# Framework Deployment Guide

Management Framework 8.5.0

12/29/2021

# Table of Contents

# Management Framework Deployment Guide

Use this guide to introduce you to the concepts and terminology relevant to the Genesys Framework, and procedures to install, configure, and run Management Framework.

## About Framework

Overview

Architecture and Functionality

Connections

New in This Release

## Deployment Planning

Initial Considerations

Network Locations

Installation Worksheet

## Deploying Framework

Deployment Overview

Prerequisites

Configuration Layer

Management Layer

## Redundant Configurations

Deploy high availability (HA) Management Framework components:

HA Configuration Servers

HA Message Servers

HA Solution Control Servers

HA SNMP Master Agents

## Sharing the Load Systems

Deploy distributed components:

## Disaster Recovery/Business Continuity

Suggested Disaster Recovery Architecture

Configuration Server Proxies

Distributed Solution Control Servers

More Information and Configuration Notes

Starting and Stopping Framework Components

Using Start Files

Using the Management Layer

Starting Manually

Using Windows Service Manager

Additional Information

Silent Setup

Generic Deployment and Login Procedures

Configuration Server History Log

History of Configuration Changes Utility

Automatic Disconnect Detect Protocol (ADDP)

Internet Protocol version 6 (IPv6)

# About Genesys Framework

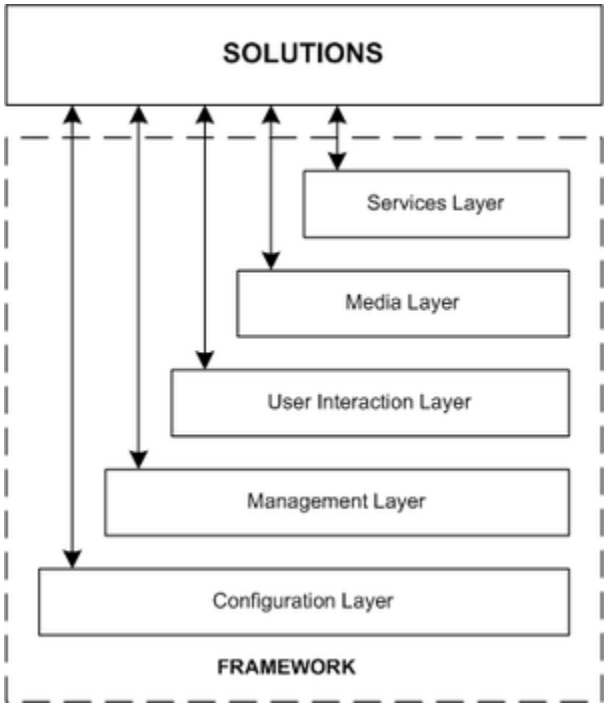
The Genesys Framework is a mandatory part of any Genesys-based interaction management system. It provides functions required for the normal operation of any Genesys solution:

- Configuration centralizes processing and storage of all the data required for Genesys solutions to work within a particular environment.
- Access Control sets and verifies users' permissions for access to, and manipulation of, solution functions and data.
- Solution Control starts and stops solutions and monitors their status.
- Alarm Processing defines and manages conditions critical to the operation of solutions.
- Troubleshooting hosts a user-oriented, unified logging system with advanced storage, sorting, and viewing capabilities.
- Fault Management automatically detects and corrects situations that might cause operational problems in solutions.
- External Interfaces enable communication with a variety of telephony systems and database management systems (DBMS).
- Attached Data Distribution supports the distribution of business data attached to interactions, within and across solutions.

# Architecture

The Genesys Framework consists of five layers (see the figure below). In sophisticated configurations using Management Layer functionality, each layer depends on the layers below it to work properly.

- The Configuration Layer processes and stores all the data required for running Genesys solutions in a particular environment; it notifies clients of any configuration changes. The Configuration Layer also controls user access to a solution's functions and data.
- The Management Layer controls the startup and status of solutions, logging of maintenance events, generation and processing of alarms, and management of application failures.
- The User Interaction Layer provides a comprehensive user interface to configure, monitor, and control the management environment.
- The Media Layer enables Genesys solutions to communicate across media, including traditional telephony systems, Voice over IP (VOIP), e-mail, and the Web. This layer also provides the mechanism to distribute interaction-related business data within and across solutions.
- The Services Layer generates the statistical data used for interaction processing and contact center reporting.



Genesys Framework Architecture

> **Important**
> A Genesys installation depends on Genesys License Reporting Manager (LRM), not

> shown in the diagram, for license control.

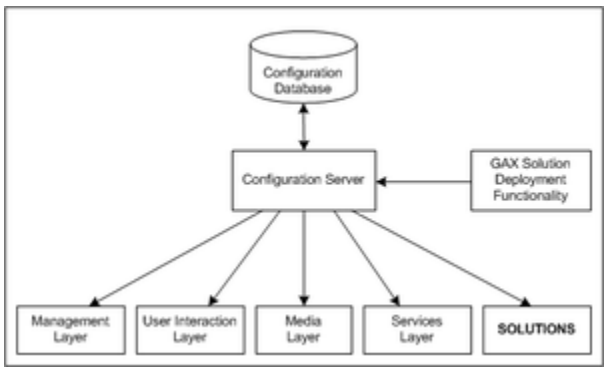
# Configuration Layer

## Functionality

The Configuration Layer provides:

- Centralized configuration data processing and storage for one-time entry of any information about contact center entities that any number of applications require to function in a particular business environment. Any number of applications can use this information.
- An advanced, configuration data-distribution mechanism, so applications can read their configuration upon startup and be notified of updates at runtime without service interruptions.
- Comprehensive data-integrity control functions that prevent entry of illogical configuration data that might cause solution malfunction.
- Advanced reconnection management which ensures that applications have up-to-date data after reestablishing connection to Configuration Server.
- Access control functions to regulate user access to solution functions and data, based on the access privileges set for each item.
- Wizards to help users through the automated process of solution deployment.
- Support for geographically distributed environments.
- Integration with external data sources, from which you can import configuration data to the Configuration Database.
- Import and export of configuration data to and from the Configuration Database.
- Secure data transfer between Genesys components using the Transport Layer Security (TLS) protocol.

## Architecture




Configuration Layer Architecture

In the Configuration Layer:

- Configuration Server provides centralized access to the Configuration Database, based on permissions that super administrators 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. Optionally, you can run Configuration Server in Proxy mode to support a geographically distributed environment. (The geographically distributed architecture is more complex than shown in the diagram.)
- Genesys Administrator, part of the User Interface Layer, provides a user-friendly interface for manipulating the contact center configuration data that solutions use and for setting user permissions for solution functions and data.
- The Configuration Database stores all configuration data.

> ### 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.

- Genesys Administrator Extension solution deployment functionality automates deployment and upgrade. This functionality also handles solution-specific data integrity.
- Configuration Conversion Wizard (CCW) (not shown in the diagram) provides a user-friendly interface for migrating Genesys configuration data to the most recent data format. Database migration is optional, but required if you want to take advantage of the most recent features of Management Framework. Starting in release 8.1.3, CCW also enables you to migrate the Configuration Database to a multi-language format using UTF-8, and to migrate a single-tenant (enterprise) Configuration Database to a hierarchical multi-tenant database. Refer to the Genesys Migration Guide for more information about CCW.

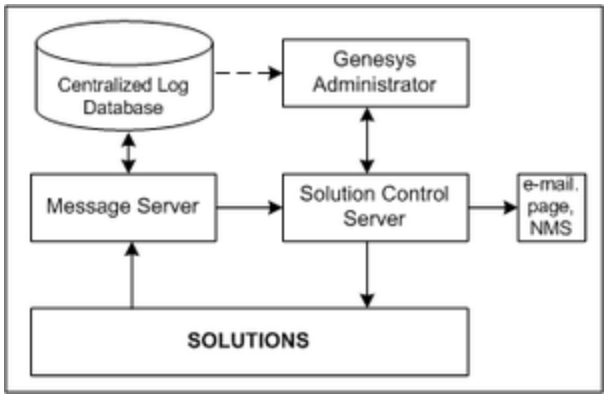
# Management Layer

## Functionality

The Management Layer provides:

- Centralized solution control and monitoring, displaying the real-time status of every configured Solution object, and activating and deactivating solutions and single applications, including user-defined solutions.
- Centralized logging that records applications maintenance events. The unified log format enables easy selection of required log records and centralized log storage for convenient access and solution-level troubleshooting. Centralized logging also allows you to track individual interactions, audit activities in your contact center, and store alarm history.
- Flexible alarm signaling that triggers alarms based on application maintenance events, system performance parameters, or Simple Network Management Protocol (SNMP) thresholds. Alarms are communicated to Genesys Administrator and can be written to system logs. You can configure the system to convert alarms into SNMP traps and send them as e-mails to a specified Internet address. (The latter automatically enables paging notifications.) The Management Layer automatically associates alarms with the solutions they affect and stores alarms as active conditions in the system until they are either removed by another maintenance event or cleared by the user.
- Fault-management functions, consisting of detection, isolation, and correction of application failures. For non-redundant configurations, the Management Layer automatically restarts applications that fail. For redundant configurations, this layer supports a switchover to the standby applications and also automatically restarts applications that fail.
- Built-in SNMP support for both alarm processing and SNMP data exchange with an SNMP-compliant network management system (NMS). As a result, you can integrate a third-party NMS with a Genesys system to serve as an end-user interface for control and monitoring functions and for alarm signaling functions.
- Individual host monitoring, including CPU and memory usage records and information about running processes and services.
- Support for geographically distributed environments.
- Support for the remote deployment of Genesys components, as performed in Genesys Administrator Extension.,

# Architecture




Management Layer Architecture

In the Management Layer:

- Local Control Agent (not shown in the diagram), located on every host that the Management Layer controls and/or monitors, is used to start and stop applications, detect application failures, and communicate application roles in redundancy context. The Local Control Agent Installation Package (IP) also includes a remote deployment agent (not shown in the diagram), referred to as the *Genesys Deployment Agent*, that is used to deploy Genesys IPs remotely.
- Message Server provides centralized processing and storage of every application's maintenance events. Events are stored as log records in the Centralized Log Database where they are available for further centralized processing. Message Server also checks for log events configured to trigger alarms. If it detects a match, it sends the alarm to Solution Control Server for immediate processing.
- Solution Control Server is the processing center of the Management Layer. It uses Local Control Agents to start solution components in the proper order, monitor their status, and provide a restart or switchover in case of application failure. Solution Control Server also includes four utilities that provide the ability to gracefully stop T-Servers, handle T-Server stuck calls, send log messages on behalf of applications, and exchange information with Solution Control Server. These utilities can be installed with or without Solution Control Server.
- Genesys Administrator, a User Interaction Layer component, displays the status of all installed Genesys solutions and information about each active alarm, enables the user to start and stop solutions or single applications (including third-party applications), and enables advanced selection and viewing of maintenance logs.
- The Centralized Log Database (also called the Log Database) stores all application log records, including interaction-related records, alarm history records, and audit records.
- Genesys SNMP Master Agent (an optional component not shown in the diagram) provides an interface between the Management Layer and an SNMP-compliant NMS. It is required to support Microsoft Operational Manager (MOM) technology, and optional to support Master Agent or a third-party AgentX protocol-compliant SNMP master agent.

# User Interaction Layer

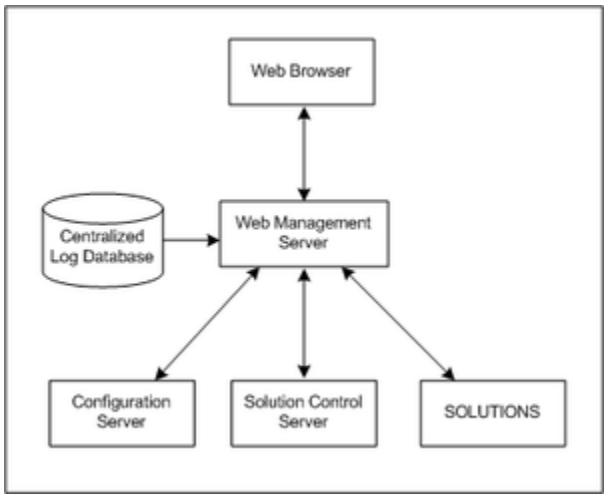
## Functionality

The User Interaction Layer provides centralized web-based functionality and interfaces for the following:

- Deployment of Genesys components to any computer on the network using the Genesys Deployment Agent (a Management Layer component). Starting in release 8.5, this functionality is part of Genesys Administrator Extension.
- Configuration, monitoring, and control of applications and solutions.

Currently, Genesys Administrator and its extension is the only component in the User Interaction layer.

## Architecture




User Interaction Layer Architecture

In the User Interaction Layer:

- The browser-based Genesys Administrator includes a comprehensive user interface to configure, monitor, and control the management environment.
- The Web Management Server:
  - Communicates with Configuration Server (a Configuration Layer component) to exchange configuration information.
  - Communicates with Solution Control Server (a Management Layer component) to exchange status,

operations, and control information.

  - Reads logs from the Centralized Log Database (a Management Layer component).
  - Provides web services for the browser-based Genesys Administrator.

- Depending on the solutions deployed in the system, the Web Management Server may also communicate with other back end servers to retrieve solution-specific information.

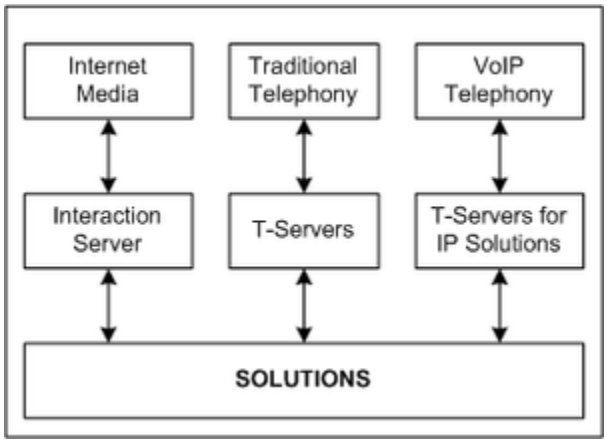
# Media Layer

## Functionality

The Media Layer provides:

- Interfaces to communication media.
- Distribution of interaction-related business data within and across solutions.

## Architecture




Media Layer Architecture

In the Media Layer:

- Interaction Server provides an interface with Internet media like e-mail and web communications. T-Server provides an interface with traditional telephony systems.
- T-Servers provide an interface with traditional telephony systems.
- T-Servers for IP Solutions provide an interface with VoIP telephony systems.

All of these servers communicate interaction-processing requests from the Genesys solutions to the media devices and distribute interaction-processing events in the opposite direction. They also maintain the current state of each interaction and all the business data collected about each interaction during processing stages. These servers distribute attached data to all the applications that participate in processing the interaction. They can also transfer that data across multiple interaction-processing sites.

Another Media Layer component, Load Distribution Server (LDS), not shown in the diagram, increases system scalability and availability.

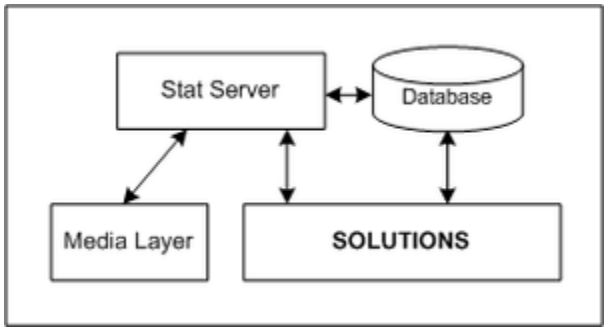
# Services Layer

## Functionality

The Services Layer provides:

- Conversion of events related to management of single interactions into statistical data, which is then used for interaction processing and contact center reporting.

## Architecture




Services Layer Architecture

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 real-time interactions. Through Genesys Reporting, you can use the data to generate real-time and historical contact center reports.

# Framework Connections

The following diagram shows connections that Framework components establish to each other and to solutions.

Framework Connections

## IPv6 Support

All Framework server components support IPv6, except for the following:

- When obtaining technical licenses connecting to the FlexNet license server, all Framework servers support IPv6 on only the RHEL 5 64-bit and Windows 2008 64-bit operating systems.

For more information about IPv6, see Internet Protocol version 6 (IPv6) and IPv6 vs. IPv4 Overview.

# New in This Release

Before you familiarize yourself with the Genesys Framework architecture and functionality, note the following major changes that were implemented in the 8.5 release of Framework, and the sources that describe them in detail.

## New in Release 8.5.0

### General Features

- **Recommendations for Disaster Recovery:** If a natural, man-made, or unintended event occurs at the main site, forcing Configuration Server, Solution Control Server (SCS), and Message Server to fail, Genesys now recommends a multi-site deployment model to maintain operations. See Disaster Recovery/Business Continuity.
- **Enhanced Migration:** Migration of Management Framework Components is improved, enabling the upgrade to occur with minimal downtime and impact to the production environment. Refer to the ''Genesys Migration Guide'' for more information.
- **Logging Resilience:** Throttling can be applied to log outputs, including the Centralized Log, to prevent a log queue from growing to a size that could impact normal operation of an application.
- Support for new Database Management Systems and a new virtual platform. For updated information about supported operating systems, Database Management Systems (DBMS), and Virtual Machines, see the *Genesys Supported Operating Environment Reference Guide*.

### Configuration Layer

- **Improved Database Access:** DB Server is no longer required for access to the Configuration Database. Refer to the *Framework 8.5 Database Connectivity Reference Guide* for more information.

> **Important**
>
> If you will be using the Configuration Conversion Wizard to convert your Configuration Database, you still need DB Server for the conversion.

- **Licensing Enhancements:** Before Configuration Server starts for the first time, it now checks and confirms that the license file is valid. This step does not require any new license or license file; the existing license file is simply checked for validity. In addition, Genesys License Reporting Manager (LRM) is now supported; it works with Configuration Server to ensure that all applications have a valid license before they can be installed and started. Refer to Licensing Prerequisites for more information.
- **Language Pack Support for Localization of Configuration Layer:** Configuration Server allows you to install language packs to enable support of a particular language in which messages are displayed. Refer to the documentation with your Language Packs for more information.

- **Improved handling of Business Attributes:** New configuration options have been introduced to control the existence of legacy values of MediaType business attributes, and the automatic inheritance of legacy business attributes when creating new tenants.
- **Extended audit trail of configuration changes:** Configuration Server now supports an extended audit trail of all changes in the Configuration Database, including new and previous values. A new utility outputs a report of this information when necessary. Refer to History of Configuration Changes for more information.
- **New types of Application configuration objects:** Users can now define the following new types of Application configuration objects:
  - LRM Server
  - Recording Crypto Server

### Management Layer

See the ''Framework 8.5 Management Layer User's Guide'' for information about the following new features that are specific to the Management Layer:

- **Improved Database Access:** DB Server is no longer required for access to the Log Database.
- **Extended Hang-up Detection:** The Message Server process thread now supports hang-up detection between Message Server and the Log Database at the thread level.
- **Enhanced Logging:** Some log events have been updated to provide extended information application .

### Security Features

- **Extended support of Kerberos authentication protocol:** Configuration Server supports Kerberos for user logins. Configuration Server can operate with Windows Active Directory and MIT key distribution centers to facilitate Single Sign-on via Genesys UI applications. Refer to the ''Framework 8.5 External Authentication Reference Manual'' for more information.
- **Reinforced user authentication:** All active sessions are immediately invalidated when a user is disabled in, or removed from, the Configuration Database. Refer to the ''Genesys 8.1 Security Deployment Guide'' for more information about user authentication measures for your system.

## Retired Features

- DB Server is no longer required by Management Framework. If you must use DB Server because you are using Genesys components that are older and/or do not support this functionality, see Using DB Server.
- Except for Configuration Conversion Wizard, all other Management Framework-related configuration and deployment Wizards, including the Configuration Import Wizard and Database Import Wizard, are no longer available as part of Management Framework 8.5. However, most are available and can be used if needed.
- The Simple Object Access Protocol (SOAP) is deprecated in Management Framework.
- Support is discontinued for all versions of the following:
  - HP-UX and HP Itanium operating systems

- IBM Informix and Sybase DBMS

# Deployment Planning

Achieving optimal performance with your Genesys installation requires comprehensive planning. How well Genesys Framework components function in a particular environment depends on a number of variables, including amount of computer memory, network location of the applications, and the specific tasks the applications perform. The information in this section describes various characteristics of Framework components and looks at how they interact with each other and the applications they serve. It 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.

Start your deployment planning by identifying the existing telephony resources in your contact center environment. Then follow the deployment recommendations for each architecture layer given in Network Locations for Framework Components.

Consider whether you can benefit from:

- Using the Management Layer.
- Having redundant components.
- Installing additional Configuration Servers in Proxy mode.
- Installing a number of Solution Control Servers in Distributed mode.
- Using Load Distribution Server.

In addition, review Solution Availability and Security Considerations, which are common aspects of any Genesys installation.

Finally, prepare an installation worksheet summarizing your configuration requirements, and fill it in and refer to it as you deploy Framework.

# Initial Considerations

How well Genesys Framework components function in a particular environment depends on a number of variables, including amount of computer memory, network location of the applications, and the specific tasks the applications perform. 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.

# Telephony Network Description

Certain information is required to deploy Framework, so prepare a description of your telephony and media network as discussed in this section. You will use data from this description when supplying configuration parameters to Deployment Wizards or when configuring objects for your contact center using Genesys Administrator.

You must have the following information available for every switch that you plan to use in your interaction management solution:

- Switch type, which usually corresponds to the switch vendor, brand name, and model number.
- Version of the switch software.
- Type of CTI Link (TCP/IP, X.25, or ISDN).
- Version of the CTI Link software.
- Information required to connect to the CTI Link (for example, for TCP/IP connection, host name and port number), including password, service id, and other parameters required for switch security.
- Types and numbers of telephony devices, also called Directory Numbers or DNs. You may have to configure specific types of DNs (for example, Routing Points) on the switches to support functions of the interaction management solutions.
- Login codes to be assigned to agents for runtime associations between agents and their working places.
- Information about how the switch DNs are arranged into working places.
- Information about how DNs that belong to a particular switch can be reached from other switches in a multi-site installation.

In addition, describe your contact center resources:

- For every user who must access any interaction management application, define the following parameters: a unique employee ID, unique user name, and password. The role of a user in the contact center defines the set of access privileges for this user in the system. For more information, see Security Considerations.
- For agents, define Login codes in every switch at which they might be working.
- For agents, define skills that might be considered as criteria for effective interaction processing.
- Note how agents are arranged into groups.
- Decide how to arrange the working places into groups.

## Guidelines for Naming Hosts

To ensure that the operating systems properly interpret host names, follow these guidelines when naming the host computers in your system:

1. If possible, use the host's DNS name.

2. If it is not possible to use the DNS name, use the host's IP address, in the format x.x.x.x. However,

verify the availability of that IP address by using the command `ping <IP address>` on the command-line before starting the installation process.

# Configuration Environments

Genesys provides its software to two types of companies:

- Companies that own their telephony equipment and use it for their own needs.
- Companies (such as service providers) that make their telephony equipment available to other companies.

A single Genesys configuration environment can be used to address the needs of both of these types of companies. You establish that configuration environment, called *Hierarchical Multi-tenant*, when you create the Configuration Database structure during the Configuration Layer installation.

## Hierarchical Multi-Tenant

The hierarchical multi-tenant configuration environment serves the needs of a company, typically a service provider, making its telephony equipment available to other companies. So, this configuration environment also serves the needs of every company using the service. In this environment, configuration information about the resources that are managed exclusively by the service provider is visible on the service provider side only. Only personnel from the service provider company can register the entities that provide the technical foundation for setting up the CTI services, such as switching offices, data network hosts, and CTI applications. These resources may be shared by some or all of the companies using the service ("Tenants"). The resources of the individual companies, such as user accounts, agent groups, outbound campaigns, and so forth, are configured separately by the personnel of these companies. This configuration is visible only to that company's users.

This general structure can be extended to an unlimited number of layers. The service provider can provide its services not only to companies that use its services directly (as existed prior to release 8.0), but to other companies, such as resellers, who in turn sell those services to other companies. The customers of these resellers can, in turn, be direct users and perhaps other resellers. This hierarchical layering can be from one to an unlimited number of levels. Tenants that provide services to other tenants are called parent tenants; those that use these services are called child tenants. Therefore, a single Tenant object can be a parent, a child, or both.

This structure can also support a single-tenant, or *Enterprise*, environment, by configuring the pre-defined Environment tenant. As an alternative, a single-tenant Configuration Server can be deployed, but Genesys strongly recommends against this for new deployments. If you are already running a single-tenant environment, refer to the ''Genesys Migration Guide'' for information about converting it to a hierarchical multi-tenant environment with only one tenant.

> **Important**
>
> Prior to release 8.0, the hierarchical multi-tenant environment was known as the multi-tenant environment, because the latter was limited to one layer of hierarchy. In release 8.0 and later, the two terms are used interchangeably, but always refer to a hierarchical multi-tenant environment.

## Recommendations for Large Configuration Environments

Genesys defines a large configuration environment as one in which the Configuration Database stores 50,000 or more configuration objects. Genesys strongly recommends that you consider these guidelines when operating within a large configuration environment:

- Use Genesys Administrator and other Configuration Server clients with special care, to prevent loading problems. For example, create user accounts with different configuration access capabilities, so that contact center staff can log in to Genesys Administrator and perform only those tasks they are required to perform over the configuration objects for which they have permissions. This saves Genesys Administrator from loading all the objects from the Configuration Database.
- There are special considerations for the number of Management Framework server components and the amount of RAM required by each component to serve a particular number of clients. Refer to the "Management Framework" section of the ''Genesys Hardware Sizing Guide'' to determine appropriate values.
- Consider using Folder objects when creating a large number of configuration objects. The recommended number of configuration objects per folder is up to 4,000. Anything larger significantly increases Genesys Administrator time for loading configuration objects.
- When creating configuration objects of the Script type (for example, routing strategies), keep in mind that both the number of Script objects and the script size significantly affect the time it takes Configuration Manager to load the Script configuration objects. If you create large scripts, reduce the number of Script objects in a subfolder to achieve an acceptable loading speed. For instance, for the script-type configuration objects approximately 150 KB in size, limiting the number of script-type objects to 30 per subfolder guarantees an acceptable loading speed.
- When creating a large number of configuration objects of the Agent Login type, assign them to User configuration objects as you create the logins. When the Configuration Database contains too many unassigned agent logins, Genesys Administrator takes a long time to open the Agent Login browse dialog box from the Configuration tab or the Person Properties dialog box. To guarantee an acceptable loading speed, keep the number of unassigned Agent Login objects below 1000 per Tenant object.
- For all configuration objects, do not store large amounts of data as text properties in an object's Annex, unless it is explicitly required by Genesys applications.

# Using National Languages

## Single-language Environments

The default (legacy) deployment of Genesys software can support only one language in addition to English with which to process data and display messages. Genesys recommends that you select one language for your installation, and use that language across all components and databases.

## Multi-language Environments

UTF-8 data encoding enables a system to work with multi-language data that is encoded with UTF-8. This support applies to all string fields of all configuration objects, with some exceptions noted later in this section.

This functionality is optional, and must be enabled to take effect.

> **Warning**
> You must use a separate set of initialization scripts to enable multi-language mode when creating the database, following the setup of the configuration file option for master Configuration Servers.

You can perform an object search of data encoded in UTF-8, using the standard wildcard symbols, with search data supplied by UTF-8. The search parameters, in UTF-8, are compared with the data. All fields that are searchable with non-UTF-8 data are searchable with the UTF-8 data.

To configure your system to support multiple languages, satisfy the database prerequisites, then follow the steps in Deploying the Configuration Layer, taking note of the special requirements to support UTF-8.

### Framework Support for UTF-8

Framework supports UTF-8 encoding of the following:

- Most configuration fields (exceptions below)
- Solution Control Server alarm names, messages, and display thereof
- Content of log messages in Message Server and in the centralized Log Database
- UTF-8 initialization of the Configuration Database and the Log Database

Framework does not support UTF-8 encoding of the following items; they must be in ASCII.

- Names of `Application` objects
- Command-line arguments specified during configuration in the `Start Info` section
- Command-line arguments used by mlcmd and logutility
- Local configuration file used by Configuration Server
- SNMP traps and scalar data
- Database parameters in Database Access Points
- Host names
- Database table name in Table Access objects
- Log names and log file names specified in the `log` configuration option section

### DBMS Support for UTF-8 Encoding

The following DBMS can be used with UTF-8 encoding:

- DB2
- MS SQL (uses UCS-2 encoding)
- Oracle
- PostgreSQL

## Converting from a non-UTF-8 Database to a UTF-8 Database

Starting in release 8.1.3, you can use the Configuration Conversion Wizard (CCW) to convert a non-UTF-8 compatible Configuration Database into a database that can store and work with encoded data. Refer to the ''Genesys Migration Guide'' for information about using CCW to convert your configuration database.

Except for the conversion of the Configuration Database, Genesys does not otherwise provide any tools to support the migration of an existing database, that cannot work with UTF-8 data, into a database than can store and work with encoded data. Genesys recommends that you use tools and utilities provided by the DBMS you are using to do any such conversion.

> ### Warning
> After you have upgraded to UTF-8, legacy applications will be unable to connect to Configuration Server, unless you use the `allow-mixed-encoding` configuration option. Refer to the ''Framework Configuration Options Reference Manual'' for more information about this option.

# Management Framework and Solution Availability

Think of the *availability* of an interaction management solution as the amount of time that the solution is available to process enterprise interactions. Two major categories of events affect availability: changes in the operating conditions and failures. The first category combines the various operational and maintenance activities that require temporary shutdown and restart of the entire system or of one of its components. The second category deals with the temporary inability of the solution to perform its required functions because of operator errors or software faults.

Given the complexity of the solution architecture, remember that:

- Any interaction management solution relies on functionality provided by a number of components, each performing a specific task. The overall availability of a solution depends on the availability of each of the components involved.
- Interaction management solutions do not operate in isolation. On the contrary, they essentially bring together various business resources, such as telephony switches, call-processing telephony terminations, database management systems, and Internet communication servers. As such, the inability of an interaction management solution to perform its required function may be the result of the unavailability of an external component or system.
- Genesys solutions, which consist of software components only, operate on hardware platforms that require maintenance and that are subject to failures. For example, running redundant processes on the same host may work in the presence of a software failure; however, it offers no protection if the computer itself or a communication link to it fails. The availability of a solution can never be greater than the availability of the underlying hardware platform.

The Genesys Framework is designed to minimize the impact on solution availability associated with operational and maintenance activities. Because the Configuration Layer updates solutions about any configuration changes at runtime, uninterrupted solution operations are guaranteed regardless of the number or frequency of changes made to the contact center environment. Dynamic reconfiguration is a standard feature of every Genesys 7.x and 8.x component and does not require you to make any special adjustments to enable configuration settings.

Solution availability can also be affected by accidental operator errors, unauthorized actions, or actions that are carried out in a less than skillful manner. The data integrity rules implemented in the Configuration Layer greatly reduce errors of the first type. The basic integrity rules common across all solutions are supported by Configuration Server, and therefore enforced regardless of the type of client application through which the data is managed. More advanced integrity rules specific to a particular solution are implemented in the solution wizards. Genesys recommends that you use wizards for the initial deployment of solutions and major configuration updates in the course of solution operation.

Solution availability can also be impacted by the occurrence of a disaster, natural of man-made, that causes an entire site to go down. See Disaster Recovery/Business Continuity for a new Disaster Recovery architecture to prevent permanent failure of Management Framework itself because of the loss of the entire site.

Genesys Framework also provides a comprehensive set of access control functions that help minimize the risk of failures associated with unskilled or unauthorized operator actions. For more information

about these functions, see Security Considerations.

Finally, to reduce the impact on solution operations, schedule all operational and maintenance activities that directly affect system behavior for off-peak hours, when solutions operate at minimum loads.

*Faults*-accidental and unplanned events causing a system to fail-present the biggest challenge to solution availability. The functions that detect, isolate, and correct various types of faults are partly incorporated into every Genesys component and partly implemented in the Management Layer of the Genesys Framework. Refer to the ''Framework 8.5 Management Layer User's Guide'' for more information about the various fault-detection mechanisms implemented in Genesys software.

# Communication Session Failures

In a distributed interaction management solution, components must communicate continuously with each other and with some external resources. A communication session with a required resource can fail for any of these reasons:

- Failure of the resource itself
- Problem with the hardware where the resource is located
- Network connectivity problem between the two points
- Forced termination of the connection that has not shown any activity for a specified amount of time

Any time a solution component cannot communicate with a required resource, the solution may not be able to perform its required function.

After a failure is detected, the fault correction procedure normally consists of repeated attempts to regain access to either the resource in question or to a redundant resource, if one is available.

Each underlying communication protocol is typically equipped with functions that monitor open communication sessions. When a failure is detected, the communication software signals an abnormal condition to the interacting processes. This detection mechanism is fully supported in the Genesys solution, whose connection layer translates system messages into appropriate events on the application level.

However, communication protocols do not always provide adequate detection times. The TCP/IP stack, for example, may take several minutes to report a failure associated with a hardware problem (such as when a computer goes down or a cable is disconnected). This delay presents a serious challenge to the availability of any interaction management solution.

## Software Exceptions

A *software exception* is an interruption in the normal flow of a program caused by an internal defect. An operating system generates exceptions in response to illegal operations that a software program attempts to perform. After generating an exception, the operating system terminates the process, which may make unavailable all solutions that use the functionality of this component.

Genesys provides an exception-handling function that monitors the exceptions that the operating system generates. The function attempts to prevent application termination by skipping the program block from which the exception originated. In most cases, this action amounts to losing one processing step with respect to a single interaction in favor of preventing an application failure.

Although the function attempts to prevent application termination, it still reports the exception with the highest priority marking. This ensures that operators know about the exception and can take appropriate measures.

You can configure the number of times during which the function tries to prevent an application from failing if it continues to generate the same exception. If this threshold is exceeded, the exception-

handling function abandons the recovery procedure, allowing the operating system to terminate the application. This termination can then be detected and corrected by external fault-management functions.

By default, the exception-handling function is enabled in any daemon application; six exceptions occurring in 10 seconds will not cause an application to terminate. To change these parameters or disable the exception handling, use a corresponding command-line parameter when starting an application.

## Application Failures

A complete application failure may be a result of either an internal defect (for example, an infinite loop) or an external event (for example, a power failure). It may manifest as either a process nonresponse or termination. Typically, if a solution component stops working, the solution is no longer available to process customer interactions.

Because the application that fails cannot perform any functions, you must use an external mechanism for both detection and correction of faults of this type. In Framework, the Management Layer is this mechanism. For information about the architecture and components in the Management Layer, see the ''Framework 8.5 Management Layer User's Guide''.

### Configuration Server Failure Because of Memory Starvation

When Configuration Server responds to client requests with data, the responses are stored in Configuration Server memory until they are sent. The rate at which they are send depends on several factors, such as:

- load on Configuration Server
- network throughput
- ability of the client to receive and process the data

In some cases, the unsent messages might accumulate in memory. In severe cases, they could accumulate to the point where Configuration has to terminate unexpectedly because it has used 100% of memory.

To resolve this, you can impose flow control by limiting how much memory is used by unsent mail. When this limit is reached, Configuration Server stops processing client requests. When the backlog of unsent requests starts to clear and its memory usage drops below the imposed limit, Configuration Server starts process client requests again, in the order in which they were received.

Flow control is activated by two configuration options. `max-client-output-queue-size` provides flow control for communications for a single client. `max-output-queue-size` defines flow control for all clients.

> **Warning**
> Be very careful when using this option, as it effectively stops Configuration Server

> until all of its output buffers drop below the specified limit. Use this option only as a last resort.

Refer to the ''Framework Configuration Options Reference Manual'' for detailed descriptions about these options.

## Remote Site Failures

Starting in release 8.0, each Solution Control Server in a Distributed Solution Control Server environment can detect the failure of a remote site controlled by another Solution Control Server. Refer to the ''Framework 8.5 Management Layer User's Guide'' for more information.

# Security Considerations

This section outlines some of the security capabilities provided in Configuration Layer for your data, both from access by unauthorized users and during its transfer between components. For more information about these and other security features, and for full implementation instructions, refer to the ''Genesys 8.1 Security Deployment Guide''.

## Access to Hosts File at Start-up

By default, Genesys components try to read from the hosts file at startup to enable them to resolve host names. If an organization has a security policy against this, they can configure the environment variable `GCTI_DNS_USE_HOSTSFILE=0` to disable this access.

## User Authentication

User authentication refers to ensuring that the user is actually who he or she claims to be. In Genesys software, this is implemented by the Configuration Server. The data that a Genesys solution requires for operating in a particular environment, as well as the applications and the solutions, is represented as Configuration Database objects. Any person who needs access to this data or these applications must have an account in this database.

### Logging In

At startup, every Genesys GUI application opens a Login dialog box for users to supply a User Name and Password, which are used for authentication. The authentication procedure succeeds only if a User with the specified User Name and Password is registered in the Configuration Database. Otherwise, the working session is stopped.

### Last Logged In

Starting in release 8.0, you can configure Configuration Server so that some Genesys GUI applications display the date and time of the previous login for the currently logged-in user. Each user can then detect if someone else had accessed the system using their credentials.

### Forced Re-Login for Inactivity

You can configure some Genesys GUIs to automatically force a logged-in user to log in again if he or she has not interacted with any element of the interface for a set period of time. In some interfaces, open windows are also minimized, and are restored only when the user logs back in.

This functionality is configured in each interface, and is therefore specific to that interface. By default, this functionality is not active, and must be activated on an instance-by-instance basis for those GUI applications that are to use the feature.

> **Important**
>
> This inactivity feature survives reconnection timeouts. In other words, if the interface application becomes disconnected from Configuration Server after the forced re-login timeout has expired but before the user has logged in again, the user must still log in before he or she can access the system.

## User Authorization

User authorization refers to ensuring that an authenticated user is entitled to access the system, either all or parts thereof, and defines what the user can do to or with the data that they can access.

The security mechanism implemented in Configuration Server allows the system administrator to define, for each valid user account, a level of access to sets of objects. The access privileges of valid user accounts define what the user can and cannot do within the corresponding set of objects.

Starting in release 8.0, an additional layer of security is available through Genesys Administrator, called Role-Based Access Control. This enables the system administrator (or a designated individual) to define access to objects based on what is to be done (viewed, modified, deleted) to the objects.

This section provides an overview of the various mechanisms in place to ensure data is accessed by only authorized users. For detailed information about how Genesys software implements user authorization, refer to the ''Genesys 8.1 Security Deployment Guide''.

### Access Permissions

The level of access to sets of objects granted by the system administrator is defined by a combination of elementary permissions. Each user must be assigned at least one permission; without it, the user has no access to any data.

Access control for daemon applications is different from that for GUI applications. Access permissions for GUI applications are determined by the profile of the person who is currently logged in.

### Access Groups

*Access Groups* are groups of Users who need to have the same set of permissions for Configuration Database objects. By adding individuals to Access Groups-and then setting permissions for those groups-access control is greatly simplified.

Genesys provides preconfigured default Access Groups. You can also create your own Access Groups to customize your own security environment.

### Master Account and Super Administrators

The Configuration Database contains a predefined User object, otherwise known as the `Master Account` or `Default User`. The Default User, named `default` and with a password of `password`, is not associated with any Access Group. The Master Account always exists in the system and has a full set

of permissions with respect to all objects in the Configuration Database. You must use this account when you log in to the Configuration Layer for the first time since the Configuration Database initialization. Genesys recommends changing the default name and password of the Master Account, storing them securely, and using this account only for emergency purposes or whenever it is specifically required.

## Changing Default Permissions

The default permissions that the Configuration Layer sets provide users with a broad range of access privileges. You can always change those default settings to match the access needs of a particular contact center environment.

> **Important**
>
> Genesys does not recommend changing the default access control setting unless absolutely necessary. Remember, the more complex the security system is, the more difficult it becomes to manage the data and the more it affects the performance of the Configuration Layer software.

Genesys provides two mechanisms to help you manage changes to your permissions-propagation and recursion. Refer to the ''Genesys 8.1 Security Deployment Guide'' for details about these mechanisms and how to use them.

## New Users

Configuration Server does not assign a new user to an Access Group when the user is created. In effect, the new user has no privileges, and cannot log in to any interface or use a daemon application. The new user must be explicitly added to appropriate Access Groups by an Administrator or by existing users with access rights to modify the user's account. Refer to ''Genesys Administrator 8.1 Help'' for more information about adding a user to an Access Group.

By default, this behavior applies to all new users added by Configuration Server release 7.6 or later. Users created before release 7.6 keep their existing set of permissions and Access Group assignments. If you want new users to be added automatically to pre-defined Access Groups, as was the behavior prior to release 7.6, you must manually disable this feature by using the Configuration Server configuration option `no-default-access`.

For more information about this feature, including how it works and how to modify it, refer to the ''Genesys 8.1 Security Deployment Guide''.

## Login Security Banner

You can create your own security banner to be displayed to a user logging in to Genesys Administrator. You define the content of the banner, typically the terms of use of the application. Users must accept the terms to proceed, or they can reject the terms to close the application without access.

The user-defined security banner is specified during the installation of each instance of a GUI application, such as Configuration Manager and Solution Control Interface, and during the installation

of any Framework Wizard.

Refer to the ''Genesys 8.1 Security Deployment Guide'' for more details about the security banner.

## Genesys Security Using the TLS Protocol

Genesys supports the optional use of the Transport Layer Security (TLS) protocol to secure data transfer between its components. TLS is supported on Windows and UNIX platforms.

To enable secure data transfer between Genesys components that support this functionality, you must configure additional parameters in the `Host` objects and `Application` objects that represent these components. Certificates and corresponding private keys are generated using standard Public Key Infrastructure (PKI) tools, such as OpenSSL and Windows Certification services.

For detailed information about Genesys Security Using the TLS Protocol, refer to the ''Genesys 8.1 Security Deployment Guide''.

### Multiple Ports

To provide flexibility in configuring a system with the Genesys Security using the TLS Protocol feature, you can configure multiple ports on a given server with either secure or unsecured connections. You specify the additional ports in the `Server Info` of the server's `Application` object.

Each port can have one of the following listening modes:

- unsecured-The port is not secured by TLS. This is the default status of a port.
- secured-The port is secured by TLS.
- auto-detect-This status applies only to ports on the Configuration Server, and is used only when configuring secure connections to the Configuration Server. If an application that is trying to connect to an auto-detect port has security settings specified in its configuration, Configuration Server checks the validity of those settings. Depending on the results, the client will be connected in secure or unsecured mode.

Refer to the ''Genesys 8.1 Security Deployment Guide'' for more information about multiple ports.

### <div="multCSports">

#### Multiple Ports on Configuration Server

When you install Configuration Server, the listening port that you specify during installation is stored in the configuration file as the port option. When Configuration Server first starts with an initialized database, it reads the `port` option in the configuration file. The value of the `port` option is also propagated to the Configuration Database, where it is stored as part of the Configuration Server `Application` object. As additional ports are configured, they are also stored in the Configuration Database as part of the Configuration Server `Application` object. On subsequent startups of Configuration Server-that is, on all startups after the first-Configuration Server reads the port information from the Configuration Server `Application` object, ignoring the `port` option in the configuration file.

If necessary, you can specify an additional unsecured listening port in the Configuration Server command line during subsequent startups. This additional port is not written to the Configuration Server `Application` object, and does not survive a restart of Configuration Server. Use this option only when regular ports cannot be opened. See `-cfglib_port` for more information about this option.

### Secure Connections

In addition to configuring secure ports on your server applications, you must configure your client applications, both server and user interface types, to connect to these ports. Use Genesys Administrator to configure these connections.

There are only two exceptions to this standard procedure, as follows:

- Configuring secure connections to the Configuration Server-You must configure a Configuration Server port as an auto-detect port.
- Configuring a secure connection between DB Server and Configuration Server-You must configure the secure connection in the configuration files of the two components.

Refer to the ''Genesys 8.1 Security Deployment Guide'' for detailed instructions for configuring secure connections.

## European Data Protection Directive Disclaimer

The Genesys suite of products is designed to make up part of a fully functioning contact center solution, which may include certain non-Genesys components and customer systems. Genesys products are intended to provide customers with reasonable flexibility in designing their own contact center solutions. As such, it is possible for a customer to use the Genesys suite of products in a manner that complies with the European Data Protection Directive (EDPD). However, the Genesys products are merely tools to be used by the customer and cannot ensure or enforce compliance with the EDPD. It is solely the customer's responsibility to ensure that any use of the Genesys suite of products complies with the EDPD. Genesys recommends that the customer take steps to ensure compliance with the EDPD as well as any other applicable local security requirements.

# 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 to the Framework 8.1 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.

#### [+] Recommendations for planning Configuration Database installation

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 enterprise installation.
- 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.

### [+] Recommendations for planning Configuration Server deployment

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.

#### [+] Recommendations for planning Configuration Server Proxy deployment

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 8.1 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 8.5 Management Layer User's Guide'' for descriptions of, and recommendations for, these components.

#### [+] Required 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 Built-in 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.

### Built-in 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 or a third-party SNMP master agent compliant with the AgentX protocol
- Message Server if SNMP alarm signaling is required

## Management Layer Components

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

### Local Control Agent

#### [+] Recommendations for planning Local Control Agent deployment

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.
- If you will be using Genesys Administrator Extension to deploy Genesys applications and solutions to any hosts in your network, you must install and run the latest instance of LCA on each target host. This will install a remote deployment agent (referred to as the *Genesys Deployment Agent*) that is used by Genesys Administrator Extension to carry out the deployment on that host.

Message Server

## [+] Recommendations for planning Message Server deployment

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`.
- 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

## [+] Recommendations for planning Solution Control Server deployment

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 |

## [+] Recommendations for planning Centralized Log Database installation

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 both of these conditions apply:

- 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.
- You don't have another AgentX-compatible SNMP master agent in place.

## 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.

**[+] Recommendations for planning T-Server deployment**

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.

# Installation Worksheet

Use the following tables to help prepare for and perform the installation of Framework components:

- Installation Summary
- Database Information
- Licensing Information
- Application Configuration Parameters
- Windows Application Program Folders (for Windows applications only)

## Installation Overview

| Installation Summary | |
|---|---|
| Person responsible | |
| Start date | |
| Completion date | |
| Database information | Refer to Database Information |
| Licensing information | Refer to Licensing Information |
| Application configuration | Refer to Application Configuration Parameters |
| Program folders (for Windows applications only) | Refer to Windows Application Program Folders |

## Database Information

| Parameter | Value | | Description |
|---|---|---|---|
| **Config Database** | **Log Database** | | |
| DBMS Name | | | The name or alias identifying the SQL server DBMS that handles the database.<br>• For DB2, this value should be set to the name or alias-name of the database specified in the db2 client configuration.<br>• For Microsoft SQL, this value should be |

| Parameter | Value | | Description |
|---|---|---|---|
| | | | set to the name of the SQL server (usually the same as the host name of the computer on which Microsoft SQL runs).<br>• For Oracle, it is the SID or the net service name as specified in the `tnsnames.ora` file.<br>• For PostgreSQL, this value should be set to the name of the PostgreSQL server (usually the same as the host name of the computer on which PostgreSQL runs). |
| DBMS Type | | | The name of the database as it is specified in your DBMS. This value is required for all database types except Oracle. For DB2, Microsoft SQL, and PostgreSQL, this value is the name of the database where the client will connect. |
| User Name | | | The user name established to access the database. |
| Password | | | The password used for accessing the database. |

## Licensing Information

| Licensing Information | |
|---|---|
| **Parameter** | **Value** |
| **License Manager** | |
| host | |
| port | |
| **License Files** | |
| Full path and filename | |

| Licensing Information | |
|---|---|
| Full path and filename | |
| Full path and filename | |

## Application Configuration Parameters

When completing this table, remember that:

- All applications must be configured in the Configuration Layer unless otherwise noted.
- Host name or IP address can be specified as the value for the host parameter.
- Application port and working directory are only specified for server applications.
- Working directory is the full path to the directory in which the application is installed and/or is to be running.

| Application Type | Application Name | Application Host | Application Port | Working Directory |
|---|---|---|---|---|
| **Configuration Layer Components** | | | | |
| Configuration Server, Primary, for Configuration Database (configured via configuration file) | | | | |
| Configuration Server, Backup, for Configuration Database (configured via configuration file) | | | | |
| **Management Layer Components** | | | | |
| Local Control Agent | Not applicable | | Configured in Host properties | Not applicable |
| Database Access Point | | Not applicable | | |
| Message Server, Primary | | | | |
| Message Server, Backup | | | | |
| Solution Control Server, Primary | | | | |
| Solution Control Server, Backup | | | | |
| SNMP Master Agent, Primary | | | | |

| Application Type | Application Name | Application Host | Application Port | Working Directory |
|---|---|---|---|---|
| SNMP Master Agent, Backup | | | | |
| **User Interaction Layer Components** | | | | |
| Genesys Administrator | | | Not applicable | |
| **Media Layer Components** | | | | |
| T-Server, Primary, for switch ... | | | | |
| T-Server, Backup, for switch ... | | | | |
| T-Server, Primary, for switch ... | | | | |
| T-Server, Backup, for switch ... | | | | |
| **Services Layer Components** | | | | |
| Stat Server, Primary | | | | |
| Stat Server, Backup | | | | |

## Windows Application Program Folders

| Application | Application Program Folder |
|---|---|
| **Configuration Layer Components** | |
| Configuration Server, Primary, for Configuration Database (configured via configuration file) | |
| Configuration Server, Backup, for Configuration Database (configured via configuration file) | |
| **Management Layer Components** | |
| Local Control Agent | |
| Database Access Point | |
| Message Server, Primary | |
| Message Server, Backup | |
| Solution Control Server, Primary | |
| Solution Control Server, Backup | |
| SNMP Master Agent, Primary | |
| SNMP Master Agent, Backup | |
| **User Interaction Layer Components** | |
| Genesys Administrator | |

| Application | Application Program Folder |
|---|---|
| **Media Layer Components** | |
| T-Server, Primary, for switch ... | |
| T-Server, Backup, for switch ... | |
| T-Server, Primary, for switch ... | |
| T-Server, Backup, for switch ... | |
| **Services Layer Components** | |
| Stat Server, Primary | |
| Stat Server, Backup | |

# Deploying Framework

This section of the Framework Deployment Guide lists the prerequisites for installing the Genesys Framework, and prescribes the deployment order. It then describes how to install and configure the Management Framework components.

> **Tip**
> Use the sample worksheet as you prepare for and perform the Framework installation.

# Deployment Overview

The various Framework components are distributed on the following product CDs

- Management Framework
- Genesys Administrator
- Media
- HA Proxy
- Real-Time Metrics Engine

The Framework deployment process involves the configuration and installation of one or more components of the same type within each architecture layer, as outlined here.

## Sequence

Deploy Framework components in the following order:

1. Bootstrap components:
    a. Configuration Database
    b. Configuration Server (master/primary instance)
    c. Genesys Administrator/Extension
    d. License Reporting Manager (LRM) (see Licensing)
    e. Local Control Agent (LCA) on the hosts on which Configuration Server and LRM are installed
    f. Solution Control Server (SCS) (master/primary instance)

7. Configuration components:
    a. (Optional) High Availability (HA) Configuration Server pair (primary/backup instances
    b. (Optional) Configuration Server Proxies

3. Management components
    a. LCAs on all of the other hosts on which will be running Genesys server applications and/or monitored third-party server applications
    b. Message Server
    c. Centralized Log Database
    d. (Optional) HA SCS pair (primary/backup instances)
    e. (Optional) Distributed SCS
    f. (Optional) Genesys SNMP Master Agent (Simple Network Management Protocol)

7. Media Layer components
    a. T-Server
    b. HA Proxy for a specific type of T-Server (if required)

> **Important**
> Configuration and installation instructions for T-Servers apply to Network T-Servers as well. You can find detailed deployment information about T-Server and HA Proxy in the latest version of the T-Server Deployment Guide for your specific T-Server.

3. Services Layer component: Stat Server

> **Important**
> Although Interaction Server, SMCP (Simple Media Control Protocol) T-Server, and Stat Server components are all parts of the Framework architecture, configuring them directly depends on their usage in a Genesys solution. Therefore, you must install them during deployment of a specific solution.

## Creation of Configuration Objects

In addition to installed Framework components, the following resources must be registered as Configuration Database objects (or configuration objects) at the time of Framework deployment:

- Hosts
- Switching Offices
- Switches
- Agent Logins
- DNs
- Access Groups
- Skills
- Persons
- Agent Groups
- Places
- Place Groups

To deploy components of the Configuration Layer, you must first configure the objects and then install them, as described later in these pages.

> **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.

## Using DB Server

Starting in release 8.5, databases are accessed directly by the servers that need to store and/or retrieve data in them, removing the need to install DB Server. However, you can still use DB Server as in previous releases, if you have legacy components that require DB Server or you are unable to configure Genesys components to access databases from their local hosts.

> **Important**
> Genesys strongly recommends that you use newer components that support direct database access. Note that, if you use DB Server, you will not be able to enjoy any benefits and new features for databases and database access that are introduced in this release.

For Configuration Server to access the Configuration Database, set the `dbthread` configuration option to `false` in the `confserv` section of the primary Configuration Server, and in the appropriately-named section of the backup server, if configured. For Message Server to access the Log Database, set the `dbthread` configuration option to `false` in the `messages` section of the primary Message Server and the backup Message Server, if configured. Refer to the ''Framework Configuration Options Reference Manual'' for more information about these options. For other products supporting this approach database access, refer to the product-specific documentation for the option name and instructions.

Then refer to the Framework 8.1 documentation for information about deploying and using DB Server to access the various databases in your environment.

Refer to the *Framework Database Connectivity Reference Guide* for detailed information about setting up and accessing a database.

# Prerequisites

Before you deploy Framework, investigate aspects of its size, security, availability and performance, as applied to the specific environment of your contact center. See Deployment Planning for recommendations on these issues. Be sure those applications that require licenses are licensed properly (see the ''Genesys Licensing Guide'').

Review the following prerequisites for your Framework installation:

- Databases
- Operating Environment, including hardware, networking, software, and internet browsers
- Licensing

For prerequisites for Genesys Administrator, refer to the ''Framework 8.1 Genesys Administrator Deployment Guide''.

# Database Prerequisites

Genesys recommends that you or your database administrator create databases in your database management system (DBMS) before you start a Genesys installation. For Framework, you must create two databases:

- Configuration Database-Mandatory for any Genesys installation.
- Centralized Log Database-Required only if you are using the Management Layer's centralized-logging function.

Genesys also recommends that you or your database administrator back up your Genesys databases on a regular basis.

Refer to Network Locations for Framework Components for recommendations on database sizing. Refer to your DBMS documentation for instructions on how to create a new database.

Refer to the Installation Worksheet for the list of database parameters you must use in your Genesys installation.

## Creating Databases for Multi-language Environments

If your system will be configured in a multi-language environment, or at least be required to handle data encoded in UTF-8 format, you may have to take special steps when creating your database, depending on the DBMS you will be using. Refer to the table in the "Creating Databases for Multi-language Environments" section of the *Framework Database Connectivity Reference Guide* for these additional steps.

## Creating Databases for Single-language Environments

If your system will be configured in a single-language environment, you must make sure that the encoding used in their database matches the encoding set up on all hosts. If they have to perform some type of conversion, because they are unable to store data in the same encoding specified at the operation system level, they must depend on the DBMS capabilities of the vendor client software.

# Operating Environment Prerequisites

## Hardware and Networking

Genesys recommends that you or your IT specialist assign host computers to Genesys software before you start Genesys installation.

If you are considering using IPv6 for some or all connections, make sure that you first review the information in IPv6.

Refer to Network Locations for Framework Components for recommendations on server locations.

## Software

Refer to the *Genesys Supported Operating Environment Reference Guide* for the list of operating systems and database systems supported in Genesys releases. Refer to the ''Genesys Supported Media Interfaces Reference Guide'' for the list of supported switch and PBX versions.

For UNIX operating systems, also review the list of patches Genesys uses for software product builds and upgrade your patch configuration if necessary. A description of patch configuration is linked to the Readme files for the Genesys applications that operate on UNIX.

## Internet Browsers

To view all elements of Genesys Administrator, you need any combination of Internet Explorer and and/or Mozilla Firefox internet browsers.

Refer to the ''Framework Genesys Administrator Deployment Guide'' for information about supported browser versions, and requirements for the Genesys Administrator web server.

# Licensing Prerequisites

Genesys applications require licenses. There are two aspects of licensing for Genesys software:

- Sellable Item licenses, which provide the legal right to deploy and use the components and functionality related to the solutions that you purchased from Genesys.
- Technical license keys, which enable you to use particular functionality. For example, if you are planning to deploy redundant configurations of any Genesys servers, you must have a special high-availability (HA) license. Otherwise, the Management Layer will not perform a switchover between the primary and backup servers. As another example, a technical license is required to deploy Configuration Server Proxy.

Technical licenses are managed and controlled by the FlexNet Publisher (formerly FlexLM) License Manager. In release 8.5, the use of sellable item licenses is now measured by License Reporting Manager (LRM), which provides historical usage reports to system administrators.

For information about which products require what types of licenses, refer to the ''Genesys Licensing Guide''. That Guide also describes how to install FlexNet Publisher License Manager, if required, before you start to deploy Management Framework.

## License File

Genesys Technical licensing is based on a valid license file that contains license key information required to operate Genesys components, where required. Request the initial license file from Genesys after you purchase your Genesys system, when you are ready to deploy Management Framework. FlexNet Publisher uses the license keys in the license file to enable certain components to operate. Starting in release 8.5, Configuration Server also uses the license file to authenticate the right to use the software at startup of every new deployment of Genesys Framework.

## License Files and the Configuration Database

Configuration Server stores the license file in the Configuration Database. When you are setting up your new Genesys environment, or when you have just upgraded your Configuration Database in an existing Genesys environment, you must upload the license file into the Database before you start Configuration Server for the first time. To do this, run the following command on the command-line, as appropriate:

- On UNIX: `confserv –license <license file name>`
- On Windows: `confserv.exe –license <filename>`

After that, you can start Configuration Server.

## Genesys License Reporting Manager

Genesys Framework uses the Genesys License Reporting Manager (LRM) to report on historical usage of licensed Genesys products (sellable items) and user-defined bundles. This data is used to provide Genesys users with license management reports, and Hosted Service Providers with billing data.

For a new deployment of Genesys Framework, LRM must be installed after Configuration Server and Genesys Administrator are installed. After you have uploaded the contents of the license file to the Configuration Database and LRM is installed, additional applications can then be deployed, based on the validity of their licenses.

The License Reporting Manager (LRM) Server connects only to the master Configuration Server.

> **Important**
>
> Genesys strongly recommends that you start LRM before you install a backup Configuration Server. If you start LRM afterwards, restart the backup Configuration Server to avoid a period of downtime for clients of Configuration Server, other than LRM, when Configuration Server switchover occurs.

When the first LRM instance is connected (or reconnected) to the Configuration Server instance that is enabled for LRM monitoring, Configuration Server generates the log event `21-25100 LRM Server connected successfully, system operating normally`.

A connection between LRM Server and Configuration Server is not required for Configuration Server to accept connections from other Genesys Framework components. However, if Configuration Server is running on a new (or upgraded) database and is only in the first startup stage (LRM has not started yet), it will not accept a connection from any Genesys Business Application.

At initial startup only, when a Genesys Business Application tries to connect to Configuration Server and Configuration Server cannot validate the presence of LRM, Configuration Server generates log event `21-25101 Unable to accept connection: LRM Server has not been started` and refuses the connection request. After LRM has been detected at least once, connections are no longer refused for this reason.

If the connection to the LRM Server is lost, Configuration Server generates log event `21-25102 LRM Server has disconnected`. However, Configuration Server still continues to accept connections from Genesys Business Applications.

For more information about LRM, including how to install and use it, refer to LRM documentation.

## Configuration Server and LRM

Periodically, at startup and during normal operations, Configuration Server and LRM interact to ensure that the license file and the Configuration Database are synchronized.

## At Intial Startup

After Configuration Server has started up for the first time against a new (or upgraded) database, Configuration Server is able to accept client applications of the following types:

- Genesys Administrator and Genesys Administrator Extension
- Message Server and Solution Control Server
- LRM Server
- ITC Utility (IP installer)

Attempting to start and connect any other application at this stage, before LRM has started, will result in Configuration Server generating an error and log message `21-25101 Unable to accept connection: LRM Server has not been started`.

> **Tip**
> Genesys recommends that if you want to configure a backup Configuration Server, you do so only after LRM has started.

At this point, LRM must be installed and started, after which it creates the entitlement description based on the license and entitlement information retrieved from the copy of the license file in the Configuration Database. LRM uses this entitlement information as a reference and to flag over-use on reports.

If the license information has uploaded successfully and Configuration Server initialized properly, the read-only option `license` might appear in the configuration options of the Configuration Server object.

> **Warning**
> Do not attempt to modify the value of this option in any way. Any such attempt might render Configuration Server to become inoperable.

## At Subsequent Restarts

After subsequent restarts (after LRM has started), all connections are allowed. If LRM does not connect shortly after the current Configuration Server switching to primary, Configuration Server generates log message `21-25102 LRM Server has disconnected`. When LRM finally reconnects, log message `21-25100 LRM Server connected successfully, system operating normally` is generated, to clear the previous condition. Otherwise, there is no impact on Configuration Server functionality if LRM does not reconnect.

> **Warning**
> Genesys License Compliance policy requires that LRM be connected and operating at all times for Genesys 8.5 and later releases. Disconnection of LRM for an extended period may be considered a violation of Genesys licensing terms and agreements.

### During Normal Operations

Configuration Server constantly monitors the content of the license file stored in the Configuration Database to confirm that the information is still valid. When the file expires, Configuration Server logs an error message but continues to serve clients. To dismiss this error, you must load the new license file by running the following command on the command-line, as appropriate:

- On UNIX: `confserv –license <license file name>`
- On Windows: `confserv.exe –license <filename>`

You do not need to stop and/or restart the Configuration Server that is currently running in primary mode.

> **Important**
> After the database is updated, it may take up to 10 minutes for the new license information to propagate to LRM and for Configuration Server to stop generating out-of-compliance log messages.

# Permission Prerequisites

This section describes the minimum permissions required to install and run Management Framework components. For information about minimum permissions required for other Genesys components, refer to product- or component-specific documentation.

## System Permissions

The following table provides the minimum permissions required to install and run Framework components.

| Component | Minimum Permissions (UNIX) | Minimum Permissions (Windows) |
|---|---|---|
| Configuration Server | `users` group | `Administrators` group [a] |
| Solution Control Server | `users` group | `Administrators` group |
| Message Server | `users` group | `Administrators` group |
| SNMP Master Agent | `users` group | `Administrators` group |
| Local Control Agent [b] | `root` | `Administrators` group |

a. The user account for the running process is usually determined by the user or object that started the process. For example, if a process is started by LCA, then the process inherits its permissions from LCA.

b. `root` or `Administrators` permission is required to install the component because, during installation, it updates the startup file and registry.

After a component is installed, you can update the component to start under a different user account with lower privileges. However, before doing so, make sure that you updated the working directories with the correct read and write permissions.

### Example

To run LCA and Genesys Deployment Agent (GDA) as a non-root user, do one of the following, depending on your operating system:

## On UNIX

Create startup scripts for LCA and GDA that set up LCA and GDA to run under the non-root user. For these scripts, it is assumed that LCA is installed in `/home/genesys/GCTI`, and the name of the non-root user is `genesys`. See LCA Startup Script-gctilca and GDA Startup Script-gctigda for examples of these scripts. To install the startup scripts, put them in the directory `/etc/rc/d/init.d/` and run one or both of the following commands, as required:

```
chkconfig -add gctilca
chkconfig -add gctigda
```

## On Windows

Change the account associated with the LCA service. One way to do this is through Windows Administrative Services, as follows:

1. Go to Start > Settings > Control Panel > Administrative Services > Services, right-click LCA and select Properties.
2. Open the Log On tab and in the Log on as section, select This account, and change the account associated with the LCA service.

## Database User Privileges

A database user that accesses the Configuration Database on behalf of Configuration Server, that is, the user identified in the Configuration Server configuration file, requires basic database privileges, as defined in this section.

When the database is created, it is assumed that it is created under the new user and the initialization scripts are under that user account, unless otherwise stated.

## Oracle

After the new database user is created, grant the necessary privileges as follows:

```
GRANT CONNECT TO <DB user>
GRANT CREATE TABLE TO <DB user>
GRANT UNLIMITED TABLESPACE TO <DB user>
GRANT CREATE PROCEDURE TO <DB user>
```

## MS SQL

For MS SQL 2000, grant the public role to the new database user on the Database Access tab of the SQL Server Login Properties dialog box for the new user. In addition, grant the following privileges:

```
GRANT CREATE TABLE TO <DB user>
GRANT CREATE PROCEDURE TO <DB user>
```

For MS SQL 2005 and later, grant the public and db_owner roles to the new database user.

## DB2

Grant the necessary privileges as follows:

```
CONNECT TO <database>;
GRANT CREATE TAB,CONNECT ON DATABASE TO USER <DB user>;
CONNECT RESET;
```

## PostgreSQL

From pgAdmin, grant the following privileges:

- Can create database object
- Can create roles

Or, you can execute the following query:

```
CREATE ROLE <DB user> LOGIN ENCRYPTED PASSWORD <encrypted password> NOINHERIT CREATEDB CREATEROLE VALID UNTIL 'infinity';
```

To configure client authentication, update the pg_hba.conf file, located in the data directory under the PostgreSQL installation folder. For example:

```
host GCTI_Test gctitest <IP address1>/32 trust
host GCTI_Test gctitest <IP address2>/32 trust
```

This enables the DB user gctitest to connect to the GCTI_Test database from the hosts <IP address1> and <IP address2>.

## Sample Scripts

This section contains sample scripts required to run LCA and GDA on UNIX under a non-root user.

### LCA Startup Script-gctilca

The following is an example of a script to allow LCA to run under a non-root user.

```
#!/bin/bash
#
# chkconfig: 345 80 20
# description: run lca
#
# You should put this script to /etc/rc.d/init.d and run command:
# chkconfig --add gctilca
#GCTI home dir
GCTI=/home/genesys/GCTI
DIRNAME=LCA
HOMEDIR=$GCTI/$DIRNAME
USER=genesys
SCRIPTNAME=gctilca
HOME_USER=/home/genesys
```

```
PATH=/sbin:/bin:/usr/bin:/usr/sbin
prog=lca
RETVAL=0
if [ ! -x $HOMEDIR/$prog ]; then
exit 1
fi
# Source function library.
. /etc/rc.d/init.d/functions
start () {
echo -n $"Starting $SCRIPTNAME: "
if [ -e /var/lock/subsys/$prog ]; then
echo -n $"$SCRIPTNAME is already running.";
failure $"cannot start $SCRIPTNAME: $SCRIPTNAME already running.";
echo
return 1
fi
daemon --user=$USER ". $HOME_USER/.bash_profile ; cd $HOMEDIR ;
   ./run.sh >/dev/null 2>/dev/null &"
sleep 1
CHECK=`ps -e | grep $prog | grep -v $SCRIPTNAME | awk '{print $4}'`
if [ "$CHECK" = "$prog" ]; then
RETVAL=0
else
RETVAL=1
fi
[ $RETVAL -eq "0" ] && touch /var/lock/subsys/$prog
echo
return $RETVAL
}
stop () {
echo -n $"Stopping $SCRIPTNAME: "
if [ ! -e /var/lock/subsys/$prog ]; then
echo -n $"$SCRIPTNAME is not running."
failure $"cannot stop $SCRIPTNAME: $SCRIPTNAME is not running."
echo
return 1;
fi
killproc $prog
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/$prog;
return $RETVAL
}
usage ()
{
echo "Usage: service $PROG {start|stop|restart}"
}
case $1 in
start)
start
;;
stop)
stop
;;
restart)
stop
start
;;
*)
usage ; RETVAL=2
;;
esac
exit $RETVAL</tt>
```

## GDA Startup Script-gctigda

The following is an example of a script to allow GDA to run under a non-root user.

```
#!/bin/bash
#
# chkconfig: 345 80 20
# description: run gda
#
# You should put this script in /etc/rc.d/init.d and run command:
# chkconfig --add gctigda
#GCTI home dir
GCTI=/home/genesys/GCTI
DIRNAME=LCA
HOMEDIR=$GCTI/$DIRNAME
USER=genesys
SCRIPTNAME=gctigda
HOME_USER=/home/genesys
PATH=/sbin:/bin:/usr/bin:/usr/sbin
prog=gda
RETVAL=0
if [ ! -x $HOMEDIR/$prog ]; then
exit 1
fi
# Source function library.
. /etc/rc.d/init.d/functions
start () {
echo -n $"Starting $SCRIPTNAME: "
if [ -e /var/lock/subsys/$prog ]; then
echo -n $"$SCRIPTNAME is already running.";
failure $"cannot start $SCRIPTNAME: $SCRIPTNAME already running.";
echo
return 1
fi
daemon --user=$USER ". $HOME_USER/.bash_profile ; cd $HOMEDIR ;
   ./gda >/dev/null 2>/dev/null &"
sleep 1
CHECK=`ps -e | grep $prog | grep -v $SCRIPTNAME | awk '{print $4}'`
if [ "$CHECK" = "$prog" ]; then
RETVAL=0
else
RETVAL=1
fi
[ $RETVAL -eq "0" ] && touch /var/lock/subsys/$prog
echo
return $RETVAL
}
stop () {
echo -n $"Stopping $SCRIPTNAME: "
if [ ! -e /var/lock/subsys/$prog ]; then
echo -n $"$SCRIPTNAME is not running."
failure $"cannot stop $SCRIPTNAME: $SCRIPTNAME is not running."
echo
return 1;
fi
killproc $prog
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/$prog;
return $RETVAL
}
usage ()
```

```
{
echo "Usage: service $PROG {start|stop|restart}"
}
case $1 in
start)
start
;;
stop)
stop
;;
restart)
stop
start
;;
*)
usage ; RETVAL=2
;;
esac
exit $RETVAL
```

# Deploying Configuration Layer

The Framework Configuration Layer is a mandatory part of any Genesys installation and is the first step of the Framework deployment.

### Important

Before you install Framework components:

- Refer to Network Locations for Framework Components for recommendations on the network locations of these components.
- Create a new database following the instructions in your DBMS documentation.

### Warning

During installation on UNIX, all files are copied into a user-specified directory. The installation creates no subdirectories within this directory, so be careful to not install different products into the same directory.

If you are installing the Framework for the first time, follow the instructions for a first time deployment. If you are upgrading your Genesys Framework, refer to the ''Genesys Migration Guide''. Otherwise, to install new individual components, follow the instructions on the following pages to install the appropriate Configuration Layer component.

After you have a successfully installed and configured Configuration Layer components, you can implement any of the following, as appropriate:

- Enable the Management Layer to control the Configuration Layer (recommended)
- Encrypt a password for the Configuration Database (recommended)
- Configure a user inactivity timeout to disable logged-in users after a period of inactivity. Refer to the ''Genesys 8.1 Security Deployment Guide'' for instructions.
- Configure redundant Configuration Servers in HA pairs.
- Configure one or more Configuration Server Proxies.

# First-Time Deployment

To install the Framework Configuration Layer components for the first time, follow these steps:

1. Install Configuration Server
2. Initialize the Configuration Database
3. Configure Configuration Server
4. Start Configuration Server
5. Deploy and start Genesys Administrator
6. Deploy and start License Reporting Manager (LRM) as described in the *LRM 8.5 Deployment Guide*
7. Create Hosts for each computer in your network

# Configuration Database

After you have created a database in your DBMS (see Databases), you can populate the tables of the Configuration Database manually (using your DBMS tools).

## Setting Up the Configuration Database

### Important

If you install Configuration Server and the Configuration Database separately, you must install and configure an SQL Server client for your database type on the same host where Configuration Server is running. Please refer to the *Framework Database Connectivity Reference Guide* for recommendations on environment settings for your database client.

### Warning

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.

1. In the directory in which Configuration Server is installed, open the `sql_scripts` folder.
2. Open the folder that matches your database type.
3. Load and execute the initialization script that corresponds to your DBMS and your environment (enterprise or multi-tenant), as listed in the table below.

### Tip

If you are using the DB2 DBMS, Genesys recommends using the DB2 Command-Line Processor to run Genesys SQL scripts. **[+] Show steps**

1. Start the Command-Line Processor.
2. Type `quit` at the DB2 prompt to exit the `DB2.exe` process.
3. Specify the database connection parameters by typing the following command line, substituting values in brackets with the actual values:
   `db2 connect to <database name> user <user> using <password>`

4. Execute the script by typing the following command line, substituting the value in brackets with the actual value:
   `db2 -f <script name including full path>`
   For example, to execute the initialization script for the enterprise version of the Configuration Database, type (all on one line):
   `db2 -f C:\GCTI\ConfigurationServer\sql_scripts\db2\init_single_db2.sql`

| DBMS | Enterprise Script Name | Multi-Tenant Script Name | Multi-language Script Name (see Note) |
|---|---|---|---|
| DB2 | init_single_db2.sql | init_multi_db2.sql | Enterprise: init_single_multilang_db2.sql<br>Multi-tenant: init_multi_multilang_db2.sql |
| Microsoft SQL | init_single_mssql.sql | init_multi_mssql.sql | Enterprise: init_single_multilang_mssql.sql<br>Multi-tenant: init_multi_multilang_mssql.sql |
| Oracle | init_single_ora.sql | init_multi_ora.sql | Enterprise: init_single_multilang_ora.sql<br>Multi-tenant: init_multi_multilang_ora.sql |
| PostgreSQL | init_single_postgre.sql | init_multi_postgre.sql | Enterprise: init_single_multilang_postgre.sql<br>Multi-tenant: init_multi_multilang_postgre.sql |

**Note:** Use the multi-language scripts if you are setting up Configuration Server in multi-language mode.

4. Load and execute the script that loads the `CfgLocale` table into the initialized database, depending on your database type, as shown in the table below.

### Tip

If you are using the DB2 DBMS, Genesys recommends using the DB2 Command-Line Processor to load and execute the script, as follows: **[+] Show steps**

1. Start the Command-Line Processor.
2. Type `quit` at the DB2 prompt to exit the `DB2.exe` process.
3. Specify the database connection parameters by typing the following command line, substituting values in brackets with the actual values:

```
db2 connect to <database name> user <user> using <password>
```

4. Execute the script by typing the following command line, substituting the value in brackets with the actual value:
   `db2 -f <script name including full path>`
   For example, to execute the `CfgLocale` script, type (all on one line):
   `db2 -f C:\GCTI\ConfigurationServer\sql_scripts\db2\CfgLocale_db2.sql`

| DBMS | Script Name |
|---|---|
| DB2 | CfgLocale_db2.sql |
| Microsoft SQL | CfgLocale_mssql.sql |
| Oracle | CfgLocale_ora.sql |
| PostgreSQL | CfgLocale_postgre.sql |

## About the Initialized Configuration Database

### 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 Technical Support before you do so.

The Configuration Database contains the following predefined objects, which allow initial access to the database through Genesys Administrator:

- A `User` object with user name set to `default`, and password set to `password`. Use this Master Account to log in to the Configuration Layer for the first time. A user logged on through this Master Account has all possible privileges with respect to objects in the Configuration Database. The Master Account is not alterable in any way, and you should not use it to perform regular contact center administrative tasks. Rather, it exists as a guarantee that, no matter what happens to the regular accounts, you will always be able to access the Configuration Database.
  Genesys recommends changing the default user name and password of the Master Account during the first session, securing these login parameters, and using the Master Account for emergency purposes only. For regular operations, create a real working account and add it to the access group Super Administrators. (By default, this Access Group has the same privileges as the Master Account.) Use this real working account for any subsequent sessions.

> **Important**
>
> For instructions on creating new configuration objects, and working with existing configuration objects, refer to ''Framework 8.1 Genesys Administrator Help''.

- Four `Application Template` objects, as follows:
  - Configuration Server
  - Configuration Manager
  - Genesys Administrator
  - Genesys Administrator Server
- Five `Application` objects, as follows:
  - `confserv` object of type Configuration Server.
  - `default` object of type Configuration Manager.
  - `Genesys Administrator` object of type Genesys Administrator.

    > **Tip**
    >
    > Consider changing the name of this application during the first session.

  - `Genesys AdministratorServer` object of type Genesys Administrator Server.
  - Installation Configuration Utility `Application` object with the name set to `ITCUtility`. This utility supports configuration updates during installation processes for Genesys components. No additional configuration is needed..
- The default `Access Groups` objects: `Users`, `Administrators`, and `Super Administrators`. For more information, refer to Security Considerations.
- Folders for all types of objects managed by the Configuration Layer.

The Configuration Database also contains a number of other predefined objects (for example, `Alarm Conditions`) that help you set up some Genesys functionality as you deploy other Framework and solution components.

# Configuration Server

If you want Configuration Server to operate with the Configuration Database, you must install Configuration Server in *Master* mode. This Configuration Server must be configured through a local configuration file.

> **Important**
>
> - The procedures given in this section are for deploying a primary Configuration Server. To deploy a Configuration Server Proxy, refer to Configuration Server Proxy for relevant installation instructions. To install a backup Configuration Server, refer to Redundant Configuration Servers.
> - Refer to the *Framework 8.5 External Authentication Reference Manual* for information about Configuration Server's External Authentication feature and for relevant deployment instructions.

## Deploying Configuration Server

For more information about the Configuration Server configuration file, see Configuration Server Configuration File. For information about Configuration Server configuration options and their values, refer to the *Framework Configuration Options Reference Manual*.

1. Install Configuration Server. **[+] Show steps**

### Installing on UNIX

#### Installing Configuration Server on UNIX

1. On the Management Framework 8.5 product CD, locate and open the installation directory appropriate for your environment:
   - For an enterprise (single-tenant) environment, the installation directory is `configuration_layer/configserver/single/<operating_system>`.
   - For a multi-tenant environment, the installation directory is `configuration_layer/configserver/multi/<operating_system>`.

   The installation script, called `install.sh`, is located in the appropriate directory.
2. Type the file name at the command prompt, and press `Enter`.
3. For the installation type, type 1 to select Configuration Server Master Primary, and press `Enter`.

4. For the external authentication option, type the number corresponding to the type of external authentication that will be used (LDAP, Radius, both, or neither), and press `Enter`.

> **Tip**
> If you select LDAP, be prepared with the URL to access the LDAP Server. For more information about LDAP configuration, see the *Framework 8.5 External Authentication Reference Manual*.

5. Specify the full path of the destination directory, and press `Enter`.
6. If the target installation directory has files in it, do one of the following:
   - Type 1 to back up all the files in the directory, and press `Enter`. Specify the path to where you want the files backed up, and press `Enter`.
   - Type 2 to overwrite only the files in this installation package, and press `Enter`. Then type y to confirm your selection, and press `Enter`. Use this option only if the application already installed operates properly.
   - Type 3 to erase all files in this directory before continuing with the installation, and press `Enter`. Then type y to confirm your selection, and press `Enter`.

   The list of file names will appear on the screen as the files are copied to the destination directory.
7. For the product version to install, do one of the following:
   - Type 32 to select the 32-bit version, and press `Enter`.
   - Type 64 to select the 64-bit version, and press `Enter`.
8. To configure the Configuration Server during, or after, installation, do one of the following:
   - Type y to configure Configuration Server during installation (now), and press `Enter`. Go to Step 9 to specify values for the configuration file. For information about the Configuration Server configuration options and their values, refer to the *Framework Configuration Options Reference Manual*.
   - Type n to not configure Configuration Server during installation. In this case, you have finished installing Configuration Server-do not continue to the next step in this procedure. Before you can start Configuration Server, however, you must create a configuration file and set the configuration options in it.
9. For the `[confserv]` section:
   a. Specify a value for the Configuration Server port, and press `Enter`.
   b. Specify a value for the Configuration Server management port, and press `Enter`.
10. For the `[dbserver]` section:
    a. Type the number corresponding to the database engine that this Configuration Server uses (`dbengine`), and press `Enter`.
    b. Specify the name or alias of the DBMS that handles the Configuration Database (`dbserver`), and press `Enter`.
    c. To specify the name of the Configuration Database (dbname), do one of the following:

- If you are using an Oracle database engine (that is, you typed 3 in Step c), press Enter. This value is not required for Oracle.
- If you are using any other database engine, specify the name of the Configuration Database, and press Enter.

  {{NoteFormat|If you are using DB Server to access the Configuration Database, you must also specify values for host and port fields. Refer to Framework 8.1 documentation in this case.

d. Specify the Configuration Database username, and press Enter.

e. To specify the Configuration Database password, do one of the following:

- Specify the password, and press Enter.
- Press Enter if there is no password; that is, the password is empty, with no spaces.

When the installation process is finished, a message indicates that installation was successful. The process places Configuration Server in the directory specified during the installation process. The installation script also writes a sample configuration file, confserv.sample, in the directory in which Configuration Server is installed.

If you chose to configure the Configuration Server during installation, the sample configuration file, confserv.sample, is renamed confserv.conf, and the parameters specified in Steps 9 through 11 are written to this file.

If you chose to configure the Configuration Server after installation, you must manually rename the sample file confserv.conf and modify the configuration options before you start Configuration Server. Go to the next step.

# Installing on Windows

## Installing Configuration Server on Windows

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

1. On the Management Framework 8.5 product CD, locate and open the installation directory appropriate for your environment:
   - For an enterprise (single-tenant) environment, the installation directory is configuration_layer/configserver/single/windows.
   - For a multi-tenant environment, the installation directory is configuration_layer/configserver/multi/windows.
2. Locate and double-click setup.exe to start the Genesys Installation Wizard.
3. Click About on the wizard's Welcome page to review the read_me file. The file also contains a link to the server's Release Notes file.
4. On the Welcome page, click Next.
5. On the Configuration Server Run Mode page, select Configuration Server Master Primary.
6. On the Configuration Server Parameters page:

a. Specify the Server Port and Management Port for Configuration Server.

b. Click Next.

7. On the Database Engine Option page, select the database engine that the Configuration Server uses, and click Next.
8. On the DB Server Parameters page:
   a. Specify the Database Server Name and Database Name.
   b. Specify the Database User Name and Password.
9. On the Configuration Server External Authentication page, select the type of external authentication that the Configuration Server uses, or select None if Configuration Server is not using external authentication.
10. On the Choose Destination Location page, the wizard displays the destination directory specified in the Working Directory property of the server's Application object. If the path configured as Working Directory is invalid, the wizard generates a path to C:\Program Files\GCTI\<Singletenant or Multitenant> Configuration Server.

    If necessary, click one of the following:

    - Browse to select another destination folder. In this case, the wizard will update the Application object's Working Directory in the Configuration Database.
    - Default to reinstate the path specified in Working Directory. Click Next to proceed.
11. On the Ready to Install information page, click one of the following:
    - Back to update any installation information.
    - Install to proceed with the installation.
12. On the Installation Complete page, click Finish.

As a result of the installation, the wizard adds Application icons to the:

- Windows Start menu, under Programs > Genesys Solutions > Framework.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

2. Configure Configuration Server. If you manually installed Configuration Server on Windows, it was configured automatically during the installation process. You can skip this step. If you manually installed Configuration Server on UNIX and chose not to configure it during the installation process, you must configure it now. **[+] Show steps**

### Prerequisites

- You manually installed Configuration Server on UNIX.
- You chose not to configure Configuration Server during the installation process.
- The Configuration Database has been initialized.

### Procedure

1. From the directory in which Configuration Server is installed, open the sample configuration file (`confserv.sample`) in a text editor.
2. Set the configuration options to work with the Configuration Database and DB Server. Consult the relevant chapters in the *Framework Configuration Options Reference Manual* for option descriptions and values. Refer also to Configuration Server Configuration File for a description of the configuration file.
3. Save the configuration file as `confserv.conf`.

### End of procedure

3. If required, configure Configuration Server for multi-language environment support. **[+] Show steps**

### Enable Configuration Server to Support UTF-8 Encoding in Multi-language Environments

Add the following options to the `confserv` (for Configuration Server) or `csproxy` (for Configuration Server Proxy) section of the configuration file:

- Set the `locale` option to the value corresponding to English (US). The database against which a UTF-8 enabled Configuration Server or Configuration Server Proxy is launched must be initialized using English locale scripts.
- Set the `encoding` option to `utf-8`.
- Set the `multi-languages` option to `true`. You must set this option after initializing the database and before you start Configuration Server against the UTF-8 enabled database.

For more information about these options, refer to the *Framework Configuration Options Reference Manual*.

4. Start Configuration Server. **[+] Show steps**

### Parameters

For descriptions of command-line parameters specific to Configuration Server, refer to Configuration Server.

> **Important**
>
> Use the `-c` command line option to point Configuration Server to a configuration file with the name other than the default name (`confserv.conf` on UNIX or `confserv.cfg` on Windows). For example, `confserv -c <configuration file name>`.

### Prerequisites

- Configuration Database is initialized.
- DB Server is installed and running.
- Configuration Server is installed.
- The Configuration Server configuration file is configured. Configuration Server uses this file for startup.

## Starting on UNIX

### Starting Configuration Server on UNIX

Go to the directory in which Configuration Server is installed and do one of the following:

- To use only the required command-line parameters, type the following command line:

```
sh run.sh
```

- To specify the command line yourself, or to use additional command-line parameters, type the following command line:

```
confserv [<additional parameters and arguments as required>]
```

## Starting on Windows

### Starting Configuration Server on Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which Configuration Server is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which Configuration Server is installed, and type the following command line:

```
confserv.exe [<additional parameters and arguments as required>]
```

- Use Windows Services Manager. Refer to Starting and Stopping with Windows Services Manager for more information.

# Configuration Server Configuration File

At a minimum, the configuration file contains the Configuration Server, Configuration Database, and Log sections.

The Configuration Server section contains the configuration options that define Configuration Server. The name of the section corresponds to the name of the Configuration Server `Application` object. For the initial installation of Configuration Server, it is called `confserv` by default. You can choose to rename this Configuration Server later. In all other cases, or if you rename the initial Configuration Server, the name of this section will be different. The `server` configuration option in this section specifies the name of the Configuration Database section.

By default, the Configuration Database section does not have a name. The section name must be the same as the value of the `server` configuration option that you specified in the Configuration Server section. The Configuration Database section contains information about the Configuration Database.

The name of the Log section is `log`. This section contains configuration information about the logging to be done by Configuration Server.

You can find a sample Configuration Server configuration file in the *Framework Configuration Options Reference Manual*.

## Configuring Configuration Server Logging

If you plan to use the centralized logging and auditing functionality of the Management Layer, specify appropriate log options in the Configuration Server configuration file before you start using Configuration Server. Most importantly, enable the network log output (for example, create a new option called `standard` and set its value to `network`). Refer to the *Framework Configuration Options Reference Manual* for more information.

## Changing Configuration Server Port Assignments

When you install Configuration Server, you specify values for the listening and management ports in the configuration file. You can change these values at any time.

Changing these port assignments depends on the type of port. To change the value of the management port, you must update the configuration file with the revised information, and restart Configuration Server.

Changing the value of the listening port is more complex. As described in Multiple Ports on Configuration Server, Configuration Server reads its listening port assignment from the configuration file once, at initial startup. For subsequent startups, it reads the port value from the Configuration Database. Therefore, you must change the value in the Configuration Database by modifying the `Port` property of the Configuration Server `Application` object.

### [+] Show steps

#### Prerequisites

- You are logged in to Genesys Administrator.

#### Procedure

1. In Genesys Administrator, select the `Provisioning` tab, go to `Environment` > `Applications`, and double-click the Configuration Server `Application` object for which you want to change the listening port.
2. On the `Configuration` tab, open the `Server Info` section.
3. In the list of Listening Ports, do one of the following:

- Click the port number that you want to change, enter the new port number, and either click outside of the edit box or press Enter.
- Highlight the port that you want to change and click Edit. On the General tab of the Port Info dialog box, enter the new port number in the Port text box. Then click OK to close the Port Info dialog box.

4. Click Save or Save & Close in the toolbar to save your configuration changes.

## Encrypting the Configuration Database Password

You can use Configuration Server to encrypt your password for accessing the Configuration Database so that it does not appear in plain text in the Configuration Server logs. This improves the security of your configuration data.

You can encrypt the password at any time, either during installation, or later. However, keep in mind that Configuration Server must be stopped during the encryption process.

For instructions on encrypting the Configuration Database password, refer to the *Genesys 8.1 Security Deployment Guide*.

# Install Genesys Administrator

Genesys Administrator is a web-based GUI application that replaces Configuration Manager and Solution Control Interface. You must install it before you can deploy the rest of your system.

Refer to the detailed instructions in ''Framework 8.1 Genesys Administrator Deployment Guide'' to deploy and start Genesys Administrator for your system.

# Create Hosts

Host objects represent computers in a network. Before you set up the Management Layer, you must configure a Host object for each computer on the data network on which you are going to run the Genesys daemon processes (usually server applications).

## Prerequisite

- You are logged in to Genesys Administrator.

## Procedure

1. In Genesys Administrator, go to Provisioning > Environment > Hosts.
2. Click **New**.
3. On the Configuration tab:
   a. Enter the name of the host, exactly as it is defined in the system configuration.

   > **Warning**
   > The host Name must be exactly the same as the host name defined in the system configuration.

   b. Enter the IP address of the host.
   c. Select the type of operating system from the OS Type drop-down list, and enter its version, if known.
   d. Enter the Local Control Agent (LCA) port number or accept the default (4999), to enable the Management Layer to control applications running on this host. This is also the port used by other applications installed on this host to connect to LCA. Refer to Notes on Configuring the LCA Port for additional information about configuring the LCA port value.
4. To customize the Advanced Disconnect Detection Protocol (ADDP) functionality that will be enabled between Solution Control Server (SCS) and LCA, on the Options tab:
   a. In the View drop-down list, select Advanced View (Annex).
   b. To specify the ADDP timeout between LCA and SCS, create a section called addp, add the option addp-timeout inthis section, and specify a value.
   c. To enable sending LCA polling messages to SCS, in the section addp, add the option addp-remote-timeout, and specify a value.

   Refer to Configuring ADDP Between Solution Control Server and Local Control Agent for more information. For detailed information about the configuration options themselves, refer to the ''Framework Configuration Options Reference Manual''.
5. Click **Save and Close**.

For more information about setting configuration options using Genesys Administrator, refer to

''Genesys Administrator 8.1 Help''. For more information about specific configuration options, refer to the ''Framework Configuration Options Reference Manual''.

# Enabling Management Layer to Control Configuration Layer

To enable the Management Layer to control (start, stop, and monitor) Configuration Server, you must modify the Configuration Server application to communicate with the Local Control Agent (LCA), as follows:

## Prerequisites

- Configuration Server is installed and running, and its `Application` object is created.
- A Host object exists for the computer on which this Configuration Server will be running. See Creating Hosts.
- You are logged in to Genesys Administrator.

## Procedure

1. Go to `Provisioning` > `Environment` > `Applications`, and click the Configuration Server `Application` object (named `confserv`) to open its properties.
2. On the `Configuration` tab, open the `Server Info` section.
3. Select the host on which this Configuration Server runs.
4. Define the `Working Directory` and `Command Line` properties for the primary Configuration Server, if not already defined.
5. Click `Save and Close` to save the changes.

# Deploying Management Layer

The Management Layer controls the startup and status of solutions, logging of maintenance events, generation and processing of alarms, and management of application failures.

## Deployment Summary

Deploy Management Layer in this order:

1. Local Control Agent (LCA)—LCA must be installed to enable the Management Layer's solution-control and fault-management capabilities. You must install one LCA on each host running a Genesys server application.

   > **Important**
   > An application started by LCA inherits the environment variables from LCA. Therefore, when an application requires that particular environment variables be set, the same environment variables must be set for the account that runs LCA.

2. Database Access Point (DAP) for the Log Database
3. Message Server—You must configure a connection to Message Server for each Genesys server application to enable the Management Layer's centralized-logging and alarm-signaling capabilities.
4. Initialize the Log Database
5. Solution Control Server
6. Genesys SNMP Master Agent

Starting in 8.5, Genesys Administrator replaces Configuration Manager and Solution Control Interface (SCI) as the preferred interface for Management Framework. If you still want to use SCI, deploy it using the deployment instructions in the ''Framework 8.1 Deployment Guide''.

## Remote Deployment

You can deploy the Management Layer servers (Message Server, Solution Control Server, and Genesys SNMP Master Agent) to any host on your network using Genesys Administrator Extension. Refer to Genesys Administrator Extension documentation for more information and instructions.

# Next Steps

After you have successfully installed and configured the Management Layer components, consider whether you would like to configure the following:

- Force logged-in users to log in again after a period of inactivity. See Forced Re-Login for Inactivity.
- Redundant Message Servers, Solution Control Servers, or SNMP Master Agents. See Redundant Configurations.
- Distributed Solution Control Servers.

## Continuing the Installation of Your System

Once the Management Layer is set up, you can then deploy the rest of the Framework components, the contact center environment, and other Genesys Voice and Data applications.

# Local Control Agent (LCA)

To enable the Management Layer to control the startup and status of applications and solutions, and manage application failures, you must install an instance of Local Control Agent on every computer that is to run either Genesys server applications or third-party server applications you want to control with Management Layer.

Installing LCA also installs and activates a remote deployment agent, called the Genesys Deployment Agent, on that computer. Genesys Administrator Extension uses the Genesys Deployment Agent to remotely deploy Installation Packages to remote hosts in the network. See the *Genesys Administrator Extension Help* for more information about this functionality.

## Notes on Configuring the LCA Port

- The LCA port must be set to a value of 2000 or greater. When the LCA port is specified within the range of 1-1999, LCA starts on port number 4999 (default value).
- If the LCA port value is changed in the Host configuration while Solution Control Server (SCS) is connected to LCA, SCS does not disconnect from and reconnect to LCA; instead, the new LCA port value takes effect after LCA restarts.
- If you change the LCA port value for the LCA installed as a Windows Service, you must also change the LCA port number in the LCA startup parameters in the Registry Editor. The LCA Registry Key is located at:
  `(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lca_service\ImagePath)`
  The value must have the following format:
  `<full path>\lca.exe lt;LCA port number> -service <lca_service_name>`
  Change the LCA port number to the current value.

## Installing Local Control Agent

> **Important**
> All running LCA processes must be stopped before installing another LCA.

### [+] Installation Steps

## Installing on UNIX

## Installing LCA on UNIX

1. Stop all LCA processes that are running. If there are any LCA processes that are running when you begin the installation, the installation process will stop, and not restart until you have stopped those processes (see Step 4).
2. On the Management Framework product CD in the appropriate `management_layer/lca/<operating_system>` directory, locate a shell script called `install.sh`.
3. Type the file name at the command prompt, and press `Enter`.
4. Type `Enter`. This action will have one of the two following results.
   - If there are any LCA processes still running, you must exit from the installation and have to stop these processes before you can restart it.
   - Otherwise, you continue with the installation.
5. To specify the hostname for this LCA, do one of the following:
   - Type the name of the host, and press `Enter`.
   - Press `Enter` to select the current host.
6. Enter the Configuration Server host name, and press `Enter`.
7. Enter the Configuration Server network port, and press `Enter`.
8. Enter the Configuration Server user name, and press `Enter`.
9. Enter the Configuration Server password, and press `Enter`.
10. To specify the destination directory, do one of the following:
    - Press `Enter` to accept the default.
    - Enter the full path of the directory, and press `Enter`.
11. If the target installation directory has files in it, do one of the following:
    - Type 1 to back up all the files in the directory, and press `Enter`. Then specify the path to which you want the files backed up, and press `Enter`.
    - Type 2 to overwrite only the files in this installation package, and press `Enter`. Then type y to confirm your selection, and press `Enter`. Use this option only if the application already installed operates properly.
    - Type 3 to erase all files in this directory before continuing with the installation, and press `Enter`. Then type y to confirm your selection, and press `Enter`.

    The list of file names will appear on the screen as the files are copied to the destination directory.
12. For the product version to install, do one of the following:
    - Type 32 to select the 32-bit version, and press `Enter`.
    - Type 64 to select the 64-bit version, and press `Enter`.
13. If you are authorized to modify startup (RC) files, you are prompted to add LCA to the startup files. Do one of the following:
    - Press `Enter` to add LCA to the startup files.
    - Type n to leave LCA out of the startup files, and press `Enter`.

> **Important**
>
> On UNIX systems, LCA 8.1.0 and earlier is installed with the autostart capability created automatically for run level 3. If you are using another run level, you must modify your operating system startup scripts by adding the startup of LCA.

# Installing on Windows

## Installing LCA on Windows

1. Stop all LCA processes that are running.
2. On the Management Framework product CD in the appropriate `management_layer\lca\windows` directory, locate and double-click `setup.exe` to start the Genesys Installation Wizard.
3. Use the `About` button on the wizard's `Welcome` page to view the `read_me` file. The file also contains a link to the server's Release Notes file.
4. Click `Next` to start the installation.
5. On the `Connection Parameters to the Genesys Configuration Server` page, specify the host name, port, user name, and password for Configuration Server, and then click `Next`.
6. On the `Choose Destination Location` page, the wizard displays the default folder `C:\Program Files\GCTI\Local Control Agent`.
   If necessary, click one of the following:
   - `Browse` to select another destination folder.
   - `Default` to reinstate the default folder, `C:\Program Files\GCTI\Local Control Agent`.
7. On the `Ready to Install` page, click one of the following:
   - `Back` to update any installation information.
   - `Install` to proceed with the installation.
8. On the `Installation Complete` page, click `Finish`.

As a result of the installation, the wizard adds Application icons to the:

- Windows `Start` menu, under `Programs` > `Genesys Solutions` > `Management Layer`.
- Windows `Add or Remove Programs` window, as a Genesys server.
- Windows `Services` list, as a Genesys service, with `Automatic` startup type.

{{NoteFormat|

- Because the Management Layer functionality requires LCA to be always running while its host computer is up, LCA is installed as a Windows Service with the `autostart` capability.

## LCA Log Options

Local Control Agent supports the unified set of log options (common log options) to allow precise configuration of log output. For a complete list of unified log options and their descriptions, see the "Common Log Options" section of the ''Framework Configuration Options Reference Manual''.

If you do not specify any log options for LCA, the default values apply. To specify log options for LCA, modify the `lca.cfg` configuration file that was created during LCA deployment, and is located in the same directory as the LCA executable. The LCA configuration file has the following format:

```
[log]
<log option name> = <log option value>
<log option name> = <log option value>
...
```

A sample LCA configuration file is available in the ''Framework Configuration Options Reference Manual''.

## Configuring ADDP Between Solution Control Server and Local Control Agent

Advanced Disconnection Detection Protocol (ADDP) is enabled automatically between Solution Control Server (SCS) and LCA. By default, SCS generates polling messages to LCA. If SCS does not receive messages from LCA within this interval, SCS sends a polling message. A lack of response to the polling message from LCA within the same time period is interpreted as a loss of connection.

If you want to change the ADDP timeout between SCS and LCA, configure the `addp-timeout` option. If you also want to enable LCA polling messages to SCS, configure the `addp-remote-timeout` option. Both of these options are set in the `Annex` of the `Host` object configured for the computer on which LCA runs. For detailed instructions on specifying these options, refer to the ''Framework Configuration Options Reference Manual''.

To avoid false disconnect states that might occur because of delays in the data network, Genesys recommends setting the ADDP timeouts to values equal to or greater than ten seconds.

# Database Access Points

To cover the variety of ways the applications in the Genesys installation can be interfaced with databases, the Configuration Layer uses the concept of a Database Access Point.

A Database Access Point (DAP) is a configuration object of the `Application` type that describes both the parameters required for communication with a particular database, such as JDBC parameters, and the parameters of the database itself. The DAP application you configure for the Management Layer enables Message Server to connects to the Log Database directly. If, according to your configuration, a database can be accessed by multiple applications simultaneously, register one DAP for each possible connection.

For detailed instructions for configuring the Log DAP, and more information about how Management Framework servers connect to databases, refer to the *Framework Database Connectivity Reference Guide*.

To interface an `Application` object with a database through a certain Database Access Point, add the DAP to the list of the application's Connections.

# Message Server

To deploy Message Server, do the following:

1. Configure a Message Server Application object. **[+] Show steps**

## Prerequisites

- A Database Access Point for the Log Database is configured.
- You are logged in to Genesys Administrator.

## Procedure

1. In Genesys Administrator, go to `Provisioning` > `Environment` > `Applications`, and select `New` in the toolbar. This opens a `Browse` dialog box that lists the available application templates. If a Message Server template file is not listed, do one of the following:
   - Import the `Message_Server_<current-version>.apd` file from the Management Framework 8.1 product CD.
   - Create a new template and repeat this step.
2. In the `Browse` dialog box, select the Message Server template file. The `Configuration` tab for the new Message Server `Application` object appears in the Details panel.
3. In the General section:
   - Enter a descriptive name in the `Name` field; for example, `MsgServer`.
   - Add a connection to the Log Database DAP. In the `Connections` field:
     i. Click `Add`.
     ii. Enter the properties of the connection in the `Connection Info` dialog box.
     iii. Click `OK`.
4. In the `Server Info` section:
   a. In the `Host` field, click the magnifying glass icon to select the host on which this Message Server is running.
   b. For each listening port that an application must use to connect to Message Server:
      i. In the `Listening Ports` field, click `Add`.
      ii. Enter the port properties in the `Port Info` dialog box.
      iii. Click `OK`.
   c. For the `Working Directory`, `Command Line`, and `Command Line Arguments` fields, do one of the following:
      - Enter the appropriate information in the three text boxes. For information about command-line parameters, see Message Server.

- Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install Message Server, but only if the Installation Package can connect to Configuration Server.

5. If you want Message Server to direct log events to the Log Database, on the Options tab:
   a. In the drop-down list in the top-right corner, select Options if not already selected.
   b. In the messages section, change the value of the db_storage option to true.
6. Click Save or Apply in the toolbar to save the new object. The new object will appear in the list of applications.

2. Install Message Server. **[+] Show steps**

## On UNIX

> **Warning**
> During installation on UNIX, all files are copied into the directory you specify. The install process does not create any subdirectories within this directory, so do not install different products into the same directory.

### Prerequisite

- A Message Server Application object exists.

### Procedure

1. On the Management Framework 8.1 product CD in the appropriate management_layer/message_server/<operating_system> directory, locate a shell script called install.sh.
2. Type the file name at the command prompt, and press Enter.
3. To specify the host name for this Message Server, do one of the following:
   - Type the name of the host, and press Enter.
   - Press Enter to select the current host.
4. Enter the Configuration Server host name, and press Enter.
5. Enter the Configuration Server network port, and press Enter.
6. Enter the Configuration Server user name, and press Enter.
7. Enter the Configuration Server password, and press Enter.
8. The installation displays the list of Application objects of the specified type configured on this Host object. Type the number corresponding to the Message Server Application object you configured above, and press Enter.

9. To specify the destination directory, do one of the following:
   - Press Enter to accept the default.
   - Enter the full path of the directory, and press Enter.
10. If the target installation directory has files in it, do one of the following:
    - Type 1 to back up all the files in the directory, and press Enter. Specify the path to which you want the files backed up, and press Enter.
    - Type 2 to overwrite only the files in this installation package, and press Enter. Then type y to confirm your selection, and press Enter.
      Use this option only if the application already installed operates properly.
    - Type 3 to erase all files in this directory before continuing with the installation, and press Enter. Then type y to confirm your selection, and press Enter.

      The list of file names will appear on the screen as the files are copied to the destination directory.
11. For the product version to install, do one of the following:
    - Type 32 to select the 32-bit version, and press Enter.
    - Type 64 to select the 64-bit version, and press Enter.

## On Windows

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

### Prerequisite

- A Message Server Application object exists.

### Procedure

1. On the Management Framework 8.1 product CD in the appropriate management_layer\message_server\windows directory, locate and double-click setup.exe to start the Genesys Installation Wizard.
2. Click About on the wizard's Welcome page to review the read_me file. The file also contains a link to the server's Release Notes file.
3. Click Next to start the installation.
4. On the Connection Parameters to the Genesys Configuration Server page, specify the host name, port, user name, and password of Configuration Server, and then click Next.
5. On the Select Application page, select the name of the Message Server Application object that

you configured above, and then click Next.

6. On the Choose Destination Location page, the wizard displays the destination directory if specified in the Working Directory property of the server's Application object during configuration. If you entered a period (.) in this field when configuring the object, or if the path specified in this property is invalid, the wizard generates a path to the destination directory in the C:\Program Files\GCTI\<Product Name> format.
   If necessary,click one of the following:
   - Browse to select another destination folder. In this case, the wizard will update the Application object's Working Directory property in the Configuration Database.
   - Default to reinstate the path specified in the Working Directory property.

   Click Next to proceed.
7. On the Ready to Install page, click one of the following:
   - Back to update any installation information.
   - Install to proceed with the installation.
8. On the Installation Complete page, click Finish.

As a result of the installation, the wizard adds Application icons to the:

- Windows Start menu, under Programs > Genesys Solutions > Management Layer.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

# Centralized Log Database

## Initializing the Log Database

> **Important**
>
> - Message Server can only write logs to a PostgreSQL DBMS if the corresponding DB Server also supports PostgreSQL.
> - If you are using the Oracle DBMS, Genesys strongly recommends that you use the SQL Plus command line utility initializing the Log Database.
> - If you are setting up the Log Database for use in a multi-language environment, refer to the *Framework Database Connectivity Reference Guide* for additional information.

### Prerequisites

- A DBMS is installed, and a blank database has been created.
- Message Server is installed and running.

### Start of procedure

1. In your DBMS interface, go to the directory in which Message Server is installed and open the `scripts` folder.
2. Open the folder that matches your database type.
3. Load and execute the script that corresponds to your DBMS, as provided in the following table.

| DBMS | Script Name | Multi-language Script Name [a] |
|---|---|---|
| DB2 | init_db2.sql | init_multilang_db2.sql |
| Microsoft SQL | init_mssql.sql | init_multilang_mssql.sql [b] |
| Oracle | init_oracle.sql | init_multilang_oracle.sql |
| PostgreSQL | init_postgre.sql | Not required |

**Notes:**
**a.** Use the multi-language scripts if you are setting up your Centralized Log system in multi-language mode.
**b.** A multi-language MS SQL database uses UCS-2 encoding instead of UTF-8 encoding. You must set `utf8-ucs2=true` in the `dbclient` section in the annex of the corresponding Database Access Point. Refer to the ''Framework Configuration Options Reference Manual'' for more information about this option.

4. Save the initialized database.

## DBMS Adjustment

You must install and configure an SQL Server client for your database type. Refer to the *Framework Database Connectivity Reference Guide* for recommended environment settings for your database client.

# Solution Control Server

## Deploying Solution Control Server

To deploy Solution Control Server, do the following:

1. Configure a Solution Control Application object. **[+] Show steps**

### Prerequisite

- You are logged in to Genesys Administrator.

### Procedure

1. In Genesys Administrator, go to Provisioning > Environment > Applications, and select New in the toolbar. This opens a Browse dialog box that lists available application templates. If a Solution Control Server template file is not listed, do one of the following:
   - Import the Solution_Control_Server_<current-version>.apd file from the Management Framework 8.5 product CD.
   - Create a new template and repeat this step.
2. In the Browse dialog box, select the Solution Control Server template file. The Configuration tab for the new Solution Control Server Application object appears in the Details panel.
3. In the General section:
   a. Enter a descriptive name in the Name field-for example, SCS.
   b. If you want to enable alarm signaling, add a connection to the Message Server. In the Connections field:
      i. Click Add.
      ii. Enter the properties of the connection in the Connection Info dialog box.
      iii. Click OK.
4. In the Server Info section:
   a. In the Host field, click the magnifying glass icon to select the Host object on which this Solution Control Server is running.
   b. For each listening port that an application must use to connect to Solution Control Server:
      i. In the Listening Ports field, click Add.
      ii. Enter the port properties in the Port Info dialog box.
      iii. Click OK.
   c. For the Working Directory, Command Line, and Command Line Arguments fields, do one of the following:

- Enter the appropriate information in the three text boxes. For information about command-line parameters, see Solution Control Server.
- Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install Solution Control Server, but only if the Installation Package can connect to Configuration Server.

5. Click Save or Apply in the toolbar to save the new object. The new object will appear in the list of applications.

2. Install Solution Control Server. **[+] Show steps**

<tabber> On UNIX=

> **Warning**
> During installation on UNIX, all files are copied into the directory you specify. The install process does not create any subdirectories within this directory, so do not install different products into the same directory.

### Prerequisites

- A Solution Control Server Application object exists.

### Procedure

1. On the Management Framework 8.1 product CD in the appropriate management_layer/solution_control_server/<operating_system> directory, locate a shell script called install.sh.
2. Type the file name at the command prompt, and press Enter.
3. When prompted to install only the utilities, type n to install SCS and its utilities, and press Enter.
4. To specify the host name for this SCS, do one of the following:
   - Type the name of the host, and press Enter.
   - Press Enter to select the current host.
5. Enter the Configuration Server host name, and press Enter.
6. Enter the Configuration Server network port, and press Enter.
7. Enter the Configuration Server user name, and press Enter.
8. Enter the Configuration Server password, and press Enter.
9. The installation displays the list of Application objects of the specified type configured on this Host object. Type the number corresponding to the SCS Application object you configured above, and press Enter.
10. To specify the destination directory, do one of the following:
    - Press Enter to accept the default.
    - Enter the full path of the directory, and press Enter.

11. If the target installation directory has files in it, do one of the following:
    - Type 1 to back up all the files in the directory, and press Enter. Specify the path to which you want the files backed up, and press Enter.
    - Type 2 to overwrite only the files in this installation package, and press Enter. Then type y to confirm your selection, and press Enter.
      Use this option only if the application already installed operates properly.
    - Type 3 to erase all files in this directory before continuing with the installation, and press Enter. Then type y to confirm your selection, and press Enter.

      The list of file names will appear on the screen as the files are copied to the destination directory.
12. For the product version to install, do one of the following:
    - Type 32 to select the 32-bit version, and press Enter.
    - Type 64 to select the 64-bit version, and press Enter.
13. To decide whether you require a license, refer to the ''Genesys Licensing Guide'' for information about licensing requirements. Then, do one of the following:
    - Type y if you require a license, and press Enter.
    - Type n if you do not require a license, and press Enter.
14. If you typed y in the previous step, enter the license location format, press Enter, and enter the required parameters.

|-|

On Windows=

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

### Prerequisite

- A Solution Control Server Application object exists.

### Procedure

1. On the Management Framework 8.1 product CD in the appropriate management_layer\solution_control_server\windows directory, locate and double-click setup.exe to start the Genesys Installation Wizard.
2. Click About on the wizard's Welcome page to review the read_me file. The file also contains a link to the server's Release Notes file.
3. Click Next to start the installation.
4. On the Solution Control Server Installation Mode page, select Solution Control Server and Utilities, and then click Next.

5. On the Connection Parameters to the Genesys Configuration Server page, specify the host name, port, user name, and password of Configuration Server, and then click Next.
6. On the Select Application page, select the name of the SCS Application object that you configured above, and then click Next.
7. On the Run-time License Configuration page, select whether you are using a license. Refer to the ''Genesys Licensing Guide'' for information about licensing requirements, and then click Next.
8. If you selected Use License in the previous step, on the Access to License page, enter the license access type and required parameters.
9. On the Choose Destination Location page, the wizard displays the destination directory if specified in the Working Directory property of the server's Application object during configuration. If you entered a period (.) in this field when configuring the object, or if the path specified in this property is invalid, the wizard generates a path to the destination directory in the C:\Program Files\GCTI\<Product Name> format.
   If necessary, click one of the following:
   - Browse to select another destination folder. In this case, the wizard will update the Application object's Working Directory property in the Configuration Database.
   - Default to reinstate the path specified in the Working Directory property.

   Click Next to proceed.
10. On the Ready to Install page, click:
    - Back to update any installation information.
    - Install to proceed with the installation.
11. On the Installation Complete page, click Finish.

As a result of the installation, the wizard adds Application icons to the:

- Windows Start menu, under Programs > Genesys Solutions > Management Layer.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

## Solution Control Server Utilities

Solution Control Server includes four utilities:

- ccgs.pl-Graceful Call Center T-Servers stop script.
- gstuckcalls utility and Stuck Calls detection and deletion scripts-To handle T-Server stuck calls and raise alarms.
- logmsg utility-To send log messages on behalf of applications.
- mlcmd utility-To send and receive information to and from Solution Control Server.

For more information about these utilities and how to use them, see the ''Framework 8.5 Management Layer User's Guide''.

By default, the utilities are installed with SCS, but can be installed separately. **[+] Show steps**

## On UNIX

### Separately Installing SCS Utilities on UNIX

1. On the Management Framework 8.1 product CD in the appropriate directory under `management_layer/solution_control_server/<operating_system>` locate a shell script called `install.sh`.
2. Type the file name at the command prompt, and press `Enter`.
3. Type `y` to specify that you want to install only the utilities, and press `Enter`.
4. Enter the full path of the directory in which you want to install the utilities, for example, `/opt/genesys/scsutil`, and press `Enter`. The installation displays the list of files being extracted and copied to the destination directory.
5. Enter the bit version of the system on which you are installing the utilities, either 32 or 64, and press `Enter`.

## On Windows

### Separately Installing SCS Utilities on Windows

1. On the Management Framework 8.1 product CD in the appropriate directory in: `management_layer\solution_control_server\windows` locate and double-click `setup.exe` to start the Genesys Installation Wizard.
2. On the wizard's `Welcome` page, click `Next` to start the installation.
3. On the `Solution Control Server Installation Mode` page, select `Solution Control Server Utilities`, and then click `Next`.
4. On the `Choose Destination Location` page, do one of the following to specify the directory where the utilities will be installed:
   - Click `Next` to accept the default directory.
   - Specify a different path and directory by entering it in the text box or using the `Browse` button. If necessary, use the `Default` button to reinstate the original default. Click `Next` to proceed.
5. On the `Ready to Install` page, click:
   - `Back` to update any installation information.
   - `Install` to proceed with the installation.
6. On the `Installation Complete` page, click `Finish`.

# Genesys SNMP Master Agent

For the Management Layer to communicate with an SNMP Master Agent, provided by either a third-party or Genesys, you must configure an Application object of type SNMP Agent in the Configuration Database, and configure a connection to this Application object in Solution Control Server.

If you do not want to use a redundant configuration or your SNMP Master Agent application does not support redundant configuration, configure your SNMP Master Agent as a stand-alone application. This section provides instructions for deploying a stand-alone SNMP Master Agent application.

> **Important**
> Depending on the solutions for which you want to enable SNMP monitoring, you may need to install several instances of SNMP Master Agent, using the same approach given in this section.
> Generally, you have to install and configure one instance of Genesys SNMP Master Agent on each computer on which you will be using SMNP functionality.

For more information about Genesys SNMP Master Agent, refer to the ''Framework 8.5 Management Layer User's Guide''.

To deploy SNMP Master Agent, do the following:

1. Configure an SNMP Master Agent Application object. **[+] Show steps**

### Prerequisites

- You are logged in to Genesys Administrator.

### Procedure

1. In Genesys Administrator, go to Provisioning > Environment > Applications, and select New in the toolbar. This opens a Browse dialog box that lists available application templates. If an SNMP Master Agent template file is not listed, do one of the following:
   - Import the SNMP_Master_Agent_<current-version>.apd file from the Management Framework 8.5 product CD.
   - Create a new template and repeat this step.
2. In the Browse dialog box, select the SNMP Master Agent template file. The Configuration tab for the new SNMP Master Agent Application object appears in the Details panel.
3. In the General section, enter a descriptive name in the Name field-for example, SNMP_MA.
4. In the Server Info section:

a. In the Host field, click the magnifying glass icon to select the Host object on which this SNMP Master Agent is running.

b. For each listening port that an application must use to connect to SNMP Master Agent:

i. In the Listening Ports field, click Add.

ii. Enter the port properties in the Port Info dialog box.

iii. Click OK.

c. For the Working Directory, Command Line, and Command Line Arguments fields, do one of the following:

- Enter the appropriate information in the three text boxes. For information about command-line parameters, see SNMP Master Agent.
- Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install SNMP Master Agent, but only if the Installation Package can connect to Configuration Server.

5. Click Save or Apply in the toolbar to save the new object. The new object will appear in the list of applications.

6. Add a connection from Solution Control Server to this SNMP Master Agent, as follows:

a. Open the Solution Control Server Application object's Configuration tab.

b. In the General section, add the connection to the SNMP Master Agent object just created. In the Connections field:

i. Click Add to open the Connection Info dialog box.

ii. Enter the properties of the connection.

iii. Click OK.

c. Click Save or Apply in the toolbar to save the configuration changes

2. Installing SNMP Master Agent. **[+] Show steps**

## On UNIX

> ### Warning
> During installation on UNIX, all files are copied into the directory you specify. The install process does not create any subdirectories within this directory, so do not install different products into the same directory.

### Prerequisite

- A SNMP Master Agent Application object exists.

### Procedure

1. On the Management Framework 8.1 product CD in the appropriate `management_layer/snmp_master_agent/<operating_system>` directory, locate a shell script called `install.sh`.
2. Type the file name at the command prompt, and press `Enter`.
3. To specify the host name for this SNMP Master Agent, do one of the following:
   - Type the name of the host, and press `Enter`.
   - Press `Enter` to select the current host.
4. Enter the Configuration Server host name, and press `Enter`.
5. Enter the Configuration Server network port, and press `Enter`.
6. Enter the Configuration Server user name, and press `Enter`.
7. Enter the Configuration Server password, and press `Enter`.
8. The installation displays the list of `Application` objects of the specified type configured on this `Host` object. Type the number corresponding to the SNMP Master Agent `Application` object you configured above, and press `Enter`.
9. To specify the destination directory, do one of the following:
   - Press `Enter` to accept the default.
   - Enter the full path of the directory, and press `Enter`.
10. If the target installation directory has files in it, do one of the following:
    - Type 1 to back up all the files in the directory, and press `Enter`. Specify the path to which you want the files backed up, and press `Enter`.
    - Type 2 to overwrite only the files in this installation package, and press `Enter`. Then type y to confirm your selection, and press `Enter`.
      Use this option only if the application already installed operates properly.
    - Type 3 to erase all files in this directory before continuing with the installation, and press `Enter`. Then type y to confirm your selection, and press `Enter`.

      The list of file names will appear on the screen as the files are copied to the destination directory.
11. For the product version to install, do one of the following:
    - Type 32 to select the 32-bit version, and press `Enter`.
    - Type 64 to select the 64-bit version, and press `Enter`.

## On Windows

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

### Prerequisite

- A SNMP Master Agent Application object exists.

### Procedure

1. On the Management Framework 8.1 product CD in the appropriate management_layer\snmp_master_agent\windows directory, locate and double-click setup.exe to start the Genesys Installation Wizard.
2. Click About on the wizard's Welcome page to review the read_me file. The file also contains a link to the server's Release Notes file.
3. Click Next to start the installation.
4. On the Connection Parameters to the Genesys Configuration Server page, specify the host name, port, user name, and password of Configuration Server, and then click Next.
5. On the Select Application page, select the name of the SNMP Master Agent Application object that you configured above, and then click Next.
6. On the Choose Destination Location page, the wizard displays the destination directory if specified in the Working Directory property of the server's Application object during configuration. If you entered a period (.) in this field when configuring the object, or if the path specified in this property is invalid, the wizard generates a path to the destination directory in the C:\Program Files\GCTI\<Product Name> format.
   If necessary, click one of the following:
   - Browse to select another destination folder. In this case, the wizard will update the Application object's Working Directory property in the Configuration Database.
   - Default to reinstate the path specified in the Working Directory property.

   Click Next to proceed.
7. On the Ready to Install page, click:
   - Back to update any installation information.
   - Install to proceed with the installation.
8. On the Installation Complete page, click Finish.

As a result of the installation, the wizard adds Application icons to the:

- Windows Start menu, under Programs > Genesys Solutions > Management Layer.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

# Deploying the Rest of Your Framework

Now that you deployed the Configuration Layer and, if required, the Management Layer, you can deploy the rest of the Framework components and the contact center environment.

## Recommended Order

Manual deployment of the other Framework components and contact center environment objects involves:

- Configuring the components using Genesys Administrator. Refer to ''Genesys Administrator 8.1 Help'' for more information.
- Manually installing the configured components.

Before you proceed, make sure that the Configuration Layer and Management Layer components are installed, configured, and running. To help you prepare accurate configuration information and become familiar with the configuration process, review Deployment Planning for help with object-configuration information.

Follow this order for the manual deployment of the other Framework components and contact center environment objects:

1. Media Layer:
   - T-Server
   - HA Proxy for a specific type of T-Server (if applicable)

   > **Important**
   > Deployment instructions for T-Server and HA Proxy (if applicable) are located in the latest version of the Framework T-Server Deployment Guide for your specific T-Server.

2. Telephony Objects:
   - Switching Offices
   - Switches
   - Agent Logins
   - DNs

   > **Important**

> Configuration instructions for telephony objects are located in the latest version of the Framework T-Server Deployment Guide for your specific T-Server.

3. Contact Center Objects:
   - Access Groups
   - Skills
   - Persons
   - Agent Groups
   - Places
   - Place Groups
4. Services Layer:
   - Stat Server

Genesys recommends registering only those entities that you plan to use in the current configuration. The more data in the Configuration Database, the longer it takes for your system to start up, and the longer it takes to process configuration data. Remember that adding configuration objects to the Genesys Configuration Database does not cause any interruption in the contact center operation.

Depending on how much work it is to configure all applications and objects, consider registering more `User` objects first, with a set of privileges that lets them perform configuration tasks.

> **Warning**
>
> When configuring redundant applications, do not select the redundancy type `Not Specified` unless using a switchover mechanism other than that provided by the Management Layer. It is acceptable, however, to leave the redundancy type `Not Specified` for non-redundant applications (that is, applications that do not have backup servers associated with them).

.

## Media Layer

Component (T-Server and HA Proxy, if applicable) configuration and installation for the Media Layer is covered in the latest version of the Framework T-Server Deployment Guide for your specific T-Server. Also covered in that Guide is information about deploying components for redundant and multi-site configurations.

## Telephony Objects

The configuration of Configuration Database objects for the telephony equipment used in the contact center is described in the latest version of the Framework T-Server Deployment Guide for your specific T-Server.

## Contact Center Objects

Configure Configuration Database objects for the contact center personnel and related entities.

### Access Groups

Before deciding what kind of Access Groups you must configure, look at the default Access Groups the Configuration Layer supports and the default access control settings in general.

The default security system may cover all of your needs. If a more complex access control system makes sense for your contact center, Genesys recommends managing it through Access Groups and folders rather than at the level of individuals and objects.

To define an Access Group and its permissions:

1. Identify groups of people that are handling specific activities in the customer interaction network.
2. Create the required Access Group objects.
3. Set Access Group privileges with respect to the object types, using the folders' `Permissions` and `Roles` tabs.

In addition, to simplify the security settings, make sure that permissions are set and changed recursively using the permission propagation mechanism.

### Skills

Define agent skills that might be considered as criteria for interaction processing. Skills are configured as independent configuration objects; any Agent can be associated with more than one configured Skill. Therefore, it may be more practical to register Skills before the Agents are configured.

### Users

There are two major categories of Users: Agents and Non-agents. The latter category includes all Users other than agents that need access to the CTI applications; for example, Center Administrators, Data Network and Telephony Network personnel, designers of interaction-processing algorithms, and Supervisors.

The characteristics of your business environment and your current priorities completely determine the order of registering Persons. Most often, you will want to first configure a few registered Non-agents with a high level of access to help you set up the Configuration Database.

Assign Agent Logins and Skills when registering Agents.

> **Important**
>
> You create Agent Logins when you are configuring the Switch object. Refer to the latest version of the Framework T-Server Deployment Guide for your specific T-Server for instructions.

If a few Agents have a certain Skill of the same level, consider using a wizard that adds the Skill to multiple `User` objects after you create them. To launch the wizard, select two or more `User` objects that have the `Is Agent` check box selected, right-click, and select `Manage Skills`. Refer to ''Genesys Administrator 8.1 Help'' for more information.

Remember that the Configuration Layer requires that you assign a unique user name to each User, including agents. Consider using employee IDs configured in `User` objects as default user names and passwords.

New Users by default are not automatically assigned to any access group, by default. They must be assigned to one or more Access Groups explicitly. If you want new users to be added automatically to predefined Access Groups, you must manually disable this feature using the configuration option `no-default-access`. Refer to the chapter "No Default Access for New Users" in the ''Genesys 8.1 Security Deployment Guide'' for more information about this feature, and how to use or disable it.

Some GUI applications also use Ranks to determine what functionality is made available to the User currently logged in. Unless Agents are required to use rank-dependent applications in their work, you do not have to assign any specific Ranks to them.

Ranks and access privileges are more important when registering non-agents. When registering non-agents, consider the role they have in the customer interaction business. Do these Users need to monitor agents' performance? Will they need to configure the telephony resources? Are they going to design routing strategies? Having answers to these questions makes it easier to correctly set up the access privileges with respect to configuration objects, and Ranks with respect to different applications objects.

Remember that Ranks with respect to applications are not the same as access privileges with respect to the configuration objects. You must explicitly define Ranks. Access privileges are assigned by default, according to whether the User is an agent or not.

Genesys does not recommend changing the default access-control setting unless absolutely necessary. Remember, the more complex the security system implemented, the more difficult it becomes to administer the database, and the more it affects the performance of the Configuration Layer software.

## Agent Groups

Agent Groups are an indispensable element of almost every contact center. Remember that you can assign an agent to more than one group at a time. If you create agent groups based on Skills, use the `Find` command or the `Dependency` tab of a Skill to quickly identify all the agents that have the Skill in question.

### Places

If you use Genesys CTI applications to distribute calls to individual agents or agent groups that are not limited by the switch ACD configuration, set up Places and assign individual DNs to them. Because a typical Place consists of more than one DN, prepare the actual layout of the numbering plan to correctly configure the Places, and assign DNs to them.

### Place Groups

Define Place Groups and assign individual Places to them only if they will be used for distributing calls to groups of Places and, therefore, you will need to collect availability information and real-time statistics for such groups.

## Services Layer

Genesys recommends that you configure and install components of the Services Layer when you deploy the solution they will serve.

### Stat Server

The configuration and installation procedures for Stat Server are described in the documentation for Stat Server.

# Redundant Configurations

You can increase the availability of your Genesys solutions by deploying redundant pairs of primary and backup servers of the same type, controlled by the Management Layer. You must have special licenses to use these configurations.

All Management Framework servers support the *warm standby* redundancy type, meaning that a backup server application remains initialized and ready to take over the operations of the primary server. Redundancy types are described in the ''Genesys 8.1 Security Deployment Guide''.

Configuration Layer and Management Layer also support switchovers between redundant client applications, regardless of the redundancy type specified by those applications.

## Important

- The instructions in this section assume that the primary server is already installed and operating. This section provides only instructions for installing the backup server and configuring the primary and backup servers to operate as a redundant pair.
- When configuring the backup component in a redundant pair, use the same account as for the primary component. Two applications with different accounts cannot be linked (configured) as a redundant high availability (HA) pair.
- If you need to make changes in the configuration of one or both servers in the HA pair, you must unlink the two servers before any changes are made. They can then be linked together and restarted.

# Redundant (HA) Configuration Servers

This section describes how to deploy redundant Configuration Servers.

## Redundancy

Redundant Configuration Servers support only the `warm standby` redundancy type.

Both the primary and backup Configuration Servers operate with the same Configuration Database. The backup Configuration Server does not accept client connections or make changes to the data until its role is switched to primary. When the backup Configuration Server starts, it establishes a connection to the primary Configuration Server. During the operation, the primary Configuration Server sends notifications about all changes made in the Configuration Database to the backup Configuration Server.

If there are any Configuration Server Proxies connected to the primary Configuration Server when it fails, those Proxy servers connect to the backup Configuration Server when it assumes the primary role.

## Deploying Redundant Configuration Servers

This section describes how to install and set up redundant Configuration Servers.

### Installation Recommendations

- To ensure proper redundancy, Genesys recommends running the primary and backup Configuration Servers on separate computers.

> **Warning**
>
> - When both the primary and backup Configuration Servers are running, do not remove the backup Configuration Server `Application` object from the configuration.
> - You are responsible for ensuring that the configuration options of the primary and backup Configuration Servers are the same, with some exceptions: the log options in the primary Configuration Server can differ from those in the backup Configuration Server configuration.

## Prerequisites

- Configuration Layer components are installed and running as described in Deploying Configuration Layer.
- You are logged into Genesys Administrator.

> **Important**
> Once installed, both Configuration Servers must be started from the `default` account.

## Installation and Configuration

1. Configure an `Application` object for the backup Configuration Server. **[+] Show steps**

1. Go to `Provisioning` > `Environment` > `Applications`, and click `New`.
2. In the `General` section of the `Configuration` tab:
    a. Enter a descriptive name (not `confserv`) in the `Name` text box.
    b. Select the appropriate template, as follows:
        i. Click the search icon in the `Application Template` field to open a `Browse` dialog box that lists the available application templates. If a Configuration Server template file is not listed, close the dialog box and import the `Configuration_Server_<current-version>.apd` file from the Management Framework 8.5 product CD.
        ii. In the `Browse` dialog box, select the Configuration Server template file.
        iii. Click `OK`.

    <div="step3">

- In the `Server Info` section:

a. Select the `Host` object on which this Configuration Server runs.
b. Specify the `Listening Ports` that Configuration Server clients must use to connect to this Configuration Server.
c. In the `Working Directory`, `Command Line`, and `Command Line Arguments` text boxes, do one of the following:
    - Enter the appropriate information in each of the text boxes. For information about command-line parameters, see Starting a Backup Configuration Server.
    - Type a period (`.`) in the `Working Directory` and `Command Line` text boxes, and leave the `Command Line Arguments` text box blank. The information will be filled in automatically when you install the backup Configuration Server, but only if the Installation Package can connect to the primary Configuration Server.
d. Enter appropriate values for the other mandatory fields (those indicated by red asterisks).

- Click `Save & Close` to save the configuration.

2. Install the backup Configuration Server. **[+] Show steps**

### Prerequisite

- The backup Configuration Server `Application` object exists.

## On UNIX

### Installing the Backup Configuration Server on UNIX

1. On the Management Framework 8.1 product CD, run the installation script `install.sh` located in one of the following:
   - For an enterprise (single-tenant) environment, `configuration_layer/configserver/single/<operating_system>/`
   - For a multi-tenant environment, `configuration_layer/configserver/multi/<operating_system>/`.
2. Type the file name at the command prompt, and press `Enter`.
3. For the installation type, type 2 to select `Configuration Server Master Backup`, and press `Enter`.
4. For the external authentication option, type the number corresponding to the type of External Authentication that will be used (LDAP, Radius, both, or neither), and press `Enter`.

   > **Important**
   > If you select LDAP, be prepared with the URL to access the LDAP Server. For more information about LDAP configuration, see the ''Framework 8.5 External Authentication Reference Manual''

   .
5. For the host name of this backup Configuration Server, do one of the following:
   - Specify the host name, and press `Enter`.
   - Press `Enter` to select the host on which this backup Configuration Server is being installed.
6. Specify the primary Configuration Server, as follows:
   a. Specify the primary `Configuration Server Hostname`, and press `Enter`.
   b. Specify a value for the `port` for the primary Configuration Server, and press `Enter`.
   c. Specify the `User name` of the primary Configuration Server, and press `Enter`.
   d. Specify the `Password` for the primary Configuration Server, and press `Enter`.
7. Type the number corresponding to the `Application` object for the backup Configuration Server that you created, and press `Enter`.
8. Specify the full path of the destination directory, and press `Enter`.

9. If the target installation directory has files in it, do one of the following:
   - Type 1 to back up all the files in the directory, and press Enter. Then specify the path to where you want the files backed up, and press Enter.
   - Type 2 to overwrite only the files in this installation package, and press Enter. Then, type y to confirm your selection, and press Enter. Use this option only if the application already installed operates properly.
   - Type 3 to erase all files in this directory before continuing with the installation, and press Enter. Then, type y to confirm your selection, and press Enter.

   The list of file names will appear on the screen as they are extracted and written to the destination directory.
10. For the product version to install, do one of the following:
    - Type 32 to select the 32-bit version, and press Enter.
    - Type 64 to select the 64-bit version, and press Enter.
11. Do one of the following:
    - Type y to configure the backup Configuration Server during installation (now), and press Enter. Go to Step 12 to specify values for the configuration file. For information about Configuration Server configuration options and their values, refer to the ''Framework Configuration Options Reference Manual''.
    - Type n to not configure backup Configuration Server during installation. In this case, you have finished installing Configuration Server; do not continue to the next step in this procedure. Before you can start Configuration Server, however, you must create a configuration file and set the configuration options in it, as described in Configuration Server Configuration File.
12. For the confserv section:
    a. Specify a value for the backup Configuration Server port, and press Enter.
    b. Specify a value for the backup Configuration Server management port, and press Enter.
13. For the dbserver section:
    a. Type the number corresponding to the database engine that this Configuration Server uses (dbengine), and press Enter.
    b. Specify the name or alias of the DBMS that handles the Configuration Database (dbserver), and press Enter.
    c. To specify the name of the Configuration Database (dbname), do one of the following:
       - If you are using an Oracle database engine (that is, you typed 3 in Step a), press Enter. This value is not required for Oracle.
       - If you are using any other database engine, specify the name of the Configuration Database, and press Enter.
    d. Specify the Configuration Database username, and press Enter.
    e. To specify the Configuration Database password, do one of the following:
       - Specify the password, and press Enter.
       - Press Enter if there is no password; that is, the password field is empty, with no spaces.

When the installation process is finished, a message indicates that installation was successful. The process places the backup Configuration Server in the directory specified during the installation process. The installation script also writes a sample configuration file, `confserv.sample`, in the directory in which the backup Configuration Server is installed.

If you chose to configure the backup Configuration Server during installation, the sample configuration file, `confserv.sample`, is renamed `confserv.conf`, and the parameters specified in Steps 12 through 14 are written to this file.

### Next Steps

If you chose to configure the backup Configuration Server after installation, you must manually rename the sample file as `confserv.conf` and modify the configuration options before you start the backup Configuration Server. See Configuration Server Configuration File.

## On Windows

### Installing the Backup Configuration Server on UNIX

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

1. On the Management Framework 8.5 product CD, locate and open the appropriate installation directory for your environment:
   - For an enterprise (single-tenant) environment, the installation directory is `configuration_layer/configserver/single/windows`.
   - For a multi-tenant environment, the installation directory is `configuration_layer/configserver/multi/windows`.

   The installation script, `setup.exe`, is located in the appropriate directory.
2. Double-click `setup.exe` to start the Genesys Installation Wizard.
3. Click `About` on the wizard's `Welcome` page to review the `read_me` file. The file also contains a link to the server's Release Notes file.
4. Click `Next` on the `Welcome` page to proceed with the installation.
5. On the `Maintenance Setup Type` page, select `Install new instance of the application` and click `Next`.
6. On the `Configuration Server Run Mode` page, select `Configuration Server Master Backup` and click `Next`.
7. On the Configuration Server Parameters page, specify the `Server Port` and `Management Port` for Configuration Server, and click `Next`.
8. On the `Database Engine Option` page, select the database engine used by Configuration Server, and click `Next`.
9. On the `Database Parameters` page:

a. Specify the Database Server Name and Database Name.

b. Specify the Database User Name and Password.

c. Click Next.

10. On the Configuration Server External Authentication page, select the type of external authentication Configuration Server uses, or select None if Configuration Server is not using external authentication. Click Next.

11. On the Connection Parameters to the Genesys Configuration Server page:

a. Specify the Host name and Port of the primary Configuration Server.

b. Specify the User name and Password for the primary Configuration Server.

c. Click Next.

12. In the upper pane of the Select Application page, select the backup Configuration Server Application object that you just configured, and click Next.

13. On the Choose Destination Location page, the wizard displays the destination directory (if specified during installation) in the Working Directory property of the server's Application object. If you entered a period (.) in this property, or if the specified path is invalid, the wizard generates a path to the destination directory in the C:\Program Files\GCTI\<Product Name> format.
If necessary, click:

- Browse to select another destination folder. In this case, the wizard will update the Application object's Working Directory in the Configuration Database.
- Default to reinstate the path specified in the Working Directory property.

Click Next to proceed.

14. On the Ready to Install information page, click:

- Back to update any installation information.
- Install to proceed with the installation.

15. On the Installation Complete page, click Finish.

As a result of the installation, the wizard adds Application icons to the:

- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

For more information about the Configuration Server configuration file, see Configuration Server Configuration File. For information about Configuration Server configuration options and their values, refer to the relevant chapters in the ''Framework Configuration Options Reference Manual''.

3. Modify the primary Configuration Server Application object to work with the backup Configuration Server. **[+] Show steps**

### Prerequisite

- The primary and backup Configuration Server Application objects exist.

### Procedure

1. Go to Provisioning > Environment > Applications, and click the primary Configuration Server Application object (named confserv) to open its properties.
2. On the Configuration tab, open the Server Info section.
3. Use the Browse button next to the Backup Server property to locate the backup Configuration Server Application object you want to use as the backup server.
4. Select Warm Standby as the Redundancy Type.
5. Select Auto-Restart.
6. Click Save & Close to save the changes.

4. If you installed the backup Configuration Server on UNIX and chose to configure it after installation, create and modify the configuration file for the backup Configuration Server. **[+] Show steps**

The configuration file for the backup Configuration Server must be the same as that for the primary Configuration Server with the following exceptions:

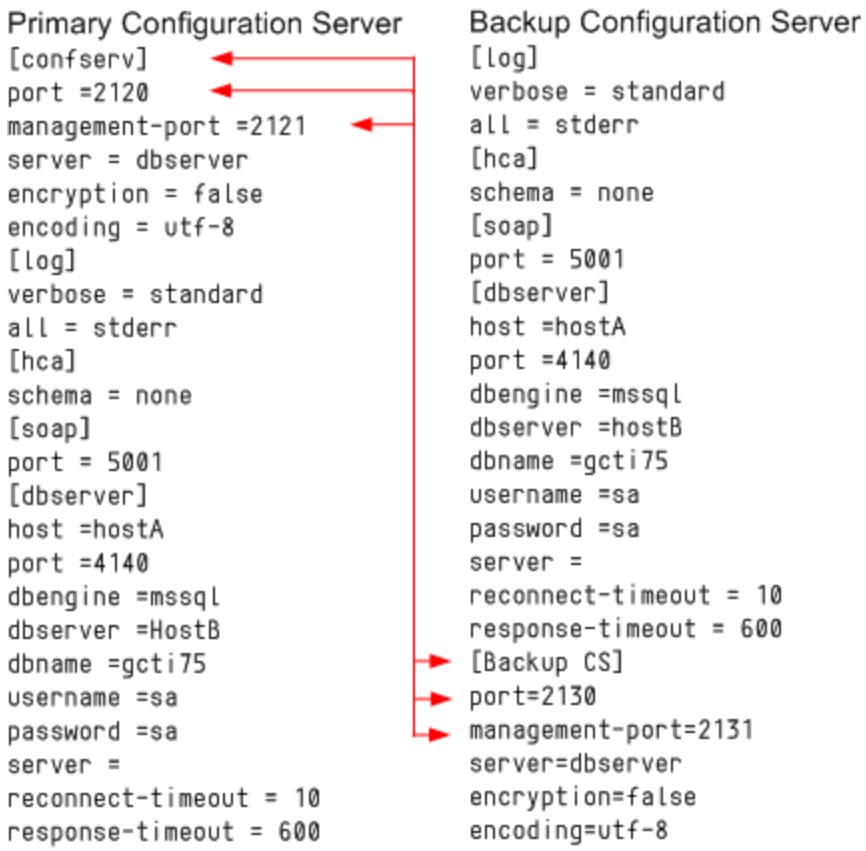
- The name of the section in the backup Configuration Server configuration file must match the name of the backup Configuration Server Application object.
- The values for the port and management-port options in the backup Configuration Server configuration file must be those values specified as Communication Port and Management Port values, respectively, during installation of the backup Configuration Server.
- The log options can be different.

The name of the Configuration Server section must be exactly the same as the name of the Application object for the backup Configuration Server.

For both the primary and backup Configuration Servers, specify the same database and user account for accessing this database, for both the primary and backup Configuration Servers.

The No Default Access for New Users feature must be configured the same in both the primary and backup Configuration Servers. In other words, both Configuration Servers must have the feature either configured or not.

Sample configuration files are shown side-by-side in the figure below. The arrows show the differences described in this section.



Sample Configuration Files for Primary and Backup Configuration Servers.

5. If you installed the backup Configuration Server on UNIX, modify the `run.sh` file to enable the backup server to be started. **[+] Show steps**

1. In a text editor, open the `run.sh` file.
2. Add the following at the end of the command line in the file:

```
-s <section name> -c <configuration file name>
```

6. Manually synchronize options and ports between the redundant Configuration Servers.

7. Manually synchronize high-availability (HA) ports between the redundant Configuration Servers. **[+] Show steps**

When Configuration Servers operate in a high-availability (HA) environment, the backup Configuration Server must be ready to take on the primary role when required. This requires that both Configuration Servers are running and that they must have the same information. When you configure redundant Configuration Servers to operate with the `warm standby` redundancy type, the primary Configuration Server uses the connection to the backup to deliver synchronization updates. Genesys recommends that you enable Advanced Disconnect Detection Protocol (ADDP) for this connection.

> **Important**
>
> You can configure multiple ports for any application of type Server. When multiple ports are configured for a

> server in a `warm standby` redundancy pair, the number of ports, their `Port IDs`, and the `Listening Mode` settings of the primary and backup servers must match respectively.

8. Solution Control Server is required for HA Configuration Servers to switch over. Modify and start the SCS responsible for that pair to work with the Configuration Server running in Primary mode. **[+] Show steps**

The SCS configuration file has a filename extension of `.cfg` (for Windows), and `.conf` (for UNIX). Here is a sample of the contents:

```
[backup_configserver]
host=<backup CS host name>
port=<backup CS port>
name=<SCS application name>
server=primary_configserver
[primary_configserver]
host=<primary CS host name>
port=<primary CS port>
name=<SCS application name>
server=backup_configserver
```

When using HA Configuration Servers, you must restart Solution Control Server to enable it to connect it to the Configuration Server running in Primary mode. If a Master Configuration Server is part of an HA pair, the SCS responsible for that pair of servers must be provisioned with a startup option as follows:

```
scs.exe -f <SCS configuration file>
```

## Starting the Backup Configuration Server

When starting a backup Configuration Server, specify the following values in the startup command line:

| | |
|---|---|
| `-s` | The name of the Configuration Server section within the configuration file for the backup Configuration Server. |
| `-c` | The name of the configuration file that contains configuration information for the backup Configuration Server. |

For a description of the command-line parameters specific to Configuration Server, refer to Configuration Server.

## On UNIX

### Starting a Backup Configuration Server on UNIX

> **Important**
> Make sure you have modified the `run.sh` file as directed in step 5, above.

- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, go to the directory in which the backup Configuration Server is installed, and do one of the following:
  - To use only the required command-line parameters, type the following command line:
    `sh run.sh`
  - To specify the command line yourself, or to use additional command-line parameters, type the following command line:
    `confserv -s <section name> -c <configuration file name> [<additional parameters as required>]`

## On Windows

### Starting a Backup Configuration Server on Windows

- To start as a Windows Service, refer to Starting and Stopping with Windows Services Manager.
- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, do one of the following:
  - Use the `Start` > `Programs` menu.
  - To use only the required command-line parameters, go to the directory in which the backup Configuration Server is installed, and double-click the file `startServer.bat`.
  - To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which the backup Configuration Server is installed, and type the following command line:
    `confserv.exe -s <section name> -c <configuration file name> [<additional parameters as required>]`

## Configuring ADDP between Redundant Configuration Servers

Advanced Disconnect Detection Protocol (ADDP) is supported between primary and backup Configuration Servers. Use the new configuration options `protocol`, `addp-timeout`, `addp-remote-timeout`, and `addp-trace`, setting them in the configuration server section of the configuration files for both Configuration Servers. For the primary Configuration Server, this section is called `confserv`. For the backup Configuration Server, this section has the same name as the backup Configuration Server `Application` object. For detailed descriptions of these options, refer to the ''Framework Configuration Options Reference Manual''.

For example, in a primary Configuration Server configuration file, the ADDP options would appear as follows:

```
[confserv]
...
protocol=addp
addp-timeout=16
addp-remote-timeout=32
addp-trace=both
...
```

# Redundant (HA) Message Servers

This section describes how to deploy redundant Message Servers.

## Redundancy

Redundant Message Servers support only the `warm standby` redundancy type, with the addition that the data is synchronized between the primary and backup servers.

## Deploying Redundant Message Servers

This section describes how to install and set up redundant Message Servers.

### Installation Recommendations

If you are installing the primary and backup Message Servers on the same host computer:

- Install them in different directories.
- Specify a different port number for each server.

### Prerequisites

- Configuration Layer components are installed and running as described in Deploying Configuration Layer.
- You are logged into Genesys Administrator.

> **Important**
> Once installed, the two Message Servers must be started from the same account.

### Installation and Configuration

> **Tip**
> (Optional) If the backup Message Server is to reside on a remote Host, you can deploy it to that Host using Genesys Administrator Extension. For instructions, refer to the

''Framework 8.1 Genesys Administrator Extension Help''.

1. Configure an Application object for the backup Message Server. **[+] Show steps**

### Configuring an Application Object for the Backup Message Server

1. Go to Provisioning > Environment > Applications.
2. If the Application object for this backup Message Server does not already exist, click New to create it.
3. In the General section of the Configuration tab:
   a. Enter a descriptive name in the Name text box.
   b. Select the appropriate template, as follows:
      i. Click the search icon in the Application Template field to open a Browse dialog box that lists the available application templates. If a Message Server template file is not listed, close the dialog box and import the Message_Server_<current-version>.apd file from the Management Framework 8.1 product CD.
      ii. In the Browse dialog box, select the Message Server template file.
      iii. Click OK.
4. In the Server Info section of the Configuration tab, enter the following information, as required:
   a. In the Host field, click the magnifying glass icon to select the Host object on which this Message Server is running.
   b. For each listening port that an application must use to connect to this Message Server:
      i. In the Listening Ports field, click Add.
      ii. Enter the port properties in the Port Info dialog box.
      iii. Click OK.
   c. For the Working Directory, Command Line, and Command Line Arguments fields, do one of the following:
      - Enter the appropriate information in each of the text boxes. For information about command-line parameters, see Starting a Backup Message Server.
      - Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install Message Server, but only if the Installation Package can connect to Configuration Server.
   d. Select the Auto-Restart check box.
5. Click **Save and Close** in the toolbar to save the new object.

2. If you did not deploy the backup Message Server using Genesys Administrator Extension, install it now.

3. Modify the primary Message Server Application object to work with the backup Message Server. **[+] Show steps**

### Prerequisite

- The primary and backup Message Server Application objects exist.

### Procedure

1. Go to Provisioning > Environment > Applications, and double-click the primary Message Server Application object to open its properties.
2. In the Server Info section of the Configuration tab:
   a. Select the backup Message Server Application object.
   b. Select Warm Standby as the redundancy type.
   c. Select Auto-Restart if required.
3. Click Save and Close to save the configuration.

4. If you installed the backup Message Server on UNIX, check the run.sh file and modify it, if necessary, so the application can be started properly. **[+] Show steps**

1. In a text editor, open the run.sh file.
2. Check if the following parameters are currently in the command line in the file, and if not, add them:
   `-host <configuration server host> -port <configuration server port> -app <application object name>`

5. Synchronize options and ports between the redundant Message Servers.

## Starting the Backup Message Server

When starting a backup Message Server, be sure to use the following command-line options:

| | |
|---|---|
| -host | The name of the host on which Configuration Server is running. |
| -port | The communication port that client applications must use to connect to Configuration Server. |
| -app | The exact name of the backup Message Server Application object as configured in the Configuration Database. |

For a description of the command-line parameters specific to Message Server, refer to Message Server.

## On UNIX

### Starting the Backup Message Server on UNIX

#### Prerequisite

- The `run.sh` file has been modified accordingly. See Step 5, above.

#### Procedure

- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, go to the directory in which the backup Message Server is installed, and do one of the following:
  - To use only the required command-line parameters, type the following command line:
    ```
    sh run.sh
    ```
  - To specify the command line yourself, or to use additional command-line parameters, type the following command line:
    ```
    MessageServer -host <Configuration Server host> -port <Configuration Server port>
    -app <backup Message Server Application> [<additional parameters and arguments as
    required>]
    ```

## On Windows

### Starting the Backup Message Server on Windows

- To start as a Windows Service, refer to Starting and Stopping with Windows Services Manager.
- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, do one of the following:
  - Use the `Start` > `Programs` menu.
  - To use only the required command-line parameters, go to the directory in which the backup Message Server is installed, and double-click the file `startServer.bat`.
  - To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which the backup Message Server is installed, and type the following command line:
    ```
    MessageServer.exe -host <Configuration Server host> -port <Configuration Server
    port> -app <backup Message Server Application> [<additional parameters and
    arguments as required>]
    ```

# Redundant (HA) Solution Control Servers

This section describes how to deploy redundant Solution Control Servers.

## Redundancy

Redundant Solution Control Servers support only the `warm standby` redundancy type, with the addition that the data is synchronized between the primary and backup servers.

## Deploying Redundant Solution Control Servers

This section describes how to install and set up redundant Solution Control Servers.

### Recommendations

If you are installing the primary and backup Solution Control Servers on the same host computer:

- Install them in different directories.
- Specify a different port number for each server.

### Prerequisites

- Configuration Layer components are installed and running as described in Deploying Configuration Layer.
- You are logged into Genesys Administrator.

> **Important**
> Once installed, the two Solution Control Servers must be started from the same account.

### Installation and Configuration

> **Tip**
> (Optional) If the backup Solution Control Server is to reside on a remote Host, you can

deploy it to that Host using Genesys Administrator Extension. For detailed instructions, refer to ''Framework Genesys Administrator Extension Help''.

1. Configure an Application object for the backup Solution Control Server. **[+] Show steps**

### Configuring an Application Object for the Backup Solution Control Server

1. Go to Provisioning > Environment > Applications.
2. If the Application object for this backup Solution Control Server does not already exist, click New to create it.
3. In the General section of the Configuration tab:
   a. Enter a descriptive name in the Name text box.
   b. Select the appropriate template, as follows:
      i. Click the search icon in the Application Template field to open a Browse dialog box that lists the available application templates. If a Solution Control Server template file is not listed, close the dialog box and import the Solution_Control_Server_<current-version>.apd file from the Management Framework 8.1 product CD.
      ii. In the Browse dialog box, select the Solution Control Server template file.
      iii. Click OK.
4. In the Server Info section of the Configuration tab, enter the following information, as required:
   a. In the Host field, click the magnifying glass icon to select the Host object on which this Solution Control Server is running.
   b. For each listening port that an application must use to connect to this Solution Control Server:
      i. In the Listening Ports field, click Add.
      ii. Enter the port properties in the Port Info dialog box.
      iii. Click OK.
   c. For the Working Directory, Command Line, and Command Line Arguments fields, do one of the following:
      - Enter the appropriate information in each of the text boxes. For information about command-line parameters, see Starting a Backup Solution Control Server.
      - Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install Solution Control Server, but only if the Installation Package can connect to Configuration Server.
   d. Select the Auto-Restart check box.
5. Click Save & Close in the toolbar to save the new object.

2. If you did not deploy the backup Solution Control Server remotely using Genesys Administrator, install it now.

3. Modify the primary Solution Control Server Application object to work with the backup Solution

Control Server. **[+] Show steps**

### Prerequisites

- The primary and backup Solution Control Server Application objects exist.

### Procedure

1. Go to `Provisioning` > `Environment` > `Applications`, and double-click the primary Solution Control Server `Application` object to open its properties.
2. In the `Server Info` section of the `Configuration` tab:
   a. Select the backup Solution Control Server `Application` object.
   b. Select `Warm Standby` as the redundancy type.
   c. Select `Auto-Restart` if required.
3. Click `Save & Close` to save the configuration.

4. If you installed the backup Solution Control Server on UNIX, check the `run.sh` file and modify it, if necessary, so the application can be started properly. **[+] Show steps**

1. In a text editor, open the `run.sh` file.
2. Check if the following parameters are currently in the command line in the file, and if not, add them:
   `-host <configuration server host> -port <configuration server port> -app <SCS application object name>`

5. Synchronize options and ports between the redundant Solution Control Servers.

## Starting the Backup Solution Control Server

When starting a backup Solution Control Server, be sure to use the following command-line options:

| | |
|---|---|
| `-host` | The name of the host on which Configuration Server is running. |
| `-port` | The communication port that client applications must use to connect to Configuration Server. |
| `-app` | The exact name of the backup Solution Control Server `Application` object as configured in the Configuration Database. |

For a description of the command-line parameters specific to Solution Control Server, refer to Solution Control Server.

## On UNIX

### Prerequisite

- The `run.sh` file has been modified accordingly. See Step 4, above.

### Procedure

- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, go to the directory in which the backup Solution Control Server is installed, and do one of the following:
  - To use only the required command-line parameters, type the following command line:
    ```
    sh run.sh
    ```
  - To specify the command line yourself, or to use additional command-line parameters, type the following command line:
    ```
    scs -host <Configuration Server host> -port <Configuration Server port> -app
    <backup Solution Control Server Application> [<additional parameters and arguments
    as required>]
    ```

## On Windows

### Starting the Backup Solution Control Server on Windows

- To start as a Windows Service, refer to Starting and Stopping with Windows Services Manager.
- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, do one of the following:
  - Use the `Start` > `Programs` menu.
  - To use only the required command-line parameters, go to the directory in which the backup Solution Control Server is installed, and double-click the file `startServer.bat`.
  - To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which the backup Solution Control Server is installed, and type the following command line:
    ```
    scs.exe -host <Configuration Server host> -port <Configuration Server port> -app
    <backup Solution Control Server Application> [<additional parameters and arguments
    as required>]
    ```

# Redundant (HA) SNMP Master Agents

The Management Layer supports configuration with a redundant pair of SNMP master agents. Redundant configuration assumes the presence of two SNMP master agent applications, one primary and one backup. When Solution Control Server loses a connection with the primary SNMP master agent, SCS switches all NMS communications to the backup SNMP master agent.

If your SNMP master agent application can operate in a redundant mode (as does, for example, Genesys SNMP Master Agent), and you would like to deploy this configuration, follow the instructions in this section.

## Redundancy

Redundant SNMP Master Agents support only the `warm standby` redundancy type.

## Deploying Redundant SNMP Master Agents

This section describes how to install and set up redundant SNMP Master Agents.

### Installation Recommendations

If you are installing the primary and backup SNMP Master Agents on the same host computer:

- Install them in different directories.
- Specify a different port number for each server.

### Prerequisites

- Configuration Layer components are installed and running as described in Deploying Configuration Layer.
- Management Layer components are installed and running as described in Deploying Management Layer.
- The SNMP Master Agent to be designated as primary is deployed as described in Deploying SNMP Master Agent.
- You are logged into Genesys Administrator.

## Installation and Configuration

> **Tip**
> (Optional) If the backup SNMP Master Agent is to reside on a remote Host, you can deploy it to that Host using Genesys Administrator Extension. Refer to ''Framework 8.1 Genesys Administrator Extension Help'' for instructions.

1. Configure an Application object for the backup SNMP Master Agent. **[+] Show steps**

### Configure an Application Object for the Backup SNMP Master Agent

1. Go to Provisioning > Environment > Applications.
2. If the Application object for this backup SNMP Master Agent does not already exist, click New to create it.
3. In the General section of the Configuration tab:
   a. Enter a descriptive name in the Name text box.
   b. Select the appropriate template, as follows:
      i. Click the search icon in the Application Template field to open a Browse dialog box that lists the available application templates. If an SNMP Master Agent template file is not listed, close the dialog box and import the SNMP_Master_Agent_<current-version>.apd file from the Management Framework 8.5 product CD.
      ii. In the Browse dialog box, select the SNMP Master Agent template file.
      iii. Click OK.
4. In the Server Info section of the Configuration tab, enter the following information, as required:
   a. In the Host field, click the magnifying glass icon to select the Host object on which this SNMP Master Agent is running.
   b. For each listening port that an application must use to connect to this SNMP Master Agent:
      i. In the Listening Ports field, click Add.
      ii. Enter the port properties in the Port Info dialog box.
      iii. Click OK.
   c. For the Working Directory, Command Line, and Command Line Arguments fields, do one of the following:
      - Enter the appropriate information in each of the text boxes. For information about command-line parameters, see Starting a Backup SNMP Master Agent.
      - Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install SNMP Master Agent, but only if the Installation Package can connect to Configuration Server.

d. Select the Auto-Restart check box.

5. Click Save & Close in the toolbar to save the new object.

2. If you did not deploy the backup SNMP Master Agent to a remote site using Genesys Administrator Extension, install it now.

3. Modify the primary SNMP Master Agent Application object to work with the backup SNMP Master Agent. **[+] Show steps**

### Prerequisite

- The primary and backup SNMP Master Agent Application objects exist.

### Procedure

1. Go to Provisioning > Environment > Applications, and double-click the primary SNMP Master Agent Application object to open its properties.
2. In the Server Info section of the Configuration tab:
   a. Select the backup SNMP Master Agent Application object.
   b. Select Warm Standby as the redundancy type.
   c. Select Auto-Restart if required.
3. Click Save and Close to save the configuration.

4. If you installed the backup SNMP Master Agent on UNIX, check the run.sh file and modify it, if necessary, so the application can be started properly. **[+] Show steps**

1. In a text editor, open the run.sh file.
2. Check if the following parameters are currently in the command line in the file, and if not, add them:
   `-host <configuration server host> -port <configuration server port> -app <backup SNMP Master Agent application object name>`

## Starting the Backup SNMP Master Agent

> **Important**
> Once installed, the two SNMP Master Agents must be started from the same account.

When starting a backup SNMP Master Agent, be sure to use the following command-line options:

| | |
|---|---|
| -host | The name of the host on which Configuration Server is running. |
| -port | The communication port that client applications |

| | |
|---|---|
| | must use to connect to Configuration Server. |
| `-app` | The exact name of the backup SNMP Master Agent `Application` object as configured in the Configuration Database. |

For a description of the command-line parameters specific to SNMP Master Agent, refer to SNMP Master Agent.

# On UNIX

## Starting a Backup SNMP Master Agent on UNIX

### Prerequisites

- The `run.sh` file has been modified accordingly. See Step 4, above.

### Procedure

Do one of the following:

- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, go to the directory in which the backup SNMP Master Agent is installed, and do one of the following:
  - To use only the required command-line parameters, type the following command line:
    ```
    sh run.sh
    ```
  - To specify the command line yourself, or to use additional command-line parameters, type the following command line:
    ```
    gsnmpmasteragent -host <Configuration Server host> -port <Configuration Server port> -app <backup SNMP Master Agent Application> [<additional parameters and arguments as required>]
    ```

# On Windows

## Starting the Backup SNMP Master Agent on Windows

Do one of the following:

- To start as a Windows Service, refer to Starting and Stopping with Windows Services Manager.
- To start from Genesys Administrator, refer to Starting and Stopping with the Management Layer.
- To start manually, do one of the following:
  - Use the `Start` > `Programs` menu.

- To use only the required command-line parameters, go to the directory in which the backup SNMP Master Agent is installed, and double-click the file `startServer.bat`.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which the backup SNMP Master Agent is installed, and type the following command line:
  ```
  gsnmpmasteragent.exe -host <Configuration Server host> -port <Configuration Server port> -app <SNMP Master Agent Application> [<additional parameters and arguments as required>]
  ```

# Sharing the Load Configurations

Large enterprises often run contact-center operations at numerous locations worldwide. Yet, for Genesys software to function as a single unit it is usually critical that all configuration objects comprising an enterprise be stored in a single Genesys Configuration Database. Under these circumstances, network delays, component failures, and similar factors might complicate or slow down the operations of a large enterprise.

By operating two Framework components in different modes you can somewhat simplify the operation of a distributed installation with a single Configuration Database:

- Distributed configuration environments
- Distributed management environments
- Distributing call loads

Starting Configuration Server in Proxy mode or Solution Control Server in Distributed mode requires special licenses. Refer to the ''Genesys Licensing Guide'' for more information.

## Distributed Configuration Environments

In a distributed configuration environment, the master Configuration Server is running at the site where the Configuration Database is located. Configuration Servers at multiple remote sites are working in so-called Proxy mode and are connecting to the master Configuration Server.

## Distributed Management Environments

In a distributed management environment, Solution Control Servers are communicating with each other and controlling a particular part of the Genesys environment while running at multiple remote sites (but within the same configuration environment).

## Distributing Loads

Genesys recommends deploying additional of Configuration Server Proxies and Solution Control Servers in Distributed mode to distribute loads.

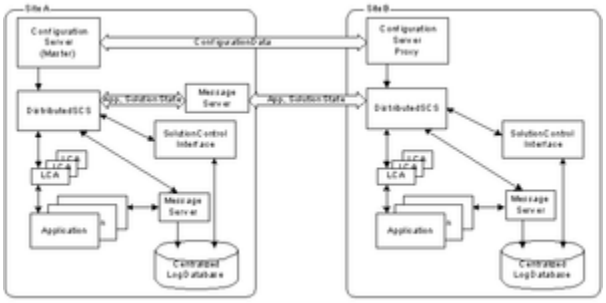
The number of instances deployed at the same site for purposes of load distribution should be calculated based on the number of clients to serve (for Configuration Server Proxy) and the number of hosts to control (for Distributed Solution Control Servers). Refer to the Management Framework section of the ''Genesys Hardware Sizing Guide''.

Genesys also recommends using Configuration Server Proxy and Distributed Solution Control Servers

in multi-site and/or multi-tenant environments.

## Architecture

The figure below illustrates how Configuration Server Proxy and Distributed Solution Control Servers fit into a Genesys configuration environment. This diagram does not include distributed components for Disaster Recovery/Business Continuity.




Distributed Installation

# Configuration Server Proxy

Using Configuration Server Proxy increases the robustness of the whole system, decreases the number of client connections to Configuration Server, and minimizes network traffic. That is, existing clients can continue, and new clients start, their operations when Configuration Server fails. In addition, after Configuration Server recovers, the client reconnect takes far less time than if all clients were directly connected to Configuration Server.

Configuration Server Proxy is an `Application` of the Configuration Server type operating in a special mode. As such, it replaces Configuration Server seamlessly for the clients. You can also configure Configuration Server Proxy permissions so that clients of a particular proxy access only the part of the configuration environment relevant to their site. See User Authorization and the ''Genesys 8.1 Security Deployment Guide'' for more information about setting permissions.

## How it Works

In a distributed configuration environment, the master Configuration Server is running at the site where the Configuration Database is located. Configuration Server Proxies at multiple remote sites are connecting to the master Configuration Server.

Instead of sending all the requests to Configuration Server, Configuration Server clients that require read-only access to Configuration Server can operate with one or more Configuration Server Proxies. Configuration Server Proxy passes messages to and from Configuration Server. Moreover, the proxy keeps the configuration data in its memory and responds to client data requests. Any configuration data updates are passed immediately to Configuration Server Proxy, so that it is always up to date; no additional configuration is required to specify an update interval.

### Configuration Server Proxy Functions

- Receives subscription requests from clients and handles them without passing the requests to Configuration Server.
- Stores in internal memory all configuration data it receives from Configuration Server.
- Receives notifications on data changes from Configuration Server, updates internal memory, and passes notifications to clients.
- Receives read-data requests from clients and responds to them using the data stored in the internal memory.

> **Warning**
>
> Always run Configuration Server Proxy under the default account `Environment\default`.

> **Important**
> A hierarchical configuration of Configuration Server Proxies-for example, a Configuration Server Proxy application working with another Configuration Server Proxy that operates directly with Configuration Server-is not supported.

# Deploying Configuration Server Proxy

> **Important**
> To ensure faultless operation, all Configuration Servers in the configuration environment must be running the same release. Configuration Server Proxy may start with a master Configuration Server running a later release, but only during the migration process. Refer to the ''Genesys Migration Guide'' for more information.

## Prerequisites

- The Configuration Layer components, including the master Configuration Server, are installed and running as described in Deploying Configuration Layer.
- You are logged in to Genesys Administrator.

## Installation and Configuration

1. Configure as many instances of Configuration Server Proxy as needed. **[+] Show steps**

### Prerequisite

- You are logged in to Genesys Administrator.

### Procedure

1. Go to `Provisioning` > `Environment` > `Applications`, and select New in the toolbar. This opens a `Browse` dialog box that lists available application templates. If a Configuration Server Proxy template file is not listed, do one of the following:
   - Import the `Configuration Server Proxy_<current-version>.apd` file from the Management Framework 8.5 product CD.
   - Create a new template using the procedure in [https://docs.genesys.com/Documentation/IW/8.5.0/Dep/StdConf#appTmplts Application Templates, and repeat this step.
2. In the `Browse` dialog box, select the Configuration Server Proxy template file.
3. In the `General` section of the `Configuration` tab:

a. Enter a descriptive name in the Name text box.

b. In the list of Connections, add a connection to the master Configuration Server Application object. If redundant master Configuration Servers are configured, specify a connection to the primary Configuration Server.

4. In the Server Info section:

a. Select the Host object on which this Configuration Server Proxy runs.

b. Specify the Listening Ports that Configuration Server Proxy clients must use to connect to this Configuration Server.

c. In the Working Directory, Command Line, and Command Line Arguments text boxes, do one of the following:

- Enter the appropriate information in each of the text boxes. For information about command-line parameters, see [[CSProxy#stCSP|Starting Configuration Server Proxy].
- Type a period (.) in the Working Directory and Command Line text boxes, and leave the Command Line Arguments text box blank. The information will be filled in automatically when you install Configuration Server Proxy, but only if the Installation Package can connect to the master Configuration Server.

d. Enter appropriate values for the other mandatory fields (those indicated by red asterisks).

e. In the Log On As Account field, you must use the default account, Environment\default.

> **Warning**
> Always run Configuration Server Proxy under the default account Environment\default.

5. (Optional) On the Options tab, do any of the following as required:

- If you want this Configuration Server Proxy to be writable, set the option proxy-writable in the csproxy section to true.
- Set the values of the log configuration options.

6. Click Save & Close to save the configuration.

2. Install the corresponding number of Configuration Server Proxies. **[+] Show steps**

### Prerequisite

- The Configuration Server Proxy Application object is created.

## On UNIX

## Installing Configuration Server Proxy on UNIX

1. On the Management Framework 8.5 product CD, locate and open the installation directory appropriate for your environment:
   - For an enterprise (single-tenant) environment, the installation directory is `configuration_layer/configserver/single/<operating_system>`.
   - For a multi-tenant environment, the installation directory is `configuration_layer/configserver/multi/<operating_system>`.

   The installation script, called `install.sh`, is located in the appropriate directory.
2. Type `install.sh` at the command prompt, and press `Enter`.
3. For the installation type, type `3` to select `Configuration Server Proxy`, and press `Enter`.
4. To specify the host name for this Configuration Server Proxy, do one of the following:
   - Type the name of the host, and press `Enter`.
   - Press `Enter` to select the current host.
5. Enter the Master Configuration Server host name, and press `Enter`.
6. Enter the Master Configuration Server network port, and press `Enter`.
7. Enter the Master Configuration Server user name, and press `Enter`.
8. Enter the Master Configuration Server password, and press `Enter`.
9. The installation displays the list of `Application` objects of the specified type configured for this `Host` object. Type the number corresponding to the Configuration Server Proxy `Application` object you configured in step 1, and press `Enter`.
10. To specify the destination directory, do one of the following:
    - Press `Enter` to accept the default.
    - Enter the full path of the directory, and press `Enter`.
11. If the target installation directory has files in it, do one of the following:
    - Type `1` to back up all the files in the directory, and press `Enter`. Specify the path to which you want the files backed up, and press `Enter`.
    - Type `2` to overwrite only the files in this installation package, and press `Enter`. Then type `y` to confirm your selection, and press `Enter`. Use this option only if the application already installed operates properly.
    - Type `3` to erase all files in this directory before continuing with the installation, and press `Enter`. Then type `y` to confirm your selection, and press `Enter`.

    The list of file names will appear on the screen as the files are copied to the destination directory.
12. Specify the full path to, and the exact name of, the license file that Configuration Server Proxy will use, and press `Enter`. When the installation process is finished, a message indicates that installation was successful. The process places Configuration Server Proxy in the directory that you specified during installation.

# On Windows

## Installing Configuration Server Proxy on Windows

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

1. On the Management Framework 8.5 product CD, locate and open the installation directory appropriate for your environment:
   - For an enterprise (single-tenant) environment, the installation directory is `configuration_layer/configserver/single/windows`.
   - For a multi-tenant environment, the installation directory is `configuration_layer/configserver/multi/windows`.

   The installation script, called `setup.exe`, is located in the appropriate directory.
2. Locate and double-click `setup.exe` to start the Genesys Installation Wizard.
3. Use the `About` button on the wizard's `Welcome` page to review the `read_me` file. This file also contains a link to the server's Release Notes file.
4. Click `Next`.
5. On the `Configuration Server Run Mode` page, select `Configuration Server Proxy`.
6. On the `Connection Parameters to the Genesys Configuration Server` page, specify the host name, port, user name, and password for the Master Configuration Server, then click `Next`.
7. On the `Select Application` page, select the name of the Configuration Server `Application` object that you created in step 1, and click `Next`.
8. On the `Access to License` page, specify the license access type and the appropriate parameters, and click `Next`.
9. On the `Choose Destination Location` page, the wizard displays the destination directory specified in the `Working Directory` property of the server's `Application` object. If the specified path is invalid, the wizard generates a path to `C:\Program Files\GCTI\<Singletenant or Multitenant> Configuration Server`. If necessary, click:
   - `Browse` to select another destination folder. In this case, the wizard will update the `Application` object's `Working Directory` property in the Configuration Database.
   - `Default` to reinstate the path specified in the `Working Directory` property.

   Click `Next` to proceed.
10. On the `Ready to Install` information page, click:
    - `Back` to update any installation information.

- Install to proceed with the installation.

11. On the Installation Complete page, click Finish. When the installation process is finished, a message indicates that installation was successful. The process places Configuration Server Proxy in the directory that you specified during the installation process.

3. Modify each Configuration Server Proxy client to work with Configuration Server Proxy. **[+] Show steps**

### Prerequisites

- The Configuration Server Proxy Application object is created.
- You have identified the client applications that are to operate with this particular Configuration Server Proxy.
- You are logged in to Genesys Administrator.

> **Important**
> Repeat this procedure for each application that is to be a client of Configuration Server Proxy.

### Procedure

1. Go to Provisioning > Environment > Applications, and double-click the client Application object that you want to connect to Configuration Server Proxy.
2. In the General section of the Configuration tab, add a Connection to the Configuration Server Proxy to which the client application should connect.
3. Click Save & Close to save the configuration changes.

   Now, when you start the client application, it will operate with the given Configuration Server Proxy.
4. Start the client application using one of the following methods:
   - From Genesys Administrator.
   - From the command line. In this case, you must use the parameters -host and -port to point to the Configuration Server Proxy with which the application will be operating.
5. Click Save & Close to save the changes.

4. (Optional) Configure redundant Configuration Server Proxies. **[+] Show steps**

### Prerequisites

- A primary Configuration Server Proxy Application object already exists.
- You are logged in to Genesys Administrator.

### Procedure

1. Configure an Application object for the backup Configuration Server Proxy as described in step 1 above.
2. Install a backup Configuration Server Proxy as described in step 2, above.
3. In Genesys Administrator, go to Provisioning > Environment > Applications and double-click the primary Configuration Server Proxy client Application object.
4. On the Configuration tab, open the Server Info section.
5. In the Backup Server field, specify the Configuration Server Proxy application you want to use as the backup server.
6. Open the Properties dialog box of the Configuration Server Proxy application that you want to configure as a primary server.
7. In the Redundancy Type field, select Warm Standby.
8. Select Auto-Restart.
9. Click Save & Close to save the configuration changes.

## Starting Configuration Server Proxy

> **Warning**
> Always run Configuration Server Proxy under the default account Environment\default.

The startup command line for Configuration Server Proxy must identify the:

- Configuration Server Proxy executable file
- Configuration Server Proxy application name (the -app parameter)
- Configuration Server host (the -host parameter)
- Configuration Server port (the -port parameter)
- Configuration Server Proxy license file or license server location (the -l parameter)

Configuration Server Proxy supports the command-line parameters common to Genesys server applications, as described in Starting and Stopping Manually.

> **Important**

> If using a primary-backup pair of Configuration Server Proxies, follow the same starting procedure for both primary and backup applications but make sure you specify the correct application name for each.

## On Unix

### Starting Configuration Server Proxy on UNIX

Go to the directory in which Configuration Server Proxy is installed, and do one of the following:

- To use only the required command-line parameters, type the following command line: `sh run.sh`
- To specify the command line yourself, or to use additional command-line parameters, type the following command line:
  ```
  confserv -host <Configuration Server host> -port <Configuration Server port> -app <CS proxy application objects name> [<additional parameters and arguments as required>]
  ```

## On Windows

### Starting Configuration Server Proxy on Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which Configuration Server Proxy is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which Configuration Server Proxy is installed, and type the following command line:
  ```
  confserv.exe -host <Configuration Server host> -port <Configuration Server port> -app <CS proxy application objects name> [<additional parameters and arguments as required>]
  ```

## Writable Configuration Server Proxies

By default, Configuration Server Proxy provides read-only access to configuration data. Configuration Server clients that require write access to Configuration Server must still connect directly to Configuration Server. Some of Genesys Supervisor- and Agent-facing applications (such as Workspace Desktop Edition), while deployed in high numbers, require write access to configuration data and should be deployed against Configuration Server Proxy in Writable mode.

Administrative applications, such as Genesys Administrator, should still connect to the Master

Configuration Server to perform complex configuration updates, because Configuration Server Proxy is writable mode is not designed to handle all types of configuration updates. Updates made in bulk might result in a significant extra load on the system when done by the Proxy server rather than the Master server.

To configure a Configuration Server Proxy as writable, use the Configuration Server Proxy configuration option `proxy-writable`. For more information about this option, refer to the ''Framework Configuration Options Reference Manual''.

## Redundant Configuration Server Proxies

The high-availability (HA) architecture implies the existence of redundant applications, a primary and a backup, monitored by a management application. Like Configuration Server, Configuration Server Proxy supports the `warm standby` redundancy type between redundant Configuration Server Proxies. For more information, refer to Redundant Configuration Servers.

Prior to release 8.1.3, when a switchover occurred between the primary and backup Configuration Server Proxies, Configuration Server Proxy clients had to read configuration information anew and reestablish the connections to the backup server themselves. Especially in large configuration environments, this often led to detrimental effects on system performance, leading clients to question the usefulness of the backup proxy server.

Starting in release 8.1.3, client connections are restored automatically by the backup Configuration Server Proxy when it switches to primary mode if the connection between the main Configuration Server and Configuration Server Proxy is lost, because the main Configuration Server is stopped via the Management Layer. This makes the switchover practically invisible to clients, and essentially eliminates the performance impact on the system. This restoration is made possible by the backup Configuration Server Proxy keeping its own record of client connections and disconnections. Under normal conditions, the primary proxy server notifies the backup proxy of client connections and disconnections, which the backup stores in its History Log Database. When the backup switches to primary, it is able to restore client connections based on the connection and disconnection information it has stored.

If the connection between the main and proxy servers is lost, and ADDP is configured between Configuration Server Proxy and the main Configuration Server and also between the proxy server and its client, the session is not restored. Clients of the Configuration Server Proxy must reregister and read all data from scratch.

> **Important**
>
> Two Configuration Server Proxies configured as an HA pair cannot be separated into two standalone servers in runtime. Each of the servers must be stopped, re-configured, and then restarted.

## Using Configuration Server Proxy with External Authentication

## Systems

In distributed systems prior to release 8.0, external authentication was configured only on the Master Configuration Server, and each Configuration Server Proxy passed authentication requests to it. Now, RADIUS and LDAP external authentication, starting in release 8.0 and 8.1, respectively, can be configured on the Master Configuration Server and on each Configuration Server Proxy. Therefore, each Configuration Server Proxy can process authentication requests itself, and does not need to pass them on to the Master Configuration Server. For more information about setting up external configuration on Configuration Server Proxy, refer to the ''Framework 8.5 External Authentication Reference Manual''.

## Support for Multi-Language Environments

You do not need to perform any additional configuration to have Configuration Server Proxy support multi-language environments. If the master Configuration Server supports UTF-8 encoded data, all Configuration Server Proxies connected to that master Configuration Server also support UTF-8 encoding. See Multi-language Environments for more information about using UTF-8 encoding to enable multi-language environments.

## Configuration History Log

You can configure a history log with Configuration Server Proxy to store historical information about client sessions and changes to configuration objects. Refer to Configuration History Log for more information.

## Failure of Configuration Server Proxy

When Configuration Server Proxy fails or disconnects from its clients, the clients attempt to reconnect to Configuration Server Proxy. If it is not available and if a backup Configuration Server Proxy is configured, the clients attempt to connect to the backup.

When Configuration Server Proxy fails, you must restart it manually or use the Management Layer for autorestart.

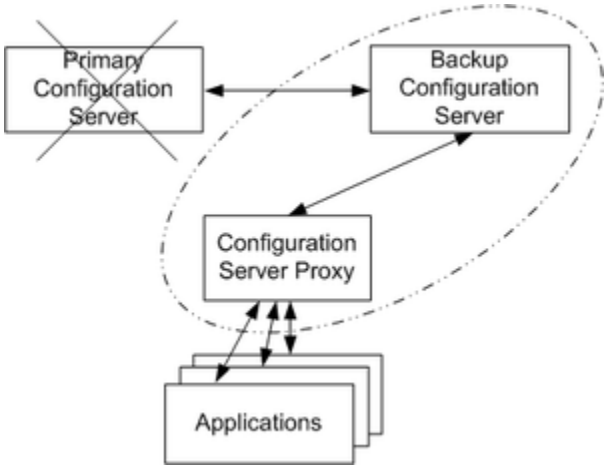
## Failure of Master Configuration Server

When the master Configuration Server fails or the connection to it is lost, the clients of Configuration Server Proxy continue their normal operations. Configuration Server Proxy initiates reconnect attempts to the master Configuration Server. Meanwhile, Configuration Server Proxy responds to client requests using the configuration data stored in its memory.

When the master Configuration Server fails, you must restart it manually or use the Management

Layer for autorestart.

The following diagram shows Configuration Server Proxy behavior when a primary-backup pair of master Configuration Servers is configured.




Distributed Installation

When the primary master Configuration Server fails or the connection to it is lost, Configuration Server Proxy initiates reconnect attempts to the master Configuration Server and, if it is not available, to the backup Configuration Server. If the connection to the backup Configuration Server is established, Configuration Server Proxy remains connected to the backup server until:

- The connection to the backup Configuration Server is lost.
- The backup Configuration Server fails.
- Configuration Server Proxy fails or is restarted.

# Distributed Solution Control Servers

Multiple Solution Control Servers operating in `Distributed` mode (referred to as *Distributed Solution Control Servers*) distribute management-related tasks among the sites in a distributed enterprise that uses a single Genesys Configuration Database. In these installations, each SCS controls its own subset (defined by you) of the hosts, applications, and solutions, and communicates with the others through a dedicated Message Server.

Specifically, Distributed Solution Control Servers perform the following functions:

- Performs the same functions of monitoring, control, alarm detection, and alarm processing as the SCS in non-Distributed mode, but on a subset of hosts, applications and solutions explicitly assigned to this SCS in the Configuration Database.
- Communicates all the updates to statuses of the assigned objects to other Distributed Solution Control Servers, using a dedicated Message Server.
- Receives notifications about updates to the status of non-assigned objects (that is, objects assigned to other Solution Control Servers) from Message Server.
- When receiving a control command on an object not assigned to this SCS, forwards this command via Message Server to the appropriate SCS.

Because Distributed Solution Control Servers communicate with each other, they all have the same information about all hosts, applications, and solutions. Thus, you can connect the interface object associated with Genesys Administrator to any Distributed SCS and monitor and control the whole environment as a single entity (given appropriate permissions). When a Distributed SCS receives a control command for an object that this SCS does not control, it forwards this command to the appropriate SCS and passes any further notifications back to the requestor.

Using Distributed Solution Control Servers helps you resolve some problems common to distributed installations:

- It eliminates false switchovers that occur when SCS disconnects from LCA at a remote site because of the slow network connection between sites or because of temporary network problems.
- It prevents a single point of failure. A failure of one Distributed SCS only means a temporary loss of control over a subset of hosts, applications, and solutions; other Distributed Solution Control Servers continue to control the rest of the environment.

Because Distributed Solution Control Servers communicate with each other, they all have the same information about all hosts, applications, and solutions. Therefore, given appropriate permissions, you can connect to any Distributed Solution Control Server and monitor and control the whole environment as a single entity.

# Deploying Distributed Solution Control Servers

## Warning

- Do not use Solution Control Servers in Distributed and non-Distributed modes simultaneously within the same Configuration environment. If you plan to use Distributed SCS in your installation, turn on Distributed mode for all Solution Control Servers you install.
- When using Distributed Solution Control Servers, always ensure that each Solution Control Server, either by itself or as part of a high-availability pair, is running on the host which it controls. Failure to do so can, in some cases, result in unpredictable behavior of the Solution Control Servers in the Distributed configuration. For example, different Solution Control Servers may start competing for control over applications on the host.

**1.** Configure Distributed Solution Control Servers in Distributed mode. **[+] Show steps**

### Configuring Distributed Solution Control Servers in Distributed Mode

1. Configure as many Solution Control Server `Application` objects as necessary, as described in Solution Control Server.
2. Turn on Distributed mode for each Solution Control Server `Application` object, by setting the following configuration options in the `general` section:
   - `distributed_mode=ON`
   - `distributed_rights=DEFAULT`
3. If you are planning to leave any of the `Host`, `Application`, or `Solution` objects unassigned-that is, without specifying which SCS is to control them-dedicate one SCS to the control of all unassigned hosts, applications, and solutions. To instruct one SCS to work in this mode, set the following values for configuration options in the general section for that particular SCS application:
   - `distributed_mode = ON`
   - `distributed_rights = MAIN`

#### Important

Only one of the Distributed Solution Control Servers can have the value `MAIN` for the `distributed_rights` configuration option.

**2.** Divide your configuration environment between the Solution Control Servers. **[+] Show steps**

When you are using Distributed Solution Control Servers, you must explicitly configure the servers' ownership of hosts, applications, and solutions. That is, you must associate each host, application, and solution object with a particular SCS by changing the object's properties:

> **Important**
>
> To distribute control over the primary and backup servers in a redundant pair between different Distributed Solution Control Servers, all Solution Control Servers in the configuration must be running release 7.6 or later.

### Recommendations

- Do not distribute control over the primary and backup servers in a redundant pair between different Distributed Solution Control Servers if any SCS in the configuration environment is running a pre-7.5 release. Genesys recommends that you configure the same SCS to control both the primary and backup servers in a redundant pair.
- When you are distributing control over the configuration objects among Distributed Solution Control Servers, ensure that the same SCS that controls a solution also controls all applications included in this solution. Although one SCS can technically control a solution while other servers control applications included in that solution, avoiding this configuration helps minimize network traffic between Solution Control Servers.
- Genesys strongly recommends that you not assign each component in an HA pair to different Solution Control Servers in a distributed environment. In this configuration, the functionality of each Solution Control Server in the HA pair might be limited to handling simple application failures only (the failure of an application within the pair). In addition, the state of each component in the monitored HA pair might become inconsistent if network failures occur between the Distributed Solution Control Servers.

### Assigning a Distributed Solution Control Server

- To control a host: Specify the SCS application in the `Solution Control Server` field in the `General` section of the `Configuration` tab of the `Host` object.
- To control an application: Do not make any changes to the `Application` object. Specifying SCS ownership of the application's host is enough. The Distributed SCS automatically controls any applications assigned to the host this SCS controls.
- To control a solution: Specify the SCS application in the `Solution Control Server` field in the `General` section of the `Configuration` tab of the `Solution` object.

**3.** Configure a dedicated Message Server through which the Distributed Solution Control Servers will communicate with each other. **[+] Show steps**

### Recommendations

Distributed Solution Control Servers communicate with each other through Message Server. Genesys recommends that you use a dedicated Message Server for this purpose.

### Prerequisites

- An `Application` object exists for each Distributed SCS in the configuration environment.
- You are logged in to Genesys Administrator.

### Configuring a Dedicated Message Server

1. Configure a Message Server `Application` object with appropriate configuration parameters. Refer to Message Server.
2. Double-click the Message Server `Application` object, and click the `Options` tab.
3. Create a new configuration options section called `MessageServer`.
4. In this section, create a new configuration option called `signature` and set its value to `scs_distributed`. Each Distributed SCS will process this option to determine which of the Message Servers specified in its `Connections` to use for communications with other Solution Control Servers.
5. In the `Application` object for each Distributed Solution Control Server, add a connection to this Message Server, as follows:
   a. Enter `ADDP` as the `Connection protocol`.
   b. Set the `ADDP Local Timeout` and `Remote Timeout` to values that are less than half the minimum `alive_timeout` values between all Distributed Solution Control Servers in the configuration environment.
   In other words:
   $T_{addp} < T_{scs} * 0.5$
   where:
   $T_{addp}$ = ADDP timeout
   $T_{scs}$ = minimum `alive_timeout` between all Distributed Solution Control Servers
   Refer to the ''Framework Configuration Options Reference Manual'' for a detailed description of the `alive_timeout` option.

**4.** (Optional) Configure a Message Server for centralized logging at each site with Distributed Solution Control Servers. **[+] Show steps**

For distributed environments using a single Configuration Database, Genesys recommends using a dedicated Message Server for centralized logging at each site. In most cases, you have to configure as many Message Servers as there are Distributed Solution Control Servers.

> **Important**
> You can configure as many Message Servers for centralized logging as you need per site. These are in addition to the Message Server dedicated to handle communications between the distributed servers.

After you have installed the Message Servers, you should verify that each Message Server used for centralized logging is configured and connected to a Solution Control Server and to each of the applications controlled by that Solution Control Server as follows:

### Prerequisites

- Distributed Solution Control Servers are set up in the configuration environment.
- The Message Server used for centralized logging in this environment is installed.
- You are logged in to Genesys Administrator.

### Verifying Configuration of Message Servers used for Centralized Logging

1. Go to `Provisioning` > `Applications`, and double-click a particular Solution Control Server

Application object to open its Configuration tab.

2. In the General section, make sure that a connection to the Message Server that is providing the centralized logging is added to the list of Connections.
3. For each Application object that this particular Solution Control Server controls:
   a. Open the Configuration tab of the object.
   b. In the General section, make sure that a connection to that same Message Server is added to the list of Connections.

**5.** (Optional) Configure redundant applications for Distributed Solution Control Servers. **[+] Show steps**

Distributed Solution Control Servers support the warm standby redundant configuration in the same way as other Genesys servers, with the added benefit that the backup maintains data synchronization with the primary. That is, you can configure a primary and a backup pair of Distributed Solution Control Servers to operate with warm-standby redundancy. Refer to Redundant Solution Control Servers for more information.

**6.** After you are finished with the configuration tasks, physically install all instances of Solution Control Server and Message Server to match the configuration.

## Starting Distributed Solution Control Servers

> ### Important
> Starting a Solution Control Server in Distributed mode requires a special license. Refer to the ''Genesys Licensing Guide'' for more information.

Start each Distributed Solution Control Server in the same way as you would start a non-distributed SCS. See Starting SCS and Starting a Backup SCS for more information.

# Disaster Recovery / Business Continuity

This section describes a recommended architecture to ensure successful disaster recovery, or business continuity, following a scenario in which the main site was rendered inoperable because of some natural or other disaster. For more information, including configuration details, see Disaster Recovery Configuration.

## Overview

The Genesys system configuration is stored in a single database and can be accessed by only one primary master Configuration Server connection at a time. The Configuration Database is constantly modified by Configuration Server clients, is archived periodically to prevent the loss of data. Database maintenance and periodic backup can cause significant downtime. It cannot prevent partial or whole loss of configuration data if a major disaster occurs, such as one in which the Configuration Database and all updates and modifications made since the last backup is completely lost.

To improve the robustness of the Management Framework solution and to reduce downtime for system maintenance, this architecture replicates a live database to a secondary live standby database. If a major disaster occurs, that secondary database can be accessed by a secondary master Configuration Server that is brought online from a dormant state, and changing IP address name resolution for Configuration Server Proxies to the host running that secondary master Configuration Server. Operations at sites can be continued uninterrupted in limited mode without a configuration change until the secondary master Configuration Server is brought online and restored to normal mode after the Proxy servers reconnect to the secondary master Configuration server.

## Components

This architecture consists of the following components:

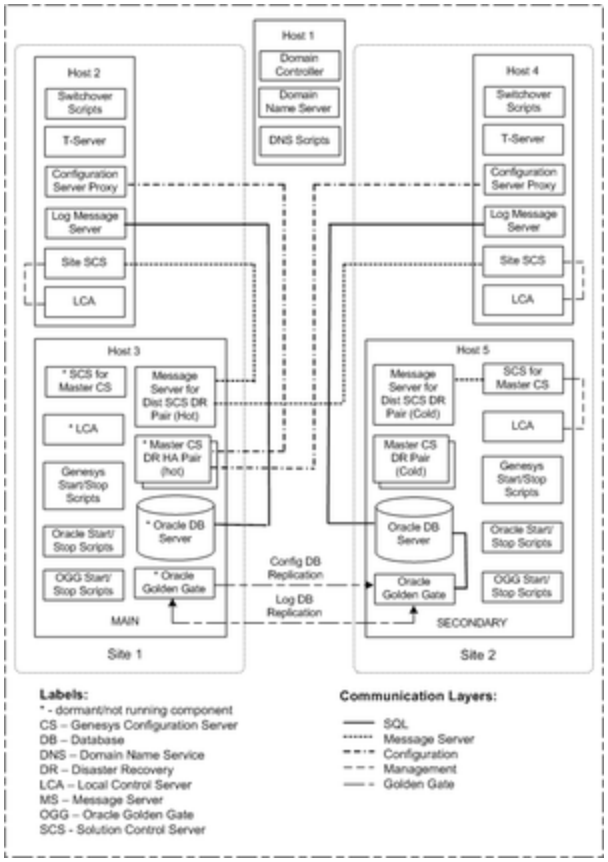
- Main live DBMS database server at Site 1.
- Secondary live DBMS at Site 2.
- DBMS solution to replicate the live Configuration Database to a secondary live standby database and log message databases cross sites replication.
- Main live redundant pair master Configuration Server primary/backup pair at Site 1.
- Secondary dormant (not running in normal operation mode) master Configuration Server primary/backup pair at Site 2.
- Main live Solution Control Server in distributed mode to control the main master Configuration Server pair at Site 1.
- Secondary dormant Solution Control Server in distributed mode to control the secondary Master Configuration Server pair at Site 2.
- Main Message Server at Site 1 to support communication between Solution Control Servers controlling

site components, such as Configuration Server Proxy pairs, T-Servers, Log Message Servers.

- Secondary dormant (not running in normal operation mode) Message Server at Site 2 to support communication between Solution Control Servers controlling site components, such as Configuration Server Proxy pairs, T-Servers, and Log Message Servers.
- Live Configuration Server Proxy pair at Site 1.
- Live Configuration Server Proxy pair at Site 2.
- Live Solution Control Server at Site 1.
- Live Solution Control Server at Site 2.
- Live Message Server for network logging at Site 1, connected to the Log Database at Site 1.
- Live Message Server for network logging at Site 2, connected to the Log Database at Site 1.
- Scripts to start and stop the master Configuration Server primary/backup pair and master Solution Control Servers.
- DBMS scripts to enable and disable database access.
- DBMS solution scripts to start and stop replication processes.
- A script residing at the DNS server host to change IP address name resolution for the master Configuration Server host.
- A switchover script to push name resolution changes for Configuration Server Proxy hosts at Sites 1 and 2 after the IP address name resolution changes at the DNS server host.

## Architecture

The following diagram illustrates the disaster recovery architecture for a multi-site configuration under normal conditions.



Multi-Site Disaster Recovery Architecture under Normal Operations

## Solution Control Server

The Solution Control Servers used in this deployment are configured in distributed SCS mode. Some or all can also be configured in HA pairs at each site.

At each site, a Solution Control Server is deployed on the management host (Hosts 3 and 5 in the diagram above) and is dedicated to managing applications on the management hosts, specifically the Configuration Server and the dedicated Message Server for the distributed Solution Control Servers, described next.

For distributed Solution Control Servers to communicate with each other, a Message Server dedicated for distributed Solution Control Server use (that is, configured with `[MessageServer]signature=scs_distributed`) is also installed on each of the management hosts.

Each site also has a separate Solution Control Server deployed on the application host configured to manage Genesys applications running on each site (that is, the site SCS in the diagram above).

Depending on the number of applications, it is possible to deploy additional distributed Solution Control Servers for load balancing.

For additional fault tolerance, Solution Control Servers can be deployed in high-availability (HA) pairs.

## Message Server

Each site has its own instance of a Log Message Server to be used for network logging by applications running on the same site. The Message Servers are installed on the application host and managed by the site Solution Control Server. A Log Database is used at each site.

In addition, a Message Server is also dedicated to communications between the distributed Solution Control Servers. This requires two instances (or two HA pairs) of Message Servers to be deployed, one of which is dormant.

## DNS Server Configuration and Switchover Scripts

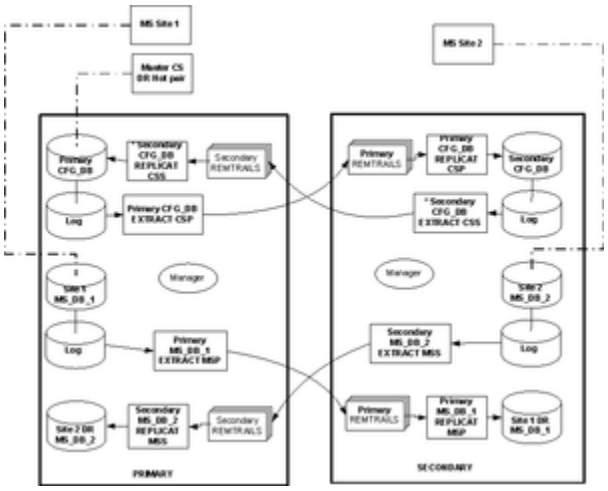
The DNS Server configures a record type A to resolve the IP address of a host running the live master Configuration Server primary/backup pair. It resolves the IP address to the main host in normal mode, and to the secondary host in failover mode. It consists of two scripts setting the IP address resolution, one for the main host and the second for the secondary host.

## DBMS Solution Replication Processes Configuration

The DBMS Solution must have replication processes designed to cross-replicate the Configuration and Log Databases, such as:

- From the database on the main system to that on the secondary system.
- From the database on the secondary system to that on the main system.

The following diagram illustrates the DBMS configuration in normal operating mode. In this mode, the Configuration Database replication process from the secondary system to the main system is in STOPPED state (marked *). It is started only when the secondary Configuration Database is switched from live standby to live mode and used for the initial data replication from the secondary to main database after the main system is restored.



Multi-Site Database Replication

# Starting and Stopping Framework Components

You can start and stop a Framework component in any of the following ways:

- Using the startup file created by the installation script. This file can only be used to start the component, you must use one of the other ways to stop the component.
- Using the Management Layer.
- Manually, specifying command-line parameters.
- Using the Windows Services Manager, available only in Windows.

# Using Startup Files

Startup files are files named `run.sh` (on UNIX) or `startServer.bat` (on Windows), and which installation scripts create and place in the applications' directories during installation. For additional information about how to use startup files, refer to the ''Framework 8.5 Management Layer User's Guide''.

> **Important**
>
> You must manually modify the `run.sh` file created for a redundant server before you can use it to start the server. Refer to Configuring Redundant Components for more information.

### Prerequisites

- The startup parameters in the startup file are correct.
- The required applications that should be running for this application to start are installed and running. See the appropriate sections in Starting Components to identify which applications should be running for a particular application to start.

## On UNIX

To start the application on UNIX, go to the directory in which the application is installed and type the following on the command line:

```
sh run.sh
```

## On Windows

To start the application on Windows, do one of the following:

- Go to the directory in which the application is installed and double-click the following:
  `startServer.bat`
- From the MS-DOS window, go to the directory in which the application is installed and type the following on the command line:
  `startServer.bat`

# Using the Management Layer

You can use Genesys Administrator to start and stop applications via the Management Layer.

> **Important**
>
> To operate with the Management Layer, Genesys Administrator must be configured as described in the ''Genesys Administrator 8.1 Deployment Guide''.

Before starting an application with the Management Layer, make sure the application's startup parameters are correctly specified in the `Application` properties. In the `Server` Info section of the application's `Configuration` tab, check that the following entries are correct:

- `Working Directory` - Directory in which the application is installed and/or is to run
- `Command Line` - Name of the executable file
- `Command Line Arguments` - Command-line parameters

See Command-line parameters for Framework components for descriptions of the parameters.

After you correctly specify the command-line parameters, you can start and stop the following Framework components from Genesys Administrator:

- Configuration Server (the Command Line Arguments are not required for the primary Configuration Server)

> **Important**
>
> For the Management Layer to start Configuration Server, you must modify the Configuration Server application.

- Configuration Server Proxy
- Message Server
- SNMP Master Agent
- T-Server
- HA Proxy
- Stat Server

The Management Layer can also restart failed applications; to enable the `autorestart` functionality for a particular application, select the corresponding check box in the properties of the Application.

Note that when an application is started (or restarted) via the Management Layer, it inherits

environment variables from LCA, which executes the startup command. Therefore, you must also set the environment variables required for the application for the account that runs LCA.

> **Warning**
> Stopping an application via the Management Layer is not considered an application failure. Therefore, the Management Layer does not restart applications that it has stopped unless you have configured an appropriate alarm condition and alarm reaction for them.

## Stop vs. Graceful Shutdown

When you stop an application or a solution, the application or solution shuts down, ceasing all processing immediately. This may have a detrimental effect on the rest of the system.

Starting in release 8.0, you can stop an application or a solution gracefully, known as a *graceful shutdown* or *graceful stop*. Applications refuse any new requests, but continue to process their current requests. A solution gracefully shuts down all of its composite applications, then stops.

> **Important**
> Because a number of solutions can share the same applications, some solution components may continue to have `Started` status after you stop the solution.

Only applications and solutions that support the graceful stop functionality can be stopped gracefully. Applications and solutions that do not support this functionality shut down ungracefully.

If you are unsure if the application supports graceful shutdown, you can use the `suspending-wait-timeout` configuration option to configure a timeout. If the status of the application changes to `Suspending` within this time, the application supports graceful shutdown. If the status does not change to `Suspending` within the timeout, the application does not support graceful shutdown, and the application will then stop ungracefully after the timeout expires. Refer to the ''Framework Configuration Options Reference Manual'', for a detailed description of this configuration option and how to use it.

Refer to ''Genesys Administrator 8.1 Help'' for more information about stopping gracefully, and about configuring a timeout.

# Starting Manually

When using a manual procedure to start an application, specify the startup parameters in the command prompt. In the command prompt, command-line parameters must follow the name of the executable file. On the Shortcut tab of the Program Properties dialog box, command-line parameters must also follow the name of the executable file.

Some Genesys interface components also require that you log in to them using preassigned login credentials. Use the procedure Logging In.

## Common Command Line Parameters

### [+] Show Parameters

The following table lists command-line parameters that are common to all Framework components.

| | |
|---|---|
| `-host` | The name of the host on which Configuration Server is running. |
| `-port` | The communication port that client applications must use to connect to Configuration Server. |
| `-app` | The exact name of an application as configured in the Configuration Database. |
| `-l` | The license address. Use for the server applications that check out technical licenses. Can be either of the following:<br>• Full path to and the exact name of the license file used by an application. For example, `-l /opt/mlink/license/license.dat`.<br>• The host name and port of the license server, as specified in the SERVER line of the license file, in the `port@host` format. For example, `-l 7260@ctiserver`. |
| `-v` | The version of a Framework component. This parameter does not start an application, but returns its version number instead. Either uppercase (V) or lowercase (v) letter can be used. |
| `-nco X/Y` | The Nonstop Operation feature is activated; X exceptions occurring within Y seconds do not cause an application to exit. If the specified number of exceptions is exceeded<br>within the specified number of seconds, the application exits or, if so configured, the Management Layer restarts the application. If you do not specify a value for the `-nco` parameter, the default value (6 exceptions handled in 10 seconds) applies. To disable |

| | |
|---|---|
| | the Nonstop Operation feature, specify `-nco 0` when starting the application. |
| `-lmspath` | The full path to the log messages files (the common file named `common.lms` and the application-specific file with the extension `*.lms`) that an application uses to generate log events. This parameter is used when the common and application-specific log message files are located in a directory other than the application's working directory, for example, when the application's working directory differs from the directory to which the application is originally installed. Note that if the full path to the executable file is specified in the startup command line (for instance, `c:\gcti\multiserver.exe`), the path specified for the executable file is used for locating the `*.lms` files, and the value of the `-lmspath` parameter is ignored.<br>**Warning**<br>An application that does not find its *.lms file at startup cannot generate application-specific log events and send them to Message Server. |

## Starting Components

> **Important**
>
> When an application is installed on a UNIX operating system and the application name, as configured in the Configuration Database, contains spaces (for example, `My T-Server`), you must surround the application name by quotation marks (`" "`) in the command line, as follows:
>
> ```
> -app "My T-Server"
> ```
>
> Specify the rest of the command-line parameters as for any other application.

This section contains prerequisites, procedures, and other information about starting each Framework component, as follows:

- Configuration Server
- Configuration Server Proxy
- Local Control Agent
- Genesys Deployment Agent
- Message Server

- Solution Control Server
- Genesys SNMP Master Agent

Prerequisites for starting other Framework components are also provided, as follows:

- License Manager
- Genesys Administrator
- HA Proxy
- T-Server
- Stat Server

## Configuration Server

### Prerequisites

- The license file has been uploaded into the Configuration Database and is valid.
- FlexNet Publisher License Manager is installed and running.

Configuration Server does not require any of the common command-line parameters for startup. To verify the database object integrity, you can specify the following additional command-line parameters that are specific to Configuration Server:

| | |
|---|---|
| `-checkdb` | An instance of Configuration Server starts, verifies the database object integrity, and terminates; all log messages are written in the log output. |
| `-checkerrors` | An instance of Configuration Server starts, verifies the database object integrity, and terminates; error log messages are written in the log output. |

You can also use the following command-line parameters when starting Configuration Server:

| | |
|---|---|
| `-c` | Configuration Server reads its configuration settings from a configuration file with the specified name. If you set this parameter, its value overrides the default name of the configuration file (`confserv.conf` on UNIX or `confserv.cfg` on Windows). |
| `-s` | Configuration Server reads its configuration settings from a configuration section with the specified name. The section must be configured within Configuration Server's configuration file; the section name must be the same as the name of the Configuration Server application configured in the Configuration Database. Use this parameter to start a backup Configuration Server. |
| `-p` | Forces an instance of Configuration Server to start, encrypt the database password in the configuration file, and terminate. Refer to the ''Genesys 8.1 |

| | |
|---|---|
| | Security Deployment Guide'' for instructions on encrypting the Configuration Database password. |
| `-cfglib_port` | Configuration Server opens the listening port specified in the command line. The port is opened in unsecured mode. This port is not written to the Configuration Server `Application` object, and does not survive a restart of Configuration Server. Do not use this option as a part of normal startup. Use it only as a last resort when regular secure ports cannot be accessed because of a configuration problem, such as incorrect or expired security certificates, or when a duplicate port (not necessarily secure) is specified in the configuration and therefore cannot be opened. |

## On UNIX

Go to the directory in which Configuration Server is installed and do one of the following:

- To use only the required command-line parameters, type the following on the command line:
  `sh run.sh`
- To specify the command line yourself, or to use additional command-line parameters, type the following command on the command line:
  `confserv [<additional parameters and arguments as required>]`

## On Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which Configuration Server is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which Configuration Server is installed, and type the appropriate command on the command line:
  `confserv.exe [<additional parameters and arguments as required>]`

### Configuration Server Proxy

Configuration Server Proxy supports only the command-line parameters common to Framework server components; it does not support the additional command-line parameters specific to Configuration Server.

#### Prerequisites

- The Master Configuration Server is installed and running.

- License Manager is installed and running.

## On UNIX

Go to the directory in which Configuration Server Proxy is installed and do one of the following:

- To use only the required command-line parameters, type the following on the command line:
  `sh run.sh`
- To specify the command line yourself, or to use additional command-line parameters, type the following command on the command line:
  `confserv [<additional parameters and arguments as required>]`

## On Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which Configuration Server Proxy is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which Configuration Server Proxy is installed, and type the appropriate command on the command line:
  `confserv.exe [<additional parameters and arguments as required>]`

### Local Control Agent

With default settings, Local Control Agent starts automatically every time a computer is started or rebooted. In Windows, you can manually start LCA from the `Start` > `Programs` menu. You can also change the default LCA port value, following the instructions in Step 3 when Creating a Host.

#### Starting LCA on Linux Without Root Privileges

On Red Hat Enterprise Linux systems, you can configure LCA to start automatically when the Host starts, and without root privileges.

To configure the runlevel for LCA and Genesys Deployment Agent (GDA) on Linux, do one of the following:

- For runlevel 3:
  - LCA: `ln -s /etc/init.d/gctilca /etc/rc3.d/S99gctilca`
  - GDA: `ln -s /etc/init.d/gctigda /etc/rc3.d/S98gctigda`
- For runlevel 5:
  - LCA: `ln -s /etc/init.d/gctilca /etc/rc5.d/S99gctilca`

- GDA: `ln -s /etc/init.d/gctigda /etc/rc5.d/S98gctigda`

> **Important**
>
> Do not use `/etc/rc.local`, which will cause LCA and GDA to start at run levels 2, 3, 4, and 5, which you do not need.

There are various run levels available for Linux, and some of them are listed in the following table. Refer to the Linux website for a complete list of run levels.

| Run Level | Description |
|---|---|
| 0 | System halt; no activity, the system can be safely powered down. |
| 1 | Single user; rarely used. |
| 2 | Multiple users, no Network File System (NFS); rarely used. |
| 3 | Multiple users, command-line (all-text mode) interface; the standard runlevel for most Linux-based server hardware. |
| 4 | User-definable. |
| 5 | Multiple users, graphical user interface; the standard runlevel for most Linux-based desktop systems. |

### Configuring different (but non-root) <user> and <group> for LCA and GDA on Linux

1. Install the LCA as root.
2. Select the <user> and <group> that you want to use as a replacement for the user "root" and the group "root".
3. Ensure that the <user> and <group> each have the adequate privileges for the folders/directories in which LCA is installed, and for the other applications and modules that will be controlled/managed by LCA.
4. Change the owner and group for LCA, as follows:
   a. Set the current working directory to the location where LCA is installed.
   b. Enter the following commands and press `Enter` after each:
      - `chown <user> lca`
      - `chgrp <group> lca`
5. Change the current user from root to <user>.
6. On the command line, enter `su - <user>`, and press `Enter`.
7. Set the `setUID` and `setGID` attributes for LCA. On the command line, enter `chmod ug+s lca`, and press `Enter`.
   This essentially equates the user/group ID to <user>/<group> when LCA is launched by another user.

8. Change the current user from <user> to root, and check how LCA will be launched using the root account, by entering the following commands on the command line, pressing Enter after each:
   ```
   su -
   ./lca &
   ps -ef | grep lca
   ```
   You should see something like this:
   ```
   UID process
   <user> ./lca
   ```
   This indicates that the effective user for LCA is <user> and all applications launched by LCA should have the same effective user id <user>. Normally, this approach of setting UID and GID is used to elevate privileges, but in this case, it is used to downgrade privileges.

## Genesys Deployment Agent

### Prerequisites

LCA is installed.

# On UNIX

1. Open the directory in which Genesys Deployment Agent is installed.
2. Do one of the following:
   - To use the default port (5000), enter the following at the command line:
     ```
     /etc/init.d/gctigda start
     ```
   - To use a different port:
     a. In a text editor, open the script file /etc/init.d/gctigda that was created by the IP when Genesys Deployment Agent was installed.
     b. Edit the following line in the script, entering the new port number:
     ```
     /tmp/lcainst/gda <new port number> >/dev/null &
     ```

     > **Important**
     > The port number entered in the command line must be the same value as the port option configured in the rdm section of the corresponding Host object. Refer to the ''Framework Configuration Options Reference Manual'', for information about this option.

     c. Save the script.
     d. Enter the following on the command line:
     ```
     /etc/init.d/gctigda start
     ```

# On Windows

1. Open the directory in which Genesys Deployment Agent is installed.
2. Do one of the following:
   - To use the default port (5000), run the gda.exe file.
   - To use a different port, enter the following command on the command line: `gda.exe <new port number>`

> **Important**
>
> The port number entered in the command line must be the same value as the `port` option configured in the `rdm` section of the corresponding Host object. Refer to the ''Framework Configuration Options Reference Manual'' for information about this option.

### Message Server

Message Server supports the common command-line parameters.

#### Prerequisites

- Configuration Server is installed and running.

## On UNIX

Go to the directory in which Message Server is installed and do one of the following:

- To use only the required command-line parameters, type the following on the command line:
  ```
  sh run.sh
  ```
- To specify the command line yourself, or to use additional command-line parameters, type the following command on the command line:
  ```
  MessageServer -host <Configuration Server host> -port <Configuration Server port> -app <Message Server Application> [<additional parameters and arguments as required>]
  ```

## On Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which Message Server is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which Message Server is installed, and type the appropriate command on the command line:
  ```
  MessageServer.exe -host <Configuration Server host> -port <Configuration Server port>
  ```

```
-app <Message Server Application> [<additional parameters and arguments as required>]
```

### Solution Control Server

Solution Control Server uses the command-line parameters common to Framework server components described above. You can also use the following command-line parameters when starting Solution Control Server:

| **-f <SCS configuration file>** | |
|---|---|
| | SCS gets Configuration Server's settings from the SCS configuration file. Because the SCS configuration file contains a list of Configuration Servers to which it should try to connect, this option allows SCS to connect to Configuration Server that is running in primary mode.<br><br>The SCS configuration file has the filename extension **.cfg** for Windows; **.conf** for UNIX. Here is a sample of the contents:<br><br>`[backup_configserver]`<br>`host=<backup CS host name>`<br>`port=<backup CS port>`<br>`name=<SCS application name>`<br>`server=primary_configserver`<br><br>`[primary_configserver]`<br>`host=<primary CS host name>`<br>`port=<primary CS port>`<br>`name=<SCS application name>`<br>`server=backup_configserver`<br><br>where `host` is the name of the Host object on which the appropriate Configuration Server is running, as defined in the Configuration Database. |

#### Prerequisites

- Configuration Server is installed and running.
- If you are starting SCS in Distributed mode, or if HA support or SNMP functionality is required, License Manager must be installed and running.

## On UNIX

Go to the directory in which SCS is installed and do one of the following:

- To use only the required command-line parameters, type the following on the command line:
  `sh run.sh`
- To specify the command line yourself, or to use additional command-line parameters, type the following command on the command line:
  `scs -host <Configuration Server host> -port <Configuration Server port> -app <Solution Control Server Application> [<additional parameters and arguments as required>]`

> **Important**
>
> If you are operating on a dual-stack machine, and dual stack is enabled, add the following start-up parameter on the command line:
>
> ```
> -transport-ip-version 6,4
> ```
>
> This specifies what internet protocol versions you are using, in this case IPv4 and IPv6.

## On Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which SCS is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which SCS is installed, and type the appropriate command on the command line:
  `scs.exe -host <Configuration Server host> -port <Configuration Server port> -app <Solution Control Server Application> [<additional parameters and arguments as required>]`

> **Important**
>
> If you are operating on a dual-stack machine, and dual stack is enabled, add the following start-up parameter on the command line:
>
> ```
> -transport-ip-version 6,4
> ```
>
> This specifies what internet protocol versions you are using, in this case IPv4 and IPv6.

### Genesys SNMP Master Agent

Genesys SNMP Master Agent uses the command-line parameters common to Framework server components, described above.

#### Prerequisites

- Configuration Server is installed and running.
- If you plan to use SNMP alarm signaling, Message Server must be installed and running.

## On UNIX

Go to the directory in which SNMP Master Agent is installed and do one of the following:

- To use only the required command-line parameters, type the following on the command line:
  ```
  sh run.sh
  ```
- To specify the command line yourself, or to use additional command-line parameters, type the following command on the command line:
  ```
  gsnmpmasteragent -host <Configuration Server host> -port <Configuration Server port>
  -app <SNMP Master Agent Application> [<additional parameters and arguments as
  required>]
  ```

## On Windows

Do one of the following:

- Use the `Start` > `Programs` menu.
- To use only the required command-line parameters, go to the directory in which SNMP Master Agent is installed, and double-click the `startServer.bat` file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS window, go to the directory in which SNMP Master Agent is installed, and type the appropriate command on the command line:
  ```
  gsnmpmasteragent.exe -host <Configuration Server host> -port <Configuration Server
  port> -app <SNMP Master Agent Application> [<additional parameters and arguments as
  required>]
  ```

### License Manager

For information about starting License Manager, see the ''Genesys Licensing Guide''.

### Genesys Administrator

Information about starting and stopping Genesys Administrator is located in the ''Framework 8.1 Genesys Administrator Deployment Guide''.

#### Prerequisites

- Configuration Server is installed and running.

### HA Proxy

Details on starting and stopping HA Proxy, if applicable, are located in the latest version of the Framework T-Server Deployment Guide for your specific T-Server.

If one or more HA Proxy components are required for T-Server connection to its switch, start HA Proxy before starting T-Server.

#### Prerequisites

- Configuration Server is installed and running.

### T-Server

Details on starting and stopping T-Server are located in the latest version of the Framework T-Server Deployment Guide for your specific T-Server.

Before starting T-Server, be sure that the following components are running:

- Configuration Server
- License Manager

> **Important**
> If an HA Proxy component is required for T-Server connection to its switch, you must start HA Proxy before starting T-Server.

### Stat Server

Details on starting and stopping Stat Server are located in the documentation for your release of Stat Server.

#### Prerequisites

- Configuration Server is installed and running.

> **Important**
> For Stat Server to operate correctly, T-Server must also be running.

## Stopping

### Server Applications

## On UNIX

To stop a server application on UNIX, use one of the following commands:

- `Ctrl+C`
- `kill <process number>`

## On Windows

To stop a server application on Windows, do one of the following:

- Type `Ctrl+C` in the application's console window.
- Click `End Task` in the Windows Task Manager.

### GUI Applications

## Windows-based

To stop a Windows-based GUI application, select `File` > `Exit` in the main window.

## Web-based

To stop a web-based GUI application, such as Genesys Administrator, click `Logout` on the main page.

# Using Windows Service Manager

The Genesys setup procedures on Windows operating systems automatically install Genesys daemon applications as Windows Services, with the autostart capability.

When starting an application installed as a Windows Service, make sure that the startup parameters of the application are correctly specified in the ImagePath in the application folder that you can find in the Registry Editor.

The ImagePath must have the following value data:

| | |
|---|---|
| | `<full path>\<executable file name> -service <Application Name as Service> -host <Configuration Server host> -port <Configuration Server port> -app <Application Name> -l <license address>` |

where the command-line parameters common to Framework server components are described here and where

| | |
|---|---|
| `-service` | Name of the application running as a Windows service (typically, it matches the application name specified in the `-app` command-line parameter) |

Framework components installed as Windows services with autostart capability are automatically started each time a computer on which they are installed is rebooted.

To start Framework components installed as Windows Services with manual start capability, click `Start` in Services Manager.

> **Important**
>
> Use the `Windows Services` window to change the startup mode from Automatic to Manual and vice versa.

To stop any Framework components installed as Windows Services, regardless of the start capability, click `Stop` in Services Manager.

# Additional Information

The following pages contain additional information that will help you use Genesys Framework.

# Silent Setup

Genesys Silent Configuration allows for an automated electronic software distribution, also known as a *silent setup*. With silent setup, you do not have to monitor the setup or provide input via dialog boxes. Instead, the setup parameters are stored in a response file, and the silent setup runs on its own, without any intervention by the end-user.

An installation procedure for a server application differs slightly from an installation procedure for a GUI application. Both, however, require that you update a response file with the necessary parameters and then use it for the actual installation.

Genesys Silent Configuration works on both UNIX and Windows operating systems.

The following Framework components support Silent Setup installation:

- Configuration Server
- Message Server
- Solution Control Server
- T-Server
- HA Proxy
- Stat Server

## Creating the Response File

A template for the response file, called `genesys_silent.ini`, is included in the Installation Package (IP) for each supporting component. This template file, called `genesys_silent.ini`, guides you through the task of entering required information, by providing the following information for each field:

- A full description of the field.
- If applicable, a description of valid values, either a range or a list.
- If application, any conditions in which the parameters may not be used.

Open this file and provide values for all required fields by replacing the text contained in angle brackets (<>)(see the examples). Then save the file. By default, it is saved as `genesys_silent.ini` in the installation folder.

Subsequently, you can use the same response file any time you need to install an application with the configured parameters.

### Sample Response File Entries (genesys_silent.ini)

The following is an example of the Genesys Configuration Server information section in the genesys_silent.ini for Configuration Server, with values entered for the required fields.

### [+] Show sample entries

```
#==============================================================================
#        Genesys Configuration Server information section
#        NOTE:        If Genesys Configuration Wizard .ini file (GCTISetup.ini file) is
#                        detected in IP root directory, then Host, Port, User,
#                        xPassword/Password Configuration Server parameters specified in
#                        Genesys Silent Configuration file are ignored.
#==============================================================================
[ConfigServer]

#------------------------------------------------------------------------------
#        Host name where Genesys Configuration Server is running.
#------------------------------------------------------------------------------
Host=CSHost

#------------------------------------------------------------------------------
#        Port number of Genesys Configuration Server.
#------------------------------------------------------------------------------
Port=2010

#------------------------------------------------------------------------------
#        User name in Genesys Configuration Server.
#------------------------------------------------------------------------------
User=User1

#------------------------------------------------------------------------------
#        User's password in Genesys Configuration Server.
#        The password can be specified in encrypted or none encrypted form:
#                xPassword - is used to specify the encrypted password;
#                Password - is used to specify the non encrypted password;
#        If 'xPassword' key value specified then 'Password' key value is ignored.
#------------------------------------------------------------------------------
xPassword=********

#------------------------------------------------------------------------------
#        Application name in Genesys Configuration Server.
#        NOTE:        This parameter is ignored if only one application was defined in
#                        GCTISetup.ini file by Genesys Configuration Wizard (Setup reads
#                        application name from '[<ApplicatonName>]' section name
#                        of GCTISetup.ini file).
#                        This is a mandatory parameter if Installation uses application
#                        template in Genesys Configuration Server and GCTISetup.ini file
#                        does not exist or contains more then one defined application.
#------------------------------------------------------------------------------
ApplicationName=config
```

## Running the Silent Installation

The silent setup program does not display a message if an error occurs. The status information for the silent installation is recorded in a file called (by default) genesys_install_result.log.

Use the appropriate command line to launch the Genesys Silent Configuration, depending on your operating platform as follows:

## On UNIX

```
./install.sh -s -fr <full path to the setup response file> -fl <full path to the setup log file>
```

where:

| | | |
|---|---|---|
| | `<full path to the setup response file>` | |
| | | The full path to the the setup response file. By default, `install.sh` looks for a response file called `genesys_silent.ini` in the same directory as `install.sh`. |
| | | |
| | `<full path to the setup log file>` | |
| | | The full path to the setup log file. By default, `genesys_install_result.log` is generated in the same directory as the response file being used. |

Example

```
.\install.sh -s -fr /home/user/genesys_silent.ini -fl /home/user/genesys_install_result.log
```

## On Windows

```
.\setup.exe /s /z"-s <full path to the setup response file> -sl <full path to the setup log file>"
```

where:

| | | |
|---|---|---|
| | `<full path to the setup response file>` | |
| | | The full path to the setup response file. By default, `setup.exe` looks for a response file called `genesys_silent.ini` in the same directory as `setup.exe`. |

| | | |
|---|---|---|
| | `<full path to the setup log file>` | |
| | | The full path to the setup log file. By default, `genesys_install_result.log` is generated in the same directory as the response file being used. |

> **Important**
>
> - Enclose the entire string of parameters `-s <full path to the setup response file> -sl <full path to the setup log file>` in double quotation marks.
> - Do not enter a space between the `/z` parameter and its value.

Example

```
.\setup.exe /s /z"-s c:\win\genesys_silent.ini -sl c:\win\genesys_install_result.log"
```

## Silent Setup Log File

The silent setup program prints installation results into a setup log file. By default, the results file is named `genesys_install_result.log`, and is stored in the same folder as `genesys_silent.ini`.

# Generic Configuration Procedures

This section provides generic instructions for using Genesys Administrator to configure a Genesys Framework Application object. Refer to instructions for a particular application for any application-specific deviations from the standard configuration procedure.

## Application Templates

The application template provides a majority of the configuration options for server applications and the default values of those options. Using one application template, you can create as many Application objects of the same type as you need.

Before you configure an Application object, import a template for this application. If a suitable predefined template is not available, create a new template.

> **Tip**
> Before you continue, make sure you have selected Show Advanced views in User Preferences. Refer to *Genesys Administrator 8.1 Help* for more information about setting User Preferences.

## Import an Application Template

### Start of procedure

1. In Genesys Administrator, go to Provisioning > Environment > Application Templates, and select Import template, located in the slide-out Tasks panel on the right.

   > **Important**
   > If Application Templates is not listed under Environment, open User Preferences, and select Show advanced views on the General tab. Refer to *Genesys Administrator 8.1 Help*, if necessary.

2. In the window that appears, click Add.
3. In the Choose file dialog box, locate the installation CD for your product and open the TEMPLATES folder.
4. Select the template file for your application.
5. Click Open to import the template file. The Configuration tab for this template is displayed.

6. Make any changes that you require, then click Save to save your changes and return to the list of available templates.
7. If there is metadata associated with this template, import the metadata file.

End of procedure

## Create an Application Template

### Start of procedure

1. In Genesys Administrator, go to `Provisioning` > `Environment` > `Application Templates`, and click New in the toolbar.

> **Important**
>
> If `Application Templates` is not listed under `Environment`, open `User Preferences`, and select the `Show advanced views` checkbox on the `General` tab. Refer to *Genesys Administrator 8.1 Help* if necessary.

2. Specify the template `Name`, select a template `Type`, and specify a `Version`.
3. If required, define default configuration options on the `Options` tab.
4. Click Save to save the changes and return to the list of available templates.
   The new template is stored in the `Environment` > `Application Templates` folder, and can be used to create a new `Application` object; you do not have to import it.

End of procedure

### Application Metadata

Starting with release 8.0, application templates for some Genesys components come with additional XML files called Application Metadata files. These files are used by only Genesys Administrator, and provide a user-friendly way to further configure an object. The metadata file contains all of the configuration options that can be used for the particular application, including those that are already in the template.

The metadata file is located in the same folder with the corresponding application template, and has the same filename with the extension `.xml`. To enable the metadata, you must import the metadata file and associate it with the application template.

#### Prerequisites

- The application template to be associated with the metadata is available.
- You are logged in to Genesys Administrator.

### Start of procedure

1. Go to Provisioning > Environment > Application Templates, and select the application template to which the metadata is to be imported. The Configuration tab for this template is displayed.
2. Click Import Metadata in the toolbar.
3. In the window that appears, click Add.
4. In the Choose file dialog box, locate the installation CD for your particular product and open the TEMPLATES folder.
5. Select the metadata file for the application.
6. Click Open to import the metadata file and associate the metadata with the application template.

### End of procedure

After the metadata is imported for a template, a new tab, Settings, appears in the details pane for each Application object created from that template. In that new tab, Genesys Administrator displays additional detailed information about configuration options that can be used with that application.

For more information about metadata, refer to *Genesys Administrator 8.1 Help*.

# Server Applications

This section contains the procedures necessary to create and configure Server applications.

## Creating and Configuring a Server Application

## [+] Show steps

### Prerequisites

- The Configuration Layer is installed and running.
- You are logged in to Genesys Administrator.

### Start of procedure

1. Go to Provisioning > Environment > Applications, and select New in the toolbar.
2. From the list of available application templates in the Browse dialog box, choose the template for this application. (See Application Templates for information about templates.)
3. In the General section of the Configuration tab:
   - Enter a name for this application in the text box. The application template provides information for the application type and version.
   - If you are in a multi-tenant environment, add the tenants who will be using this application.
   - In the Connections field, do any of the following as required:

- Add a connection to any server application to which this application should be a client. To enable Advanced Disconnect Detection Protocol (ADDP) for this connection, see Configuring ADDP.
- To enable ADDP between this server and Configuration Server, add the Configuration Server Application object (named `confserv`) to the connections and specify the values for the connection protocol, in seconds (see Configuring ADDP.) For more information, refer to ''Genesys Administrator 8.1 Help''.
- Add a connection to Message Server to provide alarm-signaling and centralized-logging capabilities.

4. In the `Server Info` section, specify the following:
   - The host computer on which this server is to be installed and/or to run.
   - Listening ports that applications must use to connect to this server.
   - `Working Directory`-The full path to the directory from which the application starts.
   - `Command Line properties`-The command line used for starting the application; usually, it is the name of the executable file.
   - `Command Line Arguments`-Additional parameters, if any, used for starting the application. Note that the path, command line, and command-line parameters are updated automatically during the application's installation procedure.
   - If another server application is used as a backup for this one, specify the `Backup Server` and the `Redundancy Type`.

   > **Warning**
   > You must have a special high-availability (HA) license to use redundant configurations. Otherwise, the Management Layer does not perform a switchover between the primary and backup servers. Refer to the ''Genesys Licensing Guide'' for details.

5. Select the `Options` tab and specify (or change) the values of the configuration options as necessary. Click on the option name for its description. For additional information about the options, see:
   - The ''Framework Configuration Options Reference Manual'' for Configuration Layer and Management Layer component options.
   - The latest version of the *Framework T-Server Deployment Guide* for your specific T-Server and/or HA Proxy options.
   - The latest version of the *Framework 8.1 Stat Server User's Guide* for Stat Server options.

   If the application's working directory differs from the directory in which the application was originally installed, configure an option named `messagefile` in the `log` section. Specify the full path to the application-specific log messages file (`*.lms`) as the option value. Otherwise, the application is unable to generate its specific log events.
6. Click Save or `Apply` to save your changes. The new application is now listed in the list of applications.

End of procedure

> **Important**
>
> If you configure two applications as a redundant pair (primary and backup), Genesys strongly recommends that you synchronize configuration options and server ports between the two applications. When a port is defined on the primary server application, a compatible port is automatically allocated on the backup server application. If the two server applications are configured as a redundant pair, you cannot remove or change the ports on the backup server. If the two are not linked as a redundant pair, you can delete the ports on the application that had been the backup.

## Configuring ADDP

You can enable ADDP for a connection between any two Genesys applications that are configured as client-server pair and that support ADDP.

> **Important**
>
> Some applications do not support ADDP for certain connections. Refer to application-specific documentation or Release Notes to determine if your application supports ADDP.

### [+] Show steps

#### Prerequisites

- The Configuration Layer is installed and running.
- Application objects for each application in the client-server pair exist.
- You are logged in to Genesys Administrator.

#### Start of procedure

1. In Genesys Administrator, go to `Provisioning` > `Environment` > `Applications`, and select the client application in the client-server pair.
2. Select the `Configuration` tab, and expand the `General` section.
3. In the `Connections` list, click `Add`.
4. In the `CfgConnectionInfo` dialog box that opens:
   a. From the list of servers, select the application name that represents the connection for which you want to configure ADDP.
   b. Specify `addp` as the value for the `Connection Protocol` field.
   c. Specify any integer as the value for the `Local Timeout` field. This indicates how often, in seconds, the client application sends polling signals to the server application.

> **Tip**
>
> To avoid false disconnect states that might occur because of delays in the data network, Genesys recommends setting the ADDP timeouts to values equal to or greater than ten (10) seconds.

d. If you also want to enable polling signals from the server application to the client, specify any integer as the value for the Remote Timeout field. This timeout is also measured in seconds.

e. In the Trace Mode field, select one of the following:

   a. Select Trace On Client Side to turn on ADDP at the client. The client application will generate ADDP-related messages in its logs.

   b. Select Trace On Server Side to turn on ADDP at the server. The application will generate ADDP-related messages in its logs.

   c. Select Trace On Both Sides to turn on ADDP at both the client and server. The Client and server applications will both generate ADDP-related messages in their logs.

   d. Select Trace Is Turned Off to turn off ADDP tracing altogether. ADDP-related messages will not be generated.

f. Click OK, and then Save to save the configuration changes.

End of procedure

## Graphical User Interface Applications

To create and configure a GUI Application object:

### Prerequisites

- The Configuration Layer is installed and running.
- At least one of the servers to which the GUI connects is installed.
- You are logged in to Genesys Administrator.

### Start of procedure

1. In Genesys Administrator, go to Provisioning > Environment > Applications, and select New in the toolbar.
2. From the available application templates in the Browse dialog box, choose the template for this application. See Application Templates for information about templates.
3. In the General section of the Configuration tab, enter a name for this application in the text box. The application template provides information for the application type and version.
4. Select the Connections tab. If necessary, add connections to any server applications to which this GUI application must connect.
5. Click Save to save your changes. The new GUI application is now listed in the list of applications.

End of procedure

# Generic Installation Procedures

This section provides instructions for installing a typical Genesys application that you have configured using Genesys Administrator.

Refer to the instructions for a particular application for the location of installation packages on a product CD and for any application-specific deviations from the standard installation procedure.

## Server Applications

This section describes a standard installation procedure for a server application on UNIX and Windows operating systems.

### Prerequisites

- An Application object exists for the server application. See Creating and Configuring a Server Application object.

## On UNIX

> **Warning**
> During installation on UNIX, all files are copied into the directory you specify. The install process does not create any subdirectories within this directory,; therefore, do not install different products into the same directory.

1. On the product CD, locate a shell script called `install.sh`.
2. Run this script from the command prompt by typing the file name.
3. When prompted, specify the `Host Name` of the computer on which this server is to run.
4. When prompted, specify the:
   - `Host Name` of the computer on which Configuration Server is running.
   - `Port` used by client applications to connect to Configuration Server.
   - `User Name` used to log in to the Configuration Layer.
   - `Password` used to log in to the Configuration Layer.
5. The installation displays the list of applications of the specified type configured for this host. Type the number of the server application to be installed.

6. Specify the the full path of the destination directory into which this server is to be installed.
   If the installation script finds that the destination directory is not empty, it prompts you to do one of the following:
   - Back up all files in the directory.
   - Overwrite only the files contained in this package.
   - Wipe the directory clean.

   Type the number that corresponds to your selection and confirm your choice.
7. If asked which version of the product to install, 32-bit or 64-bit, choose the one appropriate to your environment.
8. If you plan to use functionality that requires a license, such as Solution Control Server (SCS) with Simple Network Management Protocol (SNMP), type y when prompted and enter one of the following:
   - The full path to the license file
   - The License Manager port and host

As soon as the installation process is finished, a message appears indicating that installation was successful. The process places the server application in the directory specified during the installation.

## On Windows

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

1. On the product CD, locate and double-click `setup.exe` to start the Genesys Installation Wizard.
2. Click `About` on the wizard's `Welcome` page to review the `read_me` file. The file also contains a link to the server's Release Notes file.
3. Click `Next` on the `Welcome` page to proceed with the installation.

> **Tip**
> Click Next at the end of each step to proceed to the next page.

4. On the `Connection Parameters to the Genesys Configuration Server` page, specify the following login parameters:
   - `Host` and `Port` of Configuration Server
   - `User name` and `Password` used to log in to the Configuration Layer.
5. The `Select Application` page displays all applications of this type that the Configuration Database

contains. When you select one application from the list, the wizard displays some parameters configured for the selected application (such as application type, host, working directory, command line, and command-line arguments).
Select the application to install.

> **Warning**
> If the component does not require a technical license, omit step 6 and step 7. If the component requires a technical license for startup, omit step 6. If the component requires a technical license to enable a certain feature, but the license is not otherwise required, proceed with step 6.

6. On the Run-time License Configuration page, select one of the following options:
   - Use License if you plan to use features that require special licenses.
   - Without License if you do not plan to use features that require special licenses. In this instance, go to step 8.
     If you decide to use a licensed feature later on, reinstall the server and enter the appropriate license information through the Genesys Installation Wizard.
7. On the Access to License page, select one of the following options:
   - License Manager-You want your server application to use host and port parameters to connect to the license server. In this instance, you must enter values for the host and the port of the license server.
   - License File-You want your server application to retrieve license server information from the license file. Click Browse to navigate to the license file.
8. On the Choose Destination Location page, the wizard displays the destination directory, as specified in the Working Directory property of the server's Application object. If the path configured as Working Directory is invalid, the wizard generates a path to the destination directory in the C:\Program Files\GCTI\<Product Name> format.</bw> If necessary, click one of the following:
   - Browse to select another destination folder. In this case, the wizard will update the Application object's Working Directory in the Configuration Database.
   - Default to reinstate the path specified in Working Directory.
9. On the Ready to Install information page, click:
   - Back to update any installation information.
   - Install to proceed with installation. Installation Status displays the progress of the installation.
10. On the Installation Complete page, click Finish.

As a result of the installation, the wizard adds Application icons to the:

- Windows Start menu, under Programs > Genesys Solutions.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

## Graphical User Interface Applications

This section describes a standard installation procedure for a graphical user interface (GUI) application on Windows operating systems. If you are installing a web- or UNIX-based GUI, refer to the product documentation for installation instructions.

If you want to implement a security banner with a GUI application, make sure that you have the necessary files prepared before you start installing the GUI application. Refer to the ''Genesys 8.1 Security Deployment Guide'' for detailed information about the Security Banner feature.

1. From the product CD, locate and double-click `setup.exe` to start the Genesys Installation Wizard.
2. Use the `About` button on the wizard's Welcome page to review the `read_me file`. The file also contains a link to the application's Release Notes file.
3. Click `Next` to proceed with the installation.
4. On the `Security Banner Configuration` page, choose whether you want to configure a security banner for this GUI application.
   Do one of the following:
   - If you do not want to configure a security banner for this application, clear the `Enable Security Banner` check box, and click `Next`.
   - If you want to configure a security banner for this application:
     i. Select `Enable Security Banner`.
     ii. Follow the instructions in the procedure "Installing and configuring the Security Banner" in the ''Genesys 8.1 Security Deployment Guide''. When you are finished that procedure, return here and finish this procedure.
5. On the `Choose Destination Location` page, the wizard displays the path to the destination directory in the `C:\Program Files\GCTI\<Product Name>` format. If necessary, use the:
   - `Browse` button to select another destination folder.
   - `Default` button to reinstate the wizard-generated path (C:\Program Files\GCTI\<Product Name>).

   Click `Next`.

> **Important**
>
> ....
> If the GUI application requires any non-standard installation input from the user, extra pages appear here.
>
> ....

6. On the `Ready to Install` page, click:
   - `Back` to update any installation information.
   - `Install` to proceed with the installation. `Installation Status` displays the progress of the installation progress.
7. On the `Installation Complete` page, click `Finish`.

As a result of the installation, the wizard adds Application icons to the:

- Windows `Start` menu, under `Programs > Genesys Solutions`.
- Windows `Add or Remove Programs` window, as a Genesys application.

## Troubleshooting the Installation of a Genesys Application

To determine and fix the cause of a warning generated during the installation procedure for any Genesys application that Configuration Server is unavailable and that configuration cannot be updated, do the following:

1. Finish installing the Genesys application.
2. When installation of the application is complete, open the `Configuration` tab of the corresponding Application object.
3. Select the `State Enabled` check box.
4. Verify that the `Working Directory`, `Command Line`, and `Command Line Arguments` are specified correctly.
5. Save the configuration updates.

# Standard Login

When you start a Framework graphical user interface (GUI) application, or if you are being forced to log in again after a period of inactivity, a `Login` dialog box displays. The Configuration Layer checks the information specified in the Login dialog box and determines the user's permission to view, create, and modify objects in the Configuration Database.

> **Important**
>
> Configuration Layer will not allow users whose use of Genesys Administrator has been disabled to log into Genesys applications.

## Logging In

To login to a Framework GUI, do the following:

1. Start the application. Refer to the documentation for the particular application for specific instructions.
2. In the `Login` dialog box:
   a. Enter a user name. If you are logging in to the Configuration Layer for the first time, use the Master Account user name, which is `default`. After the appropriate configuration objects of the User type are added to the configuration, use a customized user name.
   b. Enter a user password. If you are logging in to the Configuration Layer for the first time, use the Master Account password, which is `password`. After the appropriate configuration objects of the User type are added to the configuration, use your own password. Your System Administrator will notify you if any requirements or restrictions apply to your password (see User Password Requirements and Restrictions).
   If you have configured Configuration Server to allow access with a blank password, you can optionally leave the `Password` field empty. Refer to the ''Framework Configuration Options Reference Manual'' for information on configuring this functionality.
   c. Click either `Details` or `More` options to display additional input login fields.
   d. Enter the application name, which is the instance of the application to which you are logging in, as it is registered in the Configuration Database.

      > **Important**
      >
      > The predefined name of the Genesys Administrator object is default. You can rename it later.

   e. Enter a host name, which is the name of the computer on which Configuration Server runs.
   f. Enter a port number, which is the number of the communication port that client applications use to connect to Configuration Server.

If your configuration uses both primary and backup Configuration Servers, your GUI applications might automatically reconnect to the backup server if they lose their connection to the primary server. You can specify automatic or manual reconnection; refer to the on-line Help file of your GUI application.

## User Password Requirements and Restrictions

Starting in release 8.1.1, the System Administrator or other authorized person can configure restrictions for user passwords and how they are used. The restrictions include:

- The type and case of characters allowed in a password.
- Whether a password can expire, and after how long.
- After using a given password, how many different passwords must be used before using that given password again, or if re-use is permitted at all.
- Whether the user must change their password the next time they log in.
- The number of unsuccessful login attempts that can be made after which the account is locked.

For more information about these requirements, and how to configure them, refer to the ''Genesys 8.1 Security Deployment Guide''.

# Configuration History Log

The Configuration History Log consists of a set of a records that contains historical information about client sessions and changes to configuration objects. It enables a client to restore a session that was terminated by a service interruption, and request any changes to configuration objects that occurred during that service interruption.

For all Configuration Servers, the records are stored in the Configuration Database. Configuration Server Proxy reads the information from its primary Configuration Server.

The History Log is installed with default parameters when you install Configuration Server. You configure the History Log parameters in the options of the Configuration Server `Application` object in Genesys Administrator. Refer to the ''Framework Configuration Options Reference Manual'' for detailed descriptions of the configuration options that relate to the History Log.

When requested by a client that is recovering from a service interruption, Configuration Server or Configuration Server Proxy does the following:

- Restores the client's session according to a client session record.
- Returns all data that has been changed since that client disconnected.

History Log functionality is mandatory, and cannot be turned off permanently.

## History Log Maintenance

No maintenance is required for the History Log, because it is maintained automatically by Configuration Server. The history log records are stored in the Configuration Database and are maintained using configuration records. Based on the expiration parameters, Configuration Server purges information from the database, both at startup and during normal operations.

## History Log Errors

Any errors that occur when writing to the History Log generate Log Event 21-22138.

> **Important**
> Genesys strongly recommends that you associate an alarm with this Log Event, and that you inform Genesys Customer Care if you encounter any errors or corruption.

## Minimizing Performance Impacts

Depending partially on the size of the updates, the History Log can affect the performance of Configuration Server. To minimize these performance impacts, you can turn off the History Log functionality temporarily by setting the `active` option to false for the Configuration Server Application object. The functionality will be turned back on either when you manually reset the option (to `true`), or when you restart Configuration Server.

> ### Warning
> When History Log functionality is turned off, current activities are not recorded. Therefore, clients that are disconnected during this time cannot retrieve the updates necessary to restore their sessions.

If you want to keep the History Log active (that is, `active=true`, consider setting `write-former-value=false` when performing large or significant updates. This will prevent previous values from being written to the history database, but will greatly improve performance.

Refer to the ''Framework Configuration Options Reference Manual'' for more information about the options used to configure the Configuration Server History Log.

# Accessing History of Configuration Changes

Configuration Server uses the Configuration History Log to keep track of changes being made in the Configuration Database. The History Log within Configuration Server contains more dealied information than is output in Audit-level log messages. Starting in release 8.5.0, Genesys provides a tool to extract this detailed information.

Also in release 8.5.0, previous values (as they were before a change) can also be stored in the history log along with the actual changes.

> **Important**
>
> The history log does not provide complete information about changes to assigned access Permissions

## Retrieving the History

Extract the changes history to an XML file by starting an instance of Configuration Server (any instance in the configuration will suffice; it does not have to be the Configuration Server currently running) and specifying the following parameter on the command line with the startup command:

```
-dumpauditxml <file name> [-last <days>]
```

where:

`<file name>` - The name of the XML file to which the information will be extracted. The information will be in the XML format shown in the example below.

`-last <days>` - (Optional) The results for the operations for the last number of days; if this argument is not specified, all audit history in the database is exported.

The Configuration Server starts, exports the information into the file specified in the parameter, and then terminates.

## Exported File Format

The exported XML file contains two primary sections. The `CfgAuditEntry` section contain information about the type of update, what object was updated, and who updated it. Its fields are described in the table below. Each `CfgAuditEntry` section contains one or more `CfgHistoryRecord` sections, that contain the former value and the action that was taken during the update identified in the `CfgAuditEntry`. An excerpt of a sample exported file is available after the table.

| Field Name | Description |
|---|---|
| id | The ID of the audit record that exists in the database. |
| operation_type | The type of operation performed based on the internal enumeration of the Configuration Server implementation. |
| operation_time | The timestamp when the operation occurred. |
| object_dbid | The internal DBID of the object being updated. |
| user_name | The username of the user performing the update. |
| object_data_size | The size of the audit record, as contained in the CfgHistory Record tag. |
| object | The name of the object being updated. |
| host | The name of the host or IP address from which the user performing the update is connected to Configuration Server. |
| application | The name of the user application that is connected to Configuration Server when performing the update operation. |
| application_dbid | The DBID of the user application that is connected to the Configuration Server when performing the update operation. |
| user_tenant | The name of the tenant to which the user performing the update belongs. |
| user_tenant_dbid | The DBID of the tenant to which the user performing the update belongs. |
| tenant | The name of the tenant to which the object being updated belongs. |
| tenant_dbid | The DBID of the tenant to which the object being updated belongs. |

## Sample File

### [+] Show sample file

```
<CfgAuditEntry
   id="187"
   operation_type="4"
   operation_time="[01/07/14 09:35:04]"
   object_type="CfgCampaign"
   object_dbid="101"
   user_name="default"
   object_data_size="529"
   object="CampaignA"
   host="135.17.178.16"
   application="default"
   application_dbid="100"
   user_tenant="Environment"
```

```
   user_tenant_dbid="1"
   tenant="Environment"
   tenant_dbid="1">
<CfgHistoryRecord
  id="187">
 <former_value>
  <action
    action="change">
   <CfgCampaignUpdate
     DBID="101">
    <callingLists
      action="change">
     <CfgCallingListInfo
       linkDBID="101"
       share="22"     />
    </callingLists>
   </CfgCampaignUpdate>
  </action>
 </former_value>
 <action>
  <CfgCampaignUpdate
    DBID="101">
   <callingLists
     action="change">
    <CfgCallingListInfo
      linkDBID="101"
      share="20"    />
   </callingLists>
  </CfgCampaignUpdate>
 </action>
</CfgHistoryRecord>
 </CfgAuditEntry>
```

# Advanced Disconnect Detection Protocol

All but a few Genesys interfaces use the TCP/IP stack. To compensate for the manner in which this stack operates, Genesys components use the Advanced Disconnect Detection Protocol (ADDP), which periodically polls the opposite process when no actual activity occurs at a given connection. If a configurable timeout expires without a response from the opposite process, the connection is considered lost and an appropriate event is sent to the application.

Genesys recommends enabling ADDP on the links between any pair of Genesys components. ADDP helps detect a connection failure on both the client and the server side. For most connections, enabling detection on the client side only is sufficient and it reduces network traffic. However, Genesys strongly recommends that you use detection on both sides for all connections between Configuration Server and its clients (including Solution Control Interface), as well as between any two T-Servers.

To enable ADDP between two applications, specify addp as the Connection Protocol when configuring the connection between applications; also, set values for the `Local Timeout`, `Remote Timeout`, and `Trace Mode` properties. For more information, refer to the ''Framework Configuration Options Reference Manual''.

For complete instructions on configuring ADDP between two applications, refer to Configuring ADDP. For instructions on configuring ADDP between the primary and backup T-Servers, refer to the Deployment Guide for your specific T-Server.

After a communication session failure is detected, the application makes repeated attempts to regain access to the required resource. If a redundant process is not configured, the reaction is a repeated attempt to restore the communication session with the same process. If a redundant process is configured, the application makes alternate attempts to restore the failed communication session and to establish a session with the redundant process. This way, if the session has terminated because of a failure of the opposite process, the application eventually connects to the standby process configured to provide the same type of service.

> **Important**
>
> Backwards compatibility of the Keep-Alive Protocol (KPL) is not supported. If you used KPL in previous versions of Genesys, consider using ADDP instead.

# Disaster Recovery Configuration

This section describes the configuration of a Disaster Recovery / Business Continuity architecture, as described in Disaster Recovery Architecture. The configuration is based on the Oracle GoldenGate software.

## Operation

### System Startup Procedure and Normal Operating Mode

1. Start the replication process. **[+] Show steps**

> **Tip**
>
> For reference, use the Oracle® GoldenGate Windows and UNIX Administrator's Guide 11g Release 1 (11.1.1) E17341-01 (Ref 1.)

a. On the MAIN and SECONDARY systems, run the script that removes INSERT, UPDATE, and DELETE permissions to CFG_DB and MS_DB users.

b. Use the `START MANAGER` command to start manager processes at both sites.

c. At the SECONDARY site, using GGSCI, start REPLICATs in preparation to receive changes from the Configuration and Log Databases on the live MAIN system.

```
START REPLICAT CSP
START REPLICAT MSP
```

d. At the MAIN site, using GGSCI, start REPLICAT MSS in preparation to receive changes from the log Database on the live SECONDERY system.

```
START REPLICAT MSS
```

e. On the MAIN site system, alter the primary Extract to begin capturing data based on the current timestamp. Otherwise, Extract will spend unnecessary time looking for operations that date back to the time that the group was created using the `ADD EXTRACT` command.

```
ALTER EXTRACT CSP, BEGIN NOW
ALTER EXTRACT MSP, BEGIN NOW
```

f. On the SECONDARY site system, alter the secondary Extract to begin capturing data based on the current timestamp. Otherwise, Extract will spend unnecessary time looking for operations that date back to the time that the group was created with the `ADD EXTRACT` command.

```
ALTER EXTRACT MSS, BEGIN NOW
```

g. On the MAIN system, start the primary Extracts so they are ready to capture transactional changes.

```
START EXTRACT CSP
START EXTRACT MSP
```

h. On the SECONDARY system, start the secondary Extract so it is ready to capture transactional changes

at the secondary Log Database.
`START EXTRACT MSS`

i. On the MAIN system, do the following:
   - Run the script that grants INSERT, UPDATE, and DELETE permissions to CFG_DB and MS_DB users.
   - Run the script that enables triggers and cascade delete constraints.

j. On the SECONDARY system, do the following:
   - Run the script that grants INSERT, UPDATE, and DELETE permissions to MS_DB users.
   - Run the script that enables triggers and cascade delete constraints.

At this point, the database system is ready for normal operation.

2. Start the system. **[+] Show steps**

a. Run the scripts that switchover `cfgmaster` host name IP resolution to a MAIN live system.
b. Launch the MAIN live Master Configuration Server primary/backup pair at Site 1.
c. Launch the MAIN live Master Solution Control Server to control the main Master Configuration server pair at Site 1.
d. Launch the MAIN Message server at Site 1 to support communications for Solution Control Servers controlling site components.
e. Launch Solution Control Server at Sites 1 and 2.
f. Using Solution Control Server, start the Configuration Proxy Server pair at Sites 1 and 2.
g. Using Solution Control Server, start the Framework site components.

## Disaster Recovery Switchover

At this point, all system components residing at the MAIN site on Host 3 are lost and not running:

- MAIN live Master Configuration Server primary/backup pair
- MAIN live Master Solution Control Server
- MAIN Message server at Site 1
- Oracle database
- Oracle GoldenGate

Operations on other sites can be continued non-stop in limited mode without a configuration change using Configuration Server Proxies running in Read-Only mode until the SECONDARY Master Configuration Server is brought on-line.

Perform the following steps to move activity to the SECONDARY live Master Configuration Server primary/backup pair.

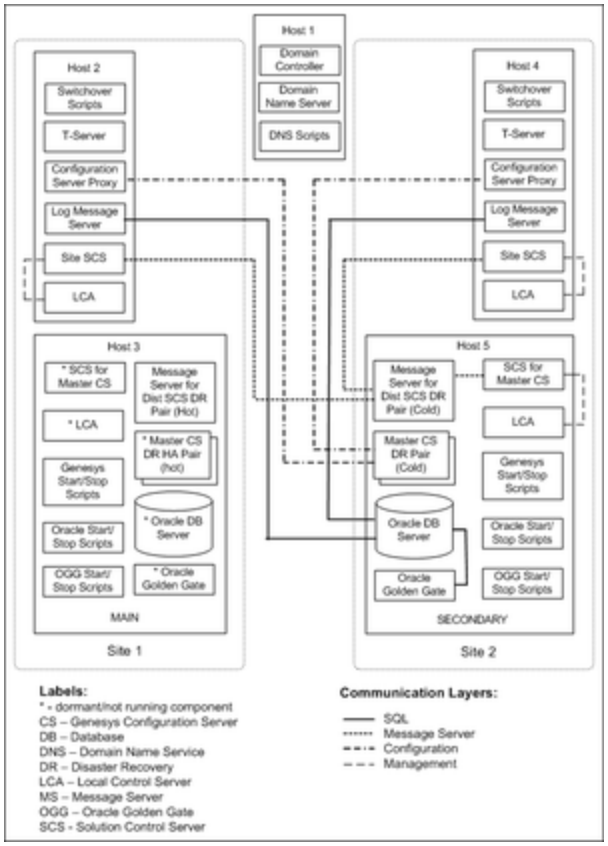
1. On the SECONDARY live standby system, using GGSCI, issue the `LAG REPLICAT` command until it returns `At EOF (end of file)` to confirm that REPLICAT applied all of the data from the trail to the

| |
|---|
| database.<br>`LAG REPLICAT CSP`<br>`LAG REPLICAT MSP` |
| 2. Stop the REPLICAT processes.<br>`STOP REPLICAT CSP`<br>`STOP REPLICAT MSP` |
| 3. On the SECONDARY system, run the script that grants INSERT, UPDATE, and DELETE permissions to the CFG_DB and MS_DB users. |
| 4. Run the script that enables triggers and cascade delete constraints. |
| 5. Launch the SECONDARY live Master Configuration Server primary/backup pair at Site 2. |
| 6. Launch the SECONDARY live Master Solution Control Server to control the MAIN Master Configuration server pair at Site 2. |
| 7. Launch the SECONDARY Message Server at Site 2 to support communication for Solution Control Servers controlling site components. |
| 8. Run the `dnsname` script that switches over `cfgmaster` host name IP resolution to a MAIN live system. |
| 9. On the host running Configuration Server Proxies, run the switch over script to flush the DNS cache. |

Communication Server Proxies reconnect to the SECONDARY live Master Configuration Server primary/backup pair and resume normal operation.

> **Warning**
>
> Do not start the data EXTRACTOR on the SECONDARY system. The user transactions must accumulate in the SECONDARY system database until the MAIN system is to be restored. Use the Secondary CSS replication group for database replication from SECONDARY to MAIN system before switching back to the MAIN system.

The diagram below shows the system in completed failover mode.



Multi-Site Disaster Recovery Architecture

# Configuration Example

## Configuration for Oracle GoldenGate Replication Processes

1. At the MAIN and SECONDARY Oracle databases, create a user `CFG_DB` for the Configuration Server datable, and user `MS_DB` for the Log Message Server database.

2. Using the initialization scripts in the Installation Package, create the database objects for the Configuration and Log Message Server Databases.

3. Use Oracle® GoldenGate Oracle Installation and Setup Guide11g Release 1 (11.1.1) E17799-01 (Ref 1.) and the examples of Parameter files below to configure the EXTRACT and REPLICAT processes. **[+] Show details**

| Process | Table (EXTRACT) / Map (REPLICAT) Parameters |
|---|---|
| `EXTRACT CSP` | `SEQUENCE CFG_DB.*;` |
| `EXTRACT CSS` | `TABLE CFG_DB.*;`<br>`TABLEEXCLUDE CFG_DB.cfg_refresh;` |

| Process | Table (EXTRACT) / Map (REPLICAT) Parameters |
|---|---|
| EXTRACT MSP | SEQUENCE MS_DB_1.*;<br><br>TABLE MS_DB_1.*;<br>TABLEEXCLUDE MS_DB_1.G_LOG_SCHEMA_INFO; |
| EXTRACT MSS | SEQUENCE MS_DB_2.*;<br><br>TABLE MS_DB_2.*;<br>TABLEEXCLUDE MS_DB_2.G_LOG_SCHEMA_INFO; |
| REPLICAT CSS | MAP CFG_DB.*,TARGET CFG_DB.*;<br><br>MAPEXCLUDE CFG_DB.cfg_refresh; |
| REPLICAT CSP | |
| REPLICAT MSP | MAP MS_DB_1.*,TARGET MS_DB_1.*;<br><br>MAPEXCLUDE MS_DB_1.G_LOG_SCHEMA_INFO; |
| REPLICAT MSS | MAP MS_DB_2.*,TARGET MS_DB_2.*;<br><br>MAPEXCLUDE MS_DB_2.G_LOG_SCHEMA_INFO; |

4. Register Oracle GoldenGate EXTRACT and REPLICAT using GGSCI. **[+] Show steps**

On the MAIN live system:
```
dblogin userid gg_user, password gg_password
register extract CSP, LOGRETENTION
register extract MSP, LOGRETENTION
```

On the SECONDARY live standby system:
```
dblogin userid gg_user, password gg_password
register extract CSS, LOGRETENTION
register extract MSS, LOGRETENTION
```

## Extract Group CSP at Primary Site Configuration Example

1. At MAIN system, start GGSCI.

2. Use the ADD EXTRACT command to create an Extract group CSP.

```
   ADD EXTRACT CSP , TRANLOG, BEGIN NOW
```
Use TRANLOG as the data source option.

3. Use the ADD RMTTRAIL command to specify a remote trail to be created on the target system.

```
   ADD RMTTRAIL ./CS, EXTRACT CSP
```
Use the EXTRACT argument to link this trail to the Extract group.

4. Use the EDIT PARAMS command to create a parameter file for the Extract group. Include the following parameters plus any others that apply to your database environment.

```
   EDIT PARAMS CSP
```

CSP EXTRACT Parameters File Example: **[+] Show file**

```
EXTRACT CSP
```

```
RMTHOST <Secondary host name>, MGRPORT 7809
RMTTRAIL ./dirdat/CP
USERID gg_user PASSWORD gg_password
TRACE ./trace/cfg_db.trc
--Only use if DDL is configured
WILDCARDRESOLVE DYNAMIC
DDL INCLUDE MAPPED OBJNAME cfg_db.*
DDLOPTIONS ADDTRANDATA RETRYOP RETRYDELAY 20 MAXRETRIES 60 REPORT
-- TRANLOGOPTIONS DBLOGREADER, DBLOGREADERBUFSIZE 1024000
-- TRANLOGOPTIONS  DBLOGREADERBUFSIZE 1024000

STATOPTIONS RESETREPORTSTATS
REPORT AT 00:01
REPORTROLLOVER AT 00:01
REPORTCOUNT EVERY 60 SECONDS, RATE
--
SEQUENCE cfg_db.*;
TABLE cfg_db.*;
TABLEEXCLUDE cfg_db.cfg_refresh;
```

### REPLICAT Group CSP at Secondary Site Configuration Example

1. At the SECONDARY system, start GGSCI.

2. Use the ADD REPLICAT command to create a Replicat group CSP.

```
ADD REPLICAT CSP, EXTTRAIL CSP, BEGIN NOW
```

Use the EXTTRAIL argument to link the Replicat group to the remote trail.

3. Use the EDIT PARAMS command to create a parameter file for the Replicat group. Include the following parameters plus any others that apply to your database environment:

```
EDIT PARAMS CSP
```

CSP REPLICAT Parameters File Example: **[+] Show file**

```
MACRO #exception_handler
BEGIN
, TARGET ggate.exceptions
, COLMAP ( rep_name = "rep"
, table_name = @GETENV ("GGHEADER", "TABLENAME")
, errno = @GETENV ("LASTERR", "DBERRNUM")
, dberrmsg = @GETENV ("LASTERR", "DBERRMSG")
, optype = @GETENV ("LASTERR", "OPTYPE")
, errtype = @GETENV ("LASTERR", "ERRTYPE")
, logrba = @GETENV ("GGHEADER", "LOGRBA")
, logposition = @GETENV ("GGHEADER", "LOGPOSITION")
, committimestamp = @GETENV ("GGHEADER", "COMMITTIMESTAMP"))
, INSERTALLRECORDS
, EXCEPTIONSONLY;
END;
-- This ends the macro
REPLICAT CSP
HANDLECOLLISIONS
--END RUNTIME
USERID gg_user, PASSWORD gg_password
ASSUMETARGETDEFS
DISCARDFILE ./dirrpt/CP.dsc, purge
TRACE ./trace/CSP.trc
```

```
-- INCLUDE ALL -- &
-- STATOPTIONS RESETREPORTSTATS
DDL INCLUDE  ALL
--INCLUDE MAPPED  --  &

-- DBOPTIONS SUPPRESSTRIGGERS, DEFERREFCONST
DBOPTIONS  DEFERREFCONST
REPORT AT 00:01
REPORTROLLOVER AT 00:01
REPORTCOUNT EVERY 60 SECONDS, RATE
---
DDLOPTIONS REPORT
DDLERROR DEFAULT IGNORE
REPERROR (DEFAULT, EXCEPTION)
REPERROR (DEFAULT2, ABEND)
REPERROR (-1, EXCEPTION)
MAP CFG_DB.*,TARGET CFG_DB.*;
MAPEXCLUDE CFG_DB.cfg_refresh;
--MAP CFG_DB.* #exception_handler();
```

## Configuration of Genesys Components

| |
|---|
| 1. Start the replication process (P.3.3.1.1). |
| 2. Run the `dnscmd` script that switches over `cfgmaster` host name IP resolution to a MAIN live system. |
| 3. Install the MAIN live Master Configuration Server primary/backup pair at Site 1. |
| 4. Install the SECONDARY dormant Configuration Server primary/backup pair at Site 2. |
| 5. Launch the MAIN live Master Configuration Server primary/backup pair at Site 1. |
| 6. Using Genesys Administrator connected to the Primary Master Configuration Server at Site 1, configure Master Solution Control Server, Message Server for distributed SCS, and Backup Master Configuration Server. |
| 7. Install Master Solution Control Server, Message Server for distributed SCS, and Master Backup Configuration Server on Site 1. |
| 8. Copy Master Solution Control Server, Message Server for distributed SCS, and Master Backup Configuration Server working directories to Site 2. |
| 9. Launch Master Solution Control Server and Message Server for distributed SCS. |
| 10. Using Genesys Administrator connected to the Primary Master Configuration Server at Site 1, configure and install Configuration Server Proxies, Solution Control Servers, and Message Servers for network logging for Sites 1 and 2. |
| 11. Start Configuration Server Proxies at Sites 1 and 2. |
| 12. Start Solution Control Servers at Sites 1 and 2. |
| 13. Start Message Servers for network logging at Sites 1 and 2. |
| 14. Install Framework Components at Site 1 using the Configuration Server Proxy host and port at Site 1. |
| 15. Install Framework Components at Site 2 using the Configuration Server Proxy host and port at Site 2. |

# File and Script Examples

## EXTRACT Parameters File

### [+] Show file

```
EXTRACT <extract_name>
RMTHOST <target databse host name>, MGRPORT 7809
RMTTRAIL ./dirdat/<rmttrail_name>
USERID <golden_gate_user> PASSWORD <golden_gate_password>
TRACE ./trace/<oracle_user_name>.trc
--Only use if DDL is configured
WILDCARDRESOLVE DYNAMIC
DDL INCLUDE MAPPED OBJNAME <oracle_user_name>.*
DDLOPTIONS ADDTRANDATA RETRYOP RETRYDELAY 20 MAXRETRIES 60 REPORT
-- TRANLOGOPTIONS DBLOGREADER, DBLOGREADERBUFSIZE 1024000
-- TRANLOGOPTIONS  DBLOGREADERBUFSIZE 1024000

STATOPTIONS RESETREPORTSTATS
REPORT AT 00:01
REPORTROLLOVER AT 00:01
REPORTCOUNT EVERY 60 SECONDS, RATE
--
SEQUENCE <oracle_user_name>.*;
TABLE <oracle_user_name>.*;
TABLEEXCLUDE <exclude_filter>;
```

## REPLICAT Parameters File

### [+] Show file

```
MACRO #exception_handler
BEGIN
, TARGET ggate.exceptions
, COLMAP ( rep_name = "rep"
, table_name = @GETENV ("GGHEADER", "TABLENAME")
, errno = @GETENV ("LASTERR", "DBERRNUM")
, dberrmsg = @GETENV ("LASTERR", "DBERRMSG")
, optype = @GETENV ("LASTERR", "OPTYPE")
, errtype = @GETENV ("LASTERR", "ERRTYPE")
, logrba = @GETENV ("GGHEADER", "LOGRBA")
, logposition = @GETENV ("GGHEADER", "LOGPOSITION")
, committimestamp = @GETENV ("GGHEADER", "COMMITTIMESTAMP"))
, INSERTALLRECORDS
, EXCEPTIONSONLY;
END;
-- This ends the macro
REPLICAT <replicat_name>
HANDLECOLLISIONS
--END RUNTIME
USERID <golden_gate_user>, PASSWORD <golden_gate_password>
ASSUMETARGETDEFS
DISCARDFILE ./dirrpt/<discard_file_name>.dsc, purge
TRACE ./trace/<traice_file_name>.trc
-- INCLUDE ALL -- &
-- STATOPTIONS RESETREPORTSTATS
DDL INCLUDE  ALL
--INCLUDE MAPPED  --  &
```

```
-- DBOPTIONS SUPPRESSTRIGGERS, DEFERREFCONST
DBOPTIONS  DEFERREFCONST
REPORT AT 00:01
REPORTROLLOVER AT 00:01
REPORTCOUNT EVERY 60 SECONDS, RATE
---
DDLOPTIONS REPORT
DDLERROR DEFAULT IGNORE
REPERROR (DEFAULT, EXCEPTION)
REPERROR (DEFAULT2, ABEND)
REPERROR (-1, EXCEPTION)
MAP <oracle_user_name>.*,TARGET <oracle_user_name>.*;
MAPEXCLUDE <exclude_filter>;
--MAP CFG_DB.* #exception_handler();
```

## dnscmd Scripts

### [+] Show scripts

#### Switch to SECONDARY Master Server

```
rem DNSCMD DELETE command
dnscmd 135.17.36.102 /RecordDelete mst.lab cfgmaster A /f
rem DNSCMD ADD command
dnscmd 135.17.36.102 /RecordAdd mst.lab cfgmaster A 135.17.36.140
```

#### Switch to MAIN Master Server

```
rem DNSCMD DELETE command
dnscmd 135.17.36.102 /RecordDelete mst.lab cfgmaster A /f
rem DNSCMD ADD command
dnscmd 135.17.36.102 /RecordAdd mst.lab cfgmaster A 135.17.36.139
```

## Switch over Script

### [+] Show script

```
ipconfig /flushdns
ping cfgmaster.mst.lab
```

# Internet Protocol version 6 (IPv6)

IPv6 is a network layer for packet-switched inter-networks. It is designated as the successor of IPv4, the current version of the Internet Protocol, for general use on the Internet.

> **Important**
>
> - This section contains a detailed description of IPv6 and deployment considerations associated with it. See IPv6 vs. IPv4 Overview for information about activating support for IPv6 for a Genesys component. For a list of Framework connections that support IPv6, see IPv6 Support.
> - This section includes material that is freely available on the Internet and from other public sources.

## Addressing

The primary change from IPv4 to IPv6 is the length of network addresses. IPv6 addresses are 128 bits long (as defined by RFC 4291), whereas IPv4 addresses are 32 bits. This amounts to an address space for IPv4 of approximately 4 billion addresses, compared to 3.4 x $10^{38}$ unique addresses for IPv6.

IPv6 addresses are typically composed of two logical parts: a 64-bit network or subnetwork prefix, and a 64-bit host part. This host part is either generated automatically from the MAC address of the interface, or assigned sequentially. Because globally unique MAC addresses offer an opportunity to track user equipment (and therefore users) across IPv6 address changes, RFC 3041 was developed to reduce the chance of user identity being permanently tied to an IPv6 address, thus restoring some of the anonymity existing with IPv4. RFC 3041 specifies a mechanism by which time-varying random bit strings can be used as interface circuit identifiers, replacing unchanging and traceable MAC addresses.

### Notation

IPv6 addresses are normally written as eight groups of four hexadecimal digits separated by colons (:). For example:

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

If one or more four-digit groups is `0000`, the zeros can be omitted and replaced with two colons (::). For example:

```
2001:0db8:0000:0000:0000:0000:1428:57ab
```

can be shortened to

```
2001:0db8::1428:57ab
```

Following this rule, any number of consecutive `0000` groups can be reduced to two colons, as long as

there is only one double colon used in an address. Leading zeros in a group can also be omitted (as in `::1` for a `localhost` address). Therefore, the following addresses are all valid and are equivalent:

```
2001:0db8:0000:0000:0000:0000:1428:57ab
2001:0db8:0000:0000:0000::1428:57ab
2001:0db8:0:0:0:0:1428:57ab
2001:0db8:0:0::1428:57ab
2001:0db8::1428:57ab
2001:db8::1428:57ab
```

Note that having more than one double-colon syntax element in an address is invalid, as it would make the notation ambiguous. For example, the following address:

```
2001:0000:0000:FFD3:0000:0000:0000:57ab
```

abbreviated to

```
2001::FFD3::57ab
```

could imply any of the following:

```
2001:0000:0000:0000:0000:FFD3:0000:57ab
2001:0000:FFD3:0000:0000:0000:0000:57ab
```

or any other similar permutation.

For more information about IPV6 addressing, refer to RFC 4291.

## Literal IPv6 Addresses in URLs

In a URL, the IPv6 address is enclosed in brackets. For example:

```
http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]/
```

This notation enables the parsing of a URL without confusing the IPv6 address and port number, such as in:

```
https://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:443/
```

Additional information can be found in RFC 2732 and RFC 3986.

## Network Notation

IPv6 networks are written using Classless Inter-Domain Routing (CIDR) notation.

An IPv6 network (or subnet) is a contiguous group of IPv6 addresses, the size of which must be a power of two. The initial bits of any address in the network are called the prefix, and are identical for all hosts in the network.

A network is denoted by the first address in the network, and the size (in bits) of the prefix (in decimal), separated with a forward-slash (`/`). For example:

```
2001:0db8:1234::/48
```

stands for the network with addresses

```
2001:0db8:1234:0000:0000:0000:0000:0000
```

through

```
2001:0db8:1234:ffff:ffff:ffff:ffff:ffff
```

Because a single host can be seen as a network with a 128-bit prefix, host addresses are often followed with `/128`.

## Kinds of IPv6 addresses

IPv6 addresses are divided into the following categories (see RFC 4291 - IP Version 6 Addressing Architecture):

- unicast addresses
- multicast addresses
- anycast addresses

### Unicast Addresses

A unicast address identifies a single network interface. A packet sent to a unicast address is delivered to that specific computer. The following types of addresses are unicast IPv6 addresses:

- Global unicast addresses
- Link-local addresses (prefix `fe80::/10`): Valid only on a single link; analogous to `169.254.0.0/16` in IPv4
- Unique local IPv6 unicast addresses
- Special addresses (see examples in the following table)

| | |
|---|---|
| `::/128` | The address with all zeros is an unspecified address, and is to be used only in software. |
| `::1/128` | The loopback address is a localhost address. It corresponds to `127.0.0.1` in IPv4. |
| `::ffff:0:0/96` | This prefix is used for IPv4-mapped addresses (see Transition Mechanisms). |
| `2002::/16` | This prefix is used for 6to4 addressing. |
| `2001:db8::/32` | This prefix is used in documentation (RFC 3849). Anywhere where an example of an IPv6 address is given, addresses from this prefix should be used. |

### Multicast Addresses

Multicast addresses are used to define a set of interfaces that typically belong to different nodes instead of just one. When a packet is sent to a multicast address, the protocol delivers the packet to all interfaces identified by that address. Multicast addresses begin with the prefix `FF00::/8`. The second octet identifies the scope of the addresses, that is, the range over which the multicast address is propagated. Commonly used scopes include link-local (`0x2`), site-local (`0x5`) and global (`0xE`).

### Anycast Addresses

Anycast addresses are also assigned to more than one interface belonging to different nodes. However, a packet sent to an anycast address is delivered to just one of the member interfaces, typically the closest as defined by the routing protocol. Anycast addresses cannot be easily identified. They have the structure of normal unicast addresses, and differ only by being injected into the routing protocol at multiple points in the network.

### Broadcast Addresses

There are no address ranges reserved for broadcast in IPv6. Applications use multicast to the all-hosts group instead. The Internet Assigned Numbers Authority (IANA) maintains the official list of the IPv6 address space. Global unicast assignments can be found on the various Regional Internet Registries (RIR) or on the Ghost Route Hunter Default Free Prefixes (GRH DFP) pages.

## Transition Mechanisms

Until IPv6 completely supplants IPv4, which is not expected to occur in the foreseeable future, a number of transition mechanisms are needed to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach the IPv6 Internet over the IPv4 infrastructure. An overview of some of the various IPv6 transitions that currently exist is provided at: [1]

### Dual Stack

Because IPv6 is a conservative extension of IPv4, it is relatively easy to write a network stack that supports both IPv4 and IPv6 while sharing most of the source code. Such an implementation is called a *dual stack*, and a host implementing a dual stack is called a *dual-stack host*. This approach is described in RFC 4213.

Most current implementations of IPv6 use a dual stack. Some early experimental implementations used independent IPv4 and IPv6 stacks. There are no known implementations that implement IPv6 only.

### Tunneling

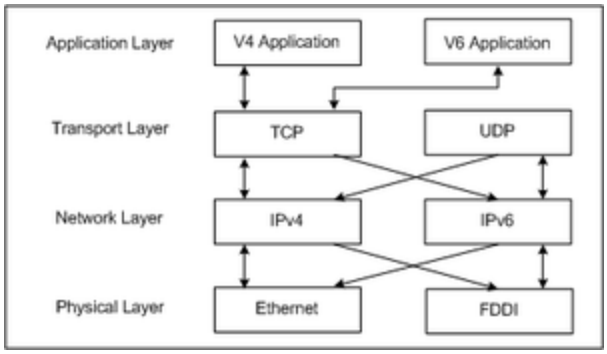
To reach the IPv6 Internet, an isolated host or network must be able to use the existing IPv4 infrastructure to carry IPv6 packets. This is done using a technique referred to as *tunneling*. Tunneling consists of encapsulating IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

IPv6 packets can be directly encapsulated within IPv4 packets using Protocol 41. They can also be encapsulated within User Datagram Protocol (UDP) packets, for example, to cross a router or Network Address Translation (NAT) device that blocks Protocol 41 traffic. They can also use generic encapsulation schemes, such as Anything In Anything (AYIYA) or Generic Routing Encapsulation (GRE).

# Architecture

## Dual-Stack IPv6 Implementation

Genesys support for IPv6 relies on true dual-stack IPv6 implementation of the operating system as specified in RFC 3493. Conceptually, the configuration of a dual-stack machine with a v4 TCP and a v6 TCP application is shown in the following figure.



Dual-Stack Architecture

Using this approach, you can write an application that can operate with both IPv4 and IPv6 peers using just one socket. In addition, an application that uses a properly designed Transport Layer library and does not have to operate directly with IP addresses (and other Network Layer elements) may not be aware of the IP version used at all.

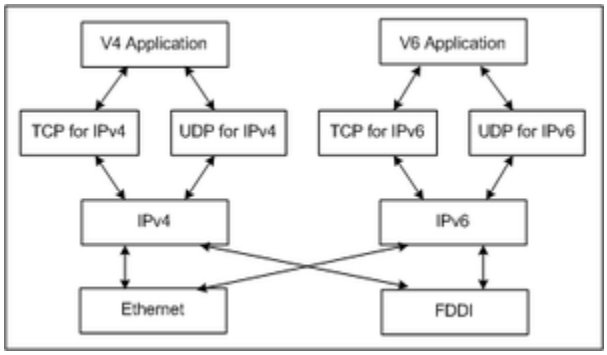
## Microsoft Windows Implementation

Microsoft uses slightly different terminology when describing IPv6 architecture. For Microsoft, dual-layer refers to dual-network layers sharing a single transport layer. Dual-stack refers to dual-network layers and dual transport layers, that is, two separate stacks. Only a dual-layer architecture is compliant with RFC 3493.

> **Important**
>
> In this document dual-stack always refers to RFC 3493-compliant implementations, not the Microsoft definition.

### Windows Server 2000/2003 and Windows XP

The following figure illustrates Microsoft Windows IPv6 implementation prior to Windows Vista. Microsoft calls this a dual-stack architecture, but it is actually implemented as two separate stacks with separate TCP and UDP paths. This implementation forces an application to open separate sockets to talk to IPv4 and IPv6 peers.



Microsoft IPv6 Stack Prior to Windows Vista

### Windows Vista

In Windows Vista, Microsoft calls its next generation IP stack dual-layer architecture, but it is actually a correct dual-stack implementation as described above, where there is only a single transport layer component for TCP and UDP.

## Operating Systems Supporting Dual-Stack Architecture for IPv6

Operating system support of dual-stack IPv6 implementation (RFC 3493-compliant) by different operating system platforms is provided in the following table. Refer to platform-specific documentation (including web sites) for additional information about supporting and implementing IPv6.

| Operating System | Supporting Releases |
|---|---|
| AIX | AIX 4.3.3 and later |
| Linux | kernel 2.6 (Red Hat Enterprise Linux release 4) and later |
| Mac OS X | Mac OS 10.3 Panther and later |
| Solaris | Solaris 8 and later |
| Windows | Windows Vista and later, Windows Server 2008 and later |

# DNS

Genesys products are using Domain Name System (DNS) resolution of hostnames specified in configuration, and require that the DNS is operating according to the AAAA schema. IPv6 addresses are represented in the Domain Name System by AAAA records (so-called `quad-A records`) for forward lookups; reverse lookups take place under `ip6.arpa` (previously `ip6.int`), where the address space is delegated on nibble boundaries. This scheme, which is a straightforward adaptation of the familiar A record and in-addr.arpa schemes, is defined in RFC 3596. The following table describes the fields in an AAAA record.

| Field Name | Description |
|---|---|
| NAME | Domain name |
| TYPE | AAAA (28) |
| CLASS | Internet (1) |
| TTL | Time to live (seconds) |
| RDLENGTH | Length of RDATA field |
| RDATA | String form of the IPv6 address as described in RFC 3513 |

RFC 3484 specifies how applications should select an IPv6 or IPv4 address for use, including addresses retrieved from DNS. For mixed networks, the DNS must provide both A and AAAA records.

On a historical note, the AAAA schema was one of two proposals at the time the IPv6 architecture

was being designed. The other proposal, designed to facilitate network renumbering, would have had A6 records for the forward lookup and a number of other innovations such as bit-string labels and DNAME records. It is defined in the experimental RFC 2874 and its references (with further discussion of the advantages and disadvantages of both schemes in RFC 3364).

## Virtualization

There are no known restrictions from the Genesys side for deploying IPv6 in a virtual operating environment. Check with the documentation specific to the virtual environment you are using for more information and any limitations.

## License Control

> **Important**
> The information in this section is based on information provided in Flexera documentation, and may be specific to their products. For information about IPv6 support and implementation for other licensing products, consult documentation specific to the product.

Genesys uses FlexLM 9.5 and FlexNet Publisher 11.9-based license control, but only the FlexNet Publisher Licensing toolkit 11.9 supports IPv6. Genesys License Server 8.1 uses FlexNet Publisher 11.9 for all platforms.

The following table summarizes the addressing compatibility of a FlexNet License Server Machine and a Flex-enabled Application Server, as described in this section.

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="4">FlexNet License Server Machine</th></tr>
<tr><th>IPv4-only</th><th>Dual IPv4/ IPv6 Stack</th><th>IPv6-only</th><th>No Server</th></tr>
<tr><td rowspan="5">Flex-enabled Application Server</td><td>IPv4-only</td><td rowspan="3">Use IPv4 only</td><td>Use IPv4 only</td><td rowspan="2">Not supported</td><td rowspan="2">Use IPv4 only</td></tr>
<tr><td>Dual Stack using IPv4 only</td><td rowspan="2">Use IPv4, IPv6, or both</td></tr>
<tr><td>Dual Stack using IPv4 and IPv6</td><td rowspan="3">Use IPv6 only</td><td>Use IPv4, IPv6, or both</td></tr>
<tr><td>Dual Stack using IPv6 only</td><td rowspan="2">Not supported</td><td rowspan="2">Use IPv6 only</td><td rowspan="2">Use IPv6 only</td></tr>
<tr><td>IPv6 only[a]</td><td>Use IPv6 only</td></tr>
</table>

[a] Genesys does not recommend or support IPv6 environments.

In the license file, an IPv6 address should be defined as the `host` value in the SERVER line. Entries in the license search path that use the `port@host` convention to identify the license server can also specify an IPv6 address as the `host` value.

## Deploying License Servers in Mixed Protocol Environments

For FlexNet Publisher components to work properly using IPv6 addresses, all systems in an enterprise (including the network hardware and software) must be configured properly to support communication using IPv6 addresses.

Before testing or deploying a FlexEnabled application that supports IPv6 or IPv4/IPv6 dual communication, make sure that all systems on the network can communicate successfully. If the license server can run under any of the following operating systems:

- Any supported edition of Windows Vista
- Any supported Linux platform
- Any supported Unix platform

it can communicate with FlexEnabled clients using either IPv4 or IPv6, so long as the network is configured properly.

Because these operating systems support dual-layer communication, both IPv4 and IPv6 FlexEnabled clients can communicate with an IPv6 license server. In addition, IPv6 clients can communicate with an IPv4 license server using the IPv4 address.

The FlexNet Publisher license server lmadmin supports both IPv4 and IPv6 clients. If you are using it, you must rename one of your vendor daemon executable files, because separate IPv4 and IPv6 vendor daemons are required.

If the license server runs on Windows XP or Windows Server 2003, there are certain limitations because of the limited dual-layer support on these operating systems (see Windows Server 2000/ 2003 and Windows XP). IPv4 FlexEnabled clients cannot communicate with an IPv6 license server running on these operating systems. However, IPv6 FlexEnabled clients can communicate with an IPv4 license server running on these operating systems.

If an enterprise runs license servers on Windows 2003 or Windows XP, the license administrators should create and maintain two separate networks - one for IPv6 FlexEnabled clients that will use the IPv6 license server, and one for IPv4 FlexEnabled clients that will use the IPv4 license server.

## Using Wildcards in an IPv6 Address

An asterisk (*) can be used as a wildcard character in place of an entire field or on a byte-by-byte basis to specify a range of addresses without having to list them all.

For example, the following feature definition line is locked to four specific addresses:

```
FEATURE f1 myvendor 1.0 1-jan-2010 uncounted \
HOSTID="INTERNET=127.17.0.1,\
INTERNET=2001:0db8:0000:0000:ff8f:effa:13da:0001,\
INTERNET=127.17.0.4,\
NTERNET=2001:0db8:0000:0000:ff8f:effa:13da:0004" \
SIGN="<...>"
```

The following feature definition line specifies an entire range of addresses, including the four specific ones from the line above:

```
FEATURE f1 myvendor 1.0 1-jan-2010 uncounted \
HOSTID="INTERNET=127.17.0.*,\
INTERNET=2001:0db8:0000:0000:*:*:*:000*"\
SIGN="<...>"
```

# Genesys 8.1 IPv6 Support

Genesys supports IPv6 as described in this section.

## Common Principles

The implementation of IPv6 in Genesys is based on the following assumptions:

- Dual-stack requirement and backward compatibility
- Dual IPv4/IPv6 server sockets
- IPv4 preference for DNS

### Dual-Stack Requirement and Backward Compatibility

Only dual-stack IPv6 implementations are supported. Support of IPv6 on Windows 2002/2003 and XP is not required, while all recent versions of UNIX have dual-stack support already. However, the connection layer must still operate on all other platforms in IPv4 mode only.

On the platforms where IPv6 support is available, the default mode of operation is IPv4 for backward compatibility. IPv6 support must be turned on explicitly by each application using one of the following methods:

- Set the environment variable `GCTI_CONN_IPV6_ON` to 1.
- In the `common` section of the `Application` object's options, set `enable-ipv6` to 1.

Refer to IPv6 vs. IPv4 Overview for more details about enabling IPv6 in Genesys software.

> **Important**
> IPv6 is, by default, not enabled. But once it is enabled using one of the methods described above, it can only be disabled by turning it off in both places-the environment variable and the option. That is, turning it off in one location only disables it if it is not enabled in the other.

### Dual IPv4/IPv6 Server Sockets

By default, a server socket opened by a standard method should accept both IPv4 and IPv6 client connections. That is, unless IPv6 is disabled on a particular node, unbound server sockets are opened

with the AF_INET6 family and use the AI_V4MAPPED flag to interact with IPv4 clients. However, a server socket bound to a particular IP address (either IPv4 or IPv6) only accepts a connection of the same IP family.

#### IPv4 Preference for DNS

Within an application, a name service should be used whenever possible. An AAAA record may return both a IPv4 and IPv6 address for dual stack nodes. For backward compatibility reasons, client connections in this case should prefer IPv4 over IPv6. That preference can be set using the configuration option ip-version.

However, a client connection bound to a particular IP address (either IPv4 or IPv6) can only interact with the server using a connection of the same IP family.

### Implementation Characteristics

Individual Genesys components support the following features related to IPv6:

- Full IPv6 support in DNS lookup: Support both AAAA records and DNS over IPv6.
- Transparent server-side socket handling: The existing server-side interface allows IPv6 connections whenever possible using the AI_V4MAPPED flag.
- Transparent client-side connection: The existing client-side connection interface allows IPv6 connections by host name or explicit IP address in text format.
- DNS Lookup modes: Full DNS support using the synchronous method (name lookup using standard system calls) and asynchronous DNS (enabled by the enable-async-dns option in the common section of an Application object's options). Server and client side IPv6 sockets and connections are supported transparently, including hosts being addressed either by name, or by textual IP address in either IPv4 or IPv6 format.
- IPv6-related changes in the configuration environment: Configuration Server keeps IP addresses for all configured hosts, but it is not a replacement for DNS. However it is expected to be affected very little. In particular, a new field for the IPv6 address is not added to the CfgHost structure; while the new configuration option ip-version set at the connection level determines whether the connection uses IPv4 first (4,6; the default), or IPv6 first (6,4). To achieve compatibility with legacy servers (that is, a server without IPv6 support running on a dual-stack host, while IPv6-enabled clients try to connect), the suggested solution is to create an IPv4-only hostname alias for that host.

For more information about the two configuration options, refer to IPv6 vs. IPv4 Overview.

### IPv6 Support by Genesys Products

To determine if a Genesys product supports IPv6, refer to the documentation for that product. Framework connections that support IPv6 are listed in IPv6 Support.

## Deployment Considerations

When deploying IPv6 in your Genesys environment, you must take into consideration the factors discussed in this section.

## Security

Preparation for IPv6 utilization will require careful planning of security measures, because IPv6 presents new challenges compared to IPv4. Some, but not all, of the challenges are discussed in this section.

### TLS

In some deployments, multiple hostnames are assigned to a given computer, and are resolved to different IP versions. In this case, the TLS certificate of the given computer will have to be generated for all assigned hostnames.

Refer to the ''Genesys 8.1 Security Deployment Guide'' for information about generating certificates.

### Firewall and Client-Side Port

Genesys supports fine-grain firewall configuration at the port-level and applied both to incoming client connections and their target server destinations.

In IPv6 deployments, this might become even more valuable, for example, as a countermeasure against Network Discovery (ND) attacks. ND in IPv6 utilizes five different types of ICMPv6 messages for several purposes. ND attacks in IPv6 will likely replace ARP spoofing in IPv4.

### Internet Protocol Security

Internet Protocol Security (IPSec) is an optional feature in IPv4, but is mandatory in IPv6. In certain deployments, it could make the use of TLS unnecessary.

### DNS Security Extensions

Genesys recommends the use of DNS Security Extensions (DNSSEC), but it is not mandatory. There are no dependencies from the Genesys side.

## IP Tunneling

When connecting sites, you may want to use IP tunneling. For example, two sites could be operating in IPv4 mode while the interconnection requires IPv6. In this case, one could consider embedding the IPv4 protocol into an IPv6 connection between sites.

## Licensing

The G8.1 License Server (the Genesys vendor daemon) is based on FlexNet Publisher 11.9, and is IPv6 enabled.

However, within G8.1 the IPv6-enabled licensing client libraries (FlexNet Publisher 11.9) are implemented for only the RHEL 5 64-bit, Windows 2008 64-bit, and HP-UX Integrity (Itanium) operating systems. For all other platforms, the G8.1 applications are still using the older client libraries, which are not IPv6 enabled. This is done to provide backward compatibility; otherwise, the deployment of a G8.1 application in an existing environment would have required a complete upgrade of the licensing system.

Therefore, Genesys recommends that IPv4 be used for licensing.

### SIP

The SIP protocol can contain explicit IP address values. This creates additional challenges, for example at the NAT level, but also if the same SIP Server instance has to concurrently support multiple SIP interfaces where one is operating in IPv4 mode and another in IPv6 mode.

It is recommended to address those scenarios by using a dedicated SIP Server for IPv4 only and another one for IPv6 only.

You could also consider using available NAT solutions that perform configurable SIP protocol inspection and conversion. One example is F5 Networks Big-IP LTM.

> **Important**
> IPv6 support for SIP is not yet implemented in Genesys components.

### Thin Clients

Some Genesys client applications offer a web browser interface with an HTTP connection to a web server. These connections are under control of the given web technology, and all modern browsers already support IPv6. However, IPv6 must be enabled at both the client computer and server computer sides, and the DNS involved must also support IPv6.

### External Interfaces

IPv4 dependencies at external interfaces must be considered. This includes, for example, interfaces to Session Border Controllers (SBC), media gateways, switches, and databases.

### Dynamic Runtime Changes

Changes in the IPv4/IPv6 configuration should be performed during maintenance windows, as they will require a restart of impacted processes. These changes will include setting the following:

- Transport parameter `ip-version`
- DNS entries for hostnames
- Local computing node settings

### Third-Party Dependencies

Genesys uses several third-party products as part of the suite. The IPv6 capabilities of those products must be considered.

# IPv6 vs. IPv4 Overview

> **Important**
>
> This section provides a high-level view of IPv6, and how to enable it in a Genesys component. For detailed information about IPv6, the operating systems that support it, and things to consider when deploying it, see Internet Protocol version 6 (IPv6). For a list of Framework connections that support IPv6, see IPv6 Support.

Internet Protocol version 6, commonly known as IPv6, is a network layer protocol for packet-switched inter-networks. It is designated as the successor of IPv4, the current version of the Internet Protocol, for general use on the Internet.

## Configuring IPv6

IPv6 must be configured on each component that is going to support it. You can do this using an environment variable or a configuration option, depending on the situation:

You must use an enironment variable if:

- An IPv6 connection is to be established before an application is able to, or must, read information from Configuration Server.
- You want all Genesys applications on the same host to support IPv6. You only have to configure this on the host once, rather than configure each application on that host individually. The host-level setting will override any application-level setting.

Otherwise, you can use either an environment variable or a configuration option.

## Set Environment Variable

Set the environment variable `GCTI_CONN_IPV6_ON` to `true` (represented by any non-zero integer value) to enable IPv6; or to `false` (represented by zero (`0`)) to disable IPv6. The default value of this environment variable is false (`0`), indicating that IPv6 support is disabled. This default value ensures backward compatibility.

## Set Configuration Option

Using Genesys Administrator, set the `enable-ipv6` option in the `common` section of the options of the component's `Application` object. Refer to the ''Framework Configuration Options Reference Manual''

for more information about this option.

Refer to component-specific documentation and Internet Protocol version 6 (IPv6) for more information about IPv6 and any specific considerations for deploying IPv6 in your situation.

## Mixed IPv4 and IPv6 Environments

You can configure IPv6 and IPv4 in the same environment, as described in Internet Protocol version 6 (IPv6). In this mixed environment, you can configure connections with servers that support IPv4, IPv6, and both. For connections with servers that support both IPv4 and IPv6, you can specify which version you prefer to use. For example, if you are setting up a connection to a DB Server that supports both IP4 and IPv6, you can choose to use IPv4 or IPv6 for that connection. There is no universal rule that determines what version should be used, so the choice is up to you.

To configure this choice, you can use either an environment variable or a transport option.

## Set Environment Variable

Set the environment variable `GCTI_CONN_IP_VERSION` to either `4,6` to indicate a preference for IPv4; or to `6,4` to indicate a preference for IPv6. The default value of this environment variable is 4,6, indicating that IPv4 is preferred. This default value ensures backward compatibility. The value of this environment variable is overridden if the transport parameter `ip-version` is configured at the application level.

## Set Transport Option

Using Genesys Administrator, set the Transport parameter `ip-version` on the `Advanced` tab of the `Connection Info` dialog box for the connection. Refer to the ''Framework Configuration Options Reference Manual'' for more information about this parameter.

> **Important**
>
> This option has no affect on connections to Configuration Server that are established before the option value can be read from the Configuration Database.

The same option can also be set in the transport section of the Host's Annex to set the IP version used on the connection between Solution Control Server and LCA. Otherwise, Management Framework components do not support this option. When the same transport option is set on the application level, it overrides the value of the environment variable `GCTI_CONN_IP_VERSION`.

Refer to the ''Framework Configuration Options Reference Manual'' for more information about setting this option in an application or in a host.

The following table summarizes how this environment variable or option affects the connection for which it is configured.

| Connecting Server | 4,6 | 6,4 |
|---|---|---|
| Supports only IPv4 | ipv4 is used | ipv4 is used |
| Supports both IPv4 and IPv6 | ipv4 is used | ipv6 is used |
| Supports only IPv6 | ipv6 is used | ipv6 is used |

> **Warning**
> Genesys does not recommend or support IPv6-only environments.