Framework Deployment Guide

Network Locations for Framework Components

5/6/2025

Contents

Network Locations for Framework Components

This section provides basic data and makes recommendations that will help you select the optimal components for your specific needs, choose a computer for each component, and define the optimal location for each component on the network.

A separate section presents the information for each layer of Framework.

> **Important**
>
> In release 8.x, Genesys Administrator is the recommended interface for Management Framework, in place of Configuration Manager and Solution Control Interface, both of which are still available for download and use with this release of Management Framework. For this reason, Configuration Manager and Solution Control Interface are not mentioned in this section. For more information, refer to User Interaction Layer (Genesys Administrator), and the *Framework Genesys Administrator Deployment Guide*.

Configuration Layer

The Configuration Layer is a mandatory part of any Genesys CTI installation. You cannot configure and run any other layers of Framework-or any solutions-unless Configuration Layer components are running.

This section provides recommendations for planning and installing the Configuration Layer components.

Configuration Database

The Configuration Database stores all configuration data.

When planning your installation, follow these recommendations for the Configuration Database:

- The size of the Configuration Database depends on the size of the contact center, or—more precisely—on the number of entities in the contact center that you specify as configuration data objects. If data storage capacity is limited, consider allocating 10 KB of space for every object in the contact center as a general guideline. Otherwise, allocating 300 MB accommodates a Configuration Database for a typical installation with one tenant.
- If you want to deploy a Disaster Recovery/Business Continuity architecture, you must set up Configuration Databases across sites. Refer to Disaster Recovery/Business Continuity for more information.

- Treat the Configuration Database as a mission-critical data storage. Ensure that only the properly qualified personnel gain access to the DBMS that contains the Configuration Database itself. Information about access to the database is stored in the configuration file of Configuration Server. To protect this file, place it in a directory that is accessible only to the people directly involved with Configuration Layer maintenance.
- Consider encrypting the database access password via Configuration Server.
- As with any mission-critical data, regularly back up the Configuration Database. Base the frequency of scheduled backups on the rate of modifications in a particular configuration environment. Always back up the database before making any essential modifications, such as the addition of a new site or solution.
- Switch Configuration Server to Read-Only mode before performing any maintenance activities related to the Configuration Database.
- Save the records of all maintenance activities related to the Configuration Database.
- Users of the Configuration Database should have at least the following privileges for all tables in the database:
  - SELECT
  - INSERT
  - UPDATE
  - DELETE

Warning

- Never add, delete, or modify any data in the Configuration Database, except through applications developed by Genesys, or through applications instrumented with the Genesys Configuration Server application programming interface (API). If you have compelling reasons for accessing the database directly, consult Genesys Customer Care before you do so.
- Configuration Server treats its information and checks integrity constraints in a case-sensitive manner. Therefore, your SQL database must be installed and configured in case-sensitive mode. Refer to your SQL Server Administrator documentation for additional information.

Configuration Server

Configuration Server provides centralized access to the Configuration Database, based on permissions that you can set for any user to any configuration object. Configuration Server also maintains the common logical integrity of configuration data and notifies applications of changes made to the data.

When planning your installation, follow these recommendations for Configuration Server:

- Genesys solutions installed in a particular environment can have only one Configuration Database managed though one Configuration Server at a time.
- Because Configuration Server keeps all configuration data in its memory, allocate memory for this

server based on the expected size of the Configuration Database. Refer to the *Management Framework* section of the *Genesys Hardware Sizing Guide* for assistance in determining the amount of memory to allocate for Configuration Server.

- If you want to deploy a Disaster Recovery/Business Continuity architecture, you must set up Configuration Servers across sites. Refer to Disaster Recovery/Business Continuity for more information.
- For client connections:
  - Connect all administrative applications that do WRITE operations to Configuration Server directly.
  - Any other Genesys server applications should be connected to either Configuration Server (if server capacity permits) or Configuration Server Proxy. Server applications that communicate directly with each other, such as URS and T-Server, must be connected to the same Configuration Server or Configuration Server Proxy.
- You can deploy redundant (HA) Configuration Servers.
- Always use SCS to control Configuration Server HA pairs. This SCS must be directly connected to the master Configuration Server.

> **Important**
>
> Configuration Servers in HA Pairs cannot be switched over manually.

Configuration Server Proxy

To support a large number of clients and/or distributed installations, Configuration Server can operate in Proxy mode. In this document, a Configuration Server that operates in Proxy mode is called *Configuration Server Proxy*. For more information about Configuration Server Proxy, see Solution Availability.

When planning your installation, follow these recommendations for Configuration Server Proxy:

- Refer to the *Management Framework* section of the *Genesys Hardware Sizing Guide* for assistance in determining the amount of memory to allocate for Configuration Server Proxy.
- You can install Configuration Server Proxy anywhere on the network because it does not generate heavy traffic.
- If you want to deploy a Disaster Recovery/Business Continuity architecture, you might consider setting up Configuration Server Proxies across sites. Refer to Disaster Recovery/Business Continuity for more information.
- If you are using any agent-facing interfaces, such as Workspace Desktop Edition, or interfaces that will be accessing the Configuration Database on a read-only basis, connect those interfaces to Configuration Server Proxy.
- You can deploy redundant (HA) Configuration Server Proxies.
- Always use SCS to control Configuration Server Proxy.

Genesys Security Pack on UNIX

Genesys Security Pack on UNIX, an optional component of the Configuration Layer, provides the components, such as shared libraries, which are used for generation of certificates and their deployment on UNIX computers on which Genesys components are installed. For more information, refer to the *Genesys Security Deployment Guide*.

Management Layer

The exact configuration of the Management Layer depends on which of the following management functions you would like to use. Genesys recommends that you use all of these capabilities to optimize solution management.

Required Components

If you intend to use one or more of the Management Layer capabilities, plan to install the components required for each capability, as outlined below. Refer to the *Framework Management Layer User's Guide* for descriptions of, and recommendations for, these components.

Solution and application control and monitoring

Install these components to control and monitor solutions and applications:

- Local Control Agent
- Solution Control Server

Centralized Logging

Install these components to use centralized logging:

- Centralized Log Database
- Message Server

> **Important**
> Although Solution Control Server is not required, it is a source of log events vital for solution maintenance. For example, Solution Control Server generates log events related to detection and correction of application failures. As such, it is useful for centralized logging.

Alarm Signaling

Install these components to provide alarm signaling:

- Message Server
- Solution Control Server
- Genesys SNMP Master Agent, if SNMP alarm signaling is required. See also SNMP Support.

Application Failure Management

Install these components to detect and correct application failures:

- Local Control Agent
- Solution Control Server

See Application Failures for information about the application-failure management mechanism.

SNMP Support

Install the following components to integrate Genesys Framework with an SNMP-compliant third-party network management system (NMS):

- Local Control Agent
- Solution Control Server
- Genesys SNMP Master Agent, Net-SNMP, or another third-party SNMP Master Agent compliant with the AgentX protocol
- Message Server if SNMP alarm signaling is required

Note: Starting in release 8.5.1, Net-SNMP can be used to provide the same functionality as the built-in SNMP support, and the two can run in parallel. In this case, Net-SNMP must also be installed.

Management Layer Components

This section provides recommendations for planning and installing the Management Layer components.

Local Control Agent

When planning your installation, follow these recommendations for Local Control Agent:

- Install an instance of LCA on each computer running a monitored application, whether a Genesys daemon or a third-party application. LCA is installed at the port number you specify in the LCA Port property of the corresponding Host object in the Configuration Database. If you do not specify a value for LCA Port, the LCA default port number is 4999. By default, LCA runs automatically on computer startup.

> **Important**
> On Windows operating systems, the installation script always installs LCA as a

> Windows Service. If you are changing the LCA port number in the host configuration after the installation, you must also change the port number in the ImagePath in the application folder, which you can find in the Registry Editor. Refer to Notes on Configuring the LCA Port for instructions.

- If you want to deploy a Disaster Recovery/Business Continuity architecture, you must set up an LCA across all sites. Refer to Disaster Recovery/Business Continuity for more information.
- On UNIX platforms, LCA must be added to the **r/c** files during the installation, so that LCA can start automatically on computer startup. In practice, this means that the person installing LCA must have sufficient permissions.

Message Server

When planning your installation, follow these recommendations for Message Server:

- Genesys recommends the use of one Message Server and of one Log Database for all but large installations. If you are working within a large installation and are considering evenly dividing the total log-event traffic among number of Message Servers, each serving any number of clients, keep the following facts in mind:
  - Although any number of Message Servers can store log records in the same Log Database, one Message Server cannot store log records in more than one Log Database.
  - Because any number of Message Servers can send log records to Solution Control Server, Genesys Administrator can display alarms based on log records from a few Message Servers.
- If you want to deploy a Disaster Recovery/Business Continuity architecture, you must set up Message Servers across sites, with one dedicated for communication between all Solution Control Servers at all sites. Refer to Disaster Recovery/Business Continuity for more information.
- If you want an application to generate alarms, you must configure it to send log events to Message Server. Use the same Message Server for both the centralized logging and alarm signaling.
- If you want Message Server to provide alarms, you must connect it to Solution Control Server. This means that you must configure a connection to every Message Server in the SCS Application object.
- As with any other daemon application, you can deploy redundant Message Servers.
- To optimize the performance of the connection to the Log Database, configure the number of messages that the Message Server sends to the database before receiving a response. The smaller the number of messages, the greater the decrease in performance. See the "Message Server" section of the *Framework Configuration Options Reference Manual*, for more information.

Solution Control Server

When planning your installation, follow these recommendations for Solution Control Server:

- Given that you can install and use more than one SCS that is operating in Distributed mode within a given configuration environment, consider deploying a few Solution Control Servers in this mode for large or geographically distributed installations. In these installations, each server controls its own subset of Host, Application, and Solution objects. Distributed Solution Control Servers communicate with each other through a dedicated Message Server.
- If you want to deploy a Disaster Recovery/Business Continuity architecture, you must set up Distributed

Solution Control Servers across sites. Refer to Disaster Recovery/Business Continuity for more information.

- As with any other daemon application, you can deploy redundant Solution Control Servers. Redundancy support for SCS is implemented through direct communication between the backup SCS and the LCA of the host on which the primary SCS runs. Be sure to synchronize the ports between primary and backup Solution Control Servers.

> **Important**
> You cannot perform a manual switchover for Solution Control Server.

Centralized Log Database

As with any historical database, the size of the Centralized Log Database grows with time. When you are planning your installation, keep in mind that:

- The maximum allowable record size is 1 KB.
- The size of the Centralized Log Database depends on:
  - The number of applications in the system.
  - The log level you have set for the network output for each application.
  - The required time the log records should be kept in the database. The following table provides general timing recommendations:

Logging Level	Supported Call Volume	Recommended Storage Time
STANDARD	100 calls/sec	10 days
INTERACTION	10 calls/sec	1 day
TRACE	5 calls/sec	1 day

With these limits in mind, follow these recommendations for the Centralized Log Database:

- For efficient online log viewing, allocate temporary database space of at least 30 percent of the expected Centralized Log Database size.
- Limit permissions to modify the Centralized Log Database content to Message Servers only.
- Define how long the log records are to be kept in the database before they become obsolete. Use the Log Database Maintenance Wizard to delete obsolete records or configure the removal of obsolete records using the DBMS mechanisms.
- Users of the Centralized Log Database should have at least the following privileges for all tables in the database:
  - SELECT
  - INSERT
  - UPDATE
  - DELETE

- Make a trade-off between how long the log records are to be kept and the ability to access them efficiently. If both a considerable period of record storage and quick online access to the log records are important, back up the more dated records in a separate database.
- If you want to deploy the Disaster Recovery/Business Continuity feature, you must set up log databases across sites. Refer to Disaster Recovery/Business Continuity for more information.

SNMP Master Agent

When planning your installation, Genesys recommends that you use SNMP Master Agent only if you want to access the Management Layer functions via an NMS interface; or you have another SNMP-enabled Genesys application and want to access its features via an NMS interface.

User Interaction Layer (Genesys Administrator)

Install the Genesys Administrator web server preferably in close proximity with Configuration Server. You can then install as many web browsers as required, from which you can access and use Genesys Administrator.

Media Layer

For every switch that you plan to make a part of your interaction management solution, install at least one T-Server application.

T-Server

T-Server provides an interface between traditional telephony systems and Genesys applications.

When planning your installation, follow these recommendations for T-Server:

- At the premise level, always associate one switch with one T-Server.
- Allocate memory for T-Server based on the number of interactions you expect to be simultaneously processed at a given site during the busiest hour and the typical amount of business data attached to the interactions. Allocate at least 500 bytes per interaction plus memory space for a "typical" amount of attached data.
- Provide sufficient RAM to run T-Server processes. To ensure adequate performance, do not run T-Server processes in Swap mode.
- Do not install real-time third-party applications on the computer running T-Server.
- Consider using a dedicated subnetwork for T-Server connection to the link.
- Do not enable IP routing between the link subnet and the network when T-Server is installed on a computer with two or more network cards (one of which is used for link connection and the others for connection to the rest of the network).

Services Layer (Stat Server)

Although StatServer is considered an element of Framework, it is logical to install it when you install the solution that it will serve.

Stat Server tracks real-time states of interaction management resources and collects statistics about contact center performance. Genesys solutions use the statistical data to more "intelligently" manage interactions. Use Genesys Reporting to generate real-time and historical contact center reports based on data that Stat Server collects.

For specific recommendations on Stat Server installation, refer to Stat Server documentation.