Genesys Administrator Extension Deployment Guide

Genesys Administrator 8.1.4

12/29/2021

Table of Contents

Genesys Administrator Extension Deployment Guide

Welcome to the Genesys Administrator Extension Deployment Guide. This document describes the deployment, starting and stopping, and troubleshooting procedures that are relevant to Genesys Administrator Extension.

About Genesys Administrator Extension

Genesys Administrator Extension (GAX), part of the Genesys Framework, is a web-based graphical user interface (GUI) that provides advanced administrative and operational functionality that is targeted to Hosted Service Providers as well as Enterprise customers. In brief, you can find the following information in this guide:

- How to deploy Genesys Administrator Extension.
- How to access Genesys Administrator Extension.
- Suggestions for troubleshooting your Genesys Administrator Extension 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 Deployment Guide.

Contacting Genesys Customer Care

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.

About This Book

The following list explains different features of GAX:

Overview

This chapter introduces you to the core features of GAX and its architecture.

Setting up GAX

This chapter explains how to deploy GAX.

Accessing GAX

This chapter explains how to access GAX.

Troubleshooting

This chapter explains how to troubleshoot GAX.

Role Privileges

This chapter explains all of the role privileges used by GAX.

Configuration Options

This chapter explains all of the configuration options used by GAX.

Overview

This chapter provides a brief description of Genesys Administrator Extension and its architecture.

This chapter contains the following sections:

Genesys Administrator Extension

Genesys Administrator Extension (GAX) is an application that provides additional administrative capabilities to both technical and business users of Genesys Administrator. Currently, the following GAX core modules are supported:

- Solution Deployment
- Operational Parameter Management
- Audio Resource Management
- Configuration Object Management
- GAX/Genesys Administrator Single-Sign-on

Genesys Administrator Extension also supports plug-in resources from other Genesys products, such as Pulse and GVP Reporting. Refer to Plug-ins for more information.

Genesys Administrator is unaffected by Genesys Administrator Extension. It provides the interface to configure, monitor, and control the management environment.

The following subsections describe some of the features of the GAX interface.

Tenant Filtering

GAX comprises a set of modules that are selected and viewed in a browser interface. Each of the modules enables you to filter the information that you view about the applications that you have configured and deployed in the Genesys environment.

In a multi-tenant environment, GAX enables you to filter your views by a single tenant or by multiple tenants. By default, when you log in the view is of your default tenant. You can use the tenant selector to change the view so that you can view by one or more tenants.

Filtering and Sorting Lists and Tables

All lists and tables in the GAX interface can be sorted by clicking on the column headings. Tables and lists can also be filtered by appropriate criteria, for example:

- Tenant
- Date
- Date range
- Name
- Deployed by
- Deployed date

Field Auto-completion

All fields in the GAX interface that have predefined values support auto-completion. When you start to enter a value in the field, GAX searches for an existing value in the database and completes the entry. You can override auto-completion by continuing to enter the value. You can accept the auto-completion value by pressing `Enter`.

Localization

GAX supports the installation of multiple language packs for the user interface. You can choose to configure one default language across all GAX instances, while each user can select a different language. Default and user-specific language selection is done in the Preferences menu. See Preferences for more information.

You can install language packs by using the plug-in installation procedure. See Installing a GAX compatible plug-in by using the Software Installation Wizard for more information, or refer to the Help pages by clicking the Help button in GAX (also available here).

Solution Deployment

Solution Deployment enables you to fully deploy solution definitions and installation packages (IPs) to remote locations. This includes installation and configuration of all of the necessary applications and updates to existing multi-Tenant applications, where appropriate.

Genesys Deployment Agent (GDA) is required to deploy solution definitions and IPs.

> **Important**
>
> GDA does not support multiple concurrent deployments on the same host. Therefore, multiple users cannot deploy a solution by using GAX on the same host at the same time that GDA is deploying. This limitation has always existed for GDA.

A solution definition consists of none, one, or multiple IPs for Genesys components. For Hosted Provider Edition, the IPs to be deployed must be primarily related to `Tenant` objects, and should contain object definitions, access permissions, and role privileges.

A solution definition consists of an XML file that defines the steps to install, upgrade, or configure IPs and system configurations to successfully deploy a solution. For information about authoring solution definition files, see the Authoring Solution Definitions page.

Solution Deployment can make changes to Tenant objects in Configuration Server, perform installations of IPs, or execute external scripts, such as database scripts.

For each deployed solution, from the Deployed Solutions window, you can export a file that contains the properties, summary, and actions for auditing purposes.

> **Important**
>
> Not all browsers enable you to use filenames that are not US-ASCII compatible; therefore, Genesys recommends that you use only filenames that are US-ASCII compatible.

Defined Privileges

Roles and their privileges are imported into GAX during the upload of an installation package (IP). All privileges that are defined in the metadata of the IP are imported into the GAX database. Privileges are defined as `task` elements in the metadata XML of the IP.

Solution Definition File Version Tracking

During normal use, solution definition files (also called solution package definitions, or SPDs) are added, upgraded, revised, and removed. Solution Deployment supports versioning, auditing, and

tracking of changes of SPDs from within the GAX interface. The tracking report can be exported to a CSV file for use outside of GAX.

Solution Deployment enables you to view and access past versions of SPDs. You can also add custom comments and notes to any version.

You can filter and sort the SPD history by one or more of the following criteria:

- Solution—Group results by deployed solutions.
- Tenant—Group results by Tenant and select a subset of a Tenant or Tenants by solution and version.
- Date—Group results by date range.
- Result—Group by successful and failed deployments.

You can generate reports for both individual solutions as well as for individual Tenants.

You can configure the reports by specific criteria, including the following parameters:

- Solution Definition name
- Solution Definition version
- Tenant name
- Profile
- Date deployed
- Deployed by (name of the individual who performed the deployment)
- Result of deployment (Success, Fail, Unknown)
- Latest (true or false)
- Application name (IP Xref)

External Script Support

Solution Deployment passes arguments to external scripts when executing them, and can receive back results from the execution of a script. For example, if you have a script to create a new virtual host by using the VMware API, you can specify a name or naming convention from within an SPD. You will then receive confirmation that the creation was successful and the name of the new host that was created.

Operational Parameter Management

Operational Parameter Management enables the creation of parameters that can be used in parameterized routing strategies, in which the values of the parameters are defined at runtime and integrated into the call flow. In most cases, parameter creation and assignment proceeds as follows:

1. The Solution Provider defines the parameters by specifying the type of parameter and a name that can be referenced in a strategy.
2. The Solution Provider groups parameters into a Parameter Group Template. A parameter can be associated with one or more templates.
3. The Solution Provider deploys Parameter Group Templates to one or more Tenants.
4. The Tenant administrator, or a user with the appropriate roles and permissions, then enters values for the parameters in the Parameter Group, enabling control of active strategies. Genesys Administrator Extension stores those values in the Configuration Database as part of a `Transaction` object.
5. The Universal Routing Server `Application` object (or any other interaction routing application, such as GVP) executes a routing strategy to read those values and integrate them into the call flow. Orchestration Server and GVP Media Server `Application` objects are also supported.

Routing Strategies

In select cases, a Tenant may create its own routing strategy. The Solution Provider then grants the Tenant permission to define parameters and create the group templates. The Solution Provider must provide the Tenant with all of the required privileges to create parameters, group templates, and deploy groups (refer to Genesys Administrator Extension Role Privileges).

Parameters

Operational Parameter Management can be used to update a parameter group after it has been deployed. You can add, remove, re-order, and modify parameters that have already been deployed to a parameter group. All modifications are tracked as part of the audit trail.

Objects and strategies can be associated with specific Parameter Group Templates to ensure that they are not deployed with the incorrect objects or strategies. Operational Parameter Management provides a view of all of the objects and strategies that are associated with a specific Parameter Group so that you know where the objects are used, including information about Tenant ownership and associated applications and scripts.

You can specify the application type or the specific application object for which the Parameter Group Template is compatible. If the type is set, it becomes a permanent attribute of the application. If there are multiple simple-routing-type routing scripts in the system, you can specify that only one matches the Parameter Group Template and is therefore compatible, rather than all scripts of a type.

When you create the Parameter Group Template, you can select an existing application of a particular type to associate the Parameter Group Template with the application. This ensures that the correct applications are deployed at deployment time.

GVP

Operational Parameter Management can be used to deploy parameters that can be used by Genesys Voice Platform (GVP) and other VXML applications. You can use Operational Parameter Management to deploy a set of parameters to create a new Configuration Layer object that is associated with a specified VXML application that is used by GVP.

Orchestration Applications

Operational Parameter Management can also be used to deploy parameters that can be used by Orchestration Applications (SCXML).

Audio Resource Management

Genesys Administrator Extension provides an interface for Audio Resource Management. This enables you to manage audio resources for both announcements and music files. This module also enables the conversion of audio files (`.wav` using PCM encoding), and the deployment of audio files to Media Servers throughout the network.

> **Important**
>
> Audio Resource Management supports only WAV files that use PCM encoding. If you use non-PCM encoded files, there might be conversion artifacts, or the conversion might fail completely.

Generally, audio resources are handled as follows:

1. The Solution Provider maintains Audio Resources. Each Audio Resource contains one or more Audio Resource Files. Each Audio Resource File is associated with one Personality.

   In select cases, Tenants may also create their own Audio Resource Files, Personalities, and Audio Resources. To create Audio Resources as a tenant, provide the corresponding role privilege to the tenant user.

2. The Solution Provider deploys Audio Resources to Tenants.

   If a Tenant has created its own Audio Resource Files and Personalities, they can add them to the Audio Resources deployed by the Solution Provider.

3. A Routing Strategy that is executed by the Tenant selects an Audio Resource and a Personality. The Routing Strategy might use Operational Parameter Management to make the selection.

> **Important**
>
> All Audio Resources are treated as *system* announcements — even when they are created by a tenant user. This means that a routing block must address the audio resource as resources of type `System Announcement`, not `Tenant Announcement`.

Audio Resource Management supports deployment of multiple audio resources to multiple tenants in a single step. You can select multiple audio resources from the tenant list and execute the deployment to several tenants simultaneously.

Configuration Object Management

Configuration Object Management is responsible for the general management of configuration objects on your system. Configuration objects might include:

- Users and agents
- Campaigns
- DN Groups
- Tenants
- User Access Groups

User-related functions are described in Account Management.

System-related functions are described in Configuration Management.

> **Important**
>
> Configuration objects that can be configured in the `Accounts` menu can also be configured in Configuration Manager, and vice-versa. For example, to create user accounts, you can choose to use the User Accounts page in the `Accounts` menu, or you can use the Users page in Configuration Manager. Although these processes are different, the created objects are treated the same way in the Configuration Database.

For more information about Configuration Object Management, refer to the Genesys Administrator Extension Help Wiki.

Account Management

The `Accounts` menu enables the creation and management of user accounts, agent groups, roles, skills, access groups, and capacity rules.

Configuration Management

Configuration Manager enables the creation and management of system-level configuration objects such as Alarm Conditions, Business Attributes, Hosts, and more. Configuration Manager provides functionality similar to the Configuration Manager application that is part of Management Framework.

Auditing

The auditing feature writes data to Message Server about activities in Operational Parameter Management and Audio Resource Management, and Message Server writes the data to the Genesys Log database. Auditing data is made available to the GAX user by selecting the `History` option in the `Related` menu in the panel of certain items in the GAX user interface. The auditing feature reads the information from the Log database and enables you to view the change history of objects such as Personalities and Parameter Groups.

Architecture

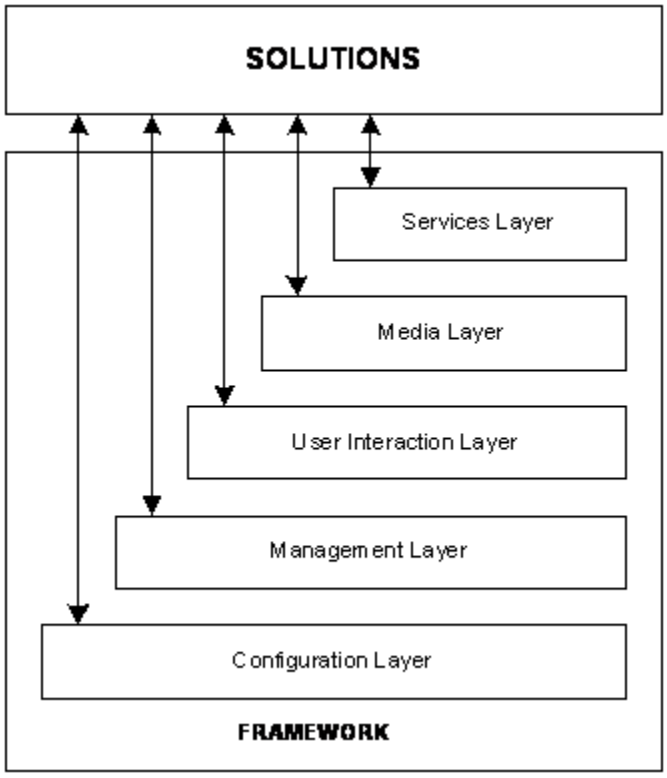
This section describes the architecture of Genesys Administrator Extension as it resides in the User Interface Layer of the Genesys Framework, and the architecture and connections within a Genesys Administrator Extension configuration.

User Interface Layer

Genesys Administrator Extension resides in the User Interaction Layer of the Genesys Framework. This Layer provides comprehensive user interfaces to:

- Configure, monitor, and control the management environment.
- Perform specific tasks related to Solution Deployment, Operational Parameter Management, Audio Resource Management, and Account Management.

The figure below illustrates how the User Interaction Layer is positioned within the Framework architecture.



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.

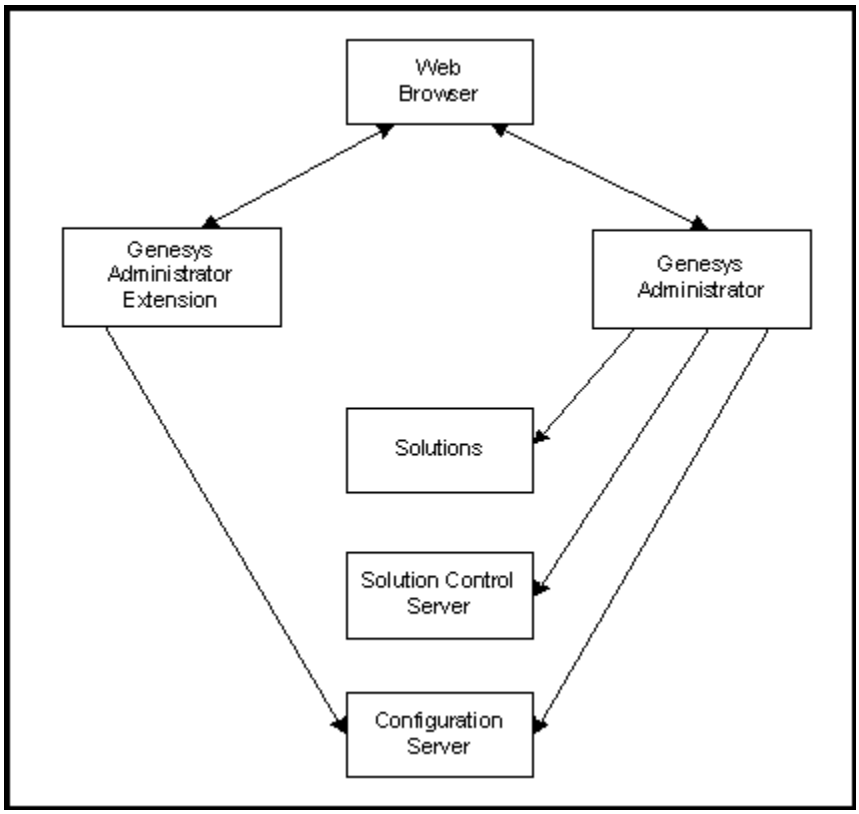
Functions

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

- Remote deployment of Genesys components by using the Genesys Deployment Agent (a Management Layer component).
- Configuration, monitoring, and control of applications and solutions.

Architecture

The figure below shows a more detailed diagram of the architecture of Genesys Administrator Extension.



User Interaction Layer Architecture

The browser-based Genesys Administrator Extension includes a comprehensive user interface to perform tasks that are related to Solution Deployment, Operational Parameter Management, Audio Resource Management, and Account Management.

Currently, Genesys Administrator and Genesys Administrator Extension are the only components in the User Interaction Layer.

Genesys Administrator Extension:

- Communicates with the Configuration Server (a Configuration Layer component) to exchange configuration data.
- Uses the GAX Database to store configuration information and other data, such as operational parameter templates and audio resource metadata.
- Uses Sound eXchange (SoX) to encode audio files.
- Sends encoded audio files to the Audio Resource Manager (ARM) Storage. From the ARM storage, the ARM Web Server distributes them to GVP Media Servers.
- Uploads IPs to Solution Deployment storage.

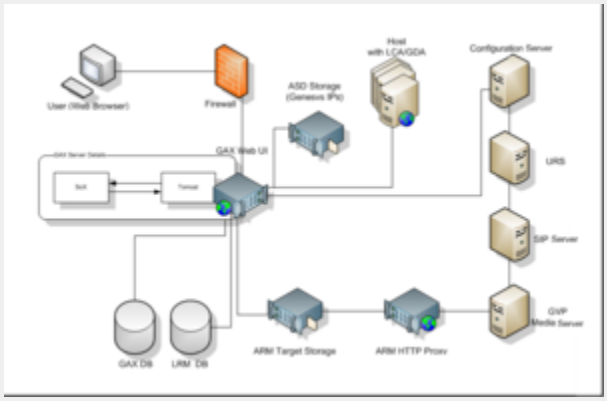
Genesys Administrator:

- 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.
- Reads logs from the Centralized Log Database (a Management Layer component).
- Uploads IPs to Solution Deployment storage.
- Depending on the solutions that are deployed in the system, Genesys Administrator and Genesys Administrator Extension might also communicate with other back-end servers to retrieve solution-specific information.

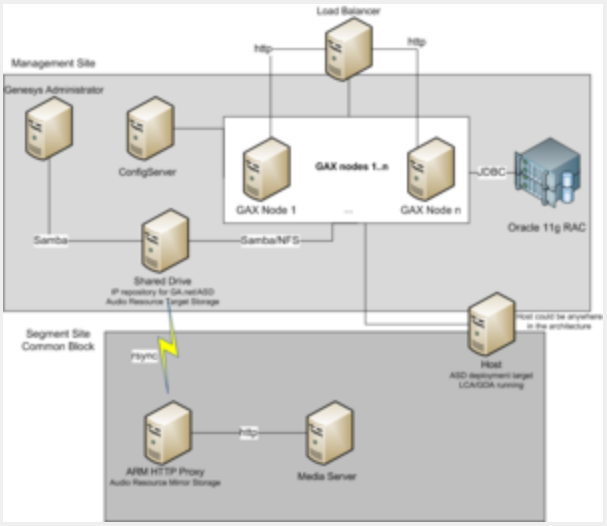
> **Important**
>
> Both TCP/IP v4 and TCP/IP v6 communications are supported between GAX and other Genesys components.

Configurations

Genesys Administrator Extension can be deployed as a single instance or in a load-balanced environment. The left figure below shows how Genesys Administrator Extension connects with its modular components. The right figure below shows the connections that Genesys Administrator Extension makes to other components in a load-balanced environment. When deployed in a load-balanced environment, Genesys Administrator Extension is located in the Management Site.



Genesys Administrator Extension Architecture



Genesys Administrator Extension Architecture in a Load-Balanced Hosted Provider Edition environment

Database Size Requirements

To help you plan to manage your space requirements for audio resources, this section provides information about space allocation for a 100-tenant system with an average of 100 announcement files per segment, including personalities.

Original Audio Resource Files

The space required for the original audio resource files that are uploaded by tenants can be calculated as:

`Original Files Storage Requirements = <# of tenants> x <avg # of announcement files> x <avg file size>`

For example, if you have 100 tenants with 100 audio files of an average size of 3 MB you would have to calculate 30 GB of space for just the original audio files:

`Original Files Storage Requirements =`

100 x 100 x 3 MB =

30,000 MB = 30 GB

Processed Audio Resource Files

The original files are stored both in the database and on the disk (unless database storage is turned off by using the configuration options). The processed files are located only on the disk. Therefore, the raw storage that is required on the disk can be calculated as:

Processed Files Storage Requirements = ((<# of tenants> x <# of announcement files> x <avg file size>) / <compression factor>) x (<# of conversion formats>)

In the example with 100 tenants, the requirement for Processed files is also 30 GB:

Processed Files Storage Requirements =

((100 x 100 x 3 MB) / 3) x (3) =

30,000 MB = 30 GB

Reserved Space

For the database, which holds only the original files, additional space should be reserved to allow for short time peaks and better database performance. Genesys recommends that 50% (1.5 times) of additional space should be reserved for this purpose:

`Database Size Requirements = <Original Files Storage Requirements> x <reserve percentage>`

In this example, the suggested database space requirement is:

```
Database Size Requirements =
```

30 GB x 1.5 = 45 GB

Your disk space requirement should also include reserved space to prevent degraded performance, which can occur if drives become too full.

Genesys recommends that the reserved space allocation is 25% (1.25) of the actual raw requirements:

```
Disk Size Requirements = (<Original Files Storage Requirements> + <Processed Files Storage Requirements>) x <reserve percentage>
```

Therefore, in total, for the original files, the converted files, and reserved space, 75 GB are required:

```
Disk Size Requirements =
```

(30 GB + 3 0 GB) x 1.25 = 75 GB

Setting Up Genesys Administrator Extension

This chapter describes how to install and configure Genesys Administrator Extension. It also describes the prerequisites and other information for setting up Genesys Administrator Extension to perform the tasks that are described in the Overview chapter.

This chapter contains the following sections:

Overview

Genesys Administrator Extension is deployed with a web application server and can be accessed by using a web browser. It does not have to be deployed in the same environment with Genesys Administrator and nothing needs to be installed on client machines.

> **Important**
> GAX is normally deployed in a multiple tenant environment; however, single-tenant environment deployment is supported as of version 8.1.2. If you deploy GAX in a single-tenant environment, the Tenant Management features and filtering are not applicable.

Prerequisites

Before you deploy Genesys Administrator Extension, you should review the planning information in

the Framework 8.1 Deployment Guide. This will help you to deploy Genesys Administrator and other components of the Framework in a manner that is most appropriate to your situation.

Genesys Administrator Extension uses Management Framework. To use the Role-based Access Control feature, Configuration Server 8.1.x is required.

Important

A new application type, `Genesys Administrator Server`, was introduced in Genesys Framework release 8.1.1 for use with Genesys Administrator Extension release 8.1.2 or higher. Previous versions of GAX do not support this new application type and must use the `Genesys Generic Server` application type.

Important

To avoid issues with role assignments, you should upgrade the application, metadata, and the roles to the new type when you migrate to the latest version of GAX or perform a fresh install (see Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.1 or higher).

The computer on which you install Genesys Administrator Extension must be capable of acting as a web application server, and must be running one of the following:

- Red Hat Enterprise Linux 5.5 (64-bit) - Enterprise Edition, with `Updates from RHN` enabled
- Red Hat Enterprise Linux 6.0 (64-bit) - Enterprise Edition, with `Updates from RHN` enabled

Or,

- Windows Server 2008 R2, with 64-bit applications running natively on a 64-bit OS.
- Windows Server 2012, with 64-bit applications running natively on a 64-bit OS.

The computer must also run the following:

- Java 6 or Java 7 Runtime (JRE) from Oracle. See the Setting up the host for Genesys Administrator Extension server for information about obtaining and installing Java, if necessary.

GAX 8.1.4 uses an embedded Jetty instance as the web application server; as a result, Tomcat is no longer a prerequisite to use GAX. For those who choose to use Tomcat instead of Jetty, GAX requires Tomcat 6.0.37 from Apache. Refer to the Upgrading GAX page for additional information.

In addition, each module of Genesys Administrator Extension might have additional prerequisites. Refer to Prerequisites for Genesys Administrator Extension Modules for more information.

> **Tip**
> Refer to the Genesys Supported Operating Environment Reference Guide for a complete list of the operating systems and databases that are supported by GAX.

Browser Requirements

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

- Microsoft Internet Explorer 8.x, 9.x, 10.x
- Mozilla Firefox 17 or higher
- Safari 6 on Macintosh systems
- Chrome

> **Important**
> Genesys Administrator Extension supports all major browsers, but it is optimized for Chrome.

Genesys Administrator Extension 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.

> **Important**
> If the download of Audio Resource Files, Encoded Files, and other GAX downloads are blocked by the Microsoft Internet Explorer 8 or 9 information bar and, after you confirm the download, you are redirected to the main page and you must repeat the download request, you can adjust your browser settings to prevent this scenario (Browser Issues).

Required Permissions and Role Privileges

Genesys Administrator Extension uses a permission-based mechanism and a role-based access control system to protect your data. Before installing and using Genesys Administrator Extension, ensure that all users have the necessary access permissions and role privileges to do their work. The following are examples of scenarios that require permissions:

- A user must have `Update` permission on his or her `User` object to set and save his or her user preferences in Genesys Administrator Extension.

- To log in to Genesys Administrator Extension, a user must have Read permission on his or her `User` object, Read and `Execute` permissions on his or her `Tenant` object, and Read and `Execute` permissions on the Genesys Administrator Extension client `Application` object. These permissions are usually assigned by adding the users to access groups.

There are no role privileges required to log in to GAX. However, GAX-specific functions might require additional role privileges to be enabled. Refer to Role Privileges for more information about role privileges.

Deploying Multiple Instances of GAX with Shared Resources

You can install multiple instances of GAX to support both High Availability (HA) and load balancing. You can also install multiple instances of GAX to take advantage of the GAX plug-in architecture. Each instance of GAX can be deployed with a different combination of plug-ins.

In either scenario, the multiple instances of GAX share the same data resources, such as Configuration Server, the GAX database, and audio resources, but are executed independently by different users on different hosts.

Minimum Required Firewall Permissions and Settings for GAX Deployment

Your firewall must allow incoming connections on the http and https ports. (for example 8080, 80, 433, and so on, based on your setup). The application server can listen on more than one port at once.

You must allow outgoing connections to allow GAX to establish connections; however, you can restrict the connections to networks that contain the following components:

- GDA hosts
- Databases
- Genesys configuration layer servers: Configuration Server, Message Server, and Solution Control Server

Minimum Required File System Permissions and Settings for GAX Deployment

The GAX operating system user is the user that runs the GAX process. The GAX operating system user must be the owner of the folder where it is deployed and must have the following permissions:

- Write permission on the log file folder
- Read/write access to the folder configured for ARM

Deploying Genesys Administrator Extension

The following table summarizes the steps necessary to perform the basic deployment of Genesys Administrator Extension. Before beginning your installation, ensure that you have met the prerequisites listed in Prerequisites. If you plan to install any of the modules in Genesys Administrator Extension, refer to Prerequisites for Genesys Administrator Extension Modules before using them.

The following procedures use Setup Mode to install GAX. Setup Mode is a new feature that can set up new instances of GAX to connect to an existing Management Framework deployment. You can also use Setup Mode to install and configure new Genesys deployments. In the latter scenario, Setup Mode will install GAX, Configuration Server, and Database Server. After these components are installed, you can use the installation package (IP) management features of GAX to deploy entire Genesys installations.

To access Setup Mode, you must be a local user on the machine where GAX will be installed. You are considered a local user if you are using this machine in person or via a remote desktop connection.

> **Important**
>
> - Not all functions are available in GAX if a Configuration Server is not present.
> - Although Configuration Server might support more database types, GAX only supports the following database types: Oracle, Microsoft SQL Server, and PostgreSQL.

Deploying Genesys Administrator Extension

1a. Set up the database for Oracle.

Setting up the Genesys Administrator Extension database (for Oracle)

Purpose

- To set up the Oracle 11g R2 or Oracle 12c database that is used by Genesys Administrator Extension.

If you prefer to use PostgreSQL or Microsoft SQL Server, see Setting up the Genesys Administrator database (for Microsoft SQL Server) or Setting up the Genesys Administrator database (for

PostgreSQL).

Start

1. Refer to the Oracle documentation to install the Oracle Database Management System on the host machine.
2. Use the following SQL commands to create the users and ensure that they do not have excessive permissions:

```
create user <username> identified by <password>;

grant connect, resource to <username>;

alter user <username> quota 10M on USERS;
```

> **Important**
>
> The above quota value is an example. Consult the Oracle documentation to determine the correct quota value for your system.

3. If you are setting up a new Configuration Server, perform the following steps on the Configuration Server host:
   - Run the Oracle Net Configuration Assistant.
   - Select `Local Net Service Name Configuration` to create an entry in the `tnsnames.ora` file to map the Local Net Service Name to the host, port, and SID (System ID) used by the database.

     > **Important**
     >
     > The Local Net Service Name must be the same as the SID in order for Setup Mode in GAX to work properly.

   - The `ORACLE_HOME` environment variable must be set to the installation directory of the Oracle database client.

   Refer to the Oracle documentation for additional details on completing this step.

End

> **Important**
>
> To enable UTF-8 character encoding, see Enabling UTF-8 character encoding (for Oracle).

1b. Set up the database for Microsoft SQL.

Setting up the Genesys Administrator Extension database (for Microsoft SQL Server)

Purpose

- To set up the Microsoft SQL Server 2008/2012 database that is used by Genesys Administrator Extension.

If you prefer to use Oracle or PostgreSQL, see Setting up the Genesys Administrator database (for Oracle) or Setting up the Genesys Administrator database (for PostgreSQL).

Start

1. Refer to the Microsoft SQL Server documentation to create the Microsoft SQL Server Database for GAX.
2. Start SQL Server Management Studio.
3. Connect to Microsoft SQL Server as `sa`.
   - Server type: `Database Engine`
   - Server name: `Local`
   - Authentication: `SQL Server Authentication`

- Create a login and password for the GAX database. For example: `gax814admin` with the password `password`.
- Create the GAX database (for example, `gax814`) by using the login to make this login the owner of the database.

> **Important**
> When you create the login, uncheck the `Enforce password policy` check box.

- Verify that you can connect to the database with the login that you created:
  - Server type: `Database Engine`
  - Server name: `Local`
  - Authentication: `SQL Server Authentication`

End

1c. Set up the database for PostgreSQL.

Setting up the Genesys Administrator Extension database (for PostgreSQL)

Purpose

- To set up the PostgreSQL database that is used by Genesys Administrator Extension.

> **Important**
>
> - It is recommended to use PostgreSQL version 9.1.x.

If you prefer to use Oracle or Microsoft SQL Server, see Setting up the Genesys Administrator database (for Oracle) or Deploying#t-1 Setting up the Genesys Administrator database (for Microsoft SQL Server).

Start

1. Refer to the PostgreSQL 9.1 documentation to create the PostgreSQL Database for GAX.
2. Start pgAdmin.
3. Select the PostgreSQL 9.1 connection and connect to the PostgreSQL database with the following user name: `postgres`.

   > **Important**
   >
   > If a PostgreSQL 9.1 connection is not available, you can create it by clicking the `Add Server` button.

4. Create a login and password for the GAX database.

   For example: `gax814admin` with the password `password`.

   You can execute queries by clicking the `Query Tool` button. For example:

   ```
   CREATE USER gax WITH PASSWORD 'gax814admin' CREATEDB;
   ```

5. Create the GAX database (for example, gax814) by using the login created in Step 4 to make this login the owner of the database.

   ```
   create database gax814 owner gax;
   ```

6. Connect to the database with the login that you created in Step 4.
7. Perform the following steps if you are setting up a new Configuration Server:
   - You must update the DBMS configuration file `pg_hba.conf` to allow the client to connect to the database.
   - Issue the command `pg_ctl reload` to complete the update of the DBMS configuration file.

> **Important**
>
> - The PostgreSQL driver `LIBPQ.dll` must be installed on the host where Database Server is installed.
> - The `PATH` environment variable must be set to the `bin` directory of PostgreSQL.

End

(Optional) Enable UTF-8 character encoding for Oracle databases.

Enabling UTF-8 character encoding (for Oracle)

To enable UTF-8 character encoding for Oracle databases in Genesys Administrator Extension releases 8.1.3 and higher, you must ensure that:

- Configuration Server 8.1.2 or higher is installed.
- UTF-8 string encoding is enabled on Configuration Server 8.1.2 or higher.

The database character set must be set to `AL32UTF8` to support the use of UTF-8 character encoding. To verify the character set, use the following SQL command:

```
SELECT * FROM NLS_DATABASE_PARAMETERS;
```

In the response, if `NLS_CHARACTERSET` is set to `AL32UTF8`, no additional actions are required. Otherwise, refer to the Oracle support guide for more information about character set migration:

http://docs.oracle.com/cd/B28359_01/server.111/b28298/ch11charsetmig.htm

> **Warning**

Character-set migration is a non-reversible process. Incorrect data conversion can lead to data corruption, so always perform a full backup of the database before attempting to migrate the data to a new character set.

Important

In most cases, a full export and import is recommended to properly convert all data to a new character set.

2. Set up the host upon which Genesys Administrator Extension will run.

Setting up the host for Genesys Administrator Extension server

Purpose: To set up Oracle Java Server JRE (Java Runtime Environment) version 6 or 7. (**Note**: GAX only supports the 64-bit version of Oracle Java HotSpot Server VM.)

Start

1. If Java JRE 6 or 7 is not already installed on the host machine where Genesys Administrator Extension will be installed, install it now as follows:
   a. Download the Oracle Java Runtime Environment Kit (JRE) from the following website:

      http://www.oracle.com/technetwork/java/javase/downloads/index.html

      (Linux) Select the `tar.gz` package.

   b. Refer to the Oracle documentation for more information on how to install the tar.gz package.

   c. (Windows) Double click the Java installer. The contents will be installed in the directory that you specify during the installation.

4. Set the following environment variables for your host, as follows:
   a. (Linux) Insert the following lines into the `/etc/profile` file:

      ```
      export JRE_HOME=/usr/lib/java/jre-<version of Java downloaded>/jre
      ```

      Log out and log in again to activate the new environment variables in the current session.

   b. (Windows) Create a new System Variable named `JRE_HOME` and use the path that was used during installation as the value (for example, `C:\Programs\Java\jre1.6.0_23`). To do this, right-click your Computer icon. Select `Properties > Advanced System Settings > Environment`

`Variables`, and then create the `JRE_HOME` variable.

3. Install Local Control Agent on this host. For detailed instructions, refer to the Framework 8.1 Deployment Guide.

End

3a. Install Genesys Administrator Extension server on a Linux host.

Installing Genesys Administrator Extension server on a Linux host

Prerequisites

- The environment variable for `JRE_HOME` has been configured (see Step 2 of Setting up the host for Genesys Administrator Extension server).

Start

1. Copy the IP to the host machine.
2. Navigate to the folder to which you copied the IP, and change the permissions of the installation file by entering the following command:

```
chmod 755 install.sh
```

3. Run the installation file to extract and copy the necessary files by entering the following command:

```
./install.sh
```

> **Important**
>
> When you install Genesys Administrator Extension, you might receive the following error message that indicates that installation was unsuccessful:
>
> ```
> Unable to find configuration information. Either you have not used
> configuration wizards and the GCTISetup.ini file was not created or the
> file is corrupted.
> ```
>
> Ignore this message; Genesys Administrator Extension was installed successfully.

4. Navigate to the folder in which you installed GAX and run the `gax_startup.sh` file.

Important

- The GAX installer creates a `setenv.sh` file that enables you to adjust the memory settings for GAX. The `setenv.sh` file defines the memory (RAM) settings for GAX to 1024 MB. You can change the memory setting in the `setenv.sh` file to a different value. If you enable TLS encryption, ensure that you make the following updates to the `setenv.sh` file. The `setenv.sh` file contains the following lines:

```
# Uncomment the following lines only if you are going to use TLS. Don't forget to set the
correct path and password.
#export JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=/path_to_jre/jre6/lib/security/
cacerts"
#export JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=secret_password"

# This line defines the memory (RAM) settings for GAX. If you have more RAM available
for GAX, adjust both values accordingly
export JAVA_OPTS="$JAVA_OPTS -Xms1024m -Xmx1024M"

# Uncomment following line to activate psdk.logs, it's recommended to let this option
deactivated
#export JAVA_OPTS=%JAVA_OPTS%
-Dcom.genesyslab.platform.commons.log.loggerFactory=com.genesyslab.platform.commons.log.Log4JLoggerFactoryI
# Enable this option for SSL Debugging
#export JAVA_OPTS=%JAVA_OPTS% -Djavax.net.debug=all
```

  Follow the instructions in the first line by uncommenting the indicated lines below it and setting the path and password.

- You must create a trust store and set the trust store path accordingly. See Transport Layer Security for more information.

End

3b. Install Genesys Administrator Extension server on a Windows Server host.

Installing Genesys Administrator Extension server on a Windows Server host

Prerequisites

- The environment variable for `JRE_HOME` has been configured (see Step 2 of Setting up the host for Genesys Administrator Extension server).

Start

1. Copy the IP to the host machine.

2. Run the `setup.exe` installation file to extract and copy the necessary files.

   If there is an existing installation of GAX on the host, the installer will display a dialog box that prompts you to confirm whether or not you want to maintain the existing installation.

3. Navigate to the folder in which you installed GAX and run the `gax_startup.bat` file.

Important

- The GAX installer creates a `setenv.bat` file that enables you to adjust the memory settings for GAX. The `setenv.bat` file defines the memory (RAM) settings for GAX to 1024 MB. You can change the memory setting in the `setnev.bat` file to a different value. If you enable TLS encryption, ensure that you make the following updates to the `setenv.bat` file. The `setenv.bat` file contains the following lines:

  ```
  REM Uncomment the following lines only if you are going to use TLS. Don't forget to set
  the correct path and password.
  REM set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStore="C:\Program Files\Java\jre6\lib\
  security\cacerts"
  REM set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStorePassword=secret_password
  ```

  Follow the instructions in the first line by uncommenting the indicated lines below it and setting the path and password.

- You must create a trust store and set the trust store path accordingly. See Transport Layer Security for more information.

End

4a. Deploy Genesys Administrator Extension Using Setup Mode (Existing Deployment).

Deploying Genesys Administrator Extension (Existing Deployment)

Start

1. Connect to GAX locally by opening a supported web browser and navigating to the location of your GAX host (for example: `http://localhost:8080/gax/`).

   > **Important**
   > Setup Mode is accessible only through a local connection. You

> cannot use Setup Mode if you connect remotely to the GAX host.

2. Select the Username field and enter root. By default, there is no password.
3. Click Log In.
4. Choose Connect to an Existing Deployment.
5. You must provide configuration information about the existing Management Framework deployment. This screen pre-populates with existing details about the deployment, such as:
   - Primary Configuration Server Host
   - Port number
   - Default Client Application Name
   - Username
   - Password

   If there are any errors, GAX prompts you to re-enter the configuration information.
6. Click Next.
7. Perform one of the following actions:
   - Select the GAX Application object to be associated with the existing instance. The list includes all objects of type CfgApplications with a subtype of either CFGGenesysAdministratorServer or CFGGenesysGenericServer. If the associated Host object has the same host names or IP addresses as the current GAX instance, it is highlighted as recommended.
   - Create a new Application object. You must provide the following information:
     - Administrator Extension Application Object Name—Enter the name of the Application object to create.
     - Template—Select the application template to use.

     If the Host object does not exist, it is automatically created.
8. Click Next.
9. GAX prompts you to enter configuration information for the GAX database. This screen pre-populates with existing details that might be stored in Configuration Server. You must provide the following configuration information:
   - Database Server Type
   - Database Host
   - Port (numeric only)
   - Database Name
   - Username
   - Password
10. Click Next.
11. GAX verifies the database version and creates (or updates) the database access configuration. If an

error occurs, an error message displays and you can either cancel or restart the deployment process.

12. Click Finish.
13. GAX restarts to finish the setup operation. When it is done, GAX displays the login screen and you can login to GAX.

End

4b. Deploy Genesys Administrator Extension using Setup Mode (New Deployment).

Deploying Genesys Administrator Extension (New Deployment)

Prerequisites

- Genesys Deployment Agent (GDA) must be installed on port 5000 on the server that will run Configuration Server and Database Server.
- The installation packages for Configuration Server and Database Server are located in a location accessible to the GAX host machine.

Start

1. Connect to GAX locally by opening a supported web browser and navigating to the location of your GAX host (for example: http://localhost:8080/gax/).

> **Important**
>
> Setup Mode is accessible only through a local connection. You cannot use Setup Mode if you connect remotely to the GAX host.

2. Select the Username field and enter root. By default, there is no password.
3. Click Log In.
4. Choose Install a New Deployment.
5. In the Installation Packages pane, provide the following information:
   - Configuration Server IP Path—Enter the path to the Configuration Server installation package .zip file (Windows) or tar.gz file (Linux). The file must contain the ip and Templates directories.
   - Database Server IP Path—Enter the path to the Database Server installation package .zip file (Windows) or tar.gz file (Linux). The file must contain the ip and Templates directories.
6. Click Next.

7. In the Configuration Server Details section, provide the following information. Some fields are populated by default values.
   - Installation Path on Target Host—The installation path to which Configuration Server will be installed.
   - Primary Configuration Server Host—Enter the name of the Primary Configuration Server host.
   - Port—Enter the port number for the Primary Configuration Server.
   - Target Host OS Type—Select the operating system used by the target host.

   > **Important**
   >
   > Although Management Framework supports various operating systems, GAX can only deploy Configuration Server and Database Server on Windows Server 2003/2008/2012 or Red Hat Enterprise Linux 5.5/6. See Prerequisites for more information on operating systems that are supported by GAX.

   - Management Port—Enter the port number for the Management Port.
8. Click Next.
9. (Optional) Click the Install Backup Configuration Server check box to install a Backup Configuration Server. You must provide the following information:
   - Backup Configuration Server Host—Enter the name of the Backup Configuration Server host.
   - Port—Enter the port number for the Backup Configuration Server.
   - Management Port—Enter the port number for the Backup Management Port.
10. Click Next.
11. In the Database Server Details section, provide the following information. Some fields are populated by default values.
    - Installation Path on Target Host—The installation path to which Database Server will be installed.
    - Port—Enter the port number for the database.
12. Click Next.
13. In the Configuration Server Database section, provide the following information. Some fields are populated by default values.
    - Database Server Type—Select the database type to be used by GAX: Oracle, PostgreSQL, or MS SQL Server.
    - Database Host—Enter the name of the database host.
    - Port—Enter the port number for the database.
    - Database Name—Enter the name of the database.
    - Username—Enter the user name to use when accessing the database.

- Password—Enter the password to use when accessing the database.

> **Important**
>
> GAX uses default values for some deployment parameters. These default values are not presented to the user. If you want to override these default values, you must edit the following file in the \conf directory: asd_hostinfo.properties, asd_silentini_<IP Nick Name>.properties

14. A progress indicator displays while GAX performs the deployment. If an error occurs, an error message displays and you can either cancel or restart the deployment process.
15. Click Next.
16. In the Configuration Server Details section, provide the following information.
    - Administrator Extension Application Object Name—Enter the name of the GAX Application object.
17. Click Next.
18. In the Administrator Extension Database Details section, provide the following information. Some fields are populated by default values.
    - Database Server Type—Select the database type to be used by the GAX database: Oracle, PostgreSQL, or MS SQL Server.
    - Database Host—Enter the name of the GAX database host.
    - Port—Enter the port number for the GAX database.
    - Database Name—Enter the name of the GAX database.
    - Username—Enter the user name to use when accessing the GAX database.
    - Password—Enter the password to use when accessing the GAX database.
19. Click Next.
20. GAX verifies the database version and creates (or updates) the database access configuration. If an error occurs, an error message displays and you can either cancel or restart the deployment process.
21. Click Finish.
22. GAX restarts to finish the setup operation. When it is done, GAX displays the login screen and you can login to GAX.

End

Important

Setup Mode reads SQL script files from IPs and executes them on the target database through a JDBC connection. SQL script files should follow these rules:

1. <Script> ::= {[<Statement>] | [<Delimiter>] | [<Comment>]}

A script consists of a sequence of statements or comments, with or without delimiters in between.

2. <Comment> ::= "/*"{ <any_character>} "*/"|//{ <any_character>}<Line Separator>|"--"{ <any_character>}<EOL>
A single-line comment starts with "//" or "--" and ends with the line.
A multi-line comment starts with "/*" and ends with "*/".

3. < Delimiter > ::= "go"|"/"|";"
An instance of go or / is a strong delimiter which delimits any statements.
An instance of ; is a weak delimiter which delimits all other statements except <CreateProcedure>.

4. <Quotations> ::= '{<any_character>}'|"{<any_character>}"
Quotations can appear inside a statement. Any characters inside quotations are not treated as a statement, delimiter, or comment.

5. <Statement> ::= <CreateProcedure>|<SimpleStatement>
<CreateProcedure>::="CREATE PROCEDURE"|"CREATE OR REPLACE PROCEDURE"{<any_character>|<Quotations>}"go"|"/"|<EOF>
<SimpleStatement>::="INSERT"|"UPDATE"|"DELETE"|"DROP"|"CREATE"|"ALTER"|"COMMIT"|"ROLLBACK"|"MERGE"|"TRUNCATE"{<any_character>|<Quotations>}[<Delimiter>]
A create procedure statement must be specifically delimited by a strong delimiter.
A simple statement can be delimited by a delimiter, a comment, or another statement.

6. All keywords are case insensitive.

Configuring GAX Properties

After GAX starts for the first time, it generates the following files in the installation directory:

- `conf/gax.properties`
- `webapp`
- `logs`
- `jsp`

You can configure GAX by editing the `gax.properties` file. The options specified in the `gax.properties` file are used by GAX before it connects to Configuration Server. To set additional configuration options, see Configuration Options.

> **Tip**
> Click this link to read more general information about Java-based *.properties* files.

The following options can be configured:

Option	Description	Value	Default
`http_port`	Defines the HTTP port	integer	`8080`
`https_port`	Defines the HTTPS port	integer	`8443`
`supported_protocol`	Defines the protocol to use when communicating with the server	`http/https/both`	`http`
`keystore_path`	Specifies the keystore path		
`keystore_password`	Specifies the keystore password	Note: The password is encrypted and must not be modified directly. Instead, refer to Step 4 of Setting up HTTPS for use with Genesys Administrator Extension.	
`root_url`	Specifies the root URL (host:port/rootURL)		`/gax`
`max_idle_time`	Specifies the maximum idle time, in milliseconds, before automatic logout		`1000*60*60`
`port`	Specifies the primary Configuration Server	integer	

Option	Description	Value	Default
	Port		
host	Specifies the primary Configuration Server Host, written as a Fully Qualified Domain Name (FQDN) or IP		
backup_port	Specifies the backup Configuration Server Port	integer	
backup_host	Specifies the backup Configuration Server Host, written as a Fully Qualified Domain Name (FQDN) or IP		
app	Specifies the GAX Application object		
clientApp	Specifies the client Application object. Setting this option will override the setting in Options > General > client_app_name		
accesslog_enabled	Enables HTTP access logging		true
accesslog_filename	File name for the HTTP access log		./logs/http-yyyy_mm_dd.log
accesslog_timezone	Time zone for the HTTP access log		GMT
accesslog_append	After GAX is restarted, specifies whether to append to existing HTTP access log		true
accesslog_extended	Specifies whether to include extended information in the HTTP access log		false
accesslog_retaindays	Specifices number of days to retain the HTTP access log	integer	90

Configuring ADDP Connections

The Advanced Disconnection Detection Protocol (ADDP) is a Genesys proprietary add-on to the TCP/IP stack. It implements a periodic poll when no actual activity occurs over a given connection. If a configurable timeout expires without a response from the opposite process, the connection is considered lost.

Genesys recommends enabling ADDP on the links between any pair of Genesys components. ADDP helps detect a connection failure on both the client and the server side. For most connections, enabling detection on the client side only is sufficient and it reduces network traffic. However, Genesys strongly recommends that you use detection on both sides for all connections between Configuration Server and its clients (including Solution Control Interface), as well as between any two T-Servers.

Refer to the Framework 8.1 Deployment Guide for more information on ADDP.

Using ADDP with GAX

Genesys Administrator Extension supports ADDP connections to the following components:

- Configuration Server (ADDP always enabled)
- Message Server (ADDP enabled optionally through connection parameters)

At startup, GAX initiates a connection to Configuration Server with ADDP enabled using the following default values:

- Local Timeout: `20`
- Remote Timeout: `20`
- Trace: `On`

After establishing the connection, GAX reads the ADDP parameters specified in the connection to Configuration Server, and if configured, the timeouts are reset dynamically based on the configured values (no re-connection is needed).

The ADDP parameters for Message Server are read from Configuration Server before the connection to Message Server is initialized. ADDP is not enabled on the connection to Message Server if configuration values are not defined.

Refer to the Genesys Administrator Extension Help Wiki for more information on configuring ADDP connections.

> **Important**

- The timeout values are adjusted based on the workload experienced by components with ADDP enabled. You can increase the timeout if the components are heavily loaded.
- You must restart GAX when an ADDP connection is severed. Restart GAX to re-establish the connection.

Prerequisites for Genesys Administrator Extension Modules

This section describes prerequisites to be met before installing or using the functional modules of Genesys Administrator Extension. These are in addition to the basic prerequisites listed here, and are specific to the corresponding module.

> **Important**
>
> Unless specified otherwise, all commands that are entered on a command line in this section should be issued as a root user (command prompt of #) or as a regular user (command prompt of $).

Solution Deployment

Before using Solution Deployment to deploy Solutions to local and remote hosts, you must ensure that the following prerequisites are met:

- Hosts are set up and running at the remote locations, and are running Local Control Agent (LCA) and Genesys Deployment Agent (GDA). Use the instructions in Genesys Administrator Extension 8.1 Help.
- The following configuration options are defined on the `Options` tab of the Genesys Administrator Extension server `Application` object in the `asd` section:
  - `silent_ini_path`
  - `local_ip_cache_dir`

  Refer to Configuration Options for more information about these options.

- An appropriate SQL client is installed for solution definitions that include `<os:execSQL>` commands. You can use the following clients for each database type:
  - Oracle—SQL*Plus
  - Microsoft SQL Server—sqlcmd
  - PostgreSQL—psql

Operational Parameter Management

For the deployment of Parameter Groups, ensure that you have write permissions to the `Transactions` folder of the tenant on which the Parameter Group is deployed. You must also have write privileges for the `Voice Platform Profiles` folder to deploy the Voice application and/or write privileges for the `Routing Scripts` folder to deploy Genesys IRD or SCXML routing strategies.

There are no additional prerequisites for using Operational Parameter Management in Genesys Administrator Extension. However, ensure that your Interaction Routing Designer (IRD) routing strategies reference the `Transaction` objects correctly.

Operational Parameter Management works together with routing strategies, SCXML routing strategies, GVP voice applications, and Genesys Business Rules.

> **Important**
>
> Operational Parameter Management does not load strategies on DNs or upload applications to application servers. You must do this manually for all parameterized objects.

Audio Resource Management

To use Audio Resource Management in Genesys Administrator Extension, you must do the following:

- Add the configuration option section and options for Linux or Windows Server.

  Linux:

  [+] Click here to reveal code

  ```
  [arm]
  local_announcement_folder=announcement
  local_music_folder=music
  local_os=RHEL5
  local_path=/opt/gax/arm
  local_sox_path=/usr/bin/sox
  target_announcement_folder=announcement
  target_music_folder=music
  target_os=RHEL5
  target_path=/mnt/arm/target
  delete_from_db_after_processing=false
  ```

  Windows Server:

  [+] Click here to reveal code

  ```
  [arm]
  local_announcement_folder=announcement
  local_music_folder=music
  local_os=Windows
  local_path=C:\GCTI\GAX\arm\local
  local_sox_path=C:\GCTI\GAX\sox\sox.exe
  target_announcement_folder=announcement
  target_music_folder=music
  target_os=Windows
  target_path=C:\GCTI\GAX\arm\target
  delete_from_db_after_processing=false
  ```

  See Configuration Options for a detailed description of the configuration options.

- If you will be converting audio file formats, you must install SoX (Sound Exchange) before doing any conversions. For Linux, Genesys Administrator Extension supports SoX version 12 or higher. For Windows, GAX supports SoX version 14.3.1 or higher.
- Follow the procedure Installing SoX below.
- Set up the target storage for Audio Resource Management by following the procedure Setting up ARM Runtime Web Server below. This procedure sets up an Apache web server on a Red Hat Enterprise Linux host. On this host, it creates a shared directory from which audio files are retrieved by Audio Resource Management, and to which Genesys Administrator Extension writes audio resource files as they are uploaded by users. The shared directory is accessible from the Genesys Administrator Extension host and is referred to as "target storage".

Installing SoX

Purpose

- To install SoX to enable conversion of audio resources to μ-law, a-law, and gsm formats. This procedure can be run at any time before or after Genesys Administrator Extension is installed.

Start

1. Download SoX for your server operating system. For more information, visit: http://sox.sourceforge.net/Main/HomePage.
2. To install SoX on Linux, enter the following command at the # prompt: `yum install sox`

   Or,

   To install SoX on Windows Server, execute the installer application and install `sox.exe` into the following directory:

   `C:\Program Files\SoX\sox.exe`

> **Important**
> The user of the host on which the GAX application is running must be configured to read and execute the sox binary.

End

Setting up ARM Runtime Web Server

Purpose

- To set up the target storage for Audio Resource Management by setting up a shared directory on an Apache web server on a Red Hat Enterprise Linux host, from which audio files are retrieved by Audio Resource Management and to which Genesys Administrator Extension writes audio resource files as they are uploaded by users.

> **Important**
> The ARM Runtime Web Server is sometimes referred to as an ARM HTTP Proxy.

Prerequisites

- Genesys Administrator Extension Host is running.
- A dedicated host machine is available for the ARM Runtime Web Server.

- Media Server is available.

Start

1. Set up your Network File System (NFS) to share data between Genesys Administrator Extension and the ARM Runtime Web Server.
   a. (Linux) On the ARM Runtime Web Server, create the required folders and subfolders by entering the following commands at the # prompt:

      ```
      mkdir /opt/genesys/arm
      ```

      mkdir /opt/genesys/arm/music

      mkdir /opt/genesys/arm/announcements

      > **Important**
      > Ensure that the user of the host on which the GAX application is running is configured to read and write these directories. GAX treats all directories as local. If the target directory and the sub-directories reside physically on a remote host and are used as network directories, or mapped as a local drive, the user must have network access configured.

   b. On the Genesys Administrator Extension host, open the `/etc/exports` in an editor and add the folder `/opt/genesys/arm` as a shared directory. When added, the file should contain the following line:

      ```
      /opt/genesys/arm * (rw,sync)
      ```

      To limit access to only certain machines, change the asterisk (*) to the fully qualified domain name or address of the Genesys Administrator Extension host. If you have multiple Genesys Administrator Extension hosts in your environment, you can create one line per host.

3. On the ARM Runtime Web Server, make sure that NFS and the supporting portmap processes have started by entering the following commands at the # prompt:

   ```
   chkconfig portmap on
   chkconfig nfs on
   ```

   If necessary, you can manually start the processes by entering the following commands at the # prompt:

   ```
   Solution nfs start
   Solution portmap start
   ```

4. Mount the shared drive on the Genesys Administrator Extension host (or hosts) as follows:
   a. On the host, create a new directory by entering the following command at the # prompt:

      ```
      mkdir -p /mnt/arm/target
      ```

   b. Open the file `/etc/fstab` in an editor and add the following line:

      ```
      <address of the ARM Runtime Web Server>/opt/genesys/arm
      /mnt/arm/target nfs rsize=8192,wsize=8192,timeo=14,intr
      ```

   c. Mount the target manually by entering the following command at the # prompt:

      ```
      mount /mnt/arm/target
      ```

The target is mounted automatically when the server restarts.

5. Install Apache Web Server as follows:
   a. Install Apache by entering the following command at the # prompt:

      ```
      yum install httpd
      ```

   b. Make sure that Apache starts when the host starts by entering the following command at the # prompt:

      ```
      chkconfig httpd on
      ```

      Alternately, you can start Apache manually by entering the following command at the # prompt:

      ```
      Solution httpd start
      ```

   c. Start or restart Apache to test that it works.

4. To have Apache serve the media files for the Media Server, open the file `/etc/httpd/conf/httpd.conf` in an editor and make the following changes:

Change This Line ...	... to this Line
`DocumentRoot "/var/www/html"`	`DocumentRoot "/opt/genesys/arm"`
`<Directory "/var/www/html">`	`<Directory "/opt/genesys/arm">`

5. Update your Media Server configuration to use the ARM Runtime Web Server (`address:http://<address of ARM Runtime Web Server>/`) instead of the local file storage.
   - When integrating the Media Server for ARM, the following Media Control Platform configuration options must be modified:
     - To reduce the number of audio files searching attempts and promote efficiency at ARM Runtime Web Server, set `msml/play.usedefaultsearchorder` to `false`.
     - To set the locations at the Services Site so that ARM Runtime Web Server can access announcement and music files, set the following options:

       ```
       msml/play.basepath=http://<ARM Runtime Web Server>
       ```

       ```
       msml/play.musicbasepath=http://<ARM Runtime Web Server>
       ```

   For more information about these options and file naming for Play Treatment requests, refer to the Genesys Media Server 8.1 Deployment Guide.

End

Configuring System Security

GAX has many features that enhance your system security. This section discusses GAX security features and describes how to configure and/or use them.

Default Account Support

Genesys uses a default user account. This is a special account that always has full privileges to all objects and can perform any action. This account ensures that there is always at least one account that enables the administrator to correct permissions and access issues if other administrative accounts are deleted, disabled, or otherwise compromised.

GAX supports the default user account. The default user account always has full access to all the functions that are specified for the GAX role, even if this account does not have any role privileges or explicit permissions specified. When the default account is created during the installation of Configuration Server, it has full control over all configuration objects; however, this account might be deleted or its permissions on objects might be revoked. If this happens, GAX cannot work around the permissions. The default account must have the permissions set to write objects in the Configuration Server.

Use the default_account_dbid option to configure the actual account to be used, and that has all privileges assigned, in case the original default user account is disabled for security reasons or has been deleted.

Transport Layer Security (TLS)

GAX employs Transport Layer Security (TLS), a cryptographic protocol that provides security and data integrity for communications over networks such as the Internet. TLS encrypts the segments of network connections at the transport layer from end to end.

GAX supports TLS-enabled connections to the following Genesys servers:

- Configuration Server
- Solution Control Server
- Message Server
- Genesys Deployment Agent

GAX also supports TLS-enabled connections to the GAX database and the LRM database.

For the GAX database connection (either Oracle, Microsoft SQL Server, or PostgreSQL), the database driver and database must also support TLS. For information about configuring your GAX database, refer to the documentation that is specific to the database that you are using:

- Oracle: Oracle Database Advanced Security Administrator's Guide
- Microsoft SQL Server: Use the documentation that came with your database application.
- PostgreSQL: Use the documentation that came with your database application.

For information about TLS and detailed instructions about configuring secure connections, and creating and managing certificates, refer to the Genesys TLS Configuration chapter of the Genesys 8.0 Security Deployment Guide.

Follow the instructions to create a certificate, assign that certificate to a host object (which is required for Genesys Server to run in TLS mode), and configure the use of a secured port for the GAX application.

Next, import the server certificate to the trust storage for GAX to enable authentication for TLS connections.

By default, trust storage is in the JRE folder at the following location:

```
C:\Program Files\Java\jre6\lib\security\cacerts
```

The default password is "changeit".

Genesys recommends that you create a separate trust store for GAX.

Perform the procedure below to create a trust store and import the certificates.

Creating a keystore and managing the trust store

Purpose

- To create storage that is separate from the default keystores that come with Java.

Genesys recommends that you do not use the default keystores that are shipped with Java. To ensure a clean separation, you should create a separate storage. If you use a standard `cacert` file, you must re-import the certificates after each JVM update.

The trust store should contain only the certificates of servers that GAX should trust. If a server sends GAX its certificate during a TLS Handshake, GAX will search for a matching certificate in this keystore. If the certificate is found, the connection is accepted; otherwise, the connection is rejected.

Prerequisites

- Your Keytool should be configured to your path.
- You have JRE or JDK installed.

Start

1. To create an empty keystore, execute the following command lines on your shell: `keytool -genkey -alias initKey -keystore trusted.keystore -storetype jks keytool -delete -alias initKey -keystore trusted.keystore`
2. Make the `trusted.keystore` file readable for the user that owns the GAX process.
3. Set a strong password on your keystore.
4. Add a certificate to the trust store by executing the following command line: `keytool -import -alias mssql -keystore trusted.keystore -file "cert/demosrc.cer"`

   `Alias` is a name under that the certificate. It can be addressed within the trust store. The option `-keystore` specifies the keystore file and the option `-file` specifies the certificate to be imported.
5. To display the whole content of a keystore, execute the following command line: `keytool -list -keystore trusted.keystore`
6. To display a specific certificate, execute the following command line: `keytool -list -v -alias mssql -keystore trusted.keystore`
7. To delete a certificate from the keystore, execute the following command line: `keytool -delete -alias mssql -keystore trusted.keystore`

End

> **Important**
>
> Most systems have multiple trusted stores. You must always use the same store for GAX.

The following options must be set to configure the trust store location for GAX. The options also enable authentication on a global level for all connections that use a secured port.

The best way to set these options is by using the `setenv.sh` or `setenv.bat` script:

```
set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStore="D:\certificates\trusted.keystore"
set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStorePassword=changeit
```

> **Important**
>
> GAX does not support Client Authentication. GAX will not authenticate itself by sending a certificate to the server.

Secure Socket Layer (SSL) Security

Genesys Administrator Extension supports Secure Socket Layer (SSL) communications between the GAX server and client-side connections using the web browser interface.

GAX can support connections through HTTP or HTTPS simultaneously. This is defined through configuration of the `supported_protocol` parameter in the `gax.properties` file, which can be found in the `conf` directory of your GAX installation.

Setting up HTTPS for use with Genesys Administrator Extension

1. Create a keystore file to store the private key and certificate for the GAX server.

   To create a self-signed certificate, execute the following command:

   ```
   keytool -keystore keystore -alias gax -genkey -keyalg RSA
   ```

   As prompted, enter the information required.

2. Start GAX in HTTP-only mode. In the `gax.properties` file, ensure `supported_protocol=http`. This is set by default.
3. As a local user (whether in person or via a remote desktop connection), log in to GAX as the local user `root`.
4. Call the webservice API by entering the following in the address bar of your web browser (for example: `http://localhost:8080/gax/api/system/setkeystorepassword?password={password}`). The password is stored in an obscured fashion in the `gax.properties` file. The password specified should be the same as the password specified for the keystore (see Step 1, above).
5. Define the parameter `https_port` in `gax.properties` with a port number. The usual default is 443. Please see Configuring GAX Properties for more information.
6. Update the parameter `supported_protocol` in `gax.properties` with either `https` or `both`.
7. Define the parameter `keystore_path` in `gax.properties` with the full path to the location of the keystore file.
8. Restart GAX in HTTPS mode.

TLS: Preparing Genesys Management Framework

To enable GAX to connect securely to Genesys servers, you must configure the Genesys Framework as described in the Genesys 8.0 Security Deployment Guide. Follow the instructions in this guide to create and manage certificates and make them usable within Genesys Framework.

Configuration Server

You must meet the following conditions to create a secure connection to Configuration Server:

1. Create a an `Auto Detect` listening port for your Configuration Server with a certificate configured.
2. Configure the GAX Server to connect when it starts up to the Configuration Server Auto Detect port by setting the GAX Server "-port" property. In the `Start Info` tab of the `GAX_Server Properties` dialog box, enter the following settings:
   - Working Directory: `/path/gax`
   - Command Line: `./startup.sh`
   - Command Line Arguments: `-host <host name> -port <auto detect port number> -app GAX_Server`

Message Server and Solution Control Server

Both Message Server and Solution Control Server are configured the same way.

1. Create a `Secured` port for Message Server and Solution Control Server.
2. Configure the GAX Server to connect to Message Server and Solution Control Server by using the *specific* `Secured` ports that you have created. In the `Properties` dialog box for the server and in the `Connections` tab of the `GAX_Server` dialog box, secured ports are displayed with a key symbol icon.
3. Restart GAX Server to connect over an encrypted session by using the secure ports.

Genesys Deployment Agent

Genesys Deployment Agent (GDA) does not read its configuration from Configuration Server. The TLS for the GDA process is activated by accessing the `security` section of the local `gda.cfg` file and setting the `gda-tls` option to a value of `1`.

The annex tab of the related host might or might not have a `security` section that contains the `gda-`

`tls` option.

The `gda-tls` option is not relevant for the GDA runtime; it is read during the installation of LCA and GDA only. GAX reads the value of the `gda-tls` option to determine in what mode GDA is running, and also to determine whether it should connect using TLS or not; therefore, these values must be kept synchronized. If the system administrator changes one of the values in the local file or in the host annex tab, the other option must also be changed to enable GAX to connect correctly.

Disabling Authentication for Certain Connections

The configuring steps outlined above engage authentication for Configuration Server, Message Server, and Solution Control Server. If GAX uses the secure ports to connect to Message Server and Solution Control Server, both server-side certificates will automatically be validated against the trust storage.

In certain rare cases you might want to disable authentication for one of the connections. To do this, add the following line to the `Advanced` tab of the `Properties` dialog box for the connections:

```
"disableAuthentication=1"
```

Do not use white spaces. To separate this option from other options, use a semi-colon.

To disable TLS authentication for Configuration Server, add the following line to the following files:

- (Linux) `setenv.sh`:

```
JAVA_OPTS="$JAVA_OPTS -Dgax.configserver.validate.cert=off"
```

- (Windows) `setenv.bat`:

```
set JAVA_OPTS=%JAVA_OPTS% -Dgax.configserver.validate.cert=off
```

> **Important**
>
> - Connections to Message Server and Solution Control Server fail if GAX does not find the received certificate in the trust store, or if Message Server and Solution Control Server do not send a certificate.
> - Connections also fail to Configuration Server and databases if they are configured for authentication and the certificate is not in the trust store.

TLS: Configuring the GAX Database

You must configure your Oracle, Microsoft SQL, or PostgreSQL server to use TLS. Refer to the documentation that came with your database for information on how to use TLS security.

Configuring the GAX Database for TLS (Oracle)

Purpose

- To enable TLS support for your GAX Oracle database.

Prerequisites

- Setting up the Genesys Administrator database (for Oracle)

Start

1. Configure Oracle as described in the related database guides, and configure a TCPS listener.
2. Set the level of TLS control on the DAP.
    a. In the GAX section of the DAP, create an option that is named `tls_mode`.
    b. Specify one of the following values for the `tls_mode` option:

- `off`—No TLS will be used.
- `required`—If a server does not support TLS, revoke the connection.
- `authentication`—GAX will validate the server send-certificate with the local trust store.
- `<option not set>`—Same as `off`.

End

Configuring the GAX Database for TLS (Microsoft SQL Server)

Prerequisites

- Setting up the Genesys Administrator database (for Microsoft SQL Server).
- Ensure that you are using the latest JTDS driver (1.2.5 or later).

Start

1. Configure Microsoft SQL Server as described in the related database guides.
2. Set the level of TLS control on the DAP.

a. In the GAX section of the DAP, create an option that is named `tls_mode`.
b. Specify one of the following values for the `tls_mode` option:

- `off`—Do not use TLS.
- `request`—If the server supports TLS, it is used.
- `required`—If the server does not support TLS, the connection is revoked.
- `authentication`—GAX validates the server-send certificate against the local trust store.
- `<option not set>`—Same as `off`.

- Verify that the configured port is identical to the TLS listener port of Microsoft SQL Server
- Due to an incompatibility between newer versions of Java and the Microsoft SQL Server driver, disable CBC Protection to enable GAX to connect to a Microsoft SQL Server database.
  - For Windows, add the following line to the `setenv.bat` file:

```
set JAVA_OPTS=%JAVA_OPTS% -Djsse.enableCBCProtection=false
```

  - For Linux, add the following line to the `setenv.sh` file:

```
JAVA_OPTS="$JAVA_OPTS -Djsse.enableCBCProtection=false"
```

End

Configuring the GAX Database for TLS (PostgreSQL)

Prerequisites

- Setting up the Genesys Administrator database (for PostgreSQL).

Start

1. Configure PostgreSQL as described in the related database guides.
2. Set the level of TLS control on the DAP.
   a. In the GAX section of the DAP, create an option that is named `tls_mode`.
   b. Specify one of the following values for the `tls_mode` option:

- `off`—Do not use TLS.
- `required`—If the server does not support TLS, the connection is revoked.
- `authentication`—GAX validates the server-send certificate with the local trust store.
- `<option not set>`—Same as `off`.

End

Cross-site Scripting and Cookies

You can configure your system to improve the protection of Genesys Administrator Extension against Cross-site Scripting (XSS) attacks by configuring the `HttpOnly` and `Secure` flags on your HTTP server to further enhance the existing GAX security. These flags tell browsers how to handle cookies.

Server-side cookies can be tagged with `HttpOnly` and `Secure` flags to tell the browser how to deal with them. To achieve a maximum level of security, administrators must make this configuration on the Application Server.

Securing Server-side Cookies

HttpOnly

Setting the `HttpOnly` flag on cookies forces the browser to prevent (disallow) scripts from accessing the cookies. This prevents JavaScript that might be introduced through an XSS attack into a browser page to access cookie data and send it to a different person. Stolen cookie data can also be used to hijack a browser session.

Secure Flag

With the Secure flag set, cookies are transmitted only from the browser to the server when the connection is secured by using the HTTPS protocol. This setting is applicable to HTTPS connections only. Therefore, you must configure GAX to use an HTTPS connector, not an HTTP connector.

Setup

Follow these recommendations to configure the `HttpOnly` and `Secure` flags.

HttpOnly

Open and edit the following file: `$CATALINA_HOME/conf/context.xml`

To set the `HttpOnly` flag, add the following attribute:

```
useHttpOnly="true"
```

The main tag should be:

```
<Context useHttpOnly="true">
```

Instead of: `<Context>`

Secure Flag

Open and edit the following file: `$CATALINA_HOME/conf/server.xml`

To set the Secure flag, add the following attribute to the HTTPS connector:

```
secure="true"
```

The flag must not be applied to any non-HTTPS connectors. If you apply the flag to an HTTP connection, it will become unusable for Genesys Administrator Extension.

The following is an example of a valid connector:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="/home/gcti/keystore.key" keystorePass="genesys"
clientAuth="false" sslProtocol="TLS" />
```

Inactivity Timeout

For security purposes, GAX can be configured to lock the application if an administrator has not used the keyboard or mouse for a period that you specify. All user input is blocked until the administrator provides login information to unlock the application. This feature ensures that no unauthorized user can access an unattended terminal that is running GAX.

Use the `inactivity_timeout` option to specify the amount of time in minutes of administrator inactivity (no mouse or keyboard usage) that triggers application locking. If the administrator has been inactive longer than the number of minutes that are specified by the `inactivity_timeout` option, the administrator must re-authenticate to be able to use the GAX application. A value of `0` disables this functionality.

GAX employs a keep-alive strategy to prevent *session* timeout; this ensures that GAX maintains your session even if the inactivity timeout feature locks the application and requires you to log in.

Configuring the Auditing Feature

To enable the Auditing feature, you must configure GAX, Message Server, and the database. GAX must have a connection to Message Server.

GAX Application

Enable Auditing by setting the value of the `auditing` option in the `general` section of the GAX Server application to `true`.

Next, in the `general` section of the GAX application, make the following configuration option settings:

- Set the number of switch-over attempts before GAX tries to switch-over to the redundant node to 1. To do this, set the value of the `max_switchovers` option in the `general` section of the GAX application to `1`. A value of `0` means switch-overs are disabled. Negative values allow an unlimited numbers of switch-overs, and, therefore, a continuous reconnect process if the server is unreachable. Setting a negative value is recommended for production systems.
- Set the number of connection attempts before GAX tries to switch over to the redundant node. To do this, set the value of the `attempts` option in the `general` section of the GAX application to `1`.
- Set the timeout interval between connection attempts to Message Server. To do this, set the value of the `warmstandby_timeout` option in the `general` section of the GAX application to any positive integer.
- Set the protocol timeout, which is the time in seconds after which GAX gives up attempting to connect. To do this, set the value of the `timeout` option in the `general` section of the GAX application to `30`.

Message Server

In the Message Server object, set the `db_storage` option in the `messages` section to the value `true`.

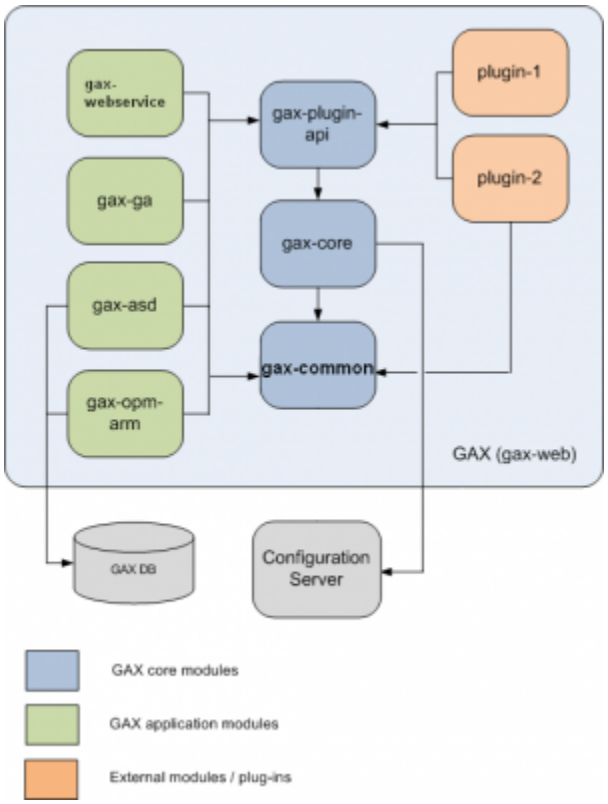
If the `db_storage` option is not set to `true`, Message Server does not save the Audit data to its database.

Database Configuration

To read the Audit data from the Log DB, a DAP must be configured and connected to the GAX Server `Application` object. Configure the DAP in the same way that DAPs were configured for the GAX database and License Usage Reporting. To identify the DAP role, set the value of the `role` option in the `GAX` section of the DAP to `auditing`.

Plug-ins

Genesys Administrator Extension is deployed as a set of plug-ins into the GAX Core. This enables you to deploy only the functionality that you require, or to restrict the availability of certain functionality to users.



GAX is based on a hierarchical dependency system. The `gax-core` plug-in depends on the `gax-common` plug-in. The `gax-plugin-api` plug-in depends on the `gax-core` and `gax-common` plug-ins. All other GAX plug-ins depend on the `gax-plugin-api` and `gax-common` plug-ins.

The `gax-common` plug-in contains classes, such as error codes, exceptions, static utility classes, and interfaces, that are shared by both the `gax-core` and `gax-plugin-api` plug-ins. Most auditing related interfaces and objects are contained in the `gax-common` plug-in.

The `gax-core` plug-in manages all system-wide resources; therefore, all connections, threads, and stateful classes are contained in the `gax-core` plug-in.

The `gax-plugin-api` plug-in contains GAX functionalities that are used by other plug-ins. This plug-in contains generic configuration APIs, the base class of web access controller (BaseController), and other utility classes.

The `gax-webservice` plug-in contains all core web service interfaces that might be used in GAX.

Important

If a plug-in contains configuration options, you must have write permissions on the GAX `Application` object for `SYSTEM`.

Managing Plug-ins

The Plug-in Management screen displays all installed plug-ins in your GAX environment. To access the screen, navigate to Configuration > Administrator > Plug-in Management.

You can click on the name of a plug-in to view details about the plug-in, such as which server hosts the plug-in. Click Plug-ins to display more information, which displays in a new panel to the right:

- Name—The name of the plug-in
- Version—The version number of the plug-in.
- Language—The language used by the interface of the plug-in
- Provider—The name of the user or company that provided the plug-in
- State—This field can be set to Enabled or Disabled, depending on the status of the plug-in. See Enabling or disabling a plug-in in GAX for more information.

The following actions can be performed in the Plug-in Management area:

- Plug-ins can be installed.
  - If your GAX instance uses Jetty, see Installing Plug-ins with the Software Installation Wizard.
  - If your GAX instance uses Tomcat, or the plug-in is designed for GAX 8.1.3 or earlier, see Installing Legacy Plug-ins.
- Language packs can be installed. See Installing Language Packs for more information.
- Plug-in options can be modified. See Modifying plug-in settings for more information.
- Plug-ins can be enabled or disabled. See Enabling or disabling a plug-in in GAX for more information.
- Plug-ins can be removed. See Removing a plug-in from GAX for more information.

Installing Plug-ins with the Software Installation Wizard

Important

- The plug-in install profile automatically fetches GAX Application objects for selected Host objects.
- Plug-in options are merged into the affected GAX Application objects. See the Genesys Administrator Extension Help Wiki for detailed information.

Purpose

- To install plug-ins that are designed for GAX 8.1.4 instances that use Jetty.

Prerequisites

- GAX is installed and deployed, as described in Deploying Genesys Administrator Extension.
- GAX has been started at least once.
- GDA is installed and running on the target machine.

Start

1. In the header, go to `Configuration > Solution Deployment > Installation Packages`.
2. In the `Installation Packages` panel, click `New`. A new panel called `Software Installation Wizard` opens to the right.
3. In the `Software Installation Wizard` panel, select a method for importing the plug-in:

> **Important**
>
> If your installation package contains two or more templates, you must use the **Installation Package Upload (includes templates)** procedure.

-

- `Installation Package Upload (includes templates)`—Upload a ZIP file that contains an installation package and its associated templates. These files are typically provided by Genesys Technical Support.

i. In the `Software Installation Wizard` panel, select `Installation Package Upload (includes templates)` and click `Next`.

ii. The panel updates. Click `Choose File` to select the file to upload.

iii. Click `Finish`.

-

- `Installation Package Upload (template uploaded separately)`—Upload an installation package and its associated template.

i. In the `Software Installation Wizard` panel, select `Installation Package Upload (template uploaded separately)` and click `Next`.

ii. The panel updates and displays three boxes—`Upload a package`, `Upload an XML template`, and `Upload an APD template`. Click `Choose File` in each field to select the file to upload.

- `Upload a package`—A ZIP file that contains the installation package.
- `Upload an XML template`—The XML template file for this installation package. This is the template that is referenced by the installation package description file. This file must not be modified from the version in the template directory.
- `Upload an APD template`—The APD template file for this installation package. This is the template that is referenced by the installation package description file. This file must not be modified from the

version in the template directory.

- Click Finish.
  - UNC Path to Mounted CD or Directory—Upload an installation package that is stored on a mounted CD or network directory.

    i. In the Software Installation Wizard panel, select UNC Path to Mounted CD or Directory and click Next.

    ii. In the text field, enter the path for where the installation package is stored.

    iii. Click Next to open the path.

    iv. The panel updates to display the installation package(s) that is found at the specified location. Click the check box(es) that is beside the installation package(s) to upload.

    v. Click Finish.
  - UNC Path to an Existing Administrator Repository—Upload an installation package from an existing Genesys Administrator repository.

    i. In the Software Installation Wizard panel, select UNC Path to an Existing Administrator Repository and click Next.

    ii. In the text field, enter the path for the existing Genesys Administrator repository.

    iii. Click Next to open the path.

    iv. The panel updates to display the installation package(s) that is found at the specified location. Click the check box(es) that is beside the installation package(s) to upload.

    v. Click Finish.
  - UNC Path to Zipped IPs through Support—Upload a .zip file provided by Genesys Customer Care that is stored on a mounted CD or network directory. This file contains an installation package and its associated templates.

    i. In the Software Installation Wizard panel, select UNC Path to Zipped IPs through Support and click Next.

    ii. In the text field, enter the path for where the IP is stored.

    iii. Click Next to open the path.

    iv. The panel updates to display the installation package(s) that is found at the specified location. Click the check box(es) that is beside the installation package(s) to upload.

    v. Click Finish.

> **Important**
>
> When you upload a plug-in, GAX uses the template file (.tpl) to create an Application Template and extracts the default options for the plug-in. GAX stores these options in

the database and merges them with the core GAX Application object upon deployment. During this merge, only new options are added—existing key value pairs are not overridden.

- The file(s) upload from your file system to Genesys Administrator Extension and a progress bar displays to show the upload progress. The progress of the upload also displays in the Status column in the `Installation Packages` panel.

Important

- A green progress bar represents a successful upload for the installation package. A red progress bar represents a failed upload for the installation package. You can review which step failed in the `Status` field in the `Installation Packages` list.
- You cannot upload a plug-in to the repository if a version of the plug-in already exists in the repository. You must have the `Replace IPs and SPDs` privilege enabled to overwrite a plug-in in the repository.

End

Installing Legacy Plug-ins

Purpose

- To install plug-ins that are designed for GAX 8.1.3 releases or earlier, or to install plug-ins for GAX instances that use Tomcat.

Prerequisites

- The `CATALINA_HOME` variable exists.
- The path `<CATALINA_HOME>/webapps/gax/WEB-INF/lib/` exists.
- GDA is installed and running on the target machine.

Start

1. Install the plug-in as indicated in the procedure Installing Plug-ins with the Software Installation Wizard.
2. The installation process copies .jar files to the following folder: `<CATALINA_HOME>/webapps/gax/WEB-INF/lib/`.
3. (Optional) If you are using GAX with Jetty, you must copy the plug-in's .jar files to `<GAX_FOLDER>/webapp/WEB-INF/lib`.

4. Restart GAX.

End

Installing Language Packs

Start

1. Copy the Language Pack IP to the host machine.
2. Run the `setup.exe` (Windows) or `install.sh` (Linux) installation file. The installation process copies the language pack .jar file to one of the following folders on the host machine:
   - Windows: The GAX folder.
   - Linux:
     - If the variable <CATALINA_HOME> is defined—The installer copies the file to the following folder: <CATALINA_HOME>/webapps/gax/WEB-INF/lib/.
     - If the variable <CATALINA_HOME> is not defined—The installer requests the location of the Tomcat folder and copies the file to the following folder: <TOMCAT FOLDER>/webapps/gax/WEB-INF/lib/.

> **Important**
> The target folder must exist for the installation process to succeed.

3. Stop GAX (if it is running).
4. Copy the language pack .jar file to the following directory: <GAX FOLDER>/webapp/WEB-INF/lib/.
5. Restart GAX.

End

See the Genesys Administrator Extension Help for more information on how to select an installed Language Pack to use with GAX.

Modifying plug-in settings

Purpose

- To provide a consolidated system settings interface for accessing and managing all system settings in GAX. System settings are managed by node.

Start

1. In the header, go to `Configuration > Administrator > Plug-in Management`.

2. Select an application in the Administrator Applications list. A new panel opens to the right.
3. Click Plug-ins to view which plug-ins are associated with the application. A new panel opens to the right.
4. Select a plug-in in the Plug-in Info list. A new panel opens to the right.
5. Click Plug-in Options. A new panel opens to the right. The panel displays the options that are associated with the plug-in.
6. Click an option to view more information about the option in a separate panel that opens to the right.
7. When you have finished modifying the option(s), perform one of the following actions:

- Click Save to save your changes.
- Click Cancel to discard your changes.

End

Enabling or disabling a plug-in in GAX

> ### Important
>
> - It is not possible to disable the gax-core plug-in.
> - The option to enable or disable a plug-in is available only for the application or node to which the user is currently connected. Other GAX applications or nodes will provide a link to manually log in to that instance.

Start

1. In the header, go to Configuration > Administrator > Plug-in Management.
2. Select an item in the Administrator Applications list. More information about the item displays in a new panel to the right.
3. Click Plug-ins. More information about the plug-ins for the item display in a panel to the right.
4. Select a plug-in from the list.
5. Do one of the following:

- If the plug-in is currently enabled, the Disable button is displayed. Click Disable to disable the plug-in.
- If the plug-in is currently disabled, the Enable button is displayed. Click Enable to enable the plug-in.

End

> **Important**
> To see the changes to the plug-in, refresh the display in your browser.

Removing a plug-in from GAX

Start

1. Stop GAX.
2. Go to `$GAX_HOME/webapps/gax/WEB-INF/lib` on the file system (where `$GAX_HOME` is your home folder for the GAX application).
3. Delete the .jar files for the plug-ins that you wish to disable. For example, to remove the `Solution Deployment` plug-in, delete `gax-asd.jar`.
4. Start GAX.

End

Upgrading GAX

This section describes how to upgrade from previous versions of GAX to the current version.

> **Important**
>
> Genesys Administrator Extension uses an embedded instance of Jetty for web-server functions, whereas previous releases have used Tomcat. The following upgrade procedures explain how to upgrade GAX to use Jetty. To continue using Tomcat, you must remove the old `<Tomcat Home>/webapps/gax` folder and copy the new `gax.war` file from the GAX installation folder to the `<Tomcat Home>/webapps` folder.

Upgrading from 8.1.x to 8.1.4

This section contains two procedures. Use the one that applies to your system:

- Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.1 or higher.
- Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.0 or lower

The following are the generalized steps to upgrade GAX 8.1.x to GAX 8.1.4:

1. Stop GAX.
2. Install the GAX IP. See Deploying Genesys Administrator Extension for more information.
3. Execute all applicable database upgrade scripts, if necessary.
4. Run Setup Mode. See Deploying Genesys Administrator Extension (Existing Deployment) for more information.
5. Re-install plug-ins that were previously used with GAX 8.1.3. These plug-ins will not function unless they are re-installed after you upgrade to GAX 8.1.4. To re-install these plug-ins:
   i. Use GAX to upload and re-install the plug-in. Refer to Managing Plug-ins for more information.
   ii. Copy the plug-in's `.jar` file from the GAX 8.1.3 folder to the GAX 8.1.4 folder.
6. Restart GAX.

> **Important**
>
> - You must upload the plug-in installation package into GAX if the plug-in contains new privileges.

- If you are migrating from Tomcat to Jetty, you might need to update the paths used in the asd configuration options if they refer to the {CATALINA_HOME} variable that was previously used by Tomcat.

Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.1 or higher

> **Important**
>
> Genesys Administrator Extension uses an embedded instance of Jetty for web-server functions, whereas previous releases have used Tomcat. The following upgrade procedure explains how to upgrade GAX to use Jetty. To continue using Tomcat, you must remove the old <Tomcat Home>/webapps/gax folder and copy the new gax.war file from the GAX installation folder to the <Tomcat Home>/webapps folder. Start GAX by using the same command-line command that was used for GAX 8.1.3.

Purpose

- To upgrade from an earlier release of GAX to the latest release for Management Framework 8.1.1 or higher.

Start

1. Stop the instance of GAX that you want to upgrade.
2. Ensure that Management Framework, Configuration Server, and Genesys Administrator are all upgraded to versions that are compatible with the latest version of GAX before proceeding (refer to Prerequisites for Genesys Administrator Extension Modules).
3. This step applies only to instances that use GAX Application object of type Genesys Generic Server.

   Create and configure the configuration objects that are required for the latest version of GAX by using Genesys Administrator to perform the following steps:

   a. Open your existing GAX Application object of type Genesys Generic Server in edit mode.

   b. Click the Options tab.

   c. Click Export to save your configured GAX options to a file on your local file system of type CONF/CFG.

   d. Create and configure a new Server Application object for Genesys Administrator Extension of type Genesys Administrator Server by following Step 4 of Creating the necessary configuration objects for Genesys Administrator Extension.

      i. Ensure that you follow the steps that pertain to the use of Management Framework Configuration Server 8.1.1, or higher.

      ii. Replicate any configuration that you wish to add to your newly created Application object by referring to the GAX Application object of your previous version.

iii. Click the Options tab.

iv. Click Import and specify the CONF/CFG file that you previously created. Select No to not overwrite any existing options.

v. (Optional) Create a DAP that points to the Log Database (refer to Step 3 of Creating the necessary configuration objects for Genesys Administrator Extension. Set the role of the DAP to auditing. Enable auditing by setting the value of the general/auditing option to true. Add the DAP to your GAX connections. On the Options tab of the DAP, in the GAX section, configure the role option with the value auditing.

5. On the target machine, run the GAX installer for the release to which you want to upgrade. The installer copies the binary file and all of the required files to the target directory.
6. Remove or deactivate all old GAX objects. You can use only one GAX Application object to point to one physical GAX instance. If you want more than one GAX Application object to point to a single machine, you must install separate physical GAX instances on the same machine.
7. Execute all applicable database upgrade scripts, if necessary. To determine if you have to apply any database scripts, check the resources/sql_scripts folder in the target directory of the installation.

> **Important**
>
> GAX database schema version numbers are not necessarily synchronized with the version numbers of plug-ins, nor will they necessarily match the GAX release number. For example, your version of GAX might be 8.1.310.36 and your database schema version might be 8.1.301.01.

Perform one of the following steps, depending on your database configuration:

- (Oracle only) Run all of the database upgrade scripts from the previous version. To determine if you have to apply any database scripts, check the resources/sql_scripts folder in the target directory of the installation.

  For example, if you intend to upgrade to the latest database version, you must execute the following SQL scripts:

  - gax_core_upgrade_db_8.1.201.15_to_8.1.301.01_ora.sql
  - (For Solution Deployment only) gax_asd_upgrade_db_8.1.301.01_to_8.1.401.01_ora.sql
  - (For Operational Parameter Management only) gax_opm_upgrade_db_8.1.201.15_to_8.1.301.01_ora.sql

- (Microsoft SQL only) Run all of the database upgrade scripts from the previous version. To determine if you have to apply any database scripts, check the resources/sql_scripts folder in the target directory of the installation.

  For example, if you intend to upgrade to the latest database version, you must execute the following SQL scripts:

  - gax_core_upgrade_db_8.1.201.15_to_8.1.301.01_mssql.sql
  - (For Solution Deployment only) gax_asd_upgrade_db_8.1.301.01_to_8.1.401.01_mssql.sql
  - (For Operational Parameter Management only) gax_opm_upgrade_db_8.1.201.15_to_8.1.301.01_mssql.sql

- (PostgreSQL only) Run all of the database upgrade scripts from the previous version. To determine if you have to apply any database scripts, check the resources/sql_scripts folder in the target directory of

the installation.

For example, if you intend to upgrade to the latest database version, you must execute the following SQL script:

- `gax_asd_upgrade_db_8.1.301.01_to_8.1.401.01_postgres.sql`

- As a local user on the host machine, whether in person or via a remote desktop connection, launch GAX and run Setup Mode. Follow the instructions in the procedure Deploying Genesys Administrator Extension (Configuration Server Present).
- (Optional) You can delete the previous GAX `Application` object after you have verified that the new release is working correctly.
- Re-install plug-ins that were previously used with GAX. These plug-ins will not function unless they are re-installed after you upgrade to GAX 8.1.4. To re-install these plug-ins:

  i. Use GAX to upload and re-install the plug-in. Refer to Managing Plug-ins for more information.

  ii. Copy the plug-in's `.jar` file from the GAX 8.1.3 folder to the GAX 8.1.4 folder.

Important

- You must upload the plug-in installation package into GAX if the plug-in contains new privileges.
- If you are migrating from Tomcat to Jetty, you might need to update the paths used in the `asd` configuration options if they refer to the `{CATALINA_HOME}` variable that was previously used by Tomcat.

End

Important

- Files that have version numbers prior to the ones from which you upgraded do not have to be executed.
- You must log in to the database schema as a GAX user and run the commands inside the SQL scripts as commands for the database.
- If you are installing GAX for the first time or upgrading from release 8.1.x to 8.1.4, when you execute the SQL upgrade scripts, make sure that the scripts are properly committed. If your client application has auto-commit switched off, you might have to add the following line(s) to the scripts.
  - For Oracle: `commit;`
  - For MS SQL: `BEGIN TRANSACTION;COMMIT TRANSACTION;`
  - For PostgreSQL: `commit;`
- If you perform the upgrade and GAX does not function properly, delete the webapp folder in the GAX directory of the host machine.

Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.0 or lower

> **Important**
>
> Genesys Administrator Extension uses an embedded instance of Jetty for web-server functions, whereas previous releases have used Tomcat. The following upgrade procedure explains how to upgrade GAX to use Jetty. To continue using Tomcat, you must remove the old `<Tomcat Home>/webapps/gax` folder and copy the new `gax.war` file from the GAX installation folder to the `<Tomcat Home>/webapps` folder. Start GAX by using the same command-line command that was used for GAX 8.1.3.

Purpose

- To upgrade from an earlier release of GAX to the latest release of GAX for Management Framework 8.1.0 or lower.

Start

1. Stop the instance of GAX that you intend to upgrade.
2. On the target machine, run the GAX installer for the release to which you want to upgrade. The installer copies the binary file to the target directory that was defined during installation, and also copies all of the required files to the target directory.
3. Execute all of the applicable database upgrade scripts, if necessary. To determine if you have to apply any database scripts, check the `resources/sql_scripts` folder in the target directory of the installation.

> **Important**
>
> GAX database schema version numbers are not necessarily synchronized with the version numbers of plug-ins, nor will they necessarily match the GAX release number. For example, your version of GAX might be 8.1.310.36 and your database schema version might be 8.1.301.01.

Perform one of the following steps, depending on your database configuration:

- (Oracle only) Run all of the database upgrade scripts from the previous version. To determine if you have to apply any database scripts, check the `resources/sql_scripts` folder in the target directory of the installation.

For example, if you intend to upgrade to the latest database version, you must execute the following SQL scripts:

- `gax_core_upgrade_db_8.1.201.15_to_8.1.301.01_ora.sql`
- (For Solution Deployment only) `gax_asd_upgrade_db_8.1.301.01_to_8.1.401.01_ora.sql`
- (For Operational Parameter Management only) `gax_opm_upgrade_db_8.1.201.15_to_8.1.301.01_ora.sql`

- (Microsoft SQL only) Run all of the database upgrade scripts from the previous version. To determine if you have to apply any database scripts, check the `resources/sql_scripts` folder in the target directory of the installation.

  For example, if you intend to upgrade to the latest database version, you must execute the following SQL scripts:

  - `gax_core_upgrade_db_8.1.201.15_to_8.1.301.01_mssql.sql`
  - (For Solution Deployment only) `gax_asd_upgrade_db_8.1.301.01_to_8.1.401.01_mssql.sql`
  - (For Operational Parameter Management only) `gax_opm_upgrade_db_8.1.201.15_to_8.1.301.01_mssql.sql`

- (PostgreSQL only) Run all of the database upgrade scripts from the previous version. To determine if you have to apply any database scripts, check the `resources/sql_scripts` folder in the target directory of the installation.

  For example, if you intend to upgrade to the latest database version, you must execute the following SQL script:

  - `gax_asd_upgrade_db_8.1.301.01_to_8.1.401.01_postgres.sql`

- As a local user on the host machine, whether in person or via a remote desktop connection, launch GAX and run Setup Mode. Follow the instructions in the procedure Deploying Genesys Administrator Extension (Configuration Server Present).
- (Optional) You can delete the previous GAX `Application` object after you have verified that the new release is working correctly; however, you can choose to maintain both versions simultaneously.
- Re-install plug-ins that were previously used with GAX. These plug-ins will not function unless they are re-installed after you upgrade to GAX 8.1.4. To re-install these plug-ins:

  i. Use GAX to upload and re-install the plug-in. Refer to Managing Plug-ins for more information.

  ii. Copy the plug-in's `.jar` file from the GAX 8.1.3 folder to the GAX 8.1.4 folder.

> ### Important
>
> - You must upload the plug-in installation package into GAX if the plug-in contains new privileges.
> - If you are migrating from Tomcat to Jetty, you might need to update the paths used in the `asd` configuration options if they refer to the `{CATALINA_HOME}` variable that was previously used by Tomcat.

End

Important

- Role privileges must be renewed if the application type is changed. Genesys stores role privileges that are associated with the application type to which they apply, but since GAX is associated with `Genesys Administrator Server` in 8.1.1 releases of Management Framework (for GAX 8.1.2 and higher), not `Genesys Generic Server`, the role privileges must be set using the correct type.
- Files that have version numbers prior to the ones from which you upgraded do not have to be executed. You must log in to the database schema as a GAX user and run the commands inside the SQL scripts as commands for the database.
- If you are installing GAX for the first time or upgrading from release 8.1.x to 8.1.4, when you execute the SQL upgrade scripts, make sure that the scripts are properly committed. If your client application has auto-commit switched off, you might have to add the following line(s) to the scripts:
  - For Oracle: `commit;`
  - For MS SQL: `BEGIN TRANSACTION;COMMIT TRANSACTION;`
  - For PostgreSQL: `commit;`
- If you perform the upgrade and GAX does not function properly, delete the webapp folder in the GAX directory of the host machine.

Customizing the GAX Homepage

When Genesys Administrator Extension is launched, it opens to the default homepage view. The default view is a placeholder that you can customize to suit your business needs.

The homepage is an HTML document (`home.html`) and a style sheet (`home.css`) that are stored in the following location after you install GAX: `<gax-installation-dir>\webapp\plugins\gax-core\home\`

The file `home.html` is a document fragment. It does not contain all of the standard HTML tags. The default, temporary content is the following:

```
<div class="home-container">
    <h1>Welcome to ${GENESYS_ADMINISTRATOR_EXTENSION}</h1>
    <p>This is a placholder page for the Home module. You can customize it by editing
home.html and home.css.</p>
</div>
```

You can change the contents of this page to suit your requirements.

The style sheet file can also be modified to suit your requirements. The default contents are as follows:

```
.home-container {
    padding: 16px;
    height: 400px;
    background-image: url(i/background.jpg);
    background-repeat: no-repeat;
}Genesys recommends that you use a class prefix like "<tt>home-</tt>" to prevent clashes with
class names that are used elsewhere within GAX.
```

The images that are referenced by the CSS file are in the folder that is named "`i`" in the same folder as `home.css`. You can store as many image files as you require in this folder. Reference your images in the CSS file.

After you edit the `home.html` file, click `Refresh` in the GAX interface to display your updates.

Cleaning the GAX Database After a Tenant is Deleted

If a tenant has been deleted from your environment, some data from that tenant might not be removed from the GAX database.

For more information on how to clean the GAX database after a tenant is deleted, please contact Genesys Technical Support.

Accessing Genesys Administrator Extension

This chapter describes how to log in to, and out of, Genesys Administrator Extension. It also explains how to set User Preferences and System Preferences.

This chapter contains the following sections:

Logging In

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

> **Important**
>
> Genesys Administrator Extension supports the use of blank passwords only if Configuration Server is configured to allow blank passwords. Refer to the Genesys 8.0 Security Deployment Guide for information about using blank passwords.

Logging in to Genesys Administrator Extension

Prerequisites

- Configuration DB Server and Configuration Server are installed and running.
- An instance of a Genesys Administrator Extension `Application` object is connected to Configuration Server and running.
- Your browser and its windows are set to a resolution of 1024x768 or greater. If you are working in 1024x768, maximize the browser.
- The user logging in must have Read permission to their own `User` object and Read and Execute permissions on the Genesys Administrator Extension client object. Refer to the Genesys 8.0 Security Deployment Guide for information about permissions. Genesys Administrator Extension respects read-write permissions that are set for Environments and Tenants. You can only access those objects that you have permission to see.

Start

1. Start GAX by using Genesys Administrator.
2. Navigate to the `Application` object for the GAX instance that you intend to start/log in to.
3. Start the application by using the `Start` button in the icon bar.
4. Open a web browser.
5. Enter the following URL in the address bar of the browser:

   ```
   http://<Host name>:8080/gax/
   ```

   where <Host name> is the name of the computer on which you installed Genesys Administrator Extension. The port number is the port that was defined when setting up GAX in Deploying Genesys Administrator Extension.
6. Log in to Genesys Administrator Extension with your assigned user name and password, and click `Log in`.

> **Important**
> Each instance of Genesys Administrator Extension is associated with a single instance of Management Framework; Configuration Server and Port selection is not required during login, nor is it possible to select it.

If you get a permissions error, refer to Required Permissions for instructions.

Your login name and the tenant to which you are logged in is displayed in the top Header Bar of the Genesys Administrator Extension window. The time of your last login is displayed in the Preferences menu. See Preferences for more information.

> **Important**
> The date and time of the local machine and the Management Framework machine must be synchronized for the last login time to be accurate.

7. Your account might be configured to set a new password the first time that you log in, or after a system administrator has reset your password. The `Change Password` dialog box is displayed:
   a. Enter a new password in the `New Password` field.
   b. Enter the same password in the `Confirm Password` field.
   c. Click OK.

> **Important**
> Please see the Genesys 8.0 Security Deployment Guide for more information about resetting passwords.

End

Logging In Remotely

Genesys Administrator Extension supports remote logins for users who might access GAX through a customized login page that is located on another website (for example, a corporate portal page).

In this scenario, the company network can pass the user's credentials to GAX, and GAX automatically logs in the user via a background process so that the user bypasses the login screen.

In addition, a logout URL can be set so the user returns to the company portal page after logging out of GAX.

To use this feature, the customized login page must submit a form to the GAX login page. The following is an example:

```
<form name="logon" action="" method="post" onsubmit = "logonGax()">
<p>UserID:<input type="text" name="username"></p>
<p>Password:<input type="password" name="password"></p>
<input type="hidden" name="newPassword" value="">
<input type="hidden" name="newPasswordConfirm" value=""></p>
<input type="hidden" name="login_success_url" value="">
<input type="hidden" name="logout_url" value="">
<p><input type="submit" value="Login"></p>
</form>
```

The following values can be set:

- The `login_success_url` value can be set to the URL for the GAX login page. If this value is not set, the page is redirected to itself and the URL is appended with `#success`.
- The `login_failure_url` value can be set to a URL to which the user will be directed if the supplied credentials are invalid. If this value is not set, the page is redirected to itself and the URL is appended with `#failure`.
- The `logout_url` value can be set to a URL to which the user will be directed after logging out of GAX. If this value is not set, the user is redirected to the initial credential screen and the URL is appended with `#logout`.

Logging In to Genesys Administrator from GAX

You can access Genesys Administrator from GAX by using the gax-ga plug-in that is part of the core plug-ins that are installed when you install GAX. Your role, and the credentials that you use to log in to GAX, must enable you to access Genesys Administrator.

Login to Genesys Administrator occurs during your login to GAX (refer to Procedure: Logging in to Genesys Administrator Extension). When you enter your GAX login credentials and click Log in, the following process is started:

1. The Log In button becomes disabled.
2. A progress indicator is displayed.
3. The credentials and role that enable you to log in to GAX and Genesys Administrator are verified by GAX.
4. The GAX interface is displayed.
5. If you are permitted to use Genesys Administrator, a menu that enables you to link to Genesys Administrator is displayed.
6. If you click the Genesys Administrator menu, you can select one of the following views in Genesys Administrator:
   - MONITORING > Environment > Dashboard
   - PROVISIONING > Environment > Applications > New Application
   - DEPLOYMENT > Repository > Installation Packages
   - OPERATIONS > Outbound Contact > Dialing Sessions

   Genesys Administrator is launched in a new browser tab or window. The content that is displayed depends on your privileges and access.
7. If you log out of Genesys Administrator, you can continue to use GAX. If you log out of GAX, you are also logged out of Genesys Administrator.

Corporate Login to Genesys Administrator and GAX

Your account might be configured to log in to GAX from a corporate page instead of directly through the GAX login page. If the gax-ga plug-in is installed in your environment, and you are provisioned to log in to both Genesys Administrator and GAX with the same credentials, when you log in by using a corporate interface, GAX is launched and the Genesys Administrator menu is displayed in the GAX interface.

Logging Out

To log out of Genesys Administrator Extension, click the Log Out button in the Header Bar.

Preferences

Genesys Administrator Extension enables you to customize the interface to suit your personal preferences. These preferences take effect each time that you, or anyone using your login credentials, logs in to Genesys Administrator Extension from any browser.

To open the Preferences menu, click `Preferences` (the gear icon) in the top header of the main Genesys Administrator Extension screen. If configured, the menu displays the last time that this user account was logged into Genesys Administrator Extension.

> **Important**
>
> To use the last login time feature, you must ensure:
>
> - The date and time of the local computer and the Management Framework computer are synchronized for the last login time to be accurate.
> - The following lines are included in the Configuration Server `confserv.cfg` file (located in the installation directory of the machine that hosts Configuration Server):
>   - `last-login = true`
>   - `last-login-synchronization = true`

The Preferences menu contains four options:

- User Preferences
- System Preferences
- About—Click this option to view information about your installation. If your user account has the Read `All` privilege, you can also view information about the Configuration Server to which you are connected.
- Genesys Administrator

> **Important**
>
> Settings in the User Preferences menu take precedence over settings in the System Preferences menu. For example, if the System Preferences language setting is `English (US)` and the User Preferences language setting is different, Genesys Administrator Extension will use the User Preferences language setting.

User Preferences

Advanced

On the Advanced window, you can specify the logging level for Genesys Administrator Extension JavaScript logging. Set this only if instructed to do so by support personnel. Use the drop-down list to set the level to one of the following:

- `Use system settings`—Use the same setting specified in the System menu.
- `Debug`—All (error, warning, info, and debug) logs are generated.
- `Info`—Error, warning, and info logs are generated.
- `Warning`—Only error and warning logs are generated.
- `Error`—Only error logs are generated.
- `Off`—Logging is disabled.

> **Important**
> These logs can be viewed in the browser console.

Locale

In the Locale window, you can set the following preferences by selecting the appropriate radio button:

- Language—The language to use in the GAX user interface. The default is `Use system settings`. You can add more language options by installing localization kit plug-ins. **Note**: A browser refresh is required for the changes to take effect.
- `Date Format`—The format in which dates are to be displayed in Genesys Administrator Extension. The default is `Use system settings`.
- `Start of Week`—The day on which you consider the week to start, either Sunday or Monday. The default is `Use system settings`.
- `Number Format`—The format in which numbers are to be displayed. The default is `Use system settings`.
- `Time Zone`—The time zone in which times are displayed in GAX. The default is `Use system settings`.

System Preferences

Throttling

Genesys Administrator Extension enables you to throttle the number of simultaneous changes that

are sent to Configuration Server. You can optimize these settings to help ensure consistent performance across your Genesys environment.

Change the `Bulk Update Batch Size` field to specify the number of bulk updates for configuration objects that can be executed simultaneously. The default value is `300`. A value of `0` indicates that there will be no throttling of changes for configuration objects (all requested operations will be sent to Configuration Server without delay). You can enter `0` or any positive integer in this field.

> **Important**
>
> The maximum Bulk Update Batch Size for users entering from Genesys Administrator is `300`.

Change the `Bulk Update Batch Timeout` field to specify the time interval (in seconds) that Genesys Administrator Extension should wait between executing bulk update operations. The default value is `1`. A value of `0` indicates there will be no delay between bulk update operations. You can enter any value between `0` and `300` in this field.

Locale

In the Locale window, you can set the following preferences by selecting the appropriate radio button:

- `Language`—The language to use in the GAX user interface. The default is `English (US)`. You can add more language options by installing localization kit plug-ins. **Note**: A browser refresh is required for the changes to take effect.
- `Date Format`—The format in which dates are to be displayed in Genesys Administrator Extension.
- `Start of Week`—The day on which you consider the week to start, either Sunday or Monday.
- `Number Format`—The format in which numbers are to be displayed.
- `Time Zone`—The time zone in which times are displayed in GAX.

Genesys Administrator

Click the `Launch Genesys Administrator` link in the Preferences menu to launch the Genesys Administrator application. This link is displayed if you are configured to log in to Genesys Administrator, when you log in to Genesys Administrator Extension.

Troubleshooting

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

This chapter contains the following sections:

Plug-in Issues

Genesys Administrator Extension is built upon the Spring Framework and is deployed as a set of plug-ins. If one of these plug-ins fails to load, the entire GAX instance fails to start.

If you install a plug-in and then GAX fails to start, you can try to fix the problem by removing the plug-in and restarting GAX. If GAX starts correctly after the plug-in is removed, the problem is with the plug-in and not within the rest of the GAX instance.

Required Permissions

Access to Genesys Administrator Extension and its functionality is protected by user permissions and Role-Based Access Control. If you get a permissions error when you try to log in to Genesys Administrator Extension or use any of its functionality, you probably do not have the appropriate permissions or role privileges.

An example of a required permission is this: a Tenant user must have write (`Create`) permission on his or her own `User` object to save his or her User Preferences in Genesys Administrator Extension.

Refer to the Genesys 8.0 Security Deployment Guide for more information about permissions and Role-Based Access Control, including how to set up appropriate permissions and role privileges.

Running Out of Memory

If you are working with a large amount of data, such as deploying large or multiple Solutions with Solution Deployment, the installation process might fail with one or both of the following indicators:

- In the `gax.log`, the following entry:

  ```
  lang.OutOfMemoryError: Java heap space
  ```

- In the Genesys Administrator Extension interface, on the Solutions Packages screen, there might be an error message similar to:

  ```
  Error while fetching lists of dns. There has been a server error.
  ```

This error is caused when the Java heap space is not large enough to support the current process. The default size of the heap is 64 MB. In the default installation, the heap size is set to 1024 MB (the Tomcat default is only 64 MB). If you still need to increase the memory assigned to Tomcat, do so by editing the `$CATALINA_HOME/bin/setenv.sh` (Linux) file or `$CATALINA_HOME/bin/setenv.bat` (Windows) file and adjusting the memory value.

However, if you still see these errors, increase the size of the heap as necessary.

Tomcat Issues

If you encounter problems with your Tomcat host, you can try the following to determine and resolve the problem:

- From the Tomcat host, ping Configuration Server and Solution Control Server by name and by IP address.
- From Solution Control Server, ping the Tomcat Host by name and by IP address.
- From Solution Control Server, telnet to the Tomcat host on all ports, disabling SELinux or any firewalls if necessary.
- A dedicated Tomcat startup script for Genesys Administrator Extension sets the environment variable `GAX_CMD_LINE_ARGS`. To check if this variable has been created correctly, use `gax_startup.sh` and pass parameters using the command line, or use Solution Control Interface or Genesys Administrator.
- Check that Database Access Points are configured and connected.
- Check that the `ojdbc6.jar` file (for Oracle) or `jtda-<version>.jar` file (Microsoft SQL Server) has been copied into the Tomcat `lib` directory.
- Check that gzip compression is enabled in Tomcat for responses.

Ports in Use

The table below shows the typical ports used in a Genesys environment.

Typical Ports Used

Port	Description
22	Remote shell (ssh) connections
80	Webserver; can only be used by Tomcat if it is started from the root.
8080	Web server; any user starting Tomcat may use this
1521	Oracle database connections
1433	Microsoft SQL Server
4999	Local Control Agent
5000	Genesys Deployment Agent (GDA)

Browser Issues

If the download of Audio Resource Files, encoded files, and other GAX downloads are blocked by the Microsoft Internet Explorer 8 or 9 information bar, and, after you confirm the download, you are redirected to the main page and then have to repeat the download request, you can adjust your browser settings to prevent this scenario.

This issue is not GAX-specific; it is related to your Internet Explorer settings. To prevent Internet Explorer from blocking your GAX downloads, you must disable the download information bar for GAX downloads.

There are two approaches that you can take to solve this issue:

- Configuring Internet Explorer to allow all downloads without warnings
- Configuring Internet Explorer to allow GAX downloads without warnings

Configuring Internet Explorer to allow all downloads without warnings

Purpose

- To prevent the information bar from blocking GAX file and software downloads.

This procedure disables the Information bar for all downloads. You will be able to download GAX files without being blocked; however, other content will also now be downloaded without warnings.

Start

1. Launch Internet Explorer.
2. Click `Tools`.
3. Select `Internet Options`.
4. Select the `Security` tab.
5. Click `Custom level`.
6. Scroll to the `Downloads` section of the list.
7. Under `Automatic prompting for file downloads`, click `Enable`.
8. Click `OK`.
9. Click `Yes` to confirm that you want to make the change.
10. Click `OK`.

    The Information bar for file downloads is now turned off. You can download GAX files without being blocked by Internet Explorer.

End

Configuring Internet Explorer to allow GAX downloads without warnings

Purpose

- Adjust the settings of Internet Explorer to make it less restrictive when you want to download GAX files.

This procedure enables you to maintain your security settings when you download files from the internet, while making GAX a trusted site from which all your GAX files are downloaded without warnings in the Internet Explorer information bar. You can choose to run with the security level set to High.

Start

1. Launch Internet Explorer.
2. Open the GAX site URL.
3. Click `Tools`.
4. Select `Internet Options`.
5. Click the `Security` tab.
6. Click `Trusted sites`.
7. Click `Sites`.
8. In the `Add this website to the zone` field, verify that the GAX URL is displayed. If not, enter the website in the field. It is not necessary to include the port number.
9. Click `Add`.
10. De-select `Require server verification (https:) for all sites in this zone`.
11. Click `Close`.
12. Click `Custom level`.
13. Scroll to the `Downloads` section of the `Settings` list.
14. Under `Automatic prompting for file downloads`, click `Enable`.
15. Scroll to the `Scripting` section of the `Settings` list.
16. Under `Active Scripting`, click `Enable`.
17. Click `OK`.
18. Click `Yes` to confirm that you want to make the change.
19. In the `Internet Options` window, click `OK`.

    The Information bar warnings for file downloads is now turned off for trusted sites only, and GAX is set as a trusted site.

End

Audio Resource File Playback Issue in Internet Explorer 8.x

Users of Internet Explorer 8 cannot play Audio Resource Files in Genesys Administrator Extension.

This is due to the lack of support for HTML5 in Internet Explorer 8.

To play Audio Resource Files, use a newer version of Internet Explorer or another supported browser. See Browser Requirements for more information.

Role Privileges

This Appendix describes the role privileges that are available and enforced by Genesys Administrator Extension. The privileges are in a hierarchy based on the modules in Genesys Administrator Extension. They are organized in this Appendix as follows:

- General
- GA Direct Login Integration
- Operational Parameter Management
- Solution Deployment
- Configuration Object Management
- Audio Resources Management-Tenant
- Audio Resources Management-System

To view these privileges on the `Role Privileges` tab of a `Role` object in Genesys Administrator, make sure that `Genesys Administrator Extension` is checked in the `Add/Remove Products` section on the tab.

> **Important**
>
> You must have Genesys Administrator 8.1.2, or later, installed when you upload the Genesys Administrator templates to Configuration Server and assign roles. The new template type, 184 (Genesys Administrator Server), is not recognized by earlier versions of Genesys Administrator; therefore, role assignments will not be functional.

For more information about role privileges specifically, and Role-Based Access Control in general, refer to the Genesys 8.0 Security Deployment Guide.

General

The following privileges apply to Genesys Administrator Extension.

Prerequisites

None

Role Privileges

View Audit History Data	Enables users to read privilege auditing history information.
Read Plug-ins	Enables users to read nodes and plug-ins.
Write Plug-ins	Enables users to enable or disable plug-ins, and also enables users to modify plug-in options.
Read System Preferences	Enables users to read system preferences.
Stay On Dashboard Indefinitely	Enables users to stay on a dashboard screen indefinitely, without being sent back to the login page due to inactivity.
Edit Dashboards	Enables users to edit any dashboard.
Edit Default Dashboards	Enables users to edit any default dashboard.
Add Widget	Enables users to add a widget to any dashboard.
Move Widget	Enables users to move a widget around in any dashboard.
Edit Widget	Enables users to edit the configuration in any dashboard.
Clone Widget	Enables users to clone a widget in any dashboard.
Remove Widget	Enables users to remove a widget from any dashboard.

GA Direct Login Integration

The following privileges apply to Genesys Administrator Extension.

Prerequisites

None

Role Privileges

`GA Direct Login Integration`	User privilege to access Genesys Administrator directly from GAX without re-entering credentials. Prerequisites: None.

Operational Parameter Management

Operational Parameter Management role privileges control what tasks a user can do in the Operational Parameter Management module of Genesys Administrator Extension.

Prerequisites

None

Role Privileges

`Read Parameters`	Allows a user to view Operational Parameters for OPM. Prerequisites: None.
`Write Parameters`	Allows a user to create, update, and delete Operational Parameters for OPM. Prerequisites: `Read Parameters`.
`Read Group Templates`	Allows a user to view Parameter Group Templates. Prerequisites: `Read Parameters`.
`Write Group Templates`	Allows a user to create, update, and delete Parameter Group Templates. Prerequisites: `Read Group Templates`.
`Read Parameter Groups`	Allows a user to view Parameter Groups. Prerequisites: None.
`Update and Delete Parameter Groups`	Allows a user to update or delete Parameter Groups. Prerequisites: `Read Parameter Groups`.
`Deploy and Re-associate Parameter Groups`	Allows a user to deploy or re-associate Parameter Groups. Prerequisites: `Read Group Templates` and `Read Parameter Groups`.

Solution Deployment

Solution Deployment role privileges control what tasks a user can perform in the Solution Deployment module of Genesys Administrator Extension.

Prerequisites

None

Role Privileges

`Delete IPs and SPDs`	Delete privilege for IPs and SPDs of ASDs. This privilege is required to delete deployments. Prerequisite: `Read Deployable IPs and SPDs`.
`Deploy IPs`	Deploy privilege for IPs of ASDs. This privilege is required to delete deployments. Prerequisite: Read `Deployable IPs and SPDs`.
`Deploy SPDs`	Deploy privilege for SPDs of ASDs. This privilege is required to delete deployments. Prerequisite: Read `Deployable IPs and SPDs`.
`Read Deployable and Undeployable IPs and SPDs`	Read privilege to read all IPs and SPDs, including those that are marked as undeployable. Prerequisite: `Read Deployable IPs and SPDs`
`Read Deployable IPs and SPDs`	Read privilege for marked IPs and SPDs of ASDs.
`Read Deployed IPs and SPDs`	Read privilege for deployed IPs, SPDs, and audit logs of ASDs. Prerequisites: None.
`Replace IPs and SPDs`	Enables a user to upload another version of an IP or SPD and replace the version that is already in the database.
`Upload IPs and SPDs`	Create privilege for IPs and SPDs of ASDs. Prerequisites: `Read Deployable IPs and SPDs` and `Write IPs and SPDs`.
`Write IPs and SPDs`	Write privilege for IPs and SPDs of ASDs. Enables the copy and move operations. Prerequisite: Read `Deployable IPs and SPDs`.

Configuration Object Management

Configuration Object Management role privileges control what tasks a user can perform in the Configuration Object Management module of Genesys Administrator Extension.

Prerequisites

None

Role Privileges

`Administer Users`	Allows a user to read and update the Force Password Reset on Next Login option in the User Accounts section. It also allows access to the User Options, Access Control, and Accessible Objects panels. Prerequisite: `Write Users`. Important • The `Force Password Reset on Next Login` option only displays if Genesys Administrator Extension connects to Management Framework version 8.1.1 and above. • Please see the *Genesys 8.1 Security Deployment Guide* for more information about resetting passwords.
`Administer Users Password`	Allows a user to access the `Change Password` task in the `Accounts > User Accounts` panel. Prerequisite: `Read Users`. Important This role privilege is only available in the 8.1.400.45 release or later.
`Modify User Password`	Allows a user to access the `Change Password` link in the `Preferences` menu. Prerequisite: None. Important This role privilege is only available in the 8.1.400.51 release or later.
`Read Agent Information`	Allows a user to access the `Agent Information` function and to view agent information in the User Accounts section. Prerequisites: None.

Read Users	Allows a user to access the User Accounts details pane, except for Force Password Reset on Next Login, User Options, Access Control, Accessible Objects, and Agent Information. Prerequisites: None.
Write Agent Information	Allows a user to create and update all values on the User Accounts details pane for agents. Prerequisite: Read Agent Information.
Write Users	Allows a user to create and update all values on the User Accounts details pane except for Force Password Reset on Next Login, User Options, Access Control, Accessible Objects, and Agent Information. Prerequisite: Read Users.
Administer Roles	Allows a user to access the User Options and Access Control buttons. Prerequisite: Write Roles.
Read Roles	Allows a user only to read Roles. The User Options and Access Control buttons are not displayed. Prerequisite: None.
Write Roles	Allows a user to create, update, and delete Roles. The User Options and Access Control buttons are not displayed. Prerequisite: Read Roles.
Administer Skills	Allows a user to access the User Options and Access Control buttons. Prerequisite: Write Skills.
Read Skills	Allows a user only to read Skills. The User Options and Access Control buttons are not displayed. Prerequisite: None.
Write Skills	Allows a user to create, update, and delete Skills. The User Options and Access Control buttons are not displayed. Prerequisite: Read Skills.
Administer Agent Groups	Allows a user to access the User Options and Access Control buttons. Prerequisite: Write Agent Groups.
Read Agent Groups	Allows a user only to read Agent Groups. The User Options and Access Control buttons are not displayed. Prerequisite: None.
Write Agent Groups	Allows a user to create, update, and delete Agent Groups. The User Options and Access Control buttons are not displayed. Prerequisite: Read Agent Groups.
Administer Access Groups	Allows a user to access the User Options and Access Control buttons. Prerequisite: Write Access Groups.
Read Access Groups	Allows a user only to read Access Groups. The User Options and Access Control buttons are not displayed. Prerequisite: None.
Write Access Groups	Allows a user to create, update, and delete Access Groups. The User Options and Access Control buttons are not displayed. Prerequisite: Read

	Access Groups.
Administer Capacity Rules	Allows a user to access the User Options and Access Control buttons. Prerequisite: Write Capacity Rules.
Read Capacity Rules	Allows a user only to read Capacity Rules. The User Options and Access Control buttons are not displayed. Prerequisite: None.
Write Capacity Rules	Allows a user to create, update, and delete Capacity Rules. The User Options and Access Control buttons are not displayed. Prerequisite: Read Capacity Rules.
Administer Bulk Change Sets	Allows a user to access the User Options and Access Control buttons. Prerequisite: Read Bulk Change Sets.
Read Bulk Change Sets	Allows a user only to read Bulk Change Sets. The User Options and Access Control buttons are not displayed. Prerequisite: None.
Write Bulk Change Sets	Allows a user to create, update, and delete Bulk Change Sets. The User Options and Access Control buttons are not displayed. Prerequisite: Read Bulk Change Sets.
Create/Full Control of Access Groups	Full control for Access Group objects (in Configuration Manager). It allows a user to create, copy, or move an Access Group. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Access Groups.
Delete Access Groups	Allows a user to delete Access Groups (in Configuration Manager). Prerequisite: Read Access Groups.
Modify General Options and State of Access Groups	Allows a user to modify the general options and state of Access Groups (in Configuration Manager). Prerequisite: Read Access Groups.
Modify Options/Annex of Access Groups	Allows a user to modify settings in the Options tab of Access Groups (in Configuration Manager) and view the Permissions and Dependencies tabs. Prerequisite: Read Access Groups.
Read Access Groups	Allows a user to view Access Groups (in Configuration Manager) in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Action Codes	Full control for Action Code objects. It allows a user to create, copy, or move an Action Code. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Action Codes.
Delete Action Codes	Allows a user to delete Action Codes. Prerequisite: Read Action Codes.
Modify General Options and State of Action Codes	Allows a user to modify the general options and state of Action Codes. Prerequisite: Read Action Codes.

Modify Options/Annex of Action Codes	Allows a user to modify settings in the Options tab of Action Codes and view the Permissions and Dependencies tabs. Prerequisite: Read Action Codes.
Read Action Codes	Allows a user to view Action Codes in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Agent Groups	Full control for Agent Group objects (in Configuration Manager). It allows a user to create, copy, or move an Agent Group. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Agent Groups.
Delete Agent Groups	Allows a user to delete Agent Groups (in Configuration Manager). Prerequisite: Read Agent Groups.
Modify General Options and State of Agent Groups	Allows a user to modify the general options and state of Agent Groups (in Configuration Manager). Prerequisite: Read Agent Groups.
Modify Options/Annex of Agent Groups	Allows a user to modify settings in the Options tab of Agent Groups (in Configuration Manager) and view the Permissions and Dependencies tabs. Prerequisite: Read Agent Groups.
Read Agent Groups	Allows a user to view Agent Groups (in Configuration Manager) in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Agent Logins	Full control for Agent Login objects. It allows a user to create, copy, or move an Agent Login. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Agent Logins.
Delete Agent Logins	Allows a user to delete Agent Logins. Prerequisite: Read Agent Logins.
Modify General Options and State of Agent Logins	Allows a user to modify the general options and state of Agent Logins. Prerequisite: Read Agent Logins.
Modify Options/Annex of Agent Logins	Allows a user to modify settings in the Options tab of Agent Logins and view the Permissions and Dependencies tabs. Prerequisite: Read Agent Logins.
Read Agent Logins	Allows a user to view Agent Logins in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Alarm Conditions	Full control for Alarm Condition objects. It allows a user to create, copy, or move an Alarm Condition. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Alarm Conditions.
Delete Alarm Conditions	Allows a user to delete Alarm Conditions. Prerequisite: Read Alarm Conditions.
Modify General Options and State of Alarm	Allows a user to modify the general options and

Conditions	state of Alarm Conditions. Prerequisite: Read Alarm Conditions.
Modify Options/Annex of Alarm Conditions	Allows a user to modify settings in the Options tab of Alarm Conditions and view the Permissions and Dependencies tabs. Prerequisite: Read Alarm Conditions.
Read Alarm Conditions	Allows a user to view Alarm Conditions in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Applications	Full control for Application objects. It allows a user to create, copy, or move an Application. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Applications.
Delete Applications	Allows a user to delete Applications. Prerequisite: Read Applications.
Modify General Options and State of Applications	Allows a user to modify the general options and state of Applications. Prerequisite: Read Applications.
Modify Options/Annex of Applications	Allows a user to modify settings in the Options tab of Applications and view the Permissions and Dependencies tabs. Prerequisite: Read Applications.
Read Applications	Allows a user to view Applications in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Application Templates	Full control for Application Template objects. It allows a user to create, copy, or move an Application Template. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Application Templates.
Delete Application Templates	Allows a user to delete Application Templates. Prerequisite: Read Application Templates.
Modify General Options and State of Application Templates	Allows a user to modify the general options and state of Application Templates. Prerequisite: Read Application Templates.
Modify Options/Annex of Application Templates	Allows a user to modify settings in the Options tab of Application Templates and view the Permissions and Dependencies tabs. Prerequisite: Read Application Templates.
Read Application Templates	Allows a user to view Application Templates in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Business Attributes	Full control for Business Attribute objects. It allows a user to create, copy, or move a Business Attribute. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Business Attributes.
Delete Business Attributes	Allows a user to delete Business Attributes.

	Prerequisite: Read Business Attributes.
Modify General Options and State of Business Attributes	Allows a user to modify the general options and state of Business Attributes. Prerequisite: Read Business Attributes.
Modify Options/Annex of Business Attributes	Allows a user to modify settings in the Options tab of Business Attributes and view the Permissions and Dependencies tabs. Prerequisite: Read Business Attributes.
Read Business Attributes	Allows a user to view Business Attributes in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Business Attribute Values	Full control for Business Attribute Value objects. It allows a user to create, copy, or move a Business Attribute Value. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Business Attribute Values.
Delete Business Attribute Values	Allows a user to delete Business Attribute Values. Prerequisite: Read Business Attribute Values.
Modify General Options and State of Business Attribute Values	Allows a user to modify the general options and state of Business Attribute Values. Prerequisite: Read Business Attribute Values.
Modify Options/Annex of Business Attribute Values	Allows a user to modify settings in the Options tab of Business Attribute Values and view the Permissions and Dependencies tabs. Prerequisite: Read Business Attribute Values.
Read Business Attribute Values	Allows a user to view Business Attribute Values in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Calling Lists	Full control for Calling List objects. It allows a user to create, copy, or move a Calling List. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Calling Lists.
Delete Calling Lists	Allows a user to delete Calling Lists. Prerequisite: Read Calling Lists.
Modify General Options and State of Calling Lists	Allows a user to modify the general options and state of Calling Lists. Prerequisite: Read Calling Lists.
Modify Options/Annex of Calling Lists	Allows a user to modify settings in the Options tab of Calling Lists and view the Permissions and Dependencies tabs. Prerequisite: Read Calling Lists.
Read Calling Lists	Allows a user to view Calling Lists in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Campaign Groups	Full control for Campaign Group objects. It allows a user to create, copy, or move a Campaign Group. It also allows a user to modify settings in the Permissions tab and view dependencies.

	Prerequisite: Read Campaign Groups.
Delete Campaign Groups	Allows a user to delete Campaign Groups. Prerequisite: Read Campaign Groups.
Modify General Options and State of Campaign Groups	Allows a user to modify the general options and state of Campaign Groups. Prerequisite: Read Campaign Groups.
Modify Options/Annex of Campaign Groups	Allows a user to modify settings in the Options tab of Campaign Groups and view the Permissions and Dependencies tabs. Prerequisite: Read Campaign Groups.
Read Campaign Groups	Allows a user to view Campaign Groups in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Campaigns	Full control for Campaign objects. It allows a user to create, copy, or move a Campaign. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Campaigns.
Delete Campaigns	Allows a user to delete Campaigns. Prerequisite: Read Campaigns.
Modify General Options and State of Campaigns	Allows a user to modify the general options and state of Campaigns. Prerequisite: Read Campaigns.
Modify Options/Annex of Campaigns	Allows a user to modify settings in the Options tab of Campaigns and view the Permissions and Dependencies tabs. Prerequisite: Read Campaigns.
Read Campaigns	Allows a user to view Campaigns in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Capacity Rules	Full control for Capacity Rule objects (in Configuration Manager). It allows a user to create, copy, or move a Capacity Rule. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Capacity Rules.
Delete Capacity Rules	Allows a user to delete Capacity Rules (in Configuration Manager). Prerequisite: Read Capacity Rules.
Modify General Options and State of Capacity Rules	Allows a user to modify the general options and state of Capacity Rules (in Configuration Manager). Prerequisite: Read Capacity Rules.
Modify Options/Annex of Capacity Rules	Allows a user to modify settings in the Options tab of Capacity Rules (in Configuration Manager) and view the Permissions and Dependencies tabs. Prerequisite: Read Capacity Rules.
Read Capacity Rules	Allows a user to view Capacity Rules (in Configuration Manager) in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Configuration Units	Full control for Configuration Units. It allows a user to create, copy, or move a Configuration Unit. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Configuration Units.

Modify General Options and State of Configuration Units	Allows a user to modify the general options and state of Configuration Units. Prerequisite: Read Configuration Units.
Read Configuration Units	Allows a user to view Configuration Units. Prerequisite: None.
Create/Full Control of DN Groups	Full control for DN Group objects. It allows a user to create, copy, or move a DN Group. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read DN Groups.
Delete DN Groups	Allows a user to delete DN Groups. Prerequisite: Read DN Groups.
Modify General Options and State of DN Groups	Allows a user to modify the general options and state of DN Groups. Prerequisite: Read DN Groups.
Modify Options/Annex of DN Groups	Allows a user to modify settings in the Options tab of DN Groups and view the Permissions and Dependencies tabs. Prerequisite: Read DN Groups.
Read DN Groups	Allows a user to view DN Groups in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of DNs	Full control for DN objects. It allows a user to create, copy, or move a DN. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read DNs.
Delete DNs	Allows a user to delete DNs. Prerequisite: Read DNs.
Modify General Options and State of DNs	Allows a user to modify the general options and state of DNs. Prerequisite: Read DNs.
Modify Options/Annex of DNs	Allows a user to modify settings in the Options tab of DNs and view the Permissions and Dependencies tabs. Prerequisite: Read DNs.
Read DNs	Allows a user to view DNs in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Fields	Full control for Field objects. It allows a user to create, copy, or move a Field. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Fields.
Delete Fields	Allows a user to delete Fields. Prerequisite: Read Fields.
Modify General Options and State of Fields	Allows a user to modify the general options and state of Fields. Prerequisite: Read Fields.
Modify Options/Annex of Fields	Allows a user to modify settings in the Options tab of Fields and view the Permissions and Dependencies tabs. Prerequisite: Read Fields.
Read Fields	Allows a user to view Fields in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Filters	Full control for Filter objects. It allows a user to create, copy, or move a Filter. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Filters.

Delete Filters	Allows a user to delete Filters. Prerequisite: Read Filters.
Modify General Options and State of Filters	Allows a user to modify the general options and state of Filters. Prerequisite: Read Filters.
Modify Options/Annex of Filters	Allows a user to modify settings in the Options tab of Filters and view the Permissions and Dependencies tabs. Prerequisite: Read Filters.
Read Filters	Allows a user to view Filters in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Folders	Full control for Folders. It allows a user to create, copy, or move a Folder. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Folders.
Modify General Options and State of Folders	Allows a user to modify the general options and state of Folders. Prerequisite: Read Folders.
Read Folders	Allows a user to view Folders. Prerequisite: None.
Create/Full Control of Formats	Full control for Format objects. It allows a user to create, copy, or move a Format. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Formats.
Delete Formats	Allows a user to delete Formats. Prerequisite: Read Formats.
Modify General Options and State of Formats	Allows a user to modify the general options and state of Formats. Prerequisite: Read Formats.
Modify Options/Annex of Formats	Allows a user to modify settings in the Options tab of Formats and view the Permissions and Dependencies tabs. Prerequisite: Read Formats.
Read Formats	Allows a user to view Formats in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Hosts	Full control for Host objects. It allows a user to create, copy, or move a Host. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Hosts.
Delete Hosts	Allows a user to delete Hosts. Prerequisite: Read Hosts.
Modify General Options and State of Hosts	Allows a user to modify the general options and state of Hosts. Prerequisite: Read Hosts.
Modify Options/Annex of Hosts	Allows a user to modify settings in the Options tab of Hosts and view the Permissions and Dependencies tabs. Prerequisite: Read Hosts.
Read Hosts	Allows a user to view Hosts in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of IVR Ports	Full control for IVR Port objects. It allows a user to create, copy, or move an IVR Port. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read IVR Ports.
Delete IVR Ports	Allows a user to delete IVR Ports. Prerequisite: Read IVR Ports.

Modify General Options and State of IVR Ports	Allows a user to modify the general options and state of IVR Ports. Prerequisite: Read IVR Ports.
Modify Options/Annex of IVR Ports	Allows a user to modify settings in the Options tab of IVR Ports and view the Permissions and Dependencies tabs. Prerequisite: Read IVR Ports.
Read IVR Ports	Allows a user to view IVR Ports in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of IVRs	Full control for IVR objects. It allows a user to create, copy, or move an IVR. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read IVRs.
Delete IVRs	Allows a user to delete IVRs. Prerequisite: Read IVRs.
Modify General Options and State of IVRs	Allows a user to modify the general options and state of IVRs. Prerequisite: Read IVRs.
Modify Options/Annex of IVRs	Allows a user to modify settings in the Options tab of IVRs and view the Permissions and Dependencies tabs. Prerequisite: Read IVRs.
Read IVRs	Allows a user to view IVRs in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Objective Tables	Full control for Objective Table objects. It allows a user to create, copy, or move an Objective Table. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Objective Tables.
Delete Objective Tables	Allows a user to delete Objective Tables. Prerequisite: Read Objective Tables.
Modify General Options and State of Objective Tables	Allows a user to modify the general options and state of Objective Tables. Prerequisite: Read Objective Tables.
Modify Options/Annex of Objective Tables	Allows a user to modify settings in the Options tab of Objective Tables and view the Permissions and Dependencies tabs. Prerequisite: Read Objective Tables.
Read Objective Tables	Allows a user to view Objective Tables in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Persons	Full control for Person objects (in Configuration Manager). It allows a user to create, copy, or move a Person. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Persons.
Delete Persons	Allows a user to delete Persons (in Configuration Manager). Prerequisite: Read Persons.
Modify General Options and State of Persons	Allows a user to modify the general options and state of Persons (in Configuration Manager). Prerequisite: Read Persons.
Modify Options/Annex of Persons	Allows a user to modify settings in the Options tab of Persons (in Configuration Manager) and view the

	Permissions and Dependencies tabs. Prerequisite: Read Persons.
Read Persons	Allows a user to view Persons (in Configuration Manager) in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Place Groups	Full control for Place Group objects. It allows a user to create, copy, or move a Place Group. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Place Groups.
Delete Place Groups	Allows a user to delete Place Groups. Prerequisite: Read Place Groups.
Modify General Options and State of Place Groups	Allows a user to modify the general options and state of Place Groups. Prerequisite: Read Place Groups.
Modify Options/Annex of Place Groups	Allows a user to modify settings in the Options tab of Place Groups and view the Permissions and Dependencies tabs. Prerequisite: Read Place Groups.
Read Place Groups	Allows a user to view Place Groups in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Places	Full control for Place objects. It allows a user to create, copy, or move a Place. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Places.
Delete Places	Allows a user to delete Places. Prerequisite: Read Places.
Modify General Options and State of Places	Allows a user to modify the general options and state of Places. Prerequisite: Read Places.
Modify Options/Annex of Places	Allows a user to modify settings in the Options tab of Places and view the Permissions and Dependencies tabs. Prerequisite: Read Places.
Read Places	Allows a user to view Places in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Roles	Full control for Role objects (in Configuration Manager). It allows a user to create, copy, or move a Role. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Roles.
Delete Roles	Allows a user to delete Roles (in Configuration Manager). Prerequisite: Read Roles.
Modify General Options and State of Roles	Allows a user to modify the general options and state of Roles (in Configuration Manager). Prerequisite: Read Roles.
Modify Options/Annex of Roles	Allows a user to modify settings in the Options tab of Roles (in Configuration Manager) and view the Permissions and Dependencies tabs. Prerequisite: Read Roles.

Read Roles	Allows a user to view Roles (in Configuration Manager) in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Scripts	Full control for Script objects. It allows a user to create, copy, or move a Script. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Scripts.
Delete Scripts	Allows a user to delete Scripts. Prerequisite: Read Scripts.
Modify General Options and State of Scripts	Allows a user to modify the general options and state of Scripts. Prerequisite: Read Scripts.
Modify Options/Annex of Scripts	Allows a user to modify settings in the Options tab of Scripts and view the Permissions and Dependencies tabs. Prerequisite: Read Scripts.
Read Scripts	Allows a user to view Scripts in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Sites	Full control for Sites. It allows a user to create, copy, or move a Site. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Sites.
Modify General Options and State of Sites	Allows a user to modify the general options and state of Sites. Prerequisite: Read Sites.
Read Sites	Allows a user to view Sites. Prerequisite: None.
Create/Full Control of Skills	Full control for Skill objects (in Configuration Manager). It allows a user to create, copy, or move a Skill. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Skills.
Delete Skills	Allows a user to delete Skills (in Configuration Manager). Prerequisite: Read Skills.
Modify General Options and State of Skills	Allows a user to modify the general options and state of Skills (in Configuration Manager). Prerequisite: Read Skills.
Modify Options/Annex of Skills	Allows a user to modify settings in the Options tab of Skills (in Configuration Manager) and view the Permissions and Dependencies tabs. Prerequisite: Read Skills.
Read Skills	Allows a user to view Skills (in Configuration Manager) in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Solutions	Full control for Solution objects. It allows a user to create, copy, or move a Solution. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Solutions.
Delete Solutions	Allows a user to delete Solutions. Prerequisite: Read Solutions.
Modify General Options and State of Solutions	Allows a user to modify the general options and state of Solutions. Prerequisite: Read Solutions.
Modify Options/Annex of Solutions	Allows a user to modify settings in the Options tab

	of Solutions and view the Permissions and Dependencies tabs. Prerequisite: Read Solutions.
Read Solutions	Allows a user to view Solutions in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Statistical Days	Full control for Statistical Day objects. It allows a user to create, copy, or move a Statistical Day. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Statistical Days.
Delete Statistical Days	Allows a user to delete Statistical Days. Prerequisite: Read Statistical Days.
Modify General Options and State of Statistical Days	Allows a user to modify the general options and state of Statistical Days. Prerequisite: Read Statistical Days.
Modify Options/Annex of Statistical Days	Allows a user to modify settings in the Options tab of Statistical Days and view the Permissions and Dependencies tabs. Prerequisite: Read Statistical Days.
Read Statistical Days	Allows a user to view Statistical Days in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Statistical Tables	Full control for Statistical Table objects. It allows a user to create, copy, or move a Statistical Table. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Statistical Tables.
Delete Statistical Tables	Allows a user to delete Statistical Tables. Prerequisite: Read Statistical Tables.
Modify General Options and State of Statistical Tables	Allows a user to modify the general options and state of Statistical Tables. Prerequisite: Read Statistical Tables.
Modify Options/Annex of Statistical Tables	Allows a user to modify settings in the Options tab of Statistical Tables and view the Permissions and Dependencies tabs. Prerequisite: Read Statistical Tables.
Read Statistical Tables	Allows a user to view Statistical Tables in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Switches	Full control for Switch objects. It allows a user to create, copy, or move a Switch. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Switches.
Delete Switches	Allows a user to delete Switches. Prerequisite: Read Switches.
Modify General Options and State of Switches	Allows a user to modify the general options and state of Switches. Prerequisite: Read Switches.
Modify Options/Annex of Switches	Allows a user to modify settings in the Options tab of Switches and view the Permissions and Dependencies tabs. Prerequisite: Read Switches.

Read Switches	Allows a user to view Switches in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Switching Offices	Full control for Switching Office objects. It allows a user to create, copy, or move a Switching Office. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Switching Offices.
Delete Switching Offices	Allows a user to delete Switching Offices. Prerequisite: Read Switching Offices.
Modify General Options and State of Switching Offices	Allows a user to modify the general options and state of Switching Offices. Prerequisite: Read Switching Offices.
Modify Options/Annex of Switching Offices	Allows a user to modify settings in the Options tab of Switching Offices and view the Permissions and Dependencies tabs. Prerequisite: Read Switching Offices.
Read Switching Offices	Allows a user to view Switching Offices in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Table Accesses	Full control for Table Access objects. It allows a user to create, copy, or move a Table Access. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Table Accesses.
Delete Table Accesses	Allows a user to delete Table Accesses. Prerequisite: Read Table Accesses.
Modify General Options and State of Table Accesses	Allows a user to modify the general options and state of Table Accesses. Prerequisite: Read Table Accesses.
Modify Options/Annex of Table Accesses	Allows a user to modify settings in the Options tab of Table Accesses and view the Permissions and Dependencies tabs. Prerequisite: Read Table Accesses.
Read Table Accesses	Allows a user to view Table Accesses in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Tenants	Full control for Tenant objects. It allows a user to create, copy, or move a Tenant. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Tenants.
Delete Tenants	Allows a user to delete Tenants. Prerequisite: Read Tenants.
Modify General Options and State of Tenants	Allows a user to modify the general options and state of Tenants. Prerequisite: Read Tenants.
Modify Options/Annex of Tenants	Allows a user to modify settings in the Options tab of Tenants and view the Permissions and Dependencies tabs. Prerequisite: Read Tenants.
Read Tenants	Allows a user to view Tenants in a list and access the object to view its details. Prerequisite: None.

Create/Full Control of Time Zones	Full control for Time Zone objects. It allows a user to create, copy, or move a Time Zone. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Time Zones.
Delete Time Zones	Allows a user to delete Time Zones. Prerequisite: Read Time Zones.
Modify General Options and State of Time Zones	Allows a user to modify the general options and state of Time Zones. Prerequisite: Read Time Zones.
Modify Options/Annex of Time Zones	Allows a user to modify settings in the Options tab of Time Zones and view the Permissions and Dependencies tabs. Prerequisite: Read Time Zones.
Read Time Zones	Allows a user to view Time Zones in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Transactions	Full control for Transaction objects. It allows a user to create, copy, or move a Transaction. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Transactions.
Delete Transactions	Allows a user to delete Transactions. Prerequisite: Read Transactions.
Modify General Options and State of Transactions	Allows a user to modify the general options and state of Transactions. Prerequisite: Read Transactions.
Modify Options/Annex of Transactions	Allows a user to modify settings in the Options tab of Transactions and view the Permissions and Dependencies tabs. Prerequisite: Read Transactions.
Read Transactions	Allows a user to view Transactions in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Treatments	Full control for Treatment objects. It allows a user to create, copy, or move a Treatment. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Treatments.
Delete Treatments	Allows a user to delete Treatments. Prerequisite: Read Treatments.
Modify General Options and State of Treatments	Allows a user to modify the general options and state of Treatments. Prerequisite: Read Treatments.
Modify Options/Annex of Treatments	Allows a user to modify settings in the Options tab of Treatments and view the Permissions and Dependencies tabs. Prerequisite: Read Treatments.
Read Treatments	Allows a user to view Treatments in a list and access the object to view its details. Prerequisite:

	None.
Create/Full Control of Voice Platform Profiles	Full control for Voice Platform Profile objects. It allows a user to create, copy, or move a Voice Platform Profile. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Voice Platform Profiles.
Delete Voice Platform Profiles	Allows a user to delete Voice Platform Profiles. Prerequisite: Read Voice Platform Profiles.
Modify General Options and State of Voice Platform Profiles	Allows a user to modify the general options and state of Voice Platform Profiles. Prerequisite: Read Voice Platform Profiles.
Modify Options/Annex of Voice Platform Profiles	Allows a user to modify settings in the Options tab of Voice Platform Profiles and view the Permissions and Dependencies tabs. Prerequisite: Read Voice Platform Profiles.
Read Voice Platform Profiles	Allows a user to view Voice Platform Profiles in a list and access the object to view its details. Prerequisite: None.
Create/Full Control of Voice Prompts	Full control for Voice Prompt objects. It allows a user to create, copy, or move a Voice Prompt. It also allows a user to modify settings in the Permissions tab and view dependencies. Prerequisite: Read Voice Prompts.
Delete Voice Prompts	Allows a user to delete Voice Prompts. Prerequisite: Read Voice Prompts.
Modify General Options and State of Voice Prompts	Allows a user to modify the general options and state of Voice Prompts. Prerequisite: Read Voice Prompts.
Modify Options/Annex of Voice Prompts	Allows a user to modify settings in the Options tab of Voice Prompts and view the Permissions and Dependencies tabs. Prerequisite: Read Voice Prompts.
Read Voice Prompts	Allows a user to view Voice Prompts in a list and access the object to view its details. Prerequisite: None.

Audio Resources Management—Tenant

Audio Resource Management—Tenant role privileges control what tasks a user can perform at the Tenant level in the Audio Resource Management module of Genesys Administrator Extension.

Prerequisites

None

Role Privileges

`Write Audio Resources`	Allows a user to create, update, and delete Audio Resources and the Audio Resource Files that they contain. Prerequisites: `Read Audio Resources` and `Read Personalities`.
`Write Personalities`	Allows a user to create, update, and delete Personalities for Audio Resources and their files. Prerequisite: `Read Personalities`.
`Process Audio Resources`	Allows a user to initiate re-encoding of Audio Resources and re-transferring them to target storage. Prerequisites: `Read Audio Resources` and `Read Personalities`.
`Read Audio Resources`	Allows a user to view Audio Resources and the Audio Resource Files that they contain. Prerequisite: None.
`Read Personalities`	Allows a user to view Personalities for Audio Resources and their files. Prerequisite: None.

Audio Resources Management—System

Audio Resource Management—System role privileges control what tasks a user can perform at the Solution Provider level in the Audio Resource Management module of Genesys Administrator Extension.

Prerequisites

None

Role Privileges

`Deploy Audio Resources`	Allows a user to deploy Audio Resources and the Audio Resource Files that they contain from the System Provider to Tenants. Prerequisites: Read `Audio Resources` and Read `Personalities`. This privilege is effective only if it is granted to a user in the Environment Tenant. Users in other Tenants are unable to deploy Audio Resources even if they are granted this privilege.

Configuration Options

This appendix describes the configuration options for Genesys Administrator Extension, and contains the following sections:

> **Important**
> There are no configuration options required for the Operational Parameters Management module.

Setting Configuration Options

The configuration options specified in this chapter are used by GAX after it has connected to Configuration Server. GAX also reads the `gax.properties` file for configuration options that are set before it connects to Configuration Server. See Configuring GAX Properties for more information about the `gax.properties` file.

Unless specified otherwise, set Genesys Administrator Extension configuration options in the `Application Options` tab of the Genesys Administrator Extension `Application` object.

> **Warning**
> Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator Extension exactly as they are documented in this appendix.

Mandatory Options

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

general Section

This section must be called `general`, and is configured in the Genesys Administrator Extension Server `Application` object of type `Generic Genesys Server`.

The options in this section are required for the general behavior of Genesys Administrator Extension.

auditing

- Default Value: `true`
- Valid Values: `true`, `false`
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- By default GAX is set to audit all actions that are performed by users. Set to `false` if auditing is not required.

client_app_name

- Default Value: `default`
- Valid Values: The valid name of an application object of type Configuration Manager.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the name of the client application. GAX requires a client application object to enable access control of the browser-based interface.

confserv_timeout

- Default Value: `30`
- Valid Values: The value of the timeout protocol.
- Changes Take Effect: Immediately.

Protocol timeout value for connections to Configuration Server.

default_account_dbid

- Default Value: `100`
- Valid Values: The database ID of the default account. A valid DBID that represents the person object that should be used as the default account (refer to Default Account Support).
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- The DBID that is assigned to default account. This DBID can be set to any DBID of any valid user. The user with the specified DBID will have all role privileges.
- If this option is not set, GAX uses the value `100` for the DBID. The default account is identified by DBID. The default value for the DBID is `100`. If the default account is deleted and recreated, it will be assigned a new DBID. Use the `default_account_dbid` option to specify the DBID of the default account if the

value is not 100.

inactivity_timeout

- Default Value: 600
- Valid Values: Any integer value.
- Changes Take Effect: Immediately.
- Specifies the value of the inactivity timeout in seconds. A negative value deactivates this timer.

msgsrv_attempts

- Default Value: 1
- Valid Values: Any positive integer value greater than 0.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the number of connection attempts that will be made until GAX tries to connect to the backup Message Server.

msgsrv_max_switchovers

- Default Value: -1
- Valid Values: Any integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the number of switch-overs between Message Servers before GAX gives up trying to reconnect. 0 specifies no reconnection attempts. A negative values specifies unlimited reconnection attempts.

msgsrv_timeout

- Default Value: 10
- Valid Values: Any positive integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the protocol timeout value for connections to Message Server.

msgsrv_warmstandby_timeout

- Default Value: 60
- Valid Values: Any integer value.
- Changes Take Effect: Immediately.
- The time in seconds between reconnection attempts to Message Server.

scs_attempts

- Default Value: 1
- Valid Values: Any positive integer value greater than 0.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the number of connection attempts that will be made until GAX tries to connect to the backup Solution Control Server.

scs_max_switchovers

- Default Value: -1
- Valid Values: Any integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the number of switch-overs between Solution Control Servers before GAX gives up trying to reconnect. 0 specifies no reconnection attempts. A negative values specifies unlimited reconnection attempts.

scs_timeout

- Default Value: 10
- Valid Values: Any positive integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the protocol timeout value for connections to Solution Control Server.

scs_warmstandby_timeout

- Default Value: 60
- Valid Values: Any integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- The time in seconds between reconnection attempts to Solution Control Server.

session_timeout

- Default Value: 900
- Valid Values: Any positive integer value.
- Changes Take Effect: Immediately.
- The time in seconds after the session timeout that the GAX user session on the server will be destroyed.

asd Section

This section must be called asd, and is configured in the Genesys Administrator Extension Server `Application` object of type `Generic Genesys Server`.

The options in this section are required for the Solution Deployment module in Genesys Administrator Extension.

local_ip_cache_dir

- Default Value: ./plugin.data/asd/gaxLocalCache
- Valid Values: Any valid folder
- Changes Take Effect: After Genesys Administrator Extension is restarted.

Specifies the folder where the IP used for the deployment is cached. Caching the IP reduces deployment time if the IP is reused. This option must be set to a UNC path or a local path that points to a directory that can be accessed (with read\write permissions) from the machine that is running the Genesys Administrator Extension server.

silent_ini_path

- Default Value: ./plugin.data/asd/installation/genesys_silent_ini.xml
- Valid Values: Any valid path and XML file name
- Changes Take Effect: Immediately.

Specifies the name of the silent installation folder used by ASD. May start with `.` to resolve the GAX base path automatically based on the local system settings. The default value is sufficient unless the path or file has been changed after installing Genesys Administrator Extension.

arm Section

This section must be called `arm`, and is configured in the Genesys Administrator Extension Server Application object of type `Generic Genesys Server`.

The options in this section are required for the Audio Resource Management module in Genesys Administrator Extension.

delete_from_db_after_processing

- Default Value: `false`
- Valid Values: `false`, `true`
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies if the original audio file is to be deleted from the database after all required processing (including any format conversion and transfer to target storage) is complete. If set to `true`, the original file located in the target storage is used for any subsequent reprocessing, and if required, is downloaded from the target storage rather than from the database (from which it was removed).

This option enables the user to decide if he or she wants the system to delete the binary audio information in the original audio file from the database after processing is done. The advantage of deleting the information is that less database space is used. The disadvantage is that reprocessing is possible on the files located in target storage. These files could be subject to corruption, loss, or a problem with the target storage itself, thereby losing the original information. In this case, the database just offers redundancy and robustness of the data.

local_announcement_folder

- Default Value: `announcement`
- Valid Values: Any valid folder
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the name of the folder where the audio data for audio resources of type Announcement is stored while the audio resource is stored in the database, encoded, and moved to target storage. This folder is specified relative to the path specified by the option local_path.

local_music_folder

- Default Value: `music`
- Valid Values: Any valid folder
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the name of the folder where the audio data for audio resources of type Music is stored while the audio resource is stored in the database, encoded, and moved to target storage. This folder is specified relative to the path specified by the option local_path.

local_path

- Default Value: `/opt/gax/arm`
- Valid Values: Any valid path
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the absolute path to the location of local audio storage, that is, to the folders specified by the options target_announcement_folder and local_music_folder.

local_sox_path

- Default Value: `/usr/bin/sox`
- Valid Values: Any valid path
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the absolute path to the SoX binary (executable) file.

target_announcement_folder

- Default Value: `announcement`
- Valid Values: Any valid folder name
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the folder where all audio files of type Announcement, both original and encoded, are stored. Media Server retrieves the files from this folder and uses them. This folder is specified relative to the path specified by the option target_path.
- If the delete_from_db_after_processing option is set to `true`, the original audio files stored in this folder are used for reprocessing, and are downloaded from this folder instead of from the database. However, the encoded files are always downloaded from this folder, not from the database.

target_music_folder

- Default Value: `music`
- Valid Values: Any valid folder name
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the folder where all audio files of type Music, both original and encoded, are stored. Media Server retrieves the files from this folder and uses them.This folder is specified relative to the path specified by the option target_path.

If the delete_from_db_after_processing option is set to `true`, the original audio files stored in this folder are used for reprocessing, and are downloaded from this folder instead of from the database. However, the encoded files are always downloaded from this folder, not from the database.

target_path

- Default Value: `/mnt/arm/target`

- Valid Values: Any valid path
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the absolute path to the location of the folders specified by the options target_announcement_folder and target_music_folder. This path must appear local to the Genesys Administrator Extension server, even though target storage is located on a different host. The path specified here must be served by the ARM Web Proxy server (this is typically the root directory from the perspective of the web server).

ga Section

ga_appName

- Default Value: `default`
- Valid Values: The valid name of the Genesys Administrator application object.
- Changes Take Effect: Immediately.
- Specifies the Application name for Genesys Administrator that is to be used to directly log in to Genesys Administrator from GAX.

ga_host

- Default Value: `""`
- Valid Values: The name of a host or an IP address.
- Changes Take Effect: Immediately.
- Specifies the Genesys Administrator host parameter that enables direct login to Genesys Administrator.

ga_port

- Default Value: `80`
- Valid Values: A valid port ID.
- Changes Take Effect: Immediately.
- Specifies the Application port number for Genesys Administrator that is to be used to directly log in to Genesys Administrator from GAX. This option is mandatory if the Genesys Administrator port number is not `80`.

ga_protocol

- Default Value: `http`
- Valid Values: `http`, `https`
- Changes Take Effect: Immediately.
- Specifies the Genesys Administrator protocol that is required to directly log in to Genesys Administrator from GAX.

ga_timeout

- Default Value: 2
- Valid Values: Any positive integer.
- Changes Take Effect: Immediately.

Specifies in seconds how long Genesys Administrator Extension waits to allow Genesys Administrator to successfully authenticate login parameters before Genesys Administrator Extension authenticates its login session and allows user to access GAX. Provide a value that is sufficient to accommodate Genesys Administrator.

log Section

all

- Default Value: `stdout, ./logs/gax.log`
- Valid Values:

Value	Description
`stdout`	Log events are sent to the Standard output.
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
`[filename]`	Log events are stored in a file with the specified name. If a path and filename are not specified, the file is created in the application's working directory.

- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured. For example: `stdout, logfile`

expire

- Default Value: `20`
- Valid Values: Any integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.

Specifies the maximum number of log files to be kept.

log-cache-size

- Default Value: `16000`
- Valid Values: Any integer value.
- Changes Take Effect: After Genesys Administrator Extension is restarted.

Specifies the maximum number of logs in the log message queue.

segment

- Default Value: `10000`
- Valid Values: Any valid file size.
- Changes Take Effect: After Genesys Administrator Extension is restarted.

Specifies the maximum log file size in kilobytes.

standard

- Default Value: `""`
- Valid Values:

Value	Description
`stdout`	Log events are sent to the Standard output.
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`[filename]`	Log events are stored in a file with the specified name. If a path and filename are not specified, the file is created in the application's working directory.

- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured. For example: `stderr, network`

trace

- Default Value: `""`
- Valid Values:

Value	Description
`stdout`	Log events are sent to the Standard output.
`network`	Log events are sent to Message Server, which can

Value	Description
	reside anywhere on the network. Message Server stores the log events in the Log Database.
`[filename]`	Log events are stored in a file with the specified name. If a path and filename are not specified, the file is created in the application's working directory.

- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured. For example: `stderr, network`

verbose

- Default Value: `all`
- Valid Values:

Value	Description
`all`	All log events (that is, log events of the `Standard`, `Trace`, `Interaction`, and `Debug` levels) are generated.
`debug`	The same as `all`.
`trace`	Log events of the `Trace` level and higher (that is, log events of the `Standard`, `Interaction`, and `Trace` levels) are generated, but log events of the `Debug` level are not generated.
`interaction`	Log events of the Interaction level and higher (that is, log events of the `Standard` and `Interaction` levels) are generated, but log events of the `Trace` and `Debug` levels are not generated.
`standard`	The same as `interaction`.
`none`	No output is produced.

Value	Description

- Changes Take Effect: After Genesys Administrator Extension is restarted.

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are `Standard`, `Interaction`, `Trace`, and `Debug`.

opm Section

write_json

- Default Value: `false`
- Valid Values: `true`, `false`
- Changes Take Effect: After Genesys Administrator Extension is restarted.
- Defines whether OPM writes JSON data directly to transaction objects in binary form (data is written as value for the key `"_json"`).

Known Issues

This section provides the latest information on known issues and limitations. Newer items appear at the top of this list.

- The Application Template for Genesys Administrator Extension cannot be imported into Genesys Administrator. The GAX template includes prerequisite information for role privileges, which is not supported by Genesys Administrator.
- Setup Mode cannot deploy Configuration Server and Database server on operating systems other than Windows Server 2003/2008/2012 and Red Hat Enterprise Linux 5.5/6.

Document Change History

This section lists all of the changes between the 8.1.3 and 8.1.4 versions of this document.

New Pages

The following pages have been added:

- Configuring GAX Properties
- Configuring ADDP Connections
- Logging In Remotely
- Plug-in Issues
- Known Issues

Deleted Pages

The following pages have been deleted:

- License Usage Reporting
- License Usage Reporting
- License Usage Reporting
- License Usage Reporting

Updated Pages

The following is a list of updates to pages since the 8.1.3 release:

Page Genesys Administrator Extension Deployment Guide

- Updated section
  - Contacting Genesys Customer Care

Overview

Page Configuration Object Management was modified.

Setting Up Genesys Administrator Extension

Page Setting Up Genesys Administrator Extension

- Updated sections
  - Overview
  - Prerequisites
  - Browser Requirements

Page Deploying Genesys Administrator Extension

- New sections
  - Deploying Genesys Administrator Extension (Existing Deployment)
  - Deploying Genesys Administrator Extension (New Deployment)
- Updated sections
  - Setting up the Genesys Administrator Extension database (for Oracle)
  - Setting up the Genesys Administrator Extension database (for Microsoft SQL Server)
  - Setting up the Genesys Administrator Extension database (for PostgreSQL)
  - Enabling UTF-8 character encoding (for Oracle)
  - Setting up the host for Genesys Administrator Extension server
  - Installing Genesys Administrator Extension server on a Linux host
  - Installing Genesys Administrator Extension server on a Windows Server host

Page Solution Deployment

- Deleted section
  - Installing Samba

Page Audio Resource Management

- Updated section
  - Setting up ARM Runtime Web Server

Page Transport Layer Security (TLS)

- New section
  - Secure Socket Layer (SSL) Security

Page Cross-site Scripting and Cookies

- Updated section
  - Secure Flag

- Deleted section
  - Load Balance for Apache Tomcat

Page Managing Plug-ins

- Updated section
  - Installing a GAX compatible plug-in by using the Software Installation Wizard
- Deleted section
  - Installing a GAX compatible plug-in by using the command line

Page Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.1 or higher

- Updated steps 7-8.

Page Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.0 or lower

- Updated steps 2-3.
- Added Step 4.

Accessing Genesys Administrator Extension

Page Preferences

- Updated sections
  - Advanced
  - Locale
- Deleted section
  - Reporting

Troubleshooting

Page Browser Issues

- Deleted sections
  - License Usage Reporting Report Download Issues with Internet Explorer 9
  - Enabling download of License Usage Reporting reports from Internet Explorer 9

Role Privileges

Page General was modified.

Page Solution Deployment was modified.

Page Configuration Object Management was modified.

Configuration Options

Page Configuration Options

- Updated section
  - Setting Configuration Options

Page general Section

- Updated sections
  - inactivity_timeout
  - msgsrv_warmstandby_timeout
  - session_timeout

Page asd Section

- Updated sections
  - local_ip_cache_dir
  - silent_ini_path

Page arm Section

- Deleted sections
  - local_os
  - target_os

Page ga Section

- Updated sections
  - ga_appName
  - ga_host
  - ga_port
  - ga_protocol
  - ga_timeout

Page log Section

- Updated sections
  - all
  - verbose