on the CIC server on port 5597 by default. Every off-server Session Manager machine must be able to access port 5597 of the CIC server (or servers, in a switchover pair).

Session Manager listens on port 3952 for incoming requests. Interaction Desktop and other IceLib-based applications connect to Session Manager on this port. Every server that is running Session Manager, including the CIC server (servers), must have permissions to open port 3952. Every computer that is running an IceLib-based client application must be able to access port 3952 of all Session Managers to which it is allowed to connect.

Some file transfers between IceLib and the server use the HTTPS protocol on port 8019. Every server that is running Session Manager, including one or more CIC servers, must have permissions to open port 8019. Every computer that is running an IceLib-based client application must be able to access port 8019 of all Session Managers to which they are allowed to connect, as well as port 8019 of any CIC servers.

For IceLib-based applications connecting over the Internet, either port 8952 or port 8951 need to be opened on a server running Session Manager (including the CIC server or servers) for WebSocket connections between the application and Session Manager. Ports 8952 or 8951 must not be publicly available over the Internet. Instead, a publicly available reverse proxy must be in place which would direct traffic to the appropriate Session Manager server. See Section [7.11 Connecting IceLib Applications over the Internet](#) for details.

QoS Driver Installation

By default, the PureConnect QoS driver is silently installed and the certificate is added to the list of Trusted Publishers. 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.

Installing Off-Server Session Manager

The installation of Session Manager does the following operations:

- Copies the Session Manager files to the installation target directory.
- Creates certificates to connect with the CIC server.

Important!

Ensure that you trust the certificate in Interaction Administrator before restarting the Session Manager host so that it can connect to the CIC server successfully when restarted. For more information, see [Certificates for Off-Server Session Manager](#).

- Creates and starts the following Session Manager services
- **IC Session Manager Service**
- **ININ Windows Service Monitor**

Use the following steps on each server where off-server Session Manager is being installed:

1. If you have not already done so, follow the procedure on the Product Information website at <https://my.inin.com/products/cic/Pages/Releases-and-Patches.aspx> to download and copy the .iso file to a file server on the CIC network.
2. On the server where you are installing off-server Session Manager, run Install.exe from the \Installs directory on the shared network resource.
3. On the **Off-Server Components** tab, select the check box for the off-server Session Manager install, and then click **Install**. The **Welcome** dialog box appears.
4. Click **Next**. The **Custom Setup** dialog box appears.
5. Click **Next**.
6. The **Domain User Validation** dialog box appears.
7. Enter the user name, password, and domain that you want to associate with this instance of Session Manager.

Note:

The information you enter is used to connect to the CIC server and as the account under which the local service process runs. This account must be a CIC account that is bound to an Windows domain account. The Windows domain user account must have local administrator rights for the server on which you are installing Session Manager.

8. Click **Next**.

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

Note:

If the installation is utilizing WAN-switchover, the CIC server name specified must be the particular CIC server of the WAN-switchover pair to which this off-server Session Manager instance is to stay connected. For more information, see [WAN-Switchover with Off-Server Session Manager Machines](#).

9. In the **IC Server** box, enter the name of the active CIC server.

Important!

If you are using CIC in a WAN-Switchover configuration, you must specify the CIC server of the WAN-Switchover pair to which the off-server Session Manager instance is to stay connected. For more information about WAN-Switchover, see [WAN-Switchover with Off-Server Session Manager Machines](#).

After installation, you must then configure the switchover mode of the off-server Session Manager. For more information, see [Specify Switchover Behavior](#).

10. (optional) In the **User** and **Password** boxes, enter CIC credentials.

11. Click **Next**.

The **Ready to install IC Session Manager** dialog box appears.

12. Click **Install**.

After the installation completes, the final dialog box appears.

13. Click **Finish**.

14. Use Interaction Administrator to trust the Session Manager certificate for the CIC server.

15. Restart the Session Manager host.

Encryption Key Management for Off-Server Session Managers

Encryption key management for off-server Session Manager is as described in Section [4.2 Encryption Key Management for On-Server Session Managers](#).

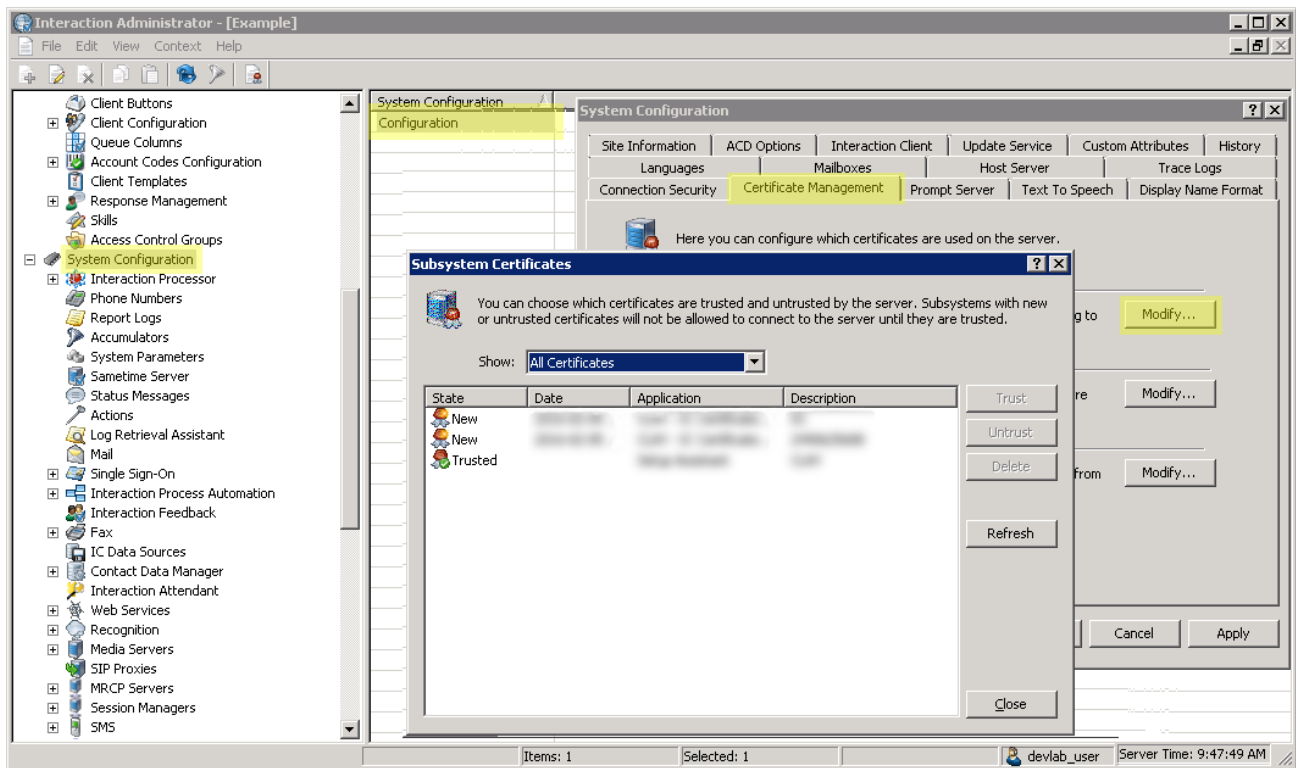
Certificates for Off-Server Session Manager

All connections to Notifier that originate from CIC products not hosted on the CIC server use SSL and certificates for authentication. As part of the off-server Session Manager installation process, the installation program creates the necessary certificates for a connection to the CIC server that you specify in CIC server installation wizard.

Trust Off-Server Session Manager Certificate

Once the Session Manager installation is complete, trust the certificates created by the installer through Interaction Administrator:

1. Start Interaction Administrator and log on with CIC administrator credentials.
2. In the left pane of the **Interaction Administrator** window, select the **System Configuration** container.
3. In the right pane of the **Interaction Administrator** window, double-click **Configuration**.
The **System Configuration** dialog box appears.
4. Select the **Certificate Management** tab.
5. In the **Subsystem Certificates Configuration** group, select the **Modify** button.
The **Subsystem Certificates** dialog box appears.



6. Select a Session Manager certificate in the **New** state and then select the **Trust** button.

The CIC server sets the certificate state to **Trusted** and the Session Manager server that uses that certificate can establish Notifier connections.

7. Select the **Close** button.

Session Manager Certificates for non-WAN-Switchover Pair

With a CIC switchover pair, when WAN-switchover is not being implemented, a separate certificate is required for each CIC server. However, if switchover is configured after the off-server Session Manager installation is performed, then the installation program does not create a certificate allowing the off-server Session Manager to connect to the backup server. To create a certificate allowing the off-server Session Manager to connect to the backup server, execute the following from the command line in the same directory where Session Manager is installed:

```
gensslcertsu r BackupCICServerName CICUserName CICUserPassword
```

Executing the gensslcertsu command creates a certificate against the backup CIC server. To trust this certificate, run Interaction Administrator again and perform the same steps for trusting a certificate on the CIC server in [Trust Off-Server Session Manager Certificate](#).

Now that you have created and trusted certificates on both the primary and backup CIC server, the off-server Session Manager instance is able to connect to either server.

Custom Authority Certificates

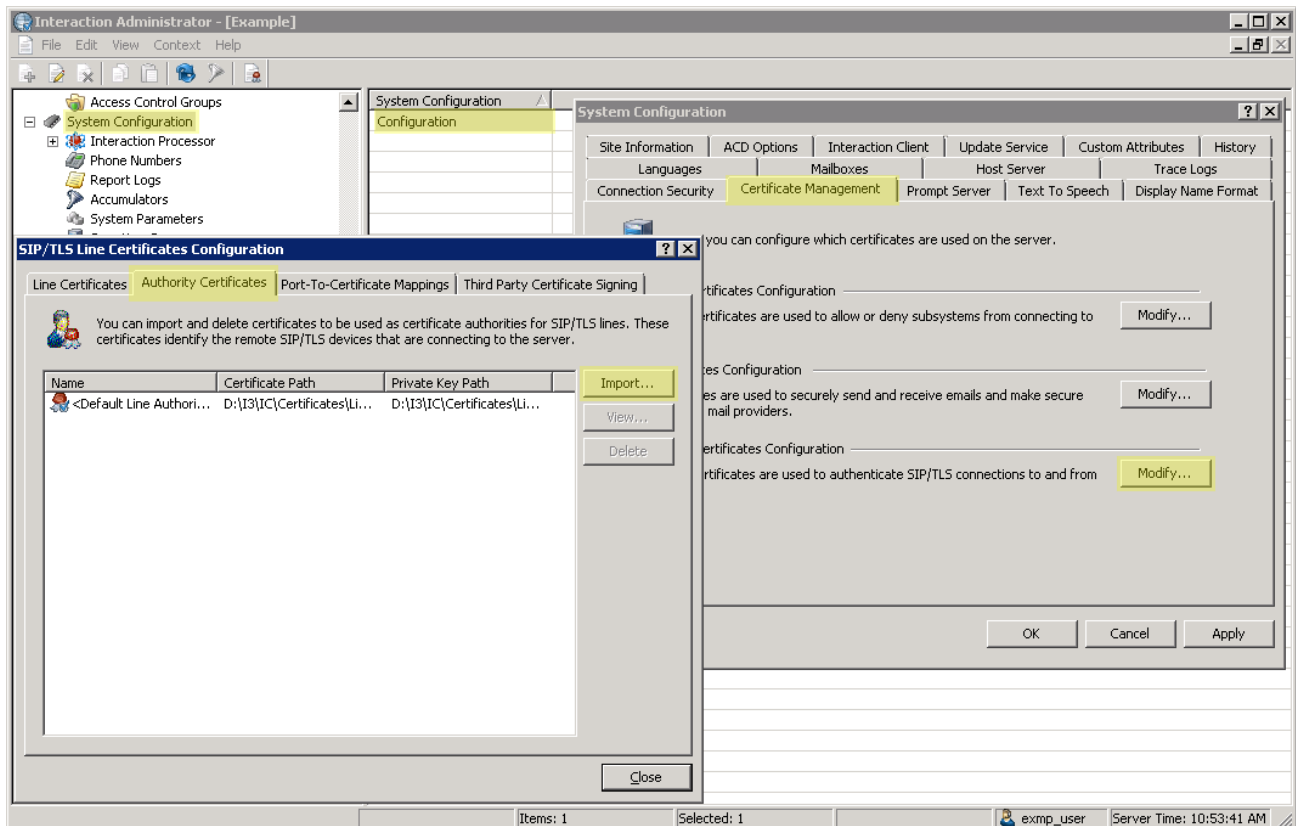
The default certificate authority certificate stored in the CIC server is used to sign all certificates. In some cases, customers might have security and/or regulatory requirements to use certificates signed by another certificate authority, such as VeriSign. CIC allows importing authority certificates for use in signing certificates used by Session Manager.

To import additional authority certificates, do the following steps:

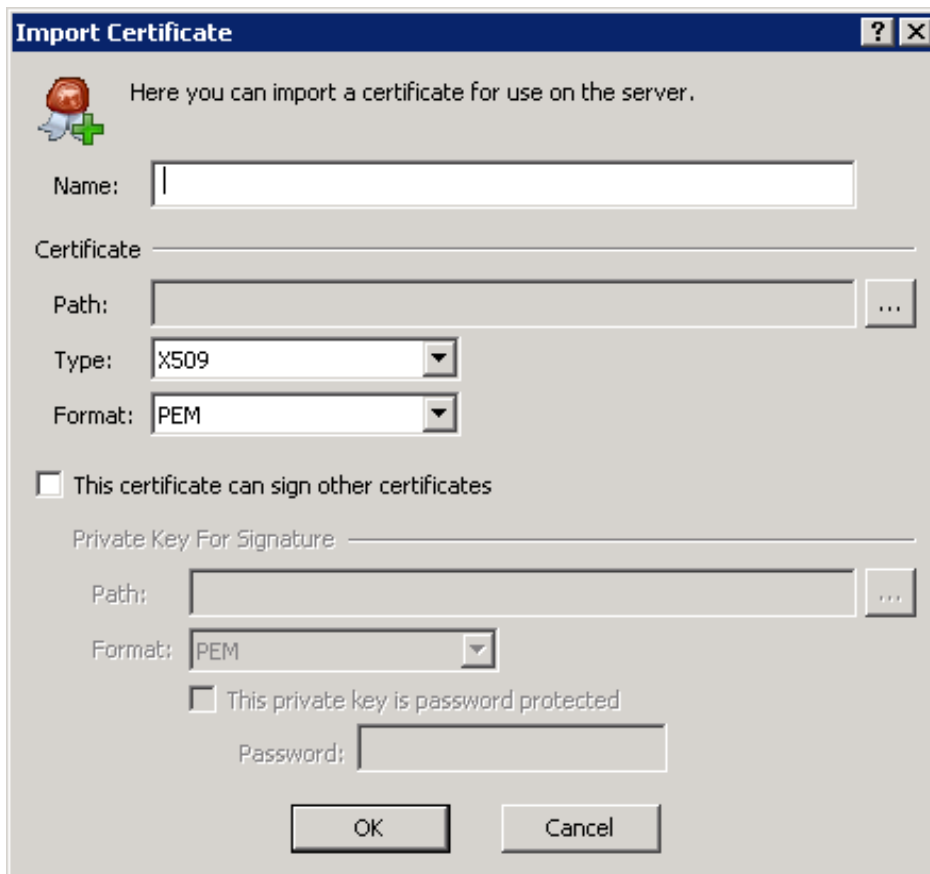
1. Start Interaction Administrator and log on with CIC administrator credentials.
2. In the left pane of the **Interaction Administrator** window, select the **System Configuration** container.
3. In the right pane of the **Interaction Administrator** window, double-click **Configuration**.
The **System Configuration** dialog box appears.
4. In the System Configuration dialog box, select the **Certificate Management** tab.
5. In the **SIP/TLS Line Certificates Configuration** group, select the **Modify** button.

The **SIP/TLS Line Certificates Configuration** dialog box appears.

6. Select the **Authority Certificates** tab.
7. Select the **Import** button.



The **Import Certificate** dialog box appears.



8. Specify the location and details for the necessary authority certificate and the private key and then select **OK**.

For more information about the controls on the **Import Certificate** dialog box and what is required to import the certificate, see [Import a certificate](#) in *Interaction Administrator Help*.

Applying Updates to Off-Server Session Manager Machines

In order to apply a patch or release to an off-server Session Manager machine, an automatic or manual process can be used.

Automatic Process

If the off-server Session Manager host has its Interactive Update application configured to pull updates from the CIC server, then an automatic update process can be used.

- Apply the update installation for the CIC server on the CIC server, following the usual procedure.
- For the off-server Session Manager host, do one of the following actions:
 - Configure and allow Interactive Update to automatically apply the update when the next scheduled check for updates occurs.
 - Manually use the Interactive Update application to check for updates and apply them.

Manual Process

If the off-server Session Manager host does not have Interactive Update configured to pull updates from the CIC server, then use a manual update process.

- Install the CIC server update on the CIC server, following the usual procedure.
- On the off-server Session Manager host, manually install the Session Manager update.

24x7 Environments

24-hour environments might prefer rolling updates, in which case Interactive Update on the off-server Session Manager machines must not be configured to pull updates automatically from the CIC server. If the deployment is properly designed for N+1, then it is possible to manually update each off-server Session Manager host individually, since the remaining off-server Session Manager hosts handle the load while one is undergoing the update. There would be a brief interruption while any connected clients reconnected to the remaining Session Manager hosts. This approach allows updating of each off-server Session Manager host without requiring the entire contact center to be down.

Session Manager Configuration and Monitoring

You can use Interaction Administrator to configure settings that affect the operation of Session Manager. Use Interaction Supervisor to monitor client connections that are in progress across the Session Manager instances of an implementation. These configuration and monitoring operations are described in the following sections.

- [Configuring Session Manager Instances](#)
- [Restrict Company Directories](#)
- [Specify an Alternate Directory for Transfers](#)
- [Configure High and Low Watermarks for Client Application Logons](#)
- [View Session Manager Connections in Interaction Supervisor](#)
- [View Connection Information for Interaction Desktop](#)
- [Manage the Off-Server Session Manager](#)
- [Windows Default Behavior with Authentication and Delegation](#)
- [IceLib Outgoing Bandwidth Limiting](#)
- [Changing CIC Time Zone](#)
- [Connecting IceLib Applications over the Internet](#)
- [Monitor Session Manager instances](#)

Configuring Session Manager Instances

Session Manager instances are configured through Interaction Administrator. These settings enable management of the existence of each Session Manager instance, identity, and regionalization settings.

Once a Session Manager instance has had its certificate trusted and then successfully connected to the CIC server, Interaction Administrator automatically displays that Session Manager in the **Session Managers > Servers** container. The list in that container serves as a roster of the available Session Managers, which informs IceLib-based applications about available Session Manager instances for connections.

If a trusted Session Manager instance is down, Interaction Administrator still displays its entry. This approach enables an IceLib-based application to cache the exact roster of available Session Managers, even if an off-server Session Manager was down for maintenance at the time that the IceLib-based application last connected. One advantage is that IceLib can trust the exact roster it receives and replace its old cache, rather than being forced to merge the roster into the cache—as it did in CIC 3.0—to remember offline off-server Session Manager instances.

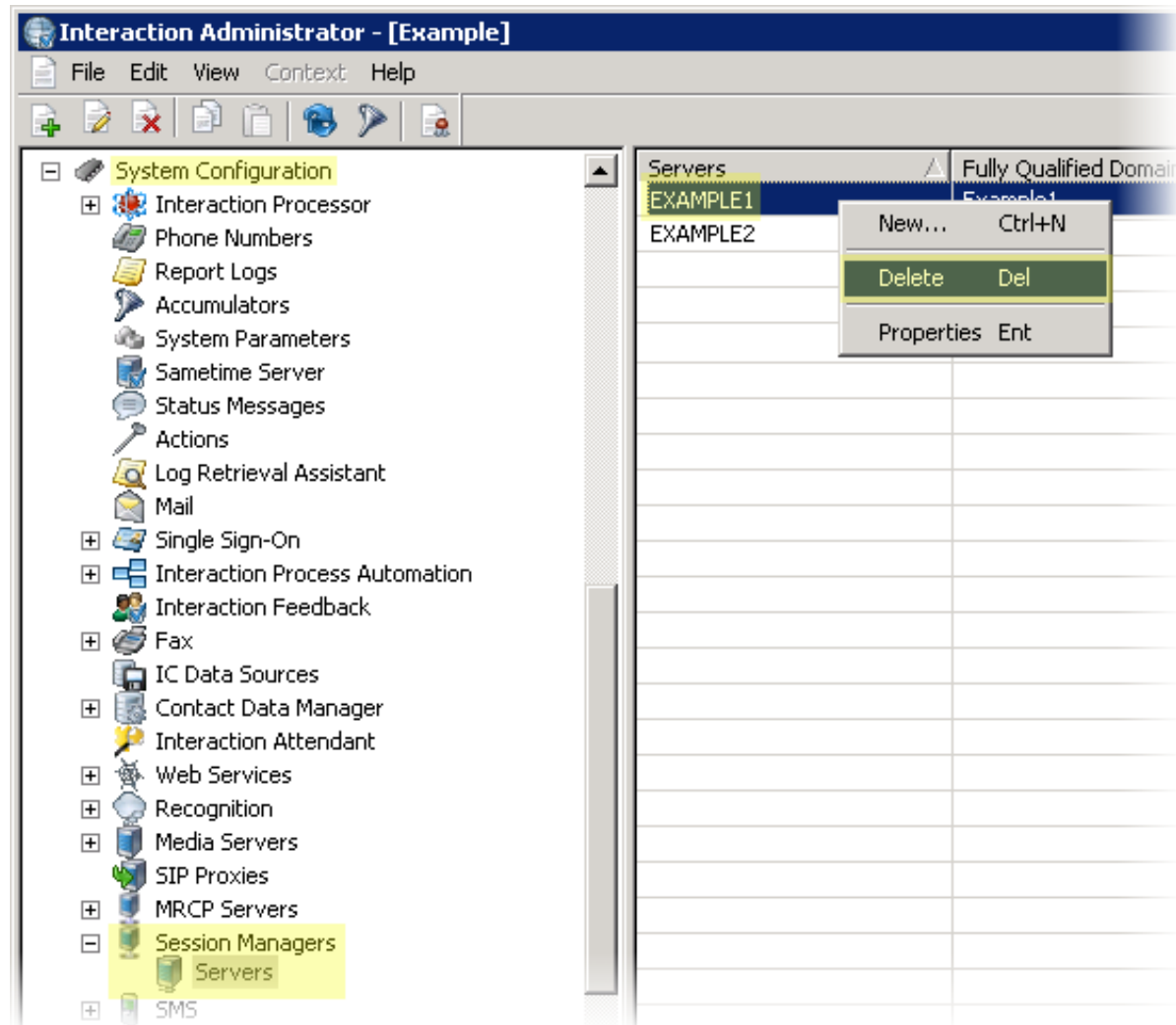
Retiring a Session Manager Instance

To permanently retire a Session Manager instance, do the following steps:

1. Ensure that the off-server Session Manager is off by stopping the following services on its host:
 - **ININ Windows Service Monitor**
 - **IC Session Manager Service**
2. Open Interaction Administrator and log on with CIC administrator credentials.
3. In the left pane of the **Interaction Administrator** window, select **System Configuration > Session Managers > Servers**.

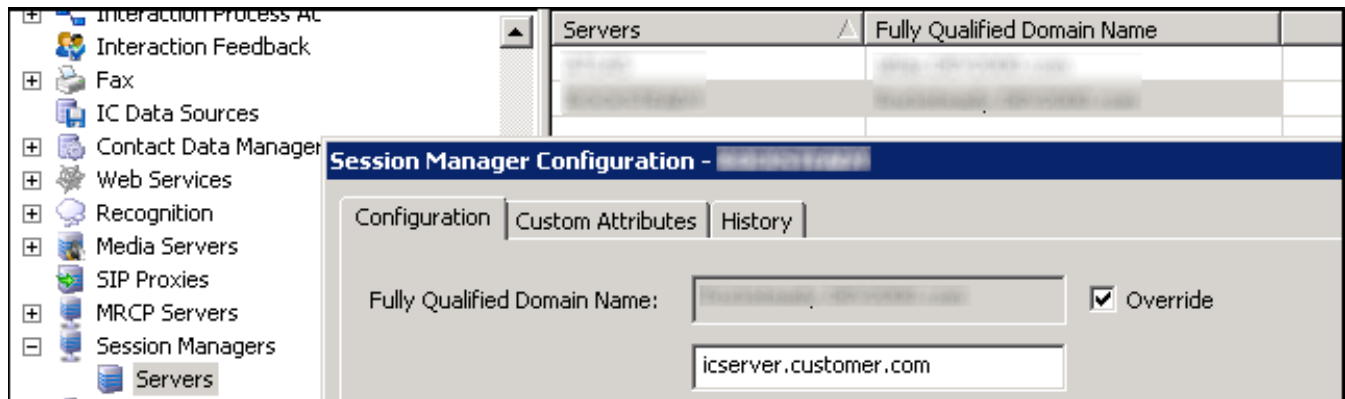
The right pane displays the current list of Session Manager instances.

4. In the right pane, right-click a Session Manager instance that you want to delete and select **Delete** from the resulting context menu.



Setting Session Manager Identity

When the roster of available Session Manager instances is returned to IceLib-based applications, each Session Manager is identified with the exact network name for IceLib to use in its connection attempts. This Session Manager identifier defaults to the Fully Qualified Domain Name (FQDN) that the Session Manager instance had for itself; however, you can override it through the Interaction Administrator entry for that Session Manager instance and specify whatever value is most appropriate for a given installation. The FQDN must be accessible from all domains from which IceLib-based applications are used to connect.



Use Regionalization with Selection Rules

You can associate Session Manager instances with a **Location** entry in Interaction Administrator to support regionalization. This configuration enables connections for users/stations associated with a particular **Location** entry to prefer Session Manager instances associated with **Location** entries based on Selection Rules. The IceLib-based application gives preference to the **Location** entry associated with the **Station** being used to connect (if any), and then to the **Location** entry associated with the CIC user. Then, the **Default Location** entry is used as a fallback. IceLib-based applications use the Selection Rule configured for the resulting selected **Location** entry to prioritize the roster of available Session Manager instances.

The screenshot shows the 'Session Manager Configuration' dialog box with the 'Configuration' tab selected. It contains fields for 'Fully Qualified Domain Name' and an 'Override' checkbox. Under 'Connections', there are three radio buttons: 'Use default behavior' (selected), 'Accept all connections', and 'Do not accept new connections (Maintenance Mode)'. Under 'Location', there are two radio buttons: 'Use the location of: dionysus' and 'Use this location:'. The 'Use this location:' option is selected, and a dropdown menu is open showing a list of locations: '<Default Location>', 'Loc1', 'Loc2', 'Loc3', 'Loc4', and 'Loc5'.

The application uses the Selection Rule configured for the **Location** entry as a guide to prioritize the best Session Manager instances. If the prioritized ones were not available, and the Selection Rule allows for connecting to Session Managers in any other locations, then connections to instances in non-prioritized locations will not be prevented.

By default, the off-server Session Manager server uses the **Location** of the CIC server.

For more information about how clients select Session Manager instances, see [Section 2.3.1 Client Application Selection with Regionalization and Selection Rules](#).

The Session Manager instances that are associated with a given **Location** appear in the configuration for that **Location** in the **Regionalization > Locations** container in Interaction Administrator.

The screenshot shows the Interaction Administrator interface. On the left is a tree view with nodes like 'Peer Sites', 'Lines', 'Line Groups', 'Stations', 'Managed IP Phones', 'Audio Sources', 'Server Parameters', 'Structured Parameters', 'Regionalization', 'Locations', and 'Default Regionalization'. The 'Locations' node is selected. On the right, a table lists locations:

Location Name	Description
<Default Location>	The system default location
Location1	
Location2	

Below the table, the 'Locations Configuration - Location2' dialog box is open, showing tabs for 'Configuration', 'Users', 'Communication', 'Endpoints', 'Server Endpoints', 'Custom Attributes', and 'History'. The 'Configuration' tab is active, showing sections for 'Media Servers', 'SIP Proxies', and 'Session Managers'. Each section contains the text 'There are no items to display.'

Specify Switchover Behavior

In a switchover environment, off-server Session Manager instances also have an option for whether they always connect to the current primary CIC server, or if they stay pinned to a particular CIC server.

Genesys recommends that you leave this setting as the default value, which is to configure the off-server Session Manager instances to switch and stay connected to the current primary CIC server.

The option for always connecting to the particular CIC server specified at installation is much less common and is left available for backward compatible behavior for some WAN-switchover sites. Genesys does not recommend the “no-switch” mode for recent CIC releases.

Switchover Behavior:

☒ Always reconnect to the primary IC server on switchover

☐ Always connect to:

SERVER1

Configure Session Manager Selection Rules

In Interaction Administrator, you can configure **Locations** to have Session Manager Selection Rules. These Selection Rules can be used to prioritize the **Location** of Session Managers to which a user in that **Location** would connect. For more information on configuring Session Manager Selection Rules, see [Client Application Selection with Regionalization and Selection Rules](#).

You can add or edit a Selection Rule in Interaction Administrator under the **Regionalization > Selection Rules** container.

Selection Rule Configuration - Example

GeneralCustom AttributesHistory

Prioritized Location list

Loc1
Loc2
Loc3
Load-Balanced Group
Loc4
Loc5

Add...

Remove

Move up

Move down

Group selected

Ungroup selected

Excluded Location list

☐ Do not use any other Locations

☒ Use any Location, except the following:

<Default Location>

Add...

Remove

Restore defaults

OK

Cancel

Select Values

Add Locations

<This Location>
<Other Locations in Audio Path>
<IC Server Location>

OK

Cancel

Each Selection Rule can have a list of **Prioritized Locations** and a list of **Excluded Locations**.

Use the **Add Locations** dialog box to add existing **Locations** to the **Prioritized Locations list** group box. CIC processes **Locations** in the **Prioritized Locations list** group box from top to bottom.

The **Add Locations** dialog box contains unassigned **Locations** and special Location variables that are unique to Selection Rules:

Table 6 Session Manager Selection Rule Variables

Selection Rules Location variable	Description
<This Location>	This variable represents the location to which the Selection Rule is applied. For example, if you configure a Session Manager Selection Rule on Location1 , then instances of <This Location> in that Selection Rule return Location1 .
<CIC Server Location>	The Location of the CIC server.
<Other Locations in Audio Path>	Session Manager does not use this Location variable in its Selection Rules. Session Manager ignores any instance of this Location variable in its Selection Rules.

You can group multiple locations using the **Group selected button** so as to give Session Manager instances in those Locations the same priority level and cause CIC to select one Session Manager instance from the Locations within that group.

The **Excluded Locations list** group enables you to specify the following Selection Rules behavior:

- **Do not use any other Locations** This option specifies that the CIC server can consider and connect to only Session Manager instances in the **Prioritized Locations list** group box.
- **Use any Location, except the following** This options specifies that the CIC server can consider and connect to any Session Manager instance, in any location, except for those Locations specified in the list box.

For more information about Selection Rules, see [Client Application Selection with Regionalization and Selection Rules](#).

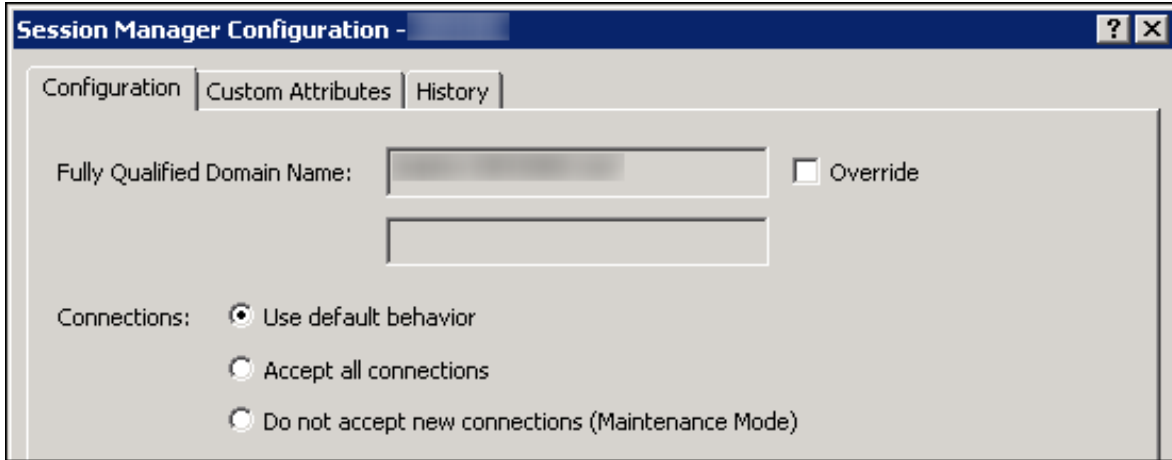
Once you have configured a Selection Rule, you can apply it to a Location as its Session Manager Selection Rule. To do so, edit a **Location** in the **Regionalization > Locations** container in Interaction Administrator, and then select a Selection Rule in the **Session Manager** list box located in the **Selection Rules** section.

The screenshot shows a window titled "Locations Configuration - Example". It has several tabs: "Configuration", "Users", "Communication", "Endpoints", "Server Endpoints", "Custom Attributes", and "History". The "Configuration" tab is active. Inside, there is a "Description:" label followed by a text input field. Below that is the "SNTP Server:" label with two radio button options: "Use IC Server" (which is selected) and "Other:" followed by a text input field. Under the "Selection Rules" section, there are two dropdown menus. The first is labeled "Media Server:" and has "<Default Selection Rule>" selected. The second is labeled "Session Manager:" and has "Example" selected.

By default, a Location uses the **<Default Session Manager Selection Rule>** for its Session Manager Selection Rule. **<Default Session Manager Selection Rule>** consists of only **<This Location>** as the top priority Location, and then includes all other Locations after that with no excluded Locations.

Configure a Session Manager's Accept Connections Status

Using Interaction Administrator, you can configure a Session Manager instance to accept client connections with the **Connections** option buttons:



The screenshot shows the 'Session Manager Configuration' dialog box with the 'Configuration' tab selected. It features three tabs: 'Configuration', 'Custom Attributes', and 'History'. The 'Configuration' tab contains a 'Fully Qualified Domain Name' field with a text input box and an 'Override' checkbox. Below this, the 'Connections' section has three radio button options: 'Use default behavior' (selected), 'Accept all connections', and 'Do not accept new connections (Maintenance Mode)'.

The **Connections** options are as follows:

- **Use default behavior** - This setting has a different meaning depending on whether the Session Manager is an on-server Session Manager or an off-server Session Manager.
 - On-server Session Manager - The default behavior depends on if there are available off-server Session Managers or not:
 - Available - Session Managers do not accept connections.
 - Not available Session Managers accept connections.
 - Off-server Session Manager - The default behavior is to accept connections.
- **Accept all connections** - With this setting, Session Manager accepts connections regardless of whether it was an on- or off-server Session Manager and if any off-server Session Managers are available.
- **Do not accept new connections (Maintenance Mode)** - With this setting, Session Manager stops accepting new connections. If there are existing connections to the Session Manager instance, those will remain live until either those clients disconnect themselves or the Session Manager instance is restarted to remove those connections.

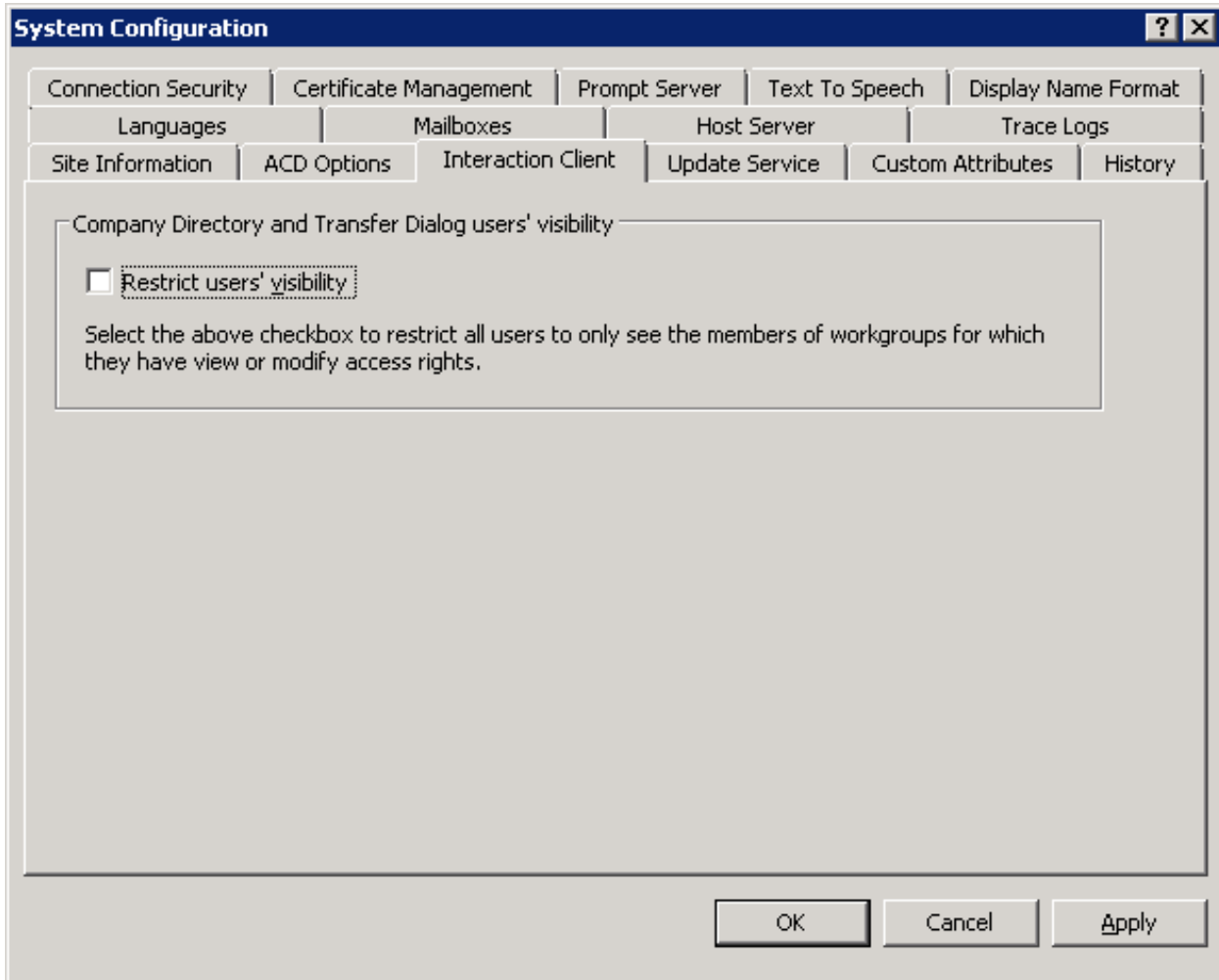
Restrict Company Directories

In Interaction Administrator, use the **Interaction Client** tab of the **System Configuration** dialog box to configure visibility settings for users of Interaction Desktop.

1. Open Interaction Administrator and log on with CIC administrator credentials.
2. In the left pane of the **Interaction Administrator** window, select the **System Configuration** container.
3. In the right pane, double-click the **Configuration** item.

The **System Configuration** dialog box appears.

4. Select the **Interaction Client** tab.



5. Set the **Restrict users' visibility** check box for the necessary behavior:
 - Enabled – Users of CIC clients see only the members of workgroups for which they have view or modify access rights in the Company Directory or when they are transferring a call by dragging and dropping the call on a directory entry.
 - Disabled – Users of CIC clients see all members of the organization in directory lists.
6. Select **OK**.
7. Restart Session Manager for this setting to take effect.

Specify an Alternate Directory for Transfers

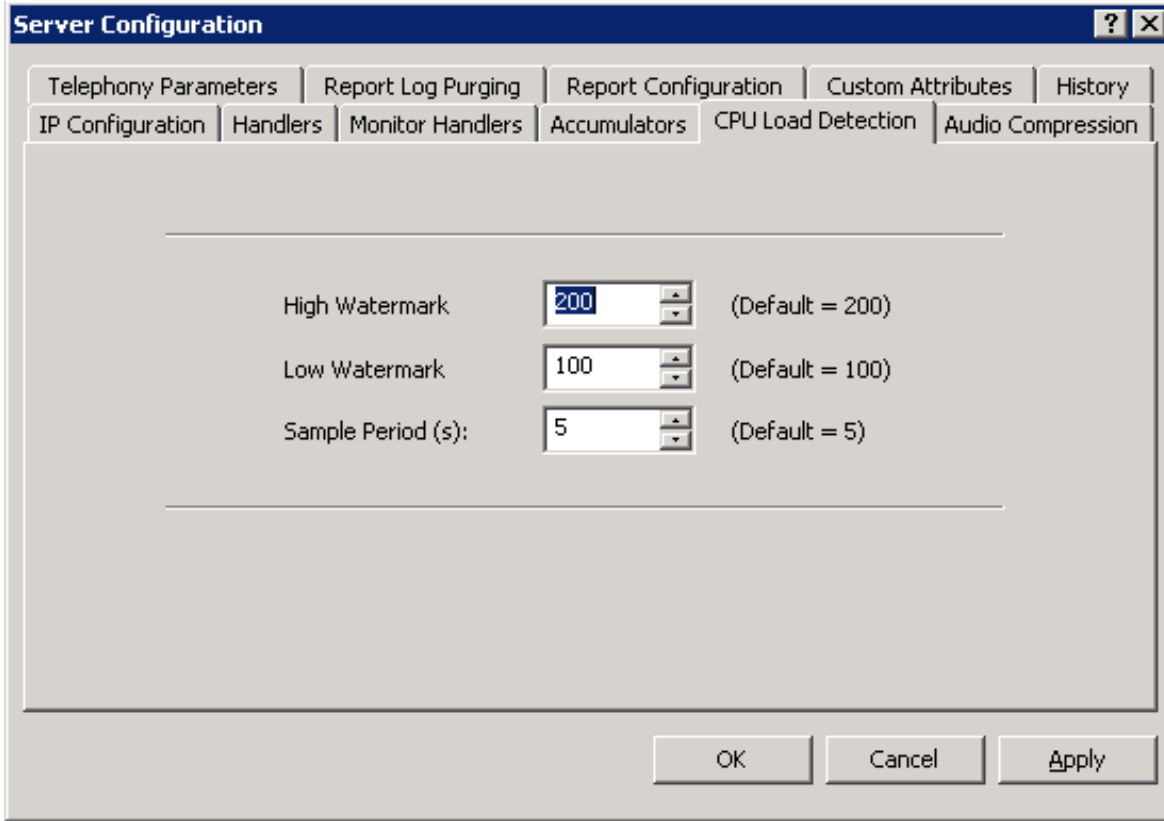
You can specify the directories from which Session Manager pulls the contact results that appear in the Transfer dialog in CIC clients. By default, the Company Directory is included in the search.

To specify one or more alternate directories, use the server parameter, TransferDialogDirectories, in the **Server Parameter** container of Interaction Administrator. To specify multiple directories, separate the directory names with a pipe (|) character. For more information about server parameters, see *Interaction Administrator Help*.

Configure High and Low Watermarks for Client Application Logons

You can specify high and low watermarks (thresholds) in Interaction Administrator so that Session Manager rejects client logon attempts during periods in which Remoco indicates that the CIC server has exceeded its high load state.

To set the watermarks, use the **CPU Load Detection** tab of the **Server Configuration** dialog box in Interaction Administrator.



The screenshot shows the 'Server Configuration' dialog box with the 'CPU Load Detection' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: 'Telephony Parameters', 'Report Log Purging', 'Report Configuration', 'Custom Attributes', 'History', 'IP Configuration', 'Handlers', 'Monitor Handlers', 'Accumulators', 'CPU Load Detection', and 'Audio Compression'. The 'CPU Load Detection' tab is active, showing three settings: 'High Watermark' with a value of 200, 'Low Watermark' with a value of 100, and 'Sample Period (s)' with a value of 5. Each setting has a text box with a value, a small up/down arrow button, and a default value in parentheses. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Setting	Value	Default
High Watermark	200	200
Low Watermark	100	100
Sample Period (s)	5	5

These settings affect more subsystems than just Session Manager. For more information, see the "CPU Load Detection" and "Configure CPU load detection for your CIC server" topics in *Interaction Administrator Help*.

View Session Manager Connections in Interaction Supervisor

Interaction Supervisor is a plug-in component that provides a single interface for the following information:

- Real-time bar chart and line graph displays to monitor agent and workgroup activities
- Interaction events
- CIC system and queue statistics

Interaction Supervisor contains a **Session Managers** view, which displays status statistics collected by Session Managers running multiple clients on the CIC server. Additionally, the **Session Managers** view enables you to open a detail dialog to interrogate the actual sessions that are connected.

When client applications disconnect from Session Manager without performing an explicit logout, the statistics displayed in this **Session Managers** view of Interaction Supervisor continue to include sessions for those client applications for a few minutes, as a side effect of internal Session Manager caching algorithms.

Note:

An Interaction Supervisor add-on license is required. See the *PureConnect Installation and Configuration Guide* for instructions on installing Interaction Supervisor.

IC Business Manager

File Edit View Workspaces Tools Window Help

New

Workspaces

Session Managers

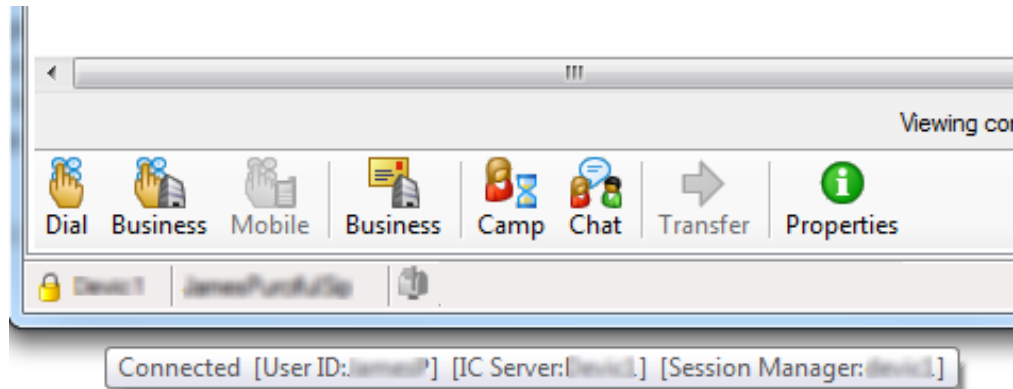
	Session count
IndyDevice1	
IndyDevice1 [69]	217
Interaction Client Mobile Edition	0
Outlook Addin	0
Salesforce CTI	0
Interaction Mobile Web Client	0
Interaction Fax .NET Edition	0
Admin.Net	4
IC Business Manager	4
IC Server Manager	1
Interaction Client .NET Edition	183
Interaction Voicemail Player	3
Interaction Web Client	19
TutorialExample.vshost	0
iSupport SmartClient Integration	3

IndyDevice1 | FredericBrunner@P | 0

Session count							
Session ID	User ID	User Name	IceLib Version	User Extension	Login Time	Client ID	Station ID
2669066	jeff.gerardot	Gerardot, Jeff	4.0.17.338	109	9/13/2011 9:41:12 PM	JEFFGERARDOTPC	JEFFGERARDOTSP
2969066	Jonathan.Keller	Keller, Jon	4.0.17.277	8780	9/13/2011 9:41:12 PM	JKELLER2	JonathanKeller@P
3069066	Ananth.Durvasi	Durvasi, Ananth	4.0.17.369	8737	9/13/2011 9:41:12 PM	MATCHBOX	ananthdurvasi@P
6569066	david.wilson	Wilson, Joe	4.0.17.290	8363	9/13/2011 9:41:19 PM	DAVIDWILSONPC	JOEWILSON@P
6669066	Kevin.O'Connor	O'Connor, Kevin	4.0.17.290	111	9/13/2011 9:41:19 PM	KEVINOPCDEV	KevinO'Connor@P
9469066	Robert.Adams	Adams, Robert	4.0.17.290	4754	9/13/2011 9:41:24 PM	ROBERTADAMSPC	ROBERTADAMS@P
10269066	Ricardol.Vergin	Vergin, Ricardol	4.0.17.290	8762	9/13/2011 9:41:25 PM	RICAROLVPC	RICAROLVERGIN@P
10869066	Mark.Milford	Milford, Mark	4.0.17.330	4048	9/13/2011 9:41:25 PM	MARKMILFORDPC	MARKMILFORD@P
11469066	Shumon.Madhumder	Madhumder, Shumon	4.0.17.338	4136	9/13/2011 9:41:26 PM	SMADHUMDERPC	shumonmadhumder@P
13869066	raminder.gill	Gill, Raminder	4.0.17.290	8263	9/13/2011 9:41:30 PM	VALSANT	ramindergill@P
16369066	Sushil.Singh	Singh, Sushil	4.0.17.330	8542	9/13/2011 9:41:40 PM	SUSHIPC	SUSHILSINGH@P
16869066	ben.zackel	Zackel, Ben	4.0.17.290	8764	9/13/2011 9:41:40 PM	BENZCKELPC	benzackel@P
18469066	Aaron.Ray	Ray, Aaron	4.0.17.368	8611	9/13/2011 9:41:46 PM	AARONRAYPC	AaronRay@P
19069066	Rabiah.Ouldroughi	Ouldroughi, Rabiah	4.0.17.338	8672	9/13/2011 9:41:47 PM	RABIAH@PC	rabiahouldroughi@P
27569066	Rick.Lyndon	Lyndon, Rick	4.0.17.338	8537	9/14/2011 7:06:14 AM	RICHAROLYNDONPC	RickLyndon@P

View Connection Information for Interaction Desktop

For diagnostic purposes with larger implementations, it can be helpful to see to which Session Manager instance an Interaction Desktop is connecting. The machine names of the CIC server and Session Manager instance to which the application is connected are displayed by hovering the cursor over the server name in the lower left-hand corner of the status bar of the application.



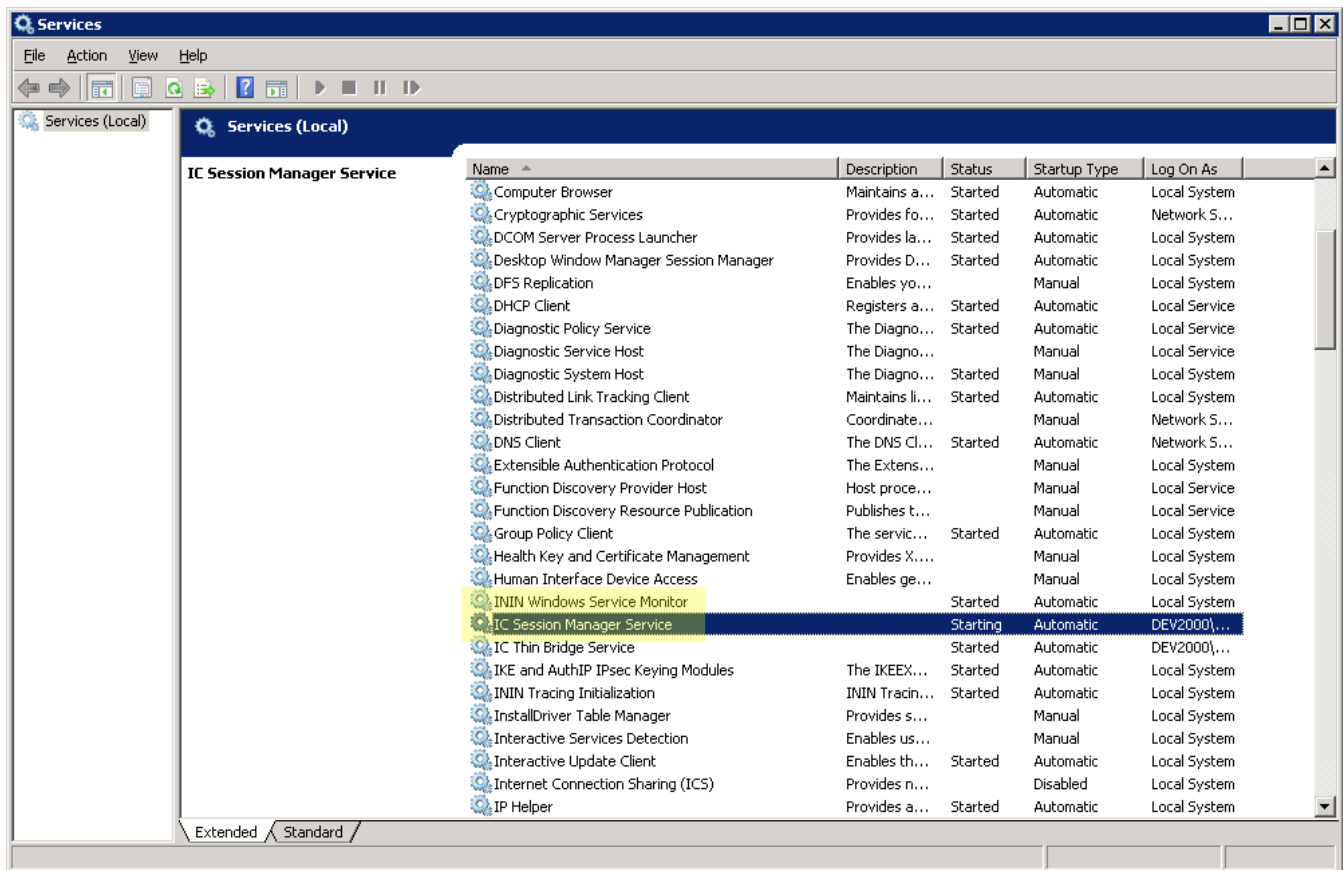
Manage the Off-Server Session Manager

The installer for the off-server Session Manager creates and registers two services with the Service Control Manager in Windows:

- **IC Session Manager Service**
- **ININ Windows Service Monitor**

IC Session Manager Service executes the Session Manager application. The **ININ Windows Service Monitor** service overcomes a limitation in the Service Control Manager to restart **IC Session Manager Service** when it shuts down after losing a Notifier connection. When the CIC server shuts down or a switchover occurs, Session Manager must shut down, restart, and connect to Notifier. In this case, **ININ Windows Service Monitor** determines that **IC Session Manager Service** is not running and restarts it within 30 seconds.

If you want to disable an off-server Session Manager, then shut down both services from Service Control Manager.



Windows Default Behavior with Authentication and Delegation

Windows authentication behavior is not specific to Customer Interaction Center; it is a standard behavior in Windows but, since it is not widely known, it is useful to describe it here. When a client application uses Windows Authentication to connect to a Session Manager internally, the application uses the standard Windows OS methods to negotiate an identity without ever sending a password from the local machine to the remote machine. It is the same method used, for example, by many web browsers and ASP.NET applications to impersonate the identity of the remote web browser.

By default, Windows does not allow this type of identity impersonation to be used as a means to *chain* that identity to a third machine. Consider the scenario of a browser running on \\YourLocalMachine that is connecting to an ASP.NET web service running on \\YourWebServer where that ASP.NET web service is an IceLib-based application. In that scenario, it is fine for the ASP.NET application to run under the identity of the Windows account that is used to log on at \\YourLocalMachine. However, if the ASP.NET app that is IceLib-based wants to log on to a Session Manager running on \\YourCICServer, Windows (by default) does not allow it. In technical terms, a Windows process is not allowed to take a set of credentials obtained through remote impersonation and send it to a third machine. If your Session Manager is running directly on \\YourWebServer, then it works, but if your Session Manager is running on a different machine, then (by default) it does not. This behavior is by design for ASP.NET.

If you have a situation where you need your ASP.NET service to be able to log on to a Session Manager using Windows Authentication, then you have some options. One option is what was already mentioned: to run the ASP.NET service and the Session Manager on the same physical machine. That approach is not always a good option though, since doing so may have resource impact and firewall/DMZ impact, and so on. Another way to solve this issue is to use the Active Directory editor to mark the relevant machine accounts and/or relevant user accounts as being “trusted for delegation”. The following Microsoft TechNET article includes additional information:

[http://technet.microsoft.com/en-us/library/cc757194\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc757194(WS.10).aspx)

IceLib Outgoing Bandwidth Limiting

To avoid the possibility of Session Manager sending too many client messages, saturating bandwidth between Session Manager and IceLib clients, and leading to packet loss and dropped client connections, functionality has been added to enable the limiting of Session Manager’s outgoing bandwidth to IceLib clients.

When the rate of Session Manager’s outgoing IceLib messages exceeds the configured limit, messages will be queued up to be sent out over time at a rate that will not exceed the configured limit. Message types are divided up into different levels of priority based on how critical the message is to client functionality. High priority messages will be sent as quickly as possible. Medium priority messages (namely non-high-priority responses) will be sent as quickly as possible after high priority messages, and a special effort will be made to not delay responses past a minute to avoid a timeout in IceLib. All other message types will be sent as quickly as possible after the high and medium priority messages have been given their due.

Bandwidth limiting will not always be on to avoid unnecessary delays when the outgoing message rate is not exceeding the configured limit. The system will recognize when the rate limit is exceeded to activate the limiting functionality, and then recognize when outgoing messages drop back below the rate limit to deactivate the limiting functionality.

Configuration

The IceLib Outgoing Bandwidth Limiting functionality can be configured using a number of server parameters.

Table 7 IceLib Outgoing Bandwidth Limiting Server Parameters

Server Parameter	Value	Default	Description
Bridge Message Bandwidth Limiter Enabled	Yes/No	No	Enable/disable the bridge message bandwidth limiting functionality. Disabled by default.
Bridge Message Bandwidth Limiter Total Outgoing Bytes Per Interval	Positive Integer (64 bit) greater than 50000	500000	Total bytes that Session Manager will be able to send out per interval. The 500000 default with 1000 millisecond interval represents 4 Mbps.
Bridge Message Bandwidth Limiter Interval Milliseconds	Positive integer between 100 and 5000	1000	Timer interval for collecting and limiting outgoing bandwidth.
Bridge Message Bandwidth Limiter Medium Priority Outgoing Bytes Per Interval Percentage	Positive integer between 20 and 80	50	The percentage of the total bytes set in "Bridge Message Bandwidth Limiter Total Outgoing Bytes Per Interval" minus bytes used for high priority messages for that interval that will be used for Medium Priority Queue messages.
Bridge Message Bandwidth Limiter High Priority Messages	(<objectType1>, <eventId1>), (<objectType2>, <eventId2>), ...	See High Priority Messages	Makes it possible to add or remove message types from the high priority message list. List of message types in form of (<objectType>, <eventId>), (<objectType>, <eventId>), Example: CreateSession would be (168,1). To remove a message from the high priority message list, make the event ID a negative value. So, for example, to remove CreateSession, the value would look like (168,-1).
Bridge Message Bandwidth Limiter Medium Priority Messages	(<objectType1>, <eventId1>), (<objectType2>, <eventId2>), ...	See Medium Priority Messages	Makes it possible to add or remove message types from the medium priority message list. See above for example.
Bridge Message Bandwidth Limiter Maximum Process Private Bytes	Positive integer (64 bit)	370000000	Process private bytes threshold at which point the Memory Safe Guard will kick in.
Bridge Message Bandwidth Limiter Small Message Limit Bytes	Positive integer (64 bit)	2000	Limit of what is considered a "small message" by this system. Small messages will be passed through and not suppressed when the memory safeguard is engaged.

High Priority Messages

High priority messages are messages that must be responded to as quickly as possible and that are also small in size so as not to take up too much of the available bandwidth for that interval. All of the messages in this queue—up to the "Bridge Message Bandwidth Limiter Total Outgoing Bytes Per Interval" limit—will be sent every interval.

These messages are meant to represent a basic functionality level for the client. Functionality like logons, logoffs, station changes, status, making calls, emails, chats, callbacks, license operations, interaction updates, and **My Interactions** queue updates are represented here. You can configure the high priority message list with a server parameter. For more information, see [Configuration](#).

Medium Priority Messages

Medium priority messages are made up of messages that may not be critical or may be slightly larger but that the client still expects in a timely fashion to maintain normal functionality.

Examples of a medium priority message would be a response to a client request or an event the client waits for. You can configure the medium priority message list with a server parameter. For more information, see [Configuration](#).

Memory Safe Guard

Bandwidth limiting is, by its nature, very prone to leading to memory growth. Since outgoing messages are queued up to be sent out over time instead of sent as quickly as possible, the queues can grow large in size. If unchecked, this could lead to process memory exhaustion. As such, this functionality has a built in safe guard to avoid that problem.

When bandwidth is being limited, the process's private bytes are constantly being checked and compared against the configured private bytes limit specified by the server parameter, Bridge Message Bandwidth Limiter Maximum Process Private Bytes. If that limit is exceeded, the memory safeguard kicks in. The memory safeguard is designed to remove or drastically reduce the potential for memory growth caused by bandwidth limiting that can lead to dangerous memory levels and memory exhaustion. It does so by suppressing non-essential messages while the memory safeguard is active. The effort is made to allow essential/critical client activity while the memory safeguard is engaged. This basic functionality is represented by all of the high priority messages. For more information, see [High Priority Messages](#).

While the memory safeguard is engaged, any large message that does not appear in the high priority message list is suppressed. A large message is defined as a message that is larger than the configured small message byte limit. For more information, see [Configuration](#). For suppressed responses, the response payload is replaced with an error message explaining that Session Manager is overloaded. For suppressed notifications, a new NotificationSuppressed notification is sent to let the client know what type of notification was suppressed. When queue updates are suppressed, a QueueSuspended notification is sent so that the client will grey-out its queue views so they do not get out of sync while updates are being suppressed. Once the memory drops to a safe point below the limit, QueueUnsuspend notifications are sent to any clients that received QueueSuspend messages. Currently with this functionality, any interactions that existed before the QueueUnsuspend notification was sent will not show up and be updated in the client view. New interactions will show up correctly. In order to fix this, Session Manager would have to send a large burst of queue notifications with the full contents of all queues that were suspended. Sending those large updates could lead to bandwidth limiting getting behind or memory issues, two things that we are trying to avoid at this point.

Changing CIC Time Zone

If you change the time zone on the CIC server through Interaction Administrator, you must restart Session Manager—both on-server and off-server. Time zone information is cached and constant for better performance, which requires an update to the information in Session Manager by doing the restart.

Connecting IceLib Applications over the Internet

With the proper configuration, IceLib applications can connect over the internet to Session Manager through a WebSocket protocol connection, instead of the typical TLS connection. As of the CIC 2016R3 release, most of the server side pieces needed to enable this functionality are installed along with Session Manager (on- an off-server Session Manager) or along with Customer Interaction Center (on a CIC server).

A WebSocket tunnel server, which is run automatically, is installed on any server that runs Session Manager (including one or more CIC servers). The WebSocket tunnel server accepts unsecured connections (ws scheme) on port 8951 and secured connections (wss scheme) on port 8952. As always, neither CIC servers nor off-server Session Manager Servers should be open to the public Internet. As such, a publicly-available reverse proxy must be in place to initially accept the WebSocket connections of the IceLib application and send them on to the CIC server or off-server Session Manager server. While an IceLib-based application could connect directly to port 8951 or 8952 on a CIC server or off-server Session Manager if those ports were available, full functionality of the IceLib applications requires a reverse proxy to direct the different types of WebSocket and HTTPS requests that an IceLib application makes.

The following table lists the IceLib applications and whether we have tested the internet connection for the application.

IceLib Applications	Internet Connection Tested?
IC Business Manager	Yes
IC Business Manager Reporting	Yes
IC Server Manager	No
Interaction Desktop	Yes
Interaction Fax Viewer	Yes
Interaction Screen Recorder Capture Client	Yes
Interaction Scripter .NET Client	Yes
Interaction Voicemail Player	Yes
Microsoft Lync Integration	No
Siebel Integration	No
Workforce Management Historical and Real-Time Integration	No
Third-party applications developed with IceLib API	No

Reverse Proxy Requirements

A reverse proxy must be in place and publicly available to the IceLib application over the internet. The reverse proxy must accept incoming WebSocket connections and route them to the CIC server or off-server Session Manager server based on information in the URI path. IceLib applications make several different types of HTTPS requests such as making file transfers (downloading status icons), transferring screen recordings, making large database transactions, and other types. The reverse proxy must know about these requests and be able to route them to the appropriate CIC server or off-server Session Manager server based on the information in the URI path. For more information, see [Table 8 - IceLibApplication URIs](#).

All traffic from the IceLib application to the reverse proxy must use a secure connection (SSL HTTPS/WSS) for security purposes. This means that the reverse proxy must be listening on a secure port—typically 443—with an SSL certificate that is trusted by the IceLib application. Usually, this action requires purchasing a certificate from a certificate authority.

IceLib Application URIs

The biggest change from the perspective of the IceLib application user is the use of a WebSocket protocol URI in the **Server:** input box in the IceLib application logon dialog or similar field in a configuration file. Where the CIC server name may be entered here, for connection over the internet, the URI might look like the following example:

wss://proxy/InternalServer/session

In this example, *proxy* represents the secure Internet URI to the reverse proxy and *InternalServer* represents the same CIC server name that was used to connect over a typical TLS connection.

If the CIC server name was ICServer1 and the proxy internet URI was client.proxy.com, the connection URI would be as follows:

wss://client.proxy.com/ICServer1/session

The reverse proxy would receive this request, determine that it is a request of type session, and forward it on to the WebSocket tunnel listening on ICServer1 port 8952 or 8951. As this is internal traffic, the use of secure WSS or WS in this configuration is up to the reverse proxy administrator.

For a list of all possible URIs by IceLib applications connecting over the Internet, see Table 8 - IceLibApplication URIs. In each case, *InternalServer* indicates to which internal server the reverse proxy must route.

Any additional path or query information included in URIs besides the session connection URI should be passed on to the destination server as the path of the request. This is represented in the following table as */additional*.

Table 8 - IceLibApplication URIs

URI	Destination	Port
wss://proxy/InternalServer/session	CIC server/OSSM	8952 (WSS) 8951 (WS)
https://proxy/InternalServer/http/additional	CIC server	8018 (HTTP)
https://proxy/InternalServer/httpsecure/additional	CIC server	8019 (HTTPS)
https://proxy/InternalServer/recorder/additional	CIC server/Remote Content Server	8106 (HTTP)
https://proxy/InternalServer/recordersecure/additional	CIC server/Remote Content Server	8107 (HTTPS)
https://proxy/InternalServer/dialer/additional	Dialer Campaign Server	8121 (HTTP)
https://proxy/InternalServer/dialersecure/additional	Dialer Campaign Server	8122 (HTTPS)
https://proxy/InternalServer/reporting/additional	Internet Reporting Plugin	8019 (HTTPS)

Server Name Aliases

You may not want to use the actual server name for these IceLib application URIs. In these cases, use server name aliases. For example, if you had a CIC server named ICServer1234, you could use an alias of just CIC so as to not publicly advertise the actual server name. The connection URI would then look resemble the following example instead of wss://proxy/ICServer1234/session:

wss://proxy/IC/session

You must maintain these aliases in at least two places:

- Within the reverse proxy so that it knows to which server to route the traffic.
- Configured on the CIC server so that Session Manager knows to use these aliases in place of the actual server names.

To configure the aliases on the CIC server, use the SM HTTPS URL Base Map server parameter detailed in [Table 10 - Common Server Parameters](#). You can set an alias from ICServer1234 to CIC by setting the SM HTTPS URL Base Map server parameter to ICServer1234|CIC or by adding &ICServer1234|CIC onto an existing value for that server parameter.

Session Manager would then use those aliases when generating the URIs that the Internet-connected IceLib applications will use. To avoid any problems, the aliases must be in sync between the reverse proxy and the SM HTTPS URL Base Map server parameter.

Additional URI Path Information

If necessary, it is possible to include additional routing information for the reverse proxy in the connection URI path. Session Manager considers only the last two segments of the URI path as the routing information and the rest of the base path for generating further URIs. So, if it is necessary for your reverse proxy configuration to include additional path information, such as `wss://proxy/additional/path/information/InternalServer/session`, which was then correctly routed by the reverse proxy to the CIC server or off-server Session Manager port 8952/8951, Session Manager would use `wss://proxy/additional/path/information/` as the base URI when generating additional URIs to be used by the Internet-connected IceLib application.

Included Custom Header

For requests made by an IceLib application connecting over the Internet, all requests—including the initial connection request—contain a custom header: `ININ-Client-Type`. The reverse proxy can use this as a very simple form of security to deny access to the system from any application that does not use this custom header.

Example nginx Configuration

This topic contains an example for part of an nginx reverse proxy configuration. This example is meant only as an example and should not be used in production since it attempts to pass data directly to any server specified in `wss://proxy/InternalServer/session` and similar URIs. Use server name aliases combined with server mappings in the reverse proxy so as to not provide actual server names in the URIs. For more information, see [Server Name Aliases](#).

```
map $1 $backend {
    icserver 10.0.0.40;
    ossm1 10.0.0.41;
    ossm2 10.0.0.42;
}

location ~* ^/(.*)/session\/?$ {
    if ($http_inin_client_type) {
        proxy_pass http://$backend:8951/websocket-tunnel;
    }
    proxy_next_upstream error timeout http_502;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
}

location ~* ^/(.*)/http/(.*) {
    if ($http_inin_client_type) {
        proxy_pass https://$backend:8018/$2;
    }

    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header Host $http_host;
    proxy_redirect off;
}

location ~* ^/(.*)/httpssecure/(.*) {
    if ($http_inin_client_type) {
        proxy_pass https://$backend:8019/$2;
    }
}
```

```

proxy_set_headerX-Real-IP $remote_addr;
proxy_set_headerX-Forwarded-For$proxy_add_x_forwarded_for;
proxy_set_headerX-Forwarded-Proto$scheme;
proxy_set_headerHost$http_host;
proxy_redirectoff;
}
location ~* ^/(.*)/recorder/(.*) {
if ($http_inin_client_type) {
proxy_pass https://$backend:8106/$2;
}
proxy_set_headerX-Real-IP $remote_addr;
proxy_set_headerX-Forwarded-For$proxy_add_x_forwarded_for;
proxy_set_headerX-Forwarded-Proto$scheme;
proxy_set_headerHost$http_host;
proxy_redirectoff;
}
location ~* ^/(.*)/recordersecure/(.*) {
if ($http_inin_client_type) {
proxy_pass https://$backend:8107/$2;
}
proxy_set_headerX-Real-IP $remote_addr;
proxy_set_headerX-Forwarded-For$proxy_add_x_forwarded_for;
proxy_set_headerX-Forwarded-Proto$scheme;
proxy_set_headerHost$http_host;
proxy_redirectoff;
}
location ~* ^/(.*)/dialer/(.*) {
if ($http_inin_client_type) {
proxy_pass https://$backend:8121/$2;
}
proxy_set_headerX-Real-IP $remote_addr;
proxy_set_headerX-Forwarded-For$proxy_add_x_forwarded_for;
proxy_set_headerX-Forwarded-Proto$scheme;
proxy_set_headerHost$http_host;
proxy_redirectoff;
}
location ~* ^/(.*)/dialersecure/(.*) {
if ($http_inin_client_type) {
proxy_pass https://$backend:8122/$2;
}
proxy_set_headerX-Real-IP $remote_addr;
proxy_set_headerX-Forwarded-For$proxy_add_x_forwarded_for;
proxy_set_headerX-Forwarded-Proto $scheme;
proxy_set_headerHost$http_host;

```

```
proxy_redirectoff;  
}
```

Monitor Session Manager instances

Starting with CIC 2016 R1, Session Manager uses the i3icsessionmanager.mib file and Simple Network Management Protocol (SNMP) for reporting the health of each Session Manager instance to a Network Management System (NMS).

For more information about i3icsessionmanager.mib and configuring SNMP on the host server, see CIC and SNMP Technical Reference in the PureConnect Documentation Library at the following website:

<http://help.genesys.com>

Note: In order for an off-server Session Manager to start, the ININ SNMP Service must be running.

Session Manager Command-Line Arguments

The Session Manager executable supports one command-line argument that specifies how Session Manager connects to a CIC server. If the command-line argument is modified, Session Manager startup can be affected.

The command-line argument is configured for on-server Session Manager during the CIC server installation and for off-server Session Manager during the off-server Session Manager installation.

Table 9 Command-Line Argument

Command-Line Argument	Description
/N=CICServerName	The CIC server to which Session Manager will connect.Without this argument, Session Manager attempts to connect to Notifier on the localhost.

Note:

In CIC 3.0, Session Manager supported additional command-line arguments to control its behavior.Those arguments were deprecated in CIC 4.0 and CIC 20nn Rn, and replaced by the new configuration options for Session Manager in Interaction Administrator. For more information about these configuration options, see [Configuring Session Manager Instances](#).

Server Parameters

Session Manager supports some server parameters used for its configuration. The following table contains the commonly-used parameters defined in Interaction Administrator.

Table 10 - Common Server Parameters

Parameter Name	Description
Work Path	The path to the work directory on the CIC server. You must specify this path correctly for Session Manager to run properly.
DirectoriestoCacheOnSMStartup	The directories that Session Manager caches on startup. By default, all directories except the Company Directory are cached upon the first request.
BridgeHostTrustedSites	A list of IP addresses, delimited by the pipe () character, that are <i>trusted</i>. By default, Session Manager trusts only connections from clients on the same subnet. If there are more than 20 connections in a 3-second span from clients on a different subnet, Session Manager rejects those connections. Note: In CIC 4.0 and CIC 20nn Rn, this setting no longer accepts a range of IP addresses.
SM HTTPS URL Base Map	A set of server name alias mappings where the DNS name that the clients should use for HTTPS resource downloads is not the actual name of the machine. This server parameter enables the machine to have a private name and a publicly-routeable name. This server parameter is often used in configurations with NAT and firewalls. Syntax: <i>MachineName</i> <i>alias</i> <i>MachineName</i> represents the actual name of the server host. <i>alias</i> represents the name or address that you want to map for <i>MachineName</i> for use in URI paths for connections. The delimiter between <i>MachineName</i> and <i>alias</i> is the pipe () character. You can append additional mappings by prepending an ampersand (&) character as displayed in the following example: <i>MachineName1</i> <i>alias1</i>&<i>MachineName2</i> <i>alias2</i>

Required Ports

A Session Manager requires some ports to be open between it, its associated CIC server (in the case of an Off-Server Session Manager), and its clients. If any of the ports in the following table are blocked by a firewall, some or all Session Manager functionality may be impacted.

Table 11 - Required Ports for Off-Server Session Managers

Port	Description
TCP 3952	(SSL and Clear) IceLib client communication
TCP 5597	(SSL) Notifier connection
TCP 6234	(SSL) ION Notifier connection with CIC server
TCP 8018	(HTTP) Client HTTP Plugin Host communication for IC Web Services and file transfers
TCP 8019	(HTTPS) Client HTTP Plugin Host communication for IC Web Services and file transfers
TCP 8951	(WS) IceLib based application communication over the internet via WebSocket protocol.
TCP 8952	(WSS) Secure IceLib based application communication over the internet via WebSocket Protocol.
TCP 445	SMB

Change Log

Date	Changes
16-November-2011	Initial Draft Author: Session Manager Team
21-December-2011	Added sizing information Author: Session Manager Team
29-May-2012	Added configuration information related to HTTP file download Author: Session Manager Team
13-July-2012	Added Selection Rules information Author: Session Manager Team
31-May-2013	Added information about Session Manager enforcing Selection Rules. Author: Session Manager Team
28-June-2013	Sizing number updates and other minor edits Author: Scalability Testing Team
25-May-2014	Added bandwidth limiting information. Author: Session Manager Team
11-September-2014	Added information about the "Work Path" server parameter. Author: Session Manager Team
23-October-2015	- Rebranded cover page - Updated "Copyright and Trademark Information" page - Added "Monitor Session Manager instances" topic under the "Session Manager Configuration and Monitoring" Author: Documentation Team
20-January-2016	- Renamed all instances of "I3 Windows Service Monitor" to "ININ Windows Service Monitor" - Added information on plug-ins for Interaction Dialer and Interaction Conference to Other PureConnect Software section. Author: Documentation Team
29-February-2016	- Added network port and configuration requirements to Hardware and Network Requirements for On-Server Session Managers and Network Requirements for Off-Server Session Managers - Added Changing CIC Time Zone - Added Connecting IceLib Applications over the Internet - Added Monitor Session Manager instances - Added Required Ports - Applied general edits for writing style compliance and clarity - Applied formatting modifications for clarity - Updated multiple screen shots Author: Documentation Team Author: Session Manager Team

20-November-2017	• Added list of IceLib Applications in Connecting IceLib Application over the Internet. • Added note to indicate that the ININ SNMP Service must be running for an off-server Session Manager to start. • Rebranded title page and terminology. Updated copyright page. Author: Documentation Team Author: Session Manager Team
24-January-2019	IC-153081 Doc SCR: Port 445 for OSSMs - Added "TCP 445/SMB" to Required Ports topic.
17-July-2019	Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section..."