GENESYS®
AN ALCATEL-LUCENT COMPANY

Framework 7.6

Deployment Guide

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

About Genesys

Genesys Telecommunications Laboratories, Inc., a subsidiary of Alcatel-Lucent, is 100% focused on software for call centers. Genesys recognizes that better interactions drive better business and build company reputations. Customer service solutions from Genesys deliver on this promise for Global 2000 enterprises, government organizations, and telecommunications service providers across 80 countries, directing more than 100 million customer interactions every day. Sophisticated routing and reporting across voice, e-mail, and Web channels ensure that customers are quickly connected to the best available resource—the first time. Genesys offers solutions for customer service, help desks, order desks, collections, outbound telesales and service, and workforce management. Visit www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the following regional numbers:

Region	Telephone	E-Mail
North and Latin America	+888-369-5555 or +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-118-974-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp

Prior to contacting technical support, please refer to the *Genesys Technical Support Guide* for complete contact information and procedures.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys 7 Licensing Guide***.

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 76fr_dep_02-2008_v7.6.002.00

Table of Contents

Chapter 5

Chapter 6

Preface

Welcome to the *Framework 7.6 Deployment Guide.* This document describes the configuration, installation, starting, and stopping procedures relevant to the Genesys Framework.

This guide is valid only for the 7.6 release(s) of this product.

Note: For releases of this guide created for other releases of this product, please visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

This chapter provides an overview of this guide, identifies the primary audience, introduces document conventions, and lists related reference information:

In brief, you will find the following information in this manual:

- How to install and use Wizard Manager.
- How to configure all Framework components with wizards or manually.
- How to install Framework components.
- How to configure redundancy—that is, backup and primary servers—for Framework components, including DB Server and Configuration Server.
- How to start and stop Framework components with the Management Layer or manually.
- How to log in to a Genesys GUI application.

Note: You can find detailed deployment information for T-Server and HA Proxy in the latest version of the *Framework T-Server Deployment Guide* for your specific T-Server.

If you use previous releases of Genesys products, consult *Genesys 7 Migration Guide* for migration-related procedures.

Intended Audience

This guide, primarily intended for system integrators, system administrators, contact center managers, and operations personnel, assumes that you have a basic understanding of:

- Computer-telephony integration concepts, processes, terminology, and applications.
- Network design and operation.
- Your own network configurations.

You should also be familiar with Genesys Framework architecture and functions, as described in the *Framework 7.6 Management Layer User's Guide,* Chapter 2 on page 31, and *Framework 7.6 Architecture Help.*

Chapter Summaries

In addition to this opening chapter, this guide contains these chapters and appendixes:

- Chapter 1, "Framework Overview," on page 17 lists major Framework functions, and highlights the new features in the initial 7.6 release.
- Chapter 2, "Framework Architecture," on page 31 describes the architecture and functionality of Framework 7.6 and its layers.
- Chapter 3, "Planning the Installation," on page 41 lists considerations such as licensing and environment, network locations for Framework components, solution availability and security considerations, and describes the main tasks that you should complete when planning your Framework installation.
- Chapter 4, "Deployment Overview," on page 69 lists the prerequisites for installing the Genesys Framework, and prescribes the deployment order. This chapter also describes the Genesys Installation Wizard and Genesys Configuration Wizards, and how to access them.
- Chapter 5, "Setting Up the Configuration Layer," on page 81 describes how to set up the Framework Configuration Layer, the mandatory part of any Genesys installation.
- Chapter 6, "Setting Up the Management Layer," on page 103 describes how to set up the Framework Management Layer.
- Chapter 7, "Setting Up the Rest of Your System," on page 133 provides a brief overview of setting up the rest of your system after you have set up the Configuration and Management Layers.

- Chapter 8, “Starting and Stopping Framework Components,” on page 139 provides instructions for starting and stopping Framework components, either using the Management Layer or manually.
- Chapter 9, “Setting Up Redundant Components,” on page 155 provides instructions for configuring primary and backup Framework Servers.
- Chapter 10, “Setting Up Geographically Distributed Systems,” on page 189 describes Genesys Framework support for geographically distributed systems. This chapter also describes how to set up Configuration Server Proxy and Distributed Solution Control Servers, and how to configure their clients to work with them.
- Appendix A, “Standard Configuration Procedure,” on page 205 provides generic instructions for configuring Genesys `Application` objects using Configuration Manager.
- Appendix B, “Standard Installation Procedure,” on page 211 provides generic instructions for installing Genesys applications that are configured using Configuration Manager.
- Appendix C, “Login Procedure,” on page 217 describes the required login parameters for any Genesys GUI application.
- Appendix D, “Windows Services,” on page 219 contains recommendations for installing Framework components as Windows Services.
- Appendix E, “Silent Setup,” on page 221 describes the InstallShield Silent Setup feature and provides instructions for using the Silent Setup for server and GUI applications.
- Appendix F, “Management Framework Deployment Manager,” on page 225 provides instructions for installing Management Framework components remotely using Management Framework Deployment Manager.
- Appendix G, “Installation Worksheet,” on page 231 provides an installation worksheet to fill in with information required during installation.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

76fr_dep_10-2007_v7.6.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

Type Styles

Italic

In this document, italic is used for emphasis, for documents' titles, for definitions of (or first references to) unfamiliar terms, and for mathematical variables.

Examples:

- Please consult the *Genesys 7 Migration Guide* for more information.
- *A customary and usual practice* is one that is widely accepted and used within a particular industry or profession.
- Do *not* use this value for this option.
- The formula, x +1 = 7 where x stands for . . .

Monospace Font

A monospace font, which looks like `teletype or typewriter text`, is used for all programming identifiers and GUI elements.

This convention includes the *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages; the values of options; logical arguments and command syntax; and code samples.

Examples:

- Select the `Show variables on screen` check box.
- Click the `Summation` button.
- In the `Properties` dialog box, enter the value for the host server in your environment.
- In the `Operand` text box, enter your formula.
- Click `OK` to exit the `Properties` dialog box.
- The following table presents the complete set of error messages T-Server distributes in `EventError` events.
- If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls.

Monospace is also used for any text that users must manually enter during a configuration or installation procedure, or on a command line:

Example:

- Enter `exit` on the command line.

Screen Captures Used in This Document

Screen captures from the product GUI (graphical user interface), as used in this document, may sometimes contain a minor spelling, capitalization, or grammatical error. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Square Brackets

Square brackets indicate that a particular parameter or value is optional within a logical argument, a command, or some programming syntax. That is, the parameter's or value's presence is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information. Here is a sample:

```
smcp_server -host [/flags]
```

Angle Brackets

Angle brackets indicate a placeholder for a value that the user must specify. This might be a DN or port number specific to your enterprise. Here is a sample:

```
smcp_server -host <confighost>
```

Related Resources

Consult these additional resources as necessary:

- *Framework 7.6 Architecture Help,* which helps you view the place of a particular component in the Framework architecture and learn about Framework functionality that is new to release 7.6. Click `Learn about the Configuration Layer Architecture` on the Configuration Import Wizard `Import your data` page.
- *Framework 7.6 Configuration Manager Help,* which helps you use Configuration Manager.
- *Framework 7.6 Configuration Options Reference Manual,* which provides descriptions of configuration options for Framework components.
- *Framework 7.6 Management Layer User's Guide,* which helps you better understand how the Management Layer works and how to enable its functions.

- *Genesys Master Glossary,* which ships on the Genesys Documentation Library CD and provides a fairly comprehensive list of the Genesys and CTI terminology and acronyms used in this document.
- *Genesys 7 Migration Guide*, which contains a documented migration strategy for each software release. Please refer to the applicable portion of this guide or contact Genesys Technical Support for additional information.
- *Genesys 7.6 Security Deployment Guide,* which describes the security features provided by Genesys software, including Transport Layer Security (TLS) support, and provides detailed instructions for deploying the features.
- The Release Notes and Product Advisories for Framework components, which you can find on the Genesys Technical Support website at `http://genesyslab.com/support`.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Systems and Databases*
- *Genesys Supported Media Interfaces*

Genesys product documentation is available on the:

- Genesys Technical Support website at `http://genesyslab.com/support`.
- Genesys Documentation Library CD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

Making Comments on This Document

If you especially like or dislike anything about this document, please feel free to e-mail your comments to `techpubs.webadmin@genesyslab.com`.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the information in this document only and to the way in which the information is presented. Speak to Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

Chapter

1

Framework Overview

This chapter lists major Framework functions and highlights new features added in each release.

This chapter contains the following sections:

Major Functions

The Genesys Framework, a mandatory part of any Genesys-based interaction management system, 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 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 (DBMSs).
- **Attached Data Distribution** supports the distribution of business data attached to interactions, within and across solutions.

New in This Release

The following sections list the new features and functions of Genesys Framework.

Framework 7.6.0

Before you familiarize yourself with the Genesys Framework architecture and functionality, note the following major changes that were implemented in the 7.6.0 release of Framework, and the sources that describe them in detail:

General Features

- **User inactivity timeout:** Users can now configure Configuration Manager and Solution Control Interface to force a logged-in user to log in again after a period of inactivity. The amount of time that the GUI will wait is configurable. See “Forced Re-Login for Inactivity” on page 67.
- **User-defined security banner:** Users can now configure Configuration Server, Solution Control Interface, and Framework Wizards to display a user-defined security banner at startup. See “Login Security Banner” on page 68.

Configuration Layer

- **Multiple LDAP servers:** Users can now configure multiple LDAP authentication servers for external authentication. See the *Framework 7.6 External Authentication Reference Manual* for details.
- **No access privileges for new users:** New users are now created with no access rights, and must be explicitly added to one or more Access Groups. See “New Users” on page 65.
- **Performance improvement for large History Log updates:** Users can now improve system performance of large updates for the History Log. See “Configuration History Log” on page 58.

Management Layer

See the *Framework 7.6 Management Layer User’s Guide* for information about the following new features that are specific to the Management Layer:

- **Customizable Log Events:** Users can now customize log events for an application by changing the log level of any log event, or by disabling the event. See the *Framework 7.6 Management Layer User’s Guide* for details.

Media Layer

- Please refer to your specific *Framework 7.6 T-Server Deployment Guide* for information about new features in T-Server 7.6.

Services Layer

- Please refer to the *Framework 7.6 Stat Server User's Guide* for information about new features in Stat Server 7.6.

Framework 7.5.0

Before you familiarize yourself with the Genesys Framework architecture and functionality, note the following major changes that were implemented in the 7.5.0 release of Framework, and the sources that describe them in detail:

General Features

- **Multiple ports:** Users can now configure multiple ports on all Applications of Server type with secure or unsecured connections. See "Genesys Security Using the TLS Protocol" on page 61.
- **Secure connections:** Users can now configure secure connections between the Genesys components that support this functionality. See "Genesys Security Using the TLS Protocol" on page 61.
- **Configuration Wizards:** Users can now install Configuration Wizards from the appropriate product CD, and run the wizards from a common Wizard Manager. There is no dependency between the wizards of any application. See "Genesys Wizards" on page 73.

Configuration Layer

- **Configuration of Cost-Based Routing:** Users can now use Configuration Manager to configure all objects and parameters for Cost-Based Routing in their environment.
- **Flexible Campaign Groups:** Users can now configure flexible properties for Campaign Groups, and assign additional servers to dedicated Campaign Groups. Additional dialing modes and a new Media Type are also available.
- **Multiple RADIUS servers:** Users can now configure multiple RADIUS authentication servers for external authentication.
- **History Log:** History Log functionality is now mandatory. Users can turn off this functionality to limit performance degradation during large update operations. History is now stored in one file, rather than in segments. See "Configuration History Log" on page 58.

- **Blank password:** Users can now configure Configuration Server to accept or reject a blank password. See Appendix C on page 217.

Management Layer

Refer to the *Framework 7.5 Management Layer User's Guide* for information about the following new features that are specific to the Management Layer:

- **SCS-generated log messages and alarms:** Solution Control Server (SCS) now processes log messages and alarms that it generates, without using the Message Server.
- **Alarm visibility:** Alarms are now visible only if you have access to the application that generated them.
- **Distributed SCSs:** You can now distribute control over the primary and backup servers in a redundant pair between different Distributed SCSs.
- **Customizable e-mail Alarm Reactions:** The Alarm Reaction Wizard now enables you to customize the `Subject` line and content of e-mail alarm reactions.
- **Timestamped logs:** SCS and Local Control Agent (LCA) logs now include date and time stamps.
- **Host name added to alarms:** Alarm reaction parameters now include the Host name.
- **Message queue controls:** You can now control the size of the LogMessages queue when the connection between Message Server and DB Server is unavailable. You can now also control how many messages Message Server sends to DB Server without waiting for a response.

Media Layer

- Please refer to your specific *Framework 7.5 T-Server Deployment Guide* for information about new features in T-Server 7.5.

Services Layer

- Please refer to the *Framework 7.5 Stat Server User's Guide* for information about new features in Stat Server 7.5.

Framework 7.2.0

General Features

Before you familiarize yourself with the Genesys Framework architecture and functionality, note the following major changes implemented in the 7.2.0 release of Framework and the sources that describe them in detail:

- **External authentication:** In a Managed Services environment, different Tenants can now authenticate through different LDAP servers. See the section "Customizing External Authentication Configuration" in chapter 2 of the External Authentication User's Guide.
- **Migration:** The Configuration Conversion Wizard (CCW) performs automatic migration from any release to release 7.2.
- **Security:** Transport of encrypted passwords between Configuration Server and its clients is secure—but only when all involved components are version 7.2.

Configuration Layer

- **Agent Group Supervisor:** Using Configuration Manager, now you can associate a Supervisor with an Agent Group. See the Configuration Manager help topic `Agent Groups > Advanced Tab`.
- **Reconnect Options:** Now you can specify automatic or manual reconnection for Configuration Manager. See the Configuration Manager help topic `View Menu`.
- **Improved Searches:** The Configuration Manager search function now accepts the wildcard characters `?` and `*`, and can be configured to be case-insensitive. See the Configuration Manager help file, the topic Configuration Manager Interface > Find command.
- **Interoperability:** Configuration Server 7.2 works with the clients of previous 6.x and 7.x releases. For more information, see the *Genesys 7 Migration Guide*.

Management Layer

- No Management Layer components or new functionality are included in this release. All 7.2 components are interoperable with 7.1 Management layer components.

Media Layer

- Please refer to your specific *Framework 7.2 T-Server Deployment Guide* for information about new features in T-Server 7.2.

Services Layer

- Please refer to the *Framework 7.2 Stat Server User's Guide* for information about new features in Stat Server 7.2.

Framework 7.1.1

Before you familiarize yourself with the Genesys Framework functionality, note the following major changes implemented in the 7.1.1 release of Framework.

- With release 7.1.1, Configuration Import Wizard no longer requires a separately-purchased license, and can be run from the Configuration Manager Tools menu.
- Configuration Manager, Genesys Wizard Manager, and Solution Control Interface display a new Login dialog that includes backup server information and a check box. See Appendix C, "Login Procedure," in this book.

Framework 7.1.0

General Features

Before you familiarize yourself with the Genesys Framework architecture and functionality, note the following major changes implemented in the 7.1 release of Framework and the sources that describe them in detail:

- **LDAP authentication:** Framework now supports external authentication for the Lightweight Directory Access Protocol (LDAP) servers:
    - Novel E-Directory
    - IBM Tivoli Directory Server
    - Microsoft Active Directory.

  See the *External Authentication Reference Manual*.
- **Detecting and clearing Stuck Calls:** SCI/SCS in the Management Layer can now detect probable stuck calls and either clear them automatically or notify you to do it manually. See the chapter "Stuck Calls Management" in the *Management Layer User's Guide*.
- **Virtual Agent Groups:** Configuration Server supports Stat Server's new ability to collect Virtual Agent Group (VAG)-based data. Configuration Server also checks VAGs converted from earlier installations and displays a message if it finds errors. See the Configuration Manager help file `Virtual Agent Groups` and the chapter "Virtual Agent Groups" in the *Stat Server User's Guide*.

Configuration Layer

- Configuration Manager users can view help for program errors directly from the menu bar: select `Help` > `Error Messages` and then choose from a list of all messages. As in previous releases, you can also click on a link to help from the error message itself.

Management Layer

- SCI now connects to the Configuration Server backup, after a lost connection, without requesting login information.
- The Management Layer supports Genesys Enterprise Telephony Software (GETS) functionality, including:
  - Integration with Microsoft Operational Manager (MOM) technology.
  - The Genesys Generic Server type.
- The Management Layer supports new SNMP Trap functionality:
  - SNMP Master Agent supports the “Clearance” alarm level (the ability to map the existing trap to the clearance trap so no additional checking is required to understand if the problem still exists). The level “Clearance” is specified in the SNMP trap sent upon alarm clearance.
  - SNMP Trap messages generated by Solution Control Server (and appearing in the Alarm Browser dialog box) now include host information.
- You can now output an Advanced Disconnect Detection Protocol (ADDP) trace for Local Control Agent and Solution Control Server to a log file; previously it was available only in `stdout`.
- You can now name a non-default configuration file, in the command line, when you start Local Control Agent. See the chapter “Local Control Agent” in the *Genesys 7.2 Configuration Options Reference Manual*.
- You can control delivery of specified log events from specified applications and application types. See “DB Filter Section” in Chapter 6 of the *Genesys 7.2 Configuration Options Reference Manual*.

Media Layer

- Please refer to your specific *Framework 7 T-Server Deployment Guide* for information about new features in T-Server 7.1.x.

Services Layer

- Please refer to the *Framework 7 Stat Server User’s Guide* for information about new features in Stat Server 7.1.x.

Framework 7.0.1

This section highlights the new features, listed by layer, included in the Genesys Framework Release 7.0.1.

General Features

- License control for redundant configurations is now enforced. You must have a special high-availability (HA) license to operate any Genesys server in a redundant configuration, whether with the redundancy type `warm standby` or `hot standby`.

Configuration Layer

- Configuration Server now supports certain third-party authentication systems. You can integrate Genesys software with your established security system, which may provide functions that Genesys does not provide. Essentially, you can deploy your system to control user access to Genesys applications and avoid creating an additional security schema in your Genesys configuration environment.
- You can perform the same configuration operation over multiple configuration objects in Configuration Manager simultaneously. In particular, you can:
    - Add or delete options and change option values on the `Annex` tab for all objects and on the `Options` tab for Applications.
    - Add or delete servers to connect to and modify connection parameters on the `Connections` tab for Applications.
    - Add or delete assigned skills and modify skill levels on the `Agent Info` tab for Persons.
    - Add or delete Switches to connect to and modify access code parameters on the `Access Codes` tab for Switches.
    - Mask a set of Alarm Condition objects.
- The Enumerator and Enumerator Value configuration objects are now called Business Attribute and Attribute Value respectively. In addition, the Configuration Database provides an increased number of predefined objects of these types.
- Support for new data sources is added to the Configuration Import Wizard, including:
    - Microsoft Excel documents.
    - NEC APEX 7400 switch configuration.

Management Layer

- You can use new commands in Solution Control Interface to start all or a set of configured solutions.
- Solution Control Interface now supports ADDP (Advanced Disconnect Detection Protocol) for its connection to Solution Control Server (SCS) and prompts users to reconnect to the backup SCS once the connection to the primary SCS is lost.

- Solution Control Server now requires a special HA license to perform a switchover between primary and backup servers for all Genesys applications.

Media Layer

- Please refer to your specific *Framework 7 T-Server Deployment Guide* for information about new features in T-Server 7.0.x.

Services Layer

- Please refer to the *Framework 7 Stat Server User's Guide* for information about new features in Stat Server 7.0.x.

Framework 7.0

This section highlights the new features, listed by layer, included in the initial Genesys Framework Release 7.0.

General Features

- The Centralized Log Database structure and logging functionality are improved. This includes performance optimization, the capability to attach attributes to the log messages in structured format, additional log outputs, and new options for more precise logging configuration.
- Generation of Audit Trail records is added to the Framework components. Audit Trail records are generated for both configuration changes and control actions performed over processes, solutions, and alarms and are stored in the Centralized Log Database.
- The Management Layer now offers the option of configuring a wait period prior to the promotion of a backup client to `Primary` mode.
- Capability to trace interactions is added to the Framework components. Interaction-tracing log events are generated as log events of the special level, with the Interaction ID attached, and are stored in the Centralized Log Database.
- To achieve better performance, server applications running on Windows operating platforms now write their logs with the character `LF (0x0A)` at the end of each line instead of the character sequence `CR LF (0x0D 0x0A)`, as was done in previous releases. This format is now the same as that of the log files written on UNIX operating systems.

Note: Because of the change in format, you can no longer view log files in real time with Windows Notepad. You can copy the file and open it with Windows WordPad. However, to view the log files in real time, you must use any third-party tool that supports this format.

Configuration Layer

- Support for geographically distributed configuration environments provided in release 6.5 with Configuration Server Proxy is now incorporated in Configuration Server itself. You may select an appropriate operational mode for the server during the installation.
- Configuration Server performance is improved at startup (up to 50%) and during interaction with the clients.
- Configuration Server fault tolerance is increased. Logical inconsistencies are now properly processed at startup and no longer cause termination of Configuration Server.
- Configuration Server now generates an audit trail for actions performed to configuration objects.
- Security in Configuration Server is further enhanced. Sensitive information like user passwords is now protected by the hashing and encryption algorithms.
- Error diagnostic in Configuration Server is improved. Descriptions are added to error messages.
- Use a new configuration object, Configuration Unit, to create complex configuration hierarchies for an enterprise.
- New configuration objects (Enumerator, Enumerator Value, and Objective Table) are added to support new functionality in other Genesys applications.
- You can now create user-defined Solution objects.
- Set customizable rules in the Application Templates to synchronize Application options for backup servers with options in primary servers.
- The `Switch` value is now synchronized between the primary and backup T-Servers.
- Certain applications can now use the new History of Changes Adapter (HCA) in Configuration Server to track the history of configuration changes.
- Starting multiple instances of Configuration Manager on the same computer and connecting them to different Configuration Servers is now possible.

- Configuration Manager now provides a more convenient way to display object properties, including configuration options, through the `Details` pane.
- Configuration Manager now enables you to move `Application` objects assigned to one Host from this Host to another one.
- Improved error handling in Configuration Manager now warns you when you are about to perform some critical operations.
- Permission management is improved in Configuration Manager: you can now perform recursive changes to permissions for specified accounts.
- Application settings for both redundancy type and backup server are now located on the `Application` object's `Server Info` tab in Configuration Manager.
- You can now customize the order of the first and last names specified in Person objects in Configuration Manager, so that you can sort these objects by the first name or by the last name.
- Properties for a DN object in Configuration Manager now include the `Register` field that enables you to select appropriate registration mode before you add a range of DNs to the Configuration Database.
- You can now also change the user's password for login to the Configuration Layer through the `File` menu in Configuration Manager interface.
- You can now use the Configuration Import Wizard to generate custom reports about the current configuration.
- Support for new data sources is added to the Configuration Import Wizard, including:
  - Microsoft Active Directory
  - Siemens Hicom 300 switch configuration
  - Intecom switch configuration (for Intecom E, Intecom E Millennium and Intecom PointSpan switch types)
  - Rockwell Spectrum switch configuration
- You can now compare two configuration sets and extract the difference suitable for subsequent import operations through the Configuration Import Wizard.
- Configuration Import Wizard now provides capability to launch Configuration Conversion Wizard when the latter is installed on the same computer.

Management Layer

- Management Layer now more accurately manages statuses of the monitored hosts. When a connection between Solution Control Server (SCS) and Local Control Agent (LCA) running on a given host cannot be established or is lost, SCS provides an appropriate descriptive status for the host.
- Management Layer now offers more details about statuses of the processes it monitors, including detection of the process's initialization phase and service availability.
- SCS now supports geographically distributed management environments. Running SCS in so-called *Distributed* mode allows you to run multiple instances of SCS within the same configuration environment to ease the solution control and monitoring tasks in geographically distributed installations.
- New log level—*Interaction*—for interaction-tracing is introduced.
- Logging functionality now includes support for Audit Trail records generation and their storage in the Centralized Log Database.
- SCS now generates Audit Trail records for control actions performed over processes, solutions, and alarms.
- SCS now generates more detailed Alarm History records for alarm activation and clearance and stores them in the Centralized Log Database.
- You can now use Solution Control Interface (SCI) to retrieve and display log records from the Centralized Log Database that are associated with interaction tracing, auditing, and Alarm History.
- SCS now provides more robust application switchover capabilities, including the ability to account for a variety of failover scenarios, in particular, those based on service availability.
- Alarming functionality is extended. New methods of Alarm detection include those based on system performance parameters and SNMP (Simple Network Management Protocol) thresholds. Capability to execute Alarm Reactions at Alarm clearance is added.
- MIB (Management Information Base) file is extended. This change offers you the following new functionality through the SNMP interface:
  - You can now monitor multiple servers simultaneously as well as retrieve configurable and selective data from multiple servers.
  - You can now monitor the status of additional objects, including Solutions (a given list of Solutions) and Hosts (a list of Hosts, including the Host name, IP address, status, and operating system).
- Management Layer now provides authorized users with graceful contact-center-shutdown capability. This customizable functionality operates through the SNMP interface. It allows you to gracefully shut down all currently running T-Servers. If you shut down T-Servers in this way, the

Management Layer provides you with information about on-going interactions and offers you the choice either to stop the shutdown or continue with it. After T-Servers are down and no new interactions are coming to the applications, you can use the Management Layer to shut down the rest of Genesys applications.

- Management Layer also provides new Predefined Alarm Conditions.

Media Layer

- Please refer to your specific *Framework 7 T-Server Deployment Guide* for information about new features in T-Server in the initial 7.0 release.

Services Layer

- Please refer to the *Framework 7 Stat Server User's Guide* for information about new features in Stat Server in the initial 7.0 release.

Retired Features

Starting with the 7.5 release, Framework no longer supports backward compatibility of the Keep-Alive Protocol (KPL) for 6.5 clients. If you used KPL in previous versions of Genesys, consider using Advanced Disconnect Detection Protocol (see page 58) instead.

Framework no longer supports Configuration Server Proxy as a separate component. Proxy functionality is transferred to Configuration Server starting with the initial 7.0 release.

Chapter

2 Framework Architecture

This chapter describes the architecture and functionality of Framework 7.6 and its layers.

This chapter contains the following sections:

High-Level Framework Architecture

The Genesys Framework consists of four layers (see Figure 1 on page 32):

- 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 **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 and enables solutions to communicate with various database management systems (DBMSs).

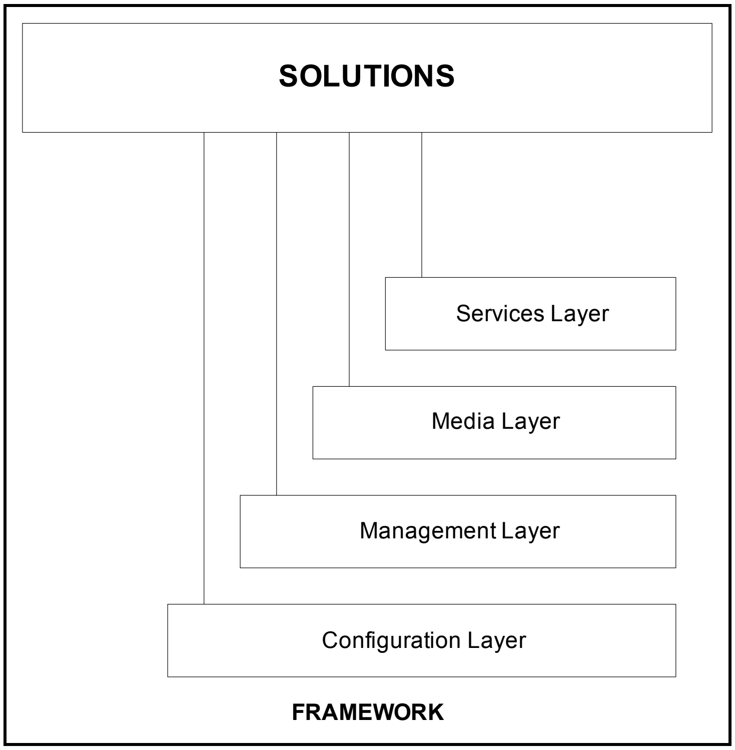


Figure 1: Framework Architecture

In sophisticated configurations using the Management Layer functionality, each layer depends on the layers below it to work properly.

Also note that a Genesys installation depends on License Manager, a third-party application not shown on the diagram, for license control.

Configuration Layer

Configuration Layer Functions

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.
- 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.
- Universal, open, Simple Object Access Protocol (SOAP) interface to the configuration, so that a broad range of third-party applications can read and write the information.

Warning! SOAP functionality is restricted to certain environments.

- Support for geographically distributed environments.
- Integration with external data sources.
- Import and export of configuration data to and from the Configuration Database.

Configuration Layer Architecture

Figure 2 shows the structure of the Configuration Layer.

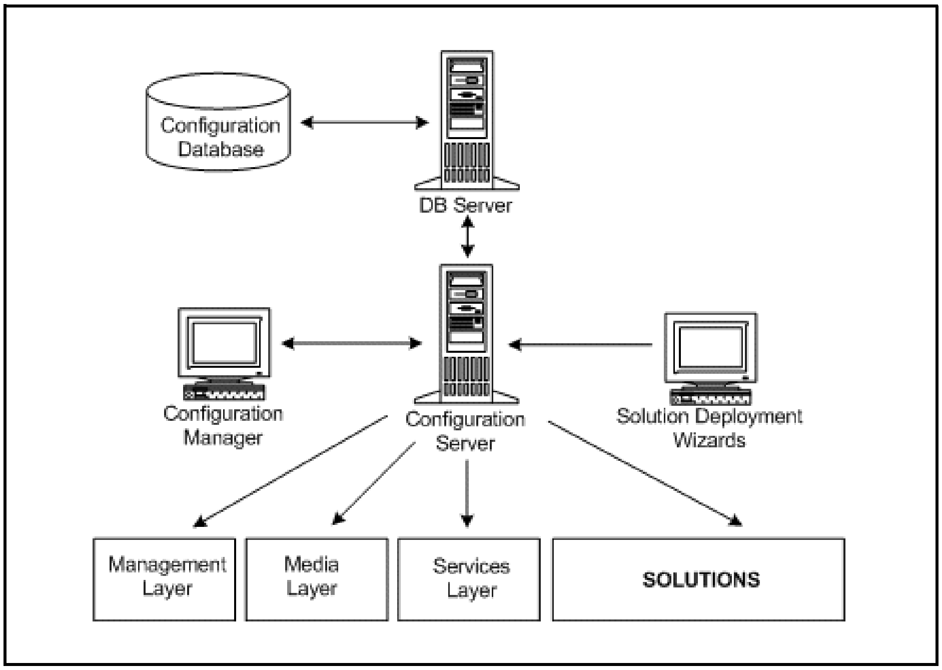


Figure 2: The Configuration Layer Architecture

- 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. See "Architecture" on page 190 for details.)

- Configuration Manager 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. DB Server—a Services Layer component—is the access point to the 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.

- Solution Deployment Wizards automate deployment and upgrade. These wizards also handle solution-specific data integrity.
- Deployment Manager (not shown in the diagram) provides a user-friendly interface for deploying certain Framework components to both local and unattended remote hosts.
- Configuration Conversion Wizard (not shown in the diagram) provides a user-friendly interface for migrating Genesys configuration data to the 7.6 data format.
- Configuration Import Wizard (not shown in the diagram) makes it easier to integrate data from external data sources into the Genesys Configuration Database. It provides a user-friendly interface to automatically import agent data from Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory databases and switch configuration data from various switches. The Wizard capabilities also include import and export of configuration data to and from Extensible Markup Language (XML) files, generation of custom reports from the Configuration Database, and comparison of two configuration sets (including import of configuration differences).

Management Layer

Management Layer Functions

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 Solution Control Interface 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 nonredundant 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 function and for alarm signaling function.
- Individual host monitoring, including CPU and memory usage records and information about running processes and services.
- Support for geographically distributed environments.

Management Layer Architecture

Figure 3 on page 36 shows the structure of the Management Layer.

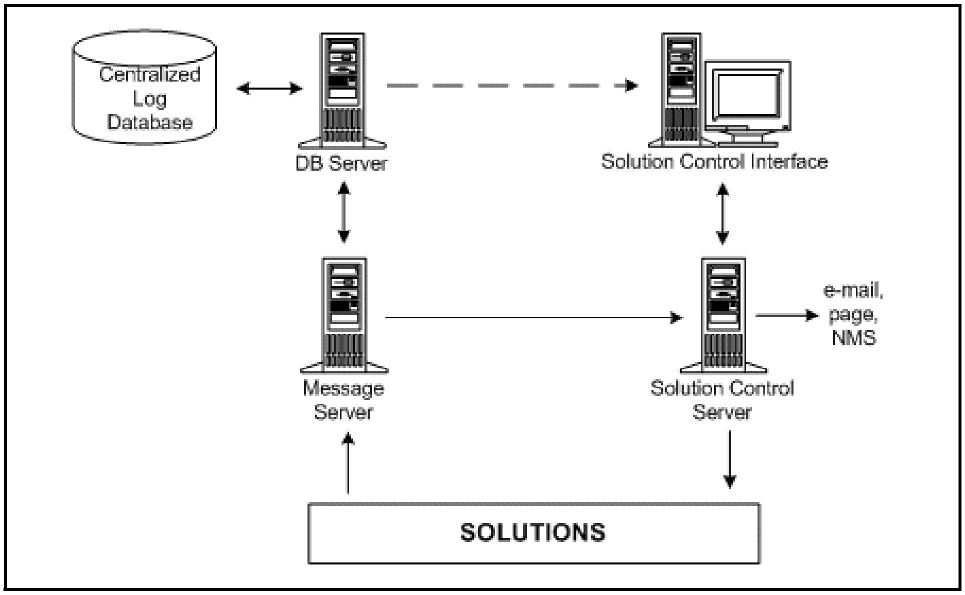


Figure 3: Management Layer Architecture

- 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.
- 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. SCS also processes alarms as specified by the user.
- Solution Control Interface 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 also allows 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. DB Server—a Services Layer component—serves as an access point to the Centralized Log Database.
- Genesys SNMP Master Agent (an optional component not shown in the diagram) provides an interface between the Management Layer and an SNMP-compliant NMS.

Media Layer

Media Layer Functions

The Media Layer provides:

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

Media Layer Architecture

Figure 4 shows the structure of the Media Layer.

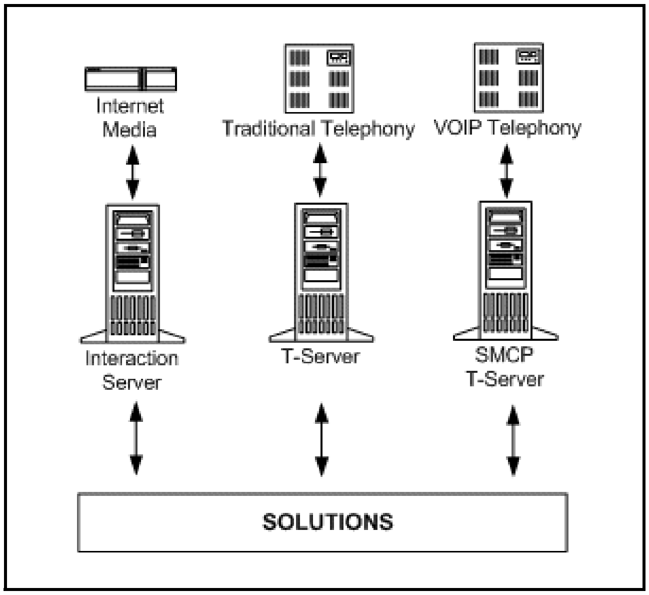


Figure 4: Media Layer Architecture

- T-Server provides an interface with traditional telephony systems.
- Interaction Server provides an interface with Internet media like e-mail and web communications.
- SMCP (Simple Media Control Protocol) T-Server provides 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. Mediating between T-Servers and T-Server clients, LDS enables an *N*+1 architecture, where *N* is the number of clients that handle the load, in situations where the total traffic of a large installation exceeds the capacity of a single client.

Services Layer

Services Layer Overview

The Services Layer provides:

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

Services Layer Architecture

Figure 5 shows the structure of the Services Layer.

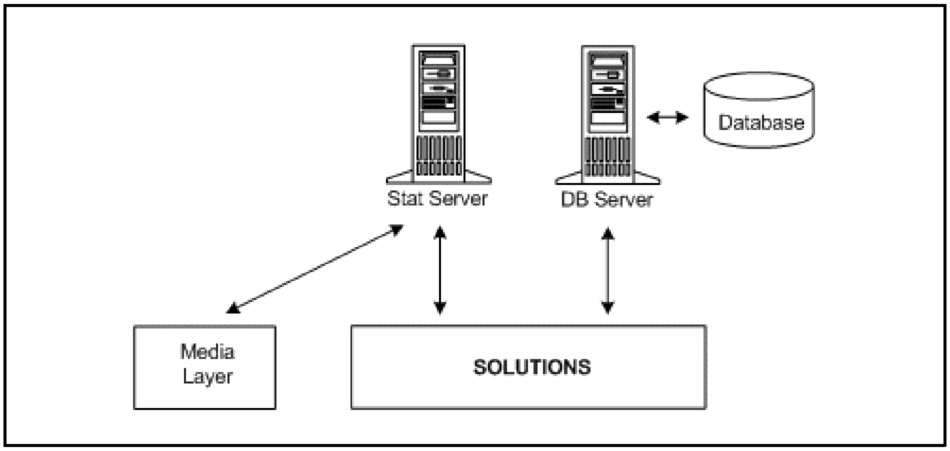


Figure 5: Services Layer Architecture

- 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.
- DB Server provides the interface between Genesys applications and the DBMS holding the operational databases for solutions.

Framework Connections

Figure 6 shows connections that Framework components establish to each other and to solutions.

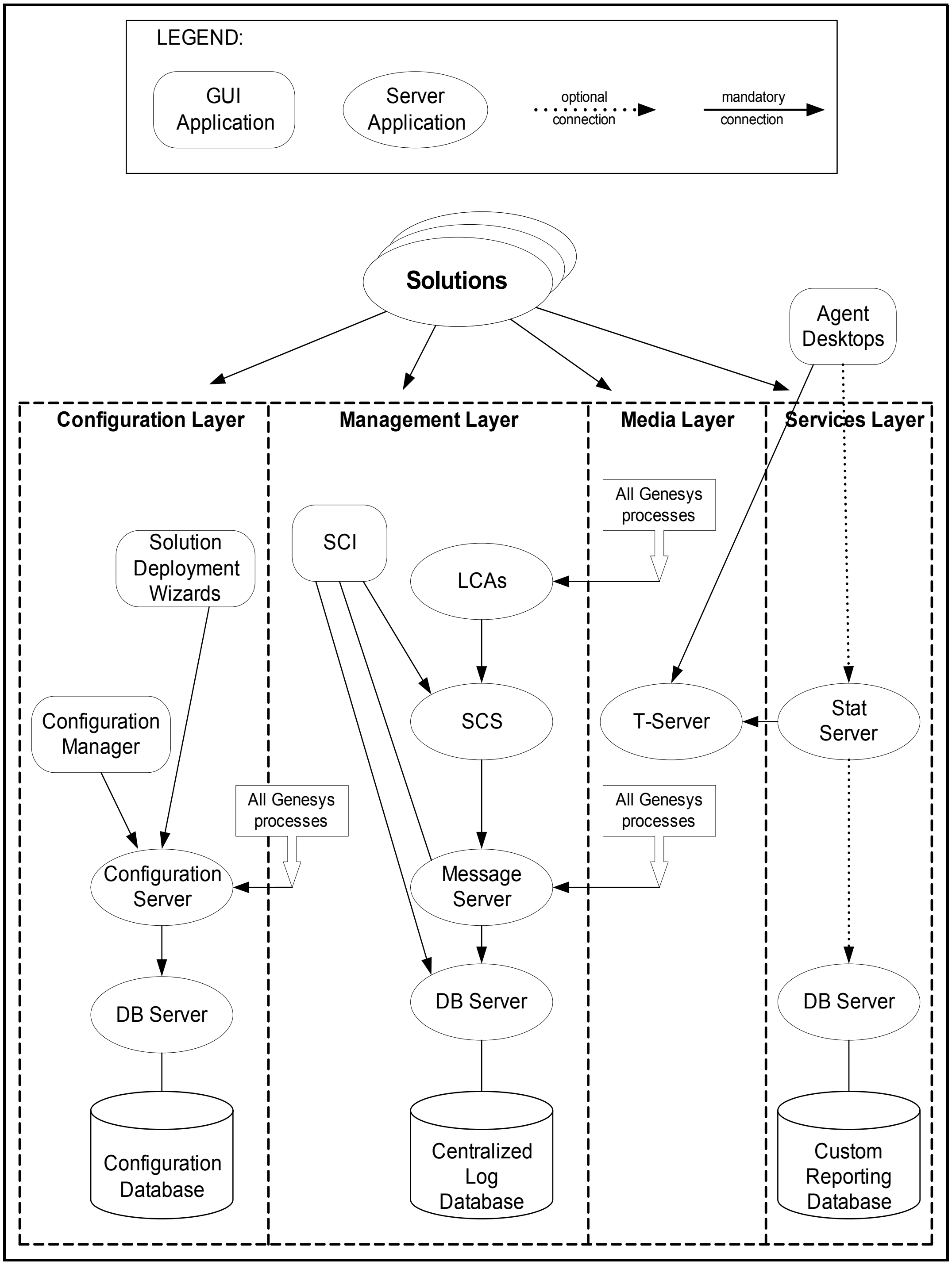


Figure 6: Detailed Framework Architecture

Chapter

3 Planning the Installation

This chapter describes the main tasks that you should complete, and the considerations you should take, when planning your Framework installation.

This chapter contains the following sections:

Initial Considerations

Major Planning Steps

Achieving optimal performance with your Genesys installation requires comprehensive planning. How well Genesys Framework 7.6 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 document describes various characteristics of Framework 7.6 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” on page 45.

Consider whether you can benefit from:

- Using the Management Layer (see “Management Layer” on page 49).

- Having redundant configurations (see “Application Failures” on page 60).
- Installing an additional Configuration Server in Proxy mode (see “Solution Availability” on page 56).
- Installing a number of Solution Control Servers in Distributed mode (see “Solution Availability” on page 56).
- Using Load Distribution Server (refer to LDS documentation for information).

In addition, review “Solution Availability” on page 56 and “Security Considerations” on page 61, which are common aspects of any Genesys installation.

Finally, prepare an installation worksheet based on the sample given in Appendix G, “Installation Worksheet,” on page 231.

Telephony Network Description

Certain information is required to deploy Framework 7.6, 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 via Configuration Manager.

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

1. Switch type, which usually corresponds to the switch vendor, brand name, and model number.
2. Version of the switch software.
3. Type of CTI Link (TCP/IP, X.25, or ISDN).
4. Version of the CTI Link software.
5. 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.
6. 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.
7. Login codes to be assigned to agents for runtime associations between agents and their working places.
8. Information about how the switch DNs are arranged into working places.
9. 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:

1. For every person who must access any interaction management application, define the following parameters: a unique employee ID, unique user name, and password. The role of a person in the contact center defines the set of access privileges for this person in the system. For more information, see “Security Considerations” on page 61.
2. For agents, define Login codes in every switch at which they might be working.
3. For agents, define skills that might be considered as criteria for effective interaction processing.
4. Note how agents are arranged into groups.
5. Decide how to arrange the working places into groups.

Licensing Your Applications

Genesys licenses its applications using the FLEXlm License Manager, produced by Macrovision. At startup, all licensed Genesys servers establish a client connection to License Manager, providing a computer host ID or IP address along with various information about the application. If the application has a valid license, License Manager allows the application to start and run properly. Note that the Management Layer can control and monitor License Manager as a third-party application but not as a Genesys server application.

To find more information about how Framework and other Genesys components are licensed, refer to the *Genesys 7 Licensing Guide*.

Configuration Environment Types

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.

Two types of the Genesys configuration environment address the difference in the needs of these two types of companies:

- *Enterprise* (also referred to as *single-tenant*) *configuration environment* serves the needs of a single company that owns its telephony equipment and uses it for its own needs. In an enterprise configuration environment, all configuration information is visible to all users—employees of the company—given that they have sufficient permissions.
- *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.

You establish a particular configuration environment when you create the Configuration Database structure during the Configuration Layer installation.

For more information about the two configuration environments and resulting differences in configuration objects, refer to *Framework 7.6 Configuration Manager Help.*

Large Configuration Environments

A single instance of Configuration Server can support over 500,000 objects with a start-up time of less than 5 minutes. This configuration would require at least 1 GB of RAM for storage.

Genesys defines a *large configuration environment* as the one where 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 Configuration Manager 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 Configuration Manager and perform only those tasks they are required to perform over the configuration objects for which they have permissions. This saves Configuration Manager from loading all the objects from the Configuration Database.
- Consider using Configuration Unit and 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 Configuration Manager 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 Person configuration objects as you create the logins. When the Configuration Database contains too many unassigned agent logins, Configuration Manager takes a long time to open the `Agent Login` browse dialog box from the `Person Properties` dialog box. To guarantee an acceptable loading speed, keep the number of unassigned agent login objects below 1000 per Tenant object.

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 7.6.

Configuration Layer

The Configuration Layer is a mandatory part of any Genesys CTI installation. You cannot configure and run any other layers of Framework 7.6—or any solutions—unless Configuration Layer components are running.

Configuration Database

The Configuration Database stores all configuration data.

Warnings! Never add, delete, or modify any data in the Configuration Database except through applications developed or those instrumented with Genesys Configuration Server API. If you have compelling reasons for accessing the database directly, consult Genesys Technical Support 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.

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.

- 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

DB Server

DB Server provides the interface between Configuration Server and the DBMS holding the Configuration Database.

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

- The Configuration Layer requires a dedicated DB Server that should not be used for any other purposes. This DB Server has a special installation and startup procedure. Refer to the DB Server sections of Chapter 5 on page 81 and Chapter 8 on page 139 for more information about installing and starting the Configuration DB Server.
- Locate DB Server on the machine where the DBMS client runs.
- Install DB Server on a multiprocessor computer to optimize its performance. As the DBMS itself, DB Server can spawn child processes that benefit from multiprocessor capabilities.

- Provide sufficient RAM to run DB Server processes. To ensure adequate performance, do not run DB Server processes in Swap mode.

Configuration Server

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

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

- Genesys solutions installed in a particular environment can have only one Configuration Database managed though one Configuration Server at a time.
- Because Configuration Server keeps *all* configuration data in its memory, allocate memory for this server based on the expected size of the Configuration Database.
- Although you can install Configuration Server anywhere on the network because it does not generate heavy traffic, the most logical location for it is on the computer running DB Server.
- When you install Configuration Server on a UNIX host computer, increase the swap area of the host to at least 600 MB to accommodate a large Configuration Database.

Configuration Server Proxy

To support geographically distributed installations, Configuration Server can operate in Proxy mode. In this document, a Configuration Server 7.6 that operates in Proxy mode, and that provides similar functionality to Configuration Server Proxy 6.x and 7.x, is called *Configuration Server Proxy 7.6.* For more information about Configuration Server Proxy, see “Solution Availability” on page 56.

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

- Genesys solutions installed in a particular environment can have only one Configuration Database managed though one Configuration Server at a time.
- Configuration Server Proxy 7.6 keeps all configuration data in its memory which improves data processing performance. Proxy 7.6 consumes approximately the same amount of RAM as Configuration Server Proxy 6.x and 7.x, and Configuration Server 7.6.
- You can install Configuration Server Proxy anywhere on the network because it does not generate heavy traffic.

- When you install Configuration Server Proxy on a UNIX host computer, increase the swap area of the host to at least 600 MB to accommodate a large Configuration Database.

Configuration Manager

Configuration Manager 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.

When planning your installation, follow this recommendation for Configuration Manager:

- Install and run as many instances of Configuration Manager on the network as needed.

Note: You can launch multiple instances of Configuration Manager on the same computer and connect them to different Configuration Servers or to the same Configuration Server. You can also open as many object `Property` dialog boxes as you need from a single instance of Configuration Manager.

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 where Genesys components are installed. For more information, refer to the *Genesys 7.6 Security Deployment Guide.*

Configuration Import Wizard

Use the Configuration Import Wizard (CIW), an optional component of the Configuration Layer, to import the following data into the Genesys Configuration Database:

- Agent data from Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory databases.
- Switch configuration data from various switches.

You can also use CIW to import and export configuration data to and from Extensible Markup Language (XML) files, generate custom reports from the Configuration Database, and compare two configuration sets (including import of the configuration differences). For more information about CIW, refer to the *Framework 7.6 Imported Configuration Data Formats Reference Manual.*

When working with CIW, Genesys recommends that you allow up to 1 GB memory for import and export operations to and from a large Configuration Database.

Management Layer

The exact configuration of the Management Layer depends on which of the following management functions you would like to use:

- Solution and application control and monitoring
- Centralized logging
- Alarm signaling
- Application failure management

Genesys recommends that you use all these capabilities to optimize solution management.

Management Layer Capabilities—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 in this section.

Solution and Application Control and Monitoring

Install these components to control and monitor solutions and applications:

- Local Control Agent
- Solution Control Server
- Solution Control Interface

Refer to the *Framework 7.6 Management Layer User's Guide* for descriptions of and recommendations for these components.

Centralized Logging

Install these components to use centralized logging:

- Centralized Log Database
- DB Server (as a client of Configuration Server)
- Message Server
- Solution Control Interface (optional)

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

Refer to the *Framework 7.6 Management Layer User's Guide* for descriptions of and recommendations for these components.

Alarm Signaling

Install these components to provide alarm signaling:

- Message Server.
- Solution Control Server.
- Solution Control Interface.
- Genesys SNMP Master Agent, if SNMP alarm signaling is required. See also "Built-in SNMP Support" on page 50.

Note: You do not need to install the Genesys application called G-Proxy to provide the alarm-signaling functions of the Management Layer.

Refer to the *Framework 7.6 Management Layer User's Guide* for descriptions of and recommendations for these components.

Application Failure Management

Install these components to detect and correct application failures:

- Local Control Agent
- Solution Control Server
- Solution Control Interface

Refer to the *Framework 7.6 Management Layer User's Guide* for descriptions of and recommendations for these components.

See the section "Application Failures" on page 60 and for information about the application-failure management mechanism.

Built-in SNMP Support

Install the following components to integrate Genesys Framework 7.6 with an SNMP-compliant third-party NMS (network management system):

- 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.

Refer to the *Framework 7.6 Management Layer User's Guide* for descriptions of and recommendations for these components.

Management Layer Components

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

Local Control Agent

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

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

> **Note:** 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” on page 111 for instructions.

- On UNIX platforms, LCA must be added to the `r/c` files during the installation, so that LCA can start automatically on computer startup. In practice, this means that the person installing LCA must have sufficient permissions.

Message Server

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

- Genesys recommends the use of one Message Server and of one Log Database for all but large installations. If you are working within a large installation and think about 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 to more than one Log Database.
    - Because any number of Message Servers can send log records to Solution Control Server, Solution Control Interface can display alarms based on log records from a few Message Servers.

- If you want an application to generate alarms, you must configure it to send log events to Message Server. Use the same Message Server for both the centralized logging and alarm signaling.
- If you want Message Server to provide alarms, you must connect it to Solution Control Server. This means that you must configure a connection to every Message Server in the SCS `Application` object's `Properties` dialog box.
- As with any other daemon application, you can deploy redundant Message Servers.
- To optimize the performance of the connection with DB Server, configure the number of messages that the Message Server sends to DB Server before receiving a response. The smaller the number of messages, the greater the decrease in performance. See the "Message Server" section of the *Framework 7.6 Configuration Options Reference Manual* for more information.

Solution Control Server

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

- Given that you can install and use more than one SCS that is operating in `Distributed` mode within a given configuration environment, consider deploying a few SCSs in this mode for large or geographically distributed installations. In such installations, each such server controls its own subset of the Host, Application, and Solution objects. Distributed SCSs communicate with each other through the dedicated Message Server.
- As with any other daemon application, you can deploy redundant SCSs. Redundancy support for SCS is implemented through direct communication between the backup SCS and the LCA of the host where the primary SCS runs. To set up HA port synchronization between Primary and Backup Solution Control Servers, see "Setting Up HA Port Synchronization" on page 182.

Note: You cannot perform a manual switchover for Solution Control Server.

Solution Control Interface

When planning your installation, follow these recommendations for SCI:

- Install and run as many instances of SCI on the network as needed.

Note: Launch only one instance of SCI per host computer.

- Keep in mind that although you can configure SCI to work with more than one Solution Control Server and more than one Log Database, SCI can only work with one SCS and one Log Database at a time.
- Use SCI for advanced viewing and handling of the log.
- Use SCI to view active alarms and define what solutions the alarms might affect.

DB Server for Log Server

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

- Locate DB Server on the machine where the DBMS client runs.
- Install DB Server on a multiprocessor computer to optimize its performance. As with the DBMS itself, DB Server can spawn child processes that benefit from multiprocessor capabilities.

Centralized Log Database

As with any historical database, the size of the Centralized Log Database grows with time. So, 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. Table 1 on page 54 provides general timing recommendations.

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 Server(s) 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.

Table 1: Recommended Log Storage Time

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

SNMP Master Agent

When planning your installation, follow these recommendations for SNMP Master Agent:

- Use SNMP Master Agent only if both of these conditions apply:
  - You want to access the Management Layer functions via an NMS interface.
  - You don’t have another AgentX-compatible SNMP master agent in place.

Media Layer

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

T-Server

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

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

- At the premise level, always associate one switch with one T-Server.
- Allocate memory for T-Server based on the number of interactions you expect to be simultaneously processed at a given site during the busiest hour and the typical amount of business data attached to the interactions. Allocate at least 500 bytes per interaction plus memory space for a “typical” amount of attached data.
- Provide sufficient RAM to run T-Server processes. To ensure adequate performance, do not run T-Server processes in Swap mode.
- Do not install real-time third-party applications on the machine 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 machine 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

Although the Services Layer components are considered elements of Framework 7.6, it is logical to install them when you install the solution that they will serve. When deploying these, consider the following recommendations.

DB Server

DB Server provides the interface between Genesys applications and the DBMS holding the operational databases for solutions.

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

- Do *not* use the DB Server that provides access to the Configuration Layer to access any databases other than the Configuration Database. (See “DB Server” on page 46.)
- Consider dividing database-related traffic evenly among any number of DB Servers, each serving up to 255 clients.
- Locate DB Servers on the machine where the DBMS client runs.
- Install DB Server on a multiprocessor computer, to optimize its performance. As the DBMS itself, DB Server can spawn child processes that benefit from multiprocessor capabilities.
- Provide sufficient RAM to run DB Server processes. To ensure adequate performance, do not run DB Server processes in Swap mode.

Stat Server

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.

Solution Availability

This section describes the events that affect the availability of Genesys solutions.

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. Since 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 6.x and 7.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.

Genesys Framework 7.6 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” on page 61.

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.

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 solutions, 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.

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 *Framework 7.6 Configuration Manager Help.*

For complete instructions on configuring ADDP between two applications, refer to Appendix A on page 205. 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.

Note: Beginning with release 7.5, backwards compatibility of the Keep-Alive Protocol (KPL) is no longer supported. If you used KPL for 6.5 clients in previous versions of Genesys, consider using ADDP instead.

Configuration History Log

The Configuration History Log is a database 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.

The History Log is installed with default parameters when you install Configuration Server. For Configuration Server in any mode (primary, backup, or Proxy), configure the History Log parameters on the `Options` tab of the Configuration Server `Application` object in Configuration Manager. Refer to the *Framework 7.6 Configuration Options Reference Manual* for detailed descriptions of the configuration options that relate to the History Log.

At startup, Configuration Server checks whether there is a pre-existing History Log database with the same name as that defined in the configuration file. If it does not find a match, it creates a new one. If it does find a match, Configuration Server backs up that file, appending the `.bak` file extension. When requested by a client that is recovering from a service interruption, Configuration Server does the following:

- Restores the client's session according to a client session record.
- Returns a set of data records to the client that exceeds the client's last known data record identifier.

No maintenance is required for the History Log database, because it is maintained automatically by Configuration Server. Based on the expiration parameters, Configuration Server purges information from the database, both at startup and during normal operations.

Errors that occur when writing to the History Log database generate Log Event 22138. If persistent or fatal errors occur as a result of a corrupt History Log database, remove the corrupt file and, optionally, replace it with the backup file created during Configuration Server startup. Then, restart Configuration Server.

Note: Genesys strongly recommends that you associate an alarm with this Log Event, and that you inform Genesys Technical Support if you encounter any errors or corruption.

History Log functionality is mandatory, and cannot be turned off permanently. However, large updates can affect the performance of Configuration Server. If necessary, you can temporarily turn off the History Log functionality by setting the `active` option to `false` for the Configuration Server `Application` object in Configuration Manager. The functionality will be turned back on either when you manually reset the option (to `true`), or when you restart Configuration Server. Refer to the *Framework 7.6 Configuration Options Reference Manual* for more information about this configuration option.

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.

Starting in release 7.6, there is another way that you can reduce the impact of large updates on system performance. Default History Log operation ensures the integrity of the internal history database if both Configuration Server and the operating system fail. However, this is CPU-intensive. Instead, you can limit the scope of this protection to failure of Configuration Server only by setting the `failsafe-store-processing` option to `false`. If the operating system fails, the history database may not be wholly preserved. However, this operation has less impact on system performance. Refer to the *Framework 7.6 Configuration Options Reference Manual* for more information about this configuration option.

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 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.

Since 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 release 7.6, the Management Layer is this mechanism.

For information about the architecture and components in the Management Layer, see the *Framework 7.6 Management Layer User's Guide.*

Common Log Options

Starting with release 7.0, 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" chapter of the *Framework 7.6 Configuration Options Reference Manual*.

Security Considerations

This section describes the Configuration Layer capabilities that help keep your configuration data secure.

Genesys Security Using the TLS Protocol

Starting with release 7.5, Genesys supports an 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 7.6 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 on the `Server Info` tab 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 7.6 Security Deployment Guide* and *Framework 7.6 Configuration Manager Help* for more information about multiple ports.

Multiple Ports on Configuration Server

When you install Configuration Server, the 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 (on the `Server Info` tab), 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` on page 145 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 Configuration Manager 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 7.6 Security Deployment Guide* for detailed instructions on configuring secure connections.

Data Access

Secure access to the resources of an interaction management system plays an important role in ensuring trouble-free operation of all system parts and functions. Changes made by unqualified users can adversely affect system availability and the quality of service.

Use the following Genesys Framework capabilities to help secure your resources:

- Password encryption for access to the Configuration Database.
- Access-control settings on a per-user basis with regard to a solution's functions and data.

But you must also take other security measures that protect general network access, access to the file systems and databases, and data transmitted over the public network. The access-control capabilities of the operating and database management systems and the use of secure network communication protocols affect these measures.

Note: For more information about how to perform password encryption, refer to "Encrypting the Configuration Database Password" on page 95.

The data a Genesys solution requires for operating in a particular environment, as well as the applications and the solutions, are described in the form of Configuration Database objects. Any person who needs access to this data or these applications must have an account in this database. The security mechanism implemented in Configuration Server allows the system administrator to define separately a level of access for any account with respect to any object. The level of access to each object is defined by the combination of elementary permissions shown in Table 2.

Table 2: Elementary Access Permissions

Permission	Description
Read	Permission to read information and receive updates about the object.
Create	Permission to create objects under the folder.
Change	Permission to change the properties of the object.
Execute	Permission to perform a predefined action or set of actions with respect to the object.
Delete	Permission to delete the object.

Table 2: Elementary Access Permissions (Continued)

Permission	Description
Read Permissions	Permission to read the access control settings for the object.
Change Permissions	Permission to change the access control settings for the object.
Read & Execute	• Permission to read information and receive updates about this object. • Permission to perform a predefined action or set of actions with respect to this object.
Propagate	For “container” objects (such as Tenants, Folders, Switches, IVRs, and Enumerators). The Propagate check box controls whether to propagate this set of elementary permissions to the child objects (by default, the check box is selected).

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 Person with the specified `User Name` and `Password` is registered in the Configuration Database. Otherwise, the working session is stopped. The access privileges of valid user accounts define what the user can and cannot do within this application. Permission `Execute` is used to control access to applications, solutions, and other configuration objects. Without such permission, the user cannot work with a given application or execute control over a given object. Combinations of the `Read`, `Create`, `Change`, and `Delete` permissions define the level of access to configuration data. For example, users may have access to a real-time reporting solution but will only get reports about objects they have permission to read.

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 on. Daemon applications do not have an explicit logon procedure. Instead, their access permissions are determined by the permissions of the account with which they are associated: a personal account or the SYSTEM account. Any personal account registered as a Person object in the Configuration Database can be used as an account for any daemon application. By default, every daemon application is associated with a special account called SYSTEM that has `Read` and `Execute` permissions with respect to all objects in the Configuration Database except Access Groups.

Access Groups and Default Security Settings

Access Groups are groups of Persons who need to have the same set of permissions with respect to Configuration Database objects. By adding individuals to Access Groups—and then setting permissions for those groups—access control is greatly simplified. You cannot delete or rename Default Access Groups although you can change their default privileges.

Genesys offers these preconfigured Default Access Groups:

- `Users:` Members have `Read` and `Execute` permissions with respect to all objects except Access Groups. For releases 7.5 and earlier, every agent added to the Configuration Database became a member of this group by default.
- `Administrators:` Members have a full set of permissions with respect to all objects except the Super Administrators Access Group. For releases 7.5 and earlier, every non-agent added to the Configuration Database became a member of this group by default.
- `Super Administrators:` Members have a full set of permissions with respect to every object in the Configuration Database. No person is added to this group by default.

In addition, in a multi-tenant configuration, Configuration Server creates these Default Access Groups for each new Tenant object:

- `Users:` Members have `Read` and `Execute` permissions with respect to all objects under this Tenant except Access Groups. For releases 7.5 and earlier, every agent added to the Tenant configuration became a member of this group by default
- `Administrators:` Members have a full set of permissions with respect to all objects under this Tenant. For releases 7.5 and earlier, every nonagent added to the Tenant configuration became a member of this group by default.

New Users

Starting with release 7.6, 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 *Framework 7.6 Configuration Manager 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. 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 chapter "No Default Access for New Users" in the *Genesys 7.6 Security Deployment Guide.*

Master Account and Super Administrators

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.

Note: In addition to emergency situations, you still must use the Master Account for some specific administrative tasks, especially during migration. Refer to the description of the specific tasks throughout this and other documents, including the *Genesys Migration Guide*, to determine whether you need to use the Master Account, or whether you can use another account that has the required permissions.

During one of the first working sessions, create nonagent accounts for everyone who needs full access to all objects, then move these accounts from the `Administrators` to the `Super Administrators` group. By default, every member of the `Super Administrators` group has the same permissions as the Master Account.

EVERYONE Group

Think of the EVERYONE group as an Access Group that includes every Person registered in the Configuration Database. You cannot delete or modify this group, which, by default, has `Read` and `Execute` permissions set for the configuration objects listed in Table 3. Therefore, everyone registered as a Person object can read information about these objects and start any application.

Table 3: Configuration Objects for Which EVERYONE Grants Read and Execute Permissions (By Default)

Single Tenant Environment	Multi-Tenant Environment
Environment: • Alarm Conditions • Application Templates • Applications • Hosts • Switching Offices Resources: • Time Zones	Environment: • Alarm Conditions • Application Templates • Applications • Hosts • Formats • Fields • Time Zones

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. Do this by either changing the permissions of the Default Access Groups or creating role-specific Access Groups and moving the individual accounts from the Default Access Groups to those role-specific groups.

A Person belonging to more than one Access Group has all the permissions that any of those Access Groups have. For example, if Access Group A has `Read` and `Change` permissions, and Access Group B has `Read & Execute` permission, a Person belonging to both groups has `Read, Change,` and `Execute` permissions.

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.

Changing Permissions Recursively and Using the Propagate Flag

The Configuration Layer offers some advanced capabilities that help you better organize permission management. Selecting the `Replace permissions recursively` check box in Configuration Manager for so-called *container* objects (such as Tenants, Folders, Switches, IVRs, and Enumerators) effectively removes all individual permission settings configured for the child objects and imposes permission settings configured for the parent object to its child objects.

In addition, selecting the `Propagate permission` flag (for release 7.0 and later) for container objects allows you to handle permissions in a flexible way. That is, to add a new account to the list of accounts that have access to a container object and all related child objects without affecting the existing permission settings, you have to add access for this account to this container object with the `Propagate` check box selected (the default setting). This effectively propagates the added account to all child objects in addition to adding the account to the parent object's access permissions. To the contrary, to add an account exclusively for a specific container object, clear the `Propagate` check box before changing the object's access permissions.

Forced Re-Login for Inactivity

Starting in release 7.6, you can configure Configuration Manager and Solution Control Interface 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. 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 which are to use the feature. Refer to the *Genesys 7.6 Security Deployment Guide* for a detailed description of this feature, and for detailed instructions about implementing it for your applications.

Login Security Banner

Starting in release 7.6, you can create your own security banner to be displayed to a user logging in to Configuration Manager, Solution Control Interface, or any Framework Wizard. You define the content of the banner, such as the terms of use of the application. Users must accept the contents of the window to proceed, or they can reject the contents 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 7.6 Security Deployment Guide* for more details about the security banner.

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.

Chapter

4 Deployment Overview

This chapter lists the prerequisites for installing the Genesys Framework, and prescribes the deployment order. This chapter also describes the Genesys Installation Wizard and the Genesys Configuration Wizards, and how to access them.

This chapter contains the following sections:

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 Chapter 3 on page 41 for recommendations on these issues. Ensure that applications that require licenses are licensed properly (see the *Genesys 7 Licensing Guide*).

Review the prerequisites for your Framework installation as described in this section.

Databases

Genesys recommends that you or your database administrator create database(s) in your database management system (DBMS) before you start Genesys installation. For the Framework installation, 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 database(s) on a regular basis.

Refer to "Network Locations for Framework Components" on page 45 for recommendations on database sizing. Refer to your DBMS documentation for instructions on how to create a new database. Refer to Appendix G on page 231 for the list of database parameters you must use in Genesys installation.

Note: Consider using the Genesys Database Initialization Wizard when creating database structures for the Configuration Database and Centralized Log Database during the Framework 7.6 deployment process.

Hardware and Network Environment

Genesys recommends that you or your IT specialist assign host computers to Genesys software before you start Genesys installation. Keep in mind the following restrictions:

- Do not install all the Genesys server applications on the same host computer.
- When installing a few server applications on the same host computer, prevent them (except for Configuration Server and Configuration Server Proxy) from using the swap area.

Refer to "Network Locations for Framework Components" on page 45 for recommendations on server locations.

Refer to the *Genesys 7 Supported Operating Systems and Databases* white paper for the list of operating systems and database systems supported in Genesys releases 7.x. This document is located on the Technical Support website at:

`http://genesyslab.com/support/dl/retrieve/default.asp?item=B6C52FB62DB42BB229B02755A3D92054&view=item`.

Refer to the *Genesys 7 Supported Media Interfaces* white paper for the list of supported switch and PBX versions. This document is located on the Technical Support website at:

`http://genesyslab.com/support/dl/retrieve/default.asp?item=A9CB309AF4DEB8127C5640A3C32445A7&view=item`.

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 installation `read_me.html` files for the Genesys applications that operate on UNIX.

Internet Browsers

To view all elements of the Configuration Manager interface, you must have Internet Explorer version 6.0 or later.

Licensing

Before configuring and installing Framework components, note that Genesys applications require licenses. Genesys recommends that you configure and install License Manager and license files at this point. For information about which products require what types of licenses and on the installation procedure for License Manager, refer to the *Genesys 7 Licensing Guide* document available on the Genesys Documentation Library CD.

If you are planning to deploy redundant configurations for any Genesys servers, you must have a special high-availability (HA) license. Otherwise, the Management Layer does not perform a switchover between the primary and backup servers.

Deployment Sequence

The various Framework components are distributed on a number of product CDs. This document covers the deployment of Framework components shipped on the following CDs:

- Management Framework
- 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.

1. Configuration Layer:
    - DB Server (providing access to the Configuration Database)
    - Configuration Database
    - Configuration Server
    - Configuration Manager
    - Configuration Server Proxy (optional)
    - Wizard Manager (optional; no configuration is required)
    - Database Initialization Wizard (optional; no configuration is required)
    - Configuration Import Wizard (optional; no configuration is required)

2. Management Layer:
   - DB Server (as a client of Configuration Server, providing access to the Centralized Log Database and other databases)
   - Message Server
   - Centralized Log Database
   - Local Control Agent (required for each computer running Genesys server applications or monitored third-party server applications)
   - Solution Control Server (SCS)
   - Solution Control Interface (SCI)
   - Genesys SNMP (Simple Network Management Protocol) required to support Microsoft Operational Manager (MOM) technology and optional to support Master Agent or a third-party AgentX protocol-compliant SNMP master agent
3. Media Layer:
   - T-Server
   - HA Proxy for a specific type of T-Server (if applicable)

Note: Configuration and installation instructions for T-Server 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 *Framework T-Server Deployment Guide* for your specific T-Server.

4. Services Layer
   - DB Server
   - Stat Server

Use the sample worksheet in Appendix G, "Installation Worksheet" on page 231 as you prepare for and perform the Framework installation.

Note: Although Interaction Server, SMCP (Simple Media Control Protocol) T-Server, and Services Layer 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.

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

- Hosts
- Switching Offices
- Switches
- Agent Logins
- DNs

- Access Groups
- Skills
- Persons
- Agent Groups
- Places
- Place Groups

Note: You will find detailed information about configuring telephony objects in the latest version of the *Framework T-Server Deployment Guide* for your specific server.

The configuration and installation procedures depend on whether you employ Wizard Manager for configuration. Whichever method you choose, you must first install and configure components of the Configuration Layer, as described in Chapter 5 on page 81.

You can choose the manual installation procedure or use the Management Framework Deployment Manager to install Configuration and Management Layer components. (See Appendix F on page 225 for details.)

Warning! Never add, delete, or modify any data in the Configuration Database except through applications developed by Genesys or those instrumented with Genesys Configuration Server API. If you have compelling reasons for accessing the database directly, consult Genesys Technical Support before you do so.

Genesys Wizards

You can deploy Genesys Framework in one of two ways, but both use Genesys wizards. You can manually install Framework with help from the Genesys Installation Wizard, or you can use the Genesys Configuration Wizards to help you install it.

This section describes the Genesys Installation Wizard and the Genesys Configuration Wizards, and how to access them.

Genesys Installation Wizard

The Genesys Installation Wizard is the standard interface for manually installing all 7.6 components on Windows platforms, with the exception of Genesys Configuration Wizards. When you install a component from the appropriate `setup.exe` file, the Installation Wizard is automatically invoked to guide you through the process.

Warning! If you are using Genesys Configuration Wizards to deploy a component, do not use the Genesys Installation Wizard.

Genesys Installation Wizard uses a standard design for installation pages and provides a consistent look across all installations for Genesys products.

Names of all components start with the word *Genesys* in both `Add or Remove Programs` and Windows `Services` windows; also, the Genesys logo appears next to components names in these windows. In the Windows `Registry`, Services names are nicknames.

Uninstalling Genesys Components

There are no uninstall shortcuts in the `Start > Programs` menu; instead, uninstall components from the standard Windows `Add or Remove Programs` window.

Genesys Configuration Wizards

Genesys product CDs that contain installation packages for a set of Genesys 7.6 components also contain Configuration Wizards that facilitate component deployment. Genesys Configuration Wizards help users set up Genesys products, including the configuration of solutions, applications, and options required to provide desired functionality.

Note: Configuration Wizards for HA Proxy components are combined with wizards for appropriate T-Servers and delivered on the Media CD.

From a security standpoint, Configuration Server treats Configuration Wizards as regular graphical user interface (GUI) applications. When Configuration Wizards are invoked from a GUI application, the account that you used to log in to that application controls your actions in the wizards. Since the wizards are designed to change configuration, rather than to review existing configuration, you must have modification-level permissions (create, change, delete) with respect to the configuration objects that need to be created or configured through the wizards.

Wizard Manager

The primary application that invokes Configuration Wizards for Genesys Framework 7.6 and Genesys solutions is Wizard Manager. This application is designed solely for deployment and upgrade tasks. Wizard Manager launches Configuration Wizards in the order required for the requested task. Some Genesys GUI applications can also invoke wizards designed to facilitate elementary configuration tasks. For example, the wizards invoked from Solution Control Interface (SCI) allow a user to define a new alarm condition or modify the logging process of a specific application. All applications from which you can launch Configuration Wizards are clients of Configuration Server. Therefore, the computers on which such applications are installed must have network connectivity with the computer on which Configuration Server runs.

Wizard Manager does not operate on UNIX, only on Windows. However, you must use this tool to configure the Framework components, regardless of whether the components are run on UNIX or Windows.

To install all the wizards that are on a particular CD, run the `setup.exe` program located in the root directory of the CD. This also installs the Wizard Manager. Only one instance of Wizard Manager is installed on your computer, even though you install wizards from multiple applications. You can access all installed Configuration Wizards from this single instance of Wizard Manager.

To install Wizard Manager and the Management Framework Configuration Wizard, run `setup.exe` from the root directory of the Management Framework 7.6 CD. To install the Configuration Wizards for T-Server applications, run `setup.exe` from the root directory of the Media 7.6 CD. Wizards that you invoke from other Genesys graphical user interface (GUI) applications are installed during the installation of those applications.

Warning! When you install wizards on a given computer, close all Genesys GUI applications that run on it.

Configuration Wizard Tasks

Genesys Configuration Wizards do not physically install applications on computers, but they do accomplish two tasks:

1. Prepare the configuration data for the Genesys environment and store the prepared data in the Configuration Database.
2. Customize the installation package to the environment, so that the installation script does not ask for parameters you have already submitted during the configuration process. To achieve this, wizards record all required data into an INI file, which becomes a part of the customized installation. This data is then used during the actual setup process to correctly install the application on a desired computer.

   Warning! It is your responsibility to provide wizards with correct directories for installations. See “Specifying Directories for Installations” for recommendations.

Configuration Wizards configure both Windows and UNIX applications, and prepare installation packages for these operating systems. After a wizard creates a customized installation package, the user has to run setup manually on a computer designated for a particular application.

Specifying Directories for Installations

After you have entered all required data about an application, the wizard prompts you to insert the CD where the installation package can be found and to specify a location to which the wizard should copy the customized installation. Keep in mind that when you are specifying:

1. The CD drive where the product CD is inserted, type or select only the first letter of the CD drive as opposed to the full path to the product installation on the CD.
2. A destination location to copy the installation package for an application installation on another computer than the computer running the wizard, specify a disk location accessible from a remote computer.

Copying Installations to Remote Computers

Often an application should be installed on another computer than the computer running the wizard. If this is the case, specify a temporary folder on the wizard's host computer as the destination location and then copy the customized installation package from this folder to a temporary directory on the host computer for the application.

When the application's future host computer is a UNIX box, follow the recommendations in this section for copying the customized installation packages from the wizard's Windows computer to the target UNIX computer.

General Recommendations for UNIX

When copying to a UNIX box, note the following:

- Use a sharing application, such as `Samba,` to make disks on computers running UNIX visible from computers running Windows.
- Use an ftp server.

Using FTP Servers Running on UNIX

To use an FTP Server running on UNIX:

1. Using the command prompt, locate the folder on the Windows-based computer to which the wizard copied the customized installation package.
2. Run the ftp client on Windows.
   Type the `ftp` command, followed by the actual host name of the UNIX-based computer in the command prompt:
   ```
   ftp <server_host_name>
   ```
3. Define the `BIN` mode of transfer.
   Type the following command in the command prompt:
   ```
   bin
   ```
4. Define the folder on the remote UNIX-based computer to which the package is to be copied.
   Type the `cd` command followed by the actual folder name in the command prompt:
   ```
   cd <folder_name>
   ```

5. To avoid a request for transfer confirmation for each file in the package, turn off the Interactive mode.
   Type the following command in the command prompt:
   ```
   prompt
   ```
6. Transfer the files.
   Type the following command in the command prompt:
   ```
   mput *
   ```

After the customized installation package is transferred, manually run the setup. The instructions for installing Framework components begin on page 82.

Using FTP Servers Running on Windows

To use an FTP Server running on Windows:

1. Locate the folder on the UNIX-based computer to which the package is to be copied.
2. Run the ftp client on UNIX. Type the `ftp` command followed by the actual host name of the Windows-based computer in the command prompt:
   ```
   ftp <server_host_name>
   ```
3. Define BIN mode of transfer.
   Type the following command in the command prompt:
   ```
   bin
   ```
4. Define the folder on the remote Windows-based computer from which the package is to be copied.
   Type the `cd` command, followed by the actual folder name in the command prompt:
   ```
   cd <folder_name>
   ```
5. To avoid a request for transfer confirmation for each file in the package, turn off Interactive mode.
   Type the following command in the command prompt:
   ```
   prompt
   ```
6. Transfer the files.
   Type the following command in the command prompt:
   ```
   mget *
   ```

After the customized installation package is transferred, manually run the setup. The instructions for installing Framework components begin on page 82.

Application State Disabled

An application prepared by wizards but not yet physically installed is marked as disabled in Configuration Manager. *Disabled* means that the application has been created and configured as an object in the Configuration Layer, that its installation package has been customized and copied over to a location on the wizard's host computer, but that the application has not been physically set up on the computer on which it is to run. When a user runs the actual setup using the customized installation package, the corresponding `application` object in the Configuration Layer is automatically enabled.

Preparing Installations for Redundant Applications

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 nonredundant applications (that is, applications that do not have backup servers associated with them).

When you choose to install redundant applications, two possibilities exist. If the host computers on which redundant applications are to run have operating systems of the same type, the wizard copies one installation package, which can be used to install both primary and backup applications. If the host computers have operating systems of different types, the wizard prepares a separate installation package for each application in the redundant pair.

Installing and Starting Configuration Wizards

Note: You should install the Configuration Wizards from every product CD before you deploy the Genesys components from those CDs.

To configure Genesys components through Configuration Wizards, install the wizards directly from your Genesys product CD. This will also install the Wizard Manager, or add the new wizards to an already existing Wizard Manager. Wizard Manager operates only on Windows.

Note: Genesys recommends that you install wizards on the same host computer where Configuration Manager is installed.

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

To install Management Framework wizards:

1. In the root directory of either the Management Framework 7.6 or Media 7.6 product CD, double-click `setup.exe` to start the installation.
2. Specify the destination directory into which you want to install the wizards.
3. Specify the `Program Folder` to which you want to add the wizards.

When the setup program is finished, Wizard Manager is ready to run.

Note: Before starting Wizard Manager, make sure that the Configuration Layer components are installed, configured, and running. (See Chapter 5 on page 81.)

Now start Wizard Manager from the Windows `Start > Programs` menu. Click `log into the Configuration Layer`, and specify the necessary parameters in the `Login` dialog box as described in “Login Procedure” on page 217. Provide the same Application name as if you were logging in to Configuration Manager.

Using Wizard Manager on Windows

Wizard Manager guides you through the deployment process for Genesys components, and the configuration process for Configuration Database objects.

When you start Wizard Manager, the Framework page opens. The left panel in Wizard Manager contains links to the configuration wizards for specific solutions. Before you deploy any solutions with Wizard Manager, click `Framework` in the left panel to run the Management Framework Configuration Manager, and configure the Framework as follows:

1. Configure the Management Layer.
2. Create Tenants, if you are setting up a multi-tenant environment.
3. Create Switch objects and deploy the T-Servers associated that are with them.
4. Configure the Switch objects— DNs and Places.
5. Create other required Framework configuration objects, such as Agent Logins, Agents, and Place Groups.

After this configuration process is complete, the Framework instance is configured and registered in the Configuration Database. You can now use Wizard Manager to deploy any solution by using the appropriate Configuration Wizard.

Chapter

5

Setting Up the Configuration Layer

This chapter describes how to set up the Framework Configuration Layer, which is a mandatory part of any Genesys installation and the first step of the Framework 7.6 deployment. Before deploying other Framework components manually, follow the steps described in the following topics:

Before you install Framework components:

- Consult “Network Locations for Framework Components” on page 45 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.

Installing DB Server

This section describes the installation of the DB Server that serves the Configuration Layer. This DB Server provides Configuration Server with access to the Configuration Database. Consequently, this DB Server must start before any other component does, which means you must configure it through a local configuration file.

Although DB Server is installed before Configuration Server, decide on the host and port for Configuration Server prior to DB Server installation.

Warning! Do not use the DB Server that provides access to the Configuration Database for access to any other database.

Note: If you are deploying the components on a remote host, you can also use the Management Framework Deployment Manager (also referred to as *Deployment Manager*) to deploy DB Server. See Appendix F on page 225, for guidelines.

On UNIX

1. On the Management Framework 7.6 product CD in the appropriate `services_layer/dbserver/<operating_system>` directory, locate a shell script called `install.sh`.
2. Run this script from the command prompt by typing `sh` and the file name. For example: `sh install.sh`. Then, press `Enter`.
3. To specify the `hostname` for this DB Server, do one of the following:
   - Type the name of the host, and press `Enter`.
   - Press `Enter` to select the current host.
4. Type `y` to specify that this DB Server will be dedicated to providing access to the Configuration Database, and press `Enter`.

   Warning! Do not use the DB Server that provides access to the Configuration Database for access to any other database.

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 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`.

- 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`.

7. Do one of the following:
   - Type `y` to configure DB Server (during installation), and press `Enter`. Go to Step 8 to specify values for the configuration file. For information about the DB Server configuration options and their values, refer to the *Framework 7.6 Configuration Options Reference Manual.*
   - Type `n` to not configure DB Server (during installation), and press `Enter`. In this case, you have finished installing DB Server—do not continue to the next step in this procedure. Before you can start DB Server, however, you must create a configuration file and set the configuration options in it. That procedure is described in "Configuring DB Server" on page 85.
8. Enter the Configuration Server `hostname`, and press `Enter`.
9. Enter the Configuration Server `network port`, and press `Enter`.
10. To specify the `hostname` for this DB Server, do one of the following:
    - Type the name of the host, and press `Enter`.
    - Press `Enter` to select the default, which is the host selected in Step 3.
11. To specify the `network port` for this DB Server, do one of the following:
    - Type the number of the network port, and press `Enter`.
    - Press `Enter` to select the default port (`4040`).
12. To specify the `management network port` for this DB Server, do one of the following:
    - Type the number of the management port, and press `Enter`.
    - Press `Enter` to select the default port (`4041`).

    The installation extracts the files from the package and displays the names of the database client processes for different types of SQL servers.
13. Type the number corresponding to the `database type`, and press `Enter`.

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

If you chose to configure DB Server during installation, a copy of the sample configuration file, `dbserver.conf.sample`, is created and saved as `dbserver.conf`, and the parameters specified in Steps 8 through 13 are written to this file.

If you chose to configure DB Server after installation, you must manually rename the sample file as `dbserver.conf`, and modify the configuration options before you start DB Server. See "Configuring DB Server" on page 85.

For information about DB Server configuration options and their values, refer to the *Framework 7.6 Configuration Options Reference Manual.*

On Windows

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

To install DB Server on Windows:

1. On the Management Framework 7.6 product CD in the `services_layer/dbserver/windows` directory, 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 server's Release Notes file.
3. On the `Welcome` page, click `Next` to start the installation.
4. On the `DB Server Run Mode` page, select `DB Server as an independent server` to install DB Server during initial setup, or to have it run independently of Configuration Server so that it provides access to the Configuration Database. Click `Next`.
5. On the `Database Engine Option` page, select the appropriate database engine, and then click `Next`.
6. On the `DB Server Parameters` page, specify `the DB Server Host, DB Server Port,` and `Management Port,` and then click `Next`.
7. On the `Connection Parameters to the Genesys Configuration Server` page, specify the `Host name` and `Port of Configuration Server,` and then click `Next`.

   Even if DB Server will be running independent of Configuration Server, these parameters are required to start DB Server via the Management Layer.
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.

   If necessary, use the:

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

   Click `Next` to proceed.

9. On the Ready to Install page, click:
   - Back to update any installation information.
   - Install to proceed with the installation. Installation Status displays the installation progress.
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 > Framework.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

For information about the DB Server configuration file, see "Configuring DB Server" on page 85 (the next section). For information about DB Server configuration options and their values, refer to the *Framework 7.6 Configuration Options Reference Manual.*

Configuring DB Server

Starting with release 6.0, DB Server can run either as an independent server or as a client of Configuration Server. The DB Server dedicated to the Configuration Database must run as an independent server and reads its configuration settings from a local configuration file. Any DB Server used for handling data other than configuration data must run as a client of Configuration Server and reads its configuration settings from the Configuration Database.

If you manually installed DB Server on UNIX and you chose not to configure DB Server during the installation process, configure DB Server for the Configuration Layer now:

1. From the directory where DB Server is installed, open the sample configuration file (dbserver.conf.sample) in a text editor.
2. Set the configuration options to work with the Configuration Database. Consult the relevant chapters in the *Framework 7.6 Configuration Options Reference Manual* for option descriptions and values. See "DB Server Configuration File" on page 86 for a description of the DB Server configuration file.
3. Save the sample configuration file as dbserver.conf.

For the Management Layer to monitor DB Server, you must:

- Specify the lcaport option in the lca section of the DB Server configuration file. (Refer to the *Framework 7.6 Configuration Options Reference Manual.*)

- Configure the DB Server `Application` object with the name `cfg_dbserver` in the Configuration Database as described in "Creating the DB Server Application Object" on page 101. Do this *after* you have installed Configuration Server and Configuration Manager and initialized the Configuration Database.

If you plan to use the centralized logging and auditing functionality of the Management Layer, be sure to specify appropriate log options in the DB Server configuration file before you start using DB Server. Most importantly, enable the network log output (for example, create a new option in the `log` section called `standard` and set its value to `network`). See the *Framework 7.6 Configuration Options Reference Manual* for more information.

DB Server Configuration File

The configuration file contains the DB Server, Log, and Local Control Agent (LCA) sections. It can also contain additional DB Server sections for any additional ports.

The name of the DB Server section is `dbserver`. This section contains configuration information about DB Server, including settings and the type of DBMS with which DB Server operates.

The `dbserver` section contains configuration options for one port. If there is more than one port configured for DB Server, configuration options for the additional ports is contained in additional DB Server sections called `dbserver-n,` where `n` is a non-zero consecutive integer. Each `dbserver-n` section contains the configuration options for one port.

The name of the Log section is `log.` This section contains configuration information about the log. If you plan to use the centralized logging and auditing functionality of the Management Layer, be sure to specify appropriate log options. Most importantly, enable the network log output (for example, create a new option called `standard,` and set its value to `network`).

The name of the LCA section is `lca`. If configured, this section contains an option that enables the Management Layer to control the DB Server dedicated to the Configuration Database.

You can find a sample DB Server configuration file in the *Framework 7.6 Configuration Options Reference Manual.*

Starting DB Server

To start DB Server as an independent server, configure a configuration file as described earlier. DB Server uses this file for startup. Be sure your DBMS is running.

Although DB Server is started before Configuration Server, you *must specify* the host and port parameters of Configuration Server in the command line for DB Server to start. Specify cfg_dbserver as a value for the -app command-line parameter (the DB Server Application name).

Note: For information about starting DB Server as a client of Configuration Server, see Chapter 8, "Starting and Stopping Framework Components," on page 139. That chapter also provides a complete description of the command-line parameters used for startup.

On UNIX

Go to the directory where DB 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:

  ```
  multiserver -host <Configuration Server host>
  -port <Configuration Server port> -app cfg_dbserver
  [<additional parameters and arguments as required>]
  ```

On Windows

Do one of the following:

- Use the Windows Start > Programs menu.
- To use only the required command-line parameters, go to the directory where DB 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 where DB Server is installed, and type the following command line:

  ```
  multiserver.exe -host <Configuration Server host>
  -port <Configuration Server port> -app <DB Server Application>
  [<additional parameters and arguments as required>]
  ```

You can also start DB Server as a Windows Service. Refer to "Starting and Stopping with Windows Services Manager" on page 153 for more information.

Installing 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.

This section contains installation instructions for such a Configuration Server.

Notes

- The procedures given in this section are for installing a primary Configuration Server. To install a Proxy Configuration Server, refer to "Deploying Configuration Server Proxy" on page 192 for relevant installation instructions. To install a backup Configuration Server, refer to "Redundant Configuration Servers" on page 161.
- Refer to the *Framework 7.6 External Authentication Reference Manual* for information about Configuration Server's External Authentication feature and for relevant installation instructions.
- You can also use the Management Framework Deployment Manager (also referred to as *Deployment Manager*) to install Configuration Server. See Appendix F, "Management Framework Deployment Manager" on page 225, for guidelines.

On UNIX

1. On the Management Framework 7.6 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`.

   Note: If you select LDAP, be prepared with the URL to access the LDAP Server. For more information about LDAP configuration, see the *Framework 7.6 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`.

- 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 7.6 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. Go to “Configuring Configuration Server” on page 97.

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`.

c. To specify the name of the History Log file, do one of the following:
- Specify a file name, and press `Enter`.
- Press `Enter` to select the default name (`histlog`).

10. For the `[soap]` section, do one of the following:
- Specify a value for the SOAP `port`, and press `Enter`.
- If you are not using SOAP functionality, press `Enter` to leave this field blank.

11. For the `[dbserver]` section:

a. Specify the name of the DB Server `host`, and press `Enter`.

b. Specify a value for the DB Server `port`, and press `Enter`.

c. Type the number corresponding to the database engine that this Configuration Server uses (`dbengine`), and press `Enter`.

d. Specify the name or alias of the DBMS that handles Configuration Database (`dbserver`), and press `Enter`.

e. 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.

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

g. 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 as confserv.conf and modify the configuration options before you start Configuration Server. See “Configuring Configuration Server” on page 97.

On Windows

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

To install Configuration Server on Windows:

1. On the Management Framework 7.6 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. Use the About button 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. Specify the Log File Name for the History Log, or accept the default value.
   c. 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 DB Server Host name and DB Server Port.
   b. Specify the Database Server Name and Database Name.
   c. 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, use the:

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

    Click Next to proceed.
11. On the Ready to Install information page, click:
    - 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.

For more information about the Configuration Server configuration file, see "Configuring Configuration Server" on page 97. For information about Configuration Server configuration options and their values, refer to the relevant chapters in the *Framework 7.6 Configuration Options Reference Manual.*

Populate History Change Adapter Tables

Note: HCA tables are applicable only if you are using Genesys Info Mart 7.2 or earlier. Users of Genesys Info Mart 7.5 or later do not require HCA.

You must populate HCA tables with Virtual Agent Group information immediately after database migration if both of the following conditions are true:

- If you have Genesys Info Mart 7.2 or earlier installed in your environment, and you have activated the History of Changes Adapter functionality in Configuration Server.
- If you have created Virtual Agent Groups in Configuration Server.

Follow these steps *only if both of the above statements are true*:

1. Stop the Primary Configuration Server.
2. Start Configuration Server using these command line options:
   ```
   -hca -s mm/dd/yyyy
   ```
   where `mm/dd/yyyy` is the creation date that you are setting for the records in the HCA tables. The format is month/day/year.

   Starting Configuration Server with these command line options will refresh data about existing configuration objects in HCA tables and add data about Virtual Agent Groups. It will not affect historic data already stored in HCA tables. See the *Genesys Info Mart Deployment Guide* for your version of Genesys Info Mart.
3. After the HCA tables are populated and Configuration Server has exited (automatically), restart Configuration Server in normal operational mode.

Initializing the Configuration Database

After you created a database in your DBMS (see “Prerequisites” on page 69), you can populate the tables of the Configuration Database manually (using your DBMS tools) or using the Database Initialization Wizard.

Populating the Configuration Database

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.

To populate the tables of the Configuration Database manually:

1. In the directory where 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.

   See Table 4 for a list of DBMS and their corresponding initialization script names for an enterprise or multi-tenant environment.

Table 4: Configuration Database Initialization Scripts

DBMS	Enterprise Script Name	Multi-tenant Script Name
DB2	init_single_db2.sql	init_multi_db2.sql
Informix	init_single_ifx.sql	init_multi_ifx.sql
Microsoft SQL	init_single_mssql.sql	init_multi_mssql.sql
Oracle	init_single_ora.sql	init_multi_ora.sql
Sybase	init_single_syb.sql	init_multi_syb.sql

4. Load and execute the script that loads the CfgLocale table into the initialized database, depending on your database type.

   See Table 5 for a list of DBMS and their corresponding localization data script names for an enterprise or multi-tenant environment.

Table 5: CfgLocale Scripts

DBMS	Script Name
DB2	CfgLocale_db2.sql
Informix	CfgLocale_ifx.sql
Microsoft SQL	CfgLocale_mssql.sql
Oracle	CfgLocale_ora.sql
Sybase	CfgLocale_syb.sql

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.

DBMS Adjustment

You must install and configure an SQL Server client for your database type. Please refer to the *Framework 7.6 DB Server User's Guide* for recommendations on environment settings for your database client.

Recommendations for DB2 Users

Genesys recommends using the DB2 Command-Line Processor to run Genesys SQL scripts. Follow these 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:
   ```
   db2 -f
   C:\GCTI\ConfigurationServer\sql_scripts\db2\init_single_db2.sql
   ```

About the Initialized Configuration Database

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

- A `Person` 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.

Note: For instructions on creating new configuration objects, and working with existing configuration objects, refer to *Framework 7.6 Configuration Manager Help*.

- An Application Template object for Configuration Manager.
- An Application Template object for Configuration Server.
- A Configuration Manager `Application` object with the name set to `default`.

  When you run Configuration Manager for the first time, you must specify this name in the `Application` property under `Details` in the `Login` dialog box. Consider changing the name of this application during the first session.
- A Configuration Server `Application` object with the name set to `confserv`.
- The default Access Groups objects: Users, Administrators, and Super Administrators. For more information, refer to “Security Considerations” on page 61.
- Folders for all types of objects managed by the Configuration Layer.
- An 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 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.

Encrypting the Configuration Database Password

Starting in release 6.5, you can use Configuration Server to encrypt your password for accessing the Configuration Database so that it does not explicitly appear in the Configuration Server logs. This improves configuration data security.

To enable access password encryption:

1. Start Configuration Server to force the encryption of the password, as described in “Encrypting the Database Password” on page 96.
2. Configure the `encryption` option in the Configuration Server configuration file, as described in “Modifying the Configuration File” on page 96.
3. Start Configuration Server for a regular operation, as described in “Starting Configuration Server” on page 98.

Encrypting the Database Password

After password encryption, Configuration Server decrypts the value when reading its configuration file at subsequent startups. It accesses the Configuration Database using the decrypted value, and prints a string of asterisks as the password value into the log.

To force Configuration Server to encrypt the password:

1. Make sure Configuration Server is not running.
2. Make sure the Configuration DB Server is running.
3. Start Configuration Server with the following command line:

```
confserv -p <section name> <password value>
```

Where

`-p` The command-line parameter that forces an instance of Configuration Server to start, encrypt the database password in the configuration file, and terminate.

`<section name>`
The section name in the Configuration Server configuration file that describes the Configuration Database whose access password is being encrypted.

`<password value>`
The password used for accessing the specified Configuration Database.

Note: If the configuration file name differs from the default name (`confserv.conf` on UNIX or `confserv.cfg` on Windows), the command line should also contain the `-c` parameter followed by the file name. For a description of command-line parameters specific to Configuration Server, see "Configuration Server" on page 144.

Repeat these steps for each Configuration Database section listed in the configuration file of Configuration Server.

Modifying the Configuration File

After Configuration Server encrypts the database password, open the server's configuration file, set the `encryption` configuration option to `true` in the `confserv` section, and save the file. Once set in the `confserv` section, this value applies to all Configuration Database sections specified in the configuration file.

Now, Configuration Server is ready to operate with the enabled password encryption. Start Configuration Server as described in "Starting Configuration Server" on page 98.

Configuring Configuration Server

If you manually installed Configuration Server on UNIX and chose not to configure Configuration Server during installation, do it now:

1. From the directory where 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 7.6 Configuration Options Reference Manual* for option descriptions and values. See "Configuration Server Configuration File" on page 97 for a description of the Configuration Server configuration file.
3. Save the sample configuration file as `confserv.conf`.

For the Management Layer to monitor Configuration Server:

- You must modify the Configuration Server `Application` object in the Configuration Database as described in "Modifying the Configuration Server Application" on page 101. Do this *after* you install Configuration Manager and initialize the Configuration Database.
- Also, if you plan to use centralized logging and auditing functionality of the Management Layer, be sure to 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`). See the *Framework 7.6 Configuration Options Reference Manual* for more information.

Configuration Server Configuration File

At a minimum, the configuration file contains the Configuration Server, Configuration Database, Log, and History of Changes Adapter sections, and possibly an additional section called SOAP.

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 and about the DB Server used to access this database.

Note: If you plan to use one or more DB Servers as a backup, you must also configure the same number of Configuration Database sections in the configuration file. The `server` configuration option within a given Configuration Database section must specify the name for the subsequent Configuration Database section.

The name of the Log section is `log`. This section contains configuration information about the log. If you plan to use the centralized logging and auditing functionality of the Management Layer, be sure to specify appropriate log options. Most importantly, enable the network log output (for example, create a new option called `standard` and set its value to `network`).

The name of the History of Changes Adapter (change tracking) section is `hca`. This section controls Configuration Server's change-tracking functionality.

The name of the SOAP section is `soap`. This section contains information about the Simple Object Access Protocol (SOAP) port that clients can use to access Configuration Server. If you work with SOAP, you must add a `[soap]` section to the Configuration Server configuration file before you start Configuration Server.

You can find a sample Configuration Server configuration file in the *Framework 7.6 Configuration Options Reference Manual.*

Starting Configuration Server

To start Configuration Server, configure a configuration file as described earlier; Configuration Server will use this file for startup. Be sure DB Server is running. On the command line, specify the name of the Configuration Server executable file (`confserv`).

Note: 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>`.

For descriptions of the command-line parameters specific to Configuration Server, refer to "Configuration Server" on page 144.

On UNIX

Go to the directory where 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>]
  ```

On Windows

Do one of the following:

- Use the `Start > Programs` menu.
- To use only the required command-line parameters, go to the directory where 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 where Configuration Server is installed, and type the following command line:

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

You can also start Configuration Server as a Windows Service. Refer to “Starting and Stopping with Windows Services Manager” on page 153 for more information.

Installing Configuration Manager

Configuration Manager is a GUI application and operates only on Windows.

If you want to implement a security banner with Configuration Manager, make sure that you have the necessary files prepared before you start installing Configuration Manager. Refer to the Genesys 7.6 *Security Deployment Guide* for detailed information about the security banner.

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

To install Configuration Manager on Windows:

1. On the Management Framework 7.6 product CD, locate and open the installation directory appropriate for your environment:
   - For an enterprise (single-tenant) environment, the installation directory is `configuration_layer/con fig manager server/single/windows`
   - For a multi-tenant environment, the installation directory is `configuration_layer/con fig manager/multi/windows`
2. Locate and double-click `setup.exe` to start the Genesys Installation Wizard.
3. On the `Welcome` page, click `About` 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` to continue with the installation.

5. On the Security Banner Configuration page, choose whether you want to configure a security banner for this Configuration Manager application. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information about the security banner. Do one of the following:
    - If you do not want to configure a security banner for this instance of Configuration Manager, clear the Enable Security Banner checkbox if it is selected, then click Next.
    - If you want to configure a security banner for this application:
        a. Select Enable Security Banner.
        b. Follow the instructions in the procedure "Installing and configuring the Security Banner" in the *Genesys 7.6 Security Deployment Guide.* When you are finished that procedure, return here and finish this procedure.
6. On the Choose Destination Location page, the wizard displays the destination directory.

    If necessary, click:

    - Browse to select another destination folder.
    - Default to reinstate that selection.

    Click Next to proceed.
7. On the Ready to Install page, click:
    - Back to update any installation information.
    - Install to proceed with the installation. Installation Status displays the installation progress.
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 > Framework.
- Windows Add or Remove Programs window, as a Genesys application.

Starting Configuration Manager

To start Configuration Manager, select Configuration Manager from the Windows Start > Programs menu or double-click Sce.exe in the directory where Configuration Manager is installed. Enter information in the Login dialog box as described in Appendix C, "Login Procedure" on page 217.

The first time you run Configuration Manager, some objects already defined in the Configuration Database will appear. At a minimum, the user name used to log in to Configuration Manager will be visible under the Persons folder. The instance of Configuration Manager defined under Applications and the Application Template that has been used to create this instance will also appear.

Modifying the Configuration Server Application

The Configuration Server Application object is preconfigured in the Configuration Database. Make the following changes in the Configuration Server Application after starting Configuration Manager, so that the Management Layer can control Configuration Server:

1. Open Configuration Manager.
2. Create a Host object for the computer on which Configuration Server runs.
3. Open the Properties dialog box of the Configuration Server Application (named confserv).
4. Click the Server Info tab.
5. Click Browse to select the Host that you created in Step 2.
6. On the Start Info tab, define the Working Directory and Command Line properties for the primary Configuration Server.
7. Click OK to save the changes.

Creating the DB Server Application Object

For DB Server to be controlled by the Management Layer, create a DB Server Application object:

1. Open Configuration Manager.
2. If a Host object does not exist for the computer where DB Server runs, create one.
3. Right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a DB Server template file is not listed, either import the DBServer_<current-version>.apd file from the Management Framework 7.6 product CD or use the procedure on page 206 to create a new template, and repeat this step.
4. In the Browse dialog box, select the DB Server template file, which opens the Properties dialog box for the new DB Server Application object.
5. On the General tab, enter a descriptive name in the Name text box—for example, cfg_dbserver.
6. On the Server Info tab:
   a. Specify the Host object mentioned in Step 2 on page 101.
   b. Specify the port that DB Server clients must use to connect to DB Server.
   c. Leave the rest of the fields at their default values.

7. On the Start Info tab, in the Working Directory, Command Line, and Command Line Arguments text boxes, do one of the following:
   - If you want to control (monitor, start, and stop) the DB Server using Solution Control Interface (SCI), enter the appropriate information in each of the text boxes. For information about command-line parameters, see Chapter 8 on page 139.
   - If you do not want to control the DB Server using SCI, type a period (.) in the Working Directory and Command Line and leave the Command Line Arguments text box blank.
8. On the Start Info tab, select Auto-Restart if required.
9. Click OK to save the configuration.

Next Steps

After you successfully install and configure the Configuration Layer components as described in this chapter, consider whether you would like to configure the following:

- User inactivity timeout to disable logged-in users for inactivity. Refer to the *Genesys 7.6 Security Deployment Guide.*
- Redundant DB Servers or Configuration Servers. Refer to Chapter 9 on page 155.
- Configuration Server Proxy. Refer to Chapter 10 on page 189.

Continuing the Installation of Your System

Once the Configuration Layer is set up, Genesys highly recommends that you create a Host object before you deploy any other objects. Then, you can set up the Management Layer. All of this is described in Chapter 6 on page 103.

Chapter

6

Setting Up the Management Layer

This chapter describes how to configure and install components of the Management Layer.

This chapter contains the following sections:

Overview

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

To enable the Management Layer's solution-control and fault-management capabilities, you must install Local Control Agent (LCA) on each host running a Genesys server application.

Note: An application started by the LCA inherits the environment variables from LCA. Therefore, when an application (such as DB Server) requires particular environment variables to be set, the same environment variables must be set for the account that runs LCA.

To enable the Management Layer's centralized-logging and alarm-signaling capabilities, you must configure a connection to Message Server for each Genesys server application.

You can deploy Management Layer in one of two ways:

- Use Wizard Manager, as described in "Deploying the Management Layer Using Wizard Manager" on page 105. Wizard Manager assists you in deploying all the required Management Layer components in the proper order.
- Manually, as described in "Deploying the Management Layer Manually" on page 111.

Deploying Hosts

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

To deploy a Host object:

1. In Configuration Manager, right-click the Environment > Hosts folder and select New > Host.
2. On the General 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 LCA port number or accept the default (4999) for the Management Layer to control applications running on this host. This is also the port that applications installed on this host use to connect to LCA. Refer to "Notes on Configuring the LCA Port" on page 111 for additional information on configuring the LCA port value.
3. To customize the Advanced Disconnect Detection Protocol (ADDP) functionality that will be enabled between Solution Control Server (SCS) and LCA, on the Annex tab:
   - To change the ADDP timeout between LCA and SCS, specify the addp-timeout parameter.
   - To enable LCA polling messages to SCS, specify the addp-remote-timeout parameter.

   Refer to "Configuring ADDP Between SCS and LCA" for information about ADDP between SCS and LCA.
4. Click OK.

Configuring ADDP Between SCS and LCA

Advanced Disconnection Detection Protocol (ADDP) is enabled automatically between Solution Control Server (SCS) and Local Control Agent (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, specify the `addp-timeout` parameter. If you also want to enable LCA polling messages to SCS, specify the `addp-remote-timeout` parameter. These parameters are set on the `Annex` tab of the `Host` object configured for the computer on which LCA runs. If you specify these parameters, specify them as option names and assign positive integer values in seconds.

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.

Refer to the *Framework 7.6 Configuration Options Reference Manual* for detailed descriptions of these parameters.

Deploying the Management Layer Using Wizard Manager

You can deploy the Management Layer using Wizard Manager. Wizard Manager helps you deploy all the required Management Layer components in the proper order.

Wizard Manager does not operate on UNIX, only on Windows. However, you must use this tool to configure the Framework components, regardless of whether the components are run on UNIX or Windows.

Deploying Management Layer Components on Windows

When you deploy Management Layer components on Windows, Wizard Manager configures and installs the necessary components. The components are set up and ready to run.

Deploying Management Layer Components on UNIX

When you deploy Management Layer components on UNIX, Wizard Manager configures the components but does not physically install them. Instead, Wizard Manager prepares a customized installation package for each component. You must copy the appropriate package to the host computer for each component, and then manually install each component on its host computer using the customized installation package.

This section describes how to install Management Layer components on UNIX.

Installing Log DB Server On UNIX

To manually install Log DB Server on UNIX:

1. Copy the Log DB Server installation package from the location you specified in Wizard Manager to the host computer for Log DB Server.
2. In the directory to which the DB Server installation package was copied, locate a shell script called `install.sh`.
3. Run this script from the command prompt by typing the file name.
4. When prompted, specify the `Host Name` of the computer on which DB Server is to be installed.
5. Type `n` when asked whether this DB Server will provide access to the Configuration Database.
6. Specify the destination directory into which DB Server is to be installed, with the full path to it.
7. The installation displays the names of the DB client processes for different types of SQL servers. Type the number of the DB client process name that should be configured.
8. If asked which version of the product to install, either the 32- or the 64-bit, choose the one appropriate to your environment.

As soon as the installation process is finished, a message appears announcing that installation was successful. The process places DB Server in the directory specified during the installation.

Installing Message Server On UNIX

To manually install Message Server on UNIX:

1. Copy the Message Server installation package from the location you specified in Wizard Manager to the host computer for Message Server.
2. In the directory to which the Message Server installation package was copied, locate a shell script called `install.sh.`
3. Run this script from the command prompt by typing the file name.
4. When prompted, specify the `Host Name` of the computer on which Message Server is to be installed.
5. Specify the destination directory into which Message Server is to be installed, with the full path to it.

6. If asked which version of the product to install, either the 32-bit or the 64-bit, choose the one appropriate to your environment.

As soon as the installation process is finished, a message appears announcing that installation was successful. The process places Message Server in the directory specified during the installation.

Initializing the Log Database

This section describes how to manually create the structure for a newly created database so that this database can serve as the Centralized Log Database. You can also use the Database Initialization Wizard for this purpose.

Using your DBMS tools:

1. From the directory where Message Server is installed, open the `scripts` folder.
2. Open the folder that matches your database type.
3. Load and execute the script that corresponds to your DBMS.

   See Table 6 for a list of database types and their corresponding script names.

Table 6: Log Database Scripts

DBMS	Script Name
DB2	init_db2.sql
Informix	init_informix.sql
Microsoft SQL	init_mssql.sql
Oracle	init_oracle.sql
Sybase	init_sybase.sql

DBMS Adjustment

You must install and configure an SQL Server client for your database type. Refer to the *Framework 7.6 DB Server User's Guide* for recommendations on environment settings for your database client.

Installing Solution Control Server On UNIX

To manually install Solution Control Server (SCS) on UNIX:

1. Copy the SCS installation package from the location you specified in Wizard Manager to the host computer for SCS.

2. In the directory to which the SCS installation package was copied, locate a shell script called `install.sh`.
3. Run this script from the command prompt by typing the file name.
4. When prompted, specify the `Host Name` of the computer on which Solution Control Server is to be installed.
5. Specify the destination directory into which SCS is to be installed, with the full path to it.
6. If asked which version of the product to install, either the 32-bit or the 64-bit, choose the one appropriate to your environment.
7. If you plan to use functionality that requires a license, answer `y` when asked that question, and then be prepared to give either the full path to the license file or the License Manager port and host.

As soon as the installation process is finished, a message appears announcing that installation was successful. The process places Solution Control Server in the directory with the name specified during the installation.

Installing SNMP Master Agent

If you agreed to configure Simple Network Management Protocol (SNMP) support while running the Management Layer Wizard, the wizard creates an application of the `SNMP Master Agent` type in the Configuration Database. With current implementation, you may use either Genesys SNMP Master Agent or a third-party SNMP master agent that is compliant with the AgentX protocol.

In the first case, the Management Framework CD contains the installation package; in the second case, you must obtain the installation package from a third-party vendor. Therefore, the wizard does not suggest that you copy an installation package to the SNMP Master Agent host computer. You must manually install the SNMP master agent of your choice:

- If installing Genesys SNMP Master Agent, follow the instructions for “Deploying SNMP Master Agent” on page 129.
- If installing a third-party SNMP master agent, follow the instructions from the relevant third-party documentation.

Regardless of your choice, review the *Framework 7.6 Configuration Options Reference Manual* to decide whether your environment requires configuring any configuration options for your SNMP master agent application.

For more information about SNMP functionality built into the Management Layer and on Genesys SNMP Master Agent, see the *Framework 7.6 Management Layer User’s Guide.*

Note: You must have a special license to enable the SNMP functionality. Refer to the *Genesys 7 Licensing Guide* for more information.

Deploying the Management Layer Remotely

Starting with release 7.0, the Management Layer provides a tool to install an instance of certain Framework components on a remote, unattended computer. The Host configuration object must be configured in the Configuration Database for the computer, and the computer must run an operating system supported by Genesys. A set of Deployment Wizards that are combined under *Management Framework Deployment Manager* (referred to as *Deployment Manager*) and are accessible through Solution Control Interface help with this task.

Note: The Configuration Server itself may or may not be involved with this deployment process.

Terminology

For the purpose of this discussion, the following terms are used:

- *Local host*—the computer on which Deployment Manager is running and from which you perform the remote installation.
- *Target host*—the remote computer to which LCA is installed.

The remote deployment function requires the installation of an instance of either SCI or Deployment Manager on each computer from which you perform the installation.

Deployment Wizards for the following Framework components are available in SCI:

- DB Server
- Configuration Server
- Solution Control Server
- Local Control Agent
- Message Server
- Solution Control Interface

Note: The deployment mechanism allows the installation of only one instance of the component to a target host running a Windows operating system. If you attempt to remotely deploy a second instance of the same component to the same host, the wizard reinstalls the component.

Keep in mind that the Deployment Wizards:

- Use the Windows Security mechanism to log in to a remote Windows host.
- Use a standard Telnet to access a remote UNIX host.

Framework 7.6 Solution Control Interface Help provides detailed instructions on how to start Deployment Wizards.

Specifying the CD with Installation Packages

Deployment Wizards take component installation packages from the Management Framework 7.6 product CD. That means the wizards have to know the location of this CD.

If you specify the CD location in Deployment Manager, it stores the path information, which is then available to all Wizards you call from Deployment Manager. If you do not specify the CD location in Deployment Manager or want to change the location, each Deployment Wizard provides for this by prompting you for the location of the CD that contains the version of the component you want to install. That prompt is on the `Host Specification` page, where you must:

1. Click the `Change CD` link.
2. In the `Browse` dialog box that appears, select the file called `CDInfo.xml` which is located in the root directory of the Management Framework 7.6 product CD.

The Wizard displays the specified location and takes the installation package from there.

Requirements for Local and Target Hosts

This section details software requirements for local and target hosts.

Windows Hosts

For a remote installation to be successful, both Windows local host and Windows target host must have:

1. Windows Installer Service, version 2.0 or later, installed and running.

Note: Microsoft Windows Installer Service is by default included in all versions of Windows 2000, Windows XP, and Windows 2003.

2. The user account used for deployment must have administrative rights to the target host.
3. Microsoft Windows Management (WMI) Service installed and running. Use Microsoft WMI Service version 1.5 or later.

Note: Microsoft WMI Service is by default included in all versions of Windows 2000, Windows XP, and Windows 2003.

UNIX Hosts

For a remote installation to be successful, your UNIX target host must have:

1. Telnet access—the Telnet daemon should be running on the standard port of the UNIX target host, so that a Deployment Wizard can open a Telnet connection.
2. An FTP client—a standard FTP client application must be installed. A Deployment Wizard uses it to download the installation package.
3. A standard UNIX shell `sh`.

Deploying the Management Layer Manually

To deploy the Management Layer manually, you must complete the following two steps for most of the Management Layer components that you require:

1. Configure the `Application` object in Configuration Manager.
2. Install the component.

The following sections contain detailed instructions on how to complete these steps for each component.

Deploying Local Control Agent

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 the Management Layer. This section describes how to install LCA.

Note: All running LCA processes must be stopped before installing another LCA.

Notes on Configuring the LCA Port

1. The LCA port must be set to 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).
2. 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.

3. 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 this format:

   ```
   "<full path>\lca.exe" <LCA port number> -service <lca_service_name>
   ```

   Change the LCA port number to the current value.

Installing Local Control Agent

On UNIX

Note: Stop all LCA processes before starting the installation of LCA

To install LCA on UNIX:

1. On the Management Framework 7.6 product CD in the appropriate `management_layer/lca/<operating_system>` directory, locate a shell script called `install.sh`.
2. Type the file name at the command prompt, and press `Enter`.
3. To ensure that there are no LCA processes running, do one of the following:
   - If you are installing LCA for the first time, or if you are upgrading an existing LCA but there are no LCA processing running, type `Enter` to confirm that no LCA processes are running.
   - If you are upgrading an existing LCA and there are LCA processes running, type `Enter` to exit the installation. Stop the processes and restart the installation.
4. 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.
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. 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.
    - 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.
12. 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.

On Windows

Note: Remove the existing LCA application from the host computer before installing a new one.

By default, LCA is installed in a directory called C:\Program Files\GCTI\Local Control Agent.

Note: 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. See “Notes on Configuring the LCA Port” on page 111 for information about how to change the LCA port number.

To install LCA on Windows:

1. On the Management Framework 7.6 product CD in the appropriate management_layer\lca\windows directory, 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 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 Choose Destination Location page, the wizard displays the default folder C:\Program Files\GCTI\Local Control Agent.

   If necessary, use the:

   - Browse button to select another destination folder.
   - Default button to reinstate the default folder, C:\Program Files\GCTI\Local Control Agent.

6. On the Ready to Install page, click:
   - Back to update any installation information.
   - Install to proceed with the installation.

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

LCA Log Options

If you do not specify any log options for LCA, the default values apply. To specify log options for LCA, create the lca.cfg configuration file and locate it in the same directory as the LCA executable. The LCA configuration file must have 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 7.6 Configuration Options Reference Manual*.

Deploying Log DB Server

Log DB Server runs as a client of Configuration Server. You must also configure a corresponding Database Access Point through which Log DB Server accesses the Log Database. For other applications to access the Log Database, you must configure both DB Server and Database Access Points as Application objects in Configuration Manager. For Database Access Point configuration instructions, see “Configuring Database Access Points” on page 118.

Configuring Log DB Server

To create a Log DB Server Application object:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a DB Server template file is not listed, either import the DBServer_<current-version>.apd file from the Management Framework 7.6 product CD, or use the procedure on page 206 to create a new template, and repeat this step.
2. In the Browse dialog box, select the DB Server template file, which opens the Properties dialog box for the new DB Server Application object.
3. On the General tab, enter a descriptive name in the Name text box—for example, LogDBServer.
4. On the Server Info tab:
   a. Click the Browse button next to the Host drop-down list, and select the Host object configured on page 104.
   b. Specify the listening port(s) and select whether each is secure or not secure. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information on specifying ports and securing connections to them.
   c. Leave the rest of the fields at their default values.
5. On the Start Info tab, 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 Chapter 8 on page 139.
   - 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 Log DB Server, but only if the Installation Package can connect to Configuration Server.
6. On the Options tab, in the dbserver section:
   a. Change the value of the dbprocess_name option to the value corresponding to the <DBMS you are using>_name option. For example, if you are using Microsoft SQL DBMS, set the value dbprocess_name to ./dblient_msql.
   b. Change the value of the management-port option to the number of the management port for this DB Server.
7. Click OK.

Installing Log DB Server

You can install Log DB Server on UNIX or Windows.

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.

To install Log DB Server on UNIX:

1. On the Management Framework 7.6 product CD in the appropriate `services_layer/dbserver/<operating_system>` directory, locate a shell script called `install.sh`.
2. Run this script from the command prompt by typing `sh` and the file name—for example, `sh install.sh`. Then, press `Enter`.
3. To specify the host name for this DB Server, do one of the following:
   - Type the name of the host, and press `Enter`.
   - Press `Enter` to select the current host.
4. Type `n` to specify that this DB Server will provide access to databases other than the Configuration Database (in this case, the Log Database), and press `Enter`.
5. When prompted, specify the:
   - Host name of the computer on which Configuration Server is running.
   - Network 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.
6. The installation displays the list of `Application` objects of the specified type configured on this `Host` object. Type the number corresponding to the DB Server `Application` object you configured on page 115.
7. Specify the destination directory into which this server is to be installed, with the full path to it.
8. 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`.
   - 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`.
9. The installation displays a list of database types. Type the number corresponding to the database you are using.

Note: Some items in the list have _32 or _64 at the end of the name, indicating a 32-bit or 64-bit database. Make sure to choose the one appropriate to your environment.

As soon as the installation process is finished, a message appears indicating that installation was successful. The process places the DB 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.

To install Log DB Server on Windows:

1. On the Management Framework 7.6 product CD in the appropriate services_layer\dbserver\windows directory, 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 server's Release Notes file.
3. Click Next to start the installation.
4. On the Maintenance Setup Type page, select Install new instance of the application.
5. On the DB Server Run Mode page, select DB Server as a client of Configuration Server to install DB Server as a client, so that it provides access to the Log Database. Click Next.
6. 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.
7. On the Select Application page, select the name of the DB Server Application object that you configured on page 115, and click Next.
8. On the Choose Destination Location page, the wizard displays the destination directory if you specified one in the Working Directory property of the server's Application object during configuration. If you entered a period (.) in this property field when configuring the object, or if the path that you 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, use the:

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

- Default button to reinstate the path specified in the Working Directory property.

Click Next to proceed.

9. On the Ready to Install page, click:
   - Back to update any installation information.
   - Install to proceed with 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 > Framework.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

Configuring Database Access Points

Most Genesys applications access various databases through a daemon process called DB Server. For example, the Log Database Access Point (DAP) provides the connection to the Log Database through the Log DB Server. Some Genesys applications use Java Database Connectivity (JDBC) to access databases. 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 an object of the Application type that describes both the parameters required for communication with a particular database—either DB Server or JDBC parameters—and the parameters of the database itself. The DAP Application you configure for the Management Layer uses DB Server to connect to the Log Database. If, according to your configuration, a database can be accessed through multiple DB Servers simultaneously, register as many DAPS as there are DB Servers.

To configure a DAP Application object:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a DAP template file is not listed, either import the Database_Access_Point_<current-version>.apd file from the Management Framework Product CD or use the procedure on page 206 to create a new template, and then repeat this step.
2. In the Browse dialog box, select the DAP template file, and click OK, which opens the Properties dialog box for the new DAP Application object.
3. On the General tab:
   a. Enter a descriptive name—for example, LogDAP.

      A DAP can have the same name as the database itself. However, it is recommended that you make their names unique if you are using multiple access points for the same database.

b. In the DB Server field, use the Browse button to select the Application object corresponding to the Log DB Server that you just installed.

Note: Do not select the JDBC Connection check box when you configure Database Access Points.

4. On the DB Info tab, specify information about the database as follows:

- DBMS Name— The name or alias identifying the DBMS that handles the database. The value of this option is communicated to DB Server so that it connects to the correct DBMS:
  - For Sybase, this value is the server name stored in the Sybase interface file.
  - For Oracle, the value is the name of the Listener service.
  - For Informix, this value is the name of SQL server, specified in the sqlhosts file.
  - For Microsoft SQL, set this value to the SQL server name (usually the same as the host name of the computer where Microsoft SQL runs).
  - For DB2, set this value to the name or alias-name of the database specified in the db2 client configuration.
- DBMS Type—The type of DBMS that handles the database. You must set a value for this property.
- Database Name—The name of the database to be accessed, as it is specified in the DBMS that handles this database. You must set a value for this property unless oracle or db2 is specified as the DBMS Type. For Sybase, Informix, and Microsoft SQL, this value is the name of the database where the client will connect.
- User Name—The user name established in the SQL server to access the database. You must set a value for this property.
- Password—The password established in the SQL server to access the database.
- Re-enter Password—Confirmation for the value entered for Password.
- Case Conversion—Case conversion method for key names of key-value lists coming from DB Server. This value specifies whether and how a client application converts the field names of a database table when receiving data from DB Server. If you select upper, field names are converted into uppercase; if you select lower, field names are converted into lowercase; and if you select any, field names are not converted. This setting does not affect the values of key-value lists coming from DB Server. That is, actual data is being presented exactly as in the database tables.

Note: For the Case Conversion option, use the default value (any) unless directed to do otherwise by Genesys Technical Support.

Note: Do not configure any properties on the JDBC Info tab when configuring a DAP Application for the Management Layer.

5. On the Server Info tab:
   a. Click the Browse button next to the Host drop-down list, and select the Host object configured on page 104.
   b. Specify the listening port(s) and select whether each is secure or not secure. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information on specifying ports and securing connections to them.

To interface an Application object with a database through a certain Database Access Point, add this access point to the list of the Application's Connections.

Deploying Message Server

This section describes how to configure and install a Message Server Application object.

Configuring Message Server

To create a Message Server Application object:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a Message Server template is not listed, import the Message_Server_<current-version>.apd file from the Management Framework Product CD or use the procedure on page 206 to create a new template, and then repeat this step.
2. In the Browse dialog box, select the Message Server template file, which opens the Properties dialog box for the new Message Server Application object.
3. On the General tab, enter a descriptive name in the Name text box.
4. On the Server Info tab:
   a. Click the Browse button next to the Host drop-down list, and select the Host object configured on page 104.
   b. Specify the listening port(s).
   c. Leave the rest of the fields at their default values.
5. On the Start Info tab, 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 Chapter 8 on page 139.

- 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.

6. On the Connections tab, add a connection to the Database Access Point for the Log Database.
7. If you want Message Server to direct log events to the Log Database, do the following:
   a. On the Options tab, double-click the messages section.
   b. Change the value of db_storage to true.
   c. Click OK.
8. Click OK.

If you want to use centralized-logging and alarm-signaling for Configuration Server, Configuration Server Proxy, and the DB Server dedicated to the Configuration Database, add a connection to the Message Server Application object to the Connections tab of the respective Application objects.

Installing Message Server

You can install Message Server on UNIX or Windows.

On UNIX

To install Message Server on UNIX:

1. On the Management Framework 7.6 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 on page 120, 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`.
    - 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.

To install Message Server on Windows:

1. On the Management Framework 7.6 product CD in the appropriate `management_layer\message_server\windows` directory, 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 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 on page 120, 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, use the:

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

Initializing the Log Database

Refer to "Initializing the Log Database" on page 107 for full instructions on how to initialize a newly created database so that it can serve as the Log Database.

Deploying Solution Control Server

This section describes how to configure and install Solution Control Server.

Configuring Solution Control Server

To create a Solution Control Server Application object:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a Solution Control Server template is not listed, import the solution_Control_Server_<current-version>.apd template file from the Management Framework CD or use the procedure on page 206 to create a new template, and then repeat this step.
2. In the Browse dialog box, select the Solution Control Server template file, which opens the Properties dialog box for the new Solution Control, Server Application object.
3. On the General tab, enter a descriptive name in the Name text box.

4. On the Server Info tab:
    a. Click the Browse button next to the Host drop-down list, and select the Host object configured on page 104.
    b. Specify the listening port(s), and select whether each is secure or not secure. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information on specifying ports and securing them.
    c. Leave the rest of the fields at their default values.
5. On the Start Info tab, 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 Chapter 8 on page 139.
    - 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.
6. If you want to enable alarm signaling, on the Connections tab, add a connection to the Message Server.
7. Click OK.

If you plan to use SNMP functionality, deploy SNMP Master Agent (see “Deploying SNMP Master Agent” on page 129). For information about SNMP functionality built into the Management Layer, refer to the *Framework 7.6 Management Layer User’s Guide.*

Installing Solution Control Server

You can install Solution Control Server on UNIX or Windows.

On UNIX

To install Solution Control Server on UNIX:

1. On the Management Framework 7.6 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. 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.
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 SCS `Application` object you just configured, 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`.
    - 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`.
12. To decide whether you require a license, refer to the *Genesys 7 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`.
13. 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.

To install Solution Control Server on Windows:

1. On the Management Framework 7.6 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. Use the `About` button 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 Solution Control Server Application object that you just configured, and then click Next.
6. On the Run-time License Configuration page, select whether you are using a license. Refer to the *Genesys 7 Licensing Guide* for information about licensing requirements, and then click Next.
7. If you selected Use License in Step 6, on the Access to License page, enter the license access type and required parameters.
8. 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 the Working Directory property is invalid, the wizard generates a 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. In this case, the wizard will update the Application object's Working Directory property in the Configuration Database.
   - Default button to reinstate the path specified in the Working Directory property.

   Click Next to proceed.
9. On the Ready to Install page, click:
   - Back to update any installation information.
   - Install to proceed with 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 > Management Layer.
- Windows Add or Remove Programs window, as a Genesys server.
- Windows Services list, as a Genesys service, with Automatic startup type.

Deploying Solution Control Interface

This section describes how to configure and install Solution Control Interface (SCI).

Note: If you configure more than one instance of Solution Control Server, and/or more than one Log Database exist in your system, you can configure SCI connections to any combination of these instances. However, note that at runtime, SCI works with only one Solution

Control Server and one Log Database. If you have defined connections to more than one SCS and/or Log Database, then at startup SCI prompts you to select the SCS and the Log Database for the current working session.

Configuring Solution Control Interface

To configure an SCI `Application` object:

1. In Configuration Manager, right-click the `Environment > Applications` folder and select `New > Application,` which opens the `Browse` dialog box with the available Application Templates. If an SCI template is not listed, import the `solution_Control_Interface_<current-version>.apd` template file from the Management Framework product CD or use the procedure on page 206 to import it, and then repeat this step.
2. In the `Browse` dialog box, select the SCI template file and click `OK,` which opens the `Properties` window for the SCI `Application` object.
3. On the `General` tab, enter a descriptive name.

   Note: Starting with release 7.0.1, you can enable the ADDP protocol for SCI connections to SCS. See "Configuring ADDP" on page 207 for instructions. Enable ADDP-related logging on the server side.

4. On the `Connections` tab:
   - Add a connection to the Solution Control Server `Application` object configured on page 123.
   - If you want to display log messages in SCI, add a connection to the Log Database Access Point `Application` object configured on page 115.

   As you add server applications to your system, you can add connections to them as required.
5. Click `OK` to save your changes and close the `Properties` dialog box.

Installing Solution Control Interface

Solution Control Interface is a GUI application that operates only on Windows.

If you want to implement a security banner with SCI, make sure that you have the necessary files prepared before you start installing SCI. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information about the security banner.

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

To install SCI on Windows:

1. On the Management Framework 7.6 product CD, in the appropriate `management_layer\solution_control_interface\windows` directory, 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 server's Release Notes file.
3. Click `Next` to start the installation.
4. On the `Security Banner Configuration` page, choose whether you want to configure a security banner for this SCI application. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information about the security banner. Do one of the following:
   - If you do not want to configure a security banner for this instance of SCI, clear the `Enable Security Banner` checkbox if it is selected, then click `Next.`
   - If you want to configure a security banner for this application:
     a. Select `Enable Security Banner.`
     b. Follow the instructions in the procedure "Installing and configuring the Security Banner" in the *Genesys 7.6 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 destination directory, as specified in the `Working Directory` property of the server's `Application` object. 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, use the:
   - `Browse` button to select another destination folder. In this case, the wizard will update the `Application` object's `Working Directory` property in the Configuration Database.
   - `Default` button to reinstate the path specified in the `Working Directory` property.

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

By default, SCI is installed in a directory called `C:\Program Files\GCTI\Solution Control Interface`.

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 application.

Deploying SNMP Master Agent

If you plan to use SNMP functionality, you must deploy SNMP Master Agent. This section describes how to configure and install SNMP Master Agent.

For more information about Genesys SNMP Master Agent, refer to the *Framework 7.6 Management Layer User's Guide.*

Configuring SNMP Master Agent

To create an SNMP Master Agent `Application` object:

1. In Configuration Manager, right-click the `Environment > Applications` folder and select `New > Application`, which opens the `Browse` dialog box with the available Application Templates. If an SNMP Master Agent template is not listed, import the `SNMP_Master_Agent_<current-version>.apd` template file from the Management Framework product CD or use the procedure on page 206 to create a template, and then repeat this step.
2. In the `Browse` dialog box, select the SNMP Master Agent template file, which opens the `Properties` dialog box for the new SNMP Master Agent `Application` object.
3. On the `General` tab, enter a descriptive name.
4. On the `Server Info` tab:
   a. Click the `Browse` button next to the `Host` drop-down list, and select the `Host` object configured on page 104.
   b. Specify the listening port(s).
   c. Leave the rest of the fields at their default values.
5. On the `Start Info` tab, 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 Chapter 8 on page 139.

- 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.

6. Click OK to save the configuration.

Installing SNMP Master Agent

You can install SNMP Master Agent on UNIX or on Windows.

On UNIX

To install SNMP Master Agent on UNIX:

1. On the Management Framework 7.6 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 SMNP 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 on page 129, 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. Type y to confirm your selection, and press Enter.
    - Type 3 to erase all files in this directory before continuing with the installation, and press Enter. 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.

To install Genesys SNMP Master Agent on Windows:

1. On the Management Framework 7.6 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. Use the About button 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 Application object that you configured on page 129, 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 specified path is invalid, the wizard generates a 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. In this case, the wizard will update the Application object's Working Directory property in the Configuration Database.
    - Default button 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.

Next Steps

After you successfully install and configure the Management Layer components as described in this chapter, consider whether you would like to configure the following:

- Force logged-in users to log in again after a period of inactivity. Refer to "Forced Re-Login for Inactivity" on page 67.
- Redundant Message Servers, Solution Control Servers, or SNMP Master Agents. Refer to Chapter 9 on page 155.
- Distributed Solution Control Servers. Refer to Chapter 10 on page 189.

Continuing the Installation of Your System

Once the Management Layer is set up, you can then deploy the rest of the Framework components and the contact center environment. This is described in Chapter 7 on page 133.

Chapter

7 Setting Up the Rest of Your System

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. This chapter provides a brief overview of this process.

This chapter contains the following sections:

Recommended Order

Note: If you are using Genesys Configuration Wizards, this section does not apply to you. Configuration Wizards automatically use the recommended order.

Manual deployment of the other Framework 7.6 components and contact center environment objects involves:

- Configuring the components via Configuration Manager.
- Manually installing the configured components.

Before you proceed, make sure that the Configuration Layer and Management Layer components are installed, configured, and running (see Chapter 5 on page 81 and Chapter 6 on page 103, respectively). To help you prepare accurate configuration information and become familiar with the configuration process, read Chapter 3, “Planning the Installation,” on page 41 for help with object-configuration information.

Follow this order for the manual deployment of the other Framework 7.6 components and contact center environment objects:

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

   Note: 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

   Note: 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
   - DB Server for solutions

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 the CTI setup 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 Person 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 nonredundant 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 Groups objects.

3. Set Access Group privileges with respect to the object types, using the folders' `Security` tabs.

Also, 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.

Persons

There are two major categories of Persons: Agents and Nonagents. The latter category includes all Persons 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, or 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 Nonagents with a high level of access to help you set up the Configuration Database.

Assign Agent Logins and Skills when registering Agents.

Note: 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 Person objects after you create them. To launch the wizard, select two or more Person objects that have the `Is Agent` check box selected, right-click, and select `Manage Skills`. Refer to *Framework 7.6 Configuration Manager Help* for more information.

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

Starting in release 7.6, newly created Persons are not automatically assigned to any Access Group, by default. They must be assigned to one or more Access Groups explicitly. Users created in release 7.5 or earlier 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 in release 7.5 or earlier, 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 7.6 Security Deployment Guide* for more information about this feature, and how to use and disable it.

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

Ranks, as well as access privileges, are more important when registering nonagents. When registering nonagents, consider the role they have in the customer interaction business. Do these Persons 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 Person is an agent or not.

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.

Note: See also the Security Considerations section of Chapter 3, "Planning the Installation," on page 41.

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 7.x.

DB Server for Solutions

The configuration and installation procedures for a DB Server being used to access databases other than the Configuration Database and Log Database are identical to the procedures for DB Server for the Log Database (see "Deploying Log DB Server" on page 114). The procedures are also described in the *Framework 7.6 DB Server User's Guide.*

Next Steps

After you have completed all of this configuration, the Framework instance is configured and registered in the Configuration Database. You can now use Wizard Manager to deploy any solution by using the appropriate Configuration Wizard.

Chapter

8 Starting and Stopping Framework Components

This chapter provides instructions on how to start and stop Framework components by using either the Management Layer or manual procedures.

This chapter contains the following sections:

Introduction

You can start and stop Framework components by using the Management Layer, a startup file, a manual procedure, or the Services Manager.

With all these methods, command-line parameters are usually required for a server application in addition to an executable file name.

Common command-line parameters are as follows:

`-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:

- Full path to and the exact name of the license file used by an application. For example, `-l /opt/mlink/license/license.dat`.
- 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.
Note that specifying 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 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 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.

Warning! An application that does not find its `*.lms` file at startup cannot generate application-specific log events and send them to Message Server.

Note: In the command-line examples in this document, angle brackets indicate variables that you must replace with appropriate values.

Starting and Stopping with the Management Layer

Before starting an application with the Management Layer, make sure the application's startup parameters are correctly specified in the `Application Properties` dialog box in Configuration Manager. On the `Start Info` tab of this dialog box check that the following entries are correct:

- `Working Directory`—The directory where the application is installed and/or is to run.
- `Command Line`—The name of the executable file.
- `Command Line Arguments`—The command-line parameters.

The command-line parameters common to Framework server components are described on page 139.

After you correctly specify the command-line parameters, you can start and stop the following Framework components from Solution Control Interface (SCI), which is the interface component of the Management Layer:

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

Note: For the Management Layer to start Configuration Server, you must modify the Configuration Server Application in the Configuration Database, as described in "Modifying the Configuration Server Application" on page 101.

- Configuration Server Proxy
- DB Server

Note: For the Management Layer to start the DB Server dedicated to the Configuration Database, you must create a DB Server Application in the Configuration Database, as described in "Creating the DB Server Application Object" on page 101.

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

To start or stop these components, SCI must be running. The starting procedure for SCI is described on page 150. *Framework 7.6 Solution Control Interface Help* provides complete instructions on starting and stopping applications. The Management Layer can also restart failed applications; to enable the autorestart functionality for a particular application, select a corresponding check box in the `Application Properties` dialog box.

Note that when an application is started (or restarted) via the Management Layer, it inherits environment variables from Local Control Agent (LCA), which executes the startup command. Therefore, you must also set the environment variables required for the application (such as DB Server) 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.

Starting with Startup Files

Startup files are files named (or having an extension) `run.sh` (on UNIX) or `startServer.bat` (on Windows) which installation scripts create and place into the applications' directories during the installations. For additional information about how to use startup files, refer to the *Framework 7.6 Management Layer User's Guide.*

Note: You must manually modify the run.sh file created for a redundant server before you can use it to start the server. Refer to Chapter 9 on page 155 for more information.

When using a startup file, verify that the startup parameters that the installation script inserted in the startup file are correct. Use the following instructions for UNIX and Windows start those applications for which startup files are created. See the appropriate sections in "Starting Manually" to identify which applications should be running for a particular application to start.

On UNIX

Go to the directory where the application is installed and type the following command line:

```
sh run.sh
```

On Windows

Double-click the `startServer.bat` icon in the directory where the application is installed or, from the MS-DOS window, go to the directory where the application is installed and type `startServer.bat` at the command line.

Starting Manually

When using a manual procedure to start an application, specify the startup parameters in the command prompt, whether starting on UNIX or Windows. 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.

The command-line parameters common to Framework server components are described on page 139.

General Limitation

When an application is installed on a UNIX operating system and the Application name, as configured in the Configuration Database, contains spaces (for example, T-Server Avaya), you must surround the Application name by quotation marks (" ") in the command line, as follows:

```
-app "T-Server Avaya"
```

Specify the rest of the command-line parameters as for any other application.

DB Server

Before starting DB Server, be sure that your DBMS server is running.

The DB Server startup procedure depends on the database to which this DB Server provides access. If DB Server provides access to the Configuration Database, it must operate as an independent server; that is, DB Server must read all configuration information from its configuration file. When you start DB Server with the Application name `cfg_dbserver`, DB Server reads all configuration information from its configuration file.

If DB Server provides access to a database other than the Configuration Database—for example, to the Log Database—it must operate as a client of Configuration Server; that is, DB Server must be started with an Application name other than `cfg_dbserver,` as configured in the Configuration Database. When you start DB Server with an Application name specified in the Configuration Database, DB Server reads all configuration information from Configuration Database. During operation, DB Server constantly receives updates on configuration changes from Configuration Server.

Whether you start DB Server as an independent server or as a client of Configuration Server, DB Server requires that you specify the Configuration Server host and port in the startup command line.

The command-line parameters common to Framework server components are described on page 139.

In addition, you can use these command-line parameters when starting DB Server:

`-c` DB 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 (`dbserver.conf` on UNIX or `dbserver.cfg` on Windows).

`-cfg` DB Server for the Configuration Database starts with an application name other than `cfg_dbserver`, but still reads its configuration from a configuration file. When you specify this parameter, the Management Layer can restart DB Server that is configured as an application even when Configuration Server is not available. Use this parameter for starting a backup DB Server for the Configuration Database. This parameter does not require any value. For more information, see Chapter 9.

On UNIX

Go to the directory where DB 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:

  ```
  multiserver -host <Configuration Server host> -port
  <Configuration Server port> -app <DB 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 where DB 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 where DB Server is installed, and type the following command line:

  ```
  multiserver.exe -host <Configuration Server host>
  -port <Configuration Server port> -app <DB Server Application>
  [<additional parameters and arguments as required>]
  ```

Configuration Server

Before starting Configuration Server, be sure the DB Server that provides access to the Configuration Database is running.

Configuration Server does not require any of the common command-line parameters for startup. You can specify additional command-line parameters, specific to Configuration Server, to verify the database object integrity:

`-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 these 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` For a description and procedure, refer to "Encrypting the Database Password" on page 96.

`-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's 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 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 where 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>]
```

On Windows

Do one of the following:

- Use the `Start > Programs` menu.
- To use only the required command-line parameters, go to the directory where 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 where Configuration Server is installed, and type the following command line:

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

Configuration Server Proxy

Before starting Configuration Server Proxy, be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server
- License Manager

The command-line parameters common to Framework server components are described on page 139.

Note: Configuration Server Proxy does not support additional command-line parameters specific to Configuration Server.

On UNIX

Go to the directory where 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 [<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 where 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 where Configuration Server Proxy is installed, and type the following command line:

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

Configuration Manager

Before starting Configuration Manager, be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server

Start Configuration Manager from the `Start > Programs` menu or double-click the `Sce.exe` icon in the directory where Configuration Manager is installed. Then, log in to Configuration Manager as described in Appendix C, “Login Procedure,” on page 217.

License Manager

For information about starting License Manager, see the *Genesys 7 Licensing Guide,* which is available on the Genesys Documentation Library CD.

Message Server

Before starting Message Server, be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server
- The DB Server that provides access to the Log Database if you intend to use centralized logging

The command-line parameters common to Framework server components are described on page 139.

On UNIX

Go to the directory where 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 <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 where 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 where Message Server is installed, and type the following command line:

  ```
  MessageServer.exe -host <Configuration Server host> -port
  <Configuration Server port> -app <Message Server Application>
  [<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. You can start LCA from the `Start > Programs` menu on Windows.

For instructions on changing the default LCA port value, refer to “Deploying Hosts” on page 104.

Solution Control Server

Before starting Solution Control Server, be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server
- License Manager, if starting SCS in Distributed mode or if HA support or SNMP functionality is needed

The command-line parameters common to Framework server components are described on page 139.

On UNIX

Go to the directory where SCS 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 <Solution Control 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 where 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 where SCS is installed, and type the following command line:

  ```
  scs.exe -host <Configuration Server host> -port <Configuration
  Server port> -app <Solution Control Server Application> [<additional
  parameters and arguments as required>]
  ```

Optional Command-line Parameter

This parameter can be used on UNIX or on Windows:

`-f <SCS Configuration file>`

SCS gets Configuration Server's settings from the SCS configuration file. Since 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 which is running in the Primary mode.

SCS Configuration File

For Windows, use the filename extension `.cfg`. For UNIX, use the extension `.conf`.

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
```

Solution Control Interface

Before starting Solution Control Interface (SCI), be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server
- Solution Control Server
- The DB Server that provides access to the Log Database, if you intend to use centralized logging

Start SCI from the `Start > Programs` menu or double-click the `Sci.exe` icon. Then log in to SCI as described in Appendix C, "Login Procedure," on page 217.

SNMP Master Agent

Before starting Genesys SNMP Master Agent, be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server
- Message Server, if you intend to use the SNMP alarm signaling

The command-line parameters common to Framework server components are described on page 139.

On UNIX

Go to the directory where Genesys 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 <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 where 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 where 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>]
  ```

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.

Before starting HA Proxy, be sure that the following components are running:

- DB Server that provides access to the Configuration Database
- Configuration Server

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:

- DB Server that provides access to the Configuration Database
- Configuration Server
- License Manager

Note: 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 Stat Server 7.x.

Before starting Stat Server, be sure that the following components are running:

- The DB Server that provides access to the Configuration Database
- Configuration Server

Note: For Stat Server to operate correctly, T-Server must also be running.

Stopping Manually

Server Applications

The described stopping procedures apply to Genesys server applications, such as DB Server, Configuration Server, Configuration Server Proxy, Message Server, Local Control Agent, Solution Control Server, HA Proxy, T-Server, and Stat Server.

On UNIX

To stop a server application from its console window on UNIX, use either of these commands:

- `Ctrl+C`
- `kill <process number>`

On Windows

To stop a server application in 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

The stopping procedures for Genesys GUI applications, such as Configuration Manager and Solution Control Interface, are described in detail in the application Help files.

Starting and Stopping with Windows Services Manager

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. (Beginning with release 7.1.0, every Genesys daemon application is installed as a Windows Service.) 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 on page 139 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 the autostart capability, are automatically started each time a computer on which they are installed is rebooted.

You can start Framework components, installed as Windows Services with the manual start capability with the `Start` button in Services Manager.

Note: Use the `Windows Services` window to change the startup mode from Automatic to Manual and vice versa.

You can stop Framework components, installed as Windows Services regardless of the start capability, with the `Stop` button in Services Manager.

Chapter

9 Setting Up Redundant Components

This chapter provides instructions for configuring primary and backup Framework Servers.

This chapter contains the following sections:

Introduction

The high availability architecture implies the existence of redundant applications, a primary and a backup, monitored by a management application.

The Configuration Layer and Management Layer support the `warm standby` redundancy type between redundant pairs of components within those layers. Both components in the pair must be configured with the `warm standby` redundancy type. The redundant architecture is described in *Framework 7.6 Architecture Help*. Redundancy types are described in the *Genesys 7.6 Security Deployment Guide*.

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

Note: This chapter assumes that the primary server is already installed and operating. This chapter provides only instructions for installing the backup server and configuring the primary and backup servers to operate as a redundant pair.

Redundant Configuration DB Servers

This section describes how to set up redundant Configuration DB Servers—that is, DB Servers that are dedicated to provide access to the Configuration Database, and that are not clients of Configuration Server.

To set up redundant DB Servers that provide access to databases other than the Configuration Database (such as the Log Database) and that are not clients of Configuration Server (such as Log DB Server), refer to “Redundant Client DB Servers” on page 172.

Note: In this section only, the term *DB Server* denotes a Configuration DB Server, not a Client DB Server.

Redundancy

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

Installation Recommendations

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

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

Prerequisites

Set up redundant Configuration DB Servers only after you have installed and run the Configuration Layer components as described in Chapter 5 on page 81.

Setting Up Redundant DB Servers

To set up redundant DB Servers:

1. Install the backup DB Server, as described in “Installing DB Server” on page 82.
2. Configure an `Application` object for the backup DB Server as described in “Creating the Backup DB Server Application Object” on page 157.

3. If an `Application` object for the primary DB Server does not already exist, create it, as described in “Creating the DB Server Application Object” on page 101.
4. Modify the `Application` object for the primary DB Server as described in “Modifying the Primary DB Server Application Object” on page 158.
5. Modify the configuration files for the primary DB Server and the backup DB Server as described in “Modifying the Configuration Files” on page 158.
6. Modify the start file `run.sh` (on UNIX) or `start_server.bat` (on Windows) as follows:
   a. Change the argument for the `-app` parameter to the correct name of the backup DB Server application.
   b. Add the following at the end of the command line:

      ```
      -cfg -c <backup_db_server_config_file_name> -cfg
      ```

Creating the Backup DB Server Application Object

To create an `Application` object for the backup DB Server:

1. In Configuration Manager, right-click the `Environment > Applications` folder and select `New > Application`, which opens the `Browse` dialog box with the available Application Templates. If a DB Server template file is not listed, either import the `DBServer_<current-version>.apd` file from the Management Framework 7.6 product CD or use the procedure on page 206 to create a new template, and repeat this step.
2. In the `Browse` dialog box, select the DB Server template file, which opens the `Properties` dialog box for the new DB Server `Application` object.
3. On the `General` tab, specify an application name other than `cfg_dbserver`.
4. On the `Server Info` tab, specify:
   a. The Host on which the backup DB Server is running.
   b. The port that DB Server clients must use to connect to DB Server.
5. On the `Start Info` tab:
   a. In the `Working Directory, Command Line, and Command Line Arguments` text boxes, do one of the following:
      - If you want to control (monitor, start, and stop) the backup DB Server using Solution Control Interface (SCI), enter the appropriate information in each of the text boxes. In the `Command Line Arguments` text box, add the argument `-cfg`. This parameter requires no arguments. For information about command-line parameters, see Chapter 8 on page 139.
      - If you do not want to control the backup DB Server using SCI, type a period (.) in the `Working Directory` and `Command Line` and leave the `Command Line Arguments` text box blank.

   b. Select the `Auto-Restart` check box.

6. Click `OK`.

Modifying the Primary DB Server Application Object

To modify the primary DB Server's `Application` object to work with the backup DB Server:

1. In Configuration Manager, open the `Properties` dialog box of the DB Server `Application` object that you want to configure as the primary server.
2. On the `Server Info` tab:
   a. Use the `Browse` button to locate and select the `Application` object corresponding to the backup DB Server you want to use as the Backup Server.
   b. Select `Warm Standby` as the redundancy type.
3. On the `Start Info` tab, select `Auto-Restart` if required.
4. Click `OK` to save the configuration changes.

Modifying the Configuration Files

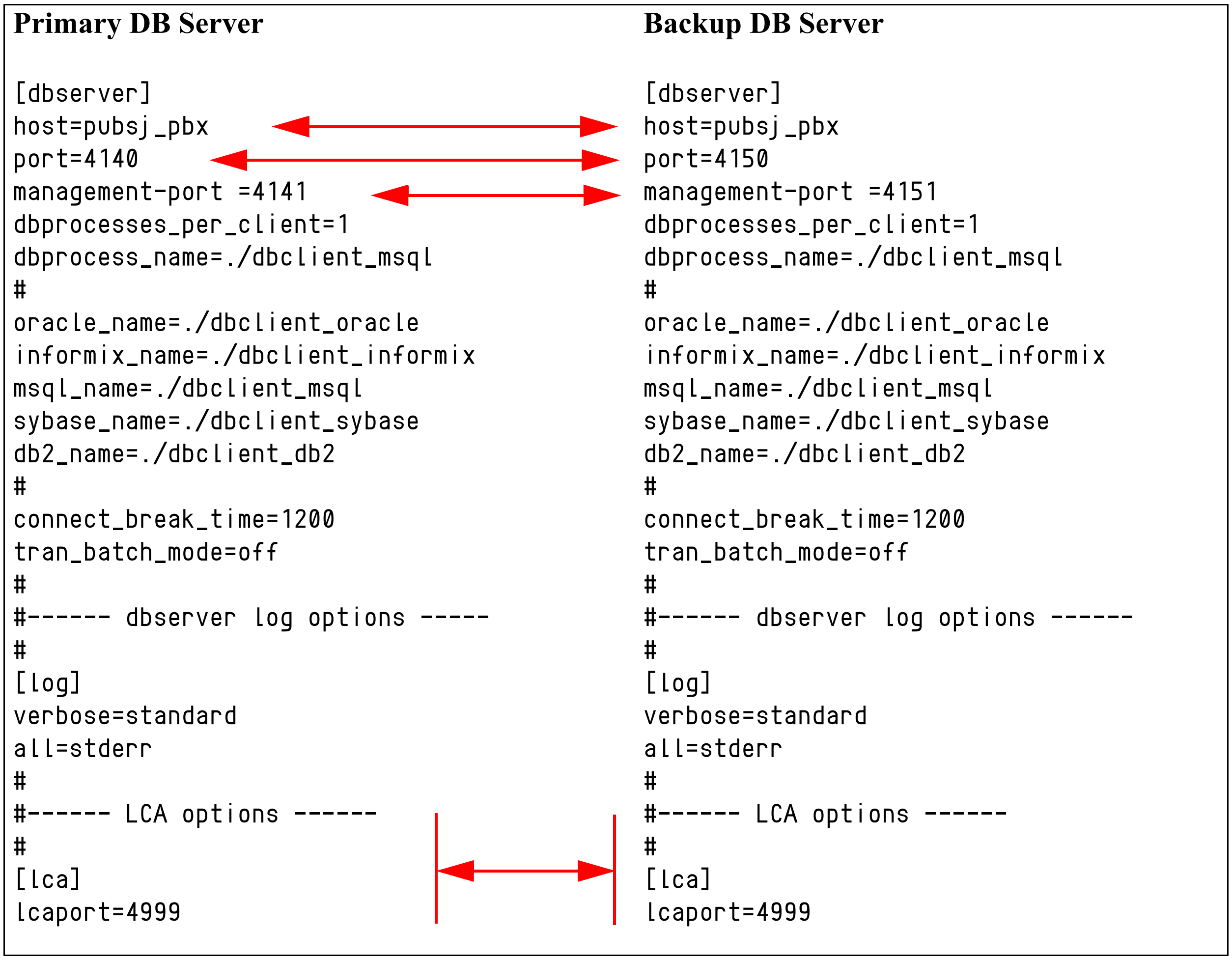
The configuration file for the backup DB Server must be the same as that for the primary DB Server, with the following exceptions:

- The host option value can be different if the backup DB Server is installed on a different host computer than the primary server.
- The port option value must be unique.

The configuration file for the backup DB Server may or may not have been created during installation, depending on the option you chose. In either case, refer to "Configuring DB Server" on page 85 for instructions on configuring a DB Server configuration file.

In both configuration files—the primary DB Server and the backup DB Server—create the `lca` section (if not already created), and configure the `lcaport` option in this section. This allows both servers to be controlled by the Management Layer, and for switchover to occur when necessary.

Sample configuration files are shown side-by-side in Figure 7 on page 159. The arrows show the areas affected by the notes in this section.



Primary DB Server

```
[dbserver]
host=pubsj_pbx
port=4140
management-port =4141
dbprocesses_per_client=1
dbprocess_name=./dbclient_msql
#
oracle_name=./dbclient_oracle
informix_name=./dbclient_informix
msql_name=./dbclient_msql
sybase_name=./dbclient_sybase
db2_name=./dbclient_db2
#
connect_break_time=1200
tran_batch_mode=off
#
#------ dbserver log options -----
#
[log]
verbose=standard
all=stderr
#
#------ LCA options ------
#
[lca]
lcaport=4999
```

Backup DB Server

```
[dbserver]
host=pubsj_pbx
port=4150
management-port =4151
dbprocesses_per_client=1
dbprocess_name=./dbclient_msql
#
oracle_name=./dbclient_oracle
informix_name=./dbclient_informix
msql_name=./dbclient_msql
sybase_name=./dbclient_sybase
db2_name=./dbclient_db2
#
connect_break_time=1200
tran_batch_mode=off
#
#------ dbserver log options ------
#
[log]
verbose=standard
all=stderr
#
#------ LCA options ------
#
[lca]
lcaport=4999
```

Figure 7: Sample Configuration Files for Primary and Backup DB Servers.

Synchronization Between Primary and Backup DB Servers

Configuration Manager can automatically synchronize options and ports between primary and backup DB Servers.

Setting Up Options Synchronization

Refer to “Setting Up Options Synchronization Between Primary and Backup Servers” on page 208 for detailed instructions.

Setting Up Ports Synchronization

Refer to “Setting Up Ports Synchronization Between Primary and Backup Servers” on page 209 for detailed instructions.

Starting the Backup DB Server

When starting a backup DB Server, be sure to use the following command line parameters:

`-c` To specify the name of the configuration file that contains configuration information for the backup DB Server

`-app` To specify the name of the backup DB Server application (see Step 6 on page 157).

In addition, make sure that the `run.sh` file (on UNIX) or `start_server.bat` file (for Windows) has been modified accordingly (see Step 6 on page 157). For a description of the command line parameters specific to DB Server, refer to "DB Server" on page 143.

On UNIX

To start the backup DB Server on UNIX, do one of the following:

- To start from SCI, refer to "Starting and Stopping with the Management Layer" on page 141.
- To start manually, go to the directory where the backup DB 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:

    ```
    multiserver -host <Configuration Server host>
    -port <Configuration Server port>
    -app <backup DB Server Application> -cfg
    -c <backup DB Server configuration file>
    ```

On Windows

To start the backup DB Server on Windows, do one of the following:

- To start as a Windows Service, refer to "Starting and Stopping with Windows Services Manager" on page 153.
- To start from SCI, refer to "Starting and Stopping with the Management Layer" on page 141.
- 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 where the backup DB 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 where the backup DB Server is installed, and type the following command line:

```
multiserver.exe -host <Configuration Server host>
-port <Configuration Server port>
-app <backup DB Server Application>
-cfg -c <backup DB Server configuration file>
```

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.

Configuration Warnings

When configuring Configuration Servers to support redundancy, remember:

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

Set up redundant Configuration Servers only after you install and run the Configuration Layer components as described in Chapter 5 on page 81.

Setting up Redundant Configuration Servers

To set up redundant Configuration Servers:

1. Configure an `Application` object for the backup Configuration Server as described in "Configuring the Backup Configuration Server Application" on page 162.
2. Install a backup Configuration Server as described in "Installing the Backup Configuration Server" on page 163.
3. Modify the primary Configuration Server `Application` object as described in "Modifying the Primary Configuration Server Application" on page 168.
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 as described in "Creating the Configuration File for the Backup Configuration Server" on page 168.
5. If you installed the backup Configuration Server on UNIX, modify the `run.sh` file by adding the following at the end of the command line in the file:

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

Configuring the Backup Configuration Server Application

1. In Configuration Manager, right-click the `Environment > Applications` folder and select `New > Application`, which opens the `Browse` dialog box with the available Application Templates. If a Configuration Server template is not listed, import the `Configuration_Server_Proxy_<current-version>.apd` template file from the Management Framework product CD or use the procedure on page 206 to import it, and then repeat this step.
2. In the `Browse` dialog box, select the Configuration Server template file, which opens the `Properties` dialog box for the new backup Configuration Server `Application` object.
3. On the `General` tab of the `Properties` dialog box, enter a name for the backup Configuration Server `Application` object. The Application Template provides information for the application `Type` and `Version`.
4. On the `Server Info` tab, specify:
   a. the host on which the backup Configuration Server is to be installed.

  b. the communication ports that clients must use to connect to this Configuration Server.

5. On the Start Info tab, 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 Chapter 8 on page 139.
   - 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
6. Click OK to create the Application object for the backup Configuration Server.
7. Open the Properties dialog box of the backup Configuration Server Application object.
8. Click the Security tab.
9. In the Log On As group section, make sure that This Account is selected, and that the account name matches the name of the Master Account.
10. Click OK to save any configuration changes.

Installing the Backup Configuration Server

Refer to “Installing Configuration Server” on page 87 for general comments about installing Configuration Server.

On UNIX

To install the backup Configuration Server on UNIX:

1. On the Management Framework 7.6 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/<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 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`.

> **Note:** If you select LDAP, be prepared with the URL to access the LDAP Server. For more information about LDAP configuration, see the *Framework 7.6 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 in Configuration Manager, 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`. 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`.
   - 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 7.6 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. That procedure is described in "Configuring Configuration Server" on page 97.

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.`

c. To specify the name of the History Log file, do one of the following:

- Specify a file name, and press `Enter.`
- Press `Enter` to select the default name (`histlog`).

13. For the `[soap]` section, do one of the following:

- Specify a value for the SOAP `port,` and press `Enter.`
- Press `Enter` to leave this field blank if you are not using SOAP functionality.

14. For the `[dbserver]` section:

a. Specify the name of the DB Server `host`, and press `Enter.`

b. Specify a value for the DB Server `port,` and press `Enter.`

c. Type the number corresponding to the database engine that this Configuration Server uses (`dbengine`), and press `Enter.`

d. Specify the name or alias of the DBMS that handles the Configuration Database (`dbserver`), and press `Enter.`

e. 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.`

f. Specify the Configuration Database `username,` and press `Enter.`

g. 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 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.

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 "Configuring Configuration Server" on page 97.

On Windows

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

To install the backup Configuration Server on Windows:

1. On the Management Framework 7.6 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, called `setup.exe`, is located in the appropriate directory.
2. 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. 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:
   a. Specify the `Server Port` and `Management Port` for Configuration Server.
   b. Specify the `Log File Name` for the History Log, or accept the default value.
   c. Click `Next`.

8. On the Database Engine Option page, select the database engine used by Configuration Server, and click Next.
9. On the DB Server Parameters page:
   a. Specify the DB Server Host name and DB Server Port.
   b. Specify the Database Server Name and Database Name.
   c. Specify the Database User Name and Password.
   d. 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 in Step 5 on page 163 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 "Configuring Configuration Server" on page 97. For information about

Configuration Server configuration options and their values, refer to the relevant chapters in the *Framework 7.6 Configuration Options Reference Manual.*

Modifying the Primary Configuration Server Application

To enable `warm standby` redundancy for the primary Configuration Server, manually modify the configuration of a primary Configuration Server `Application` object as follows:

1. In Configuration Manager, open the `Properties` dialog box of the Configuration Server Application that you want to configure as a primary server.
2. Click the `Server Info` tab.
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. Click the `Start Info` tab.
6. Select `Auto-Restart.`
7. Click the `Security` tab.
8. In the `Log On As` group section, select `This Account.` Make sure that the account name matches the name of the Master Account.
9. Click `OK` to save the configuration changes.

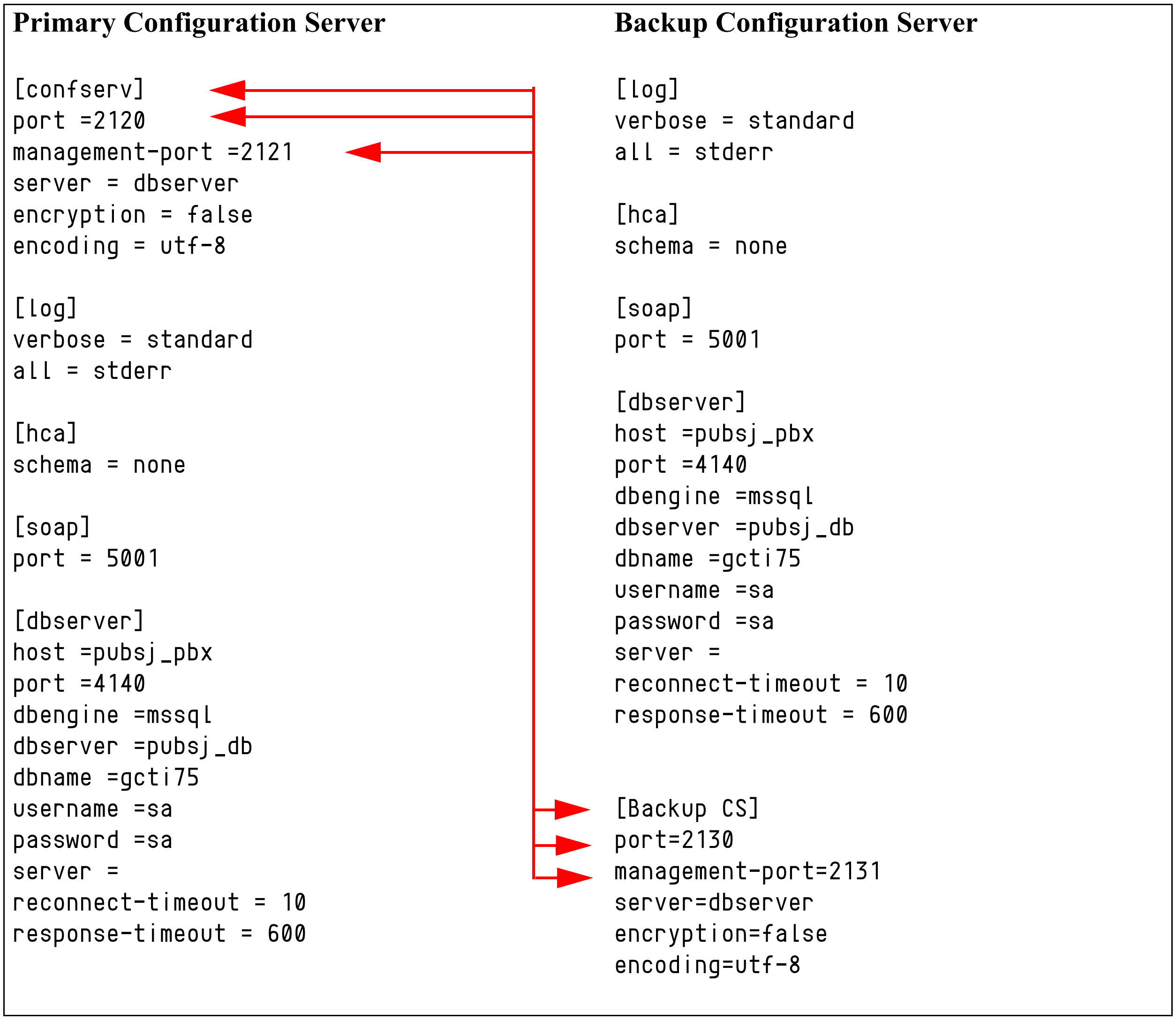
Creating the Configuration File for the Backup Configuration Server

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.

Specify the same database and the same user account for accessing this database, for both the primary and backup Configuration Servers. Note that specifying multiple DB Server sections that describe backup DB Servers is acceptable for the backup Configuration Server, as long as these sections are identical to similar sections in the configuration file of the primary Configuration Server.

Sample configuration files are shown side-by-side in Figure 8 on page 169. The arrows show the differences described in this section.



Primary Configuration Server

```
[confserv]
port =2120
management-port =2121
server = dbserver
encryption = false
encoding = utf-8

[log]
verbose = standard
all = stderr

[hca]
schema = none

[soap]
port = 5001

[dbserver]
host =pubsj_pbx
port =4140
dbengine =mssql
dbserver =pubsj_db
dbname =gcti75
username =sa
password =sa
server =
reconnect-timeout = 10
response-timeout = 600
```

Backup Configuration Server

```
[log]
verbose = standard
all = stderr

[hca]
schema = none

[soap]
port = 5001

[dbserver]
host =pubsj_pbx
port =4140
dbengine =mssql
dbserver =pubsj_db
dbname =gcti75
username =sa
password =sa
server =
reconnect-timeout = 10
response-timeout = 600


[Backup CS]
port=2130
management-port=2131
server=dbserver
encryption=false
encoding=utf-8
```

Figure 8: Sample Configuration Files for Primary and Backup Configuration Servers

Synchronization Between Primary and Backup Configuration Servers

Configuration Manager can automatically synchronize the options and ports between primary and backup Configuration Servers.

Setting Up Options Synchronization

Refer to “Setting Up Options Synchronization Between Primary and Backup Servers” on page 208 for detailed instructions.

Setting Up Ports Synchronization

Refer to “Setting Up Ports Synchronization Between Primary and Backup Servers” on page 209 for detailed instructions.

Setting Up HA Port Synchronization

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 the Advanced Disconnect Detection Protocol (ADDP), described on page 207, for this connection.

Note: Starting with release 7.5, 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.

1. Decide in advance what port on the primary Configuration Server you want to use as the port to which the backup Configuration Server connects. If you want to use a new port, do the following:
   a. On the `Server Info` tab of the properties of both the primary and backup servers, create a new port with the same `Port ID`.
   b. In the `Port Properties` dialog box of each server, click `OK` to save the new configuration.
   c. In the `Application Properties` dialog box of each server, click `Apply`.
2. If you want to use a new or existing port other than the default port of the primary server, do the following:
   a. In the `Application Properties` dialog box of the primary server, select the port to which the backup server will connect, and click `Edit`.
   b. In the `Port Properties` dialog box, select the `HA sync` check box, and click `OK`. The `Port` section of the `Application Properties` dialog box now displays this port as a port for an HA synchronization connection.

Note: If the HA sync check box is not selected, the backup server will connect to the default port of the primary server.

3. Click Apply to save the configuration changes.

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.

Note: Make sure the name of the Configuration Server section is exactly the same as the name of the Application object for the backup Configuration Server.

For a description of the command-line parameters specific to Configuration Server, refer to the section "Configuration Server" on page 144.

On UNIX

To start the backup Configuration Server on UNIX, do one of the following:

- To start from SCI, refer to "Starting and Stopping with the Management Layer" on page 141.
- To start manually, go to the directory where 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

To start the backup Configuration Server on Windows, do one of the following:

- To start as a Windows Service, refer to "Starting and Stopping with Windows Services Manager" on page 153.

- To start from SCI, refer to “Starting and Stopping with the Management Layer” on page 141.
- 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 where 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 where 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>]
```

Redundant Client DB Servers

This section describes how to set up redundant Client DB Servers—that is, DB Servers that provide access to databases other than the Configuration Database (such as the Log Database), and that are clients of Configuration Server (such as Log DB Server).

To set up redundant Configuration DB Servers that are dedicated to provide access to the Configuration Database, and that are not clients of Configuration Server, refer to “Redundant Configuration DB Servers” on page 156.

Note: In this section only, the term *DB Server* denotes a Client DB Server, not a Configuration DB Server.

Redundancy

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

Installation Recommendations

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

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

Prerequisites

Set up redundant Client DB Servers, such as Log DB Servers, only after you have installed and run the following:

- Configuration Layer components as described in Chapter 5 on page 81.
- Management Layer components as described in Chapter 6 on page 103.

Setting Up Redundant DB Servers

To set up redundant DB Servers:

1. Install the backup DB Server, as described in "Installing Log DB Server" on page 115.
2. Configure an Application object for the backup DB Server as described in "Creating the Backup DB Server Application Object".
3. Modify the Application object for the primary DB Server as described in "Modifying the Primary DB Server Application Object" on page 174.

Creating the Backup DB Server Application Object

To create an Application object for the backup DB Server:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a DB Server template is not listed, import the DBServer_<current-version>.apd template file from the Management Framework product CD or use the procedure on page 206 to create a new template, and then repeat this step.
2. In the Browse dialog box, select the DB Server template file, which opens the Properties dialog box for the new DB Server Application object.
3. On the General tab, enter a descriptive name in the Name text box—for example, LogDBS_backup.
4. On the Server Info tab, specify:
   a. The Host on which the backup DB Server is running.
   b. The port that DB Server clients must use to connect to DB Server.
5. On the Start Info tab:
   a. 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 the Backup DB Server" on page 174.

- 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 the backup DB Server starts, but only if the Installation Package can connect to the primary Configuration Server.

b. Select the Auto-Restart check box.

6. Click OK to save the configuration data.

Modifying the Primary DB Server Application Object

To modify the primary DB Server's Application object to work with the backup DB Server:

1. In Configuration Manager, open the Properties dialog box of the DB Server Application object that you want to configure as the primary server.
2. On the Server Info tab:
   - **a.** Use the Browse button to locate and select the Application object corresponding to the backup DB Server you want to use as the backup server.
   - **b.** Select Warm Standby as the redundancy type.
3. On the Start Info tab, select Auto-Restart if required.
4. Click OK to save the configuration changes.

Synchronization Between Primary and Backup DB Servers

Configuration Manager can automatically synchronize the options and ports between primary and backup DB Servers.

Setting Up Options Synchronization

Refer to "Setting Up Options Synchronization Between Primary and Backup Servers" on page 208 for detailed instructions.

Setting Up Ports Synchronization

Refer to "Setting Up Ports Synchronization Between Primary and Backup Servers" on page 209 for detailed instructions.

Starting the Backup DB Server

When starting a backup DB Server, be sure to use the command line parameter -app to specify the name of the backup DB Server application. For a description of the command line parameters specific to DB Server, refer to "DB Server" on page 143.

On UNIX

To start the backup DB Server on UNIX, do one of the following:

- To start from SCI, refer to "Starting and Stopping with the Management Layer" on page 141.
- To start manually, go to the directory where the backup DB 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:

    ```
    multiserver -host <Configuration Server host>
    -port <Configuration Server port> -app <DB Server Application>
    ```

On Windows

To start the backup DB Server on Windows, do one of the following:

- To start as a Windows Service, refer to "Starting and Stopping with Windows Services Manager" on page 153.
- To start from SCI, refer to "Starting and Stopping with the Management Layer" on page 141.
- 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 where the backup DB 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 where the backup DB Server is installed, and type the following command line:

    ```
    multiserver.exe -host <Configuration Server host>
    -port <Configuration Server port> -app <DB Server Application>
    ```

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.

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

Set up redundant Message Servers only after you install and run the Configuration Layer components as described in Chapter 5 on page 81.

Setting Up Redundant Message Servers

To set up redundant Message Servers:

1. Configure an `Application` object for the backup Message Server. See "Configuring an Application Object for the Backup Message Server".
2. Install the backup Message Server.
   - If you are installing the backup Message Server on a remote host, use the Management Framework Deployment Manager (commonly called the Deployment Manager). See Appendix F on page 225 for more information.
   - Otherwise, follow the procedure in "Installing Message Server" on page 121.
3. Modify the primary Message Server `Application` object. See "Modifying the Primary Message Server Application Object" on page 178.
4. If you installed the backup Message Server on UNIX, modify the `run.sh` file by adding the following at the end of the command line in the file:

```
-host <configuration server host> -port <configuration server port>
-app <application object name>
```

Configuring an Application Object for the Backup Message Server

To configure an Application object for the backup Message Server:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a Message Server template is not listed, import the Message_Server_<current-version>.apd file from the Management Framework Product CD or use the procedure on page 206 to create a new template, and then repeat this step.
2. In the Browse dialog box, select the Message Server template file, which opens the Properties dialog box for the new Message Server Application object.
3. On the General tab, enter a descriptive name in the Name text box—for example, MS_backup.
4. On the Server Info tab, specify:
   a. The host on which the backup Message Server is to be installed.
   b. The communication ports that clients must use to connect to this Message Server.
5. On the Start Info tab:
   a. 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 the Backup Message Server” on page 178.
      - 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 Message Server, but only if the Installation Package can connect to the primary Configuration Server.

   b. Select the Auto-Restart check box.
6. Click OK to create the Application object for the backup Message Server.
7. Open the Properties dialog box of the backup Message Server Application object that you just created.
8. On the Security tab, select This Account, making sure that the account name matches the name of the Master Account.
9. Click OK to save the configuration changes.

Modifying the Primary Message Server Application Object

To modify the primary Message Server's `Application` object to work with the backup Message Server:

1. In Configuration Manager, open the `Properties` dialog box of the Message Server `Application` object that you want to configure as the primary server.
2. On the `Server Info` tab:
    a. Use the `Browse` button to locate and select the `Application` object corresponding to the backup Message Server you want to use as the backup server.
    b. Select `Warm Standby` as the redundancy type.
3. On the `Start Info` tab, select `Auto-Restart`.
4. On the `Security` tab, select `This Account`, making sure that the account name matches the name of the Master Account.
5. Click `OK` to save the configuration changes.

Synchronization Between Primary and Backup Message Servers

Configuration Manager can automatically synchronize the options and ports between primary and backup Message Servers.

Setting Up Options Synchronization

Refer to "Setting Up Options Synchronization Between Primary and Backup Servers" on page 208 for detailed instructions.

Setting Up Ports Synchronization Between Primary and Backup Message Servers

Refer to "Setting Up Ports Synchronization Between Primary and Backup Servers" on page 209 for detailed instructions.

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.

If you installed the backup Message Server on UNIX, make sure that you modified the `run.sh` file accordingly (see Step 4 on page 176). For a description of the command line parameters specific to Message Server, refer to “Message Server” on page 147.

On UNIX

To start the backup Message Server on UNIX, do one of the following:

- To start from SCI, refer to “Starting and Stopping with the Management Layer” on page 141.
- To start manually, go to the directory where 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

To start the backup Message Server on Windows, do one of the following:

- To start as a Windows Service, refer to “Starting and Stopping with Windows Services Manager” on page 153.
- To start from SCI, refer to “Starting and Stopping with the Management Layer” on page 141.
- 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 where 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 where 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 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.

Installation 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

Set up redundant Solution Control Servers only after you install and run the Configuration Layer components as described in Chapter 5 on page 81

Setting Up Redundant Solution Control Servers

To set up redundant Solution Control Servers:

1. Configure an `Application` object for the backup SCS. See "Configuring an Application Object for the Backup SCS".
2. Install the backup SCS:
   - If you are installing the backup SCS on a remote host, use the Management Framework Deployment Manager (commonly called the Deployment Manager). See Appendix F on page 225 for more information.
   - Otherwise, follow the procedure in "Installing Solution Control Server" on page 124.
3. Modify the primary SCS `Application` object. See "Modifying the Primary SCS Application Object" on page 181.
4. If you installed the backup SCS on UNIX, modify the `run.sh` file by adding the following to the end of the command line in the file:

   ```
   -host <configuration server host> -port <configuration server port>
   -app <application object name>
   ```

Configuring an Application Object for the Backup SCS

To configure an Application object for the backup SCS:

1. In Configuration Manager, right-click the Environment > Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a Solution Control Server template is not listed, import the solution_Control_Server_<current-version>.apd template file from the Management Framework CD or use the procedure on page 206 to create a new template, and then repeat this step.
2. In the Browse dialog box, select the Solution Control Server template file, which opens the Properties dialog box for the new Solution Control, Server Application object.
3. On the General tab, enter a descriptive name in the Name text box—for example, SCS_backup.
4. On the Server Info tab, specify:
   a. The host on which the backup SCS is to be installed.
   b. The communication ports that clients must use to connect to this SCS.
5. On the Start Info tab:
   a. 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 the Backup SCS” on page 183.
      - 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 SCS, but only if the Installation Package can connect to the primary Configuration Server.

   b. Select the Auto-Restart check box.
6. Click OK to create the Application object for the backup SCS.
7. Open the Properties dialog box of the backup SCS Application object.
8. On the Security tab, select This Account, making sure that the account name matches the name of the Master Account.
9. Click OK to save the configuration changes.

Modifying the Primary SCS Application Object

To modify the primary SCS Application object to work with the backup SCS:

1. In Configuration Manager, open the Properties dialog box of the SCS Application object that you want to configure as the primary server.

2. On the `Server Info` tab:
   a. Use the `Browse` button to locate and select the `Application` object corresponding to the backup SCS you want to use as the backup server.
   b. Select `Warm Standby` as the redundancy type.
3. On the `Start Info` tab, select `Auto-Restart`.
4. On the `Security` tab, select `This Account`, making sure that the account name matches the name of the Master Account.
5. Click `OK` to save the configuration changes.

Synchronization Between Primary and Backup Solution Control Servers

Configuration Manager can automatically synchronize the options and ports between primary and backup Solution Control Servers.

Setting Up Options Synchronization

Refer to "Setting Up Options Synchronization Between Primary and Backup Servers" on page 208 for detailed instructions.

Setting Up Ports Synchronization

Refer to "Setting Up Ports Synchronization Between Primary and Backup Servers" on page 209 for detailed instructions.

Setting Up HA Port Synchronization

When Solution Control Servers operate in a high-availability (HA) environment, the backup SCS must be ready to take on the primary role when required. This requires that both Solution Control Servers are running and that they must have the same information. When you configure redundant Solution Control Servers to operate with the `warm standby` redundancy type, the primary SCS uses the connection to the backup to deliver synchronization updates. Genesys recommends that you enable the Advanced Disconnect Detection Protocol (ADDP), described on page 207, for this connection.

Note: Starting with release 7.5, 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.

1. Decide in advance what port on the primary SCS you want to use as the port to which the backup SCS connects. If you want to use a new port, do the following:
   a. On the `Server Info` tab of the properties of both the primary and backup servers, create a new port with the same `Port ID`.
   b. In the `Port Properties` dialog box of each server, click `OK` to save the new configuration.
   c. In the `Application Properties` dialog box of each server, click `Apply`.
2. If you want to use a new or existing port other than the default port of the primary server, do the following:
   a. In the `Application Properties` dialog box of the primary server, select the port to which the backup server will connect, and click `Edit`.
   b. In the `Port Properties` dialog box, select the `HA sync` check box, and click `OK`. The `Port` section of the `Application Properties` dialog box now displays this port as a port for an HA synchronization connection.

Note: If the `HA sync` check box is not selected, the backup server will connect to the default port of the primary server.

3. Click `Apply` to save the configuration changes.

Starting the Backup SCS

When starting a backup SCS, 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 SCS `Application` object as configured in the Configuration Database.

If you installed the backup SCS on UNIX, make sure that you modified the `run.sh` file accordingly (see Step 4 on page 176). For a description of the command line parameters specific to SCS, refer to “Solution Control Server” on page 148.

On UNIX

To start the backup SCS on UNIX, do one of the following:

- To start from SCI, refer to “Starting and Stopping with the Management Layer” on page 141.
- To start manually, go to the directory where the backup SCS 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

To start the backup Message Server on Windows, do one of the following:

- To start as a Windows Service, refer to “Starting and Stopping with Windows Services Manager” on page 153.
- To start from SCI, refer to “Starting and Stopping with the Management Layer” on page 141.
- 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 where the backup 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 where the backup SCS is installed, and type the following command line:

    ```
    scs.exe -host <Configuration Server host> -port <Configuration
    Server port> -app <Solution Control Server Application>
    [<additional parameters and arguments as required>]
    ```

Redundant SNMP Master Agents

Redundancy

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

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

Set up redundant SNMP Master Agents only after you install and run the Configuration Layer components as described in Chapter 5 on page 81.

Setting Up Redundant SNMP Master Agents

To set up redundant SNMP Master Agents:

1. Configure an `Application` object for the backup SNMP Master Agent. See "Configuring an Application Object for the Backup SNMP Master Agent".
2. Install the backup SNMP Master Agent.
   - If you are installing the backup SNMP Master Agent on a remote host, use the Management Framework Deployment Manager (commonly called the Deployment Manager). See Appendix F on page 225 for more information.
   - Otherwise, follow the procedure in "Installing SNMP Master Agent" on page 130.
3. Modify the primary SNMP Master Agent `Application` object. See "Modifying the Primary SNMP Master Agent Application Object" on page 186.
4. If you installed the backup SNMP Master Agent on UNIX, modify the `run.sh` file by adding the following at the end of the command line in the file:

```
-host <configuration server host> -port <configuration server port>
-app <application object name>
```

Configuring an Application Object for the Backup SNMP Master Agent

To configure an `Application` object for the backup SNMP Master Agent:

1. In Configuration Manager, right-click the `Environment > Applications` folder and select `New > Application`, which opens the `Browse` dialog box with the available Application Templates. If an SNMP Master Agent template is not listed, import the `SNMP_Master_Agent_<current-version>.apd` template file from the Management Framework product CD or use the procedure on page 206 to create a template, and then repeat this step.
2. In the `Browse` dialog box, select the SNMP Master Agent template file, which opens the `Properties` dialog box for the new SNMP Master Agent `Application` object.
3. On the `General` tab, enter a descriptive name in the `Name` text box—for example, `SNMP_MA_backup`.

4. On the Server Info tab, specify:
   a. The host on which the backup SNMP Master Agent is to be installed.
   b. The communication ports that clients must use to connect to this SNMP Master Agent.
5. On the Start Info tab:
   a. 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 the Backup SNMP Master Agent” on page 187.
      - 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 SNMP Master Agent, but only if the Installation Package can connect to the primary Configuration Server.
   b. Select the Auto-Restart check box.
6. Click OK to create the Application object for the backup SNMP Master Agent.
7. Open the Properties dialog box of the backup SNMP Master Agent Application object.
8. On the Security tab, select This Account, making sure that the account name matches the name of the Master Account.
9. Click OK to save the configuration data.

Modifying the Primary SNMP Master Agent Application Object

To modify the primary SNMP Master Agent’s Application object to work with the backup SNMP Master Agent:

1. In Configuration Manager, open the Properties dialog box of the SNMP Master Agent Application object that you want to configure as the primary server.
2. On the Server Info tab:
   a. Use the Browse button to locate and select the Application object corresponding to the backup SNMP Master Agent you want to use as the backup server.
   b. Select Warm Standby as the redundancy type.
3. On the Start Info tab, select Auto-Restart.
4. On the Security tab, select This Account, making sure that the account name matches the name of the Master Account.
5. Click OK to save the configuration changes.

Synchronization Between Primary and Backup SNMP Master Agents

Configuration Manager can automatically synchronize the options and ports between primary and backup SNMP Master Agents.

Setting Up Options Synchronization Between Primary and Backup SNMP Master Agents

Refer to "Setting Up Options Synchronization Between Primary and Backup Servers" on page 208 for detailed instructions.

Setting Up Ports Synchronization Between Primary and Backup SNMP Master Agents

Refer to "Setting Up Ports Synchronization Between Primary and Backup Servers" on page 209 for detailed instructions.

Starting the Backup SNMP Master Agent

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 SNMP Master Server `Application` object as configured in the Configuration Database.

If you installed the backup SNMP Master Server on UNIX, make sure that you modified the `run.sh` file accordingly (see Step 4 on page 185). For a description of the command-line parameters specific to SNMP Master Agent, refer to "SNMP Master Agent" on page 150.

On UNIX

To start the backup SNMP Master Agent on UNIX, go to the directory where Genesys 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 <SNMP Master Agent Application>
[<additional parameters and arguments as required>]
```

On Windows

To start 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" on page 153.
- To start from SCI, refer to "Starting and Stopping with the Management Layer" on page 141.
- 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 where 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 where 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>]
    ```

Chapter

10 Setting Up Geographically Distributed Systems

This chapter describes Genesys Framework support for geographically distributed systems. This chapter also describes how to set up Configuration Server Proxy and Distributed Solution Control Servers, and how to configure their clients to work with them.

This chapter contains the following sections:

Overview

Large enterprises often run contact-center operations at numerous locations world-wide. 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.

However, by operating two Framework components in different modes you can somewhat simplify the operation of a geographically distributed installation using a single Configuration Database:

- Use Configuration Server operating in Proxy mode (referred to as *Configuration Server Proxy*) in addition to the master Configuration Server to distribute configuration-related tasks among the sites.

- Operate two or more Solution Control Servers in Distributed mode (referred to as *Distributed Solution Control Servers*), to distribute management-related tasks among the sites.

Licensing Requirements

Starting Configuration Server in Proxy mode or Solution Control Server in Distributed mode requires special licenses. Refer to the *Genesys 7 Licensing Guide* for more information.

Architecture

Figure 9 shows how Configuration Server Proxy and Distributed SCS fit into a Genesys configuration environment.

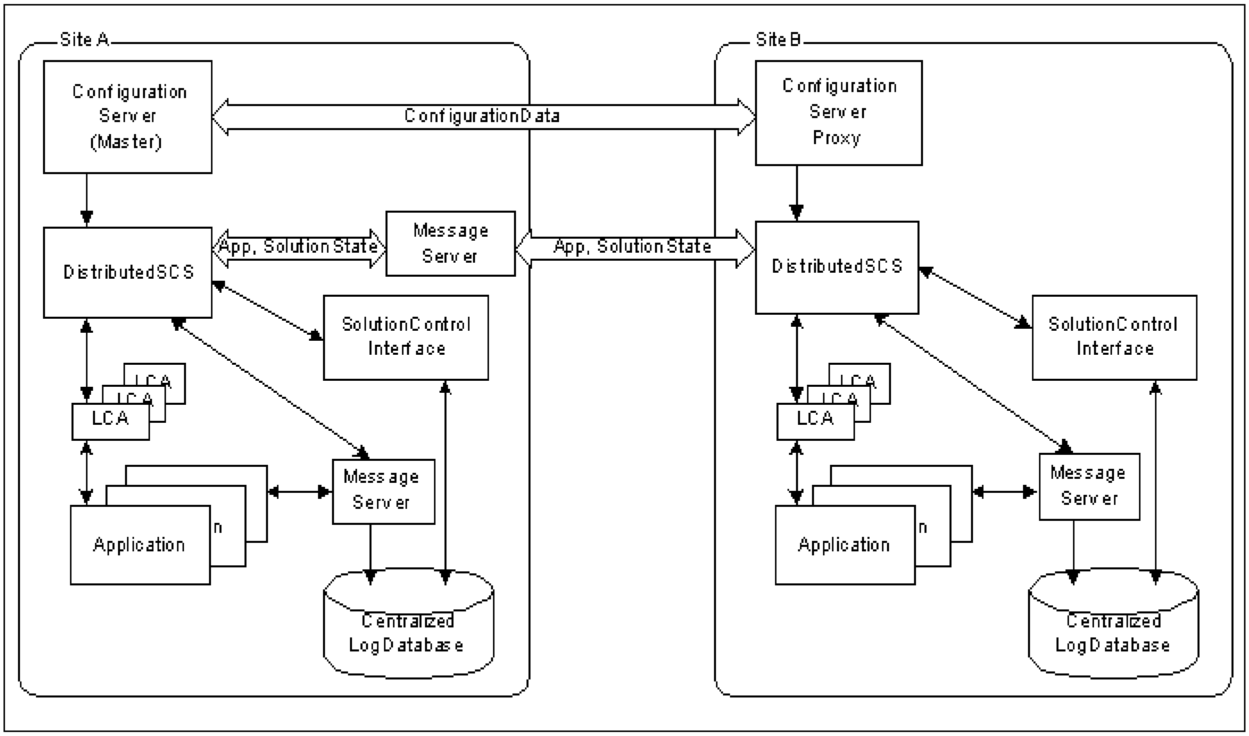


Figure 9: Geographically Distributed Installation

Configuration Server Proxy Functions

Configuration Server Proxy:

- 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.

Note: 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.

Distributed Solution Control Server Functions

Distributed Solution Control Server:

- 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 SCSs, using a dedicated Message Server.
- Receives notifications about updates to the status of non-assigned objects (that is, objects assigned to other SCSs) from Message Server.
- When receiving a control command on an object not assigned to this SCS, forwards this commands to the appropriate SCS, using Message Server.

When to Use This Architecture

Genesys recommends using Configuration Server Proxy and Distributed Solution Control Server in a multi-site and/or multi-tenant environments. Using Configuration Server Proxy in a single-site environment does not reduce network traffic or increase system robustness.

Configuration Server Proxy

In a geographically 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.

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, clients continue their operations, and new clients can start theirs, when Configuration Server fails. Also, after Configuration Server recovers, the client reconnect takes far less time than if all clients were directly connected to Configuration Server.

Note: If external authorization is used, all client authorization occurs at the Master Configuration Server. Therefore, a live connection is required between Configuration Server Proxy and the Master Configuration Server.

In Genesys configuration terms, Configuration Server Proxy is an application of the Configuration Server type operating in a special mode. As a such, it replaces Configuration Server seamlessly for the clients. However, Configuration Server Proxy provides read-only access to configuration data. Therefore, Configuration Server clients that require write access to Configuration Server (such as Configuration Manager, Deployment Wizards, and some others) must still connect directly to Configuration Server.

Note: Configuration Server Proxy 7.6 is compatible with releases 6.x and 7.x of Genesys applications, including Configuration Server.

You can also configure Configuration Server Proxy permissions so that clients of a particular proxy access only the part of configuration environment relevant to their site. See "Security Considerations" on page 61 and *Framework 7.6 Configuration Manager Help* for more information about setting permissions.

Deploying Configuration Server Proxy

Configuration Server 7.6 operating in Proxy mode provides the same functionality as the 7.0 release of Configuration Server Proxy. Beginning with the 7.0 release of Configuration Server, Configuration Server 7.6 operating in Proxy mode is now referred to as *Configuration Server Proxy.*

The setup process involves:

1. Configuring as many instances of Configuration Server Proxy as needed, as described in "Configuring Configuration Server Proxy" on page 193.
2. Installing the corresponding number of Configuration Server Proxies.
   - If you are deploying an instance on a remote host, use Management Framework Deployment Manager. See Appendix F on page 225 for instructions.
   - Otherwise, install the instance manually, as described in "Installing Configuration Server Proxy" on page 194.

3. Modifying Configuration Server clients accordingly, as described in “Modifying Client Applications” on page 196.

Configuring Configuration Server Proxy

To configure a Configuration Server Proxy Application object:

1. In Configuration Manager, right-click the Applications folder and select New > Application, which opens the Browse dialog box with the available Application Templates. If a Configuration Server Proxy template is not listed, either import the Configuration Server Proxy_<current-version>.apd file from the Management Framework product CD or use the procedure on page 206 to import it, and repeat this step.
2. In the Browse dialog box, select the Configuration Server Proxy template file, which opens the Properties dialog box for the new Configuration Server Proxy Application object.
3. On the General tab, enter a name for the Configuration Server Proxy Application.
4. On the Server Info tab, specify:
   a. the host on which the Configuration Server Proxy is to be installed.
   b. the communication ports that clients must use to connect to this Configuration Server Proxy.
5. On the Connections tab, add a connection to the Configuration Server Application object (confserv). If redundant Configuration Servers are configured, specify a connection to the primary Configuration Server.
6. On the Start Info tab, 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 Chapter 8 on page 139.
   - 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 primary Configuration Server.
7. (Optional) On the Options tab, set the values of the log configuration options.
8. Click OK to save the configuration changes.

Installing Configuration Server Proxy

On UNIX

To install Configuration Proxy on UNIX:

1. On the Management Framework 7.6 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 `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 on page 193, 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`.
    - 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

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

To install Configuration Server Proxy on Windows:

1. On the Management Framework 7.6 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. The 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 on page 193, 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, use the:

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

Modifying Client Applications

Identify the Configuration Server clients that should operate with a particular Configuration Server Proxy. Change each client configuration as follows:

1. In Configuration Manager, open the Properties dialog box of the client Application object that you want to connect to Configuration Server Proxy.
2. Click the Connections tab.
3. Add a connection to the Configuration Server Proxy to which the client application should connect.
4. Click Apply and OK to save the configuration changes.

Now, when you start the client application, it will now operate with the given Configuration Server Proxy. You can start the client application using one of the following methods:

- From Solution Control Interface.
- From the command line. In this case, you must use the parameters -host and -port to point to Configuration Server Proxy with which the application will be operating. This must be specified for each application that will be operating with Configuration Server Proxy.

Starting Configuration Server Proxy

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. For a description of these parameters, refer to Chapter 8 on page 139.

Note: 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

Go to the directory where 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 [<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 where 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 where Configuration Server Proxy is installed, and type the following command line:

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

Configuring 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. The redundant architecture is described in the *Framework 7.6 Architecture Help*.

The instructions in this section assume that you have already configured and installed one Configuration Server Proxy.

To set up redundant Configuration Server Proxies:

1. Configure an `Application` object for the backup Configuration Server Proxy following the procedure described in "Configuring Configuration Server Proxy" on page 193.
2. Install a backup Configuration Server Proxy following the procedure described in "Installing Configuration Server Proxy" on page 194.
3. In Configuration Manager, open the `Properties` dialog box of the Configuration Server Proxy Application that you want to configure as a primary server.
4. Click the `Start Info` tab.
5. Select `Auto-Restart`.
6. Click the `Server Info` tab.
7. Select `Warm Standby` as the Redundancy Type.
8. Specify the Configuration Server Proxy Application you want to use as the backup server. Use the Browse button next to the `Backup Server` property field to locate the backup Configuration Server Proxy Application.
9. Click `Apply` and `OK` to save the configuration changes.

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 Configuration Server

When 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 Configuration Server. Meanwhile, Configuration Server Proxy responds to client requests using the configuration data stored in its memory.

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

Figure 10 on page 199 shows Configuration Server Proxy behavior when a primary-backup pair of Configuration Servers is configured.

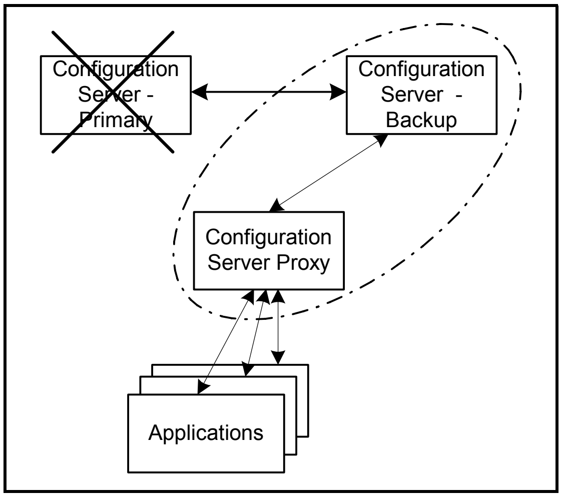

Configuration Server - Primary
Configuration Server - Backup
Configuration Server Proxy
Applications

Figure 10: Failure of Configuration Server with a Configured Backup

When the primary Configuration Server fails or the connection to it is lost, Configuration Server Proxy initiates reconnect attempts to 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

In a geographically distributed configuration environment, a number of Solution Control Servers can communicate with each other and control a particular part of the Genesys environment while running at multiple remote sites (but within the same configuration environment).

You can install and use more than one Distributed Solution Control Server within a single configuration environment. In such installations, each such server controls its own subset of the Host, Application, and Solution objects. Distributed SCSs communicate with each other through the dedicated Message Server.

When you are using Distributed SCSs, you must explicitly configure the servers' ownership of Hosts, Applications, and Solutions: you must associate each Host, Application, and Solution with a particular SCS. For instructions on relevant configuration and activating Distributed mode, refer to the *Framework 7.6 Management Layer User's Guide.*

Using Distributed SCSs helps you resolve some problems common to geographically distributed installation:

- 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 SCSs continue controlling 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. Thus, you can connect Solution Control Interface to any such server to monitor and control the whole environment as a single entity (given appropriate permissions).

SCS in Distributed Mode

Starting with release 7.0, you can use Solution Control Server operating in `Distributed` mode (referred to as *Distributed Solution Control Server*) to distribute management-related tasks among the sites in a geographically distributed enterprise that uses a single Genesys Configuration Database.

You can install and use more than one Distributed Solution Control Server within a single configuration environment. In these installations, each such server controls its own subset of the Hosts, Applications, and Solutions. Distributed Solution Control Servers communicate with each other through the dedicated Message Server.

When you are using Distributed SCSs, you must explicitly configure the servers' ownership of Hosts, Applications, and Solutions: you must associate each Host, Application, and Solution object with a particular SCS.

Using Distributed SCSs helps you resolve some problems common to geographically distributed installation:

- 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 SCSs 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. Thus, you can connect Solution Control Interface to any Distributed SCSs and monitor and control the whole environment as a single entity (given appropriate permissions).

The following sections provide instructions on ownership configuration and on activating Distributed mode.

Note: Starting Solution Control Server in Distributed mode requires a special license. Refer to the *Genesys 7 Licensing Guide* for more information.

Configuring Solution Control Servers

To adjust configuration of multiple Solution Control Servers:

1. In the Configuration Database, configure as many Solution Control Server `Application` objects as necessary.
2. For each Solution Control Server Application, turn on Distributed mode. To do so, specify the following values for configuration options within the `general` section on the `Options` tab:
   - Set the `distributed_mode` option to `ON`
   - Set the `distributed_rights` option to `DEFAULT`
3. If you are planning to leave any of the Host, Application, and Solutions 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, specify the following values for configuration options within the `general` section on the `Options` tab for that particular Solution Control Server Application:
   - Set the `distributed_mode` option to `ON`
   - Set the `distributed_rights` option to `MAIN`.

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

Warning! You cannot 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 SCSs you install.

Redundant Configurations for Distributed SCS

Distributed SCS supports 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.

To set up HA port synchronization between Primary and Backup Solution Control Servers, refer to “Setting Up HA Port Synchronization” on page 182.

Dividing Configuration Among SCSs

When you are using Distributed Solution Control Servers, you must specify which SCS controls which subset of the following objects:

- Hosts
- Applications
- Solutions

Do this in the object's `Properties` dialog box in Configuration Manager as described in the following sections.

Note: To distribute control over the primary and backup servers in a redundant pair between different Distributed SCSs, all SCSs in the configuration must be running release 7.5 or later.

Host Ownership

To assign a Distributed SCS to control a Host, specify the SCS application in the `Solution Control Server` field on the `General` tab of the `Host` object.

Application Ownership

You do not have to make any changes to the `Application` object in order to assign a Distributed SCS to control an Application. Specifying SCS ownership of the Application's Host suffices. The Distributed SCS automatically controls any Applications assigned to the Host this SCS controls.

Solutions Ownership

To assign a Distributed SCS to control a Solution, specify the SCS Application in the `Solution Control Server` field on the `General` tab of the Solution object.

Recommendations

- Do not distribute control over the primary and backup servers in a redundant pair between different Distributed SCSs 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 Distributes SCSs, ensure that the same SCS that controls a Solution also controls all Applications included in this Solution. While one SCS can technically control a Solution while other servers control Applications

included in that Solution, avoiding this configuration helps minimize network traffic between SCSs.

Specifying Message Server for SCS Communications

Distributed Solution Control Servers communicate with each other through Message Server. Genesys recommends that you use a dedicated Message Server for this purpose and configure it as follows:

1. In the Configuration Database, configure a Message Server `Application` object with appropriate configuration parameters.
2. Go to the `Options` tab of the Message Server `Application Properties` dialog box and create a new section called `MessageServer`.
3. Within this section, create a new configuration option called `signature` and set its value to `scs_distributed`. Each Distributed SCS processes this option to determine which of the Message Servers specified in SCS connections to use for communications with other SCSs.
4. Add this Message Server Application to the `Connections` tab for all `Application` objects configured for Distributed SCSs.

   For each new connection, enter `ADDP` as the `Connection protocol`. Set the ADDP `Local Timeout` and `Remote Timeout` to values that are less than half the minimum `alive_timeout` values between all Distributed SCSs 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 SCSs

Notes on Configuring SCI

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 Solution Control Interface to any Distributed SCS and monitor and control the whole environment as a single entity (given appropriate permissions).

When 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.

Notes on Configuring Message Server

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

Note: You also need an additional Message Server to handle SCS communications (see page 203).

After you configure all Message Server Application objects, check the configuration in Configuration Manager:

1. Open the Properties dialog box for a particular SCS Application.
2. Make sure that a connection to a corresponding Message Server is added to the SCS Connections tab.
3. Open the Properties dialog box for each Application that this particular SCS controls.
4. Make sure that a connection to the corresponding Message Server is added to the Application's Connections tab.

Note: You can configure as many Message Servers for centralized logging as you need per site.

Installing Applications

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

Redundancy Support

Both Configuration Server Proxy and Distributed Solution Control Server currently support warm standby redundant configuration in the same way as other Genesys servers. That is, you can configure a primary and a backup Configuration Server Proxy or Distributed SCS to operate with warm standby redundancy, so that if the primary application fails, the backup can take over current operations. The backup Distributed SCS synchronizes its data with the primary SCS; however, the backup Configuration Server Proxy does not.

Distributed SCS can handle switchovers between other redundant client applications, regardless of the redundancy type configured for those other applications. For example, redundant T-Servers can be configured as hot standby, whereas redundant Universal Routing Servers can be configured as warm standby. Distributed SCS will handle the switchover for both applications.

Appendix

A Standard Configuration Procedure

This appendix provides generic instructions for using Configuration Manager to configuring a Genesys Framework Application object.

This appendix contains the following sections:

Refer to instructions for a particular application for any application-specific deviations from the standard configuration procedure.

Importing Application Templates

Before you configure an Application object, import a template for this application. This template provides a majority of the configuration options for server applications and the option default values.

To import an application template:

1. In Configuration Manager, select the Environment > Application Templates folder.
2. Select File > Import > Application Template.
3. Click the down arrow for the Look In field.
4. Locate the installation CD for your particular product and open the TEMPLATES folder.
5. Select the template file for your particular application.
6. Click Open to open the Properties dialog box for this template.
7. Make any changes that you require, then click OK to save them and to exit the Properties dialog box.

Using one application template, you can create as many Application objects of the same type as you need.

Creating Application Templates

1. In Configuration Manager, select File > New > Application Template.
2. Specify the template name and select values for template properties.
3. Click OK to save your changes and to exit the Properties dialog box.

Configuring Server Applications

1. In Configuration Manager, select the Environment > Applications folder.
2. Select File > New > Application.
3. From the available application templates in the Browse dialog box, choose the template you imported for this application. (See “Importing Application Templates” on page 205 for instructions on importing a template.)
4. Select the General tab of the Properties dialog box and enter a name for this application. The application template provides information for the application type and version.
5. The Tenants tab displays only in a multi-tenant environment. You can add tenants for this application by selecting the Tenants tab and clicking the Add button.
6. Select the Server Info tab and specify the:
   - Host computer on which this server is to be installed and/or to run.
   - One or more communication ports that applications must use to connect to this server.
7. If another server application is used as a backup for this one, specify the Redundancy Type and the Backup Server on the Server Info tab.

   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 7 Licensing Guide* for details.

   Note: See page 208 for information about enabling option synchronization between the primary and backup servers.

8. Select the Start Info tab and define the:
   - 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 these properties are updated automatically during the application's installation procedure.

9. Select the Options tab and specify/change the values of the configuration options. For option descriptions, see:
   - The *Framework 7.6 Configuration Options Reference Manual* for Configuration and Management Layer components' options.
   - The latest version of the *Framework T-Server Deployment Guide* for your specific T-Server and HA Proxy (if applicable) options.
   - The latest version of the *Framework Stat Server User's Guide* for Stat Server options.

   If the application's working directory differs from the directory to which the application is 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.
10. Select the Connections tab:
    - Add a connection to any server application this application should be a client to. To enable Advanced Disconnect Detection Protocol (ADDP) for this connection, see "Configuring ADDP" on page 207.
    - To enable ADDP between this server and Configuration Server, add the Configuration Server Application (named confserv) to the Connections and specify the values for the connection protocol in seconds (see "Configuring ADDP" on page 207.) For more information, refer to *Framework 7.6 Configuration Manager Help.*
    - Add a connection to Message Server to provide alarm-signaling and centralized-logging capabilities.

Note: You can add a connection to Message Server for all or a set of Application objects after you configure them. To launch a Wizard that configures connections for multiple Application objects, select two or more Application objects, right-click, and select Manage Connections. Refer to *Framework 7.6 Configuration Manager Help* for more information.

11. Click OK to save your changes and to exit the Properties dialog box.

Configuring ADDP

You can enable the Advanced Disconnect Detection Protocol (ADDP) for a connection between any two Genesys applications that support ADDP.

Note: Some applications do not support ADDP for certain connections. Refer to documentation or Release Notes to find this information for particular applications.

To configure ADDP-related parameters for a connection between two applications that form a client-server pair:

1. In Configuration Manager, open the `Application Properties` dialog box for the client application in the client-server pair.
2. Select the `Connections` tab.
3. Double-click the Application name that represents the connection for which you want to configure ADDP.
4. In the `Connection Properties` dialog box that opens:
   a. Specify `addp` as the value for the `Connection Protocol` field.
   b. 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.

   Note: Genesys recommends setting the ADDP timeouts to values equal to or greater than 10 seconds.

   c. 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.
   d. If you do not want either the client or the server application to print ADDP-related messages in its log, select the `Trace Is Turned Off` value for the `Trace Mode` field. Otherwise, do one of the following:
      - Select `Trace On Client Side` for the client application to print ADDP-related messages in its log.
      - Select `Trace On Server Side` for the server application to print ADDP-related messages in its log.
      - Select `Trace On Both Sides` for both client and server applications to print ADDP-related messages in their log.

Setting Up Options Synchronization Between Primary and Backup Servers

Using Configuration Manager, you can synchronize the options between primary and backup applications. You need to complete two tasks before Configuration Server can perform this procedure:

1. Assign an Application Template to the primary server before using that template for a backup server. (This is the default behavior for Configuration Manager, but not for Wizards.)

2. Set up the Application Template's Annex properties as follows:

   List the options that you want synchronized between the corresponding Application objects. You must list both the section and option names exactly as they appear in the primary Application. *However*, instead of entering the actual option values, use one of two flags:

   - Use 1 to indicate that the corresponding option in the primary server should be copied into the backup server only at the moment when the backup is assigned to the primary. This leaves the option available for later independent changes in the primary and backup servers.
   - Use 2 to indicate that Configuration Server should not only copy the option to the backup during its assignment to the primary, but also that it should synchronize the options any time that the option is changed on the primary server.

Setting Up Ports Synchronization Between Primary and Backup Servers

Configuration Manager can automatically synchronize the ports between primary and backup server applications. To set up automatic port synchronization:

1. In Configuration Manager, select View > Options to open the Options dialog box.
2. On the General tab, in the Server Ports Assignment section:
   a. Select Auto, and enter a starting number for the range of port numbers that will automatically be assigned for ports on server applications.
   b. Select Auto For Backup, and enter the first number of a range of ports that will automatically be assigned on backup applications.
3. Click OK.

When the Auto For Backup option is selected, ports are automatically synchronized between the primary and backup server 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.

Refer to *Framework 7.6 Configuration Manager Help* for more information.

Configuring GUI Applications

To configure an Application object for a GUI application:

1. In Configuration Manager, select the Environment > Applications folder.

2. Select File > New > Application.
3. From the available application templates in the Browse dialog box, choose the template you imported for this application. (See “Importing Application Templates” on page 205 for instructions on importing a template.)
4. Select the General tab of the Properties dialog box and enter a name for this Application in the text box. The application template provides information for the application type and version.
5. Select the Connections tab. If necessary, add connections to any server applications to which this GUI application must connect.
6. Click OK to save your changes and to exit the Properties dialog box.

Appendix

B Standard Installation Procedure

This appendix provides instructions for installing a typical Genesys application that you have configured using Configuration Manager.

This appendix contains the following sections:

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.

Refer to Appendix F, "Management Framework Deployment Manager" on page 225, for instructions on the remote installation procedure.

Installing Server Applications

This section describes a standard installation procedure for a server application on UNIX and Windows operating systems.

Installing 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.

1. Insert the product CD with this application into the CD-ROM drive of the application host computer.

2. In the appropriate directory, locate a shell script called `install.sh`.
3. Run this script from the command prompt by typing the file name.
4. When prompted, specify the `Host Name` of the computer on which this server is to run.
5. 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.
6. The installation displays the list of Applications of the specified type configured for this Host. Type the number of the server Application that should be installed.
7. Specify the destination directory into which this server is to be installed, with the full path to it.

   If the installation script finds that the destination directory is not empty, it suggests that you:
   - 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.
8. If asked which version of the product to install, either the 32-bit or the 64-bit, choose the one appropriate to your environment.
9. 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 be prepared to give either the full path to the license file or 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.

Installing on Windows

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

After you create an `Application` object for your server application using Configuration Manager, install your application as follows:

1. From the product CD with this server application, open 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. 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.

Note: Click `Next` at the end of each step to proceed to the next page.

5. 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.
6. 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.

Note: If the component does not require a technical license, omit Steps 7 and 8. If the component requires a technical license for startup, omit Step 7. If the component requires a technical license to enable a certain feature, but the license is not otherwise required, proceed with Step 7.

7. 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, proceed with Step 9.

Note: If you decide to use a licensed feature later on, reinstall the server and enter the appropriate license information through the Genesys Installation Wizard.

8. On the `Access to License` page, select one of the following options:
   - `License Manager` if you want your server application to use host name and port number parameters to connect to the license server. In this instance, you must enter values for `host` and `port` of license server.
   - `License File` if you want your server application to retrieve license server information from the license file. Use the `Browse` button to navigate to the license file.

9. 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.

   If necessary, use the:

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

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

    - Back to update any installation information.
    - Install to proceed with installation. Installation Status displays the installation progress.

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

Installing GUI Applications

This section describes a standard installation procedure for a GUI application on Windows operating systems. Genesys GUI applications are designed to operate on Windows only.

If you want to implement a security banner with the Genesys GUI application, make sure that you have the necessary files prepared before you start installing the GUI application. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information about the security banner.

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

After you create an Application object for your GUI application using Configuration Manager, install your application as follows:

1. From the product CD with this application, open 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. The file also contains a link to the application's Release Notes file.

4. Click Next to proceed with the installation.
5. On the Security Banner Configuration page, choose whether you want to configure a security banner for this GUI application. Refer to the *Genesys 7.6 Security Deployment Guide* for detailed information about the security banner. Do one of the following:
   - If you do not want to configure a security banner for this application, clear the Enable Security Banner checkbox if it is selected, then click Next.
   - If you want to configure a security banner for this application:
     - **a.** Select Enable Security Banner.
     - **b.** Follow the instructions in the procedure “Installing and configuring the Security Banner” in the *Genesys 7.6 Security Deployment Guide.* When you are finished that procedure, return here and finish this procedure.
6. 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.

Note: If the GUI application requires any nonstandard installation input from the user, extra pages appear here.

7. On the Ready to Install page, click:
   - Back to update any installation information.
   - Install to proceed with the installation. Installation Status displays the installation progress.
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.
   - Windows Add or Remove Programs window, as a Genesys application.

Troubleshooting the Installation

If, during the installation procedure for any of Genesys applications, the script warns you that Configuration Server is unavailable and that configuration cannot be updated, continue with the installation. After completing the installation:

1. Open the Properties dialog box for a corresponding Application object in Configuration Manager.
2. Select the State Enabled check box on the General tab.
3. Verify that the Working Directory, Command Line, and Command Line Arguments are specified correctly on the Start Info tab.
4. Click Apply and OK to save the configuration updates.

Appendix

C Login Procedure

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.

In a `Login` dialog box:

1. 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 Person type are added to the configuration, use a customized user name.
2. 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 Person type are added to configuration, use a customized password.

   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 7.6 Configuration Options Reference Manual* for information about configuring this functionality.
3. Click `Details` if the Details pane is not displayed.
4. Enter the Application name, which is the instance of the application you are logging in to as it is registered in the Configuration Database.

Note: The predefined name of the Configuration Manager `Application` object is `default`. You can rename it later.

5. Enter a host name, which is the name of the computer on which Configuration Server runs.
6. 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, then Configuration Manager and Solution Control Interface automatically reconnect to the backup server if they lose their connection to the primary server. For Configuration Manager, you can specify automatic or manual reconnection in the Configuration Manager View menu. See the Configuration Manager Help topic `View Menu`.

Appendix

D Windows Services

Starting with release 7.1.0, the Genesys setup procedures on Windows operating systems automatically install Genesys daemon applications as Windows Services, with the autostart capability.

For more information regarding Windows Services, see “Starting and Stopping with Windows Services Manager” on page 153.

Appendix

E Silent Setup

This appendix describes the purpose and configuration of Silent Setup.

This appendix contains the following sections:

Introduction

InstallShield Silent allows for an automated electronic software distribution, also known as a *silent setup.* InstallShield Silent only works on Windows operating systems. With InstallShield Silent, you do not have to monitor the setup or provide input via dialog boxes. Once this information is stored in a *response file,* an InstallShield 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 create a response file with the necessary parameters and then use it for the actual installation.

The following Framework components support Silent Setup installation:

- DB Server
- Configuration Server
- Configuration Manager
- Message Server
- Solution Control Server
- Solution Control Interface
- T-Server

- HA Proxy
- Stat Server

Creating the Response File

To select setup options and automatically record the InstallShield Silent response file, run your setup with the following command line:

```
setup -r
```

Your responses to the dialog boxes are recorded and used to create a response file. By default, the response file is named `Setup.iss,` and is stored in the `Windows` directory of your computer. To specify a different directory or file name for the response file, add `/f1"[full_path to iss file\]<FileName>"` to the setup command. Include the double quotes and do not put a space between `/f1` and the path—for example:

```
setup ·r /f1"C:\GCTI\silent_response_files\mySetup.iss"
```

Note: In the optional argument, the `/f1` portion uses the numeral one (`1`), not the letter `l`.

Subsequently, use the response file any time you need to install an application with the configured parameters.

Sample Response File (setup.iss)

```
[InstallShield Silent]
Version=v5.00.000
File=Response File
[File Transfer]
OverwriteReadOnly=NoToAll
[DlgOrder]
Dlg0=SdWelcome-0
Count=4
Dlg1=SdAskDestPath-0
Dlg2=SdSetupTypeEx-0
Dlg3=SdFinishReboot-0
[SdWelcome-0]
Result=1
[SdAskDestPath-0]
szDir=C:\GCTI\TestSiebel2KSilentMode
Result=1
[SdSetupTypeEx-0]
Result=typical
[Application]
Name=G-Plus Adapter 6.5 for Siebel 2000
Version=6.5
Company=GCTI
```

```
Lang=0009
[SdFinishReboot-0]
Result=1
BootOption=0
```

The response file contains saved information about the number of dialog boxes displayed, the order in which the dialog boxes were displayed, the values of any data entered or selected by the end user, and which button the user clicked to close the dialog box.

Running the Silent Installation

Launch the InstallShield Silent Installation with this command line:

```
Setup.exe -s /f1"<full path to Setup.iss>" /f2"<full path to setup log
file>"
```

Where:

`<full path to Setup.iss>`
The full path to the Setup.iss file put within double quotation marks. For example: "`c:\winnt\setup.iss`" (by default, Setup.exe looks for a response file called Setup.iss in the same directory as Setup.exe)

`<full path to setup log file>`
The full path to the setup log file put within double quotation marks. For example: "`c:\winnt\setup.log`" (by default, setup.log generated in the same directory as the response file being used)

A silent installation program does not display a dialog if an error occurs. The status information for the silent installation is recorded (by default) in a file called **setup.log**.

Note: Do not enter a space between the f1 or f2 parameter and its value in double quotation marks.

The log file generated as a result of the Silent Setup procedure is described in the following section.

About the Silent Setup Log File

InstallShield Silent prints installation results into a setup log file.

The default name for the silent setup log file is `Setup.log`, and its default location is on Disk1, in the same folder as `Setup.iss`. You can specify a different name and location for you setup log file using the f2 switch when launching `Setup.exe`.

The Setup.log file contains three sections. The first entry in the first section, `[InstallShield Silent]`, identifies the version of InstallShield Silent used in the silent setup. The second entry identifies the file as a log file.

Entries in the second section, `[Application]`, identify the installed application's name and version and the company name.

The third section, `[ResponseResult]`, contains the result code indicating whether the silent setup has succeeded. One of the following integer return values is assigned to the `ResultCode` key name in this section:

0	Success.
-1	General error.
-2	Invalid mode.
-3	Required data not found in the Setup.iss file.
-4	Not enough memory.
-5	File does not exist.
-6	Cannot write to the response file.
-7	Unable to write to the uninstallation log file.
-8	Invalid path to the InstallShield Silent response file.
-9	Not a valid list type (string or number).
-10	Data type is invalid.
-11	Unknown error during setup.
-12	Dialog boxes are out of order.
-51	Cannot create the specified folder.
-52	Cannot access the specified file or folder.
-53	Invalid option selected.

Sample Setup Log File

The `Setup.log` file for a T-Server application successfully installed with InstallShield Silent is shown below.

```
[InstallShield Silent]
Version=v5.00.000
File=Log File
[Application]
Name=Genesys T-Server 7.0 for Rockwell Spectrum
Version=7.0
Company=GCTI
Lang=0009
[ResponseResult]
ResultCode=0
```

Appendix

F Management Framework Deployment Manager

This chapter describes how to install the Genesys Management Framework Deployment Manager, and how to install Framework components using the Deployment Manager.

This chapter contains the following sections:

Introduction

The Management Framework Deployment Manager (also referred to as *Deployment Manager*), introduced in release 7.1, allows you to deploy certain Framework components to remote, unattended hosts.

Note: The remote host must run a Genesys-supported operating system.

This chapter uses the terms *local host* and *target host* as follows:

- Local host—the computer on which Deployment Manager is running and from which you perform the remote installation.
- Target host—the remote computer to which a given Framework component is to be installed.

Deployment Manager Tasks

The Deployment Manager provides wizards that guide you through deployment of the following Framework components on the target host:

- DB Server
- Configuration Server
- Solution Control Server
- Local Control Agent
- Message Server
- Solution Control Interface

Note: You can also use Solution Control Interface to launch wizards for the above components. In particular, starting a wizard from the `Host` shortcut menu allows you to install an application of the specified type on the currently selected host. Refer to *Framework 7.6 Solution Control Interface Help* for more information.

You can use the Deployment Manager to deploy components with or without a connection to Configuration Server. If the Deployment Manager is connected to Configuration Server, it allows you to select from the list of applications of a given type configured for the target host to which you want to deploy an application. Deployment Manager also updates the settings of the selected application with data that you specify during deployment process.

Note: Deployment Manager allows you to deploy only one instance of a component to a single target host using the Windows operating system. If you attempt a second installation of a component to that same host, the wizard for this component prompts you to either cancel deployment or reinstall the component.

Installing and Starting Deployment Manager

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

To deploy Framework components to a remote, unattended computer, install the Management Framework Deployment Manager, which is designed to operate on Windows only.

To install Deployment Manager:

1. The installation package for Deployment Manager is located on the Management Framework 7.6 product CD in the `deployment_manager` directory. Double-click `setup.exe` to start installation.
2. Specify the destination directory into which Deployment Manager is to be installed, and click `Next`.
3. Click `Install`.

When the setup program is finished, Deployment Manager is ready to run.

To start it, select `Start > Programs > Genesys Solutions > Framework > Management Framework Deployment Manager`.

Using Deployment Manager

The following sections describe the different steps you must follow to use the Deployment Manager.

Specifying the Installation Packages CD

The Management Framework Deployment Manager uses installation packages from the Management Framework 7.6 product CD. To perform component deployments, you must specify the location of the Management Framework 7.6 product CD as follows.

If the installation packages for the components are located on a different drive, such as

1. Click the `Change CD` link on the `Welcome` page of Deployment Manager.
2. In the `Browse` dialog box, choose the `CDInfo.xml` file (located in the root directory of the Management Framework 7.6 product CD).

Deployment Manager stores and displays the specified location.

Note: The Deployment Wizard for each Framework component available with Deployment Manager allows you to select the location of the Management Framework 7.6 product CD. You can do this at the `host specification` page of each Deployment Wizard.

Specifying Default Deployment Parameters

When deploying Framework components (except Configuration Server), you must specify the host and port of Configuration Server. Framework components use these settings to connect to Configuration Server.

If Deployment Manager is connected to Configuration Server, it passes this host and port information to the installation packages being deployed. This allows the installed Framework components to connect to the appropriate Configuration Server.

The Deployment Manager also allows you to specify the default host and port for Configuration Server for cases when Deployment Manager is not connected to Configuration Server. To specify the default host and port for Configuration Server:

1. Click `Setup Default Deployment Parameters` in the left pane of Deployment Manager.
2. Click `Configure Parameters` on the displayed page.
3. Enter the default values for the Configuration Server host and port.
4. Click `Save Changes`.

Login to Configuration Server

When deploying Framework components with Deployment Manager, if desired, you can log in to Configuration Server if you have one up and running.

To login to Configuration Server from the Deployment Manager:

1. Click `Login to Configuration Server` in the left pane of Deployment Manager.
2. Click `Login to Configuration Server` in the displayed dialog box.
3. Specify parameters in the `Login` dialog box as described in “Login Procedure” on page 217.
4. Provide the application name of the Install-Time Configuration Utility (`ITCUtility`).

Deploy Framework Components

To deploy Framework Components from Deployment Manager:

1. Click `Deploy Management Framework Components` in the left pane of Deployment Manager. (This displays the page that is also shown by default.)
2. On the displayed page, select the Framework component you want to deploy. This will start the Deployment Wizard for the selected component.
3. Follow the instructions in the wizard, entering any configuration information the wizard requires.

Requirements for Local and Target Hosts

This section details software requirements for local and target hosts.

Windows Hosts

For a successful remote installation, both your local and target Windows hosts must have:

1. Windows Installer Service, version 2.0, installed and running.

   Note: Microsoft Windows Installer Service is, by default, included in all versions of Windows 2000, Windows XP, and Windows 2003 Server.

2. Microsoft Windows Management Instrumentation (WMI) Service installed and running. Use the Microsoft WMI Service version 1.5 or later.

   Note: Microsoft WMI Service is, by default, included in all versions of Windows 2000, Windows XP, and Windows 2003 Server.

Also, the user account used for deployment must have administrative rights on the target host.

UNIX Hosts

For a successful remote installation, your UNIX target host must have:

1. Telnet access. (The Telnet daemon should be running on the standard port of the UNIX target host, allowing the Deployment Manager to open a telnet connection.)
2. An FTP client. (A standard FTP client application must be installed. Deployment Manager will use it to download the installation package.)
3. A standard UNIX shell `sh`.

Appendix

G Installation Worksheet

This appendix contains tables that you can use to help prepare for and perform the installation of Framework components.

This appendix contains the following sections:

How to Prepare a Worksheet

1. Fill in the database information in Table 8 on page 232.
2. Fill in the License Manager and license file(s) information in Table 9 on page 233.
3. Fill in the main configuration parameters you specify for Framework applications in Table 10 on page 234. Note 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 where the application is installed and/or is to be running.
4. For Windows applications, fill in the `Program Folder` information in Table 11 on page 235.

Table 7: Installation Worksheet

Installation Worksheet	
Person responsible	
Start date	
Completion date	
Database information	Refer to Table 8 on page 232.
Licensing information	Refer to Table 9 on page 233.
Application configuration	Refer to Table 10 on page 234.
Program folders (for Windows applications)	Refer to Table 11 on page 235.

Table 8: Database Information

Parameter	Value	Description
Configuration Database		
DBMS Name		The name or alias identifying the SQL server DBMS that handles the database. • For Sybase, this is the server name stored in the Sybase interface file. • For Oracle, it is the name of the Listener service. • For Informix, this value is the name of SQL server, specified in the sqlhosts file. • For Microsoft SQL, this value should be set to the name of SQL server (usually the same as the host name of the computer where Microsoft SQL runs). • For DB2, this value should be set to the name or alias-name of the database specified in the db2 client configuration.
DBMS Type		The type of DBMS that handles the database.
Database Name		The name of the database as it is specified in your DBMS. This value is required for all database types except Oracle. For Sybase, Informix, DB2, and Microsoft SQL, this value is the name of the database where the client will connect.
User Name		The user name established to access the database.

Table 8: Database Information (Continued)

Parameter	Value	Description
Password		The password used for accessing the database.
Log Database		
DBMS Name		The name or alias identifying the SQL server DBMS that handles the database. • For Sybase, this is the server name stored in the Sybase interface file. • For Oracle, it is the name of the Listener service. • For Informix, this value is the name of SQL server, specified in the sqlhosts file. • For Microsoft SQL, this value should be set to the name of SQL server (usually the same as the host name of the computer where Microsoft SQL runs). • For DB2, this value should be set to the name or alias-name of the database specified in the db2 client configuration.
DBMS Type		The type of DBMS that handles the database.
Database Name		The name of the database as it is specified in your DBMS. This value is required for all database types except Oracle. For Sybase, Informix, DB2, and Microsoft SQL, 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.

Table 9: Licensing Information

Parameter	Value
License Manager	
host	
port	
License Files	
full path to and name	

Table 9: Licensing Information (Continued)

Parameter	Value
full path to and name	
full path to and name	

Table 10: Application Configuration Parameters

Application Type	Application Name	Application Host	Application Port	Working Directory
Configuration Layer Components				
DB Server, Primary, for Configuration Database (configured via configuration file)				
DB Server, Backup, for Configuration Database (configured via configuration file)				
Configuration Server, Primary (configured via configuration file)				
Configuration Server, Backup (configured via configuration file)				
Configuration Manager			Not applicable	
Management Layer Components				
Local Control Agent	Not applicable		(Configured in Host Properties)	Not applicable
DB Server, Primary, for Log Database				
DB Server, Backup, for Log Database				
Database Access Point		Not applicable		
Message Server, Primary				

Table 10: Application Configuration Parameters (Continued)

Application Type	Application Name	Application Host	Application Port	Working Directory
Message Server, Backup				
Solution Control Server, Primary				
Solution Control Server, Backup				
Solution Control Interface			Not applicable	
SNMP Master Agent, Primary				
SNMP Master Agent, Backup				
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				

Table 11: Windows Application Program Folder

Application	Program Folder
Configuration Layer Components	
DB Server, Primary, for Configuration Database (configured via configuration file)	

Table 11: Windows Application Program Folder (Continued)

Application	Program Folder
DB Server, Backup, for Configuration Database (configured via configuration file)	
Configuration Server, Primary (configured via configuration file)	
Configuration Server, Backup (configured via configuration file)	
Configuration Manager	
Management Layer Components	
Local Control Agent	
DB Server, Primary, for Log Database	
DB Server, Backup, for Log Database	
Message Server, Primary	
Message Server, Backup	
Solution Control Server, Primary	
Solution Control Server, Backup	
Solution Control Interface	
SNMP Master Agent, Primary	
SNMP Master Agent, Backup	
Media Layer Components	
T-Server, Primary, for switch ...	

Table 11: Windows Application Program Folder (Continued)

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

Database Connections

Table 12 shows how many connections to a database the Framework components require.

Table 13 shows how many connections to a database the solution and Reporting components require.

Table 12: Number of Database Connections Required for Framework 7.x Components

Framework Component	Connection to DB Server/ Database	Number of Simultaneous Connections	Comments	Total per Layer
Configuration Layer				**2 + 2**
Configuration Server	Yes	2		
Configuration Conversion Wizard	Yes	2	Temporary (either Configuration Conversion Wizard or Database Initialization Wizard uses the connection at a given moment)	
Database Initialization Wizard	Yes	2	Temporary	

Table 12: Number of Database Connections Required for Framework 7.x Components (Continued)

Framework Component	Connection to DB Server/ Database	Number of Simultaneous Connections	Comments	Total per Layer
Configuration Import Wizard	No	0		
Management Layer				**2**
Message Server	Yes	1		
Solution Control Server	No	0		
Solution Control Interface	Yes	1		
SNMP Master Agent	No	0		
Services Layer				**1**
DB Server	No	0		
Stat Server	Yes	1	Stat Server has an option to save data directly into database tables; this operation takes one connection.	

Table 13: The Number of Database Connections Required for 7.x Solutions' Components

Solution Component	Connection to DB Server/ Database	Number of Simultaneous Connections	Comments	Total per Solution
Outbound Solution				**1 + n**
Outbound Contact Server	Yes	n	One per list	
Outbound Contact Manager	Yes	1		

Table 13: The Number of Database Connections Required for 7.x Solutions' Components (Continued)

Solution Component	Connection to DB Server/ Database	Number of Simultaneous Connections	Comments	Total per Solution
Universal Routing Solution				**1**
Universal Routing Server	Yes	0–1	In theory, the number of connections is unlimited	
Reporting				**31**
Call Concentrator	Yes	1		
Data Sourcer	Yes	2	DB Server	
IS Data Sourcer	Yes	2	JDBC	
ETL Runtime	Yes	20	JDBC	
Purging	Yes	2	JDBC	
Object Tracking	Yes	1	JDBC	
BRIO Server	Yes	2	SQLNet/ODBC	
BRIO Report Designer	Yes	1	SQLNet/ODBC	

Index