GENESYS®
AN ALCATEL-LUCENT COMPANY

Genesys 7.6

Security

Deployment Guide

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

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

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)-1276-45-7002	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: 76g_dep-security_07-2008_v7.6.001.02

Table of Contents

List of Procedures

Preface

Welcome to the *Genesys 7.6 Security Deployment Guide*. This document is new in release 7.6, and describes the deployment and configuration of some of the security features provided in Genesys software.

This document is valid only for the 7.6 release of this product.

Notes: This document is not an exhaustive study of all of the security features that Genesys offers. Many security features are documented elsewhere in the Genesys documentation suite. For example, the *Framework 7.6 Deployment Guide* contains information about user management. As these features evolve, so too will this document to provide a concise one-stop reference for all of your security needs.

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

This preface provides an overview of this document, identifies the primary audience, introduces document conventions, and lists related reference information. It contains the following sections:

Genesys software incorporates many security features, primarily:

- Authentication
- Authorization
- Audit Trail
- Data Suppression
- Data Encryption
- Secure Connectivity

This *Deployment Guide* describes the steps that you must take to set up these security features. Some features can be customized for the individual components on which they operate. In these cases, see the product documentation, usually the *Deployment Guide* or *User's Guide*, for detailed information about customizing the security feature.

Intended Audience

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

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

You should also be familiar with the architecture and functions of your Genesys products as described in the latest release of your product documentation.

Chapter Summaries

This document contains deployment information for several security features. To help you plan your secured environment, this information has been organized as follows:

- Chapter 1, "Introduction," on page 15 describes the types of risks and exposures faced by contact centers, and identifies the security features that Genesys provides to address them.

Part 1: Data Confidentiality and Integrity

This part contains information about security features that help you secure your data from unauthorized users.

- Chapter 2, "No Default Access for New Users," on page 21 describes how to prevent new users from being automatically assigned any access privileges.
- Chapter 3, "Inactivity Timeout," on page 25 describes how to configure a time interval of inactivity, after which all data displayed is hidden and the user forced to be re-authenticated before continuing to work.
- Chapter 4, "Hide Selected Data in Logs," on page 29 describes how to ensure that users see only what they need to see in logs and log reports.

- Chapter 5, “Security Banner at Login,” on page 33 describes how to design and configure a security banner, which can be displayed when a user logs in to your system.

Part 2: Service Availability

This part contains information about security features that help you ensure that you can always access your data.

- Chapter 6, “Application Redundancy,” on page 49 provides information about configuring redundant applications to ensure that you will always have a fully-functioning system.
- Chapter 7, “Proxy and Parallel Servers,” on page 55 provides information about configuring proxy and parallel servers that will help you maintain an efficient level of service, and minimize the impact that any server failure has on your level of service.

Part 3: Service Integrity—Transport Layer Security

This part contains information about security features that help you use Genesys Transport Layer Security (TLS) to secure your data during transmission:.

- Chapter 8, “Introduction to Genesys Transport Layer Security,” on page 61 provides an overview of the Genesys TLS implementation and provides general guidelines for your specific Genesys deployment.
- Chapter 9, “Security Pack Installation,” on page 65 describes how to install and configure the Genesys Security Pack on UNIX.
- Chapter 10, “Certificate Generation and Installation,” on page 69 provides an overview of typical steps in the process of using the open source OpenSSL tool and Windows Certificate Services for certificate generation.
- Chapter 11, “Genesys TLS Configuration,” on page 87 describes how to configure Genesys applications to use security certificates on connections that need to be secure.
- Chapter 12, “Troubleshooting Genesys TLS,” on page 113 provides information for troubleshooting the TLS installation in your environment.

Part 4: Service Integrity—Client-Side Port Definition

This part contains information about security features that help you use Genesys client-side port definition to secure your data during transmission.

- Chapter 13, “Client-Side Port Definition,” on page 117 describes how to specify client parameters to connect to a specific server application.

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:

g_dep-security_03-2008_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:

- The *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD, and which provides a comprehensive list of the Genesys and CTI terminology and acronyms used in this document.

- The *Genesys 7 Migration Guide*, also on the Genesys Documentation Library DVD, which provides a documented migration strategy from Genesys product releases 5.1 and later to all Genesys 7.x releases. Contact Genesys Technical Support for additional information.
- The Release Notes and Product Advisories for this product, which are available 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 Introduction

This chapter provides an overview of the security risks and requirements inherent in a contact center environment, and describes how Genesys addresses those risks.

This chapter contains the following sections:

Overview

The risks and threats inherent to data networks also apply to contact centers. In general, the risks common to contact center solutions can be broken down into the following categories:

- Data confidentiality and integrity
- Service availability
- Service integrity

This chapter describes each of these risks, and indicates security features that Genesys provides to address them.

Note: This document is not an exhaustive study of all of the security features that Genesys offers. Many security features are documented elsewhere in the Genesys documentation suite. For example, the *Framework 7.6 Deployment Guide* contains information about user management. As these features evolve, so too will this document, to provide a concise one-stop reference for all of your security needs.

Data Confidentiality and Integrity

Unauthorized data access and the abuse of user privileges are common concerns for multi-user environments. Ensuring data correctness and its instant availability over the course of its lifecycle is critical for the business. Data, software, or the configuration must not be corrupted or modified by an unauthorized party.

Disclosure of confidential customer information may result in serious legal consequences for a contact center, as well as the loss of a customer. Privacy includes protecting, not only the customer proprietary data, but also transaction and call statistics, and sometimes their identification as a customer of a particular Contact Center.

In addition to standard security features, such as user authentication, Genesys provides the following security features to address data confidentiality:

- No Default Access for New Users
- Inactivity Timeout
- Security Banner at Login
- Hide Selected Data in Logs

Service Availability

Contact Center service interruption or unavailability may lead to direct revenue loss and customer dissatisfaction. Minimizing downtime and maintaining full performance capability are of the highest priority for any online service.

Availability provisioning implies using robust and quality software, preventing network intrusion and denial-of-service attacks, and protecting network and computational resources using redundant server configuration.

Genesys provides the following security features to address service availability:

- Redundancy
- Proxy and Parallel Servers

Service Integrity

In addition to the protection of data where it resides, as described in "Data Confidentiality and Integrity" on page 16, data must also be protected when it is sent over communication channels.

Genesys provides the following security features to address data and service integrity:

- Transport Layer Security (TLS)
- Client-Side Port Definition

Security Deployment

This document describes each of the Genesys security features mentioned in the preceding sections. It also includes detailed deployment instructions for those features that can be installed either system-wide, or in a manner that is consistent for all products. If the deployment process differs between components or products, you are referred to appropriate product documentation for the specific steps.

Where part of the deployment of a feature is performed as part of another procedure, this document provides an overview of that part. For detailed instructions, you are referred to the appropriate product documentation.

Security and Standards Compliance

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 security-related business standards such as European Data Protection Directive (EDPD), ISO 177999, HIPAA, PCI DSS etc. However, the Genesys products are merely tools to be used by the customer and cannot ensure or enforce compliance with these standards. It is solely the customer's responsibility to ensure that any use of the Genesys suite of products complies with these business standards. Genesys recommends that the customer take steps to ensure compliance with these business standards as well as any other applicable local security requirements.

Part

1 Data Confidentiality and Integrity

Part One of this document describes the features that Genesys provides to secure data and ensure its integrity. This information appears in the following chapters:

- Chapter 2, “No Default Access for New Users,” on page 21
- Chapter 3, “Inactivity Timeout,” on page 25
- Chapter 4, “Hide Selected Data in Logs,” on page 29
- Chapter 5, “Security Banner at Login,” on page 33

Chapter

2 No Default Access for New Users

The chapter describes how to prevent new users from being automatically assigned any access privileges.

This chapter contains the following sections:

For detailed information about access privileges and Access Groups, refer to the *Framework 7.6 Deployment Guide*.

Feature Summary

New users created in release 7.6 applications are, by default, not automatically assigned any default privileges. In effect, the new users have no privileges, and cannot log in to any interface or use a daemon application. Each new user must have the appropriate access privileges assigned by a system administrator or by another existing user with appropriate access rights.

This feature is enabled by default, and applies only to new users created in release 7.6. You can disable the feature if required.

Security Benefits

New users can be created in multiple ways—directly in a graphical user interface (GUI) or using the Software Development Kit (SDK). There may be cases where the new user does not, or should not, need all or some of the default privileges. This feature ensures that no user is assigned default privileges, regardless of how the user is created.

Supporting Components

This feature is configured in Configuration Manager. It is not supported by Configuration Server 7.5 or earlier.

Genesys Desktop

Genesys Supervisor Desktop supports a complimentary feature. For more information, see the *Genesys 7.6 Desktop Deployment Guide*.

Feature Description

Prior to release 7.6, when new users were added to the system, they were automatically assigned a set of default privileges. This feature reverses that behavior: new users created in release 7.6 are no longer automatically assigned any default privileges. In effect, the new users have no privileges, and cannot log in to any interface or use a daemon application. Each new user must be explicitly added to appropriate Access Groups by a system administrator or by existing users with access rights to modify the new user's account.

By default, this new feature applies only to new users created in release 7.6, and can be disabled if required.

Compatibility with Previous Releases

New users created for release 7.5 or earlier Configuration Server `Application` objects imported into Configuration Server 7.6 are also subject to this feature unless the feature is manually disabled in each 7.5 or earlier Configuration Server `Application` object.

Feature Configuration

Note: To determine if this section refers to you, see "Supporting Components" above.

By default, this feature is enabled for all new users created in release 7.6 with the `no-default-access` configuration option. The Configuration Server application template for release 7.6 contains this option set to its default value of zero (`0` - No default access privileges). To disable this feature, set the option to one (`1` - Default access privileges).

Restoring Default Access for Users in Previous Releases

This feature is also enabled automatically for release 7.5 or earlier Configuration Server `Application` objects imported by a release 7.6 Configuration Server. To maintain backward compatibility, you must manually add the `no-default-access` option to the `security` section on the `Options` tab of each imported Configuration Server `Application` object, and disable the feature by setting the option to one (`1` - Default access privileges). This will ensure that new users created for those imported applications are assigned default permissions based on the rules present in the original release.

Assigning Permissions to New Users

To assign permissions for those new users who are subject to this feature, use the `Member Of` tab of the `Properties` dialog box for each user. For more information, see *Framework 7.6 Configuration Manager Help*.

Configuration Options

Security Section

This section contains configuration options relating to security features. This section must be called `security,` and is configured on the `Options` tab of the Configuration Server `Application` object.

no-default-access

Default Value: `0`
Valid Values: One of the following:

`0`	No default access privileges
`1`	Default access privileges

Takes Effect: Immediately

Specifies whether new users created under this application have default privileges assigned to them. If this option is not present, the default value is assumed.

To maintain backward compatibility with prior releases, you must manually add this option to all release 7.5 or earlier Configuration Server `Application` objects imported into Configuration Server 7.6, and set its value to `1`. This will ensure that new users created for these objects are automatically assigned to the default Access Groups, as was the case in those pre-7.6 releases.

Chapter

3

Inactivity Timeout

This chapter describes how to configure a time interval after which an inactive user must be re-authenticated before continuing with the session.

This chapter contains the following sections:

Feature Summary

The inactivity timeout is a configurable period of time during which a user can be inactive (that is, not interact with the system in any way) without any impact on their session. After the timeout expires, the user is locked out of the session, and all session displays are minimized. The user must log back in to continue with the session. Alternatively, anyone can close the session completely, without logging back in.

Note: For purposes of this feature, *activity* is defined as using the mouse (clicking, moving, or scrolling), pressing a key, changing the state of a window between active and inactive, or acknowledging any warning that may be generated by the operating system’s own timeout functionality.

Security Benefits

If a user is distracted while logged in to a session, causing them to either turn away or walk away from their computer, that session is available for anyone (authorized or not) to access. The Inactivity Timeout feature minimizes the possibility of that second party viewing or accessing the system. It is a best effort because the length of the timeout is a trade-off between the inconvenience to the logged-in user of having to log in repeatedly, and the risk of exposing the system to other people.

Supporting Components

The following components support this feature:

- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager

Feature Description

When a user is inactive for the period of time equal to the inactivity timeout, all display screens are minimized (with the exception of some modal dialog screens), and a re-login dialog box is displayed. The connection to the server should be preserved. However, if the connection is lost for some reason, the High Availability (HA) functionality of the application will attempt to reestablish it automatically.

In the re-login dialog box, the user can do one of the following:

- Enter their password, and click `OK.` The user is then authenticated. One of two situations occurs:
  - If this user is not the original user, access will not be permitted.
  - If this user is the original user, that user will be logged back in, and the session state will be restored as much as possible.
- Click `Cancel` to close the application. A confirmation dialog box appears, asking the user to verify that the application is to be closed.

In any case, the user must be re-authenticated before accessing the current session.

Password Changes

Configuration Manager and Interaction Routing Designer permit an authorized individual to change a user's password for that Application. If this occurs while the user is logged in, and before the inactivity timeout expires should the user become inactive, the user must use the new password in the re-login dialog box. The old password will be interpreted as an invalid password and access will not be permitted.

In Configuration Manager, a system administrator can also change a user's password for another Application. If this occurs while the user is logged in, and before the inactivity timeout expires should the user become inactive, the user must use the old password in the re-login dialog box. The new password will be interpreted as an invalid password and access will not be permitted.

Feature Configuration

Note: This section describes a standard configuration method for this feature, as used by most components. Some components, such as those identified in “Supporting Components” on page 26, may implement this feature differently. In this case, see the product documentation for details.

The inactivity timeout is configured at the Application level, so can differ between applications. By default, the feature is disabled, and the timeout must be set to a non-zero value to enable the feature.

The inactivity timeout is specified by setting the configuration option `inactivity-timeout` on the `Options` tab of the `Application` object. Application templates, if they exist, contain this option set to the default value.

Configuration Options

Security Section

This section contains configuration options relating to security features. This section must be called `security,` and is configured on the `Options` tab of the Configuration Server `Application` object.

inactivity-timeout

Default Value: `0`
Valid Values: Any non-negative integer
Changes Take Effect: Immediately

Specifies the amount of time (in minutes) that a user who is logged in to the application can be inactive before application screens are minimized and the user forced to be re-authenticated. The default value `0` (zero) means that the feature is disabled.

This option is configured on the `Options` tab of the `Application` object.

Chapter

4 Hide Selected Data in Logs

This chapter describes how to hide selected data in log messages.

This chapter covers the following topics:

Feature Summary

This feature enables you to hide selected data in log messages generated by a Genesys component.

Security Benefits

This feature prevents unauthorized users from seeing particular data in log messages. Where logs are distributed to another party, such as for troubleshooting purposes, this feature enables you to hide confidential data that you may not want the other party to see. This feature is also useful for preserving the confidentiality of data provided to you by third parties which may be attached to the logs.

Supporting Components

This feature is supported by all Genesys server applications.

Feature Description

This feature enables you to hide selected data in log messages generated by a Genesys component. You can choose to hide just the data itself, by replacing it with a series of asterisks (*), or you can remove the whole data field from the log output.

Feature Configuration

This feature is implemented by defining the following two configuration options on the `Options` tab of the server `Application` objects:

- The `default-filter-type` in the `log-filter-section` option defines the treatment for all the data in the log.
- One or more `<key name>` options in the `log-filter-data` section defines the treatment for specific keys in the log, overriding the default treatment specified by `default-filter-type`.

Configuration Options

Log-Filter Section

This section defines the treatment of all data in the log. This section must be called `log-filter`.

default-filter-type

Default Value: `copy`
Valid Values: One of the following:

`copy`	The keys and values of the KVList pairs are copied to the log.
`hide`	The keys of the KVList pairs are copied to the log; the values are replaced with strings of asterisks.
`skip`	The KVList pairs are not copied to the log.

Changes Take Effect: Immediately

Specifies the default way of presenting KVList information (including `UserData`, `Extensions`, and `Reasons`) in the log. This setting will be applied to the attributes of all KVList pairs except the ones that are explicitly defined in the `log-filter-data` section.

Example

```
[log-filter]
default-filter-type=copy
```

The following is an example of a log using the default log filter setting. Note that all data is visible.

```
message RequestSetCallInfo
    AttributeConsultType        3
    AttributeOriginalConnID     008b012ece62c8be
    AttributeUpdateRevision     2752651
```

```
   AttributeUserData          [111] 00 27 01 00
          'DNIS'              '8410'
          'PASSWORD'          '111111111'
          'RECORD_ID'         '8313427'
   AttributeConnID            008b012ece62c922
```

Log-Filter-Data Section

This section defines the treatment of specific data in the log. It overrides the general settings in the `log-filter` section. This section must be called `log-filter-data`.

<key name>

Default Value: `copy`
Valid Values: One of the following:

`copy`	The key and value of the given KVList pair are copied to the log.
`hide`	The key of the given KVList pair is copied to the log; the value is replaced with a string of asterisks.
`skip`	The KVList pair is not copied to the log.

Changes Take Effect: Immediately

Specifies the way of presenting the KVList pair defined by the key name in the log. This setting supersedes the default way of KVList presentation as defined in the `log-filter` section for the given KVList pair.

Note: For T-Server `Application` objects, if the T-Server common configuration option `log-trace-flags` is set to `-udata`, it will disable writing of user data to the log regardless of the settings of any options in the `log-filter-data` section. Refer to the documentation for your particular T-Server for information about the option `log-trace-flags`.

Example

```
[log-filter-data]
PASSWORD=hide
```

The following is an example of a log with the option `PASSWORD` set to `hide`. Note that the data for the field `PASSWORD` has been replaced with a series of asterisks (****).

```
message RequestSetCallInfo
   AttributeConsultType       3
   AttributeOriginalConnID    008b012ece62c8be
   AttributeUpdateRevision    2752651
   AttributeUserData          [111] 00 27 01 00
          'DNIS'              '8410'
```

```
       'PASSWORD'            '****'
       'RECORD_ID'           '8313427'
AttributeConnID              008b012ece62c922
```

Chapter

5

Security Banner at Login

This chapter describes how to configure and install a security banner that is displayed to a user when logging in.

This chapter contains the following sections:

Feature Summary

The security banner is a separate window that is displayed to a user when logging in to an application. The content of this window is defined by the system administrator, and may include such items as Terms of Use of the application or some kind of disclaimer. One security banner can be used by more than one application, and different applications can use different security banners.

The security banner can be enabled and configured in one of two ways:

- During application setup
- Before or after installation of the application, by creating specific registry entries in the application's host registry

The security banner can be configured differently for each application, to support a variety of corporate policies.

Security Benefits

The security banner does not actually provide true physical or virtual protection for your system. However, it can provide legal protection if an unauthorized user violates any access restrictions, such as Terms of Use, and accesses the system anyway.

Under the strictest configuration of the security banner, a user is not allowed to log in to an application without first accepting the contents of the banner. The various degrees of security depend on the options selected during installation.

Supporting Components

The following components support the implementation of the security banner as described in this chapter:

- Configuration Wizards
- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager

Genesys Desktop

Genesys Desktop supports the security banner in concept, but implements it differently from the way described in this document. In addition to a different installation procedure, all URLs related to the security banner must be in HTTP format (`http://`). Refer to the *Genesys Desktop 7.6 Deployment Guide* for more information.

Feature Description

The security banner is intended to display a user-defined security message prior to the login to a Genesys application, and provide the user with the means to confirm acceptance of the message. The message content is specified as an arbitrary URL, pointing to a document that can be displayed as an active document by Microsoft Internet Explorer 4.0 or later. Multiple URLs can be configured for redundancy.

The following characteristics of the security banner are configurable by the user, and can be configured differently for each application:

- Regularity with which the security banner is displayed. For example, it can be displayed only once for each user, only once for each user for each type of application, or for all logins.
- Whether the security banner is to be displayed, or if user acknowledgement is required.
- Behavior if the target URL of the security banner is not available.
- Title and dimensions of the security banner window.

- The timeout within which the security banner must be loaded and displayed on the screen. If this timeout expires, an intermediate message (`Downloading terms of use... Please wait...`) is displayed while the security banner loads.

By default, the security banner window contains user-defined text, two buttons (`Accept` and `Reject`) and a check box (`I Accept. Do not show this again.`) The user logging in to the application must click `Accept` to proceed to the login dialog box. If the user clicks `Reject` or closes the security banner window without accepting the window contents, the application closes.

As previously described, an intermediate message (`Downloading terms of use... Please wait...`) is displayed whenever the security banner is not retrieved and displayed before the timeout expires. During this time, the user can close the window by clicking `Cancel`; the terms can only be accepted when the content is fully displayed.

You must also specify whether you allow a user to log in to the application if the security banner cannot be displayed; if you do not allow it, the application closes if the security banner cannot be displayed.

If the security banner cannot be retrieved at all, an error message is displayed. Error messages contain an `Exit` button instead of `Accept` and `Reject` buttons. The software includes a default error page, but you can also configure your own. The behavior of the error page depends on whether you have chosen to allow a user to log in to the application if the security banner is not displayed, as follows:

- If you have chosen to allow the user to log in, the error page closes automatically (if it is open) and the login dialog box appears. The user can then log in to the application.
- If you have chosen not to allow the user to log in, the error page included with the software is displayed, showing the error code. The login dialog box is not displayed, and the user cannot log in. For HTTP errors, refer to the HTTP specification. For system errors, refer to Microsoft technical documentation.

Warning! Genesys recommends that you use multiple redundant URLs, including a local file as appropriate, to minimize the risk that the security banner will not load.

Feature Deployment

Note: To determine if this section applies to your component, see “Supporting Components” on page 34.

Deployment of the security banner consists of three steps:

1. Design and create the required security banners and optional customized error pages, using the editor of your choice.
2. Deploy security banner documents as files or as web content, and record the URLs. Each URL must be able to be resolved by the installed Microsoft Internet Explorer (IE) and displayed as an active page within the IE window.
3. Configure the URLs in one of the following ways:
   - As directed during installation of the GUI application (see "Installing the Security Banner During Application Setup" on page 37)
   - By modifying registry entries directly (see "Configuring the Security Banner in the Registry" on page 40)

Warning! Editing a registry incorrectly can cause serious, system-wide problems, and correcting them may require you to reinstall your operating system. Genesys cannot guarantee that any problems resulting from editing the registry can be solved. Edit your registry at your own risk.

If you do decide to edit the registry, Genesys strongly recommends that you back up the registry file before editing it.

Note: If you uninstall an application for which the security banner was configured, the configuration parameters of its security banner are not removed from the registry. To clear these parameters, you must reinstall the application without enabling the security banner.

Deploying the Security Banner for Multiple Applications on the Same Host

If, on a single host, you are installing two or more applications that support and will be using a security banner, you can choose to do one of the following:

- Provide individual settings for each type of application.

  In this case, if you choose to configure the security banner for just one (*for this*) application, all other applications will be deemed to have the security banner disabled. If you want any other applications to use a banner, you must enable and configure it for each of those other applications. In subsequent application installations, you can chose the *for all* option, but this will only set default values for subsequent installations; it will not impact the values for previous installations.

- Configure one security banner for all applications.

  In this case, the security banners *for all* applications on this host will have the same content and behavior. In effect, these settings become the *default* settings. You do not have to enable and configure the security banner for each application. Having done this, for each application with security banner that you subsequently install, you can choose to do one of the following:

- Provide individual settings *for this* application only, while not impacting the default settings.
- Override the default settings by choosing to configure the security banner *for all* applications, and modifying the settings as required. The default values will appear in the installation interface, and can be overwritten or kept as is. If you change any of these values, all applications that use the default values, both those installed previously and subsequently, will be impacted.

In general, when setting up an application, the setup program looks first for a security banner configuration specific to the application (*for this*). If one is not found, it then looks for a configuration common to all applications (*for all*). In either case, it inherits the security banner attributes already defined. If it is unable to find any security banner configuration, it defaults to a disabled security banner, and you must then enable and configure the security banner from the beginning.

Installing the Security Banner During Application Setup

For those components identified in "Supporting Components" on page 34, the installation and configuration of the security banner is part of the application installation procedure. The security banner can also be installed after an application has been installed.

Refer to documentation for your application for detailed instructions about installing the application. Use the following procedure only if you select the `Enable Security Banner` option when installing the application.

Procedure:
Installing and configuring the security banner during Application setup

Purpose: To install and configure the security banner for a supporting component.

Supporting components:

- Configuration Wizards
- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer

- Outbound Contact Manager

Prerequisites

- You are installing one of the supporting components listed above, and have reached the `Security Banner Configuration` page of the installation wizard.
- You have created, and have the URLs of, the security banner and any custom error pages that will be used.

Start of procedure

1. On the `Security Banner Configuration` page of the installation wizard for the application that you are installing:
   - **a.** In the `Select Security Banner behavior and configuration` section, select whether you want the security banner that you are about to define to be used by all applications that support the security banner feature, or just by applications of this type.
   - **b.** Click `Next`.
2. On the `Security Banner Parameters` page, specify the parameters for the security banner as follows:
   - **a.** Specify how the security banner is displayed to the user the next time an application of this type is started. The choices are:
     - `Until each user chooses to turn it off`—The security banner includes an `I Accept. Do not show this again.` check box that, by default, is not selected. If the user selects this option and clicks `Accept,` the security banner will not be displayed again to that user, regardless of the application that the user is starting. Each Windows user account must explicitly select this option and click `Accept` to disable the security banner for all applications.
     - `Until each user chooses to turn it off once for each application type`—The security banner includes an `I Accept. Do not show this again.` check box that, by default, is not selected. If the user selects this option and clicks `Accept,` the security banner will not be displayed again to that user when starting any application of this type. However, each time the user starts another type of application for which the security banner is active, the security banner will be displayed. Each Windows user account must explicitly select this option and click `Accept` to disable the security banner for this type of application.
     - `Every time the application starts`—The security banner does not include an `I Accept. Do not show this again.` check box. The security banner is displayed to every user every time any Genesys application is started.

Note: If you select the first (`Until each user chooses to turn it off`) or second (`Until each user chooses to turn it off once for each application type`) option, and the user does select `I Accept. Do not show this again.` in the security banner window, this setting will apply for all subsequent installations of the one or multiple applications. It must manually be removed from the registry by an authorized person. See "AckMode" on page 43 for detailed information.

b. Specify how to proceed if the security banner message at the specified URL cannot be displayed. The choices are:

- `Proceed to login without banner`—The user can log in to the application anyway.

Warning! Selecting this option effectively disables access to the application when the document specified by the URL cannot be retrieved or rendered for any reason.

- `Exit, no login dialog box is displayed`—The user is not permitted to log in.

c. (Optional) Specify the title that appears in the title bar of the security banner window.

If you do not specify a title, the window title is derived from the following:

- If the security banner is an HTML file—the `<title>` element.
- If the security banner is an HTML file but has no `<title>` element—the URL address.
- If the security banner is not an HTML file—the URL address.

In all cases, the application name follows the title in the title bar.

Note: If rebranding resources are present, the corresponding rebranding resource overrides this entry.

d. Specify the timeout, in milliseconds, within which the security banner must be displayed. The default is `3000`. If the entire document is not available for display within this time, an intermediate message, `Downloading terms of use ... Please wait ...`, is displayed until the security banner itself can be displayed.

e. Specify the height and width, in pixels, of the security banner window, intermediate window, and any error window, if defined. The default values are `180` and `360` pixels, respectively.

If neither of these values is specified (the default), the window is sized to fit the complete content of the document at the specified `URL`. At no time does the window exceed the work area of the screen. The document retains its size between logins, and once displayed, can be resized using standard IE tools.

Note: If the exact screen size for the security banner documents cannot be determined or estimated, Genesys recommends that the height and width parameters be specified.

f. Click `Next`.

3. On the `Security Banner Documents` page, for each document containing text that will be displayed in the security banner, specify the URL of the document and click `Add`. When you have added all the URLs, click `Next`.

   If this URL is not specified, all of the other options are ignored, and:

   - If an older security banner bitmap is configured, it is displayed.
   - Otherwise, no security banner is displayed.

4. On the `Security Banner Error Documents` page, do one of the following:

   - If you selected `Proceed to login without banner` in Step 2 b on page 39, click `Next`. Do not enter any URLs on this page.
   - Otherwise, specify the URL of an error document—either the default error page or one that you specifically created—and click `Add`. When you have added all the URLs, click `Next`.

End of procedure

Next Steps

- Finish installing your application, as required. Refer to the product-specific documentation for detailed instructions.

Configuring the Security Banner in the Registry

Warning! Editing a registry incorrectly can cause serious, system-wide problems, and correcting them may require you to reinstall your operating system. Genesys cannot guarantee that any problems resulting from editing the registry can be solved. Edit your registry at your own risk.

If you do decide to edit the registry, Genesys strongly recommends that you back up the registry file before editing it.

The Security Banner feature and URLs are defined in the registry of the application's host. Only someone with write access to the HKEY_LOCAL_MACHINE registry key—normally the system administrator— can set up and maintain the security banner. This authorized person should:

- Specify the target URLs of the security banners and any customized error pages.
- Customize the windows as required.
- Subsequently modify the behavior as required, by changing the listed registry entries. This can be done either locally or remotely.

Configuring the Security Banner Functionality

Configure the security banner functionality by using the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner
```

The values in this key specify the default behavior for all applications. Each entry can be redefined for specific applications in the subkeys, as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\<CfgAppType>
```

where <CfgAppType> is the numeric value of the application type, as defined in Table 1 on page 41.

For example, to specify values specific to Configuration Manager, which has application type 19, define the registry subkey as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\19
```

When selecting the security banner to display and use, the library first looks for a corresponding subkey, and then uses the default key if the subkey does not exist.

String entries can be entered as STRING or EXPANDABLE_STRING registry values. If they are entered as EXPANDABLE_STRING, environment variable strings enclosed in percent signs (%) are replaced with their values defined by the environment variables (located in %HOMEDRIVE%%HOMEPATH%\default.htm). Integer entries can be entered either as DWORD or STRING registry values, representing decimal numbers.

Table 1: Supported Application Types for CfgAppType

CfgAppType	Application
13	Outbound Contact Manager
19	Configuration Manager Wizard Manager
44	Solution Control Interface

Table 1: Supported Application Types for CfgAppType (Continued)

CfgAppType	Application
51	Interaction Routing Designer

Configuring URLs

The URLs for the security banner and any associated error pages are configured in the following registry keys:

- For all applications:
  `HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\<seq_number>`
- For specific applications:
  `HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\<CgfAppType>\<seq_number>`

where `<seq_number>` is the sequence number for multiple URLs. Multiple URLs are tried in the order of their sequence number.

The URLs are specified by the registry options `ErrorPage` (see page 44) and `URL` (see page 46).

Example

The following sample registry entries:

```
KEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\1\URL=http://M
yServer1/Banner.htm
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\2\URL=http://
MyServer2/Banner.htm
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\3\URL=%System
Root%\AdminContacts.htm
HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\3\ErrorPage=1
```

specify the following behavior:

The dialog attempts to retrieve `Banner.htm` from `MyServer1`. If it cannot retrieve that file, the dialog attempts to retrieve `Banner.htm` from `MyServer2`. If it cannot retrieve that file, the dialog attempts to retrieve the custom error page located in the `system32` directory is displayed. And if that page cannot be displayed, the default error page is displayed.

Security Banner Registry Entries

This section describes the registry options used to specify and customize the appearance and behavior of the security banner. These options are intended only for advanced users with registry access.

Note: Unless otherwise noted, the registry entries in this section are equivalent to the options presented when installing the security banner during application setup.

AckMandatory

Default Value: `0`

Valid Values: One of the following:

`0`	Proceed with the login, without acknowledgement of the contents of the security banner. The login dialog box is displayed.
`1`	Exit the application. The login dialog box is not displayed.

Changes Take Effect: After the application restarts

Specifies whether login to the application will be allowed if the document specified in the `URL` option (see page 46) cannot be displayed for any reason.

Warning! Setting this option to `1` effectively disables access to the application when the document specified by the URL cannot be retrieved or rendered for any reason.

AckMode

Default Value: `0`

Valid Values: One of the following:

`0`	User can choose to hide the security banner for all subsequent logins, for all applications.
`1`	User can choose to hide the security banner for all subsequent logins to the current application only.
`2`	User cannot choose to hide the security banner; user must accept content of the banner whenever logging in to any application.

Changes Take Effect: After the application restarts

Specifies whether the user is presented with the option to hide the security banner, and therefore does not need to accept the security banner content, the next time an application is launched.

If this option is set to `0` or `1`, the `I Accept. Do not show this again.` check box appears in the security banner window. If the user selects this check box, they will not see the security banner at subsequent attempts to access either this (`0` or `1`) or any application (`1`) for which the security banner is configured.

Note: If option `0` or `1` is selected, the only way to have the security banner be displayed again when logging in to this (`0` or `1`) or any application (`1`) is to manually remove this entry from the registry. This registry entry and its value is persistent across installations—it is not removed when uninstalling the application, nor is it cleared or reset when reinstalling the application.

If this option is set to `2`, the `I Acknowledge. Don't show this again.` check box does not appear in the security banner window, and the security banner is displayed every time anyone tries to access the application.

ErrorPage

Default Value: 0
Valid Values:

0	The security banner is displayed.
1	An error page is displayed.

Changes Take Effect: After the application restarts

Required if you are using a custom error page. Specifies that the URL points to an error page or the security banner. If the error page is displayed, the window displays the Exit button in place of the Accept and Reject buttons. Use this setting to substitute the default error page with a customized error page.

Height

Default Value: None
Valid Values: Any positive integer greater than 180
Changes Take Effect: After the application restarts

Width

Default Value: None
Valid Values: Any positive integer greater than 359
Changes Take Effect: After the application restarts

Optional; these two options specify the dimensions (in pixels) of the document area of the security banner and error page window. If neither of these values is specified (the default), the window is sized to fit the complete content of the document specified by the URL option (see page 46). At no time does the window exceed the work area of the screen. The document retains its size between logins, and once displayed, can be resized using standard IE tools.

Note: If the exact screen size for the security banner documents cannot be determined or estimated, Genesys recommends that the height and width parameters be specified.

NoCompleteTimeout

Default Value: 2000
Valid Values: Any non-negative integer
Changes Take Effect: After the application restarts

Specifies the timeout (in milliseconds) for receiving download progress or status notifications from the WebBrowser control. To download and render the document, the security banner dialog uses components of IE in the form of WebBrowser control. In some cases, for security reasons, the WebBrowser control does not provide the client with the means to detect navigation cancellation. This timeout is used to detect and properly process these cases.

The absence of progress or status notifications from the WebBrowser control for a period exceeding this timeout is considered a failure to retrieve the document. If this timeout expires, the attempt to retrieve the document specified by the current URL is aborted, and the dialog attempts to retrieve the next URL from the URLs list. If this happens with the last URL in the list, the `System error 0x80004004: Operation aborted` error message is reported to the user.

If this option is set to zero (`0`), progress and status notifications are not used to detect download failure or cancellation.

Note: `NoCompleteTimeout` is intended only for advanced users with access to the registry. It has no equivalent option in the process of installing the security banner during application setup, and its default value is considered adequate in these situations.

ShowUpTimeout

Default Value: `3000`
Valid Values: Any non-negative integer
Changes Take Effect: After the application restarts

Specifies the timeout (in milliseconds) within which the security banner window attempts to load the document specified by the `URL` option (see page 46). If the timeout expires before the content is displayed, an intermediate window (`Downloading terms of use... Please wait...`) is displayed. During this time, the user can close the window by clicking `Cancel`; the terms can only be accepted when the content is fully displayed.

If the document cannot be retrieved, the behavior of the window depends on the value of the `AckMandatory` option, as follows:

- If `AckMandatory=0,` the window closes automatically (if it is open), and the login dialog box appears. The user can then log in to the application.
- If `AckMandatory=1,` the error page included with the software is displayed, showing the error code. For HTTP errors, refer to the HTTP specification. For system errors, refer to Microsoft technical documentation. The login dialog box is not displayed, so the user cannot log in.

Title

Default Value: None
Valid Values: Any string, or blank
Changes Take Effect: After the application restarts

Optional; specifies the title that appears in the title bar of the security banner window. If no value is specified for this option, the title is derived from the following:

- If the security banner is an HTML file—the `<title>` element.
- If the security banner is an HTML file but has no `<title>` element—the URL address.
- If the security banner is not an HTML file—the URL address.

In all cases, the application name follows the title in the title bar.

Note: If rebranding resources are present, the corresponding rebranding resource overrides this entry.

URL

Default Value: None, for backward compatibility
Valid Values: A URL address that can be resolved by the installed IE application and displayed as an active page within the IE window
Changes Take Effect: After the application restarts

Required; specifies the URL of the document displayed in the security banner window. If this value is not specified, all other options are ignored, and:

- If an old security banner bitmap is configured, it is displayed.
- Otherwise, no security banner is displayed.

Part

2 Service Availability

Part Two of this document describes the features Genesys provides to ensure service availability by keeping the system up and running.

This information appears in the following chapters:

- Chapter 6, “Application Redundancy,” on page 49
- Chapter 7, “Proxy and Parallel Servers,” on page 55

Chapter

6 Application Redundancy

This chapter describes the use of redundant applications to make your environment more robust in case of an application failure.

This chapter contains the following sections:

Feature Summary

Redundant applications, normally server applications, provide backup capability in the event that an application fails. That is, if one server (the primary server) goes out of service for some reason, such as lost connectivity, the other server (the backup server) can act as the primary server, with little or no loss of service.

Security Benefits

The use of redundant applications greatly reduces the loss of functionality and data if an application is out of service because of a security-related attack, such as a denial-of-service attack.

Supporting Components

Refer to Table 2 on page 52 for a list of components that support redundancy, and the redundancy types they each supports.

Feature Description

Redundant applications address the potential loss of functionality and data in the event of an application failure.

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

Because the application that fails cannot perform any functions, you must employ an external mechanism for both detection and correction of faults of this type. The Management Layer serves as such a mechanism. To detect an application failure, the Management Layer employs a simple monitoring component called Local Control Agent (LCA), which continuously maintains a connection with the application, confirming both its existence and its ability to communicate. To ensure that an application failure is never confused with a connection failure, the LCA that monitors a specific application always resides on the computer where the application itself is running.

LCA is installed on a one-per-host basis, and can connect to all Genesys applications located on the host. When a connection is broken, LCA generates a message to Solution Control Server (SCS), where an appropriate recovery action is chosen and executed according to the system configuration. SCS uses the Advanced Disconnect Detection Protocol (ADDP) to recognize a loss of connection with LCA. A loss of connection is interpreted as a failure of the host (that is, as failures of all Genesys components running on that host).

If a backup application is configured and running, the Management Layer automatically switches operations over to that application, provided that you have a so-called high-availability license. If the application is a server, the clients automatically connect to the backup server.

Starting with release 7.0, the Management Layer provides more robust switchover capabilities. In particular, it enables detection of situations when a running application is unable to provide service, and treats this situation as an application failure. The `Service Unavailable` application status serves this purpose.

When an application reports that its status has changed to `Service Unavailable,` if a backup server for this application is configured and running, the Management Layer automatically switches operations over to the backup server. When both the primary and backup applications are running with the `Service Unavailable` status, the backup application may report that it can now provide the service (that is, the status of the backup application changes to `Started`). In this case, the Management Layer automatically switches operations over to the backup application. As with a switchover resulting from an application failure, you must have an HA license to perform a switchover related to service unavailability.

Note: Although some applications support the `Service Unavailable` status and report it under appropriate circumstances, others do not. (For example, when T-Server loses its connection to the CTI Link, T-Server changes its status to `Service Unavailable`). The Management Layer bases its operation on the information supplied by an application, and cannot automatically detect an application's inability to provide service. Refer to the application-specific documentation to determine whether the `Service Unavailable` status is supported on the application side.

Redundancy Types

Warm Standby

Genesys uses the term *warm standby* to describe the redundancy type in which a backup server application remains initialized and ready to take over the operations of the primary server. The `Warm standby` redundancy type minimizes the inability to process interactions that may have originated during the time it took to detect the failure. It also eliminates the need to bring a backup server online, thereby increasing solution availability.

The backup server does not process client requests until its role is changed to primary by the Management Layer. When a connection is broken between the primary server and the LCA running on the same host, a failure of the primary process is reported. As a result, the Management Layer instructs the backup process to switch its role from backup to primary, and the former backup starts processing all new requests for service.

Note: To switch to `Primary` mode, the backup Configuration Server must have an active connection to the Configuration Database during the failure of the primary Configuration Server.

Although normal operations are restored as soon as the backup process takes over, the fault management effort continues. This consists of repeated attempts to restart the process that failed. Once it is restarted successfully, the process is assigned the backup role.

If Solution Control Server detects a loss of connection with the LCA of a host, it performs switchover for all applications located on the host, provided that backup applications are configured. There are two exceptions to this:

- A Configuration Server in backup mode ignores the switchover command if it detects another Configuration Server in primary mode. In other words, if the LCA residing on a host with a Configuration Server in primary mode goes down, the SCS requests that a Configuration Server in backup mode, on another host with an available LCA, switch over to primary mode.

When it receives the request, this Configuration Server checks whether the Configuration Server in primary mode is down, as indicated by a lost connection between the two Configuration Servers. The Configuration Server in backup mode switches over to primary mode only if this connection is down. If the connection still exists, no switchover occurs.

- An SCS in backup mode does not try to switch itself over if it can still detect the SCS that is in primary mode. In other words, if an SCS in backup mode loses its connection to an LCA residing on a remote host with an SCS in primary mode—either because the LCA went down or a network timeout caused the SCS to drop its connection—the SCS in backup mode checks whether it is still connected to the remote SCS in primary mode. If that connection is also lost, the SCS switches over to primary mode.

Hot Standby

Genesys uses the term *hot standby* to describe the redundancy type in which a backup server application remains initialized, clients connect to both the primary and the backup servers at startup, and the backup server data is synchronized with the primary server. Data synchronization and existing client connections to the backup guarantee higher availability of a component. For a complete description of the hot standby redundancy type, refer to the appropriate product documentation.

Supporting Components

Table 2 lists the Genesys components that support redundancy, and the redundancy types that each supports.

Table 2: Supported Redundancy Types

Component	Standby	
	Hot	Warm
Solution Control Server	X	
Message Server		X
DB Server		X
Configuration Server	X	
Stat Server		X
T-Servers	X	X
Network T-Servers	X[a]	

Table 2: Supported Redundancy Types (Continued)

Component	Standby	
	Hot	Warm
Load Distribution Server (LDS)	X	
Universal Routing Server (URS)	X	
Interaction Server		X
Universal Contact Server (UCS)		X
Call Progress Detection (CPD) Server		X
Outbound Contact Server (OCS)		X
E-mail Server Java		X
Web API Server		X
Chat Server		X
Contact Center Analyzer (CCA) Data Sourcer	X	
SIP Server	X	X
Genesys Voice Platform (GVP)	X[b]	
Integration Server (GIS)	X	
IVR Server		X

[a] Network T-Servers do not support warm or hot standby. Instead, they use a load-sharing redundancy schema. See the *Framework 7.6 Network T-Server Deployment Guide* for your T-Server for more information.

[b] Resource Manager only.

Feature Configuration

The configuration of redundant Genesys applications can vary, depending on application type. This section provides only a generic, high-level process. For more information, and for detailed instructions for setting up redundant applications in your environment, refer to the appropriate product documentation.

Procedure:
Summary—Setting up redundant applications

Purpose: To provide a generic summary of the process for setting up redundant applications. The process for some components may differ slightly. For more information, and for detailed instructions for setting up redundancy in your environment, refer to the appropriate product documentation.

Start of procedure

1. Create an `Application` object for the primary application.
2. Install the primary application.
3. Configure an `Application` object for the backup application.
4. Install the backup application.
5. In the primary `Application` object, add the backup `Application` object and select the `Redundancy Type` from the drop-down list.

End of procedure

Chapter

7 Proxy and Parallel Servers

This chapter describes the use of applications running in proxy or parallel mode to make your large configurations more efficient.

This chapter contains the following sections:

Feature Summary

Proxy and parallel servers add efficiency to large configurations, and can limit the damage caused by an outage.

Both configurations are a type of distributed configurations, but they differ in how the workload is distributed between the servers:

- In a proxy environment, each proxy server takes a portion of the workload and works on that portion exclusively.
- In a parallel environment, the workload is distributed among all of the servers, with one server attempting to keep the distribution as balanced as possible.

Proxy servers are particularly useful for systems that are widely dispersed over a large geographic area. In a proxy environment, the number of clients attached to a server is distributed across a set of servers (running in proxy mode), all of which funnel down to a central server (the Master).

Parallel servers enable load sharing. That is, multiple instances of a server run in parallel, and the load is distributed among them.

Security Benefits

The use of proxy and parallel servers greatly reduces the loss of functionality and data if a server goes out of service.

- If a proxy server fails, you lose only the clients associated with that proxy server. In a non-proxy environment with only one server instance, if that single server goes down, all the clients are lost.
- If a server in a parallel configuration fails, new requests are distributed to the remaining servers.

Supporting Components

The following components support some variation of proxy and/or parallel configuration. Refer to the appropriate product documentation for details of the configuration and how to implement it for your system.

- Solution Control Server—Distributed Solution Control Servers
- Message Server
- Configuration Server
- Load Distribution Server (LDS)—in T-Server proxy mode
- Universal Routing Server (URS)
- Interaction Server
- Call Progress Detection (CPD) Server
- E-mail Server Java
- Web API Server
- Chat Server
- Call Concentrator
- Network SIP Server
- Stream Manager
- Interaction Concentrator—does not support LDS
- Genesys Voice Platform (GVP)
- Voice Genie
- IVR Server

Feature Description

Proxy and parallel servers address the efficiency issue inherent in large configurations, and also minimize the loss of functionality and data in the event of an application failure.

Proxy servers are particularly useful for systems that are widely dispersed over a large geographic area. In a proxy environment, the clients that require a connections to a server are distributed across a set of servers (running in proxy mode), all of which down to a central server (the Master). If one proxy server fails, only the clients connected to that server are lost. Compare this to a single server environment, where, if the single server fails, the whole system is lost.

Parallel servers enable load sharing. That is, multiple instances of a server run in parallel and the load is distributed among them. If one of the parallel servers fails, new requests are distributed to the remaining servers so there should be no loss of service.

Feature Configuration

The configuration of proxy or parallel Genesys servers can vary, depending on the server type. For more information, and for detailed instructions for setting up proxy or parallel servers in your environment, refer to the appropriate product documentation.

Part

3 Server Integrity—Transport Layer Security

Part Three of this document describes the steps that you need to complete to use the Genesys Transport Layer Security (TLS) functionality, including examples of how to create certificates with the OpenSSL toolkit and Windows Certificate Services. It also describes security certificate installation and component configuration procedures for secure data exchange between Genesys components that support this functionality.

This information appears in the following chapters:

- Chapter 8, "Introduction to Genesys Transport Layer Security," on page 61
- Chapter 9, "Security Pack Installation," on page 65
- Chapter 10, "Certificate Generation and Installation," on page 69
- Chapter 11, "Genesys TLS Configuration," on page 87
- Chapter 12, "Troubleshooting Genesys TLS," on page 113

Chapter

8 Introduction to Genesys Transport Layer Security

This chapter introduces the Genesys Transport Layer Security (TLS) implementation and discusses general guidelines for your specific Genesys deployment. It contains the following section:

Feature Summary

Starting with release 7.5, Genesys supports an optional use of the Transport Layer Security protocol to secure data exchange between its components. TLS is an industry-standard protocol for secure communications on the Internet, and it is the successor of Secure Sockets Layer (SSL) 3.0.

All Genesys components are configured in Configuration Manager. To enable secure data exchange between the components, you must configure additional parameters in the `Host` objects, and in the `Application` objects that represent these components.

Note: The instructions in this document assume that you are adding the Transport Layer Security (TLS) feature to existing connections of your Genesys configuration—that is, that your applications have already been installed, properly configured, and associated with hosts and with each other. For information about configuring new hosts, applications, and associations between them, see the *Framework 7.6 Deployment Guide*.

To use the Genesys TLS functionality, you must complete the following steps:

1. For UNIX, install the Security Pack on each host computer where Genesys components run. See Chapter 9 on page 65.

2. Create and install certificates on UNIX and/or Windows platforms. See Chapter 10 on page 69.
3. Complete application-specific and/or host-specific configuration procedures in Configuration Manager. See Chapter 11 on page 87.

You can create and manage certificates and the corresponding private keys by using the OpenSSL toolkit and Windows Certification Services.

Security Benefits

TLS provides strong authentication, message privacy, and integrity capabilities. TLS secures data transmission by using a variety of encryption options. TLS also authenticates servers and, optionally, clients, to prove the identities of the parties engaged in secure communication. It also provides data integrity through an integrity check value. In addition to protecting against data disclosure, the TLS protocol can be used to help protect against masquerade attacks, man-in-the-middle attacks, bucket brigade attacks, rollback attacks, and replay attacks.

Supporting Components

This section lists the component connections that support secure data exchange.

Note: Starting with release 7.5, several Genesys components support Genesys TLS. For information about support for Genesys components, see the corresponding product documentation.

Configuration Layer Components

Secure data exchange is supported on all Configuration Layer connections:

- Between Configuration Server and Configuration Manager
- Between Configuration Server and Configuration Server Proxy
- Between Configuration Server and DB Server
- Between primary and backup Configuration Servers

Management Layer Components

Secure data exchange is supported on the following Management Layer connections:

- Between Solution Control Server (SCS) and Solution Control Interface (SCI)
- Between SCS and Configuration Server/Configuration Server Proxy
- Between SCI and Configuration Server/Configuration Server Proxy

- Between SCI and DB Server
- Between primary and backup Solution Control Servers
- Between Message Server and DB Server

Note: In release 7.5, secure data exchange is not supported on connections between Message Server and its clients.

Media Layer Components

Secure data exchange is supported on the following Media Layer connections:

- Between T-Servers
- Between Network T-Servers
- Between T-Server and Network T-Server
- Between T-Server/Network T-Server and Configuration Server/Configuration Server Proxy
- Between primary and backup T-Servers in `hot standby` mode
- Between T-Server and custom client applications that have been created with the new T-Library

Universal Routing Components

Secure data exchange is supported between all Universal Routing components and those Framework components that support this feature.

Outbound Contact Components

Secure data exchange is supported on the following Outbound Contact and Framework connections:

- Between Outbound Contact Server and CPD Server/CPD Proxy Server
- Between Outbound Contact Server and Configuration Server/Configuration Server Proxy
- Between Outbound Contact Server and T-Server
- Between Outbound Contact Server and DB Server
- Between CPD Server and CDP Proxy Server
- Between CPD Server and T-Server
- Between CPD Server/CDP Proxy Server and Configuration Server/Configuration Server Proxy

Environment Prerequisites

The instructions in this document assume that you are adding the Genesys TLS to existing connections of your Genesys configuration—that is, that your applications have already been installed, properly configured, and associated with hosts and with each other. See the *Framework 7.6 Deployment Guide* for information about and deployment instructions for these Framework components.

Supported Platforms

Note: Genesys TLS is not supported on all operating systems that Genesys products support. For UNIX-based operating systems, see "Setting the Environment Variable" on page 67 for more information.

For supported Windows versions, refer to the *Genesys 7 Supported Operating Systems and Databases* white paper that provides the list of operating systems and database systems supported in Genesys releases 7.x. You can find this document on the Genesys Technical Support website at `http://genesyslab.com/support/dl/retrieve/default.asp?item=B6C52FB62DB42BB229B02755A3D92054&view=item`

Abbreviations

This document uses the following terms and abbreviations:

CA	Certification Authority
PEM format	A text (ASCII) format that can be used to encode certificates
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
TLS	Transport Layer Security

Chapter

9 Security Pack Installation

This chapter describes how to install and configure the Genesys Security Pack on UNIX. The Security Pack provides the components—such as shared libraries and an example of a Certification Authority (CA)—that are used to generate certificates and to deploy them on UNIX computers on which Genesys components are installed.

This chapter contains the following sections:

Note: The Genesys Security Pack on UNIX must be installed on each UNIX host computer on which Genesys components are installed.

Supported Operating Systems

The Genesys Security Pack on UNIX is supported on the following operating systems:

Table 3: Supported Operating Systems

Operating System	Versions
AIX 32-bit mode	5.2, 5.3
HP-UX 32-bit mode	11.0, 11.11
HP-UX 64-bit mode	11.0, 11.11, 11i v2
Linux 32-bit mode	RHEL 3.0, RHEL 4.0

Table 3: Supported Operating Systems (Continued)

Operating System	Versions
Solaris 32-bit mode	8, 9
Solaris 64-bit mode	8, 9, 10

Security Pack Installation

Security Pack installation consists of the following steps:

1. Installing the Security Pack on UNIX
2. Setting the environment variable that corresponds to your operating system

Procedure: Installing the Security Pack on UNIX

Start of procedure

1. On the Security Pack 7.5 product CD, in the `security_pack` directory, open the directory corresponding to your operating system, and locate the shell script called `install.sh`.
2. Run this script from the command prompt by typing the following at the command line:

   ```
   sh install.sh
   ```

3. When prompted, specify the host name of the computer on which you want to install the Security Pack.
4. Specify the full path to the directory in which you want to install the Security Pack.

As soon as the installation process is finished, a message appears, indicating that the installation was successful. The installation process places the Security Pack in the directory that you specified in Step 4.

End of procedure

Next Steps

- "Setting the Environment Variable" on page 67

Setting the Environment Variable

After you install the Security Pack, you must set the environment variable that corresponds to your operating system (see Table 4), and you must also specify the path to the Security Pack libraries.

Table 4: Environment Variables

Operating System	Environment Variable Name
AIX	LIBPATH
HP-UX 32-bit mode	SHLIB_PATH
HP-UX 64-bit mode	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
Solaris	LD_LIBRARY_PATH and/or LD_LIBRARY_PATH_64

Chapter

10 Certificate Generation and Installation

This chapter provides an overview of typical steps of the process of certificate generation using the open source OpenSSL tool and Windows Certificate Services. Please keep in mind that the actual process of certificate generation in a specific environment is highly dependent on the security policies of your IT organization and tools used, and may, therefore, be different from the process described in this chapter. Genesys recommends that you consult with your network administrator before generating certificates for secure data exchange between Genesys components.

This chapter contains the following sections:

Note that, although you can use OpenSSL to generate certificates on both UNIX and Windows, Windows Certificate Services is available only on the Windows Server operating system. Nevertheless, the certificates generated by both methods can be used for secure data exchange between applications that run on both Windows and UNIX operating systems.

Genesys recommends that you use OpenSSL if you intend to run any applications that might require secure connections on UNIX. If you intend to run all your applications on Windows, Windows Certificate Services is recommended.

Generating Certificates with OpenSSL

This section provides examples of creating certificates with the OpenSSL tool. The procedure consists of the following steps:

1. Set up a Certification Authority (CA) (see page 70).

2. Generate certificates by using the CA that you set up in Step 1 (see page 72).
3. Install the certificates on UNIX and/or Windows (see page 73).

In the directory in which you installed the Security Pack, locate the following scripts:

- `create_ca.sh`—Creates the CA structure in which CA files and generated certificates are stored.
- `create_cert.sh`—Creates the certificates to use on UNIX and Windows computers.

Note: For information about the installed files, see Chapter 9 on page 65.

The scripts that are used to generate certificates require the OpenSSL toolkit, which you can obtain from the OpenSSL Project website:

`http://www.openssl.org`

You can obtain build binaries of OpenSSL tools for the Windows operating system from the following URL, which is also located on the OpenSSL Project website:

`http://www.slproweb.com/products/Win32OpenSSL.html`

Setting Up a Certification Authority

Note: Genesys recommends that you use only one CA instance for your entire call center environment.

To set up a CA:

1. Create a CA directory in which CA files—scripts, configuration files, and generated certificates—will be stored.
2. Copy the `create_ca.sh` and `create_cert.sh` scripts from the installation package to the CA directory that you just created. Make sure that these scripts have executable permissions.
3. Run the `create_ca.sh` script from the bash shell by specifying the parameters (see Table 5) in the following command line:

```
create_ca.sh [-keySz KEY_SIZE] [-time VALID_TIME] -CN COMMON_NAME
[-E EMAIL] [-OU ORG_UNIT] [-O ORGANIZATION] [-L LOCALITY] [-S STATE]
[-C COUNTRY]
```

Table 5: CA Script Parameters

Parameter	Description
KEY_SIZE	(Optional) The size, in bits, of the CA private key. The default value is `2048` bits.

Table 5: CA Script Parameters (Continued)

Parameter	Description
VALID_TIME	(Optional) The amount of time, in days, that the CA is valid. The default value is `356` days.
COMMON_NAME	(Mandatory) The name of the CA.
EMAIL	(Optional) The e-mail address of the person who is responsible for this CA.
ORG_UNIT	(Optional) The name of the organization unit that is responsible for this CA.
ORGANIZATION	(Optional) The name of the organization that is responsible for this CA.
LOCALITY	(Optional) The name of the city.
STATE	(Optional) The name of the state or region.
COUNTRY	(Optional) Two-letter abbreviation for the country.

For example:

```
create_ca.sh -CN "Basic Certification Authority" -E
"youremail@yourdomain.com" -OU "Department" -O "Genesys
Telecommunication Labs" -L "Daly City" -S CA -C US
```

Certificate Authority Files

After successful script execution, the following data structure is created:

- `ca_conf`—This directory contains the following files:
  - `ca_cert.pem`—The CA self-signed certificate file.

    Note: You must copy this file to each computer that will host Genesys components that might require secure data exchange. For more information, see “Installing Certificates” on page 73.

  - `ca_priv_key.pem`—The CA private key.

    This file is used to sign all certificates that this CA issues. This file must be read-only, and it must be readable only by the CA administrator account.
  - `ca.db`—The internal CA database used by the OpenSSL toolkit.
  - `serial.num`—The internal CA file that contains the serial number of the next generated certificate. The serial number is a unique identifier of the certificate that the CA issues.
  - `ca.conf`—The internal CA configuration file.

- repository—This directory contains the files that this CA generates. For more information, see "Generating Certificates Using CA".

Generating Certificates Using CA

After you set up the CA, you are ready to use the CA to generate certificates.

Note: Genesys recommends that you use the same CA to generate all certificates for a particular environment.

To generate a certificate for a particular host computer:

1. Go to the CA directory in which the CA files are stored.
2. Run the create_cert.sh script from the bash shell by specifying the parameters (see Table 6) in the following command line:

```
create_cert.sh [-keySz KEY_SIZE] [-time VALID_TIME] -host HOST_NAME
-CN COMMON_NAME [-OU ORG_UNIT] [-O ORGANIZATION] [-L LOCALITY] [-S
STATE] [-C COUNTRY]
```

   For example:

```
create_cert.sh -host myHOST.domain1.domain2.com -CN myWorkstation
```

Table 6: Certificate Script Parameters

Parameter	Description
KEY_SIZE	(Optional) The size, in bits, of the host private key. The default value is 2048 bits.
VALID_TIME	(Optional) The amount of time, in days, that the certificate is valid. The default value is 100 days.
HOST_NAME	(Mandatory) The full name of the DNS host.
COMMON_NAME	(Mandatory) The name of the host.
ORG_UNIT	(Optional) The name of the organization unit.
ORGANIZATION	(Optional) The name of the organization.
LOCALITY	(Optional) The name of the city.
STATE	(Optional) The name of the state or region.
COUNTRY	(Optional) The two-letter abbreviation for the country.

Host Certificate Files

After successful script execution, the following files are created in the `repository` directory:

- `<serial_#>_<host_name>_cert.pem`—The host certificate for UNIX.
- `<serial_#>.pem`—The auxiliary file for certificate generation for UNIX.
- `<serial_#>_<host_name>_priv_key.pem`—The host private key for UNIX.
- `<serial_#>_<host_name>_cert.pfx`—The PKCS #12 file format, private key, and certificate for Windows.

  Where:

  - `<serial_#>` is the serial number of the generated certificate. This number is unique for all certificates that this CA generates.
  - `<host_name>` is the name of your host computer, which is the first part of the full DNS host name.

Installing Certificates

After you generate certificates, you are ready to install them on UNIX and/or Windows.

Note: You need to install the CA self-signed certificate file, `ca_cert.pem`, and at least one certificate issued by this CA on each computer that hosts Genesys applications that may require secure data exchange.

On UNIX

To install certificates on a UNIX host computer:

1. Copy the `ca_cert.pem` file to the computer.
2. Copy the `<serial_#>_<host_name>_cert.pem` and `<serial_#>_<host_name>_priv_key.pem` files to a local directory on the computer.
3. Make sure that these files are readable by all Genesys applications that are running on this host computer.

Warning! The `<serial_#>_<host_name>_priv_key.pem` file contains critical security information. Make sure it can only be accessed by personnel authorized to work with this type of information.

When you configure an application to support secure data exchange on UNIX in Configuration Manager:

- The full path to the `ca_cert.pem` file is copied to the `Trusted CA` text box of the `Certificate` properties.

- The full path to the `<serial_#>_<host_name>_cert.pem` file is copied to the `Certificate` text box of the `Certificate` properties.
- The full path to the `<serial_#>_<host_name>_priv_key.pem` file is copied to the `Certificate Key` text box of the `Certificate` properties.

For more information, see Chapter 11 on page 87.

On Windows

Note: For server applications, the certificates must be installed under the `Local Computer` account. For client applications, the certificates must be installed under the `Current User` account. For more information, see “Managing Certificates in MMC” on page 82.

To install the certificates on a Windows computer:

1. From the Windows `Start` menu, select `Run`, and then execute the `mmc` command to start the Microsoft Management Console (MMC).
2. On the left pane of MMC, click the `Certificates` folder. (If there is no `Certificates` folder on the left pane, see “Managing Certificates in MMC” on page 82.)
3. Right-click the `Trusted Root Certificates Authorities` folder, and select `All Tasks > Import` from the shortcut menu. This starts the Certificate Import Wizard.
4. On the first Wizard page, click `Next`.
5. On the `File to Import` page, type the full name of the `ca_cert.pem` file that was created during the CA setup, and then click `Next`.
6. On the `Certificate Store` page, select `Place all certificates in the following store`. Make sure that the `Certificate store` text box is set to `Trusted Root Certification Authorities`. Click `Next`.
7. Click `Finish`.
8. On the left pane, click the `Certificates` folder.
9. On the left pane, right-click the `Personal` folder, and select `All Tasks > Import` from the shortcut menu. This starts the Certificate Import Wizard.
10. On the first Wizard page, click `Next`.
11. On the `File to Import` page, type the full name of the `<serial_#>_<host_name>_cert.pfx` file that was created during certificate generation. Click `Next`.
12. On the `Password` page, click `Next`.

    The host certificates in the PKSC #12 format are generated with an empty password.

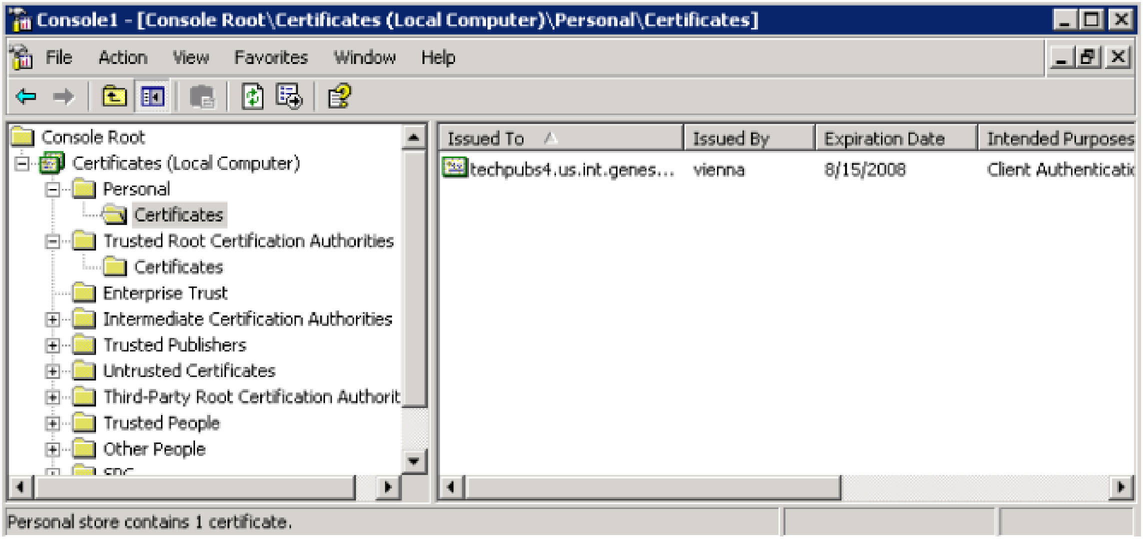
13. On the `Certificate Store` page, select `Place all certificates in the following store`. Make sure that the `Certificate store` text box is set to `Personal`. Click `Next`.

14. Click `Finish`.

15. Press `F5` to update the MMC view.

16. On the left pane, select `Certificates > Personal > Certificates`.

17. On the right pane, locate the imported certificate in the list, and double-click it (see Figure 1).


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorit
Trusted People
Other People
SPC

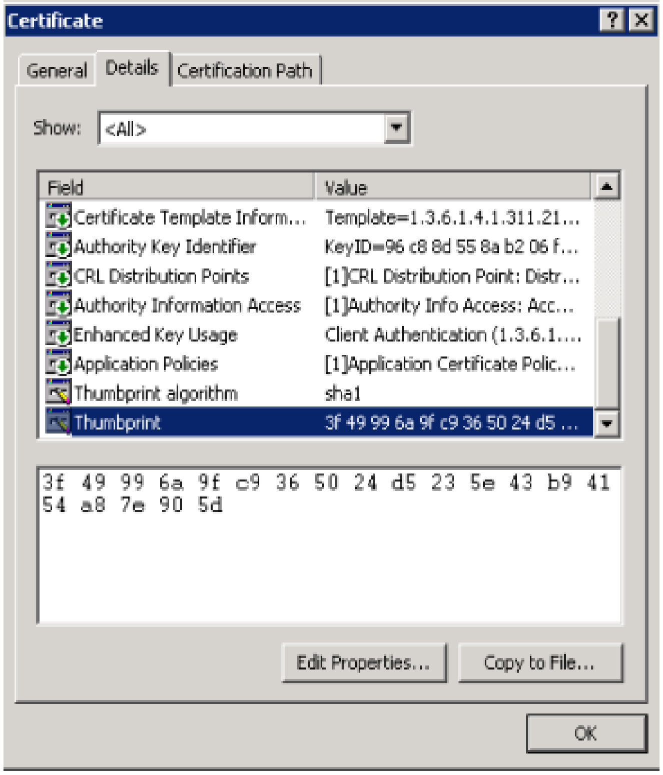
Issued To	Issued By	Expiration Date	Intended Purposes
techpubs4.us.int.genes...	vienna	8/15/2008	Client Authenticati

Personal store contains 1 certificate.

Figure 1: Microsoft Management Console Window

18. In the `Certificate` dialog box, click the `Details` tab.

19. To view the certificate thumbprint, select `Thumbprint` from the list. The thumbprint, consisting of a string of hexadecimal digits, appears in the lower part of the dialog box (see Figure 2).



Show: <All>

Field	Value
Certificate Template Inform...	Template=1.3.6.1.4.1.311.21...
Authority Key Identifier	KeyID=96 c8 8d 55 8a b2 06 f...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Application Policies	[1]Application Certificate Polic...
Thumbprint algorithm	sha1
Thumbprint	3f 49 99 6a 9f c9 36 50 24 d5 ...

```
3f 49 99 6a 9f c9 36 50 24 d5 23 5e 43 b9 41
54 a8 7e 90 5d
```

Figure 2: Certificate Dialog Box—Details Tab

Generating Certificates with Windows Certificate Services

This section provides examples of creating certificates using the Windows Certificate Services.

The Genesys TLS functionality requires that security certificates comply with following requirements:

1. The certificates that will be used by Genesys server applications must contain these extended attributes: `serverAuth`, `clientAuth`, and `emailProtection`.
2. The certificates that will be used by Genesys GUI applications must contain these extended attributes: `clientAuth` and `emailProtection`.

Make sure that certificate templates are properly configured for server and GUI applications to satisfy these requirements.

Note: The examples provided in this section assume that Windows Certificate Services have been installed and configured. For information about how to install and configure Windows Certificate Services, see the appropriate Windows documentation.

The procedure for generating certificates with Windows Certificate Services consists of the following steps:

1. Generate a certificate on a computer that is running the Windows Server operating system, and that has Windows Certificate Services installed and configured (see page 77).
2. Retrieve the certificate (see page 81).
3. Install the certificate on the computer that hosts Genesys applications. If this computer is different from the one on which you generated the certificate, you must first export the certificate. For more information, see “Exporting Certificates” on page 83.
4. Convert the certificate from the PKCS #12 format to the PEM format (see page 84). This step is necessary to install the Windows-created certificate on UNIX.

If you want to obtain the certificate from a remote computer, see “Obtaining Certificates from a Remote Computer” on page 85.

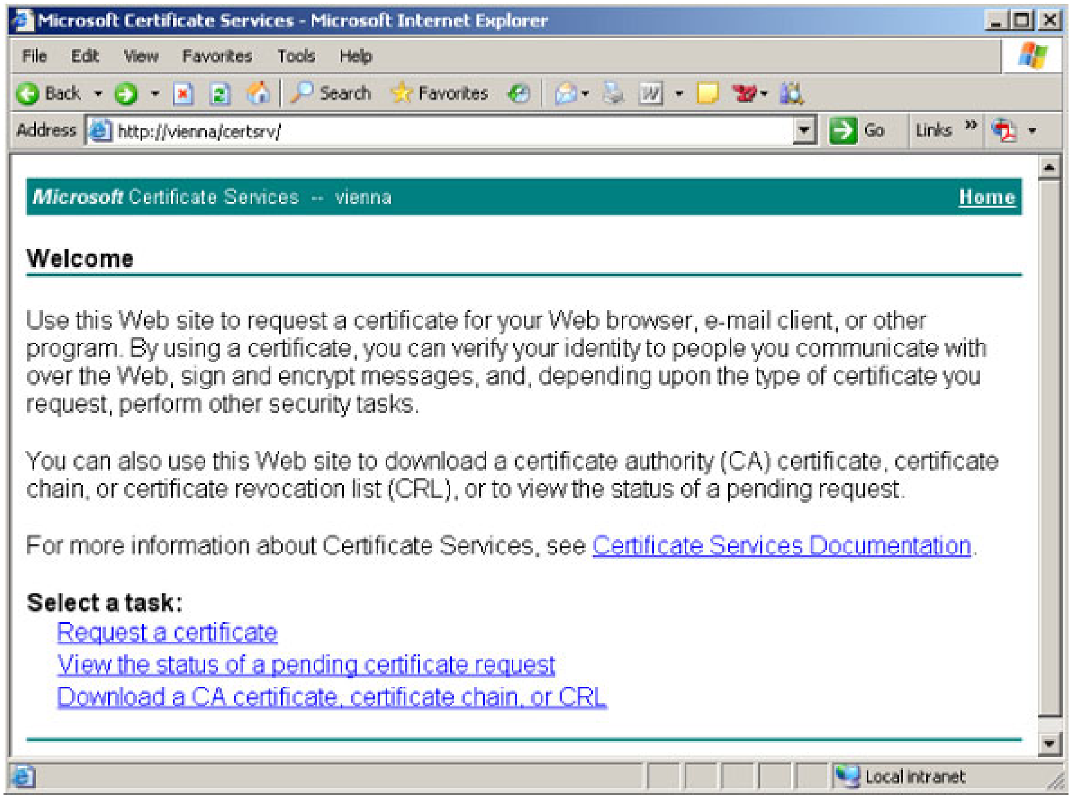
Generating Certificates

To generate a certificate:

1. Open a Web browser, and enter the following URL:

   `http://<server-name>/certsrv`

   Where: `<server-name>` is the server that runs the Windows Server operating system, and that has Windows Certificate Services installed and configured.
2. On the *Microsoft* Certificate Services `Welcome` (or `Home`) page, click the `Request a certificate` link (see Figure 3 on page 78).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://vienna/certsrv/
Go Links
Microsoft Certificate Services -- vienna
Home
Local intranet

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

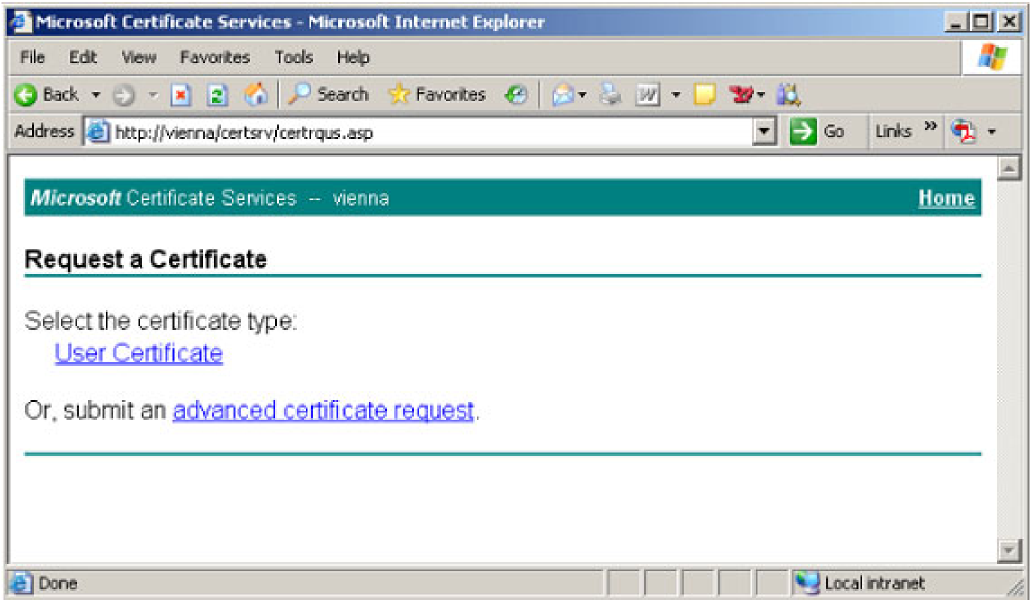
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Figure 3: *Microsoft* Certificate Services Home Page

3. On the `Request a Certificate` page, click the `advanced certificate request` link (see Figure 4).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://vienna/certsrv/certrqus.asp
Go Links
Microsoft Certificate Services -- vienna
Home
Done
Local intranet

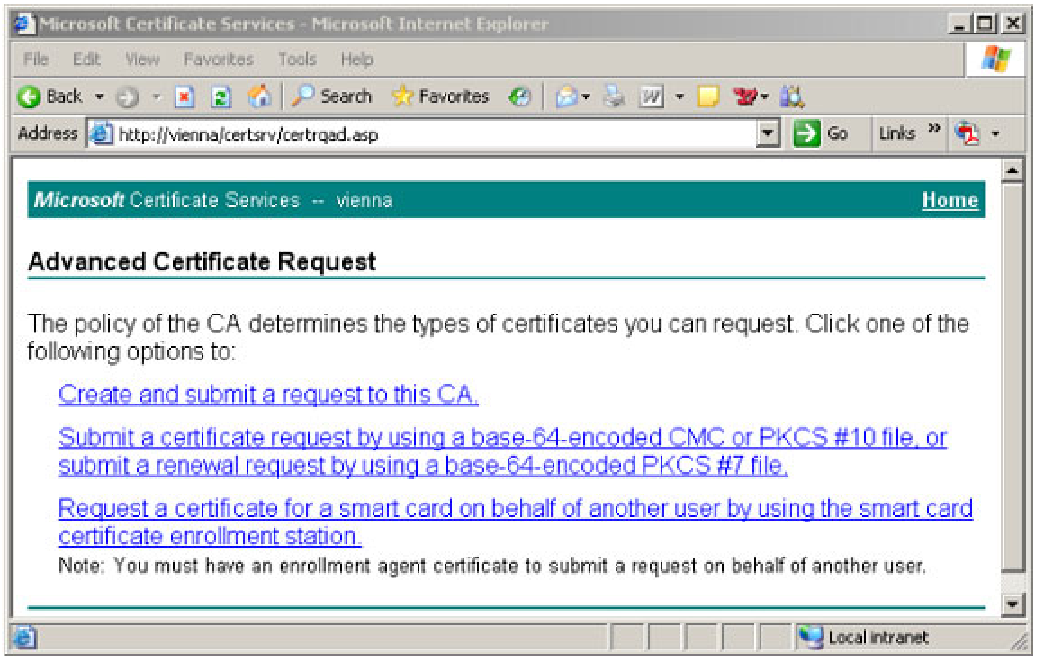
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Figure 4: Request a Certificate Page

4. On the `Advanced Certificate Request` page, click the `Create and submit a request to this CA` link (see Figure 5).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://vienna/certsrv/certrqad.asp
Go
Links
Local intranet

Microsoft Certificate Services -- vienna **Home**

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Figure 5: Advanced Certificate Request Page

5. On the `Advanced Certificate Request` page, enter the following information:

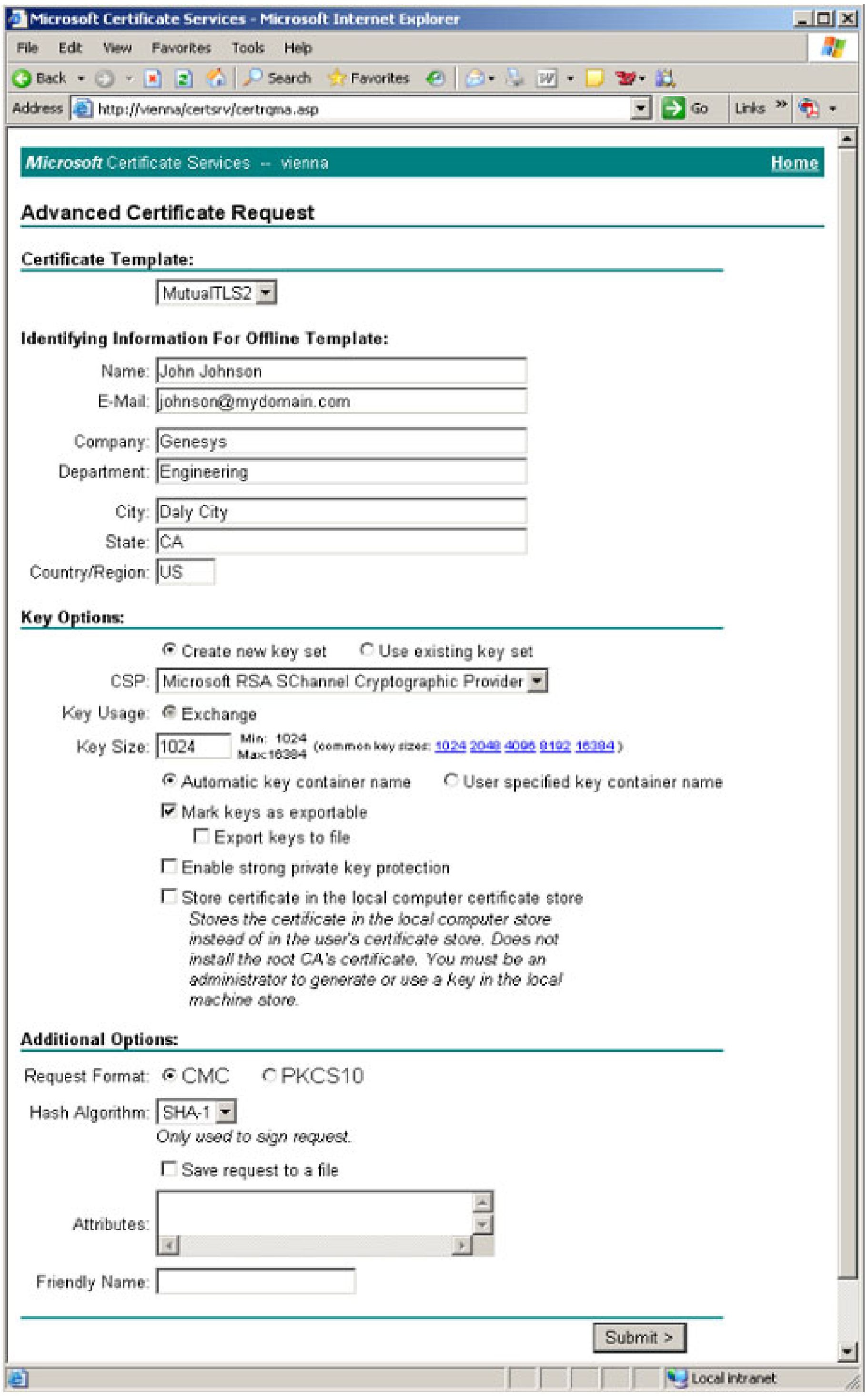
   a. In the `Certificate Template` text box, select an appropriate certificate template—for example, `MutualTLS2`.

   b. In the `Name` text box, type the full name of the DNS host.

   c. Under `Key Options`:

      - Select `Create new key set`.
      - In the `Key Size` text box, specify the size of the key.
      - Select `Automatic key container name` or `User specified key container name`, depending on your needs.
      - Select `Mark key as exportable`.

   d. Click `Submit` (see Figure 6 on page 80).



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://vienna/certsrv/certrqma.asp
Go Links
Microsoft Certificate Services -- vienna
Home

Advanced Certificate Request

Certificate Template:

MutualTLS2

Identifying Information For Offline Template:

Name: John Johnson
E-Mail: johnson@mydomain.com
Company: Genesys
Department: Engineering
City: Daly City
State: CA
Country/Region: US

Key Options:

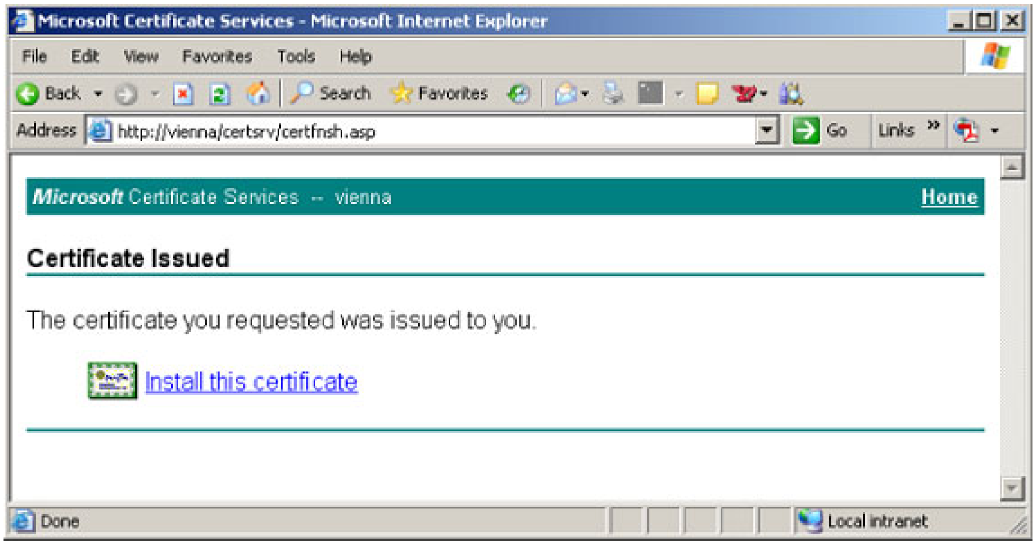
● Create new key set ○ Use existing key set
CSP: Microsoft RSA SChannel Cryptographic Provider
Key Usage: ● Exchange
Key Size: 1024 Min: 1024 Max:16384 (common key sizes: 1024 2048 4096 8192 16384)
● Automatic key container name ○ User specified key container name
☑ Mark keys as exportable
□ Export keys to file
□ Enable strong private key protection
□ Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ● CMC ○ PKCS10
Hash Algorithm: SHA-1
Only used to sign request.
□ Save request to a file
Attributes:
Friendly Name:

Figure 6: Advanced Certificate Request Page

6. After you submit the certificate request, the confirmation page appears followed by the `Certificate Issued` page. On the `Certificate Issued` page, click the `Install this certificate` link (see Figure 7).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
Done
Local intranet

Address http://vienna/certsrv/certfnsh.asp

Microsoft Certificate Services -- vienna Home

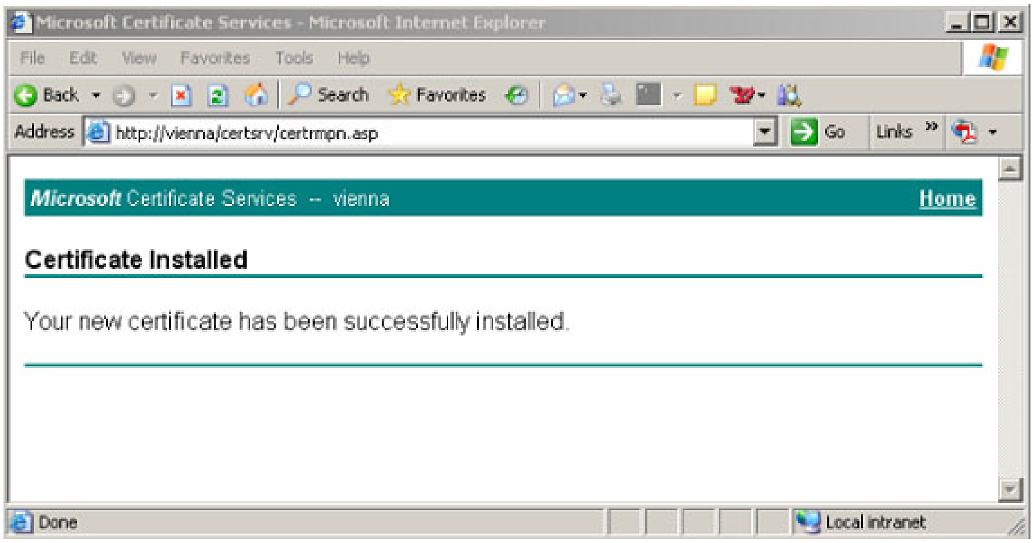
Certificate Issued

The certificate you requested was issued to you.

Install this certificate

Figure 7: Certificate Issued Page

7. After you accept the system warning prompts that appear, the `Certificate Installed` page appears (see Figure 8).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
Done
Local intranet

Address http://vienna/certsrv/certrmpn.asp

Microsoft Certificate Services -- vienna Home

Certificate Installed

Your new certificate has been successfully installed.

Figure 8: Certificate Installed Page

Retrieving Certificates

If you did not install the certificate in Step 6 on page 80, you can retrieve and install it as follows:

1. On the *Microsoft* Certificate Services `Home` page (see Figure 3 on page 78), click the `View the status of a pending certificate request` link.

2. Select the appropriate request from the list.

   If the certificate request is approved, the `Certificate Issued` page appears.

3. Click the `Install this certificate` link to install the certificate.

Managing Certificates in MMC

You can use the Microsoft Management Console (MMC) to manage the certificates on a Windows platform. For more information, see *Microsoft Management Console Help*.

Configuring MMC for Certificate Management

To configure MMC for certificate management:

1. From the Windows `Start` menu, select `Run`, and then execute the `mmc` command to start the Microsoft Management Console.
2. Select `File > Add/Remove Snap-in`.
3. In the `Add/Remove Snap-in` dialog box, click `Add`.
4. In the `Add Standalone Snap-in` dialog box, select `Certificates` from the list, and then click `Add`.
5. In the `Certificates snap-in` dialog box, select `Computer account`, and then click `Next`.

   Note: To manage certificates for client applications, select the `My user account` option.

6. In the `Select Computer` dialog box, select `Local computer,` and then click `Finish`.
7. In the `Add Standalone Snap-in` dialog box, click `Close`.
8. In the `Add/Remove Snap-in` dialog box, click `OK`.

   The `Certificates` item is added under `Console Root` on the left pane (see Figure 9 on page 83).

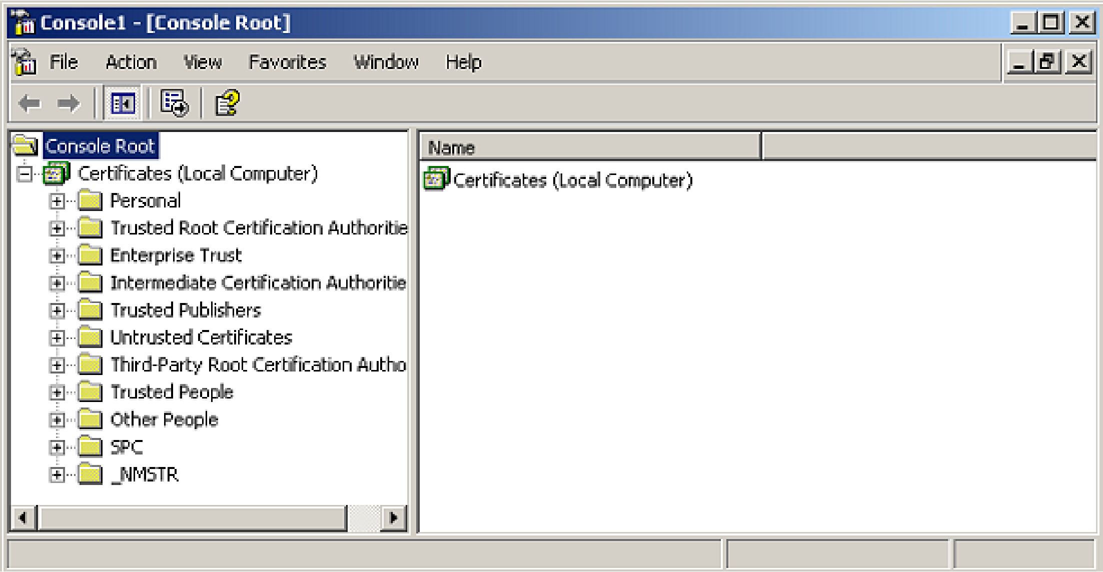

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authoritie
Enterprise Trust
Intermediate Certification Authoritie
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Autho
Trusted People
Other People
SPC
_NMSTR
Name
Certificates (Local Computer)

Figure 9: Configuring MMC for Certificate Management

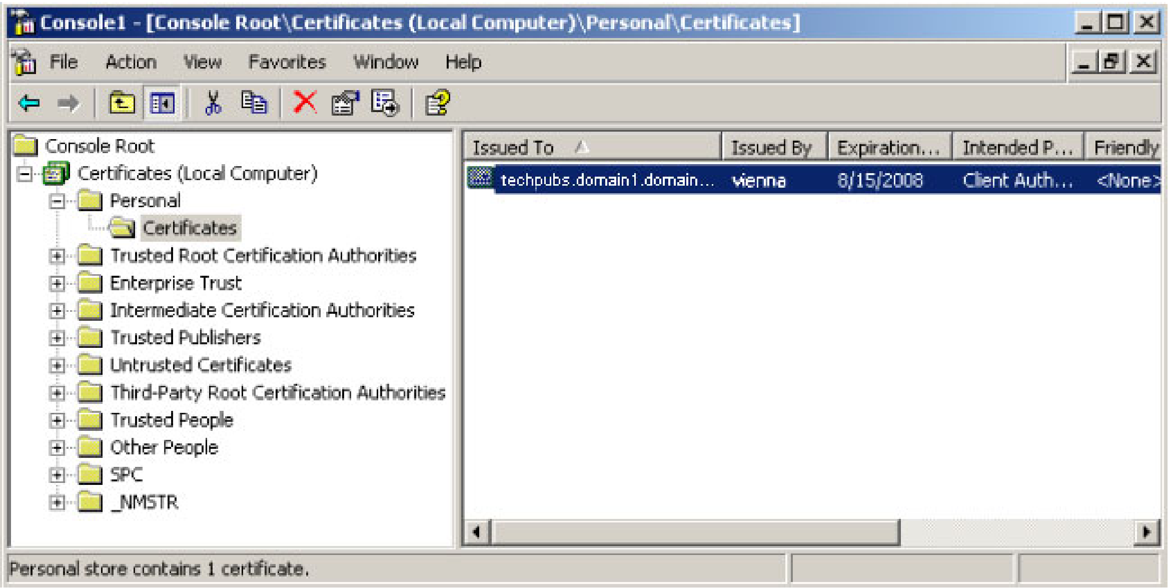
You can save the MMC configuration in the file by selecting File > Save As.

Exporting Certificates

To install the certificate and private key on another computer, you must export them, as follows:

1. From the Windows Start menu, select Run, and then execute the mmc command to start the Microsoft Management Console.
2. Open your saved console configuration, or select File > Add/Remove Snap-in.
3. In the Add/Remove Snap-in dialog box, click Add.
4. In the Add Standalone Snap-in dialog box, select Certificates from the list, and then click Add.
5. In the Certificates snap-in dialog box, select Computer account, and then click Next.
6. In the Select Computer dialog box, select Local computer, and then click Finish.
7. In the Add Standalone Snap-in dialog box, click Close.
8. In the Add/Remove Snap-in dialog box, click OK.

   The Certificates item is added under Console Root on the left pane (see Figure 10 on page 84).


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
SPC
_NMSTR

Issued To	Issued By	Expiration...	Intended P...	Friendly
techpubs.domain1.domain...	vienna	8/15/2008	Client Auth...	<None>

Personal store contains 1 certificate.

Figure 10: Exporting Certificates with MMC

9. On the right pane, locate the certificate in the list, and right-click it. Then, select `All Tasks > Export` from the shortcut menu to start the Certificate Export Wizard.
10. On the first Wizard page, click `Next`.
11. On the next page, select `Yes, export the private key`, and then click `Next`.
12. On the `Export File Format` page, the only available export file format will be `PKCS #12`. Click `Next`.
13. On the `Password` page, type and confirm your password. Click `Next`.
14. On the `File to Export` page, specify the path and file name for your certificate. Click `Next`.
15. Click `Finish` to complete the export procedure.

Converting PKCS #12 to PEM

If you must install the Windows-created certificate on a UNIX platform, type the following command line by using OpenSSL:

```
openssl pkcs12 -nodes -passin pass:<password> -in <pfx file> -out <pem
file>
```

Where:

- `<password>` is the password that you set during the PKCS #12 file export session. This field can be empty.
- `<pfx file>` is the name of the certificate file in the PKCS #12 format.
- `<pem file>` is the name of the output file.

After the conversion, the <pem file> contains both the certificate and private key data. Now you can create two separate text files for certificate and private key data and copy the corresponding data to them using the following format:

- In the certificate file, copy a certificate data block starting with "---BEGIN CERTIFICATE---" and ending with "---END CERTIFICATE---" into a certificate data file:

  ```
  ---BEGIN CERTIFICATE---
  [certificate data]
  ---END CERTIFICATE---
  ```

- In the private key file, copy an RSA private key data block starting with "---BEGIN RSA PRIVATE KEY---" and ending with "---End RSA PRIVATE KEY---" into a RSA private key data file:

  ```
  ---BEGIN RSA PRIVATE KEY---
  [private key data]
  ---END RSA PRIVATE KEY---
  ```

Obtaining Certificates from a Remote Computer

To obtain a certificate from a remote computer:

1. From the Windows Start menu, select Run, and then execute the mmc command to start Microsoft Management Console.
2. Select File > Add/Remove Snap-in.
3. In the Add/Remove Snap-in dialog box, click Add.
4. In the Add Standalone Snap-in dialog box, locate and select Certificates in the list. Click Add.
5. In the Certificates snap-in dialog box, select Computer account, and then click Next.
6. In the Select Computer dialog box, select Another computer, and then either type the name of the remote target computer or use the Browse button to search for it. Then, click Finish.
7. In the Add/Remove Snap-in dialog box, click OK.

   A new snap-in item is added under Console Root in the main snap-in console window.

   You can browse for examples of all the certificates on the target computer, or you can view information about a particular certificate. Depending on the options that you select, MMC also enables you to remotely manage certificates on a target computer.
8. On the left pane, select Certificates > Personal > Certificates.
9. On the right pane, locate the certificate in the list, and double-click it (see Figure 1 on page 75).
10. In the Certificate dialog box, click the Details tab.

11. Select `Thumbprint` from the list. The value, consisting of a string of hexadecimal digits, appears in the lower part of the dialog box (see Figure 2 on page 76 for an example).
12. Use the string of hexadecimal digits for the security configuration. For more information, see Chapter 11 on page 87.

Chapter

11 Genesys TLS Configuration

After you generate the certificates and install them on the host computers, you must configure Genesys applications to use them on the connections that need to be secure. (By default, connections between Genesys applications are not secure.) This chapter describes how to perform this configuration. It contains the following sections:

Overview

The configuration process consists of the following steps:

1. For server applications, add a new secure port or modify the existing server port for secure connections and configure a certificate to be used by this application (the host certificate is recommended).
2. For client applications, change the connection setting to connect to secure server ports.

Note: For clients of server type, complete configuration procedures required for server applications.

You configure all secure connections in the same way, regardless of the types of participating client and server applications. The only exceptions are the Configuration Server connections; for information about these connections, see

"Configuring a Secure Connection Between Configuration Server and DB Server" on page 106.

Notes: The instructions in this chapter assume that you are adding the Genesys Transport Layer Security (TLS) to existing connections of your Genesys 7.6 environment—that is, that your applications have already been installed, properly configured, and associated with hosts and with each other. For information about configuring new hosts, applications, and associations between them, see the *Framework 7.6 Deployment Guide*.

If you are using Genesys components of previous releases, you must upgrade them to release 7.6 before you can configure secure connections between them.

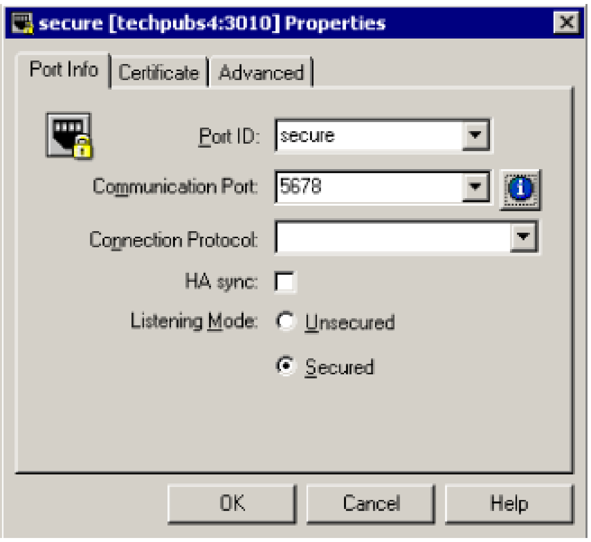
Configuring Secure Ports

In release 7.5, the server applications that support the Genesys TLS have been modified to support multiple server ports. This enables you to set up secure communications on only those connections for which security is considered necessary, rather than all server connections at the same time. If you intend to use the secure data exchange capabilities on connections to a specific server, Genesys recommends that you configure a new port for such secure connections, and that you leave the existing unsecured port intact for connections that do not require security.

Procedure: Configuring a secure port for an application of server type

Start of procedure

1. Open the `Application Properties` dialog box.
2. Click the `Server Info` tab.
3. In the `Ports` section, click `Add Port`. The `Port Properties` dialog box appears (see Figure 11 on page 89).



Port ID: secure

Communication Port: 5678

Connection Protocol:

HA sync: □

Listening Mode: ○ Unsecured ● Secured

Figure 11: Port Properties Dialog Box

4. In the `Port Properties` dialog box, on the `Port Info` tab:
   a. In the `Port ID` box, enter the port ID.
   b. In the `Communication Port` box, enter the number of the new port.
   c. In the `Connection Protocol` box, select the connection protocol, if necessary.
   d. Select the `Secured` option. (If the application whose port you are configuring is a Configuration Server, select the `Auto Detect` option instead. See "Configuring an Auto-Detect Port for Configuration Server" on page 105.)
   e. Click `OK`.
5. Click `OK` to save the new configuration.

End of procedure

Assigning Security Certificates

After you create new server ports for secure connections, you must configure certificates, in one of the following ways:

- Assign a certificate to a host, and then use this certificate to secure data exchange via any secure port of any server application that is located on this host.
- Assign a certificate to a server application, and then use this certificate to secure data exchange via any secure port of this application. A certificate that is assigned to an application takes precedence over the certificate that is assigned to a host.

- Assign a certificate directly to a specific port of a server application to secure data exchange via this port. A certificate that is assigned to a port takes precedence over certificates that are assigned to hosts and applications.

Note: Genesys recommends that, unless you have compelling reasons to have any of your applications and/or ports protected by their own individual certificate, you keep the certificate assignment at the host level and then use the host certificates to provide secure data exchange for all applications residing on your hosts.

To display security-related properties in Configuration Manager:

1. From the Configuration Manager main menu, select `View > Options`.
2. In the `Options` dialog box, select the `Show advanced security information` check box.
3. Click `OK`.

Note: Before configuring secure data exchange, make sure that certificates are installed on the host computers on which specific Genesys components run, and that the certificate information is available to you. See “Installing Certificates” on page 73.

Assigning a Certificate to a Host

To use a host’s certificate to secure data exchange via any ports of any server applications on that host, you must first assign a certificate to the host, and then complete the server application configuration.

Procedure: Assigning a certificate to a host

Start of procedure

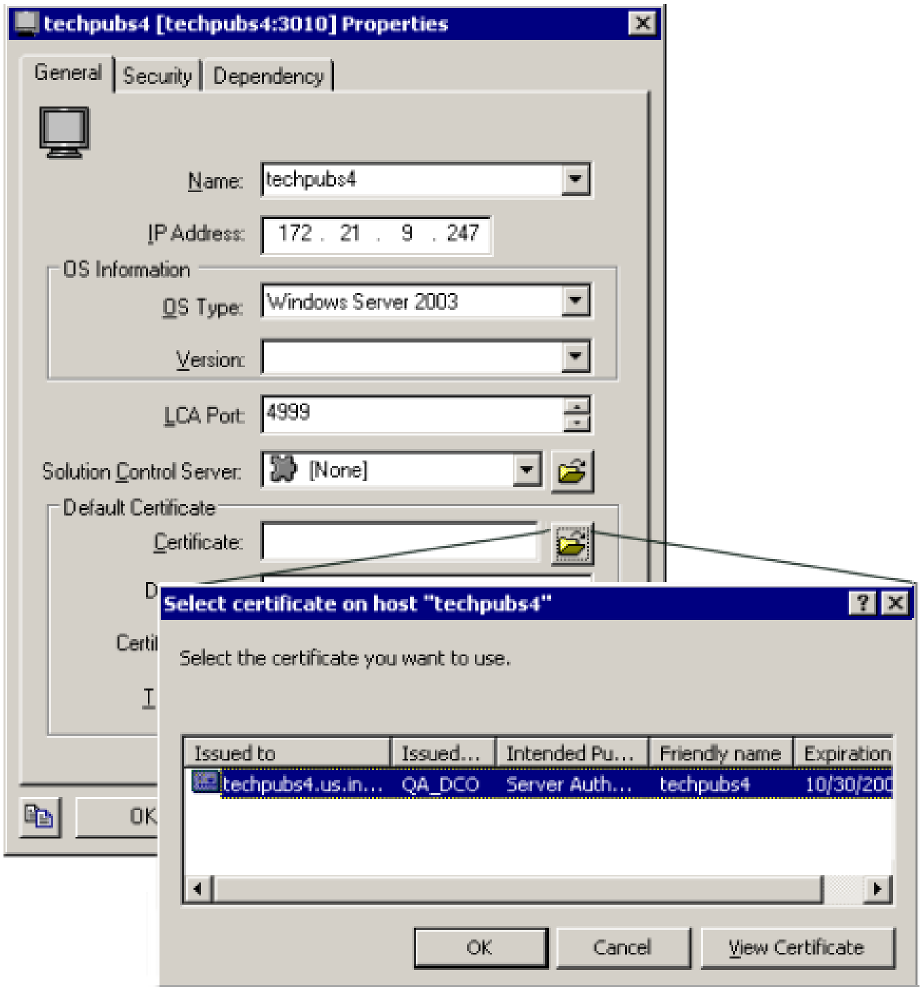
1. In Configuration Manager, select the host that accommodates the server application(s) whose connections you need to secure. To find out the name of the host that accommodates an application, look it up in the properties of that application.
2. Open the `Host Properties` dialog box.
3. On the `General` tab, in the `Default Certificate` section, specify the certificate value that you have generated and installed. The procedure for doing this varies, depending on the platform on which you run your applications:

For Windows:

a. Click the `Certificate browse` button.

b. In the `Select certificate on host <host name>` dialog box, select the certificate from the list, and then click `OK` (see Figure 12).

For information about the installed certificates, see "Installing Certificates" on page 73.



Name: techpubs4

IP Address: 172 . 21 . 9 . 247

OS Type: Windows Server 2003

Version:

LCA Port: 4999

Solution Control Server: [None]

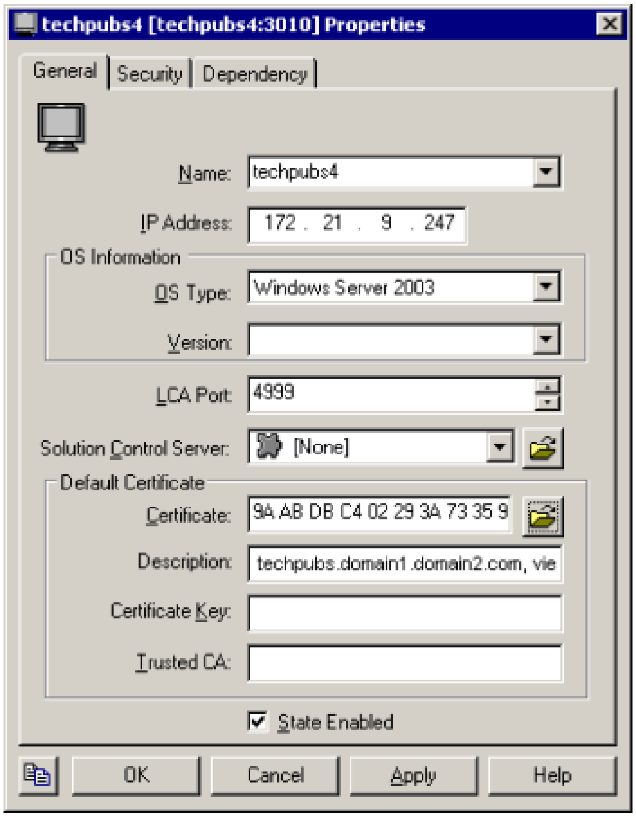
Certificate:

Select the certificate you want to use.

Issued to	Issued...	Intended Pu...	Friendly name	Expiration
techpubs4.us.in...	QA_DCO	Server Auth...	techpubs4	10/30/200

Figure 12: Host Configuration: Certificate Selection for Windows

The certificate information now appears in the appropriate fields of the `Host Properties` dialog box (see Figure 13 on page 92).



techpubs4 [techpubs4:3010] Properties

Name: techpubs4

IP Address: 172 . 21 . 9 . 247

OS Information

OS Type: Windows Server 2003

Version:

LCA Port: 4999

Solution Control Server: [None]

Default Certificate

Certificate: 9A AB DB C4 02 29 3A 73 35 9

Description: techpubs.domain1.domain2.com, vie

Certificate Key:

Trusted CA:

☑ State Enabled

Figure 13: Host Configuration: Default Certificate Section for Windows

For UNIX:

a. In the `Certificate` text box, specify the full path to the `<serial_#>_<host_name>_cert.pem` file.

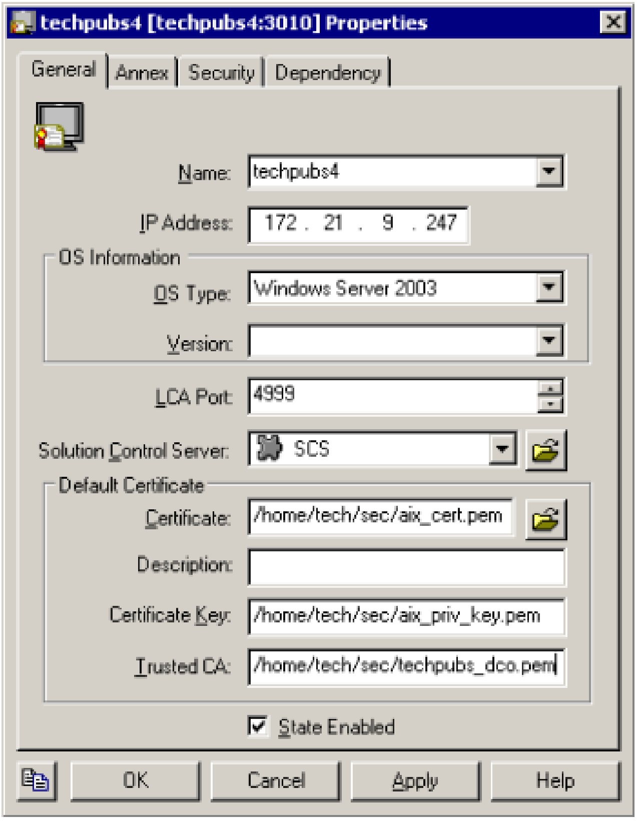
b. In the `Certificate Key` text box, specify the full path to the `<serial_#>_<host_name>_priv_key.pem` file.

c. In the `Trusted CA` text box, specify the full path to the `ca_cert.pem` file.

For information about the installed files, see “Installing Certificates” on page 73.

Note: The `Description` property is optional.

The certificate information now appears in the appropriate fields of the `Host Properties` dialog box (see Figure 14 on page 93).



Name: techpubs4

IP Address: 172 . 21 . 9 . 247

OS Information

OS Type: Windows Server 2003

Version:

LCA Port: 4999

Solution Control Server: SCS

Default Certificate

Certificate: /home/tech/sec/aix_cert.pem

Description:

Certificate Key: /home/tech/sec/aix_priv_key.pem

Trusted CA: /home/tech/sec/techpubs_dco.pem

☑ State Enabled

Figure 14: Host Configuration: Default Certificate Section for UNIX

End of procedure

Host's Annex Tab

When you configure the `Host` object, the certificate information that you specify in the `Default Certificate` section of the `Host Properties` dialog box is also displayed in the `security` section on the `Annex` tab. The configuration options in the `security` section have the same meaning as those in the `Default Certificate` section—namely, the parameters of the certificate assigned to this host.

Procedure:
Removing a previously assigned certificate from a host

Start of procedure

1. Open the `Host Properties` dialog box.

2. On the `General` tab, in the `Default Certificate` section, delete all certificate parameters, and then click `OK`.

End of procedure

Assigning a Certificate to an Application

Note: Genesys recommends that, unless you have compelling reasons to have any of your applications and/or ports protected by their own individual certificate, you keep the certificate assignment at the host level and then use the host certificates to provide secure data exchange for all applications residing on your hosts.

If you intend to use an application's certificate to secure data exchange via any ports of a specific server application, you must first assign a certificate to this application, and then complete the server application configuration.

Procedure:
Assigning a certificate to an application

Start of procedure

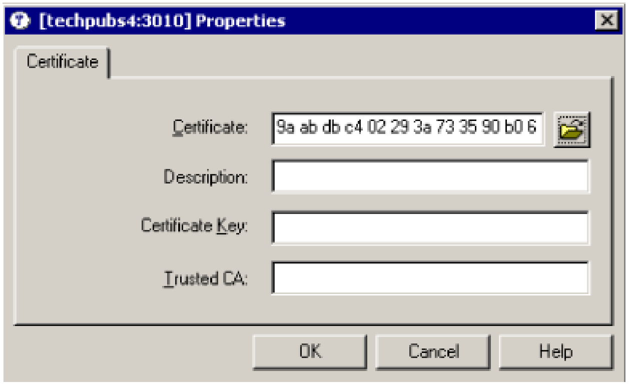
1. Open the `Application Properties` dialog box.
2. Click the `Server Info` tab.
3. In the `Certificate View` section, select the `Application` option, and then click the `Certificate properties` button.
4. In the `Certificate Properties` dialog box, specify the security parameters. The procedure for doing this varies, depending on the platform:

   For Windows:

   a. Click the `Certificate browse` button.

   b. In the `Select certificate on host <host name>` dialog box, select the certificate from the list, and then click `OK`. (See Figure 15 on page 95.)

   For information about the installed certificates, see "Installing Certificates" on page 73.



Certificate: 9a ab db c4 02 29 3a 73 35 90 b0 6

Description:

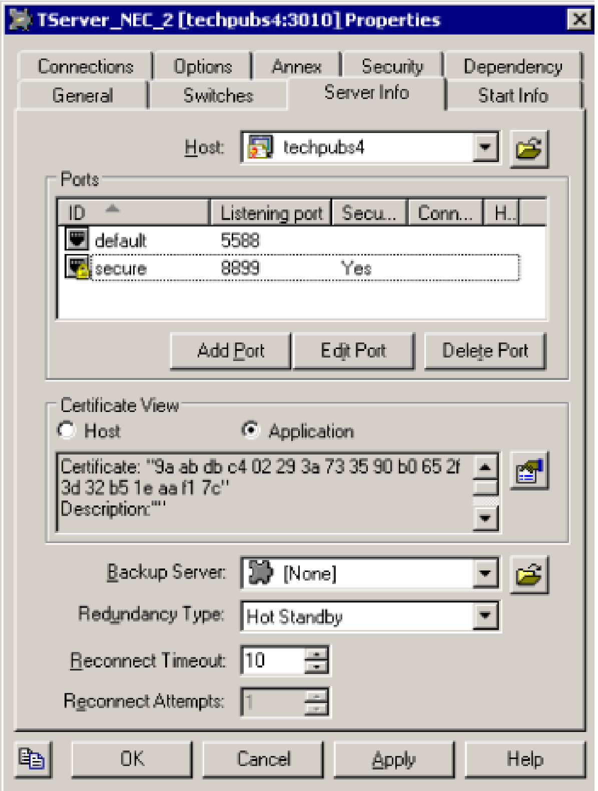
Certificate Key:

Trusted CA:

Figure 15: Application Configuration: Certificate Selection for Windows

c. In the `Certificate Properties` dialog box, click `OK`.

The `Certificate View` section of the `Server Info` tab now displays the value of the assigned certificate (see Figure 16).



Host: techpubs4

ID	Listening port	Secu...	Conn...	H..
default	5588			
secure	8899	Yes		

○ Host ● Application

Certificate: "9a ab db c4 02 29 3a 73 35 90 b0 65 2f 3d 32 b5 1e aa f1 7c"
Description:""

Backup Server: [None]

Redundancy Type: Hot Standby

Reconnect Timeout: 10

Reconnect Attempts: 1

Figure 16: Application Configuration: Assigning the Application's Certificate (Windows)

For UNIX:

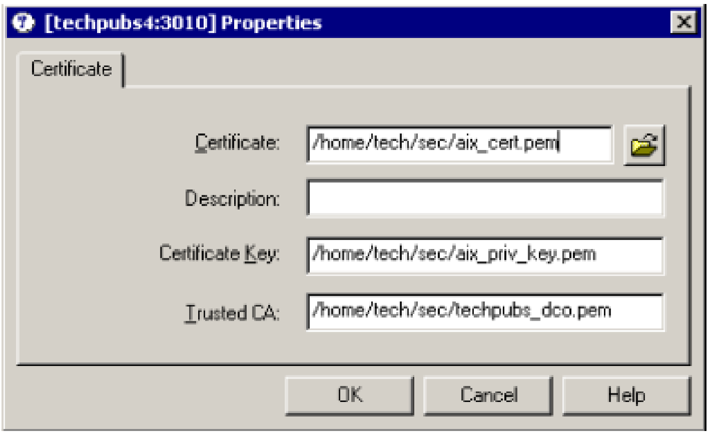
a. In the `Certificate` text box, specify the full path to the `<serial_#>_<host_name>_cert.pem` file.

b. In the Certificate Key text box, specify the full path to the <serial_#>_<host_name>_priv_key.pem file.

c. In the Trusted CA text box, specify the full path to the ca_cert.pem file (see Figure 17).

For information about the installed files, see “Installing Certificates” on page 73.

Note: The Description property is optional.



[techpubs4:3010] Properties

Certificate

Certificate: /home/tech/sec/aix_cert.pem

Description:

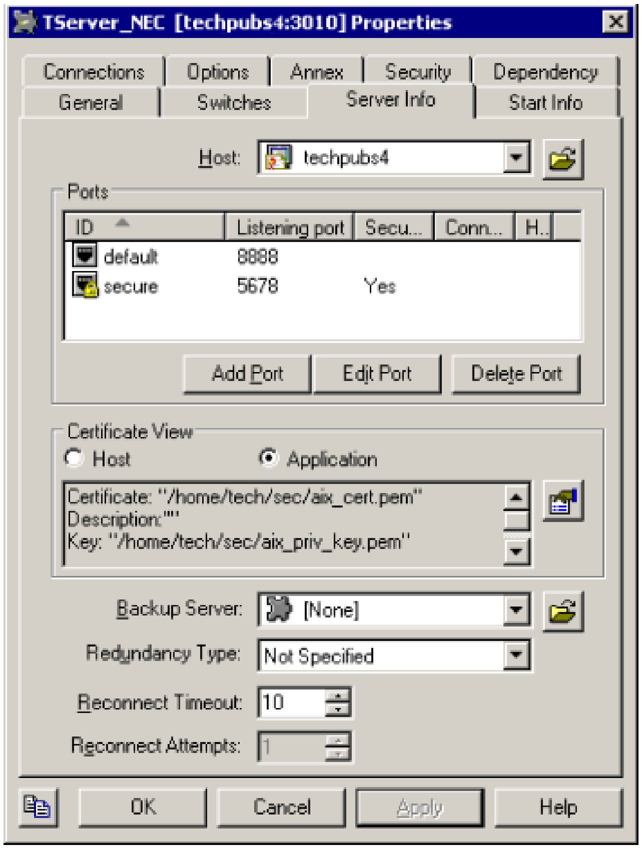
Certificate Key: /home/tech/sec/aix_priv_key.pem

Trusted CA: /home/tech/sec/techpubs_dco.pem

Figure 17: Application Configuration: Certificate Settings for UNIX

d. In the Certificate Properties dialog box, click OK.

The Certificate View section of the Server Info tab now displays the value of the assigned certificate (see Figure 18 on page 97).



TServer_NEC [techpubs4:3010] Properties

Host: techpubs4

ID	Listening port	Secu...	Conn...	H...
default	8888			
secure	5678	Yes		

○ Host ● Application

Certificate: "/home/tech/sec/aix_cert.pem"
Description:""
Key: "/home/tech/sec/aix_priv_key.pem"

Backup Server: [None]

Redundancy Type: Not Specified

Reconnect Timeout: 10

Reconnect Attempts: 1

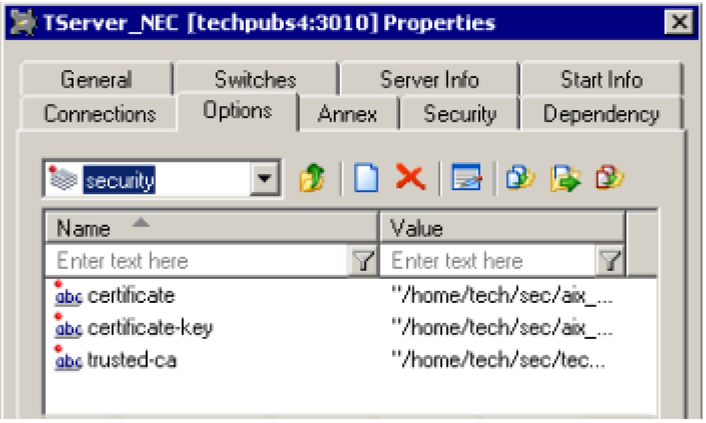
Figure 18: Application Configuration: Assigning the Application's Certificate (UNIX)

5. In the `Application Properties` dialog box, click `OK` to save the new configuration.

End of procedure

Application's Options Tab

When you configure the server application, the certificate information that you specify in the `Certificate` section on the `Server Info` tab of the `Application Properties` dialog box is also displayed in the `security` section on the `Options` tab. The configuration options in the `security` section have the same meaning as those in the `Certificate` section—namely, the parameters of the certificate assigned to this application (see Figure 19 on page 98).



Name	Value
certificate	"/home/tech/sec/aix_...
certificate-key	"/home/tech/sec/aix_...
trusted-ca	"/home/tech/sec/tec...

Figure 19: Application Configuration: Security Options

Procedure: Removing a previously assigned certificate from an application

Start of procedure

1. Open the `Application Properties` dialog box.
2. Click the `Server Info` tab.
3. In the `Certificate View` section, click the `Certificate properties` button.
4. In the `Certificate Properties` dialog box, delete all certificate parameters, and then click `OK`.

End of procedure

Note: When you switch from Application certificate assignment to Host assignment, the Application certificate parameters will be deleted.

Assigning a Certificate to a Port

Note: Genesys recommends that, unless you have compelling reasons to have any of your applications and/or ports protected by their own individual certificate, you keep the certificate assignment at the host level and then use the host certificates to provide secure data exchange for all applications residing on your hosts.

If you intend to use a port's certificate to secure data exchange via a specific port of a server application, complete the following procedure.

Procedure: Assigning a certificate to a port

Start of procedure

1. Open the `Application Properties` dialog box.
2. Click the `Server Info` tab.
3. In the `Ports` section, select the port whose connections you need to secure, and then click `Edit Port`. (See "Configuring Secure Ports" on page 88.)
4. In the `Port Properties` dialog box, click the `Certificate` tab, and then click the `Certificate properties` button.
5. In the `Certificate Properties` dialog box, specify the security parameters. The procedure for doing this varies, depending on the platform:

   For Windows:

   a. Click the `Certificate browse` button.

   b. In the `Select certificate on host <host name>` dialog box, select the certificate from the list, and then click `OK`.

   For information about the installed certificates, see "Installing Certificates" on page 73.

   For UNIX:

   a. In the `Certificate` text box, specify the full path to the `<serial_#>_<host_name>_cert.pem` file.

   b. In the `Certificate Key` text box, specify the full path to the `<serial_#>_<host_name>_priv_key.pem` file.

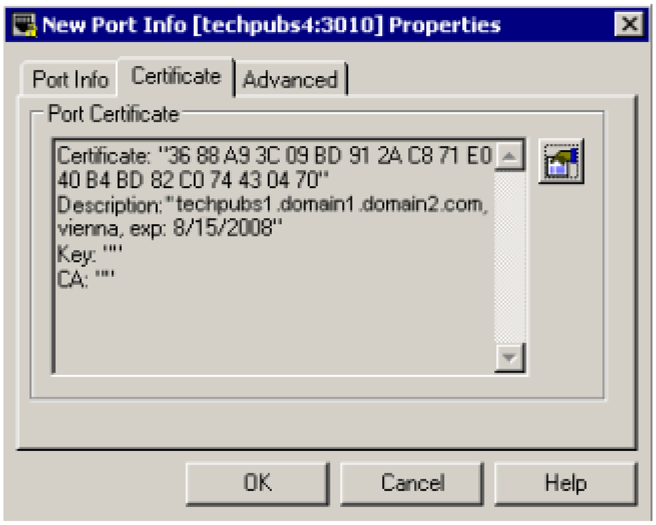
   c. In the `Trusted CA` text box, specify the full path to the `ca_cert.pem` file.

   For information about the installed files, see "Installing Certificates" on page 73.

   Note: The `Description` property is optional.

6. In the `Certificate Properties` dialog box, click `OK`.

   The `Port Certificate` section of the `Certificate` tab now displays the value of the assigned certificate (see Figure 20).



Certificate: "36 88 A9 3C 09 BD 91 2A C8 71 E0 40 B4 BD 82 C0 74 43 04 70"
Description: "techpubs1.domain1.domain2.com, vienna, exp: 8/15/2008"
Key: ""
CA: ""

Figure 20: Port Properties Dialog Box—Certificate Tab

Note: The Advanced tab of the Port Properties dialog box presents certificate parameters in a different form. This tab is reserved for future use.

7. In the Port Properties dialog box, click OK.

8. In the Application Properties dialog box, click OK to save the new configuration.

End of procedure

Procedure: Removing a previously assigned certificate from a port

Start of procedure

1. Open the Application Properties dialog box.
2. Click the Server Info tab.
3. In the Ports section, select the port whose certificate you want to remove, and then click Edit Port.
4. In the Port Properties dialog box, click the Certificate tab, and then click the Certificate properties button.

5. In the Certificate Properties dialog box, delete all certificate parameters, and then click OK.

End of procedure

Configuring a Server Application to Use a Host Certificate

After you assign a certificate to a host, you can use it to secure data exchange via any secure port of any server application that resides on that host.

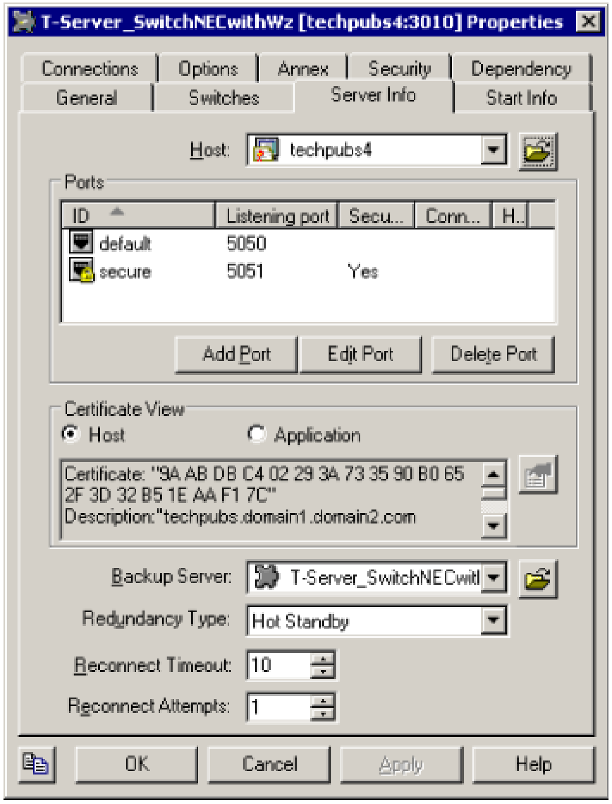
Procedure: Configuring a server application to use a host certificate

Prerequisites

- Assigning a certificate to a host, page 90

Start of procedure

1. Open the Application Properties dialog box.
2. Click the Server Info tab.
3. In the Ports section, configure a secure port. (See “Configuring Secure Ports” on page 88.)
4. In the Certificate View section, make sure that the Host option is selected, to specify that the host certificate will be used by default to secure connections to this server.
5. Click OK to save the new configuration (see Figure 21 on page 102).



Host: techpubs4

Ports

ID	Listening port	Secu...	Conn...	H..
default	5050			
secure	5051	Yes		

Certificate View

● Host ○ Application

Certificate: "9A AB DB C4 02 29 3A 73 35 90 B0 65 2F 3D 32 B5 1E AA F1 7C"
Description:"techpubs.domain1.domain2.com

Backup Server: T-Server_SwitchNECwitl

Redundancy Type: Hot Standby

Reconnect Timeout: 10

Reconnect Attempts: 1

Figure 21: Application Configuration: Selecting a Host Certificate

End of procedure

Configuring Secure Client Connections

After you configure your server applications so that they have secure ports, you must change the configuration of your client applications, so that they connect to these ports. Remember that you must do this only for the connections on which extra measures are necessary to protect the data that is transferred between the Genesys applications.

Note: Before configuring secure connections for client applications, make sure that certificates are installed on the computers on which those applications run. See “Installing Certificates” on page 73.

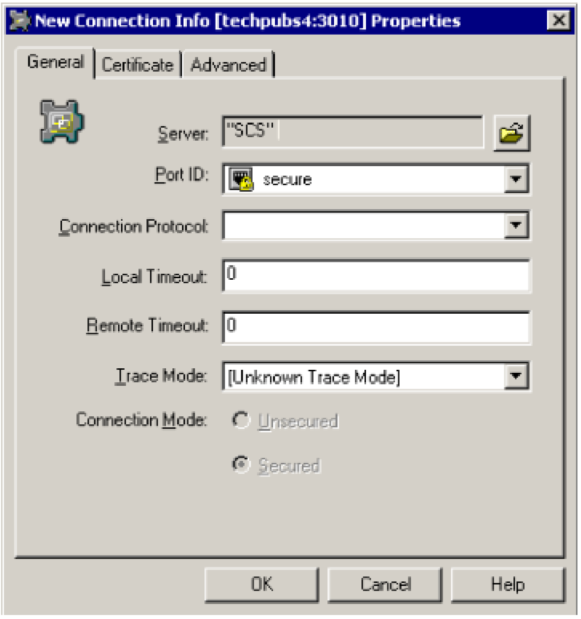
The same configuration procedure is used for client applications of server type and user-interface type.

Procedure: Configuring a secure client connection

Start of procedure

1. Open the Application Properties dialog box of the client application.
2. Click the Connections tab.
3. Select a server the connection to which you need to make secure, and then click Edit.
4. In the Connection Properties dialog box, in the Port ID box, select the secure port that you created for the server during the previous configuration steps. The read-only Connection Mode property indicates that this connection is secure (see Figure 22 on page 103).

Note: The Certificate and Advanced tabs are not used in this configuration.



New Connection Info [techpubs4:3010] Properties

Server: "SCS"

Port ID: secure

Connection Protocol:

Local Timeout: 0

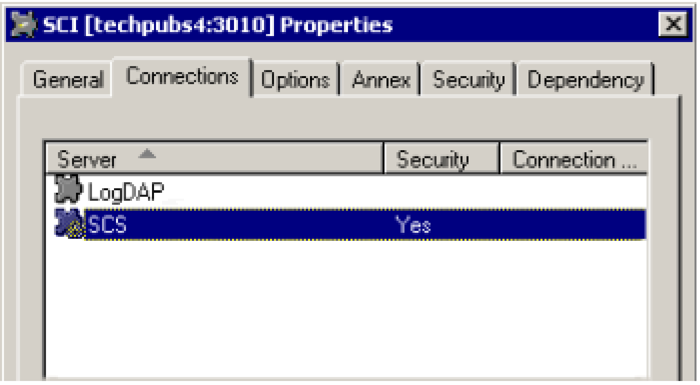
Remote Timeout: 0

Trace Mode: [Unknown Trace Mode]

Connection Mode: ○ Unsecured ● Secured

Figure 22: Application Connections: Selecting a Secure Port of Server Application

5. Click OK. The Connections tab of the Application Properties dialog box now displays this connection with the Security property set to Yes (see Figure 23).



SCI [techpubs4:3010] Properties

Server	Security	Connection ...
LogDAP		
SCS	Yes	

Figure 23: Application Properties Dialog Box—Connections Tab

6. Click OK to save the new connection configuration.

The next time this application starts, it will connect to the server over a secure connection.

End of procedure

Secure Connections to Configuration Server

To configure a secure connection of a client application with Configuration Server, complete the following procedures:

New Client Connections

- For new client applications of server type, specify the Auto-Detect port number of Configuration Server during application installation, by using the Installation Wizard. The Installation Wizard will propagate these parameters as follows:
  - To the Command·Line Arguments text box, on the Start Info tab of the server's Application Properties dialog box.
  - To the server application's startServer.bat file (for Windows) or run.sh file (for UNIX).
  - To the ImagePath in the Application folder in the Registry Editor.
- Modify a client application configuration by adding a Configuration Server Application object to the client's Connections tab, as described in "Configuring Secure Client Connections" on page 102, but select the Auto-Detect port in Step 4 on page 103.
- For client applications of user-interface type, start the applications and enter the Auto-Detect port number of Configuration Server in the Log In dialog box that appears.

Existing Client Connections

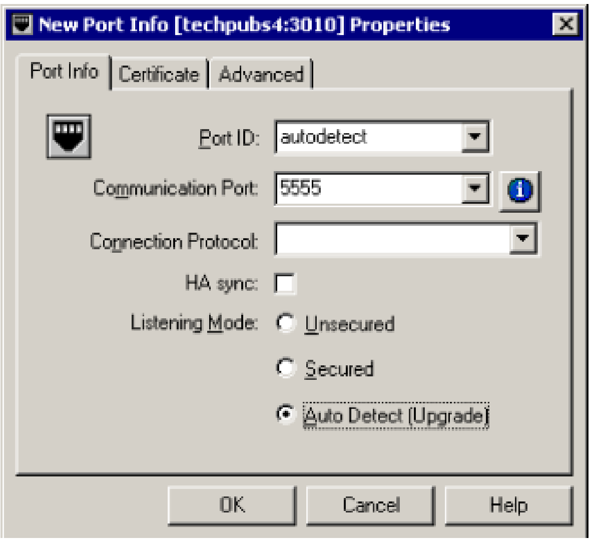
- Verify or create the Auto-Detect port of Configuration Server in the Configuration Server Application object.
- Modify a client application configuration by adding a Configuration Server Application object to the client's Connections tab, as described in "Configuring Secure Client Connections" on page 102, but select the Auto-Detect port in Step 4 on page 103.
- Depending on the method that you use for starting client applications, for existing client applications of server type, change the port information to correspond to the port ID of the Auto-Detect port that you specified for Configuration Server as follows:
  - In the Command·Line Arguments text box, on the Start Info tab of the server's Application Properties dialog box.
  - In the server application's startServer.bat file (for Windows) or run.sh file (for UNIX).
  - In the ImagePath in the Application folder in the Registry Editor.

Procedure: Configuring an Auto-Detect Port for Configuration Server

Purpose: To configure an Auto-Detect port in the Configuration Server application, so that clients can connect securely to Configuration Server.

Start of procedure

1. Open the Application Properties dialog box of Configuration Server.
2. Click the Server Info tab.
3. In the Ports section, click Add Port.
4. In the Port Properties dialog box, on the Port Info tab:
   a. In the Port ID text box, enter the port ID.
   b. In the Communication Port box, enter the number of the new port.
   c. In the Connection Protocol box, select the connection protocol, if necessary.
   d. Select the Auto Detect (Upgrade) option (see Figure 24 on page 106).



Port ID: autodetect

Communication Port: 5555

Connection Protocol:

HA sync: □

Listening Mode: ○ Unsecured ○ Secured ● Auto Detect (Upgrade)

Figure 24: Port Properties of the Configuration Server Application

e. Click `OK`.

If security parameters have been configured for the application, during the connection via `Auto-Detect` port, Configuration Server checks the validity of security settings. Depending on the results, the client is connected in secure mode or Configuration Server rejects the client connection.

5. Click `OK` to save the new configuration.

End of procedure

Configuring a Secure Connection Between Configuration Server and DB Server

You configure all connections between Genesys components secure data exchange in Configuration Manager. The only exception is the connection between Configuration Server and the DB Server of the Configuration Database. To set up a secure connection between these two components, you must modify their configuration files.

Procedure: Modifying DB Server and Configuration Server configuration files

Start of procedure

1. In the configuration file of the DB Server, add a new section, using format `dbserver-n`, where *n* can be any positive number. This section enables you to set up an additional listening port for DB Server. For more information, see the related chapter in the *Framework 7.6 Configuration Options Reference Manual.*
2. In the new section, use the `port` option to specify the number of the port that will be used for secure connection to this DB Server.
3. Use the `transport` option (see page 109) to designate this port as secure, and specify the certificate parameters that will be used to secure the connections. For more information, see "Sample Configuration File for DB Server".
4. In the `[dbserver]` section of the Configuration Server configuration file, change the value of the `port` option so that it corresponds to the secure port that you specified for DB Server.
5. Add the `transport` option to the `[dbserver]` section, to indicate that the connection to the Configuration Database is secure, and specify the certificate parameters that will be used to secure the connections. For more information, see "Sample Configuration File for Configuration Server".
6. Restart Configuration Server and DB Server.

End of procedure

Note: Before configuring secure data exchange, make sure that certificates are installed on the host computers on which specific Genesys components run, and that the certificate information is available to you.

Sample Configuration File for DB Server

The following is a sample configuration file for the DB Server of the Configuration Layer, in which the `[dbserver-1]` section provides settings for secure connections to this server:

```
[dbserver]
host = localhost
port = 4040
management-port = 4581
dbprocesses_per_client = 1
dbprocess_name =./dbclient_sybase
```

```
oracle_name =./dbclient_oracle
informix_name =./dbclient_informix
sybase_name =./dbclient_sybase
db2_name =./dbclient_db2
connect_break_time = 1200
tran_batch_mode = off

[dbserver-1]
port = 4333
transport=tls=1;certificate=9a ab db c4 02 29 3a 73 35 90 b0 65 2f 3d 32
b5 1e aa f1 7c

[log]
verbose = standard
all = stderr

[lca]
lcaport = 4999
```

Sample Configuration File for Configuration Server

The following is a sample configuration file for Configuration Server, in which the values of the port and transport options of the [dbserver] section are set to correspond to the preceding sample configuration file for DB Server in case when both Configuration Server and DB Server run on the same host computer:

```
[confserv]
port = 2020
management-port = 2021
server = dbserver
history-log-file-name = histlog
history-log-expiration = 30
history-log-client-expiration = 1
history-log-max-records = 1000
encryption = false
encoding = utf-8

[log]
verbose = standard
all = stderr

[hca]
schema = none

[soap]
port = 5555

[dbserver]
host = db-host
port = 4333
```

```
dbengine = mssql
dbserver = db-config
dbname = config
username = user1
password = user1pass
reconnect-timeout = 10
response-timeout = 600
transport=tls=1;certificate = 9a ab db c4 02 29 3a 73 35 90 b0 65 2f 3d
32 b5 1e aa f1 7c
```

Secure Connection Configuration Option

You use the `transport` option to specify the certificate-related parameters that are necessary to establish the initial secure connection between DB Server and Configuration Server.

transport

Default Value: `tls=0`
Valid Values:

`tls=0`	Regular (unsecured) connections will be used.
For Windows:	Secure connections will be used.
`tls=1;certificate=<value>`	In the `certificate` option, specify the certificate value. For information about certificates, see "Generating Certificates with OpenSSL" on page 69.
For UNIX:	Secure connections will be used.

`tls=1;certificate=<path>;`
`[certificate-key=<path>];`
`trusted-ca=<path>`
	In the `certificate` option, specify the full path to the `<serial_#>_<host_name>_cert.pem` file. In the certificate-key option, specify the full path to the `<serial_#>_<host_name>_priv_key.pem` file (unless the private key is stored together with a certificate). In the `trusted-ca` option, specify the full path to the `ca_cert.pem` file.

You specify the `transport` option in any section of the DB Server configuration file that contains port configuration, and in the Configuration Database section of the Configuration Server configuration file.

Note: Valid values for the `transport` option must have no spaces before or after the delimiter characters ";" and "=".

Configuring Secure HA Synchronization Connection

This section describes how to configure secure connections between the primary and backup components in a high-availability (HA) configuration.

Note: See "Supporting Components" on page 62 for information about components that support secure connections in high-availability configurations. For information about setting up a high-availability environment for these Genesys components, see the corresponding product documentation.

Configuring Redundant Servers

Starting with release 7.5, where the possibility to configure multiple ports has been introduced, the HA synchronization connection is configured by selecting the `HA sync` check box in a `Port Properties` dialog box of a specific port. This indicates that the port will be used by the former primary server to connect to the new primary server after a failover. If the `HA sync` check box is not selected, the former primary server will connect to the default port of the new primary server.

Note: Genesys does not recommend using the ports with the port-level assigned certificates for an HA synchronization connection between redundant servers. The secure connection should be configured on a host or an application level instead.

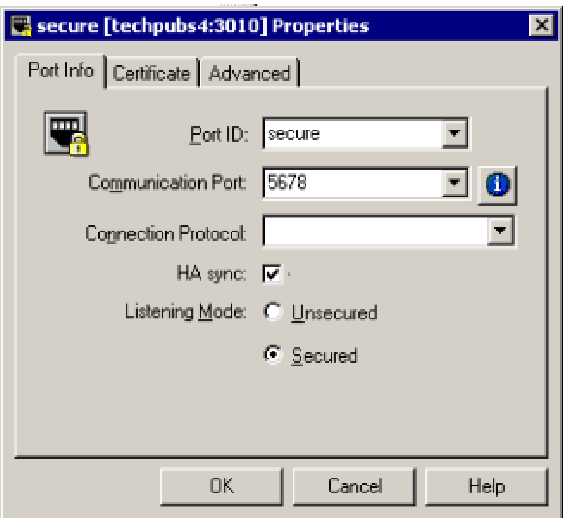
Procedure: Configuring a secure connection between redundant servers

Start of procedure

1. On the `Server Info` tab of the properties of both the primary and backup servers in a redundant pair, create a new port with the same `Port ID`, and with `Listening Mode` set to `Secure`.

   Note: When multiple ports are configured for a server in a `hot standby` redundancy pair, their `Port IDs` and the `Listening Mode` settings of the primary and backup servers must match respectively.

2. In the Port Properties dialog box of each server, click OK to save the new configuration. Then, in the Application Properties dialog box of each, click Apply.
3. In the Application Properties dialog box of each server, select the port that you just created, and then click Edit.
4. In the Port Properties dialog box, select the HA sync check box, and then click OK. The Port section of the Application Properties dialog box now displays this port as a secure port for an HA synchronization connection (see Figure 25).



Port ID: secure

Communication Port: 5678

Connection Protocol:

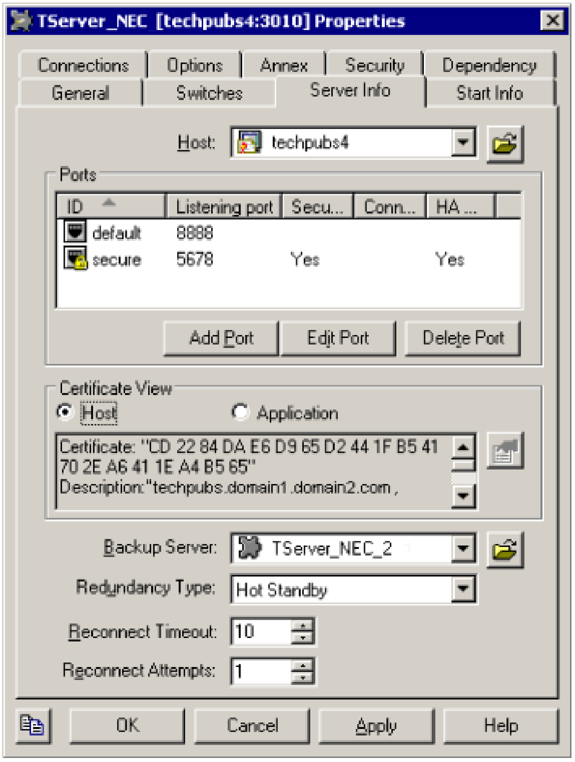
HA sync: ☑

Listening Mode: ○ Unsecured

● Secured

Figure 25: Example of a Secure Port Configuration for a Primary T-Server

5. Click Apply to save the configuration changes (see Figure 26 on page 112).



Host: techpubs4

Ports

ID	Listening port	Secu...	Conn...	HA ...
default	8888			
secure	5678	Yes		Yes

Certificate View

● Host ○ Application

Certificate: "CD 22 84 DA E6 D9 65 D2 44 1F B5 41 70 2E A6 41 1E A4 B5 65"
Description:"techpubs.domain1.domain2.com ,

Backup Server: TServer_NEC_2

Redundancy Type: Hot Standby

Reconnect Timeout: 10

Reconnect Attempts: 1

Figure 26: Example of a Primary T-Server Configuration

End of procedure

Chapter

12 Troubleshooting Genesys TLS

This chapter contains information for troubleshooting the Genesys Transport Layer Security (TLS) installation in your environment. It contains the following section:

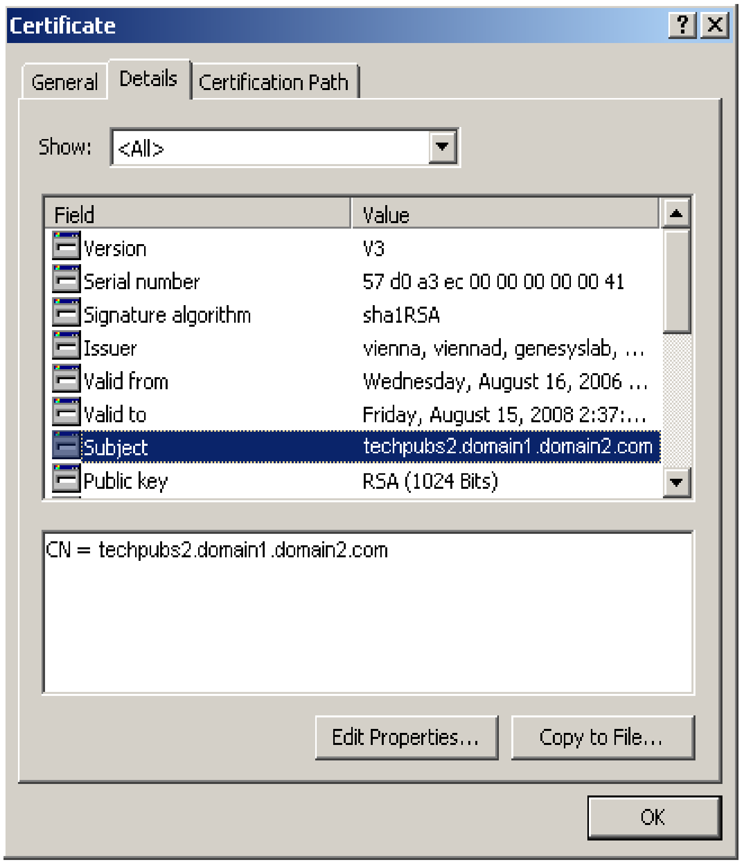
Secure Connection Cannot be Established

When secure connection between a client and server cannot be established, review the suggestions in this section:

- Make sure the Genesys components support the Genesys TLS functionality. See the corresponding product documentation.
- Make sure that Genesys TLS is supported on your operating system. See “Setting the Environment Variable” on page 67.
- Make sure that the CA self-signed certificate file and at least one certificate issued by this CA are installed on the host computers where a client and server applications run.
- For UNIX, make sure that the Genesys Security Pack on UNIX is installed on each UNIX host computer on which Genesys components are installed.
- For UNIX, make sure the environment variables that correspond to your operating systems are properly set (see Table 4 on page 67).
- For UNIX, make sure the environment variables that correspond to your operating systems are also properly set for the LCA environment (see Table 4 on page 67).
- For Windows, check if the certificates are installed under the `Local Computer` account for server applications and under the `Current User` account for client GUI applications.

- Make sure that configured certificates including CA certificates are not expired.
- If DB Server starts from the configuration file and cannot open a secure port, make sure that the `transport` option is configured correctly and there are no spaces before or after the delimiter characters “;” and “=”.
- Genesys recommends that only one instance of CA is used for your entire call center environment.
- Certificates are generated for a particular host with the full host name specified. When the certificate is installed on the host where applications run, make sure that the host name complies with these two requirements:
    - The `Subject` field of the host name contains the fully qualified domain name (FQDN) of this host (see Figure 27).
    - The host name must match the name that is resolved from other computers.

  For example:



Show: <All>

Field	Value
Version	V3
Serial number	57 d0 a3 ec 00 00 00 00 00 41
Signature algorithm	sha1RSA
Issuer	vienna, viennad, genesyslab, ...
Valid from	Wednesday, August 16, 2006 ...
Valid to	Friday, August 15, 2008 2:37:...
Subject	techpubs2.domain1.domain2.com
Public key	RSA (1024 Bits)

CN = techpubs2.domain1.domain2.com

Figure 27: Certificate Properties: Subject Field

Part

4 Server Integrity— Client-Side Port Definition

Part Four of this document describes how to implement the Client-Side Port Definition feature, which is provided by Genesys to ensure the integrity of your servers and their data.

This information appears in the following chapter:

- Chapter 13, "Client-Side Port Definition," on page 117

Chapter

13 Client-Side Port Definition

This chapter describes how to specify client parameters to connect to a specific server application. It contains the following sections:

Feature Summary

The client-side port definition feature enables a client application (of server type) to define its connection parameters before connecting to the server application. This enables the server application to control the number of client connections. In addition, if the client application is located behind a firewall, the server application will be able to accept the client connection by verifying its predefined connection parameters.

Security Benefits

The client-side port definition feature enables a customer to better control the data connections through their firewalls, by enabling them to precisely define the connections that can tunnel through the firewalls. This reduces the susceptibility to denial-of-service (DoS) attacks, where an excessive number of malicious application-level requests comes to the same server-side port. This can result in the server application dropping its performance or even becoming unstable, and it also affects the other applications on the same server or in the network.

Supporting Components

This feature applies to the following components:

- Media T-Servers when connecting to Configuration Server/Configuration Server Proxy

- Network T-Servers when connecting to Configuration Server/Configuration Server Proxy
- Universal Router Server when connecting to Configuration Server/Configuration Server Proxy, T-Server, and Custom Server
- Custom Server when connecting to Configuration Server/Configuration Server Proxy
- Outbound Contact Server when connecting to Configuration Server/Configuration Server Proxy and T-Server
- CPD Server and CPD Proxy Server when connecting to Configuration Server/Configuration Server Proxy and T-Server

Known Issues and Recommendations

Several known issues exist in the current client-side port definition feature implementation:

- Activation of this feature requires you to supply client parameters, which Genesys recommends that you do via the Genesys Installation Wizard.
- In release 7.6, the Media Configuration Wizard does not support the client-side port definition feature configuration. When installing T-Server in an environment where there will be a port-restricted firewall between T-Server and Configuration Server, you must initially configure and install such a T-Server manually.
- If the client-side port definition feature is enabled during T-Server installation, when T-Servers starts, it will report warning messages in its log about command-line parameters related to this feature. Ignore these messages.
- If a client's connection parameters to Configuration Server are defined manually in several different places, make sure that those entries are identical.
- If you add this feature to configured redundant components, the port number (and, optional, IP address) specified in the primary server `Application` object are automatically propagated to the backup server `Application` object. Correct these parameters in the backup server `Application` object manually.

Feature Configuration

Task Flow

Table 7 provides an overview of the main steps required to configure the client-side port definition feature. Complete all steps in order.

Table 7: Task flow—Client-Side Port Definition Feature Configuration

Objective	Related Procedures and Actions
1. Specify the client's connection parameters (the port number and, optional, IP address) either during its installation by using the Genesys Installation Wizard (recommended) or manually.	These parameters will be used for the initial connection to Configuration Server. Complete the following procedures as needed: • "Configuring a connection to Configuration Server on UNIX by using the Installation Wizard" on page 120 • "Configuring a connection to Configuration Server on Windows by using the Installation Wizard" on page 121 • "Manually Configuring a Connection to Configuration Server" on page 123
2. Add a Configuration Server `Application` object to the client's `Connections` configuration, and specify one or both of the client's connection parameters (the port number, or the port number and IP address) in the Configuration Server's connection properties.	These parameters will be used for reconnecting to Configuration Server. Complete the following procedure: • "Adding Configuration Server to client connections in Configuration Manager" on page 124
3. Add the client's connection parameters to the server's connections properties.	To use the feature for client connections to a server application other than Configuration Server, complete the following procedure: • "Configuring client connections" on page 125

Configuring Configuration Server Connections

This section describes how to configure connections to Configuration Server either by using the Genesys Installation Wizard or manually. After the installation is complete, modify a client's `Application` object in Configuration Manager.

Procedure:
Configuring a connection to Configuration Server on UNIX by using the Installation Wizard

Start of procedure

1. In the directory to which the component installation package was copied during Wizard configuration, 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`.
3. Proceed with the installation according to the instructions in the component's product documentation.
4. Prompts appear regarding securing connections between the component and Configuration Server.

   ```
   Client Side Port Configuration

   Select the option below to use a Client Side Port. If you select
   this option, the application can use Client Side Port number for
   initial connection to Configuration Server.

   Do you want to use Client Side Port option (y/n)?
   ```

5. When prompted, type `Y` for yes.
6. At the prompt:

   ```
   Client Side Port port
   ```

   Enter the port number that the client application will use for its TCP/IP connection to the Configuration Server. Note that the installation script will not verify the availability of the component's port number. Make sure that you specify a unique port number that is dedicated to this connection.

7. Press `Enter`.
8. At the prompt:

   ```
   Client Side IP Address (optional), the following values can be used:
   ```

   (Optional) Enter the IP address that the client application will use for its TCP/IP connection to the Configuration Server.

   Note: Genesys recommends that you specify the port number (and, optional, IP address) of a client when you install it by using the Genesys Installation Wizard. If you decide to enable this feature later, you can either re-install the component and define the client's connection parameters during the component installation, or specify parameters manually, as described in "Manually Configuring a Connection to Configuration Server" on page 123.

9. Complete the component installation as specified in the component product documentation.

   During the installation, the client's predefined port number (`- transport-port <port number>`) and IP address (`- transport-address <IP address>`) (if specified) will automatically be added to:

   - The `Command–Line Arguments` text box on the `Start Info` tab of the server's `Application Properties` dialog box, so that the application can be started by using the Management Layer.
   - The server application's `run.sh` file, so that the application can be started by using the startup files.
   - The `ImagePath` in the `Application` folder in the `Registry Editor,` so that the application can be started as a Windows Service.

End of procedure

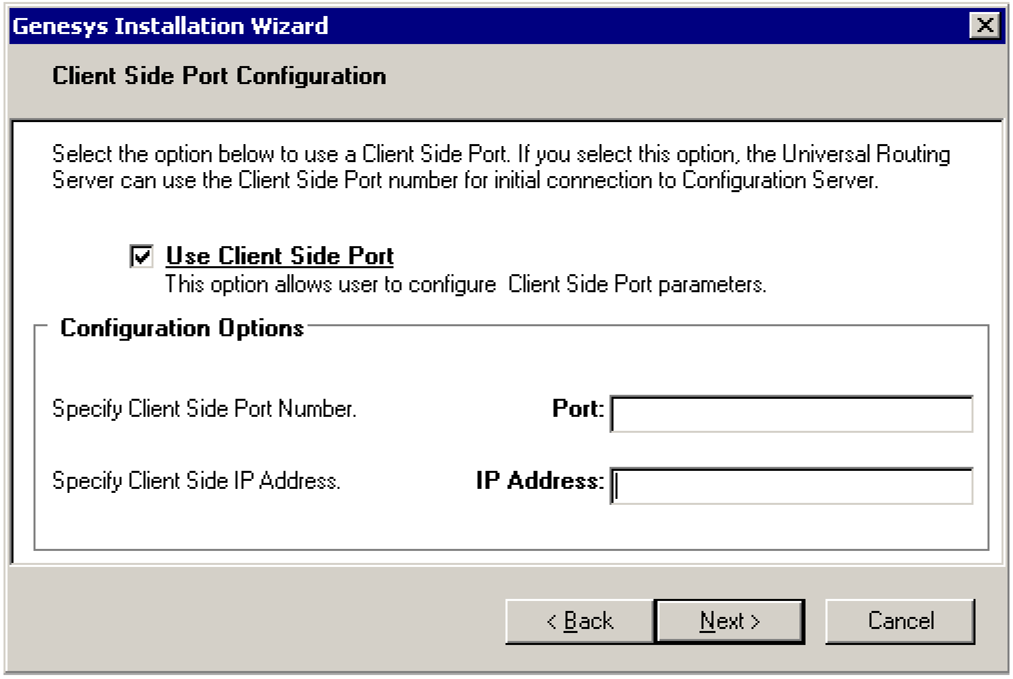
Next Steps

- Adding Configuration Server to client connections in Configuration Manager, page 124

Procedure: Configuring a connection to Configuration Server on Windows by using the Installation Wizard

Start of procedure

1. Launch the component's Genesys Installation Wizard according to the instructions in the component's product documentation.
2. On the `Client Side Port Configuration` page, select the `Use Client Side Port` check box (see Figure 28).



Genesys Installation Wizard

Client Side Port Configuration

Select the option below to use a Client Side Port. If you select this option, the Universal Routing Server can use the Client Side Port number for initial connection to Configuration Server.

☑ **Use Client Side Port**
This option allows user to configure Client Side Port parameters.

Configuration Options

Specify Client Side Port Number. **Port:**

Specify Client Side IP Address. **IP Address:**

Figure 28: Installation Wizard: Specifying Client-Side Connection Parameters

3. Specify the component's (the client's) parameters for connecting to the Configuration Server associated with this client application, as follows:
   - `Port`: Enter the port number that the client application will use for its TCP/IP connection to the Configuration Server. Note that the installation script will not verify the availability of the component's port number. Make sure that you specify a unique port number that is dedicated to this connection.
   - (Optional) `IP Address:` Enter the IP address that the client application will use for its TCP/IP connection to the Configuration Server.

Note: Genesys recommends that you specify the port number (and, optional, IP address) of a client when you install it by using the Genesys Installation Wizard. If you decide to enable this feature later, you can either re-install the component and define the client's connection parameters during the component installation, or specify parameters manually, as described in "Manually Configuring a Connection to Configuration Server" on page 123.

4. Complete the component installation as specified in the component product documentation.

   During the installation, the client's predefined port number (`- transport-port <port number>`) and IP address (`- transport-address <IP address>`) (if specified) will automatically be added to:

- The Command–Line Arguments text box on the Start Info tab of the server's Application Properties dialog box, so that the application can be started by using the Management Layer.
- The server application's startServer.bat file, so that the application can be started by using the startup files.
- The ImagePath in the Application folder in the Registry Editor, so that the application can be started as a Windows Service.

End of procedure

Next Steps

- Adding Configuration Server to client connections in Configuration Manager, page 124

Procedure: Manually Configuring a Connection to Configuration Server

Summary

You configure a client's connection parameters by adding them as command-line parameters that are be used during component startup. You can start Genesys components by using the Management Layer, a startup file, a manual procedure, or the Windows Services Manager. For a server application, all these methods usually require command-line parameters in addition to an executable file name.

Start of procedure

1. Add one or both of the following parameters to the application's command line depending on the method (see below) that will be used for starting the client application:
   - `-transport-port <port number>`
   - `-transport-address <IP address>` (if specified)

   Where:
   - `<port number>` is the port number that a client will use for its TCP/IP connection to Configuration Server.
   - `<IP address>` is the IP address that a client will use for its TCP/IP connection to Configuration Server.
2. To start the application manually, add the client's connection parameters to the application's command line—for example:

```
<switch>_server.exe -host <Configuration Server host>
-port <Configuration Server port> -app <T-Server Application>
```

```
-l <license address> -nco [X]/[Y] -transport-port <port number>
-transport-address <IP address>
```

For more information about the starting and starting Genesys components, see the product documentation for the component

End of procedure

Next Steps

- Adding Configuration Server to client connections in Configuration Manager, page 124

Procedure: Adding Configuration Server to client connections in Configuration Manager

Purpose: To specify a client's connection parameters for reconnecting to Configuration Server.

Start of procedure

1. Open the `Application Properties` dialog box of the client application.
2. Click the `Connections` tab.
3. Click `Add`.
4. In the `New Connection Info Properties` dialog box, click the `Browse` button, select the Configuration Server `Application` object to which the client will connect, and then click `OK`.
5. Click the `Advanced` tab.
6. In the `Transport Protocol Parameters` text box, enter one or both of the following parameters:
   - `port=<port number>`
   - `address=<IP address>`

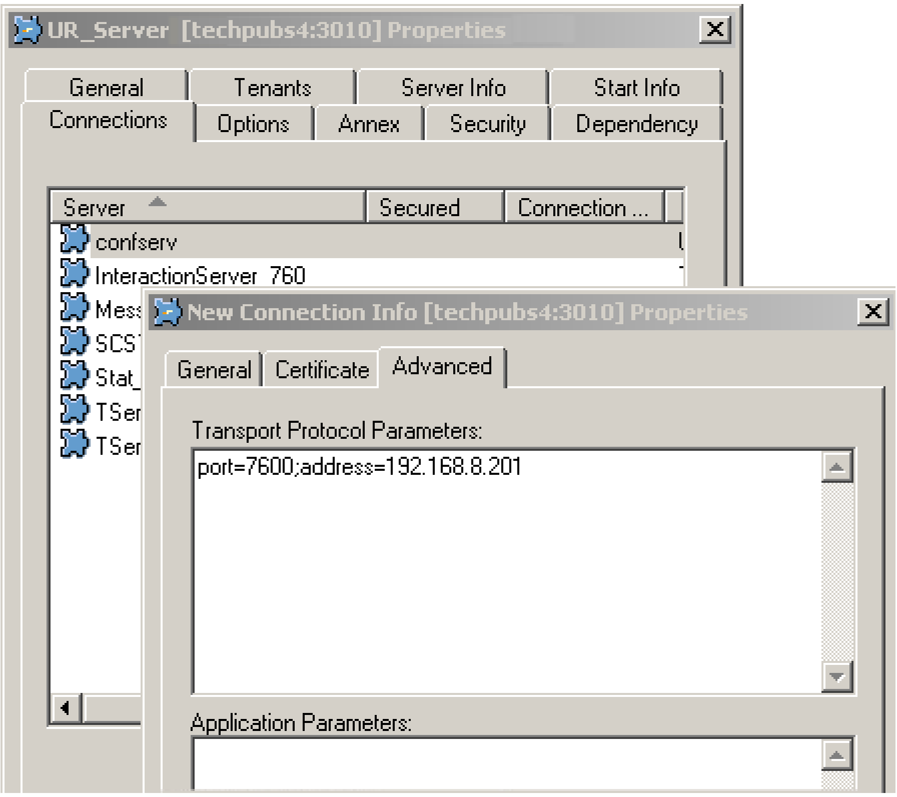
   Where:

   - `<port number>` is the port number that a client will use for its TCP/IP connection to the server.
   - `<IP address>` is the IP address (or host name) that a client will use for its TCP/IP connection to the server.

   If you specify both parameters, use a semicolon as the delimiter, as follows (see Figure 29 for an example):

   ```
   port=<port number>;address=<IP address>
   ```

Note: The parameters that you specify here must be the same as the parameters that you specified during the client installation.



port=7600;address=192.168.8.201

Figure 29: Application Connections: Adding a Configuration Server Application

6. Click `OK` to save the new connection configuration.

End of procedure

Configuring Client Connections

To enable the client-side port definition feature when connecting to other applications, complete the following procedure.

Procedure: Configuring client connections

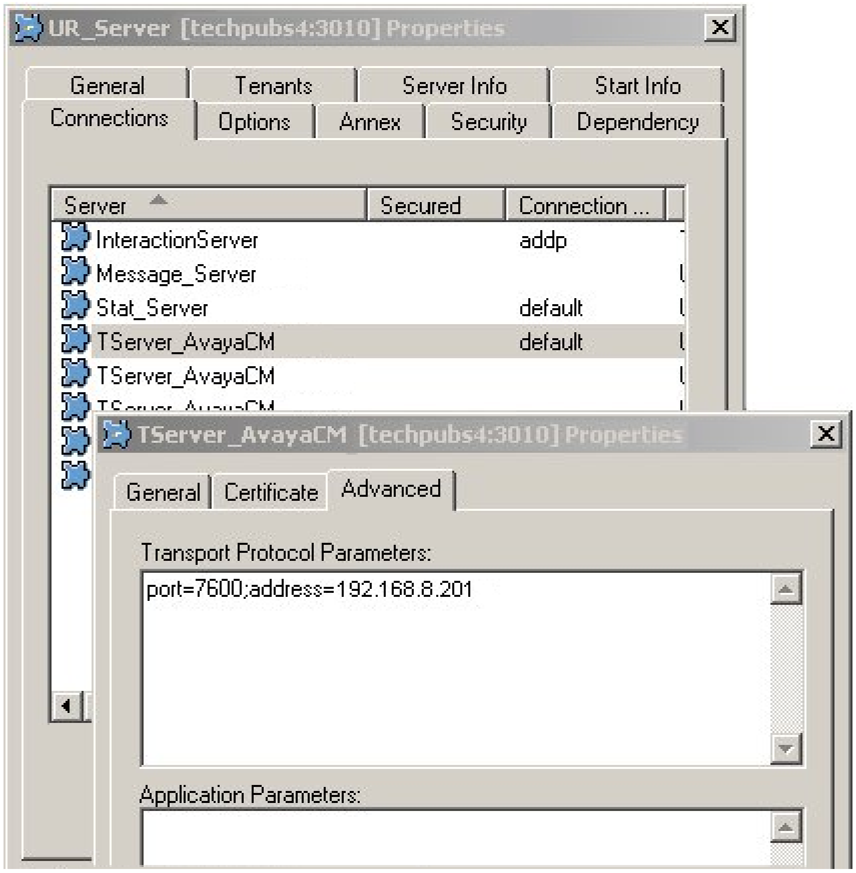
Purpose: To specify a client's parameters for connecting to a server application other than Configuration Server.

Prerequisites

- Configuring a connection to Configuration Server on UNIX by using the Installation Wizard, page 120
- Configuring a connection to Configuration Server on Windows by using the Installation Wizard, page 121
- Adding Configuration Server to client connections in Configuration Manager, page 124

Start of procedure

1. Open the `Application Properties` dialog box of the client application (of server type).
2. Click the `Connections` tab.
3. Select a server to which the client will connect, and then click `Edit`.
4. In the `Connection Properties` dialog box, click the `Advanced` tab (see Figure 30).



Server	Secured	Connection ...
InteractionServer		addp
Message_Server		
Stat_Server		default
TServer_AvayaCM		default
TServer_AvayaCM		

Transport Protocol Parameters:

port=7600;address=192.168.8.201

Application Parameters:

Figure 30: Application Connections: Selecting a Server Application

7. In the `Transport Protocol Parameters` text box, enter one or both of the following parameters:

- port=<port number>
- address=<IP address>

Where:

- <port number> is the port number that a client will use for its TCP/IP connection to the server.
- <IP address> is the IP address (or host name) that a client will use for its TCP/IP connection to the server.

If you specify both parameters, use a semicolon as the delimiter, as follows (see Figure 30 for an example):

```
port=<port number>;address=<IP address>
```

Note: When you add this feature to configured redundant components, the port number (and, optional, IP address) specified in the primary server Application configuration object are automatically propagated to the backup server Application configuration object. Correct these parameters in the backup server Application object manually.

8. Click OK to save the new connection configuration.

End of procedure

Index