Genesys

Framework 8.1

Genesys Administrator

Deployment Guide

About Genesys

Genesys is the world's leading provider of customer service and contact center software–with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multi-channel customer service - and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. Go to 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. © 2013 Genesys Telecommunications Laboratories, Inc. All rights reserved.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 Customer Care. Before contacting Customer Care, please refer to the *Genesys Care Program 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 Licensing Guide.*

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 81fr_ga-dep_12-2013_v8.1.303.00

Table of Contents

List of Procedures

Framework 8.1

Preface

Welcome to the *Framework 8.1 Genesys Administrator Deployment Guide.*
This document describes the deployment, starting and stopping, and
troubleshooting procedures relevant to Genesys Administrator.

This document is valid only for the 8.1 releases of this product.

This preface contains the following sections:

- About Genesys Administrator, page 9
- Intended Audience, page 9
- Making Comments on This Document, page 10
- Contacting Genesys Technical Support, page 10
- Changes in This Document, page 10

For information about related resources and about the conventions that are
used in this document, see the supplementary material starting on page 85.

About Genesys Administrator

Genesys Administrator, part of the Genesys Framework, provides a web-based
graphical user interface for managing Genesys components.

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

- How to deploy Genesys Administrator.
- How to access Genesys Administrator.
- Suggestions for troubleshooting your Genesys Administrator installation.

Intended Audience

This document is intended primarily for system integrators, system
administrators, contact center managers, and operations personnel. It has been
written with the assumption 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 Genesys Framework architecture and functions, as described in the *Framework 8.1 Deployment Guide*.

Making Comments on This Document

If you especially like or dislike anything about this document, 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 scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or 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.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, please contact Genesys Technical Support.

Before contacting technical support, please refer to the *Genesys Care Program Guide* for complete contact information and procedures.

Changes in This Document

Changes in version 8.1.001.00

This document has been updated for this release of Genesys Administrator as follows:

•   Added instructions for using Genesys Administrator on a machine that has ASP.Net running under a non-standard account (that is, not the NETWORK SERVICE account) (see the notes on pages 24 and 67).

•   Added recommendations for resolving an unsuccessful login; see "Unsuccessful Login" on page 64.

•   Added list of Genesys Administrator role privileges; see "Genesys Administrator Role Privileges" on page 71.

Changes in version 8.1.101.00

This document has been updated for this release of Genesys Administrator as follows:

- Added information about, and instructions for installing, a Security Banner; see "Login Security Banner" on page 25.
- Added information about using hardware load balancing in Genesys Administrator; see "Hardware Load Balancing" on page 37.
- Added instructions for adjusting regional settings in Genesys Administrator to correspond to those set in Microsoft Windows; see "Adjusting Regional Settings" on page 40 and "Regional Settings Displayed Incorrectly" on page 66.
- Clarified and corrected content of Table 5, "Required Permissions for ASPNET and NETWORK SERVICE," on page 62.
- Added troubleshooting information for a newly-created user unable to log in, or once logged in cannot see or do anything; see "New Users" on page 64.

Changes in version 8.1.201.00

This document has been updated for this release of Genesys Administrator as follows:

- Added Chapter 4, "Configuration Options," on page 49. This chapter was originally contained in the *Framework 8.0 Configuration Options Reference Manual*.
- Added information about third-party applications logging in on behalf of their users (also known as the pass-through of login credentials); see "Third-party Applications (Pass-Through Login)" on page 46.
- Added recommendations for resolving the HTTP 400 error; see "400 Error" on page 65.

Changes in version 8.1.301.00

This document has been updated for this release of Genesys Administrator as follows:

- Added information about configuring Genesys Administrator for multi-language support; see "Multi-Language Environments" on page 21.
- Clarified instructions for adjusting regional settings when using regional date and time settings with a non-localized version of Genesys Administrator; see "Adjusting Regional Settings" on page 40.
- Added recommendations for resolving the situation when uploading a file stalls with no visible notification; see "File Uploading Stalls" on page 66.

Changes in version 8.1.302.00

This document has been updated for this release of Genesys Administrator as follows:

- "New in This Release" on page 13 has been updated with information about new and modified functionality in this release, which is described in the *Genesys Administrator Help* file. No other content in this document has been changed.

Changes in version 8.1.303.00

This document has been updated for this release of Genesys Administrator as follows:

- "New in This Release" on page 13 has been updated with information about new and modified functionality in this release, which is described in the *Genesys Administrator Help* file.

- Content has been updated or removed to reflect the discontinued support by Genesys Administrator of the deployment of Genesys components to local and remote hosts.

- Information about supported browsers has been updated. See "Browser Requirements" on page 24.

- The following troubleshooting scenarios have been added:
  - "National Characters Displayed Incorrectly" on page 66
  - "Request times out Error" on page 67
  - "Errors Downloading Data from Voice Platform Reports to CSV Format" on page 68
  - "Display Anomalies with Internet Explorer 10" on page 68

- A new role privilege has been added to the Provisioning Module. See "Search" on page 77.

![Genesys logo]

1 Genesys Administrator Overview

This chapter provides a brief description of Genesys Administrator and its architecture, and highlights new features in this release.

This chapter contains the following sections:

Genesys Administrator

Genesys Administrator is a new web-based Graphical User Interface (GUI) that combines the functionality of Configuration Manager, Solution Control Interface, and other Genesys GUIs.

Genesys Administrator provides a comprehensive user interface to:

- Configure, monitor, and control your Genesys environment.
- Manage user access to your Genesys environment, particularly as it pertains to access permissions and Role-Based Access Control.

New in This Release

Before you familiarize yourself with the Genesys Administrator architecture and functionality, note the following major changes that were implemented in the 8.1 release of Genesys Administrator. Unless stated otherwise, refer to the *Framework 8.1 Genesys Administrator Help* file for details about the new functionality.

General Features

*   **Support of new operating system and web browsers:** Genesys Administrator now supports the following:
    *   Windows Server 2008 R2 64-bit native operating system
    *   Internet Explorer 8, 9, and 10 web browsers

        Note: See "Display Anomalies with Internet Explorer 10" on for information about using Internet Explorer 10.

    *   TCP/IP v6

    In addition, Genesys Administrator now supports the latest version of Mozilla Firefox web browser (as of the release date).

    Refer to the *Genesys Supported Operating Environment Reference Guide*, a link to which is provided on .

*   **Support for multiple Solution Control Servers and Log Databases:** The user can, at any time, change the Log Database Access Point (DAP) or the Solution Control Server to which Genesys Administrator is connected without having to log out and log back in. The choices of Log DAPs and Solution Control Servers to which Genesys Administrator can connect, however, is limited to those in the list of connections for the Genesys Administrator `Application` object in Configuration Server.

*   **Support for Read-only / Emergency Mode:** Genesys Administrator now supports Read-only Mode and Emergency Mode.

*   **Support for IPv6:** Genesys Administrator now supports access from client browsers and connectivity to other Genesys servers using IPv6 when IPv6 addresses are set up properly in the Domain Name System.

Provisioning Features

Refer to *Framework 8.1 Genesys Administrator Help* for more information about these features.

*   **Enhanced bulk provisioning:**
    *   Users can now export and import `User`, `DN`, `DN Group`, `Agent Group`, `Place`, `Place Group`, and `Tenant` objects to and from a `.csv` text file, in which the list separator is user-defined. This facilitates off-line updates to these objects. The exported data can also be sorted, enabling columns with master/details data to be consolidated when viewed in a spreadsheet.
    *   Users can now create a range of `User` and `Place` objects interactively.
    *   Users can now add an Agent to one or more Agent Groups while configuring the Agent.

    Throttling can be enabled for bulk operations to ensure that Configuration Server is not overwhelmed by the volume of process requests.

- **Optimized configuration of connections:** Users can now add connections with default parameters in a single step.
- **Support for SIP Business Continuity:** Users can now use the new Sync Switch Wizard in Genesys Administrator to synchronize peer SIP-type `Switches` and Switch-related objects (`Places` and `Users`). For more information about SIP Business Continuity, refer to the *Framework 8.1 SIP Server High Availability Deployment Guide*.

Solutions Support

In addition to *Framework 8.1 Genesys Administrator Help*, refer also to solution-specific documentation for more information about the new features and functionality for the following solutions:

- **Voice Platform**
  - Users can now validate the uniqueness of DIDs across all Tenants.
  - Users can use the new Recording Server Resource Group to group and manage Recording Group resources.
  - Users can now view CTI Connector (CTIC) component and Intelligent Contact Management (ICM) connection statistics using the new CTIC Dashboard.
  - The new ASR/TTS Usage and ASR/TTS Usage Peaks Reports generated by the Automatic Speech Recognition (ASR) Server and Text-to-Speech (TTS) Server components provide metrics on a per-component, -IVR Profile, -Tenant, and -deployment basis.
  - Historical Media Control Platform (MCP) Call Detail Record (CDR) reports now include additional columns to indicate whether or not a resource has been used.
  - Users can now view information about the per-call Interaction Voice Response (IVR) Actions and a list of custom variables for the session using the Historical Call Browser for MCP.
  - Users can now choose to combine information from all sites in the system in the following reports:
    - Call Arrivals Reports
    - Voice Application Reporting (VAR) IVR Action Usage and Summary
    - ASR/TTS Usage Report
  - Resource Manager (RM) CDRs displayed in the Active and Historical Call Browser now include the Site ID.
  - Users can now use the IVR Profile Wizard to enter authentication parameters used by GVP context services.
  - If primary and backup Policy Servers are configured, when Genesys Administrator tries to access the Policy Server to obtain information, it will first try the Policy Server instance that is was last successful in gaining access.

- **Routing**
  - Users can now use Genesys Administrator to load and unload Routing Strategies (Simple Routing Scripts) on DNs and DN Groups, and to schedule that loading and unloading.
  - Genesys Administrator now validates Routing Strategies, to confirm that all applicable configuration objects exist.
  - Genesys Administrator now supports the new Operational Reporting feature on the Orchestration Server (release 8.1 or later), which enables users to:
    - View specific statistics and details about active and recently active sessions in an Orchestration deployment.
    - Search for sessions in an Orchestration deployment.
    - Directly in the Genesys Administrator interface, terminate any session that appears in the list of search results.
    - Specify an alternate Universal Resource Identifier (URI) when configuring an Enhanced Routing script for Orchestration.
  - Genesys Administrator now supports UTF-8 encoding for name and value of `Business Attributes` objects. This enables multilingual data to be stored and displayed.

- **eServices**
  - Users can now use Genesys Administrator to provision Multimedia/eServices SCXML applications on Interaction Queues.
  - Genesys Administrator now supports UTF-8 encoding for name and value of `Business Attributes` objects. This enables multilingual data to be stored and displayed.

- **Outbound Contact**
  - Users can now provision `Script` objects of type `Outbound Schedule` under Outbound Contact. These Outbound Schedules enable the user to automate periodic execution of dialing sessions (for example, daily, weekly, monthly, and so on), based on preconfigured settings. Outbound Schedules also allow automatic control over dialing session executions (such as activation, deactivation, starting, stopping, modification of dialing mode, and so on) based on time or in response to meeting user-defined conditions.
  - When configuring an `Outbound Schedule` object, you can explicitly define the Outbound Contact Server that will execute this `Outbound Schedule`.
  - You can now change the name of a script associated with an Outbound schedule from within the properties dialog box of the schedule.
  - When configuring `Outbound Schedule` objects, you can define the dialing priorities for each Schedule item for only `Load`, `Start`, and `Set Dialing Mode` actions.
  - You can now create Calling Lists based on a PostgreSQL 9.0 database.

- The list of Dialing Sessions that appears under the `Operations` tab now displays the Stat Server, Max Queue Size, IVR Profile, Interaction Queue, and Trunk Group DN associated with each session.
- Genesys Administrator provides an interface to define bodies of customizable reporting-related stored procedures for Calling Lists and Campaigns. These customizable procedures enable users to define up to five custom counters for Calling List related real-time reporting metrics, and to re-define existing counters (such as number of total records and number of ready records).
- Genesys Administrator now supports setting a new dialing mode, Predictive GVP, with a new Average Distribution Time optimization parameter.
- Genesys Administrator now supports setting a new optimization parameter, Maximum Gain, for predictive dialing modes.
- Users can now import and display Calling Lists that are encoded in UTF-8.
- Users can choose which statistics to display, and define properties of these statistics, for all reports in the Outbound Contact section on the Monitoring tab of Genesys Administrator.

Security Features

Refer to the *Genesys 8.1 Security Deployment Guide* for information about the following Security enhancements:

- **Enhanced security at login:**
  - Genesys Administrator now supports the standard Genesys Security Banner feature at login.
  - Genesys Administrator can now be configured to prevent specific technical information from being displayed in authentication and connection error messages.
  - Genesys Administrator can now be configured to prompt the User to change his or her password, usually when the user is logging into the system for the first time, or when their password is about to expire. This feature must be activated in Configuration Server 8.1.1 or later to be available for use in Genesys Administrator.
- **Enhanced Role-Based Access Control:**
  - Role privileges for Genesys Administrator can be accessed only from the Environment Tenant. In a multi-tenant environment, role privileges for Applications other than Genesys Administrator can be accessed from any Tenant.
  - A User can now be granted permissions to create a new Tenant, without being able to access all existing Tenants.
  - The Search role privilege is added to enable users to access only the Search functionality on the Provisioning module.

- **Enhanced permissions management:** When using permissions, the user can now:
  - Manage permissions for all authorized users of an object at once.
  - Replace Permissions recursively.
- **Enhanced Web security:** Genesys Administrator can be configured to use a secure flag so that the cookie's information is transmitted only over an HTTPS-encrypted channel.

Usability Features

- **Localized display of date and time:** Dates and times are now displayed using the same calendar and time zone as the language pack installed on the Genesys Administrator server.
- **Automatic refresh of Applications and Solutions in list views:** The status of Applications and Solutions is refreshed automatically in list views, at the rate that is the greater of either every 15 seconds or the refresh rate you specify in User Preferences.
- **Customizable Tenant creation:** When creating new Tenants, users can set additional options to customize the information that is required at creation.
- **Enhanced display of Permissions:** In a multi-tenant environment, users can now view Permissions in a a flat list (Simple Mode) or in a logical tree structure by Tenant. In this mode, a user with the necessary permissions and role privileges can setup every possible combination of permissions. Users can switch between the two modes as required.
- **Enhanced display of Tenants:** In a multi-tenant environment, users can now view the list of Tenants as a flat list (Simple Mode) or as a logical tree in which you open the parent Tenant to view the child Tenants (Advanced Mode). Users can switch between the two modes as required.
- **Display of composite objects:** For each Host, the name, status, and mode of each Application configured on that Host is displayed. Similarly, for each Solution, the name, status, and mode of each Application that is as part of that Solution is displayed.
- **Display of Host statistics:** Users can now view operating statistics about a Host.
- **User accountability in Solution Control Server logs:** Individual, unshared connections between Genesys Administrator and Solution Control Server can now be established for the user at login, enabling the identification of a user session in the SCS log.
- **Pass-through of login credentials:** Third-party applications can now log in to Genesys Administrator on behalf of the user, without the user having to interact with the Genesys Administrator login dialog box. Refer to "Third-party Applications (Pass-Through Login)" on for more information.

- **Enhanced support for Alarm Reaction Script Definitions:** Genesys Administrator can now work with Scripts that identify the application, host, or object by DBID or by its name as supported by Management Layer 8.1.1 and later. This ensures full compatibility with new and legacy script definitions.

- **Additional viewing and filtering capability for audit logs:** Users can view additional fields added to audit logs, and can use these new fields as filter criteria.

- **Multiple Supervisors for Agents:** An Agent Group can now be configured with multiple supervisors.

- **Enhanced Agent filtering:** A list of Agents can now also be filtered by Skill and Skill Level.

- **Display of UTF-8-encoded data:** Genesys Administrator can now display UTF-8-encoded data from a MS SQL Log database.

Discontinued Features

- Effective in Genesys Administrator 8.1.3, the functionality for deploying Genesys components to remote and local hosts is moved to Genesys Administrator Extension 8.1.4. Refer to Genesys Administrator Extension documentation for additional information.

Architecture

Genesys Administrator resides in the User Interaction Layer of the Genesys Framework. This Layer provides a comprehensive user interface to configure, monitor, and control the management environment.

Figure 1 on page 20 illustrates how the User Interaction Layer is positioned within the Framework architecture.
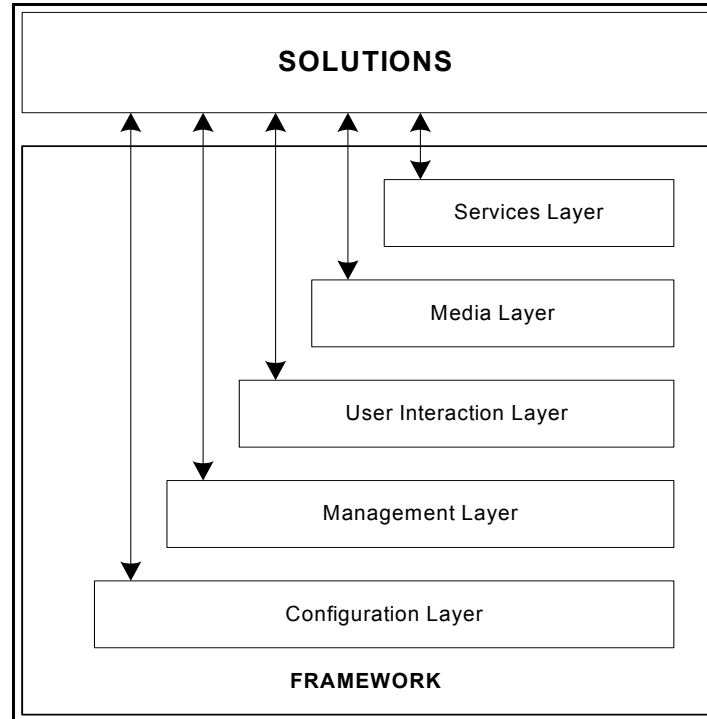
Figure 1: Framework Architecture

Refer to the *Framework 8.1 Deployment Guide* or *Framework 8.0 Architecture Help* for more information about Framework architecture as a whole.

Functions

- The User Interaction Layer provides centralized web-based functionality and interfaces for the configuration, monitoring, and control of applications and solutions.

Architecture

Figure 2 on page 21 shows the structure of the User Interaction Layer, and with what elements of your system it interacts.
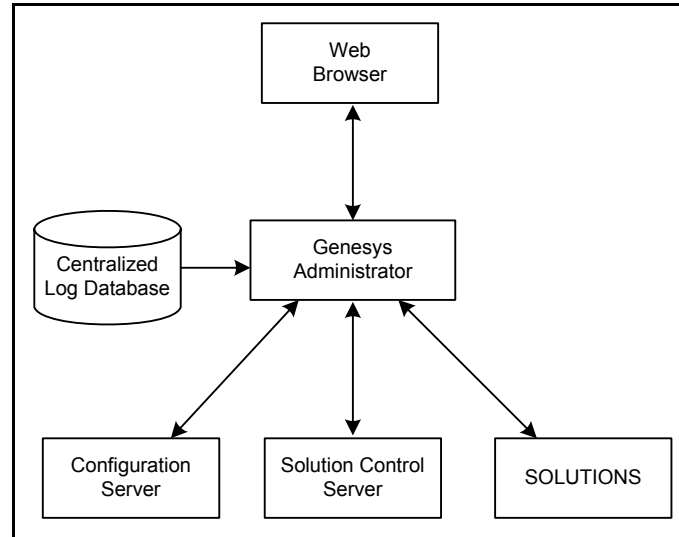
Figure 2: User Interaction Layer Architecture

- The browser-based Genesys Administrator includes a comprehensive user interface to configure, monitor, and control the management environment. Currently, Genesys Administrator is the only component in the User Interaction Layer.

- Genesys Administrator:
  - Communicates with the Configuration Server (a Configuration Layer component) to exchange configuration information.
  - Communicates with the Solution Control Server (a Management Layer component) to exchange status, operations, and control information. Genesys Administrator connects to Solution Control Server individually for each user. This enables the user to be identified in the SCS logs, and for each user to run their session to completeness.
  - Reads logs from the Centralized Log Database (a Management Layer component).
  - Provides the web services for the interface part of Genesys Administrator.

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

Multi-Language Environments

Starting in release 8.1.3, Genesys Administrator supports the entry and display of UTF-8 encoded data in multi-language environment, if the Configuration Database and Configuration Server to which Genesys Administrator is connected are configured to support the same multi-language functionality.

Currently, UTF-8 encoding is supported for the name and value of `Business Attributes` objects.

For information about configuring this support in the Configuration Layer, refer to the *Framework Deployment Guide*. For instructions about configuring this support in Genesys Administrator, refer to "Localization and Multi-language Support" on .

![Genesys]

2 Setting Up Genesys Administrator

This chapter describes how to install and configure Genesys Administrator.

This chapter contains the following sections:

Overview

The User Interaction Layer provides a centralized server environment for a Graphical User Interface (GUI), through which all Genesys applications and solutions can be provisioned, monitored, and otherwise controlled. Genesys Administrator can also manage third-party applications.

Genesys Administrator

The User Interaction Layer consists of one component, Genesys Administrator, that is deployed on a web server and can be accessed using a web browser. At the Framework level, this interface combines the functionality of Configuration Manager and Solution Control Interface.

Prerequisites

Before you start to deploy Genesys Administrator, you should review planning information in the *Framework 8.1 Deployment Guide*. This will help you in

deploying Genesys Administrator and other components of the Framework in a manner that is most appropriate to your situation.

Genesys Administrator requires Management Framework 8.0 or later.

The web server can be any computer that is running Windows Server 2003, 2008, or 2008 R2, and that is capable of acting as a web server. To support Genesys Administrator, however, you must have the following:

- on Windows Server 2003:
  - Microsoft Information Internet Services (IIS), version 6
  - .NET Framework 3.5 SP1/ ASP.Net 2.0
- on Windows Server 2008 (except R2):
  - Microsoft IIS, version 7
  - .NET Framework 3.5 SP1/ ASP.Net 2.0
- on Windows Server 2008 R2:
  - Microsoft IIS, version 7.5
  - .NET Framework 3.5 SP1/ ASP.Net 2.0

Genesys Administrator can also be deployed on a guest Windows Server 2003, 2008, or 2008 R2 operating system running under the supervision of the vmWare vSphere 4 virtualization platform.

Notes: If you are deploying Genesys Administrator on a machine that has ASP.Net running under a non-standard account (that is, not the `NETWORK SERVICE` account, or, when using IIS 7.5 on Windows 2008 R2, not a built-in `DefaultAppPool` account), you must manually grant to that account permissions to the necessary subfolder under the installation folder. See "Required Permissions" on for more information.

Browser Requirements

Genesys Administrator includes a web-based GUI with which you can manage both Genesys and third-party applications and solutions. It is compatible with the following browsers:

- Mozilla Firefox 3.x and later
- Microsoft Internet Explorer 6.x, 7.x, 8.x, 9.x, and 10.x

  Note: Genesys Administrator works in Internet Explorer 10, but you might encounter some problems with the display of the information. Refer to "Display Anomalies with Internet Explorer 10" on for more information.

Genesys Administrator is designed to be viewed at a minimum screen resolution of 1024x768, although higher resolutions are recommended. If you are working in 1024x768 mode, maximize your browser to ensure that you can

see all of the interface. In addition, all windows of the browser must be set to a resolution of 1024x768 or greater.

Login Security Banner

Starting in release 8.1.0, you can create your own security banner to be displayed to a user logging in to Genesys Administrator. You define the content of the banner, typically the terms of use of Genesys Administrator. Users must accept the terms to proceed, or they can reject the terms to close the application without access.

The user-defined security banner is specified during the installation of each instance of Genesys Administrator. See the procedure "Installing Genesys Administrator" on page 26.

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

Deploying Genesys Administrator

The table on the next page summarizes the steps necessary to deploy Genesys Administrator.

Note: Genesys Administrator runs only on servers running the Windows operating system.

Task Summary: Deploying Genesys Administrator

Task	Related Procedures and Information
1. Install Genesys Administrator.	Use the procedure "Installing Genesys Administrator" below.
2. Verify that Microsoft Internet Information Services (IIS) is configured correctly.	Use one of the following procedures, as appropriate: • If installing on Windows Server 2008 R2, use "Verifying configuration of IIS in Windows Server 2008 R2" on page 28. • If installing on Windows Server 2008 (any version other than R2), use "Verifying configuration of IIS in Windows Server 2008 (except R2)" on page 30. • If installing on Windows Server 2003, use "Verifying configuration of IIS in Windows Server 2003" on page 32.

Task Summary: Deploying Genesys Administrator (Continued)

Task	Related Procedures and Information
3. (Optional) Secure the connection between a web browser and the server on which Genesys Administrator is installed.	Use one of the following procedures, as appropriate: • If using Windows Server 2008 R2, "Securing connection between web browser and Genesys Administrator server running Windows Server 2008 R2" on page 33. • If using Windows Server 2008 (any version other than R2), use "Securing connection between web browser and Genesys Administrator server running Windows Server 2008 (except R2)" on page 34. • If using Windows Server 2003, use "Securing connection between web browser and Genesys Administrator server running Windows Server 2003" on page 35.
4. Define external repositories for metadata.	When uninstalling Genesys Administrator, all data in embedded storage is removed. Likewise, when upgrading Genesys Administrator, any metadata already present will be removed from embedded storage. If you will be installing more than one instance of Genesys Administrator, it is strongly recommended that you configure external metadata storage before you import the metadata. Use the configuration option `metadata-store` in the `Application` object used to log in to Genesys Administrator.

Procedure: Installing Genesys Administrator

Prerequisites

• See "Prerequisites" on page 23.

Start of procedure

1. On the Genesys Administrator 8.1 product CD, locate and open the installation directory `/web_configuration_manager/`.

2. To start the Genesys Installation Wizard, locate and run `setup.exe` using Window's `Run as administrator` functionality. Refer to Windows documentation for more information about this functionality.

3. Use the `About` button on the wizard's `Welcome` page to review the `read_me` file. This file also contains a link to Genesys Administrator's Release Notes file.

4. On the `Security Banner Configuration` page, choose whether you want to configure a security banner for this Genesys Administrator application. Refer to the *Genesys 8.1 Security Deployment Guide* for detailed information about the security banner. Do one of the following:

   • If you do not want to configure a security banner for this application, clear the `Enable Security Banner` check box, and click `Next`.

   • If you want to configure a security banner for this application:

      i. Select `Enable Security Banner`.

      ii. Follow the instructions in the procedure "Installing and configuring the Security Banner" in the *Genesys 8.1 Security Deployment Guide*. When you are finished that procedure, return here and finish this procedure.

5. On the `Choose Destination Location` page, the wizard displays the destination directory.

   If necessary, click:

   • `Browse` to select another destination folder.

   • `Default` to reinstate that selection.

   Click `Next` to proceed.

6. On the `Ready to Install` page, click:

   • `Back` to update any installation information.

   • `Install` to proceed with the installation. `Installation Status` displays the installation progress.

7. On the `Installation Complete` page, click `Finish`.

   As a result of the installation, the application `wcm` is created in IIS under the port 80 website (the `Default Web Site` in IIS).

End of procedure

Next Steps

• Verify the configuration of IIS, using one of the following procedures as appropriate:

   ◆ "Verifying configuration of IIS in Windows Server 2008 R2" on page 28

   ◆ "Verifying configuration of IIS in Windows Server 2008 (except R2)" on page 30

   ◆ "Verifying configuration of IIS in Windows Server 2003" on page 32

Procedure:
Verifying configuration of IIS in Windows Server 2008 R2

Purpose: To ensure that IIS 7.5 is configured properly on Windows Server 2008 R2 and can support the Genesys Administrator interface.

Prerequisites

* Genesys Administrator is installed, using the procedure "Installing Genesys Administrator" on page 26.

Start of procedure

1. In Windows, select `Start` > `Administrative Tools` > `Server Manager`.

2. In the left panel of the `Server Manager` dialog box, select `Roles` > `Web server (IIS)` > `Internet Information Services (IIS) Manager`.

3. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, open the `<your computer name>` folder and click `Application Pools`.

4. In the `Application Pools` pane, double-click `DefaultAppPool` to select `Edit Application Pool`.

5. In the `Edit Application Pool` dialog box, verify the following:
   a. `.NET Framework version` is set to `.NET Framework v<latest version number starting with 2.0>`.
   b. `Managed pipeline mode` is set to `Integrated`.

   Click `OK` to close the dialog box.

6. If ASP.Net is not installed, close IIS Manager and install the ASP.Net component located under `IIS` > `World Wide Web Services` > `Application Development Features`. To install ASP.Net:
   a. Select `Start` > `Server Manager`.
   b. Expand the tree in the left pane of the Server Manager, and select `Manage Roles` > `Web Server (IIS)`.
   c. In the right pane, under the `Add Role Services` option, select `ASP.Net`.

7. Ensure that IIS Manager recognizes Genesys Administrator, as follows:
   a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Sites` > `Default Web Site` folder.
   b. With `Default Web Site` selected, select `View Applications` from the `Actions` menu.

    c. If Genesys Administrator is not listed, do the following:

       i. Select `Add Application` from the `Actions` menu.

       ii. In the `Edit Application` dialog box, set the following fields as directed:

- `Alias` = `wcm`
- `Application Pool` = `DefaultAppPool`
- `Physical Path` = \<Genesys Administrator installation path\>

       iii. Click `OK`.

8. Ensure that IIS recognizes the Genesys Administrator virtual directories, as follows:

    a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Sites` > `Default Web Site` folder.

    b. With `Default Web Site` selected, select `View Virtual Directories` from the `Actions` menu.

    c. If the Genesys Administrator virtual directory is not listed, do the following:

       i. Select `Add Virtual Directory` from the `Actions` menu.

       ii. In the `Edit Virtual Directory` dialog box, set the following fields as directed:

- `Alias` = `wcm`
- `Physical Path` = \<Genesys Administrator installation path\>

       iii. Click `OK`.

9. Ensure that Anonymous Authentication is enabled with the correct settings, as follows:

    a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Sites` > `Default Web Site` folder.

    b. Select the folder in which you installed Genesys Administrator, and select `Properties` from the context menu.

    c. Double-click `Authentication` in the `IIS` section.

    d. In the `Authentication` pane, select `Anonymous Authentication` and then select `Edit` from the `Actions` menu.

    e. In the `Edit Anonymous Authentication Credentials` dialog box, select `Application pool identity`.

    If you are using a different account to run the application pool, make sure that the same account is used for anonymous access here, and that permissions to the `<targetdir>` folder of the local file system includes this account with Read, Execute and List permissions.

    f. Click `OK` to close the dialog box.

10. Verify that MIME mapping is correct, as follows:

    a. In the `Connections` pane of the `Internet Information Services (IIS)` `Manager` dialog box, expand the `<your computer name>` > `Sites` > `Default Web Site` folder.

    b. Right-click on the folder in which you installed Genesys Administrator, and select `Properties` from the context menu.

    c. Select `MIME Types` in the `IIS` section and ensure that the settings default to one of the IIS server levels.

End of procedure

Next Steps

- (Optional) Secure the connections for Genesys Administrator. Use the procedure "Securing connection between web browser and Genesys Administrator server running Windows Server 2008 R2" on page 33.

Procedure:
Verifying configuration of IIS in Windows Server 2008 (except R2)

Purpose: To ensure that IIS 7 is configured properly on Windows Server 2008, and can support the Genesys Administrator interface.

Prerequisites

- Genesys Administrator is installed, using the procedure "Installing Genesys Administrator" on page 26.

Start of procedure

1. In Windows, select `Start` > `Settings` > `Control Panel` > `Administrative` `Tools` > `Internet Information Services (IIS) Manager`. The `Internet` `Information Services (IIS) Manager` dialog box appears.

2. In the `Connections` pane of the `IIS Manager` dialog box, open the `<your` `computer name>` folder, click `Application Pools`, and double-click `DefaultAppPool`.

3. In the `Edit Application Pool` dialog box, verify the following:

    a. `.NET Framework version` is set to `.NET Framework v<latest version` `number starting with 2.0>`.

    b. `Managed pipeline mode` is set to `Integrated`.

Click `OK` to close the dialog box.

4. If ASP.Net is not installed, close IIS Manager and install the ASP.Net component located under `IIS` > `World Wide Web Services` > `Application Development Features`. To install ASP.Net:

    a. Select `Start` > `Server Manager`.

    b. Expand the tree in the left pane of the Server Manager, and select `Manage Roles` > `Web Server (IIS)`.

    c. In the right pane, under the `Add Role Services` option, select `ASP.Net`.

5. Ensure that Anonymous Authentication is enabled with the correct settings, as follows:

    a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Sites` > `Default Web Site` folder.

    b. Right-click on the folder in which you installed Genesys Administrator, and select `Properties` from the context menu.

    c. Select `Authentication` in the `IIS` section, and select `Edit` from the `Actions` menu.

    d. In the `Edit Anonymous Authentication Credentials` dialog box, select `Application pool identity`.

    If you are using a different account to run the application pool, make sure that the same account is used for anonymous access here, and that permissions to the `<targetdir>` folder of the local file system includes this account with Read, Execute and List permissions.

    e. Click `OK` to close the dialog box.

6. Verify that MIME mapping is correct, as follows:

    a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Sites` > `Default Web Site` folder.

    b. Right-click on the folder in which you installed Genesys Administrator, and select `Properties` from the context menu.

    c. Select `MIME Types` in the `IIS` section and ensure that the settings default to one of the IIS server levels.

End of procedure

Next Steps

- (Optional) Secure the connections for Genesys Administrator. Use the procedure "Securing connection between web browser and Genesys Administrator server running Windows Server 2008 (except R2)" on .

Procedure:
Verifying configuration of IIS in Windows Server 2003

Purpose: To ensure that IIS 6 is configured properly on Windows Server 2003, and can support the Genesys Administrator interface.

Prerequisites

- Genesys Administrator is installed, using the procedure "Installing Genesys Administrator" on page 26.

Start of procedure

1. In Windows, select `Start` > `Settings` > `Control Panel` > `Administrative Tools` > `Internet Information Services (IIS) Manager`. The `Internet Information Services (IIS) Manager` dialog box appears.

2. In the left pane of the `IIS Manager` dialog box, open the `<your computer name>` > `Web Sites` > `Default Web Site` folder.

3. Right-click the `wcm` application, and select `Properties` from the menu. The `wcm Properties` dialog box appears.

4. In the `wcm Properties` dialog box:
   a. On the `ASP.Net` tab, verify that the latest version number of ASP.Net starting with 2.0 is selected in the `ASP.NET version` field.
   b. On the `Virtual Directory` tab, verify that the `Local path` is the directory where you installed Genesys Administrator. If not, click `Browse` to set the correct path.

   Click `OK` to close the dialog box.

5. In the left pane of the `IIS Manager` dialog box, click `Web Services Extensions`.

6. In the right pane, select from the `Web Service Extension` list the item starting with `ASP.NET v` and ending with the same version number you selected in step 4, and do one of the following:
   - If the `Allow` button is enabled, click the button.
   - If the `Allow` button is disabled, your selection is already allowed and you do not have to click the button.

7. Verify that MIME types are correct, as follows:
   a. Right-click the `wcm` application, and select `Properties` from the menu. The `wcm Properties` dialog box appears.
   b. On the `HTTP Headers` tab, click `MIME Types`, and make sure it is blank. The default settings from the IIS Server are sufficient and should apply.

8. Close the `IIS Manager` dialog box.

End of procedure

Next Steps

- (Optional) Secure the connections for Genesys Administrator. Use the procedure "Securing connection between web browser and Genesys Administrator server running Windows Server 2003" on .

Procedure:
Securing connection between web browser and Genesys Administrator server running Windows Server 2008 R2

Start of procedure

1. In Windows, select `Start` > `Server Manager`.

2. In the left panel of the `Server Manager` dialog box, select `Roles` > `Web server (IIS)` > `Internet Information Services (IIS) Manager`.

3. Install a security certificate on this host server, as follows:

   a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, right-click ⟨`your computer name`⟩ and select `Server Certificates`.

   b. In the `Actions` pane, click `Import` and do one of the following:
      - Import a security certificate from an existing `.pfx` file.
      - Follow the instructions in the `Create Certificate Request Wizard` to create and install a security certificate on this server.

4. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `Default Web Site` folder.

5. Set up the secure channel to this web site, as follows:

   a. Click `Bindings` in the `Action` pane.

   b. Add `https binding` for the site, selecting the certificate installed in Step 3.

   c. For the wcm web application:
      i. Select `Error Pages` in the `IIS` section on the center pane.
      ii. Select or add error 403.4.
      iii. Customize this error as follows:
         - Select `Execute a URL on this site`.
         - Type `/wcm/NonSSL/SSLRedirect.aspx` in the `URL` field.
      iv. Click `OK` to close the dialog box.

6. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, open the `wcm` application.

7. Modify the secure channel to non-secured web sites, as follows:

  a. In the `Connections` pane of the `Internet Information Services (IIS) Manager` dialog box, select `NonSSL`.

  b. Select `SSL Settings` in the center pane to open the `SSL Settings` dialog box.

  c. In the `SSL Settings` dialog box and select `Properties` from the menu to open the `NonSSL Properties` dialog box.

  d. In the `NonSSL Properties` dialog box, for `NonSSL`, clear the `Require SSL` checkbox.

  e. Click `OK` to close the dialog box.

8. Close the `Internet Information Services (IIS) Manager` dialog box.

End of procedure

Procedure:
Securing connection between web browser and Genesys Administrator server running Windows Server 2008 (except R2)

Start of procedure

1. In Windows, select `Start` > `Settings` > `Control Panel` > `Administrative Tools` > `Internet Information Services (IIS) Manager`.

2. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Web Sites` folder.

3. Install a security certificate on this host server, as follows:

  a. In the center pane of the `Internet Information Services (IIS) Manager` dialog box, right-click `<your computer name>` and select `Server Certificates`.

  b. In the `Action` pane, click `Import` and do one of the following:
  - Import a security certificate from an existing `.pfx` file.
  - Follow the instructions in the `Create Certificate Request Wizard` to create and install a security certificate on this server.

4. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `Default Web Site` folder.

5. Set up the secure channel to this web site, as follows:

  a. Click `Bindings` in the `Action` pane.

  b. Add `https binding` for the site, selecting the certificate installed in Step 3.

    c. For the wcm web application:

      i. Select `Error Pages` in the `IIS` section on the center pane.

      ii. Select or add error 403.4.

      iii. Customize this error as follows:

        • Select `Execute a URL on this site`.

        • Type `/wcm/NonSSL/SSLRedirect.aspx` in the `URL` field.

      iv. Click `OK` to close the dialog box.

6. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, open the `wcm` application.

7. Modify the secure channel to non-secured web sites, as follows:

    a. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, select `NonSSL`.

    b. Select `SSL Settings` in the center pane to open the `SSL Settings` dialog box.

    c. In the `SSL Settings` dialog box and select `Properties` from the menu to open the `NonSSL Properties` dialog box.

    d. In the `NonSSL Properties` dialog box, for `NonSSL`, clear the `Require SSL` checkbox.

    e. Click `OK` to close the dialog box.

8. Close the `Internet Information Services (IIS) Manager` dialog box.

End of procedure

Procedure:
Securing connection between web browser and Genesys Administrator server running Windows Server 2003

Start of procedure

1. In Windows, select `Start` > `Settings` > `Control Panel` > `Administrative Tools` > `Internet Information Services (IIS) Manager`.

2. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `<your computer name>` > `Web Sites` folder.

3. Install a security certificate on this host server, as follows:

    a. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, right-click `Default Web Site` and select `Properties` from the menu to open the `Default Web Site Properties` dialog box.

    b. In the `Default Web Site Properties` dialog box, select the `Directory Security` tab, and click `Server Certificate`.

     c. Follow the instructions in the `Web Server Certificate Wizard` to create (if necessary) and install a security certificate on this server.

     d. When you have finished installing the certificate, click `OK` to close the `Default Web Site Properties` dialog box.

4. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, expand the `Default Web Site` folder.

5. Set up the secure channel to this web site, as follows:

     a. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, right-click `wcm` and select `Properties` from the menu to open the `wcm Properties` dialog box.

     b. In the `wcm Properties` dialog box, select the `Directory Security` tab, and click `Edit` in the `Secure communications` section to open the `Secure Communications` dialog box. Select the `Require secure channel (SSL)` check box, then click `OK` to close the `Secure Communications` dialog box.

     c. In the `wcm Properties` dialog box, select the `Custom Errors` tab, select error `403;4` in the list, and click `Edit` to open the `Edit Custom Error Properties` dialog box. Customize this error as follows:

        • In the `Message type` field, select `URL` from the drop-down list.

        • In the `File` field, type `/wcm/NonSSL/SSLRedirect.aspx`.

     Click `OK` to close the `Edit Custom Error Properties` dialog box.

     d. Click `OK` to close the `wcm Properties` dialog box.

6. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, open the `wcm` application.

7. Modify the secure channel to non-secured web sites, as follows:

     a. In the left pane of the `Internet Information Services (IIS) Manager` dialog box, right-click `NonSSL` and select `Properties` from the menu to open the `NonSSL Properties` dialog box.

     b. In the `NonSSL Properties` dialog box, select the `Directory Security` tab and click `Edit` in the `Secure communications` section to open the `Secure Communications` dialog box. Clear the `Require secure channel (SSL)` check box, then click `OK` to close the `Secure Communications` dialog box.

8. Close the `Internet Information Services (IIS) Manager` dialog box.

End of procedure

Enabling Genesys Administrator to Control The System

To enable you to use Genesys Administrator to control your system, you must first associate Genesys Administrator with a non-server configuration object, normally a Configuration Manager `Application` object.

To start, stop, and monitor applications and solutions, you must add a connection to the Solution Control Server to the Configuration Manager `Application` object with which Genesys Administrator is associated.

To monitor the Configuration Layer components (Configuration DB Server and Configuration Server), you must modify those `Application` objects accordingly. Refer to the section "Enabling Management Layer Control of Configuration Layer" in the *Framework 8.1 Deployment Guide* for detailed instructions.

To access the Centralized Log, you must add a connection to the Database Access Point that provides access to the Log Database to the Configuration Manager `Application` object with which Genesys Administrator is associated.

If you have not set up the Management Layer or the Centralized Log system, you can come back and do this step after the necessary components have been installed.

Solutions

If you are going to use Genesys Administrator to manage other solutions, you might have to add additional configuration options to its Configuration Manager `Application` object after installing the solution. Refer to the product documentation for details about any additional configuration required.

Hardware Load Balancing

Genesys Administrator uses F5 Networks BIG-IP Local Traffic Manager (BIG-IP LTM) for hardware load balancing. The BIG-IP system offers both browser-based and command line configuration tools, so that users can work in the environment where they are most comfortable.

The Configuration Utility is a browser-based application that you can use to install, configure, and monitor the BIG-IP system.

BIG-IP system software has a feature called the single configuration file (SCF). An SCF is a flat, text file that contains a series of bigpipe commands, and the attributes and values of those commands, that reflect the entire configuration of one BIG-IP system. For details on creating and using a single configuration file, see the import and export command descriptions in the *Bigpipe Utility Reference Guide.*

Configuring Secure Network Address Translation

Secure Network Address Translation (SNAT) is used to ensure that replies from servers always traverse to the load balancer on the way back to the client.

One of the most popular SNAT modes is the automap feature that allows the mapping of all original IP addresses of clients to the self address of the F5 unit, or the SNAT pool that allows mapping all the original IP addresses of clients to that SNAT pool.

SNAT with a single IP address, has a limit of 65535 ports. The SNAT connections can fail if a large number of client requests are traversing the SNAT. To mitigate port collisions create SNAT pools or use SNAT automap with an appropriate number of self IP addresses on the Virtual LAN to support the expected level of concurrent connections using SNAT. Table 1 illustrates the SNAT Pool list settings for load balancing Genesys Administrator.

Table 1: SNAT Pool List Settings for Genesys Administrator

SNAT Pool List Name	List of Addresses Used by the SNAT Pool
clientext	\<Load Balancer Virtual Network IP 1 - N\>
	\<Load Balancer Virtual Network IP 1 - N\>
	...
	\<Load Balancer Virtual Network IP 1 - N\>

Using the Configuration Utility, create the SNAT Pool list, so that it resembles the following SCF configuration excerpt:

```
snatpool clientext {
   members
      <Load Balancer Virtual Network IP 1 - N>
      <Load Balancer Virtual Network IP 1 - N>
      ...
      <Load Balancer Virtual Network IP 1 - N>
}
```

Configuring the Load Balancer

Table 2 on page 39 lists the settings that are used to configure the load balancer for Genesys Administrator.

Table 2: Load Balancer Settings for Genesys Administrator

Type	Hostname	IP Address	Configuration Object Name	Notes
Monitor			httpGA	/wcm
Node 1	<DNS hostname of GA1>	<ip address of GA1>	GA1	
Node 2	<DNS hostname of GA2>	<ip address of GA2>	GA2	
...	...	...	...	
Node n	<DNS hostname of GAn>	<ip address of GAn>	GAn	
Pool			poolGA	TCP 80
Virtual IP	hlb-GA.domain.com	<ip address of GA VIP>	GAvip	TCP 80

Using the load balancer Configuration Utility, create the Monitor, Nodes, Pool, and Virtual IP so that the configuration resembles the following SCF configuration excerpt:

```
snatpool clientext {
   members
      <ip address of GA1>
      <ip address of GA2>
      ...
      <ip address of GAN>
}
monitor httpGA {
   defaults from http
   send "GET /wcm"
}
node <DNS hostname of GA1> {
   monitor icmp
   screen GA1
}
node <DNS hostname of GA2> {
   monitor icmp
   screen GA2
}
...
node <DNS hostname of GAn> {
   monitor icmp
   screen GAn
}
pool poolMS1GA {
   monitor all httpGA
   members
```

```
            <DNS hostname of GA1>:http
            <DNS hostname of GA2>:http
            ...
            <DNS hostname of GAn>:http
}
virtual GAvip {
    snatpool clientext
    pool poolGA
    destination <ip address of GA VIP>:http
    ip protocol tcp
    profiles
        http
        tcp
    persist cookie
}
```

Adjusting Regional Settings

Windows operating systems allow you to change regional data and time formats through the Control Panel. However, Microsoft IIS, and therefore Genesys Administrator, does not recognize changes to these settings. Instead, the date and time format that is displayed in Genesys Administrator is that of the Genesys Administrator IIS server.

Depending on the version of Windows that you are running, use one of the procedures in this section to overwrite the default settings, as follows:

*   If you are using Windows 2003, use the procedure "Adjusting regional settings when using Windows 2003", below.

*   If you are using Windows 2008, use the procedure"Adjusting regional settings when using Windows 2008 (except R2)" on page 41.

*   If you are using Windows 2008 R2, use the procedure"Adjusting regional settings when using Windows 2008 R2" on page 42.

If you want to use regional date and time formats with a non-localized version of Genesys Administrator (that is, with no language pack installed), you must also manually update the `Web.config` file (found in the Genesys Administrator installation directory), by editing the following line:

```
<system.web>
    ...
    <globalization culture="en-US" uiCulture="en-us"/>
    ...
</system.web>
```

Change both occurrences of `"en-US"` in this line to the same culture to which you set your regional settings. For example, to change your culture to French (France), use `"fr_FR"`, as follows:

```
<system.web>
```

```
            ...
            <globalization culture="fr_FR" uiCulture="fr_FR"/>

            ...
        </system.web>
```

Procedure:
Adjusting regional settings when using Windows 2003

Start of procedure

1. In Windows, select `Start` > `Run`, and enter `Regedit` in the `Open:` text box.
2. In the `Registry Editor` window, select `HKEY_USERS` > `S-1-5-20` > `Control Panel`, and click on `International`.
3. In the list of registry entries, change each required entry, as follows:
    a. Right-click on the name of the entry, and select `Modify`.
    b. In the `Edit String` dialog box, modify the format as required.
    c. Click `OK`.
4. When you have made all your changes, restart the computer.

End of procedure

Procedure:
Adjusting regional settings when using Windows 2008 (except R2)

Start of procedure

1. In Windows, select `Start` > `Control Panel` > `Region and Language`.
2. On the `Formats` tab, customize any field as required.
3. On the `Administrative` tab:
    a. Click `Copy Settings`.
    b. Select `Welcome screen and system accounts`.
4. Click `OK` to save your changes.
5. Restart the computer.

End of procedure

Procedure:
Adjusting regional settings when using Windows 2008 R2

Start of procedure

1. In Windows, select `Start` > `Control Panel` > `Clock, Language, and Region` > `Change the date, time, or number format`.

2. On the `Formats` tab, customize any field as required.

3. On the `Administrative` tab:
   a. Click `Copy settings`.
   b. Select `Welcome screen and system accounts`.

4. Click `OK` to save your changes.

5. Restart the computer.

End of procedure

Localization and Multi-language Support

Starting with release 8.1.3, Genesys Administrator supports the entry and display of UTF-8 encoded data. This support requires Configuration Server 8.1.2 or later.

Prerequisites

For Genesys Administrator to use UTF-8 encoded data in a multi-language environment, the following prerequisites must be met *before* Genesys Administrator first connects to Configuration Server:

- The Configuration Database and Outbound Contact Database must be set up to be able to store UTF-8 data.

- The Configuration Server to which Genesys Administrator is to be connected must be configured to handle UTF-8 encoded data, and switched into multi-language mode.

- Configuration Server and Genesys Administrator must have compatible settings for UTF-8 support. If the settings are incompatible, data corruption may occur on the Configuration Server side.

Refer to the *Framework Deployment Guide* for more information about configuring databases and Configuration Server in a multi-language environment.

Configuring Genesys Administrator

Genesys Administrator must be configured to handle UTF-8 data, and to use the appropriate locale.

Handling UTF-8 Data

To enable Genesys Administrator to handle UTF-8 encoded data, set the following in the `Web.config` file:

```
PSDKEncoding=UTF-8
```

Locale Settings

Locale refers to the set of error messages and field labels used to localize software. If the Configuration Server locale does not match the locale required by the Genesys Administrator interface, you have two options:

• Use the English US locale file embedded in Genesys Administrator for all fields related to Configuration Server.

• Configure Genesys Administrator to read the latest locale file from the Configuration Server with the desired language and version to which it is connected, and store the locale in a local file for future use. This is particularly helpful if new versions of Configuration Server are available, but the language still is not what is required by Genesys Administrator.

Set the following options in the `Web.config` file to control how Genesys Administrator handles this situation.

OverrideCSLocaleFromLocalCopy

Default Value: `false`
Valid Values: `false`, `true`

If set to `true`, Genesys Administrator uses the locale from a local file, instead of loading it from Configuration Server. This can be useful when the Configuration Server language does not match the Genesys Administrator language pack.

If set to `false` (the default), Genesys Administrator loads the locale file from the Configuration Server.

CSLocaleStorageFileName

Default Value: `cslocale.xml`
Valid Values: <valid filename>`.xml`

Specifies the base file name (without the path) for the name of the locale file that is stored locally if `OverrideCSLocaleFromLocalCopy=true`. The resulting filename is constructed from the specified name by appending the version number of the Configuration Server to which Genesys Administrator is currently connected. The default file (`cslocale.xml`) is embedded in the

application's binaries. If a filename is specified, the file is stored in the local metadata repository of this instance of Genesys Administrator (that is, the `resources/metadata` folder).

If the file cannot be accessed by Genesys Administrator, the locale file from Configuration Server is used.

UpdateCSLocaleCopyOnEachRun

Default Value: `false`
Valid Values: `false`, `true`

Specifies if, each time a member of the `Super Administrators` access group logs in, Genesys Administrator verifies that it has a local copy of the locale for the version of Configuration Server to which it is connected. If set to `true` (default), Genesys Administrator performs the check, and if it does not have a local copy of the locale, it loads the locale information from Configuration Server and stores it in a local file. The name of the local file is the same as that specified in the `CSLocaleStorageFileName option` with the Configuration Server version appended to it. The file is stored in the local metadata repository of this instance of Genesys Administrator (that is, the `resources/metadata` folder).

If set to `false` (the default), Genesys Administrator does not perform the check.

![Genesys logo]

Chapter

3   Accessing Genesys Administrator

This chapter describes how to log in to, and log out of, Genesys Administrator.

This chapter contains the following sections:

Logging In

The Genesys Administrator web-based interface runs on a web server. It is loaded into your browser each time that you open the website where you installed Genesys Administrator. You then log in.

Procedure:
Logging in to Genesys Administrator

Prerequisites

- Configuration DB Server and Configuration Server are installed and running.
- Genesys Administrator is configured, and IIS is running.
- Your browser and its windows are set to a resolution of 1024x768 or greater. If you are working in 1024x768, maximize the browser.

Start of procedure

1. Open a web browser.

2. Enter the following URL in the address bar of the browser:

   `http://<computer name>/wcm/Default.aspx`

   where `<computer name>` is the name of the computer acting as the web server, and on which you installed Genesys Administrator.

   If a Windows error occurs, use the procedure "Troubleshooting Windows error after starting Genesys Administrator" on page 63 to try to fix the problem. Then go back to the computer on which you were logging in to Genesys Administrator and repeat this procedure.

3. Log in to Genesys Administrator as follows:

   a. `User Name`: If you are logging in to the Configuration Layer for the first time, use the Master Account user name, which is `default`. After the appropriate configuration objects of the `Person` type are added to the configuration, use a customized user name.

   b. `Password`: If you are logging in to the Configuration Layer for the first time, use the Master Account password, which is `password`. After the appropriate configuration objects of the `Person` type are added to configuration, use a customized password.

      If you have configured Configuration Server to allow access with a blank password, you can optionally leave the Password field empty. Refer to the *Framework 8.1 Configuration Options Reference Manual* for information about configuring this functionality.

   c. If they are not already displayed, click `More` to display these additional input login fields:

      i. `Application`: The name of the Configuration Manager `Application` object with which it is associated. See "Enabling Genesys Administrator to Control The System" on page 37 for more information.

      ii. `Host name`: The name of the computer on which Configuration Server runs.

      iii. `Port`: The number of the communication port that client applications use to connect to Configuration Server.

   d. Click `Log in`.

   If you get a permissions error, refer to "Required Permissions" on page 61 for instructions.

   End of procedure

Third-party Applications (Pass-Through Login)

Starting in release 8.1, third-party applications can log in to Genesys Administrator on behalf of their user, without that user interacting with the Genesys Administrator login dialog box. In addition, they can open Genesys

Administrator to any page that is accessible from the Genesys Administrator navigation menu.

When this pass-through functionality is implemented, the login request from the third-party application contains all connection parameters for successful login. If the user account on whose behalf the third-party application is logging in is using an expired password and has been configured to be changed at next login, then the login request will fail. The user will have to interact with the Genesys Administrator login dialog box to change their password and log in.

To implement this functionality, third-party applications must follow these guidelines:

- HTTP POST is used.

- The login request is sent to:

  `<Genesys Administrator URL>/LoginEJS.aspx`

- The optional parameter `ReturnUrl` of the POST request is appended to the URL string using the ? (question mark) symbol, in the following format:

  ```
  "ReturnUrl=Default.aspx?menuID=<any valid menu ID from any valid
  GA xml project file, as it appears under App_Data within GA
  installation>"
  ```

  Without this parameter, Genesys Administrator will open to the default page that is specified in its User Preferences.

- The HTTP POST `content-type` must be set to the following:

  `application/x-www-form-urlencoded`

- HTTP POST must contain the following key=value pairs:

  ```
  ApplicationName=<name of Configuration Server Application
    configuration object used to log in to Genesys Administrator>
  Host=<Configuration Server's host's Name or IP address>
  Port=<Configuration Server port used to log in to Genesys
    Administrator>
  UserName=<name of Configuration Server user on whose behalf the
    third-party application is logging in>
  Password=<this user's Configuration Server password, in plain
    text>
  bannerAck=<"" (empty)> or <URL of the Security Banner that this
    user has acknowledged sometime previously>
  bannerShown=<"" (empty)> or <"Yes" token if banner has already
    been shown to the user in the current session>
  ```

Logging Out

Procedure:
Logging out of Genesys Administrator

Start of procedure

To log out of Genesys Administrator, click `Log out` in the Genesys Administrator header.

End of procedure

4 Configuration Options

This chapter describes the configuration options for Genesys Administrator, and includes the following sections:

Setting Configuration Options

Unless specified otherwise, set Genesys Administrator configuration options in the `Options` of the `Application` object to which Genesys Administrator was deployed, using the following navigation path:

- Genesys Administrator or Configuration Manager `Application` object > `Options` tab > `Advanced View (Options)`

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start Genesys Administrator.

Importing and Exporting Configuration Objects

Genesys Administrator enables you to import configuration data from, and export it to, a comma-separated value (CSV), file. The CSV files in both cases are fully compatible with the import and export functionality, and use the same formats and follow the same guidelines. Therefore, you can use the import/export functionality interchangeably. This functionality is available for the configuration object types listed in Table 3, below.

When creating the CSV file, you can define the column names, which map to field names, using configuration options. The options are defined in the configuration section corresponding to the object type, as listed in Table 3. Changes to the options take effect immediately.

Table 3: Object Types and Configuration Sections for Importing and Exporting Configuration Objects

Object Type	Section
Agents / Users	AgentBulkProcess
Agent Groups	AgentGroupBulkProcess
DNs	DNBulkProcess
DN Groups	DNGroupBulkProcess
Places	PlaceBulkProcess
Place Groups	PlaceGroupBulkProcess
Tenants	TenantBulkProcess

For general information about this functionality., refer to *Framework 8.1 Genesys Administrator Help.* For information about the options for each object type, refer to *Framework 8.1 Genesys Administrator Help* and navigate as follows:

```
Provisioning Your Environment >
    Core Object Types >
        <Object Type> >
            Importing and Exporting >
                Customizing the CSV File
```

default Section

This section must be called `default`, and is configured in the Genesys Administrator or Configuration Manager `Application` object with which Genesys Administrator was deployed.

csv_separator

Default Value: `c` (comma)
Valid Values: `,` (comma) `;` (semicolon), or any non-empty string with an ASCII code value of less than 127
Changes Take Effect: Immediately

Defines the list separator to be used by the agent import and agent export utilities in Genesys Administrator.

This can be used anytime that your system uses a different list separator than that expected by the agent import utility, to ensure that the export file can be imported back into the Configuration Database by Genesys Administrator.

metadata_store

Default Value: `<Genesys Administrator installation folder>\resources\metadata`
Valid Values: Any valid path and folder
Changes Take Effect: Immediately

Specifies the folder where all metadata files are stored. This folder must have the necessary permissions as described in the section "Required Permissions" on .

security Section

This section must be called `security`, and is configured in the Genesys Administrator or Configuration Manager `Application` object with which Genesys Administrator was deployed.

enable_reconnection

Default Value: `true`
Valid Values: `true`, `false`
Changes Take Effect: After re-login to Genesys Administrator

If set to `true` (default), specifies that Genesys Administrator is to reconnect to a Configuration Server if the connection is lost. Genesys Administrator will continue trying to reconnect for the period of time specified by the option `reconnection_timeout`.

If set to `false`, Genesys Administrator will not attempt to reconnect to Configuration Server, and will redirect the user to the Login dialog.

disable-rbac

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: At next login

Enables (`true`) or disables (`false`) Role-Based Access Control for an application.

Refer to the chapter "Role-Based Access Control" in the *Genesys 8.1 Security Deployment Guide* for complete information about Role-Based Access Control.

reconnection_timeout

Default Value: `60`
Valid Values: `5–600` seconds
Changes Take Effect: After re-login to Genesys Administrator

Specifies the period of time that Genesys Administrator will try to reconnect to a Configuration Server if the connection is lost. This option applies only if the option `enable_reconnection` is set to `true`.

TenantCreateDialog Section

This section contains the options that you can use to customize the creation of a new Tenant. Use these options to display additional fields on the configuration tab, and to define additional steps that will be carried out during creation depending on input you provide in these additional fields

For full descriptions about these options, refer to *Framework 8.1 Genesys Administrator Help*.

Note: These options must be set before configuring a new Tenant. These options apply only while the Tenant is being created; once the Tenant is created and saved, these options no longer apply to that Tenant. These options cannot be used when importing new Tenants from a .csv file (see "Importing and Exporting Configuration Objects" on).

CSThrottling Section

This section contains the options required to implement throttling to prevent Configuration Server from being overwhelmed by the number of requests it receives when a user is bulk provisioning objects through Genesys Administrator. For more information about throttling, refer to *Framework 8.1 Genesys Administrator Help*.

This section must be called `CSThrottling`.

BulkUpdateBatchSize

Default Value: `0`
Valid Values: `0` or any positive integer
Changes Take Effect: Immediately

Specifies the number of requests for bulk provisioning of configuration objects to send to Configuration Server before pausing for the timeout specified by the BulkUpdateBatchTimeout option. The default value of zero (`0`) specifies that all requested updates will be sent to Configuration Server, one at a time, for processing.

BulkUpdateBatchTimeout

Default Value: `0`
Valid Values: `0–300`
Changes Take Effect: Immediately

Specifies the timeout (in seconds) after Genesys Administrator has stopped sending requests for bulk provisioning of configuration objects to Configuration Server (specified by the BulkUpdateBatchSize option) before starting to send them again. The default value of zero (0) indicates that no timeout will occur.

GAOutboundCampaignStats Section

This section contains options that define Outbound Contact statistics that you can select to include in the Outbound Contact reports generated by Genesys Administrator on the `Monitoring` tab.

This section must be called `GAOutboundCampaignStats`.

Stat<n>

Default Value: No default value
Valid Values: Any valid name of an Outbound Contact statistic
Changes Take Effect: Immediately

Specifies the name of a statistic that is defined for the Outbound Contact solution, and can be included in an Outbound Contact report generated by Genesys Administrator on the `Monitoring` tab. The statistic named by this option appears in the `Select Statistics` dialog box, in which you select the statistic for inclusion in, or exclusion from, a report, and define an `Alias` name for the statistic name as it will appear in the report.

The `<n>` in the name of this option is a number, starting with one (1), that permits you to specify multiple statistics if required. If you are specifying only one statistic, use `Stat1`. If you are specifying more than one statistic, use `Stat1`, `Stat2`, `Stat3`, and so on, as shown in the following example that specifies two statistics.

```
[GAOutboundCampaignStats]
Stat1=Statistic1Name
Stat2=Statistic2Name
```

For more information about Outbound Contact Statistics, refer to Outbound Contact Solution documentation.

Changes from 8.0 to 8.1

Table 4 on provides all the changes to Genesys Administrator options between release 8.0 and the latest 8.1 release.

Table 4: Genesys Administrator Option Changes from 8.0 to 8.1

Option Name	Option Values	Type of Change	Details
AgentBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	`255 – 9999`	New	
UserName	Any string	New	
FirstName	Any string	New	
LastName	Any string	New	
Email	Any string	New	
Password	Any string	New	
EmployeeID	Any string	New	
State	Any string	New	
AgentFlag	Any string	New	
SkillAdded	Any string	New	
SkillLevel	Any string	New	
SkillRemove	Any string	New	
SwitchName	Any string	New	
AgentLogin	Any string	New	
WrapUpTime	Any string	New	

Table 4: Genesys Administrator Option Changes from 8.0 to 8.1 (Continued)

Option Name	Option Values	Type of Change	Details
SectionName	Any string	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
OptionName	Any string	New	
OptionValue	Any string	New	
SwitchRemove	Any string	New	
AgentLoginRemove	Any string	New	
AccessGroup	Any string	New	
AccessGroupRemove	Any string	New	
AgentGroup	Any string	New	
AgentGroupRemove	Any string	New	
ExternalID	Any string	New	
DefaultPlace	Any string	New	
CapacityRule	Any string	New	
CostContract	Any string	New	
Site	Any string	New	
Rank	Any string	New	
RankAdded	Any string	New	
RankRemoved	Any string	New	
RequirePasswordChange	Any string	New	
AgentGroupBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	255 – 9999	New	
AgentGroupName	Any string	New	
State	Any string	New	
Agent	Any string	New	

Table 4: Genesys Administrator Option Changes from 8.0 to 8.1 (Continued)

Option Name	Option Values	Type of Change	Details
AgentRemoved	Any string	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
SectionName	Any string	New	
OptionName	Any string	New	
OptionValue	Any string	New	
DNBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	255 – 9999	New	
Number	Any string	New	
Type	Any string	New	
State	Any string	New	
Register	Any string	New	
RouteType	Any string	New	
SwitchSpecificType	Any string	New	
Association	Any string	New	
Alias	Any string	New	
SectionName	Any string	New	
OptionName	Any string	New	
OptionValue	Any string	New	
DNGroupBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	255 – 9999	New	
DNGroupName	Any string	New	
State	Any string	New	
GroupType	Any string	New	

Table 4: Genesys Administrator Option Changes from 8.0 to 8.1 (Continued)

Option Name	Option Values	Type of Change	Details
DNName	Any string	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
DNRemoved	Any string	New	
SectionName	Any string	New	
OptionName	Any string	New	
OptionValue	Any string	New	
PlaceBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	255 – 9999	New	
PlaceName	Any string	New	
State	Any string	New	
DN	Any string	New	
DNRemoved	Any string	New	
SectionName	Any string	New	
OptionName	Any string	New	
OptionValue	Any string	New	
PlaceGroupBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	255 – 9999	New	
PlaceGroupName	Any string	New	
State	Any string	New	
Place	Any string	New	
PlaceRemoved	Any string	New	
SectionName	Any string	New	
OptionName	Any string	New	

Table 4: Genesys Administrator Option Changes from 8.0 to 8.1 (Continued)

Option Name	Option Values	Type of Change	Details
OptionValue	Any string	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
TenantBulkProcess (new section)			
RowIdx	1 – number of lines in import file	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
MaxRowColumns	`255` – `9999`	New	
TenantName	Any string	New	
State	Any string	New	
ParentName	Any string	New	
ChargNumber	Any string	New	
SectionName	Any string	New	
OptionName	Any string	New	
OptionName	Any string	New	
TenantCreateDialog (new section)			
EnableNewTenantCustomization	`0`, `1`	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
TenantAdminAccountChkBox	`0`, `1`	New	
TenantAdministratorsRoles	Empty string or list of Roles	New	
TenantAdministratorsRolesChkBox	`0`, `1`	New	
TenantUsersRoles	Empty string or list of Roles	New	
TenantUsersRolesChkbox	`0`, `1`	New	
TenantAdminLoginChkbox	`0`, `1`	New	
TenantUsersLoginChkbox	`0`, `1`	New	
TenantAdministratorsAccess	`0`, `1`, `2`	New	

Table 4: Genesys Administrator Option Changes from 8.0 to 8.1 (Continued)

Option Name	Option Values	Type of Change	Details
TenantAdminCreateDefaultLegacyRanks	Empty string or list of application types	New	Refer to *Framework 8.1 Genesys Administrator Help* for complete details about these options.
TenantAppFolderCreateMode	`0`, 1	New	
TenantAppAccountCreateMode	`0`, 1	New	
TenantAppAccountCreateFormat	String	New	
default			
csv_separator	semicolon, comma, non-empty string with ASCII value less than 127	New	See page 51
security			
disable-rbac	true, false	Added in 8.0	See page 52. Not previously documented.
CSThrottling (new section)			
BulkUpdateBatchSize	`0` or any positive integer	New	See page 53.
BulkUpdateBatchTimeout	`0 − 300`	New	See page 53.
GAOutboundCampaignStats (new section)			
Stat<n>	Statistic name	New	See page 53.

![Genesys logo]

5 Troubleshooting Genesys Administrator

Follow the suggestions in this chapter if your Genesys Administrator installation does not seem to work correctly.

This chapter contains the following sections:

Required Permissions

The Genesys Installation Wizard for Genesys Administrator automatically sets up the required permissions. If you get permission errors when you try to log in to Genesys Administrator, verify that users ASPNET (DefaultAppPool on

Windows Server 2008 R2 with IIS 7.5) and NETWORK SERVICE have been granted the required permissions described in Table 5.

Table 5: Required Permissions for ASPNET and NETWORK SERVICE

Folder	Required permissions
\<Windows install directory>\Microsoft.NET\Framework\\<.NET version>	Read
\<Windows install directory>\Microsoft.NET\Framework\\<.NET version>\Temporary ASP.NET Files	Full Control
\<Windows install directory>\temp	Read/Write/Delete
\<Windows install directory>\system32	Read
\<local Genesys Administrator install directory>	Read/Write/List
\<local Genesys Administrator install directory>\tmp	Read/Write
\<local Genesys Administrator install directory>\resources\metadata	Read/Write
\<local Genesys Administrator install directory>\resources\deployment	Full Control
\<local Genesys Administrator install directory>\resources\deployment\data\repository_ip	Full Control
\<local Genesys Administrator install directory>\resources\deployment\data\scenarios	Full Control
\<local Genesys Administrator install directory>\resources\GVP	Full Control

---

Notes: • If you are deploying Genesys Administrator on a machine that has ASP.Net running under a non-standard account (that is, not the NETWORK SERVICE account, or, when using IIS 7.5 on Windows 2008 R2, not a built-in `DefaultAppPool` account), you must manually grant to that account permissions to the necessary subfolder under the installation folder. See Table 5 on page 62.

• If you are deploying Genesys Administrator on IIS that uses a non-standard anonymous authentication account (that is, not `IUSR_<machine_name>` for Windows 2003, `IUSR` for Windows 2008, or `DefaultAppPool` identity on Windows 2008 R2), make sure that this non-standard account has been granted the same set of permissions as listed in Table 5 on page 62.

• If you are using Windows 2008 R2, to grant permissions to the file system folders for the `DefaultAppPool` account, you must do the following in the `Select users or groups` dialog box in Windows:

  • Enter the exact name `IIS AppPool\DefaultAppPool` in the `Select users or groups` dialog box in Windows.

  • Ensure that you have selected the local machine name as the location search in the same dialog.

  • Click `Check Names`. Windows will confirm the account name.

Error After Entering Genesys Administrator URL

If you get a Windows error after entering the URL of Genesys Administrator in your browser, follow the steps in the procedure "Troubleshooting Windows error after starting Genesys Administrator" on page 63.

Procedure:
Troubleshooting Windows error after starting Genesys Administrator

Purpose: To try to diagnose and repair the scenario in which a Windows error is displayed after entering the Genesys Administrator URL in a browser.

Start of procedure

1. Log on to the host computer on which Genesys Administrator is installed.

2. Open `Microsoft Internet Information Services (IIS) Manager` from the Windows `Start` menu.

   a. In the left pane, open the `<your computer name>` > `Web Sites` folder.

b. If (Stopped) appears after Default Web Site, do the following:

    i. Stop all other web servers on that computer.

    ii. Right-click Default Web Site and select Start from the menu.

    iii. Go back to the computer on which you were logging in to Genesys Administrator and log in again.

c. Verify that MIME Types are set correctly for the wcm application, as follows:

- For IIS 6 on Windows 2003:

    i. Right-click the wcm application and open its Properties.

    ii. Select the HTTP Headers tab.

    iii. Click MIME Types.

    iv. Ensure that the list is blank, so the default MIME types on the Server level will be used.

- For IIS 7 or 7.5 on Windows 2008:

    i. Select the wcm application.and open its Properties.

    ii. In the IIS section on the right, click MIME Types.

    iii. Ensure that the list is the same as the list of the default MIME types at the Server level.

End of procedure

Unsuccessful Login

The amount of specific information displayed in the Error dialog box when a log in attempt is unsuccessful depends on the settings of the options EnableLoginDenialDetails and EnableLoginCommFailureDetails in the Web.config file. By default, only generic information providing a general description of the error is displayed. However, you can configure Genesys Administrator to display more specific information by using one or both of these options.

For more information about these options, refer to the *Genesys Security Deployment Guide*.

New Users

If a newly-created user is unable to log in to Genesys Administrator, or has logged in but cannot see or do anything, it is probably because that user has not been given any permissions or role privileges, or have been given inappropriate ones.

Normally, new users are assigned to Access Groups and through those groups, the users are granted the necessary permissions and role privileges necessary to log in to Genesys Administrator and do their assigned tasks. However, if you

are creating a new user that, for some reason, is not or can not be assigned to such an Access Group, provide that new user with the following minimum permissions and role privileges:

- Read and Execute permissions for the Application object used to log in to Genesys Administrator. This enables the new user to log in.

- At least one role privilege, so that once they are logged in, they can at least see or do something. This role privilege must have no prerequisites. Normally, they will be assigned to appropriate roles corresponding to their work responsibilities while they are being created, that is, before the users log in for themselves.

400 Error

The `HTTP 400 - request headers too long` error message means the size of the HTTP request headers received on an IIS server exceeds the maximum allowed limit permitted on that particular IIS instance. When this happens, IIS may reject the request and send this error as the response.

To resolve this, Genesys makes the following recommendations:

- Try increasing the `MaxRequestBytes` and `MaxFieldLength` values on each IIS server on which the problem is observed as described at the URL `http://support.microsoft.com/kb/820129`. You may need to adjust both of these fields.

- Use other browsers (Mozilla Firefox, Google Chrome, or Microsoft Internet Explorer) to test Genesys Administrator.

500 Error

You might see a 500 Error after you have successfully logged in to Genesys Administrator, while the Dashboard is loading. The error will be something like `Server indicated error: 500. Object reference not set to an instance of an object.`

If you encounter this error, check the following:

- In the Configuration Manager `Application` object with which Genesys Administrator was bound, there is a connection to the Log Database DAP.

- In the Log Database DAP, the `DBMS Name` property in the `DB Info` section contains a full name or IP address of the host on which the database is installed, and not `localhost`.

File Uploading Stalls

There is a limit to the number of records, such as calling lists or configuration data, that can be uploaded using Genesys Administrator. This is a limit imposed by ASP.NET.

If, when uploading files, the uploading message does not close even though all progress has stopped, you have encountered this limit. As a workaround, Genesys recommends that you check the size of the file and the number of records, and do one of the following:

- Split the original file and upload each section of it. This is the preferred method.
- Set the `maxRequestLength parameter` in ASP.NET on the Genesys Administrator host to allow more data to be transferred, and increase the timeout to enable the transfer to complete. Refer to the Microsoft article, located at:

  `http://msdn.microsoft.com/en-us/library/e1f13641(v=vs.90).aspx`

  Warning! Genesys does not recommend this approach, because it could decrease IIS/ASP.NET performance and increase memory consumption. If absolutely necessary, change the parameters only for long enough to transfer the data, then reset them to their original values and restart the server.

Regional Settings Displayed Incorrectly

If you have set your regional settings, such as a date or time format, specific to your location or culture, they may not be displayed properly in Genesys Administrator. This is because Microsoft IIS does not read these settings.

If you encounter this problem, use one of the procedures in "Adjusting Regional Settings" on page 40.

National Characters Displayed Incorrectly

If you are working in an environment with national characters, you might encounter issues as described in this section.

- If you are working in a multi-language environment and rely on UTF-8 encoding as supported by Management Framework, some national characters might not be displayed correctly in some browsers. To remedy this problem, make sure that you are using one of the following browsers:
  - Microsoft Internet Explorer 8.x or later
  - Mozilla Firefox 20 or later

- If you are working in single-language mode and are having issues with display of data in its national language, ensure that the settings for DB Server and the DBMS client software are correct, as described in the *Framework Deployment Guide* and the *DB Server User's Guide*.

If you encounter these or any other problems in a multi-language environment, confirm that your multi-language Configuration Server has been set up properly, with the correct settings for DB Server and the DBMS client software, as discussed in the *Framework Deployment Guide* and the *DB Server User's Guide*.

Note: For multi-language mode to work properly, one of the following must be used:
- Genesys Administrator 8.1.303 or later, which detects multi-language mode automatically.
- `PSDKEncoding` option be set in the `Web.Config` file, which enables Genesys Administrator 8.1.301 or later to work properly.

Statistical Information Missing on Dashboard

If you are using remote Solution Control Servers, statistical information (such as the number and status of hosts and alarms) might be missing or not updated on the Dashboard. This problem likely occurs for one of the following reasons:

- Network latency caused by the distance between Genesys Administrator and Solution Control Server.

  To solve this problem, reconfigure your system architecture with Distributed Solution Control Servers, which are designed specifically to address the problem of network latency. Refer to the *Framework 8.1 Deployment Guide* for information about setting up Distributed Solution Control Servers.

- Using Solution Control Servers of release 7.6 or earlier with Genesys Administrator.

  Note: Genesys strongly recommends that you use release 8.0 or later Solution Control Servers with Genesys Administrator.

Request times out Error

You might encounter the error message `Request times out` when Genesys Administrator is performing an operation that appears to require more than expected time to complete. This problem might occur because of slow

performance, Configuration Server, Voice Platform reporting server, or any other component on which Genesys Administrator depends.

If the problem persists, or if it is not possible to obtain results from the remote system fast enough, add the following lines to the Genesys Administrator configuration file `Web.config`:

```
<system.web>
<httpRuntime executionTimeout="1200"/>
</system.web>
```

and restart Genesys Administrator. This will cause Genesys Administrator to wait 1200 seconds (20 minutes) for an operation to complete before generating this error message. The default time out is 120 seconds, or 2 minutes.

Errors Downloading Data from Voice Platform Reports to CSV Format

You might encounter an internal server error message when attempting to download data from Voice Platform reports into a `.csv` file. This occurs when the amount of data being downloaded exceeds the limits imposed by ASP.Net.

To resolve this problem, do either one of the following:

- Using the filters provided in Genesys Administrator, regenerate the report with a lesser amount of data.

- Add (or modify) the following lines in the Genesys Administrator configuration file `Web.config`, as follows:

```
<appSettings>
<add key="aspnet:MaxJsonDeserializerMembers" value="30000"
</appSettings>
```

and then restart the default web site (`/wcm`).

Display Anomalies with Internet Explorer 10

If you are viewing Genesys Administrator with Internet Explorer 10, you might find that some things are not displayed as expected. For example:

- In expanded tree structures, the names of contained items might appear on a separate line after their corresponding ellipse or expand/contract boxes, and aligned with the left-hand margin.

- In an object's properties, some fields may not be partially or fully displayed, even though values for those properties have been configured.

- In Wizards, the instructions might be only half visible.

- The contents of drop-down lists might not be visible.

This is a known issue, and appears to be a problem with the browser. Refer to the *Genesys Administrator 8.1 Release Note* for information about the status of these issues (refer to Known Issue GA-5177).

However, Genesys Administrator does work as expected whether or not these display problems occur. If you experience these problems, you can run Internet Explorer in compatibility mode, as follows:

1. In your browser, press the `F12` key to open a utility pane at the bottom.

2. Click on `Browser Mode: IE10 Compat View`.

3. In the drop-down list, select `Internet Explorer 10 Compatibility View`.

Genesys Administrator Role Privileges

This Appendix describes the role privileges that are available and enforced by Genesys Administrator.

The privileges are generally arranged in a hierarchy based on the four modules of Genesys Administrator. They are organized in this Appendix as follows:

For more information about role privileges for other products, refer to the first Appendix of the product-specific Deployment Guide. For more information about role privileges specifically, and Role-Based Access Control in general, refer to the *Framework 8.1 Security Deployment Guide*.

Common

Prerequisites:

None

Role Privileges

Change Configuration Server Mode	Allows a user to change Configuration Server's operational mode to either Read-Only or Emergency mode as supported by Configuration Server. Emergency mode requires that the user is a member of the Super Administrators access group.

Create Tenants	Allows access to the Import Tenant task and the New button on the Tenants view where they can create new Tenant objects.

Modules

Modules role privileges control whether or not a user has access to the Genesys Administrator modules. Module level access is required as a pre-requisite to all Modules-specific role privileges.

Prerequisites:

None

Role Privileges

Monitoring	Allows access to the Monitoring Module in Genesys Administrator.
Operations	Allows access to the Operations Module in Genesys Administrator.
Provisioning	Allows access to the Provisioning Module in Genesys Administrator.

Monitoring

Monitoring role privileges control whether or not a user has access to the sections in the Monitoring module. Monitoring level access is required as a pre-requisite to all sub-section role privileges.

Prerequisites:

Modules role privilege—Monitoring

Role Privileges

Environment Monitoring	Allows access to the Environment section in the Monitoring module.
Orchestration Monitoring	Allows access to the Orchestration section in the Monitoring module.
Outbound Monitoring	Allows access to the Outbound Contact section in the Monitoring module.
Voice Platform Monitoring	Allows access to the Voice Platform section in the Monitoring module.

Environment Monitoring

Environment Monitoring role privileges control whether or not a user has access to the views in the Environment section of the Monitoring module.

Prerequisites:

Modules role privilege—Monitoring

Monitoring role privilege—Environment Monitoring

Role Privileges

Active Alarms	Allows access to the Active Alarms view in the Environment section of the Monitoring module, where users can view and clear active alarms.
Centralized Log	Allows access to the Centralized Log view in the Environment section of the Monitoring module, where users can view Centralized Log records and can perform log record maintenance.
Dashboards	Allows access to the system Dashboard view in the Environment section of the Monitoring modules, where users can monitor the overall status of all applications, hosts, solutions, and active alarms.

Orchestration Monitoring

Orchestration Monitoring role privileges control whether or not a user has access to the views in the Orchestration section of the Monitoring module.

Prerequisites:

Modules role privilege—Monitoring

Monitoring role privilege—Orchestration Monitoring

Role Privileges

Operational Reporting	Allows access to the Operational Reporting view in the Orchestration section of the Monitoring module, where Users can view statistics and details about active and recently active Orchestration sessions, and terminate active sessions from a list of search results.

Outbound Contact Monitoring

Outbound Contact Monitoring role privileges control whether or not a user has access to the views in the Outbound Contact section of the Monitoring module.

Prerequisites:

Modules role privilege—Monitoring

Monitoring role privilege—Outbound Monitoring

Role Privileges

Calling List Reports	Allows access to the Calling List Reports view in the Outbound Contact section of the Monitoring module, where users can generate Calling List reports for Campaigns.
Campaign Reports	Allows access to the Campaign Reports view in the Outbound Contact section of the Monitoring module, where users can generate real-time Campaign reports.
Dialing Session Reports	Allows access to the Dialing Session Reports view in the Outbound Contact section of the Monitoring module, where users can generate real-time Dialing Sessions reports for Campaigns.

Voice Platform Monitoring

Voice Platform Monitoring role privileges control whether or not a user has access to the views in the Voice Platform section of the Monitoring module.

Prerequisites:

Modules role privilege—Monitoring

Monitoring role privilege—Voice Platform Monitoring

Role Privileges

ASR/TTS Usage	Allows access to the ASR/TTS Usage view in the Voice Platform section of the Monitoring module, where users can view the overall ASR/TTS usage on calls.
ASR/TTS Usage Peaks	Allows access to the ASR/TTS Usage view in the Voice Platform section of the Monitoring module, where users can view the peak ASR/TTS usage on calls.
Active Call Browser	Allows access to the Active Call Browser view in the Voice Platform section of the Monitoring module, where users can view the list of calls currently being processed by GVP.
All Tenants Filter	Allows access to the All Tenants option in the Call Browser report filter pane.

CTIC Dashboard	Allows access to the CTIC Dashboard view in the Voice Platform section of the Monitoring module, where users can view near-real-time CTI Connector component and ICM connection statistics.
Call Dashboard	Allows access to the Call Dashboard view in the Voice Platform section of the Monitoring module, where users can view real-time usage information.
Component Call Arrivals	Allows access to the Component Call Arrivals view in the Voice Platform section of the Monitoring module, where users can view a summary of call arrival date for each component.
Component Call Peaks	Allows access to the Component Call Peaks view in the Voice Platform section of the Monitoring module, where users can view the peak volume of calls during a given time interval.
Fetch Dashboard	Allows access to the Fetch Dashboard view in the Voice Platform section of the Monitoring module, where users can view raw latencies with no exposure to thresholds.
Historical Call Browser	Allows access to the Historical Call Browser view in the Voice Platform section of the Monitoring module, where users can view call details for completed calls.
IVR Profile Call Arrivals	Allows access to the IVR Profile Call Arrivals view in the Voice Platform section of the Monitoring module, where users can view a summary of call arrival data for an IVR Profile.
IVR Profile Call Peaks	Allows access to the IVR Profile Call Peaks view in the Voice Platform section of the Monitoring module, where users can view the peak volume of calls for an IVR Profile.
PSTNC Dashboard	Allows access to the PSTNC Dashboard view in the Voice Platform section of the Monitoring module, where users can view real-time metrics for the PSTN Connectors and their managed Dialogic boards.
SQ Call Failures	Allows access to the SQ Call Failures view in the Voice Platform section of the Monitoring module, where users can view SQ call failures information for Media Control Platform components.
SQ Failure Summary	Allows access to the SQ Failure Summary view in the Voice Platform section of the Monitoring module, where users can view SQ call summaries for Media Control Platform components.
SQ Latency Dashboard	Allows access to the SQ Latency Dashboard view in the Voice Platform section of the Monitoring module, where users can view SQ latency utilization for selected Media Control Platform components.
SQ Latency Summary	Allows access to the SQ Latency Summary view in the Voice Platform section of the Monitoring module, where users can view SQ latency summaries for Media Control Platform components.

SSG Dashboard	Allows access to the SSG Dashboard view in the Voice Platform section of the Monitoring module, where users can view SSG usage information.
Tenant Call Arrivals	Allows access to the Tenant Call Arrivals view in the Voice Platform section of the Monitoring module, where users can view a summary of call arrival data for Tenants.
Tenant Call Peaks	Allows access to the Tenant Call Peaks view in the Voice Platform section of the Monitoring module, where users can view a peak call arrival data for Tenants.
VAR Call Completion	Allows access to the VAR Call Completion view in the Voice Platform section of the Monitoring module, where users can view total call and calls grouped by Call End Action Data.
VAR IVR Action Usage	Allows access to the VAR IVR Action Usage view in the Voice Platform section of the Monitoring module, where users can view statistics on IVR Actions used for an IVR Profile.
VAR Last IVR Action	Allows access to the VAR IVR Action view in the Voice Platform section of the Monitoring module, where users can view details of on IVR Actions used at the end of calls.

Provisioning

Provisioning role privileges control whether or not a user has access to the sections in the Provisioning module. Provisioning level access is required as a pre-requisite to all sub-section role privileges.

Prerequisites:

Modules role privilege—Provisioning

Role Privileges

Accounts	Allows access to the Accounts section in the Provisioning module.
Desktop	Allows access to the Desktop section in the Provisioning module.
Environment	Allows access to the Environment section in the Provisioning module.
Outbound	Allows access to the Outbound Contact section in the Provisioning module.
Routing/eServices	Allows access to the Routing/eServices section in the Provisioning module.

Search	Allows access to the Search section in the Provisioning module.
Switching	Allows access to the Switching section in the Provisioning module.
Voice Platform	Allows access to the Voice Platform section in the Provisioning module.

Environment Provisioning

Environment Provisioning role privileges control whether or not a user has access to the views in the Environment section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Environment

Role Privileges

Alarm Conditions	Allows access to the Alarm Conditions view in the Environment section of the Provisioning module, where users can create, modify, or delete Alarm Condition objects.
Application Templates	Allows access to the Application Templates view in the Environment section of the Provisioning module, where users can create, modify, or delete Application Templates.
Applications	Allows access to the Applications view in the Environment section of the Provisioning module, where users can create, modify, or delete Application objects.
Business Units/Sites	Allows access to the Business Units/Sites view in the Environment section of the Provisioning module, where users can create, modify, or delete Business Unit or Site objects.
Fields	Allows access to the Fields view in the Environment section of the Provisioning module, where users can create, modify, or delete Field objects.
Formats	Allows access to the Formats view in the Environment section of the Provisioning module, where users can create, modify, or delete Format objects.
Hosts	Allows access to the Hosts view in the Environment section of the Provisioning module, where users can create, modify, or delete Host objects.

Scripts	Allows access to the Scripts view in the Environment section of the Provisioning module, where users can create, modify, or delete Script objects.
Solutions	Allows access to the Solutions view in the Environment section of the Provisioning module, where users can create, modify, or delete Solution objects.
Table Access Points	Allows access to the Table Access Points view in the Environment section of the Provisioning module, where users can create, modify, or delete Table Access Point objects.
Tenants	Allows access to the Tenants view in the Environment section of the Provisioning module, where users can create, modify, or delete Tenant objects in a multi-tenant configuration.
Time Zones	Allows access to the Time Zones view in the Environment section of the Provisioning module, where users can create, modify, or delete Time Zone objects.

Switching Provisioning

Switching Provisioning role privileges control whether or not a user has access to the views in the Switching section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Switching

Role Privileges

DN Groups	Allows access to the DN Groups view in the Switching section of the Provisioning module, where users can create, modify, or delete DN Group objects.
IVRs	Allows access to the IVRs view in the Switching section of the Provisioning module, where users can create, modify, or delete IVR objects.
Place Groups	Allows access to the Place Groups view in the Switching section of the Provisioning module, where users can create, modify, or delete Place Group objects.
Places	Allows access to the Places view in the Switching section of the Provisioning module, where users can create, modify, or delete Place objects.

Switches	Allows access to the Switches view in the Switching section of the Provisioning module, where users can create, modify, or delete Switch objects.
Switching Offices	Allows access to the Switching Offices view in the Switching section of the Provisioning module, where users can create, modify, or delete Switching Office objects.

Routing/eServices Provisioning

Routing/eServices Provisioning role privileges control whether or not a user has access to the views in the Routing/eServices section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Routing/eServices

Role Privileges

Business Attributes	Allows access to the Business Attributes view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Business Attribute objects.
Interaction Queues	Allows access to the Interaction Queues view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Interaction Queue objects.
Objective Tables	Allows access to the Objective Tables view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Objective Table objects.
Orchestration	Allows access to the Orchestration view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Orchestration Script objects.
Routing Scripts	Allows access to the Routing Scripts view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Routing Script objects.
Schedules	Allows access to the Schedules view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Schedule Script objects.

Statistical Days	Allows access to the Statistical Days view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Statistical Day objects.
Statistical Tables	Allows access to the Statistical Tables view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Statistical Table objects.
Transactions	Allows access to the Transactions view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Transaction objects.
Voice Prompts	Allows access to the Voice Prompts view in the Routing/eServices section of the Provisioning module, where users can create, modify, or delete Voice Prompt objects.

Desktop Provisioning

Desktop Provisioning role privileges control whether or not a user has access to the views in the Desktop section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Desktop

Role Privileges

Action Codes	Allows access to the Action Codes view in the Desktop section of the Provisioning module, where users can create, modify, or delete Action Code objects.
Scripts	Allows access to the Scripts view in the Desktop section of the Provisioning module, where users can create, modify, or delete Script objects.

Accounts Provisioning

Accounts Provisioning role privileges control whether or not a user has access to the views in the Accounts section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Accounts

Role Privileges

Access Groups	Allows access to the Access Groups view in the Accounts section of the Provisioning module, where users can create, modify, or delete Access Group objects.
Agent Groups	Allows access to the Agent Groups view in the Accounts section of the Provisioning module, where users can create, modify, or delete Agent Group objects.
Agent Info	Allows access to the Agent Info of a User object of type Agent.
Roles	Allows access to the Roles view in the Accounts section of the Provisioning module, where users can create, modify, or delete Role objects.
Skills	Allows access to the Skills view in the Accounts section of the Provisioning module, where users can create, modify, or delete Skill objects.
Users	Allows access to the Users view in the Accounts section of the Provisioning module, where users can create, modify, or delete User objects.

Voice Platform Provisioning

Voice Platform Provisioning role privileges control whether or not a user has access to the views in the Voice Platform section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Voice Platform

Role Privileges

DID Groups	Allows access to the DID Groups view in the Voice Platform section of the Provisioning module, where users can create, modify, or delete DID Group objects.
IVR Profiles	Allows access to the IVR Profiles view in the Voice Platform section of the Provisioning module, where users can create, modify, or delete IVR Profile objects.
Resource Groups	Allows access to the Resource Groups view in the Voice Platform section of the Provisioning module, where users can create, modify, or delete Resource Group objects.

Outbound Contact Provisioning

The Outbound Contact Provisioning role privileges control whether or not a user has access to the views in the Outbound Contact section of the Provisioning module.

Prerequisites:

Modules role privilege—Provisioning

Provisioning role privilege—Outbound

Role Privileges

Calling Lists	Allows access to the Calling Lists view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Calling List objects.
Calling Lists Advanced	Allows access to the Calling Lists Advanced view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Calling Lists Advanced objects.
Campaign Sequences Creation and Modification	Allows user access to the Dialing Sessions / Sequence view in the Outbound Contact section in the Operations module to create and modify Campaign Sequences.
Campaigns	Allows access to the Campaigns view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Campaign objects.
Dialogic Boards	Allows access to the Dialogic Boards view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Dialogic Board objects.
Do Not Call List	Allows access to the Do Not Call List view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Do Not Call List objects.
Fields	Allows access to the Fields view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Field objects.
Filters	Allows access to the Filters view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Filter objects.
Formats	Allows access to the Formats view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Format objects.

Request Log	Allows access to the Request Log view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Request Log objects.
Schedules	Allows user access to the Schedules view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Schedule Script objects.
Tables Access Points	Allows access to the Tables Access Points view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Tables Access Point objects.
Treatments	Allows access to the Treatments view in the Outbound Contact section of the Provisioning module, where users can create, modify, or delete Treatments objects.

Outbound Contact Operations

Outbound Contact Operations role privileges control whether or not a user has access to the sections in the Operations module.

Prerequisites:

Modules role privilege—Operations

Role Privileges

Calling Lists	Allows access to the Calling Lists view in the Outbound Contact section in the Operations module.
Dialing Sessions	Allows access to the Dialing Sessions view in the Outbound Contact section in the Operations module.

Outbound Contact

Outbound Contact role privileges control whether or not a user has access to the views in the Outbound Contact sections of the Operations module.

Prerequisites:

Modules role privilege—Operations

Operations role privilege—either Calling Lists (CL) or Dialing Sessions (DS) as indicated in the table below.

Role Privileges

Calling Lists Data Write Access	Allows user access to the Calling Lists view in the Outbound Contact section in the Operations module to modify Calling List data.
Dialing Session/Sequence Control	Allows user access to the Dialing Lists view in the Outbound Contact section in the Operations module to control Dialing Sessions and Campaign Sequences.
Import Do Not Call List Data	Allows user access to the Calling Lists view in the Outbound Contact section in the Operations module to import Do Not Call List data.
Import/Export Calling List Data	Allows user access to the Calling Lists view in the Outbound Contact section in the Operations module to import and export Calling List data.
Manage Dialing Parameters	Allows user access to the Dialing Lists view in the Outbound Contact section in the Operations module to manage Dialing Parameters.

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

Genesys Framework

- *Framework 8.1 Genesys Administrator Help,* which helps you use Genesys Administrator.
- *Framework 8.0 Architecture Help,* which helps you view the place of a particular component in the Framework architecture and learn about Framework functionality that is new to this release.
- *Framework 8.1 Deployment Guide*, which helps you configure, install, start, and stop Framework components.
- *Framework 8.1 Configuration Options Reference Manual,* which provides descriptions of configuration options for Framework components.
- Release Notes and Product Advisories for this product, which are available on the Genesys Customer Care website at `http://genesyslab.com/support`.

Genesys

- *Genesys 8.1 Security Deployment Guide,* which describes the security features provided by Genesys software, including Transport Layer Security (TLS) support, and provides detailed instructions for deploying the features.
- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.

- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.

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

- *Genesys Supported Operating Environment Reference Guide*
- *Genesys Supported Media Interfaces Reference Manual*

Consult the following additional resources as necessary:

- *Genesys Hardware Sizing Guide,* which provides information about Genesys hardware sizing guidelines for the Genesys 8.x releases.
- *Genesys Interoperability Guide,* which provides information on the compatibility of Genesys products with various Configuration Layer Environments; Interoperability of Reporting Templates and Solutions; and Gplus Adapters Interoperability.
- *Genesys Licensing Guide,* which introduces you to the concepts, terminology, and procedures that are relevant to the Genesys licensing system.
- *Genesys Database Sizing Estimator 8.x Worksheets,* which provides a range of expected database sizes for various Genesys products.

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Documentation website.

Genesys product documentation is available on the:

- Genesys Customer Care website at `http://genesyslab.com/support`
- Genesys Documentation website at `http://docs.genesyslab.com/`
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

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:

81fr_ga-dep_04-2012_v8.1.201.00

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

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. 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.

Type Styles

Table 6 describes and illustrates the type conventions that are used in this document.

Table 6: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 88).	Please consult the *Genesys Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x + 1 = 7$ where x stands for...

Table 6: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	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. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages 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. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (<>)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index