This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Administrator Extension Deployment Guide

Genesys Administrator 9.0.0

12/20/2024

Table of Contents

Genesys Administrator Extension Deployment Guide

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.

This document contains the following information:

Overview

Solution Deployment

Configuration Object Management

Architecture

Setting up GAX

Deployment Task Summary

Managing Plug-ins

Upgrading GAX

Accessing GAX

Logging In

Logging in to Genesys Administrator from GAX

Troubleshooting

Including:

Required Permissions

Memory Issues

Browser Issues

GAX Role Privileges

Including:

GAX Configuration Options

Including:

Operational Parameter Management

Solution Deployment

Configuration Object Management

...

general Section

arm Section

log Section

...

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 advanced administrative capabilities to both technical and business users of Genesys contact centers. Currently, the following GAX core modules are supported:

- Solution Deployment
- Operational Parameter Management
- Audio Resource Management
- Configuration Object Management

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

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 Profile menu. See Profile Menu in GAX Help for more information.

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

> **Important**
>
> Product translation is limited to contents of this product only. Display data coming from other products might appear in English.

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

- Starting from Local Control Agent 8.5.100.31, GDA is no longer installed and supported as part of Management Framework and therefore all functionality using GDA (including the installation of IPs) is deprecated.
- 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 Authoring Solution Definitions.

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

You can also define a list of trusted URLs, called whitelisted hosts, to and from which the IPs are sent and retrieved. Use the **host_whitelist** and **host_whitelist_enabled** options, as described in the security section.

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)

Protection Against External XML Entity Injection Protection

GAX includes XML validation to protect against external XML entity injection. This validation rejects any XML file that includes the external entity definition DOCTYPE.

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 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.

You can create Personalities to help you organize which files belong to a particular speaker. For example, you might have a personality called `John` that uses dialog spoken in English by a male speaker. Or, you might have a personality called `Marie` that uses dialog spoken in French by a female speaker.

A personality ID is assigned automatically when you create a personality. You can create and use a maximum of 100 personalities in a single-tenant configuration. Starting in GAX release 8.5.240, you can increase this limit to 1000 by setting the [new_arf_name_format] configuration option to `true`.

> **Warning**
>
> Genesys strongly recommends that you use this new functionality ONLY if you require more than 100 personalities, and if so, that you use this option with exteme caution.

You can upload two types of audio resources:

- Announcements—These are files that contain spoken dialog that will be played for customers. For example, you might have an announcement file that tells customers about your business hours.
- Music—These are files that play music for customers. For example, you might have a music file that plays music for customers who are about to be transferred to an Agent.

The **Audio Resources** window in Genesys Administrator Extension (GAX) displays a list of audio resources and the personalities to which they are assigned.

Configuration Object Management

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

Configuration Manager

The **Configuration Manager** window enables the creation and management of system-level configuration objects such as Alarm Conditions, Business Attributes, Hosts, and more. Refer to Configuration Manager in Genesys Administrator Extension Help for more information.

Agents Window

The Agents window consolidates all aspects of agent management into a streamlined interface. From one window, you can:

- create agents and their associated objects such as Agent Logins, DNs, and Places.
- edit agent information.
- copy, delete, and enable/disable agents, one at a time or in bulk.

Refer to Agents in Genesys Administrator Extension Help for more information.

Auditing

The auditing feature writes data to Message Server about activities in Operational Parameter Management and Solution Definitions, 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.

See Configuring the Auditing Feature for more information.

Architecture

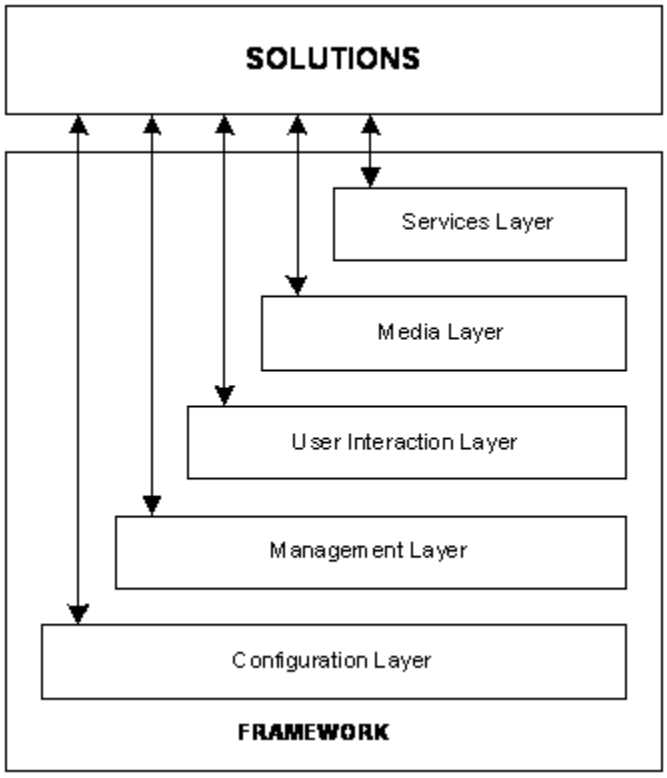
This section describes the architecture of Genesys Administrator Extension as it resides in the User Interface Layer of the Genesys Framework, and the architecture and connections within a Genesys Administrator Extension configuration.

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 Deployment Guide 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 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 Configuration Object 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.
- Communicates with the Solution Control Server (a Management Layer component) to exchange status, operations, and control information.
- Depending on the solutions that are deployed in the system, Genesys Administrator Extension might also communicate with other back-end servers to retrieve solution-specific information.
- 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.
- Displays logs from the Centralized Log Database.

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

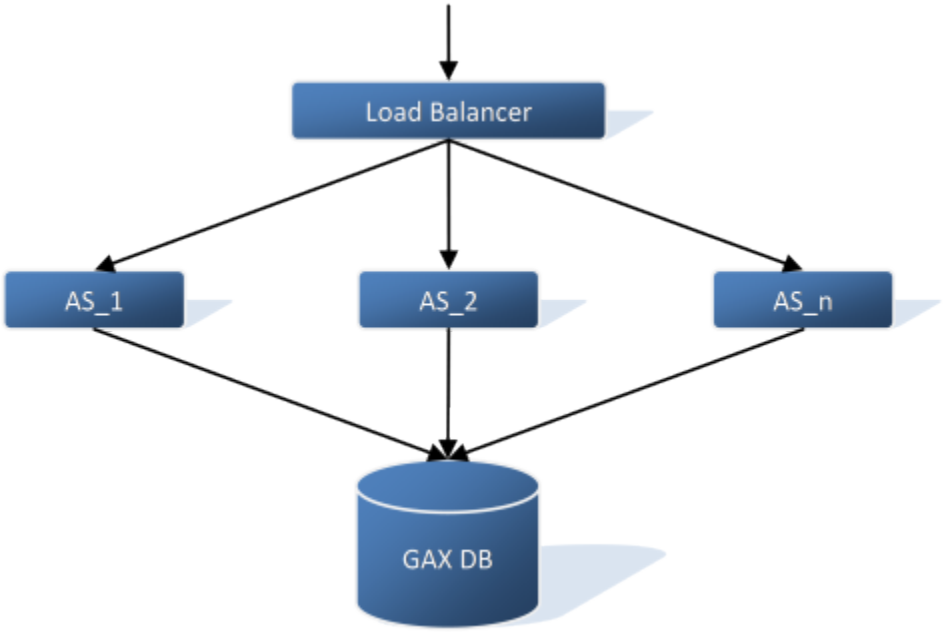
Configurations

You can deploy Genesys Administrator Extension as a single instance, or you can deploy multiple instances of GAX in a load-balanced environment to support High-Availability (HA).

> **Tip**
> As GAX is a web application, it does not support the typical Genesys HA model of Primary/Backup instances.

To support HA, you must deploy multiple active instances of GAX that connect to a common configuration environment and share common resources. For example, you can have multiple instances of GAX that connect to the same Configuration Database and DB Server.

The figure below provides an example of a GAX deployment in an HA environment. A load balancer distributes traffic to three or more GAX instances. Each GAX instance is connected to a common GAX database (see Database High Availability for more information on database HA).



To provide HA functionality, a load-balancer and at least two instances of an application server (AS) are required. The load-balancer distributes the load to all nodes.

To use the configuration described above, follow the instructions for Deploying Genesys Administrator Extension for each GAX instance. In Setup Mode, choose **Existing Deployment** and specify the same information for Configuration Database and DB Server for each GAX instance that you set up.

> **Important**
>
> If multiple GAX instances are using the same database, you must ensure that all GAX plug-ins work with the schema version of the database. For example, if you have two GAX instances with different plug-in versions that use different schema versions, you might encounter problems.

Database High-Availability

Databases that are supported by GAX have their own HA functionality. Refer to the documentation specific to your database for information on how to configure the database for HA.

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 and minimum of 5 GB is to be maintained for both database and disk.

```
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

Secure Communication with Configuration Server

Starting in Genesys Administrator Extension (GAX) 8.5.25, GAX can connect to Configuration Server using a token to ensure secure communication, instead of a password, as is the case with single sign-on (SSO) deployments. This means that for connections associated with user accounts, GAX can use short-lived encrypted tokens instead of actual passwords to authenticate the connection request.

How It Works

Generally, GAX generates a symmetric key (in essence, a shared encryption key). Configuration Server also generates a symmetric key, and it must be the same for both Configuration Server and the client. For connections associated with user accounts, GAX creates a password token by signing the username and expiry timestamp with HMAC-SHA256, using the value of **token-uuid** as a salt to create the token, and then prefixes the preamble tag.

When the client sends a connection request to Configuration Server, the server determines if the **Password** field contains a password token or a user password by looking for a tag at the beginning of the field's value. If the value does start with a tag (the preamble), Configuration Server decodes the token, extracts the token expiration time and username, and then processes the request as follows:

1. If the token is expired, the expired connection request is rejected.
2. If the token is not expired, and the username is valid, the request is accepted and GAX connects to the Configuration Server.

How to Enable It

Token-based authentication is not enabled by default. To enable it, you must enable it on Configuration Server (if not already configured), and then on GAX.

On Configuration Server

Configure the following configuration options in the **[system]** section of Configuration Server:

1. **token-authentication-mode—**Set this option to `enable`, to enable token-based authentication on all ports.
2. **token-preambula—**Specifies the preamble tag that is affixed to the start of the password token. Default value is {PXZ}. Genesys recommends that you do not configure this option and use the default value, unless you have an overriding reason.

> **Important**
>
> The password token must be small enough to fit into the existing Password field of your GAX interface (approximately 64 bytes, including the preamble tag).

3. **token-uuid—**Specifies a UUID to be used to generate a symmetric key. If not specified, Configuration Server uses a value generated internally by the primary master Configuration Server for the particular Configuration Database.

For detailed information about these options, refer to the "Configuration Server Configuration Options" chapter of the Framework Configuration Options Reference Manual.

On GAX

To configure token-based authentication on GAX, set the following options in the **[general]** section of the GAX Application object:

- **confserv_trusted**—Set this option to `true` to enable GAX to use token-based authentication.
- **token_life_in_minutes**—Specifies the length of time for which the token will be valid; once the token has expired, connection requests with this token will be rejected. Genesys recommends that you use the default value for this option, unless you have an overriding reason.

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.

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

To use the Role-based Access Control feature, Configuration Server 8.1.x or higher is required.

> **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).

Refer to the Genesys Supported Operating Environment Reference Guide for information on which operating environments are supported by GAX.

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

Browser Requirements

Refer to the Genesys Supported Operating Environment Reference Guide for information on which web browsers are supported by GAX. Although GAX supports all major browsers, it is optimized for Google Chrome.

If you use Microsoft Internet Explorer or Safari, see Browser Issues for troubleshooting information specific to your browser.

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.

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

GAX is a web application. As such, you can deploy multiple active instances of GAX behind a web load balancer to support both High Availability (HA) and load balancing. Note that this setup is different than the typical Genesys HA model that features Primary/Backup servers.

If you deploy multiple active GAX instances, the load balancer evenly distributes traffic among all instances in the cluster. If one instance fails, the load balancer redirects traffic to the remaining instances. In the meantime, Local Control Agent (LCA) auto-restarts the failed instance.

> **Important**
>
> If a GAX instance fails, users who are logged in to that instance must log in again to GAX. The load balancer redirects these login requests to the remaining active GAX instances.

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.

See the Architecture page for more information.

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

> **Important**
>
> Starting from Local Control Agent 8.5.100.31, Genesys Deployment Agent (GDA) is no longer installed and supported as part of Management Framework and therefore all functionality using GDA (including the installation of IPs) is deprecated.

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

This page describes how to install and deploy 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.

Genesys Administrator Extension can be deployed using Setup Mode or the command line.

Important

- Although Configuration Server might support more database types, GAX only supports the following database types: Oracle, Microsoft SQL Server, and PostgreSQL. Genesys Supported Operating Environment Reference Guide for information on which operating environments are supported by GAX.
- Do not connect GAX to a Configuration Server Proxy; connect it to Configuration Server only. Configuration Server Proxy does not support some functionality that is required by GAX.
- Although Management Framework supports various operating systems, GAX can only be deployed on an Operating System that is also supported by Configuration Server and DB Server. For more information, see Genesys Administrator Extension and Framework pages of *Genesys Supported Operating Environment Reference*.

Deploying Genesys Administrator Extension via Setup Mode

Setup Mode 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 DB Server (where applicable). After these components are installed, you can use the installation package (IP) management features of GAX to deploy other installation packages.

If you are using Setup Mode to install GAX for the first time, you must be a local user on the machine on which GAX will be installed. You are considered a local user if you are using this machine in person or via a remote desktop connection. After the set up is completed, the local user account is no longer used for subsequent installations.

> **Warning**
> Any interruption in the Setup Mode process might result in only partial and incomplete configuration of your environment. A complete restart of the setup process is needed. If you encounter an interruption while deploying GAX using Setup Mode, first reset Configuration Server (for example, stop any running Configuration Server processes) and your environment (for example, reset the Configuration Database) to their initial values. Then restart Setup Mode from scratch.

To deploy GAX via Setup Mode

To deploy GAX using Setup Mode, you must do the following:

1. Set up the GAX database
2. Set up the Host on which GAX will be installed
3. Install the GAX Server on the Host
4. Deploy GAX
5. Set up a connection to Solution Control Server
6. Configure Centralized Logs

Step 1 -- Set Up the GAX Database

> **Important**
> In Setup mode, results of executing SQL statements that contain the `drop` keyword are ignored, although they are still logged by GAX. This is because some databases return errors when dropping tables or views; you can ignore these errors. If required, you can find the errors in the logs of the GAX server.

Choose one of the following database types:

[+] Show steps for Oracle

To set up the Genesys Administrator Extension database for Oracle:

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 <quota> on USERS;
```

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 Oracle documentation for additional details on completing this step.

To enable UTF-8 character encoding for Oracle databases (Optional):

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

To enable UTF-8 character encoding for Oracle databases in Genesys Administrator Extension, note the following:

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

[+] Show steps for Microsoft SQL

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`, with the following parameters:
   - Server type: `Database Engine`
   - Server name: `Local`
   - Authentication: `SQL Server Authentication`
4. Create a login and password for the GAX database. For example: A username of `gax850admin` with the password `password`.

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

5. Create the GAX database (for example, `gax850`) by using the login to make this login the owner of the database.
6. Verify that you can connect to the database with the login that you created:

[+] Show steps for Postgre SQ

> **Important**
> It is recommended to use PostgreSQL version 9.1 or higher and to set **compatible** as **true** under the **[GAX]** section of the postgres Database Access Point (DAP). If you are using **custom_jdbc_url** , append `?compatible=7.1` to the custom JDBC URL.

1. Refer to the PostgreSQL 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 **Add Server**.

4. Create a login and password for the GAX database. For example: login `gax850admin` with the password `password`. You can also create a query to create the credentials using the **Query Tool**. For example:

```
CREATE USER gax WITH PASSWORD 'gax850admin' CREATEDB;
```

5. Create the GAX database (for example, `gax850`) by using the login created in the previous step to make this login the owner of the database.

```
create database gax850 owner gax;
```

6. Connect to the database with the login that you created in Step 4.
7. If you are setting up a new Configuration Server, you must do the following:
   - 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.

Database Access Points

After you have set up the GAX database, you must configure a Database Access Point (DAP) through which GAX can access the GAX Database. Normally, a basic DAP is all you need. Follow the instructions here.

Starting in GAX 8.5.25x, you can create a custom JDBC URL to connect to the GAX Database. This URL is specified in the Database Access Point (DAP), and is an alternative to using a connection based on the DAP object that enables access to the GAX Database.

To configure a custom JDBC URL, use the **jdbc_url** option in the **[GAX]** section of the DAP object. If this option is not configured, GAX will use the DAP object values for establishing the connection.

Option Name: **jdbc_url**
Valid Values: Any valid URL to an existing configured database.
Changes take effect: After restart of GAX

A sample URL for an MSSQL database is:
`jdbc:sqlserver://hostname:portnumber;Database=gax_https;username=sa;password=sa@2008;ssl=off`
In this URL, `username` and `password` are optional for security reasons, and may not be specified. If specified, GAX will consider them to be the access credentials to the GAX Database, and make the connection. If not specified, GAX will use the username and password values from the General tab of the DAP object.

> **Warning**
>
> Each DBMS configures URL in different ways. You must provide the URL in the correct format and syntax as required for your DBMS. GAX cannot establish a connection to the Database if the URL is incorrect or not improperly formed.

Step 2 -- Set Up the Host

To set up the host on which GAX will be installed:

1. If Java Server JRE 8 is not already installed on the host machine where Genesys Administrator Extension will be installed, install it now by downloading it from the following website: http://www.oracle.com/technetwork/java/javase/downloads/index.html

   > **Important**
   > JRE 1.8 is mandatory to install GAX 9.0.x. It is recommended to use the latest JRE 1.8 version.

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

   > **Important**
   > GAX only supports the 64-bit version of Oracle Java HotSpot Server VM.

2. Set the following environment variables for your host, as follows:

Linux

1. Insert the following lines into the **/etc/profile** file:

   ```
   export JAVA_HOME=/usr/lib/java/jre-<version of Java downloaded>/jre
   export PATH=$PATH:/usr/lib/java/jre-<version of Java downloaded>/jre/bin
   ```

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

Windows

1. Create a new System Variable named `JAVA_HOME` and use the path that was used during installation as the value. For example, `C:\Programs\Java\jre1.6.0_23`.
2. Edit the **Path** variable and append `C:\Programs\Java\jre1.6.0_23\bin` to the existing value.

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

Step 3 -- Install the GAX server on a host

To install the GAX Server, follow the instructions for the type of Operating System you are using.

Prerequisite:

- The environment variable **JAVA_HOME** has been configured in Step 2 -- Set Up the Host.

Linux

To install the GAX Server on Linux: **[+] Click to show steps**

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.
5. Install the Genesys Deployment Agent on port 5000 of this Host. Follow the instructions in the Framework Deployment Guide, but when asked to provide installation information for Local Control Agent, provide dummy values for now. After Configuration Server is installed, you can go back and install LCA with the correct values.

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, you must do the following:
  - Update the **setenv.sh** file. This 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 -Xms2048m -Xmx2048M"

# Uncomment the following line to activate psdk.logs, Genesys recommends that you keep this this option deactivated.
#export JAVA_OPTS="$JAVA_OPTS
-Dcom.genesyslab.platform.commons.log.loggerFactory=com.genesyslab.platform.commons.log.Log4JLoggerFactoryImpl

# 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 two lines following it, and setting the actual path and password.
  - You must create a trust store and set the trust store path accordingly. See Transport Layer Security for more information.

Windows

To install the GAX server on Windows: **[+] Click to show steps**

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. Follow the installation wizard to complete the installation.

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, you must do the following: 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 two lines following it and setting the the correct path and password.
  - You must create a trust store and set the trust store path accordingly. See Transport Layer Security for more information.

Step 4 -- Deploy GAX

The deployment procedure for GAX depends on the installation environment. Follow the steps that corresponds to your situation.

- Deploy GAX to an Existing Management Framework Deployment **[+] Click to show steps**

  Prerequisites:

  - Management Framework is deployed and configured.
  - The host property of the Configuration Server application is set.

  Steps:

  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**
>
> - Ensure to run the **gax_startup** batch file before accessing the GAX Setup Mode.
> - Setup Mode is accessible only through a local connection. You cannot use Setup Mode if you connect remotely to the GAX host.
> - Ensure that the port 8080 is accessible in the GAX host as GAX uses the port 8080.

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. Associate this instance of GAX with an Application object. Do one of the following:

> **Important**
>
> When you are first installing GAX, be sure to use an Application object that is based on the template from the GAX IP.

   - To use an existing Application object, select the Application object from the list. If the Host object on which the object is configured has the same Host name or IP address as the current GAX instance, the Application object is highlighted as **recommended**.
   - To create a new Application object, provide the following information in the corresponding fields:
     - **Administrator Extension Application Object Name**—The name of the Application object to create.
     - **Template**—The application template to use.

     This creates an application of type Genesys Administrator. 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.

> **Important**
>
> If you start or stop GAX from GA or SCI when GAX is using gax_starup.bat, then GAX status appears incorrectly in Windows Services. To view the synchronized status in Windows Services, GA and GAX, you must manually edit the GAX application in Configuration Server and update the command line to `gaxservice.exe` and the command line arguments to, for example, `-service GAX64 -immediate - app` *GAX application name*.

- Deploy GAX 8.5.000.65 or Later and Management Framework 8.5.x/8.1.x **[+] Click to show steps**

  Prerequisites:

  - Genesys Deployment Agent (GDA) must be installed on port `5000` on the server that will run Configuration Server and Database Server.

    > **Important**
    >
    > Starting from Local Control Agent 8.5.100.31, GDA is no longer installed and supported as part of Management Framework and therefore all functionality using GDA (including the installation of IPs) is deprecated.

  - The installation packages for Configuration Server and Database Server (required for Management Framework 8.1.x only) are in a location accessible to the GAX host machine.
  - You are familiar with the prerequisites for deploying Management Framework. Refer to the Management Framework documentation for more information.

  Steps:

  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 **Configuration Server Installation Package Path** field, 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.
6. Click **Next**.
7. (This step appears only if you are using an installation package for Configuration Server 8.1.x or lower.)
   In the **Database Server Installation Package Path** field, 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. When you are done, click **Next**.
8. 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.x. See Prerequisites for more information on operating systems that are supported by GAX.

   - **Management Port**—Enter the port number for the Management Port.
9. Click **Next**.
10. (This step appears only if you are using an installation package for Configuration Server 8.5.x or higher.)
    In the **Configuration Server License Path** field, enter the path to the Configuration Server license file and then click **Next**.
11. (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.

12. Click **Next**.
13. (This step appears only if you are using an installation package for Configuration Server 8.1.x or earlier.)
    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.

    When you are done, click **Next**.
14. In the **Configuration Server Database** section, provide the following information. Some fields are pre-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**

15. Click **Next**.
16. 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.
17. Click **Next**.
18. In the **Application Object Details** section, enter the name of the GAX Application object in the **Administrator Extension Application Object Name**field.
19. Click **Next**.
20. In the **Administrator Extension Database Details** section, provide the following information. Some fields are pre-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.

21. Click **Next**.
22. 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.
23. Click **Finish**.
24. GAX restarts to finish the setup operation. When it is done, GAX displays the login screen and you can login to GAX.

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.
```

- Deploy GAX 8.5.000.58 or Earlier and Management Framework 8.1.x **[+] Click to show steps**

> **Important**
>
> This procedure describes how to use Setup Mode to deploy GAX 8.5.000.58 (or earlier) and Management Framework 8.1.x. If you want to deploy Management Framework 8.5.x, you must use GAX 8.5.000.65 or later and refer to the section above - **Deploy GAX 8.5.000.65 or Later and Management Framework 8.5.x./8.1.x.**

Prerequsites:

- Genesys Deployment Agent (GDA) must be installed on port `5000` on the server that will run Configuration Server and Database Server.

> **Important**
>
> Starting from Local Control Agent 8.5.100.31, GDA is no longer installed and supported as part of Management Framework and therefore all functionality using GDA (including the installation of IPs) is deprecated.

- The installation packages for Configuration Server and Database Server are in a location accessible to the GAX host machine.
- You are familiar with the prerequisites for deploying Management Framework. Refer to Management Framework documentation for more information.

Steps:

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, enter the name of the GAX Application object in the **Administrator Extension Application Object Name**field.
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**.

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

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.
```

Step 5 -- SCS Connection

GAX must have a connection to Solution Control Server (SCS) for the System Dashboard to function.

Prerequsites:

- Solution Control Server is installed and configured.

Steps:

1. In GAX, go to Configuration Manager.
2. Hover over the **Environment** icon and select **Applications** in the pop-up list.
3. In the **Applications** list, open the Application object for GAX.
4. In the GAX Application object details window, click the **Connections** tab.
5. Click **Add**.
6. In the pop-up window, enter information about the connection to SCS. Refer to the procedure "Creating Application Objects" on the Applications page for more information.
7. Click **OK**.
8. Click **Save**. You might see an error in the system dashboard at this point but it is resolved in the next step when you restart GAX.
9. Restart GAX.

Deploying GAX via the Command Line

You can also deploy GAX (with or without Management Framework) via the command line by using a setup file to provide deployment instructions. This feature is useful for situations in which you cannot access the GAX host via a remote desktop connection.

To install GAX into an existing Management Framework Deployment, do the following:

[+] Show steps

1. Before creating the setup file, make sure the that following prerequisites are met:
   - The database is set up

> **Important**
>
> When setting up Oracle databases manually, you must execute the scripts in the following order:
>
> - Core
> - Automatic Solution Deployment

> - Operational Parameter Management

- The host is set up
- The GAX server is installed on the host
- The host property of the Configuration Server application is set.

2. Now create the setup file, to provide deployment instructions for the command-line argument. The setup file must contain the following content:

```
Configuration_Server_Host=
Configuration_Server_Port=
Default_Client_Application_Name=
Configuration_Server_Username=
Configuration_Server_Password=
Application_Object_Name=
Database_Server_Type=
Database_Host=
Database_Port=
Database_Name=
Database_Username=
Database_Password=
```

Notes:

- You must provide a valid value for each parameter in the setup file.
- If you are installing on Oracle, you need an Oracle JDBC driver, with a filename of **ojdbc<number>.jar**. You can download one from here.
- For the `Database_Host=` parameter, enter the DNS address of the database.
- For `Database_Server_Type` only the following values are valid: `oracle`, `mssql`, or `postgre`.

The following is an example of a completed setup file:

```
Configuration_Server_Host=192.168.0.1
Configuration_Server_Port=2020
Default_Client_Application_Name=default
Configuration_Server_Username=default
Configuration_Server_Password=password
Application_Object_Name=GAX_APP
Database_Server_Type=Oracle
Database_Host=135.17.176.99
Database_Port=1521
Database_Name=GAX_DB
Database_Username=gax_admin
Database_Password=password
```

3. Enter the following command in a command-line window, replacing <*setup_file_name*> with the name of the setup file you just created: `java -jar gax.war -setup gax <setup_file_name>`

To deploy GAX and Management Framework, do the following:

> **Important**
>
> You can only deploy Management Framework 8.5.x if you are using GAX 8.5.000.65 or later. GAX 8.5.000.58 or earlier can deploy only Management Framework 8.1.x.

[+] Show steps

1. Before creating the setup file, make sure the that following prerequisites are met:
   - The database is set up
   - The host is set up
   - The GAX server is installed on the host
   - You are familiar with the prerequisites for deploying Management Framework. Refer to the Management Framework documentation for more information.
2. Now create the setup file, to provide deployment instructions for the command-line argument. The setup file must contain the following content:

```
#MF settings
Configuration_Server_IP=
Database_Server_IP=(Use this line only for Management Framework 8.1.x or lower)
MF_Installation_Path=
Configuration_Server_Licence_File=(Use this line only for Management Framework 8.5.x or
higher)
Configuration_Server_Host=
Configuration_Server_Port=
Configuration_Server_OS=
Configuration_Server_OS_Bit=
Configuration_Server_Management_Port=
Database_Server_Port=(Use this line only for Management Framework 8.1.x or lower)
Install_Backup_Configuration_Server=
Backup_Configuration_Server_Host=(Optional)
Backup_Configuration_Server_Port=(Optional)
Backup_Configuration_Server_Management_Port=(Optional)
Configuration_Server_Database_Type=
Configuration_Server_Database_Host=
Configuration_Server_Database_Port=
Configuration_Server_Database_Name=
Configuration_Server_Database_Username=
Configuration_Server_Database_Password=

#GAX settings
Default_Client_Application_Name=
Configuration_Server_Username=
Configuration_Server_Password=
Application_Object_Name=
Database_Server_Type=
Database_Host=
Database_Port=
Database_Name=
Database_Username=
Database_Password=
```

Notes:

- You must provide a valid value for each parameter in the setup file, unless it is marked as optional.

- You must ensure that there are no trailing whitespace characters at the end of each parameter value line.
- If you are installing on Oracle, you need an Oracle JDBC driver, with a filename of **ojdbc<number>.jar**. You can download one from here
- For the `Database_Host=` parameter, enter the DNS address of the database.
- For `Database_Server_Type`, only the following values are valid: `oracle`, `mssql`, or `postgre`.
- For `Configuration_Server_OS`, only the following values are valid: `CFGRedHatLinux`, `CFGWinNT`, `CFGWindows2000`, `CFGWindowsServer2003`, `CFGWindowsServer2008`. If you are using Windows Server 2012, you must use the `CFGWindowsServer2008` value to prevent compatibility issues.
- For `Configuration_Server_OS_Bit`, only the following values are valid: 32 or 64.
- Windows file paths should contain escaped backslashes. For example: `C:\\GAX\\CS85mt.zip`.

The following are examples of completed setup files.

Management Framework 8.1.x (Windows)

```
#MF settings
Configuration_Server_IP=C:\\GAX\\CS64mt.zip
Database_Server_IP=C:\\GAX\\DB64.zip
MF_Installation_Path=C:\\genesys\\GCTI\\
Configuration_Server_Host=cs_primary_host
Configuration_Server_Port=2020
Configuration_Server_OS=CFGWindowsServer2008
Configuration_Server_OS_Bit=64
Configuration_Server_Management_Port=2021
Database_Server_Port=4040
Install_Backup_Configuration_Server=true
Backup_Configuration_Server_Host=cs_backup_host
Backup_Configuration_Server_Port=7020
Backup_Configuration_Server_Management_Port=7021
Configuration_Server_Database_Type=Oracle
Configuration_Server_Database_Host=cs_db_host
Configuration_Server_Database_Port=1521
Configuration_Server_Database_Name=cs_db
Configuration_Server_Database_Username=default
Configuration_Server_Database_Password=password

#GAX settings
Default_Client_Application_Name=default
Configuration_Server_Username=default
Configuration_Server_Password=password
Application_Object_Name=GAX_8.5
Database_Server_Type=Oracle
Database_Host=gaxdb_host
Database_Port=1521
Database_Name=gaxdb
Database_Username=default
Database_Password=password
```

Management Framework 8.5.x (Linux)

```
#MF settings
Configuration_Server_IP=/opt/genesys/cs850linux64.tar.gz
MF_Installation_Path=/home/genesys/GCTI/
Configuration_Server_Licence_File=/opt/genesys/license.dat
Configuration_Server_Host=cs_primary_host
Configuration_Server_Port=2020
```

```
Configuration_Server_OS=CFGRedHatLinux
Configuration_Server_OS_Bit=64
Configuration_Server_Management_Port=2021
Install_Backup_Configuration_Server=true
Backup_Configuration_Server_Host=cs_backup_host
Backup_Configuration_Server_Port=7020
Backup_Configuration_Server_Management_Port=7021
Configuration_Server_Database_Type=Oracle
Configuration_Server_Database_Host=cs_db_host
Configuration_Server_Database_Port=1521
Configuration_Server_Database_Name=cs_db
Configuration_Server_Database_Username=default
Configuration_Server_Database_Password=password

#GAX settings
Default_Client_Application_Name=default
Configuration_Server_Username=default
Configuration_Server_Password=password
Application_Object_Name=GAX_8.5
Database_Server_Type=Oracle
Database_Host=gaxdb_host
Database_Port=1521
Database_Name=gaxdb
Database_Username=default
Database_Password=password
```

3. Enter the following command in a command-line window, replacing <*setup_file_name*> with the name of the file you just created above: `java -jar gax.war -setup mf-install <setup_file_name>`

Deploying GAX into an existing Tomcat installation

> ### Important
>
> **These steps are optional.** GAX uses an embedded instance of Jetty for web-server functions, so this procedure only applies if you prefer to deploy GAX into an existing Tomcat installation.

For this procedure, see Deploying GAX into Tomcat 8 in the Genesys Administrator Extension Migration Guide.

Configuring Centralized Logs

To configure a Centralized Log, do the following:

1. Configure Message server Database Access Point (DAP):
   a. Create a non-JDBC DAP object which connects the Message Server to log database.
   b. Specify the log database details in the **DB Info** tab of this DAP.
   c. Add the Message Server DAP to the Message Server **Connections** tab.
2. Configure GAX DAP for Centralized Logs:
   a. Create a JDBC DAP object which connects GAX to Log database.
   b. Specify the log database details in the **DB Info** tab of this DAP.
   c. Under the **Options** tab, please create a section named **[GAX]** and then create an option named **role** and set the value as `auditing`.
   d. Add the GAX DAP for Centralized Log into the **Connections** tab of the GAX application.
   e. Restart GAX and then access the Centralized Log.

For more information about Centralized Logs, see *Management Framework Deployment Guide* and *Framework Database Connectivity Reference Guide*.

Configuring GAX Properties

After GAX starts for the first time, it generates the following files and folders 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**
> Read more general information about Java-based *.properties* files here.

The following options can be configured:

Option	Description	Possible Values	Default Value
`accesslog_enabled`	Enables HTTP access logging	true, false	true
`accesslog_filename`	File name for the HTTP access log	Valid filename	./logs/http-yyyy_mm_dd.log
`accesslog_timezone`	Time zone for the HTTP access log	Any valid timezone code (see Time Zones for a list). **Note:** It is recommended to specify the time zone value in canonical format instead of three-letter time zone IDs. For example, Australia/Sydney, Asia/Kolkata, America/Los_Angeles, and so on.	GMT
`accesslog_append`	After GAX is restarted, specifies whether to append to existing HTTP access log	true, false	true
`accesslog_extended`	Specifies whether to include extended	true, false	false

Option	Description	Possible Values	Default Value
	information in the HTTP access log		
`accesslog_cookies`	Specifies whether to include cookies in the HTTP access log	true, false	false
`accesslog_retaindays`	Specifies number of days to retain the HTTP access log	integer	90
`app`	Specifies the GAX Application object	Existing Application object name	
`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 address	Valid FQDN or IP address	
`cache_control`	Enables Cache-Control in the response header.	Any valid value accepted by Cache-Control HTTP header	`no-cache, no-store, must-revalidate`
`disable_xframe_options`	When its set to `true` in the **gax.properties** file, the response header will not have X-Frame-Options, and the GAX login page will load properly in new tab from other Genesys applications, such as Workspace Web Edition.	true, false	false
`enable_web_notification`	Enables real-time notification if the configuration object currently being modified has been updated by another user while the current user was modifying it; that is, since the object's properties window was opened. See Coordinating Simultaneous Changes to Data. **Note:** This feature is currently supported only in the Configuration	`true, false`	`false`

Option	Description	Possible Values	Default Value
	Manager view.		
host	Specifies the primary Configuration Server Host, written as a Fully Qualified Domain Name (FQDN) or IP address	Valid FQDN or IP address	
http_port	Defines the HTTP port	integer	8080
https_port	Defines the HTTPS port	integer	8443
input_deny_list	Enables configuration of patterns for input validation.	Space separated regex patterns. You can add more strings in space separated format. The following example has three strings: `.alert\(` `.(?i)img[\s<].?src\s?=.*` `.script`	
invalidate_session_on_login	Specifies whether GAX regenerates JSESSIONID immediately after user login and logout.	true, false	false
keystore_path	Specifies the keystore path.	Valid path, for example: Windows: `C:\\OpenSSL-Win32\\bin\\keystore` Linux: `/opt/genesys/gax/conf/keystore`	
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.	
max_cfg_connection	Specifies the maximum number of connections to allow from GAX to Configuration Server. To allow unlimited connections, set the value to -1.	-1 or any positive integer	200
max_idle_time	Specifies the maximum idle time,	integer	1000*60*60

Option	Description	Possible Values	Default Value
	in milliseconds, for HTTP connection.		
`port`	Specifies the primary Configuration Server Port	integer	
`root_url`	Specifies the root URL (host:port/rootURL)		`/gax`
`session_httponly`	Specifies whether the **HTTPOnly** flag is set automatically on session cookie JSESSIONID.	true, false	true
`session_securecookies`	Specifies whether the **secure** flag is set automatically on session cookie JSESSIONID.	true, false	true
`supported_protocol`	Defines the protocol to use when communicating with the server	`http/https/both`	`http`
`saml`	Enables SSO login to GAX using SAML	true, false	false
`saml_entityid`	Specifies entity ID used by GAX metadata	Any value	
`saml_external_userid`	Defines the protocol to correlate to the External User ID in Genesys Person object. GAX must extract DSID from SAML assertion and query the user by using the external ID, then use the username to enable the user to log in.	Valid SAML attribute (DSID) value	
`saml_idp_metadata`	Specifies the path or URL of the IDP's metadata XML file	Valid path (or) URL	
`saml_jksfilelocation`	Specifies the location or path of custom JKS Keystore.	Valid path	
`saml_jkspassword`	Defines the custom JKS Keystore's password.	Any value (password entered during key store generation)	
`saml_landingpage`	Logout URL to redirect when users log out of SSO GAX.	URL	

Option	Description	Possible Values	Default Value
saml_signingkeyname	Defines the signing key name (alias provided during custom key store generation)	Any value (alias name given during key store generation)	
saml_signingkeypassword	Defines the signing key password	Any value (key password entered during key store generation)	

Coordinating Simultaneous Changes to Data

Genesys Administrator is a web-based application, and so can support many users using it at the same time. To prevent users working on the same configuration object from overwriting the other's changes, GAX provides a real-time web notification service.

> **Important**
>
> This feature is currently supported only in the Configuration Manager view.

With this feature, the first user to save their changes can do so, and a warning message is immediately sent to all other users modifying the same configuration object. Those other users can only refresh the page, which loses all of their changes, or view the object with their own changes. In the latter case, though, the users cannot save or apply the changes—they must transfer them to an updated copy of the object or save them to an external file for import later. Regardless of what option they choose, the users are unable to overwrite each other's changes when modifying the same object at the same time.

To enable this feature, set the **gax.properties** parameter **enable_web_notification** to `true` before restarting GAX.

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 Deployment Guide for more information on ADDP.

Using ADDP with GAX

Genesys Administrator Extension supports ADDP connections to the following components:

- Configuration Server
- Message Server

For GAX to use ADDP as configured on Configuration Server, the Configuration Server ADDP connection must be added in the GAX Application.

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 for more information about 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.

ADDP Logging

ADDP uses PSDK logging, which is disabled by default. Run the following command in Java to turn on logging at the **WARN** level:

```
Dcom.genesyslab.platform.commons.log.loggerFactory=<logger_name>.commons.log.Log4JLoggerFactoryImpl -jar gax.war
```

where <logger name> is the name of the PSDK logger you are are using for these logs.

To change the logging level, add a new logger in the **webapp\WEB-INF\classes\log4j\Log4j.xml** file. For example, to change the level to **DEBUG** , add the following lines to the file.

```
<logger name=<logger_name from above>>
<level value="debug"/>
</logger>
```

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 Help*.

  > **Important**
  > Starting from Local Control Agent 8.5.100.31, GDA is no longer installed and supported as part of Management Framework and therefore all functionality using GDA (including the installation of IPs) is deprecated.

- 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

Important

- Internet Explorer does not support playing an audio file directly. You have to download the file and playback the file locally. Firefox cannot play μ-law and A-law audio codecs. Only PCM Audio codecs can be played in Firefox.
- If you will be converting audio file formats, you must install SoX (Sound Exchange) before doing any conversions. Use the procedure under the appropriate tab below.

Setting up ARM on Linux

Before using ARM on Linux, you must do the following:

1. Add the configuration option section **[arm]** and define the following configuration options on the **Options** tab of the Genesys Administrator Extension server Application object: **[+] Show options**

[arm]

- **local_announcement_folder**
- **local_music_folder**
- **local_os**
- **local_path**
- **local_sox_path**
- **target_announcement_folder**
- **target_music_folder**
- **target_os**
- **target_path**
- **delete_from_db_after_processing**

See Configuration Options for a detailed description of these options.

2. 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 14.3.1 or higher. **[+] Show procedure**

Procedure: 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.

Steps

1. Download SoX for Linux. 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
```

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

3. Now you are ready to set up the ARM Runtime Web Server on Linux. **[+] Show procedure**

Procedure: Setting up the ARM Runtime Web Server on Linux

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. 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*.

> **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.

Steps

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 ARM Runtime Web Server, 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 command at the # prompt:

   ```
   Solution portmap start
   Solution nfs 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=600,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 8.5 Deployment Guide.

Setting up ARM on Windows

Before using ARM on Windows, you must do the following:

1. Add the configuration option section **[arm]** and define the following configuration options on the **Options** tab of the Genesys Administrator Extension server Application object: **[+] Show options**

[arm]

- **local_announcement_folder**
- **local_music_folder**
- **local_os**
- **local_path**
- **local_sox_path**
- **target_announcement_folder**
- **target_music_folder**
- **target_os**
- **delete_from_db_after_processing**

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

2. If you will be converting audio file formats, you must install SoX (Sound Exchange) before doing any conversions. For Windows, GAX supports SoX version 14.3.1 or higher. **[+] Show procedure**

Procedure: 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.

Steps

1. Download SoX for Windows. For more information, visit http://sox.sourceforge.net/Main/HomePage.
2. 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.

3. Now you are ready to set up a Network File System for ARM. **[+] Show the procedure**

Procedure: Setting up ARM Runtime Web Server on Windows

Purpose: To set up a Network File System (NFS) to share data between Genesys Administrator Extension and the ARM Runtime Web Server.

> **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.

Steps

1. On the host designated as the Windows ARM Runtime Web Server, create the following required folders and subfolders:

   ```
   C:\genesys\arm
   C:\genesys\arm\music
   C:\genesys\arm\announcements
   ```

2. On the ARM Runtime Web Server, share the `arm` folder on the network, as follows:
   a. Right-click the `arm` folder and select **Properties**.
   b. Click the **Sharing** tab and select **Share**.
   c. In the **Sharing** window, enter a name for the shared folder (for example, `ARM`), and then click **Add** and then **Share** to complete the sharing.

   Now the drive is shared and can be accessed at **\\host-name\arm**.

3. On the GAX host, map the shared folder from the ARM Runtime Web Server (step 2) to, for example, the Z drive (**Z:**), as follows:

   > **Important**
   > The network mapped drive, such as Z:\, applies only to the user account that mapped the driver. GAX has to run and start under the same user account with which the network drive was mapped. Otherwise, GAX cannot access the files from the network drive.

   a. On the GAX host machine, click **Start**, and select **Computer**.
   b. In the **Tools** menu, select **Map network drive**.
   c. In the **Drive** list, select a drive to which to map the shared folder.
   d. In the **Folder** box, enter `\\<host-name>\arm`.
   e. Click **Finish**.

4. On the ARM Runtime Web Server, configure Internet Services Manager (IIS) to serve the C:\genesys\arm folder as the root directory for the new website, as follows:
   a. Log on to the Web server computer as an Administrator.
   b. Click **Start**, expand **Settings**, and click **Control Panel**.
   c. Double-click **Administrative Tools**, and then double-click **Internet Services Manager**.
   d. Click **Action**, expand **New**, and click **Web Site**.
   e. After the **Web Site Creation Wizard** starts, click **Next**.
   f. Enter a description for the Web site. This description is used internally to identify the Web

site in IIS only.

g. Select the IP address to use for the site. If you select **All** (unassigned), the web site is accessible on all interfaces and all configured IP addresses.

h. Enter the TCP port number on which to publish the site.

i. Enter the Host Header name (the real name that is used to access this site).

j. Click **Next**.

k. Do one of the following to specify the folder that contains the web site documents, and then click **Next**.

- Enter the path to the folder.
- Click **Browse** to select the folder.

l. Select the access permissions for the web site, and then click **Next**.

m. Click **Finish**.

n. Right-click the web site you have created for ARM, and in the panel on the right side, click **Directory Browsing**, and click **Enable**.

5. Verify that you can access the web site at the following URL: `http://<address of ARM Runtime Web Server:port>/<site name >`.

6. In the GAX configuration options, set the **target_path** option in the **[arm]** section to the mapped network folder from step 3, as follows:

```
[arm]
target_path = \\<host-name>\arm\
```

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 TLS section of the *Genesys 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.

Cipher Lists

Starting in GAX release 8.5.25x, you can customize Jetty SSL configuration to meet customer security requirements by setting supported ciphers for HTTPS. This is done by specifying either the cipher lists used or not used in the **gax.properties** file, adding new parameters to the file as necessary.

You must configure the parameters in the **gax.properties** file before startup of the GAX server. During the GAX startup, all these configurations are read from **gax.properties** and set in the embedded Jetty configuration. If they are not configured, default values will be passed to the Jetty server.

The new parameters are described in the following table:

Parameter	Description
setIncludeProtocols	Specifies one or more protocols to be supported. Valid values are TLSv1, TLSv1.1, and TLSv1.2. Note that JDK1.8 supports only TLSv1.2 protocol.
setIncludeCipherSuites	Specifies one or more cipher suites to be used for encoding data.
setExcludeProtocols	Specifies one or more protocols that are not to be supported. Valid values are TLSv1, TLSv1.1, and TLSv1.2. Note that JDK1.8 supports only TLSv1.2 protocol.
setExcludeCipherSuites	Specifies one or more cipher suites that are not to be used for encoding data.
addExcludeProtocols	Specifies additional protocols that are not to be supported.
addExcludeCipherSuites	Specifies additional cipher suites that are not to be used for encoding data.

Each parameter is a comma-separated list of values, using the same syntax conventions as the Jetty XML descriptor.

For example, the **gax.properties** file might contain something like this::

```
port=2020
host=ca-to-dove
app=GAX_Rob
...
addExcludeCipherSuites=SSL_RSA_WITH_NULL_MD5,SSL_RSA_EXPORT_WITH_RC4_40_MD5
...
```

Note: Regular expressions for ciphers and protocols are not currently supported because OpenSSL accepts only an exact match.

Trust Store

By default, trust storage is in the JRE folder at the following location:
C:\Program Files\Java\jre<Java version>\lib\security\cacerts

> **Important**
>
> JDK is mandatory to install GAX 9.0.000.xx. For more information on recommended JDK versions, see the *Supported Operating Environment Guide* for Genesys Administrator Extension.

The default password is "changeit".

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

[+] Create a trust store and import the certificates

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 Java Virtual Machine (JVM) update.

The trust store should contain the CA certificates that GAX should trust (note that trust store may also contain a certificate used by GAX for HTTPS). If a server sends GAX its certificate during a TLS handshake, GAX will search in its keystore for a matching CA certificate (root and/or intermediate) that was used to sign the remote server certificate. If the CA certificate is found and the remote server certificate is validated, the connection is accepted; otherwise, the connection is rejected.

Prerequisites

- Your Keytool must be configured to your path.
- You have JRE or JDK installed. For more information on recommended JDK versions, see the *Supported Operating Environment Guide* for Genesys Administrator Extension.

Steps

To create a trust and key store that is separate from the default keystores that come with Java, do the following:

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"
   ```

   Note: It is recommended to use **-importcert** instead of **-import** if you are using Java 8 or above.

   Where:

   - `-alias` corresponds to the certificate being imported; it can be an address within the trust store.
   - `-keystore` specifies the keystore file.
   - `-file` specifies the certificate to be imported. It must be a PEM encoded certificate and the extension can be **.cer** or **.pem**.
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
   ```

> ### 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. On Linux or Windows, set these options by adding the following lines to the `setenv.sh` or `setenv.bat` script, respectively.

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

If you have configured GAX to start as a service, add the following arguments in the **JavaServerStarter.ini** file:

```
-Djavax.net.ssl.trustStore="D:\certificates\trusted.keystore"
-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 Use of the Auto Detect Port

When GAX connects to the Auto Detect (Upgrade) port, the **trustStore** set by the **setenv.sh** or **setenv.bat** script is ignored. You must configure the trust store based on the settings of the Auto Detect port. In addition, you usually must import the GAX certificate into the trust store.

[+] Set up secure connection to Auto Detect port on Windows

On the GAX host:

1. Import the certificate into the Windows certificate store in Microsoft Management Console (MMC), under the same user that starts the GAX processes. If GAX runs under a local system account, there are several ways to import certificates to this local account. This is the most common:
   - Enter `psexec.exe –i –s mmc.exe` on the command line, and then import the certificate for the local system account user.
   - Enter `psexec.exe -i -s certutil -f -user -p [password] -importpfx [path to the certificate]`

   Important
   - `psexec.exe` with the `-s` flag executes the specified program under the system account.
   - **psexec** is part of PSTools that you can download from http://technet.microsoft.com/en-US/sysinternals.
2. On the **Options** tab of the GAX application object, in the **[security]** section, create a new option **certificate** and set its value to the thumbprint of the certificate that you imported in step 1.
3. Try to connect to the Configuration Server Auto Detect port and see if it works.

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.

> **Tip**
>
> You must enable X-Forwarded-Proto on the F5 load balancer when GAX is accessed via HTTPS through F5 load balancer on High Availability setup.

GAX is HTTP Strict Transport Security (HSTS) compliant starting from the release 8.5.260.11. HSTS is disabled by default and you can enable it by configuring `enable_hsts=true` in the **gax.properties** file. This is a static change. Once HSTS is enabled, GAX prevents downgrading of encrypted HTTPS connection to unencrypted HTTP. It is implemented by sending a response header record from the server indicating that compliant Web browsers or other HTTP client programs must use HTTPS and they must display the appropriate confirmation message or error message in the browser console.

[+] Set up HTTPS for use with GAX

To set up HTTPS for use with GAX, do the following:

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. Note that it is mandatory to specify the value of **-alias** as **gax**.
2. Rename **gax.properties** to **gax.properties.tmp**. A new **gax.properties** file will be created. At the end of the procedure, when https is set up successfully, the other values in **gax.properties.tmp** must be copied again to **gax.properties**.

> **Warning**
>
> - If you are trying to configure GAX with plug-ins installed, remove the **webapp** and **plug-ins** folders from the GAX installation directory. When GAX configuration is complete, you can rollback all the changes and use the keystore password in your environment.
> - Make sure that GAX **gax_startup.bat** does not contain `GAX_CMD_LINE_ARGS`. Otherwise, GAX cannot enter setup mode.

3. As a local user (whether in person or via a remote desktop connection), log in to GAX as `root` user (`localhost:8080/gax` in GAX installed machine).
4. In another tab, generate gax encryption key using: `http://localhost:8080/gax/api/system/generategaxkey`
   This generates a new encryption key and stores it in a newly created `gax_store.txt` file in the `conf` folder.

> **Important**
>
> Provide read permission only for GAX user for the <GAX_installation_directory>/conf/gax_store.txt file.

> **Important**
>
> For releases from 9.0.100.56 to 9.0.100.66, GAX automatically generates the crypto_code which is used for encryption/decryption while calling the setkeystorepassword webservice API mentioned in step 5. Ignore Step 4 for those releases.

5. 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 must be the same as the password specified for the keystore (see Step 1, above).
   Alternately, use the following commands without a web browser:

```
curl -i --cookie-jar "./cookie.txt" -H "Content-Type: application/json" -d "
{\"username\":\"root\",\"password\":\"\",\"isPasswordEncrypted\":\"false\"}"
http://localhost:8080/gax/api/session/login
curl --cookie "./cookie.txt" http://localhost:8080/gax/api/system/
setkeystorepassword?password=password
```

> **Important**
>
> Password can contain special characters except #, %, &, +, and `.

> **Important**
>
> For releases from 9.0.100.72, use the following commands without a web browser:

```
curl -i --cookie-jar "./cookie.txt" -H "Content-Type: application/json" -d "
{\"username\":\"root\",\"password\":\"\",\"isPasswordEncrypted\":\"false\"}"
http://localhost:8080/gax/api/session/login
curl --cookie "./cookie.txt" http://localhost:8080/gax/api/system/generategaxkey
curl --cookie "./cookie.txt" http://localhost:8080/gax/api/system/
setkeystorepassword?password=password
```

> **Important**
> root mentioned in the above commands is the GAX root user.

- Define the parameter https_port in gax.properties with the secured port number according to your setup. The default HTTPS port for Tomcat is 8443. See Configuring GAX Properties for more information.
  - https_port=8443
  - supported_protocol=https or both.
  - keystore_path=full path of the location of keystore
- Restart GAX in HTTPS mode.
  For example gax.properties in conf folder contains the following:

```
keystore_password=***/SGo*********moXg\=\=
backup port=2020
port=2020
backup host=
https_port=8443
supported_protocol=https
keystore_path=C:\\OpenSSL-Win32\\bin\\keystore
host=xxx.xx.xxx.xx
app=gax_https1
```

> **Important**
> Sample keystore_path for Linux is keystore_path=/opt/genesys/gax/conf/keystore

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 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

> **Important**
>
> Genesys Deployment Agent (GDA) is no longer installed and supported as part of Management Framework 8.5.1 (starting from Local Control Agent *O8.5.100.31*), and therefore all functionality using GDA (including the installation of IPs) is deprecated.

Configuring mutual TLS between GAX and Configuration Server

To support mutual TLS connection between GAX and Configuration Server, you must do the following:

1. **Download OpenSSL**
2. **Add environmental variable**
   1. Set `path = C:\OpenSSL-0.9.8\bin\`
   2. Set `OPENSSL_CONF=C:\openssl-0.9.8\OpenSSL.cnf`
3. **Prepare certificate**
   1. Go to OpenSSL location.
   2. Run `Openssl>req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 5000 -config "c:\openssl-0.9.8\openssl.cnf`
   3. Set `passphrase = changeit` (password that will be used later)
   4. `Openssl> x509 -outform der -in cert.pem -out cert.der`
   5. Copy `cert.der cert.cer` in a folder, which will be used later (optional)
   6. Remove password:
      `OpenSSL rsa -in key.pem -out keynopass.pem`

7. Combine certificate and key in 1 file:
   `openssl pkcs12 -inkey keynopass.pem -in cert.pem -export -out cert.pfx`

4. **Configure certificate**
   1. In the Configuration Server machine, configure Configuration Server certificates by using the mmc utility.
   2. Import your **cert.pfx** from CME-certs directory into **Personal** > **Certificates**.
   3. Import **cert.der** (or .cer or .pem, as per UI) into **Trusted Root certification** > **certificates**.
   4. In the GAX machine, create a directory **c:\install\openssl\GAX-certs**.
   5. Copy the **Certificates** folder from the Configuration Server machine to **c:\install\openssl\GAX-certs**.
   6. Type `changeit` if prompted for password.
   7. Repeat step 1 and 2.
   8. Navigate to the location **c:\install\OpenSSL\GAX-certs** and open OpenSSL.
   9. `Openssl>pkcs12 -export -in cert.pem -inkey keynopass.pem -certfile cert.pem -out cert-and-key.p12`.
   10. Open cmd and navigate to **c:\install\openssl\GAX-certs in cmd**.
   11. Run `keytool -importkeystore -srckeystore cert-and-key.p12 -srcstoretype pkcs12 -destkeystore gax.jks -deststoretype JKS`.
   12. Run `keytool -list -v -keystore gax.jks`.
   13. Run `keytool -importcert -alias CMEcert -file c:\install\openssl\CME-certs\cert.der -keystore gax.jks -storepass changeit`.

14. **Configure confserv application in Configuration Server**
   1. Select **Confserv** and create port `3040` as auto detect.
   2. Open **Port** > **Certificate** tab and click **Import Certificate** and then choose self-signed certificate for Configuration Server machine (the machine that you configured and not the existing machine).
   3. Add thumb print copied from mmc.
   4. In the **Advanced** tab of port, add `tls-mutual=1`, so that the output is similar to: `upgrade=1;tls-mutual=1;certificate=01 11 A2 B0 42 D6 99 C8 C7 F8 C6 21 58 DD AF E4 2D FF 51 FD`.

5. **Configure in GAX application**
   1. Go to GAX installed path.
   2. Edit gax start up file with the following options:

```
set JAVA_OPTS=-server -XX:MaxPermSize=512m -XX:+CMSClassUnloadingEnabled
 -XX:+UseConcMarkSweepGC -XX:+HeapDumpOnOutOfMemoryError
 set JAVA_OPTS=%JAVA_OPTS%
 -Dcom.genesyslab.platform.commons.log.loggerFactory=com.genesyslab.platform.commons.log.Log4JLoggerF
 set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.debug=all
 set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.debug=ssl:handshake
```

```
set DEBUG_OPTS=-Xdebug
-Xrunjdwp:transport=dt_socket,address=9002,server=y,suspend=n
set SECURITY_OPTS=-Djavax.net.ssl.trustStorePassword=changeit
-Djavax.net.ssl.trustStore=C:\install\openssl\GAX-certs\gax.jks
set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%
java %JAVA_OPTS% %DEBUG_OPTS% -jar gax.war
```

3. Add line `mf_tls_mutual=true` in the **gax.properties** file.
4. Change port from `2020` to `3040` in **gax.properties** file.
5. Restart Configuration Server and GAX.

Configuring mutual TLS between GAX and Solution Control Server

To support mutual TLS connection between GAX and Solution Control Server (SCS), you must do the following:

1. **Download OpenSSL**
2. **Add environmental variable**
   1. Set `path = C:\OpenSSL-0.9.8\bin\`
   2. Set `OPENSSL_CONF=C:\openssl-0.9.8\OpenSSL.cnf`
3. **Prepare certificate**
   1. Go to OpenSSL location.
   2. Run `Openssl>req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 5000 -config "c:\openssl-0.9.8\openssl.cnf`
   3. Set `passphrase = changeit` (password that will be used later)
   4. `Openssl> x509 -outform der -in cert.pem -out cert.der`
   5. Copy `cert.der cert.cer` in a folder, which will be used later (optional)
   6. Remove password:
      `OpenSSL rsa -in key.pem -out keynopass.pem`
   7. Combine cert and key in 1 file:
      `openssl pkcs12 -inkey keynopass.pem -in cert.pem -export -out cert.pfx`
4. **Configure certificate**
   1. In SCS machine, configure certificates by using the mmc utility.
   2. Import your **cert.pfx** from CME-certs directory into **Personal** > **Certificates**.
   3. Import **cert.der** (or .cer or .pem, as per UI) into **Trusted Root certification** > **certificates**.
   4. In the GAX machine, create a directory **c:\install\openssl\GAX-certs**.
   5. Copy the **Certificates** folder from SCS machine to **c:\install\openssl\GAX-certs**.
   6. Type `changeit` if prompted for password.

7. Repeat step 1 and 2.
8. Navigate to the location **c:\install\OpenSSL\GAX-certs** and open OpenSSL.
9. Run `Openssl>pkcs12 -export -in cert.pem -inkey keynopass.pem -certfile cert.pem -out cert-and-key.p12`.
10. Open cmd and navigate to **c:\install\openssl\GAX-certs in cmd**.
11. Run `keytool -importkeystore -srckeystore cert-and-key.p12 -srcstoretype pkcs12 -destkeystore gax.jks -deststoretype JKS`.
12. Run `keytool -list -v -keystore gax.jks`.
13. Run `keytool -importcert -alias CMEcert -file c:\install\openssl\CME-certs\cert.der -keystore gax.jks -storepass changeit`.

14. **Configure SCS application in Configuration Server**
    1. Select **Confserv** and create port 3045 as auto.
    2. Open **Port** > **Certificate** tab and click **Import Certificate** and then choose self-signed certificate for SCS machine (the machine that you configured and not the existing machine).
    3. Add thumb print copied from mmc.
    4. In the **Advanced** tab of port, add `tls-mutual=1`, so that the output is similar to: `upgrade=1;tls-mutual=1;certificate=01 11 A2 B0 42 D6 99 C8 C7 F8 C6 21 58 DD AF E4 2D FF 51 FD`.

5. **Configure in GAX application**
    1. Go to GAX installed path.
    2. Edit gax start up file with the following options:

```
set JAVA_OPTS=-server -XX:MaxPermSize=512m -XX:+CMSClassUnloadingEnabled
-XX:+UseConcMarkSweepGC -XX:+HeapDumpOnOutOfMemoryError
set JAVA_OPTS=%JAVA_OPTS%
-Dcom.genesyslab.platform.commons.log.loggerFactory=com.genesyslab.platform.commons.log.Log4JLoggerF
set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.debug=all
set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.debug=ssl:handshake
set DEBUG_OPTS=-Xdebug
-Xrunjdwp:transport=dt_socket,address=9002,server=y,suspend=n
set SECURITY_OPTS=-Djavax.net.ssl.trustStorePassword=changeit
-Djavax.net.ssl.trustStore=C:\install\openssl\GAX-certs\gax.jks
set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%
java %JAVA_OPTS% %DEBUG_OPTS% -jar gax.war
```

    3. Add line `mf_tls_mutual=true` in the **gax.properties** file.
    4. Go to Configuration Server, select GAX, and then in the **Connections** tab, add SCS.
    5. Go to Port and change port to the secured port (auto).
    6. Restart SCS and GAX.

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 in the Transport parameters section:

```
"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. In addition to the appropriate procedure below, refer to the documentation that came with your database for information on how to use TLS security.

[+] Configuring the GAX Oracle Database for TLS

Prerequisite:

- Setting up the Genesys Administrator database (for Oracle)

Steps

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.
   - In the GAX section of the DAP, create an option that is named `tls_mode`.
   - 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`.

[+] Configuring the GAX MS SQL Database for TLS

Procedure: Configuring the GAX Database for TLS (Microsoft SQL Server)

Prerequisites

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

Steps

1. Configure Microsoft SQL Server as described in the related database guides.
2. Set the level of TLS control on the DAP.
   - In the GAX section of the DAP, create an option that is named `tls_mode`.
   - 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`.
3. Verify that the configured port is identical to the TLS listener port of Microsoft SQL Server
4. 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"
```

[+] Configuring the GAX PostgreSQL Database for TLS

Procedure: Configuring the GAX Database for TLS (PostgreSQL)

Prerequisites

- Set up the Genesys Administrator database for PostgreSQL.

Steps

1. Configure PostgreSQL as described in the related database guides.
2. Set the level of TLS control on the DAP.
   - In the GAX section of the DAP, create an option that is named `tls_mode`.
   - 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`.

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 Flag

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.

When GAX is running on an embedded Jetty system, GAX automatically sets the `HttpOnly` flag on the JSESSIONID session cookie. You can turn off this flag by adding the following line in the **gax.properties** file:

```
session_httponly = false
```

If GAX is using an external Tomcat web server, open and edit the `$CATALINA_HOME/conf/context.xml` file.

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

```
useHttpOnly="true"
```

The main tag should be:

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

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.

When GAX is running on an embedded Jetty system and **supported_protocol** is set to `https` in **gax.properties**, GAX automatically sets the `Secure` flag on the JSESSIONID session cookie. You can turn off this flag by adding the following line to the **gax.properties** file:

```
session_securecookies = false
```

If GAX is using an external Tomcat web server, open and edit the `$CATALINA_HOME/conf/server.xml` file.

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" />
```

Content Security Policy

GAX supports Content Security Policy (CSP) starting from the release 8.5.260.11. CSP helps users in mitigating Cross-Site Scripting, man-in-the-middle attacks, and data ex-filtration. You can limit the trusted external resources using your CSP.

You can frame your own CSP and configure the CSP headers for GAX using the `content_security_policy` option in the **gax.properties** file. This is a static change. Once CSP is configured, GAX adds the **Content-Security-Policy** header in the response with the configured policy.

> **Important**
>
> Micorsoft Internet Explorer does not support Content Security Policy.

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 seconds of administrator inactivity (no mouse or keyboard usage) that triggers application locking. If the administrator has been inactive longer than the number of seconds that is specified by the `inactivity_timeout` option, the administrator must re-authenticate to be able to use the GAX application. A negative value 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

The auditing feature writes data to Message Server about activities in Operational Parameter Management and Solution Definitions, 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 Parameter Groups.

GAX Application

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

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.

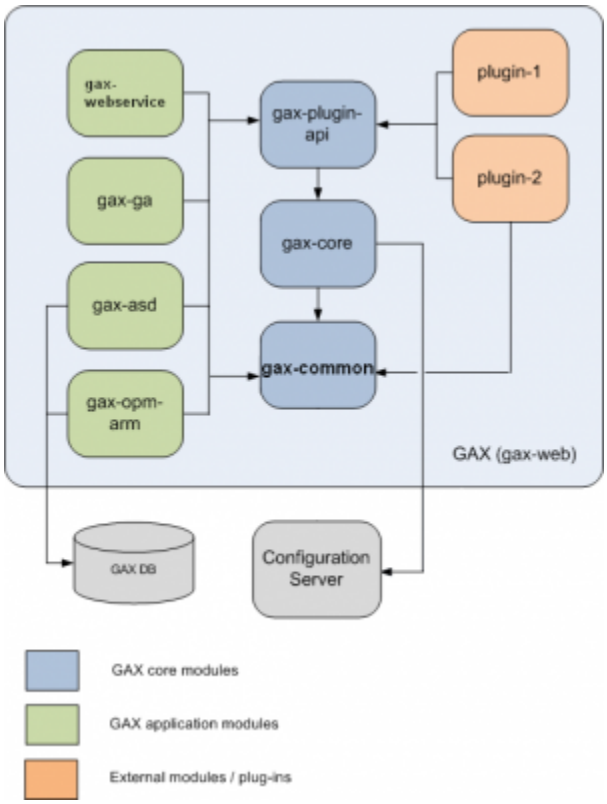
Database Configuration

To read the audit data from the Log Database, a DAP (Database Access Point) 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. To identify the DAP role, set the value of the `role` option in the GAX section of the DAP to `auditing`.

You can now view auditing information in certain panels by clicking the **Related** button and selecting the **History** option.

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 **Administration > Plug-in Management**.

You can click the name of a plug-in to view additional details, 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 Deployment Wizard tab in the Genesys Administrator Extension Help for detailed information.

[+] Click here to show procedure

Procedure: Installing Plug-ins with the Software Installation Wizard

Purpose: To install plug-ins that are designed for GAX 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.

> **Important**
>
> Starting from Local Control Agent 8.5.100.31, Genesys Deployment Agent (GDA) is no longer installed and supported as part of Management Framework and therefore all functionality using GDA including the installation of IPs and Plug-ins (with the Software Installation Wizard) is deprecated.

Steps

1. In the **Installation Packages** panel, click **+**. A new panel called **Software Installation Wizard** opens to the right.
2. 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.
- Deploy the plug-in by using the **Automated Deployment Wizard** (this method is also used to deploy installation packages). For more information, refer to Deploy Installation Packages in the Genesys Administrator Extension Help.

> **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.

- If you install a plug-in through GAX on Windows, the deployment wizard prompts you to specify only the plug-in installation path.

  If you install a plug-in through GAX on Linux, then the deployment wizard prompts you to specify both the GAX directory path and the plug-in installation path. If the path where GAX is installed is provided incorrectly, then the deployment wizard installs the plug-in but it will not copy the plug-in files to the GAX directory. In this case, you must manually copy the plug-in files from the plug-in installed path to the GAX installed path.

Installing Legacy Plug-ins

[+] Click here to show procedure

Procedure: 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.

> **Important**
> Starting from Local Control Agent 8.5.100.31, Genesys Deployment Agent (GDA) is no longer

> installed and supported as part of Management Framework and therefore all functionality using GDA including the installation of IPs and Plug-ins (with the Software Installation Wizard) is deprecated.

Steps

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.

Installing Language Packs

[+] Click here to show procedure

Procedure: Installing Language Packs

Steps

1. Copy the Language Pack IP to the host machine.
2. Stop GAX (if it is running).
3. Run the **setup.exe** (Windows) or **install.sh** (Linux) installation file.
4. Follow the prompts in the installer to install the Language Pack.
5. Restart GAX.

> **Important**
> Product translation is limited to contents of this product only. Display data coming from other products might appear in English.

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

[+] Click here to show procedure

Procedure: Modifying plug-in settings

Steps

1. Select an application in the **Administrator Applications** list. A new panel opens to the right.
2. Click **Plug-ins** to view which plug-ins are associated with the application. A new panel opens to the right.
3. Select a plug-in in the **Plug-in Info** list. A new panel opens to the right.
4. Click **Plug-in Options**. A new panel opens to the right. The panel displays the options that are associated with the plug-in.
5. Click an option to view more information about the option in a separate panel that opens to the right.
6. 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.

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.

[+] Click to show procedure

Procedure: Enabling or disabling a plug-in in GAX

Steps

1. Select an item in the **Administrator Applications** list. More information about the item displays in a new panel to the right.
2. Click **Plug-ins**. More information about the plug-ins for the item display in a panel to the right.
3. Select a plug-in from the list.
4. 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.

Important

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

Removing a plug-in from GAX

[+] Click to show procedure

Procedure: Removing a plug-in from GAX

Steps

1. Stop GAX.
2. Go to **<GAX_HOME>/webapp/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 want to remove.
4. Go to **<GAX_HOME>/webapp/plugins** on the file system (where **<GAX_HOME>** is your home folder for the GAX application).
5. Delete the folder for the plug-ins that you want to remove.
6. Start GAX.

Upgrading GAX

This page describes how to upgrade GAX from previous versions to the current version. Before you begin, it is recommended that you review Setting Up Genesys Administrator Extension to learn more about prerequisites, supported browsers, and other useful upgrade information.

To begin, open the tab that applies to your system.

> **Important**
>
> Genesys Administrator Extension uses an embedded instance of Jetty for web-server functions, whereas previous releases have used Tomcat. The upgrade procedures below 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 GAX (Management Framework 8.1.1 or higher)

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. Click the option below that describes your GAX environment. You can skip this step if your GAX Application object type is **Genesys Administrator Server** and you do not intend to use the Pulse 8.5 plug-in.
   '''[+] Click here if your GAX Application object is 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.
      i. Ensure that you follow the steps that pertain to the use of 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. 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**.

'''[+] Click here if you intend to use the Pulse 8.5 plug-in'''

You must reuse the existing GAX Application object if you intend to migrate to Pulse 8.5. To do so, use Genesys Administrator to perform the steps below:

a. Upload the GAX 8.5 Application Template. Download the Genesys Administrator Help for additional instructions on how to upload Application Templates.

b. Open the GAX 8.5 Application Template object.

c. Click the **Options** tab.

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

e. Close the GAX 8.5 Application Template.

f. Open your existing GAX Application object.

g. Click the **Options** tab.

h. Click **Import** and specify the **CONF/CFG** file that you previously created from the GAX 8.5 Application Template. Select **No** to not overwrite any existing options.

i. Click **Save & Close**.

4. Go to the GAX folder and back up the **webapp** folder by renaming it to **webapp_backup**.
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. Execute all applicable database upgrade scripts, if necessary. To determine if you have to apply any database scripts:

   a. Execute the following SQL statement on your existing GAX database: `select * from db_schema_version`.

   b. Compare the result with the update scripts in the **resources/sql_scripts** folder in the target directory of the installation.

> **Important**
>
> The latest database schema versions are:
>
> - core—8.5.260.11
> - asd—8.5.000.01
> - opm-arm—8.1.301.01
>
> Examples of upgrade scripts for Solution Deployment:
>
> - (Oracle only) **gax_asd_upgrade_db_8.1.320.01_to_8.5.000.01_ora.sql**
> - (Microsoft SQL only)

gax_asd_upgrade_db_8.1.320.01_to_8.5.000.01_mssql.sql

- (PostgreSQL only)
  gax_asd_upgrade_db_8.1.320.01_to_8.5.000.01_postgres.sql

If you do not have the latest database schema versions, execute the scripts in the following order:
-1- Core
-2- Automatic Solution Deployment

-3- Operational Parameter Management

- As a local user on the host machine, whether in person or via a remote desktop connection, launch GAX and run Setup Mode.
- (Optional) You can delete the previous GAX Application object after you have verified that the new release is working correctly.
- To use the System Dashboard feature, you must set up a connection to Solution Control Server (SCS).
- (Optional) If you backed up the **webapp** folder in Step 4 to **webapp_backup**, you must perform the following actions:

  a. Stop GAX.

  b. Copy the plug-in .jar files from **webapp_backup** to the new **webapp** folder in the GAX 9.0.* installation folder.

  c. Delete the **webapp_backup** folder.

  d. Start GAX.

Important

- Some plug-ins might require additional configuration. Refer to the plug-in documentation for more information about installing and configuring the plug-in.
- 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 GAX (Management Framework 8.1.0 or Lower)

> **Important**
>
> Refer to the Known Issues section of the Management Framework Release Notes for information about using Management Framework versions prior to the 8.1.0 release.

1. Stop the instance of GAX that you intend to upgrade.
2. (Optional) Complete this step if you intend to migrate an earlier version of Pulse to Pulse 8.5. You must reuse the existing GAX Application object if you intend to migrate to Pulse 8.5. To do so, use Genesys Administrator to perform the steps below:
   a. Upload the GAX 8.5 Application Template. Download Genesys Administrator Help for additional instructions on how to upload Application Templates.
   b. Open the GAX 8.5 Application Template object.
   c. Click the **Options** tab.
   d. Click **Export** to save your configured GAX options to a file on your local file system of type **CONF/CFG**.
   e. Close the GAX 8.5 Application Template.
   f. Open your existing GAX Application object.
   g. Click the **Options** tab.
   h. Click **Import** and specify the **CONF/CFG** file that you previously created from the GAX 8.5 Application Template. Select **No** to not overwrite any existing options.
   i. Click **Save & Close**.
3. (Optional) If you want to retain the installed plug-ins that you used with GAX 8.1.4, go to the GAX folder and back up the **webapp** folder by renaming it to **webapp_backup**.
4. 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.
5. Execute all applicable database upgrade scripts, if necessary. To determine if you have to apply any database scripts:
   a. Execute the following SQL statement on your existing GAX database: `select * from db_schema_version`.
   b. Compare the result with the update scripts in the **resources/sql_scripts** folder in the target directory of the installation.

   > **Important**
   >
   > The latest database schema versions are:
   >
   > - core—8.5.260.11
   > - asd—8.5.000.01
   > - opm-arm—8.1.301.01

Examples of upgrade scripts for Solution Deployment:

- (Oracle only) **gax_asd_upgrade_db_8.1.320.01_to_8.5.000.01_ora.sql**
- (Microsoft SQL only) **gax_asd_upgrade_db_8.1.320.01_to_8.5.000.01_mssql.sql**
- (PostgreSQL only) **gax_asd_upgrade_db_8.1.320.01_to_8.5.000.01_postgres.sql**

If you do not have the latest database schema versions, execute the scripts in the following order:
-1- Core
-2- Automatic Solution Deployment

-3- Operational Parameter Management

- 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 Deploy GAX Using Setup Mode (Existing Deployment).
- (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.
- To use the System Dashboard feature, you must set up a connection to Solution Control Server (SCS). Refer to the procedure "Add_SCS_Connection" in step 5 of Deploying Genesys Administrator Extension via Setup Mode for more information.
- If you backed up the **webapp** folder in Step 4 to **webapp_backup**, you must perform the following actions:

  a. Stop GAX.

  b. Copy the plug-in .jar files from **webapp_backup** to the new **webapp** folder in the GAX 9.0.* installation folder.

  c. Delete the **webapp_backup** folder.

  d. Start GAX.

Important

- Some plug-ins might require additional configuration. Refer to the plug-in documentation for more information about installing and configuring the plug-in.
- 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.

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.
- Database upgrade scripts 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 previous releases, 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;**

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 "'''home-'''" 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 Customer Care.

Accessing Genesys Administrator Extension

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

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 Security Deployment Guide* for information about using blank passwords.

Procedure: 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 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.

Steps

1. Start GAX.
2. Open a web browser.
3. 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.
4. 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 is displayed in the Header Bar of the Genesys Administrator Extension window. Select **About** in the Profile menu to see when you last logged in.

> **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.

5. 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 Security Deployment Guide* for more information about resetting passwords.

Logging In Remotely

Genesys Administrator Extension supports three types of remote logins, as follows:

- Customized Login Page
- Whitelisted Hosts
- Login API

The following three parameters specify to where the user is directed in the case of a successful or unsuccessful remote login, and logout. While not mandatory, you might want to define a list of trusted URLs to which these three variables can be set.

- `login_success_url`—Set this 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`.
- `login_failure_url`—Set this 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`.
- `logout_url`—Set this 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 login screen and the URL is appended with `#logout`.

Customized Login Page

Users can log in to GAX using 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:

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<script>
"use strict";
function logonGax(Form)
{
  var xhr = new XMLHttpRequest();
  xhr.open (Form.method, Form.action, true);
  xhr.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  xhr.setRequestHeader("Access-Control-Allow-Origin", "*");
  xhr.send (new FormData (Form));
}
</script>
</head>
<body>
```

```
<form id="logon" action="http://localhost:8080/gax/api/session/login" method="post"
onsubmit="logonGax(this)">
<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="https://localhost:8080/
gax/?#/!/view:com.cm.home/1">
<input type="hidden" name="logout_url" value="https://www.google.com">
<input type="hidden" name="login_failure_url" value="https://www.google.com">
<p><input type="submit" value="Submit"></p>
</form>
</body>
</html>
```

Whitelisted Hosts

If you have not done so already, define a list of one of more trusted hosts, called whitelisted hosts, to which these three variables can be set. Then in the **[security]** section, set the following options:

- **host_whitelist_enabled**=`true`
- **host_whitelist**=<semicolon-separated list of hosts specified by `login_success_url`, `login_failure_url`, and `logout_url`>

See more details about these two options here.

> **Important**
>
> The `host_whitelist` option is not meant for blocking/permitting IP addresses. It is only used for defining login, logout, and failure redirect URLs of GAX and not for individual IP addresses. If you want to restrict access to GAX URLs, Do it at System or Network level. Please consult your System or Network Administrator for the same.

Example

Using the same values used in the example above, assume the list of trusted hosts has been defined and assigned to the three variables, as follows:

- `login_success_url=https://localhost:8080/gax/?#/!/view:com.cm.home/1`
- `login_failure_url=https://www.google.com`
- `logout_url=https://www.google.com`

The option assignments would then be as follows:

```
[security]
host_whitelist_enabled=true
host_whitelist=https://localhost:8080/gax/?#/!/view:com.cm.home/
```

```
1;https://www.google.com;https://www.google.com
```

Login API

You can use a login API, such as:

Function:	Login (cross domain)
URL:	`/session/login`
Method:	POST
Content type:	`application/x-www-form-urlencoded`
Request Body:	`{ "username":"default", "password":"password", "newPassword": "password2", "newPasswordConfirm": "password2" "login_success_url": "http://xyz.com/success.html" "login_failure_url": "http://xyz.com/failure.html" "logout_url": "http://xyz.com/logout.html" }`

When calling the function, precede the URL with **http://<gaxserver>:<port>/api**.

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.

> **Important**
>
> This feature is deprecated starting from GAX 9.0.100.*.

To log in to Genesys Administrator from GAX, do the following:

1. Log in to GAX using your GAX credentials.
2. In the Profile menu, select **Genesys Administrator**. This menu option is visible only if you have the necessary permissions and privileges to access Genesys Administrator.
3. In the Genesys Administrator log in dialog box, enter your GAX credentials and click **Log in**.

Genesys Administrator is launched in a new browser tab or window. The content that is displayed depends on your privileges and access.

Note: 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.

Logging Out

To log out of Genesys Administrator Extension, click your user name in the Header Bar and select **Log Out**.

Starting and Stopping GAX

There are several ways to start and stop GAX, depending on your operating system.

Linux

Linux users can start and stop GAX by using one of the following methods:

- The System Dashboard in GAX.
- Genesys Administrator
- Solution Control Interface (SCI)

Refer to product-specific documentation for details on how to start and stop an Application.

Windows

Windows users can start and stop GAX by using one of the following methods:

- The System Dashboard in GAX.
- Genesys Administrator
- Solution Control Interface (SCI)
- Restarting the GAX Windows Service

Refer to product-specific documentation for details on how to start and stop an Application.

> **Important**
> You cannot use the GAX System Dashboard to stop the GAX instance you are currently using.

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 your User name in the Header Bar. 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 the following options:

- **Log Out**—Log out of Genesys Administrator Extension.
- User Preferences
- System Preferences
- **Set Current Page As Home**—Set the currently displayed page as the home page for your User account. Once set, this page is displayed each time that you log in to Genesys Administrator Extension.
- Change Password
- About—Click this option to view information about your installation. If your user account has the **Read Deployable and Undeployable IPs and SPDs** 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

In the **Advanced** window, you can specify the logging level for Genesys Administrator Extension JavaScript logging. You need to 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 Preferences 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, and should not be confused with Tomcat logs.

Configuration Manager

In the **Configuration Manager** window, you can set the following display preferences for Configuration Manager:

- **Show DBID**—When viewing details about a configuration object, also show the database ID.
- **Show Recent**—On the Configuration Manager homepage, show a list of configuration objects that you have recently accessed. This list displays the configuration object type and name (for example, `DNs`, `80708`), the Tenant to which the object belongs, and the last accessed date. Hover the mouse cursor over the item to see additional information, such as the specific date and time the object was accessed, and its path. You can click the item to access the object.
- **Maximum number of recent items to display**—Specify how many items to display in the **Show Recent** list.

Locale

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

Preference (field name)	Description
Language	The language to use in the GAX user interface. The default is **Use system settings**. You can add more language options by installing language pack plug-

Preference (field name)	Description
	ins. Important 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. 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 how many simultaneous requests are sent to Configuration Server, to minimize the risk of the server being overloaded. You can optimize these settings to help ensure consistent performance across your Genesys environment.

Bulk Update Batch Size specifies the maximum number of configuration updates that can be sent to Configuration Server 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). Valid values are `0` or any positive integer.

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

Bulk Update Batch Timeout specifies how long (in seconds) Genesys Administrator Extension should wait after sending one batch before sending the next batch. The default value is `1`. A value of `0` indicates that there will be no delay between bulk-update operations. Valid values are `0` to `300`.

Agent Management

In the **Agent Management** menu, you can choose whether the Agents window is displayed using the **Cloud** layout or **Premise** layout. For more information on the differences between these layouts, see Agents.

You can also set the following options for the **Add Agents** window:

- **Enforce User Name as E-mail Address**—If checked, GAX ensures that information entered in the **User Name** field is in the form of an email address.
- **Hide External ID**—If checked, GAX hides the **External ID** field when in the **Add Agent** window.
- **Default Access Group**—(Optional) The Access Group to which Agents are added when they are created in the Agents window. By default, this value is blank and Agents are not added to any Access Group.

> **Important**
>
> - If you enter the name of an Access Group that does not exist, GAX cannot assign Agents to the group. You must create the Access Group first.
> - Any value for this option does not apply when uploading Agents in bulk, since the Access Group is specified for each agent in the upload file.

Locale

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

Preference (field name)	Description
Language	The language to use in the GAX user interface. The default is **English (US)**. You can add more language options by installing language pack plug-ins. **Important** 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.

Change Password

You can change your password in the **Change Password** menu. You must have the **Modify User Password** privilege to change your password.

Genesys Administrator

Click this link 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 Security Deployment Guide* for more information about permissions and Role-Based Access Control, including how to set up appropriate permissions and role privileges.

Deployment Issues

Using Setup Mode

If you are unable to use GAX after you have used Setup Mode to deploy it, you probably encountered some interruption during the deployment. Any interruption in the Setup Mode process might result in only partial and incomplete configuration of your environment.

To resolve this, reset Configuration Server and the Configuration Database to their initial values. Stop any running Configuration Server processes. Then restart the deployment, using Setup Mode, from scratch.

Recommendation: When deploying GAX to an existing Management Framework deployment, make sure that the host property of the Configuration Server application is set.

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 entries:
  - **java.lang.OutOfMemoryError: Java heap space**
  - **java.lang.OutOfMemoryError: PermGen 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.

These errors are caused when the Java heap space or PermGen space is not large enough to support the current process.

The default size of the Java 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 one of the following, based on your operating system:

- On Linux, editing the **$CATALINA_HOME/bin/setenv.sh** file and adjust the memory file.
- On Windows, insert the following lines into the **JavaServerStarter.ini** file, creating the **[JavaArgs]** section line if necessary:

  ```
  [JavaArgs]
  -Xms2048m
  -Xmx4096M
  ```

  This file is used only by Windows Services and sets the starting parameters for GAX as a Windows Service.

To increase the PermGen space:

- Set the following field in the GAX start up file, **JavaServerStarter.ini**:
  `XX:MaxPermSize=512m`
- Change the following line in the **setenv.bat** script:

  ```
  Set JAVA_OPTS=%JAVA_OPTS% -server -XX:MaxPermSize=512m -XX:+CMSClassUnloadingEnabled
   -XX:+UseConcMarkSweepGC -XX:+HeapDumpOnOutOfMemoryError
  ```

If you continue to see these errors, continue to increase the heap or PermGen size 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) **Note:** Starting from Local Control Agent 8.5.100.31, Genesys Deployment Agent (GDA) is no longer installed and supported as part of Management Framework and therefore all functionality using GDA (including the installation of IPs) is deprecated.

Browser Issues

This section describes possible browser-related issues that you may encounter when deploying and using GAX.

Blocked Downloads in Internet Explorer 9

If you are using Microsoft Internet Explorer (IE) 9, an attempt to download Audio Resource Files, encoded files, and other GAX downloads might be blocked by the IE information bar. 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 IE settings. To prevent IE 9 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 IE 9 to allow all downloads without warnings
- Configuring IE 9 to allow GAX downloads without warnings

If you are using IE 10 or 11, the Windows Download Manager handles all download requests, and this problem does not occur.

Configuring IE 9 to allow all downloads without warnings

Thw following 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.

1. Launch Internet Explorer version 9.
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. Click **Enable** under **File download** and under **Font download**.
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.

Configuring IE 9 to allow GAX downloads without warnings

The following 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.

1. Launch Internet Explorer 9.
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. Click **Enable** under **File download** and under **Font download**.
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.

Audio Resource File Playback Issues in Internet Explorer and Firefox

Internet Explorer does not support playing an audio file directly. You must download the file and

playback the file locally. Firefox cannot play µ-law and A-law audio codecs. Only PCM Audio codecs can be played in Firefox.

Audio Resource File Playback Issue in Safari

Users of Safari cannot play Audio Resource files in Genesys Administrator Extension. This is because Safari does not support playing .wav files.

Role Privileges

This section 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, as follows:

- General
- GA Direct Login Integration
- Operational Parameter Management
- Solution Deployment
- Configuration Object Management
- Agent Management
- Bulk Operations
- Audio Resources Management-Tenant
- Audio Resources Management-System
- Centralized Logs

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

General

The following privileges apply to Genesys Administrator Extension.

Required Privileges

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.
Access Dashboard	Enables users to access the System Dashboard.
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 Default Dashboards	Enables users to edit the 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.
Save Widget	Enables users to save widgets. Important To save widgets in Pulse, users must have the required permission on their user account record in GAX. Use any of the following methods to enable permission: • Direct—In GAX, on the **Permissions** tab, add the user personal account record to the user's account records and then select both **Read** and **Update**. • Indirect—In GAX, on the **Permissions** tab, add at least one Access Group record to the user's account records and then select both **Read** and **Update**. The

	user must be a member of the selected Account Group.
Clone Widget	Enables users to clone a widget in any dashboard.
Remove Widget	Enables users to remove a widget from any dashboard.
Edit Tab	Enables users to edit the configuration in any dashboard.
Clone Tab	Enables users to clone a tab in any dashboard.
Delete Tab	Enables users to remove a tab from any dashboard.
Reset Tab	Enables users to reset a tab from any dashboard.
Add Tab	Enables users to add a tab to any dashboard.

GA Direct Login Integration

The following privileges apply to Genesys Administrator Extension.

Required Privileges

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.

Required Privileges

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.

Required Privileges

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.

Required Privileges

None

Role Privileges

Configuration Manager

[+] Click here to reveal section

> **Important**
>
> Unless otherwise specified, the following roles apply when using both Configuration Manager and Bulk Change Sets.

Access Configmanager	Allows a user to access Configuration Manager. Applies only when using Configuration Manager.
Access to the Application Log Configuration Wizard	Allows a user to access the **Configuration of Logging** window for configuration objects such as Applications, Hosts, and Solutions. Prerequisite: **Modify General Options and State of Applications**, **Modify General Options and State of Hosts**, or **Modify General Options and State of Solutions**.
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**. Applies only when using Bulk Change Sets. Important • The **Force Password Reset on Next Login** option appears only if Genesys

	Administrator Extension connects to Management Framework version 8.1.1 and above. • See the *Genesys 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**. Applies only when using Bulk Change Sets. Important This role privilege is available only in release 8.1.400.45 or later.
Modify User Password	Allows a user to access the **Change Password** option in the Profile 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. Applies only when using Bulk Change Sets.
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. Applies only when using Bulk Change Sets.
Write Agent Information	Allows a user to create and update all values on the User Accounts details pane for agents. Prerequisite: **Read Agent Information**. Applies only when using Bulk Change Sets.
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**. Applies only when using Bulk Change Sets.
Read Roles	Allows a user to only 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**. Applies only when using Bulk Change Sets.
Read Skills	Allows a user to only 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**. Applies only when using Bulk Change Sets.
Administer Agent Groups	Allows a user to access the **User Options** and **Access Control** buttons. Prerequisite: **Write Agent Groups**. Applies only when using Bulk Change Sets.
Read Agent Groups	Allows a user to only 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**. Applies only to Bulk Change Sets views.
Administer Access Groups	Allows a user to access the **User Options** and **Access Control** buttons. Prerequisite: **Write Access Groups**. Applies only when using Bulk Change Sets.
Read Access Groups	Allows a user to only 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**. Applies only when using Bulk Change Sets.
Administer Capacity Rules	Allows a user to access the **User Options** and **Access Control** buttons. Prerequisite: **Write Capacity Rules**. Applies only when using Bulk Change Sets.
Read Capacity Rules	Allows a user to only read Capacity Rules. The **User Options** and **Access Control** buttons are not displayed. Prerequisite: None. Applies only when using Configuration Manager.
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**. Applies only when using Bulk Change Sets.
Administer Bulk Change Sets	Allows a user to access the **User Options** and **Access Control** buttons. In addition, it allows the user to execute Bulk Change Sets. Prerequisite: **Read Bulk Change Sets**. Applies only when using

	Bulk Change Sets.
Read Bulk Change Sets	Allows a user to only read Bulk Change Sets. The **User Options** and **Access Control** buttons are not displayed. Prerequisite: None. Applies only when using Bulk Change Sets.
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**. Applies only when using Bulk Change Sets.

Access Groups

[+] Click here to reveal section

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.

Action Codes

[+] Click here to reveal section

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.

Agent Groups

[+] Click here to reveal section

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.

Agent Logins

[+] Click here to reveal section

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.

Alarm Conditions

[+] Click here to reveal section

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 Conditions	Allows a user to modify the general options and 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.

Alarm Scripts

[+] Click here to reveal section

Create/Full Control of Alarm Scripts	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 Scripts**.
Delete Alarm Scripts	Allows a user to delete Alarm Scripts. Prerequisite: **Read Alarm Scripts**.
Modify General Options and State of Alarm Scripts	Allows a user to modify the general options and state of Alarm Scripts. Prerequisite: **Read Alarm Scripts**.
Modify Options/Annex of Alarm Scripts	Allows a user to modify settings in the Options tab of Alarm Scripts and view the Permissions and Dependencies tabs. Prerequisite: **Read Alarm Scripts**.
Read Alarm Scripts	Allows a user to view Alarm Scripts in a list and access the object to view its details. Prerequisite: None.

Applications

[+] Click here to reveal section

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.

Application Templates

[+] Click here to reveal section

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.

Business Attributes

[+] Click here to reveal section

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.

Business Attribute Values

[+] Click here to reveal section

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.

Calling Lists

[+] Click here to reveal section

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.

Campaign Groups

[+] Click here to reveal section

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.

Campaigns

[+] Click here to reveal section

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.

Capacity Rules

[+] Click here to reveal section

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.

Configuration Units

[+] Click here to reveal section

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.

DN Groups

[+] Click here to reveal section

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.

DNs

[+] Click here to reveal section

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.

Fields

[+] Click here to reveal section

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.

Filters

[+] Click here to reveal section

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.

Folders

[+] Click here to reveal section

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.

Formats

[+] Click here to reveal section

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.

Hosts

[+] Click here to reveal section

Access Hosts Checkports	Allows a user to use the **Check Ports** feature for Host objects in Configuration Manager. Prerequisite: **Read Hosts**.
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.

IVR Ports

[+] Click here to reveal section

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.

IVRs

[+] Click here to reveal section

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.

Objective Tables

[+] Click here to reveal section

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	Allows a user to modify the general options and

Objective Tables	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.

Persons

[+] Click here to reveal section

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.

Place Groups

[+] Click here to reveal section

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.

Places

[+] Click here to reveal section

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** and **Create/Full Control of Places**.
Read Places	Allows a user to view Places in a list and access the object to view its details. Prerequisite: None.

Roles

[+] Click here to reveal section

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.

Scripts

[+] Click here to reveal section

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.

Sites

[+] Click here to reveal section

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.

Skills

[+] Click here to reveal section

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.

Solutions

[+] Click here to reveal section

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.

Statistical Days

[+] Click here to reveal section

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.

Statistical Tables

[+] Click here to reveal section

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.

Switches

[+] Click here to reveal section

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.

Switching Offices

[+] Click here to reveal section

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.

Table Accesses

[+] Click here to reveal section

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.

Tenants

[+] Click here to reveal section

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.

Time Zones

[+] Click here to reveal section

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.

Transactions

[+] Click here to reveal section

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.

Treatments

[+] Click here to reveal section

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.

Voice Platform Profiles

[+] Click here to reveal section

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.

Voice Prompts

[+] Click here to reveal section

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.

System Dashboard

[+] Click here to reveal section

Clear Active Alarms	Allows a user to clear active alarms in the **Alarms** tab of the System Dashboard.
Access Alarm Conditions Test	Allows a user to access the **Activate Alarm** function in the **Alarm Conditions** window. Prerequisite: **Read Alarm Conditions**
Start Applications	Allows a user to start applications by using the

	System Dashboard.
Stop Applications	Allows a user to stop applications by using the System Dashboard.
Switch Applications Mode	Allows a user to access the **Switch Mode** function when using the System Dashboard.
Start Solutions	Allows a user to start solutions by using the System Dashboard.
Stop Solutions	Allows a user to stop solutions by using the System Dashboard.

Agent Management

Agent Management role privileges control what tasks a user can perform in the **Agents** window of Genesys Administrator Extension.

Required Privileges

None

Role Privileges

Access to View Agents of other Tenants	Allows a user to view the **Tenant Directory** in the **Agents** window. By default, in a multi-tenant environment, users can only see Agents that belong to their Tenant. However, if users have this privilege and Read access to Agents of other Tenants, they can use the **Tenant Directory** to switch Tenants and view these Agents to which they have access. Prerequisite: **Read Agents in Agent Management**.
Create Agents in Agent Management	Allows a user to create Agents and copy Agents in the **Agents** window. Prerequisite: **Read Agents in Agent Management**.
Allow Skill Creation under Agent Management	Allows a user to create Skills when creating Agents in the **Agents** window. Prerequisite: **Modify Agents in Agent Management**. Important When you create a Skill in the **Add Agent** window, you also create a Virtual Agent Group with the same name as the Skill and all Agents that have this Skill are automatically assigned to this Virtual Agent Group.
Delete Agents in Agent Management	Allows a user to delete Agents in the **Agents** window. Prerequisite: **Read Agents in Agent Management**.
Modify Agents in Agent Management	Allows a user to modify Agents and copy Agents in the **Agents** window. Prerequisite: **Read Agents in Agent Management**.
Read Agents in Agent Management	Allows a user to view Agents in the **Agents** window.
Access Contextual Skill	Allows a user to access Contextual Skills. Prerequisite: **Read Agents in Agent Management**.
Create Skills under Contextual Skill	Allow a User to use the Contextual Skill Interface to

	create new Skills. Prerequisite: **Read Agents in Agent Management**.

Bulk Operations

Bulk Operations role privileges control what tasks a user can perform relating to Bulk Operations on Agents in Genesys Administrator Extension.

Required Privileges

Category	Privilege
Agent Management	Read Agents in Agent Management

Role Privileges

Administer User Bulk Operations	Allows a user to access History of Bulk Operations, and to delete completed or abandoned operations in the History.
Create User Bulk Operations	Allows a user to upload a spreadsheet, start or stop Bulk Operations, and access the History of Bulk Operations.
Export and Create Spreadsheet for User Bulk Operations	Allows a user to create or export a spreadsheet in .csv format for use when performing bulk creations and updates of Agents.

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.

Required Privileges

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.

Required Privileges

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.

Centralized Log

Centralized Log privileges control what level of logs a user can view in the **Centralized Logs** window of Genesys Administrator Extension.

Required Privileges

None

Role Privileges

Access Centralized Log messages	Allows a user to access (see) the Centralized Logs option in the GAX header.
Read Alarm Centralized Log messages	Allows a user to view all Alarm-level logs in the Centralized Log Database. **Prerequisite:** Access Centralized Log messages.
Read Centralized Standard Log messages	Allows a user to view all Standard-level logs in the Centralized Log Database. **Prerequisite:** Access Centralized Log messages.
Read Centralized Interaction Log messages	Allows a user to view all Interaction-level logs in the Centralized Log Database. **Prerequisite:** Access Centralized Log messages.
Read Centralized Trace Log messages	Allows a user to view all Trace-level logs in the Centralized Log Database. **Prerequisite:** Access Centralized Log messages.
Read Audit Centralized Log messages	Allows a user to view all Audit-type logs in the Centralized Log Database. **Prerequisite:** Access Centralized Log messages.
Delete Centralized Log messages	Allows a user to delete logs in the Centralized Log Database. **Prerequisite:** Access Centralized Log messages.

Configuration Options

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

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 **Genesys Administrator 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.

confserv_trusted

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: Immediately

Specifies if token-based authentication is used for secure communication with 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`.

disableCLOG

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: Dynamic

Specifies if Angular JS loading should be prevented in the browser. By default, this value is set to `true`.

disable_change_password

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: After browser refresh

Specifies if **Change Password** appears in the **default** menu of GAX. By default, **Change Password** appears on GAX unless this option is set to `true`.

enable_bulk_change_sets

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: After browser refresh

Specifies if **Bulk Change Sets** feature appears in the **Administration** menu of GAX. If set to `false` (the default) or not configured, the feature does not appear in any menu and cannot be used.

help_external_url

Default Value: `docs.genesys.com`
Valid Values: Any reachable website domain or IP address (do not include `http://` prefix). You must include a port number after the address. For example: `docs.mycompany.com:4001`
Changes Take Effect: After page refresh

Specifies the location of Genesys Administrator Extension Help content—either the Genesys Documentation website (docs.genesys.com) or an internal company server for those that have installed the offline documentation package.

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

quick_filter_only_on_enter

Default Value: false
Valid Values: true, false
Changes Take Effect: After browser refresh

Specifies if the quick filters search starts only when the user presses **Enter**.

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. A value of zero (0) specifies no reconnection attempts. A negative value 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.

search_person_required_field_choices

Default Value: Not Applicable
Valid Values: NAME_NUMBER, FIRST_NAME, LAST_NAME, EMPLOYEE_ID
Changes Take Effect: After Genesys Administrator Extension is restarted

Specifies the mandatory fields for the Person objects to avoid blank search in search page. This is an optional parameter.

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 which the session will be destroyed if there is no activity for that session. The value of this option must be greater than or equal to **inactivity_timeout**.

skill_assignment_max_agent_updates

Default Value: -1
Valid Values: Any integer value
Changes Take Effect: After browser refresh

Set the maximum number of agents that the user can select when using the **Edit Skills** operation. A warning message is shown if the user exceeds this selection limit. The value -1 indicates that there is

no limit.

skill_assignment_max_skill_updates

Default Value: `-1`
Valid Values: Any integer value
Changes Take Effect: After browser refresh

Set the maximum number of agent skill changes that the user can perform when using the **Edit Skills** operation. A warning message is shown if the user exceeds this changes limit. The value `-1` indicates that there is no limit.
The following actions count towards the number of changes:

- Assigning a new skill to the selected agents
- Removing an existing skill to the selected agents
- Changing the Rating value of the assigned skills
- Applying the skill that has been assigned to some of the selected agents to all the selected agents (Changing the checkbox from minus symbol to checked state)

token_life_in_minutes

Default Value: `1440`
Valid Values: Any positive integer value
Changes Take Effect: Immediately.

Specifies the life of the password token used in token-based authentication. Genesys recommends that you use the default value, unless you have an overriding reason.

validate_data

Default Value: `none`
Valid Values: `string`, `none`
Changes Take Effect: After browser refresh

Specifies whether to validate the input data before storing into the configuration database. This validation is enabled only when this option is set to `string`.

security Section

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

The options in this section relate to security features in Genesys Administrator Extension.

enable_un_cookie

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: After restart

Specifies if the encrypted usernames are stored in the browser cookies. If set to `true`, GAX stores the encrypted username in browser cookies for a period of 30 days. If set to `false`, GAX does not store the username in the browser cookies and it also removes the existing username (un) cookies.

host_whitelist

Default Value: Empty
Valid Values: URLs of hosts trusted by this GAX instance, separated by semi-colons (`;`); for example `132.56.54.34;host1;34.32.12.8`
Changes Take Effect: After restart

Specifies the host URLs that can be whitelisted. This option only takes effect when **host_whitelist_enabled** is set to `true`.

host_whitelist_enabled

Default Value: `false`
Valid Values: `true`, `false`
Changes Take Effect: After restart

Specifies if host whitelisting is enabled in GAX. If this option is not set or set to `false` (the default), then host whitelisting is disabled and all hosts are allowed by GAX.

If set to `true`, only those hosts specified in the option **host_whitelist** can appear as:

- values of the parameters **logout_success_url**, **logout_failure_url**, and **logout_url** when logging in remotely
- list of hosts from which to select **UNC Path to Mounted CD or Directory**, **UNC Path to an Existing Administrator Repository**, and **UNC Path to Zipped IPs** when uploading IPs.

asd Section

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

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

new_arf_name_format
Default Value: `false`
Valid Values: `false`, `true`
Changes Take Effect: After restart of GAX

> **Warning**
> Use this option with extreme caution.

Starting in release 8.5.240, this option specifies the number of digits in personality IDs, and therefore, how many personalities can be created. If this option is not set or is set to false (the default), the IDs are 2 digits long and allow for a maximum of only 99 personalities. This is existing behaviour.

When this option is set to true, the IDs are 3 digits long and allow for a maximum of 1000 personalities. This setting should be used only if you want to use more than 99 personalities. Otherwise, Genesys strongly suggests that you not use this option.

> **Important**
> This option applies only to single-tenant configurations. Multi-tenant configurations support only 20 personalities per tenant because of the way routing engine interprets Audio Resource IDs (ARID).

delete_from_db_after_processing
Default Value: `false`
Valid Values: `false`, `true`
Changes Take Effect: Immediately

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: Immediately

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: Immediately

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: Immediately

Specifies the absolute path to the location of local audio storage, that is, to the folders specified by the options local_announcement_folder and local_music_folder. The value must not be the same as that of target_path.

local_sox_path
Default Value: `/usr/bin/sox`
Valid Values: Any valid path
Changes Take Effect: Immediately

Specifies the absolute path to the SoX binary (executable) file; for example, **C:\GCTI\sox\sox.exe** on Windows.

max_upload_audio_file_size
Default Value: `20`
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the maximum file size, in megabytes, for audio files that are uploaded to GAX.

target_announcement_folder
Default Value: `announcement`
Valid Values: Any valid folder name
Changes Take Effect: Immediately

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: Immediately

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: Immediately

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). The value must not be the same as that of local_path.

ga Section

> **Important**
> This feature is deprecated starting from GAX 9.0.100.*.

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

> **Important**
>
> Starting from GAX 9.0.100.xx release, there is a minor change in the GAX log naming convention and rollover pattern as explained in the below example. Note that the **expire** option set to 2 in this example.
>
> - All log messages are written in the initial file, **gax.log.<timestamp>**.
> - During the first rollover, the **gax.log.<timestamp>** file is renamed to **gax.log.<timestamp>-1**. A new **gax.log.<timestamp>** file is created and all the log messages generated after creating the new file are written in this new log file.
> - During the second rollover, the **gax.log.<timestamp>** file is renamed to **gax.log.<timestamp>-2**. A new **gax.log.<timestamp>** file is created and all the new log messages are written in this new log file.
> - In the third and subsequent rollovers, the **gax.log.<timestamp>-1** file is deleted, **gax.log.<timestamp>-2** is renamed to **gax.log.<timestamp>-1**, and a new **gax.log.<timestamp>** file is created. All the new log messages are written in the new log file.

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. Setting the `Standard` log level option to the network output enables an application to send log events of the `Trace` level also to the Message Server.
`[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 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: `standard`
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.

Value	Description
`standard`	The same as `interaction`.
`none`	No output is produced.

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`.

clog Section

This section contains configuration options for configuring the display of log records from the Centralized log.

maxlogs

Default Value: 5000
Valid Values: Any positive integer starting at 5000
Changes Take Effect: After the browser page is refreshed

Specifies the maximum number of log records that can be displayed in GAX. When the user scrolls down or pages through to the end of the list, GAX displays a message suggesting that the user refine the search criteria to get better results. If this option is not set or set to a value less than 5000 (the default), the default is used. When used with the minlogs option, the rules in the following table might apply:

Configured Values	Value used for maxlogs	Value used for minlogs
minlogs < 5000 **maxlogs** < 5000 **minlogs** > **maxlogs**	5000 or the configured value of **maxlogs**, whichever is greater	100 or the configured value of **minlogs**, whichever is greater
minlogs >= 5000 **maxlogs** >= 5000 **minlogs** > **maxlogs**	Configured value of **minlogs**	Configured value of **minlogs**

minlogs

Default Value: 100
Valid Values: Any positive integer starting at 100
Changes Take Effect: After the browser page is refreshed

Specifies the number of log records that are to be retrieved from the Centralized Log Database when the user scrolls down or pages through the list of logs. If not set or set to a value less than 100 (the default), the default is used. When used with the maxlogs option, the rules in the table above might apply.

com Section

exclude_clone

Default Value: `provisioning_flags`
Valid Values: One or more names of valid configuration option sections, separated by a comma
Changes Take Effect: After browser refresh.

Specifies the configuration option sections that are not to be copied to new objects during the cloning process, regardless of object type.

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"`).

Using Single Sign On (SSO)

Important

- This feature might not be available to all customers.
- The activity-based SLO feature is not supported. Therefore, use the `saml_landingpage` property in the **gax.properties** file to configure the logout URL.
- Once SSO is enabled and after logging into GAX, the Change Password link may not work. You can manage the user passwords in the IdP-based user account directory.
- For releases prior to 9.0.100.56, when configuring SSO for GAX where token-based authentication is used, if the name of the Configuration Server application object is different than **confserv**, add a new section with the name **confserv** under Application Options of the Configuration Server object and then copy the **database-guid** option with its value and paste it under the newly created **confserv** section. After this change, restart GAX.
- Token-based authentication must be enabled as described in Secure Communication with Configuration Server.
- If you are using GAX version 9.0.100.72 or above for SSO and prefer to use the below JKS parameters additionally, follow the procedure provided in Including Additional JKS Parameters for SSO to add them using root login and continue with the Enabling SSO procedure.
  - `saml_jkspassword`
  - `saml_signingkeyname`
  - `saml_signingkeypassword`

You can set up Genesys Administrator Extension to use Single Sign On (SSO), so that users can use existing credentials (for example, a corporate login and password) to access GAX. When these users log out of GAX, they are simultaneously logged out of other SSO-supported applications.

GAX uses SAML2 to enable SSO.

By default, SSO is not enabled in GAX. To enable this feature, refer to the following procedure.

Enabling SSO

Procedure:

Steps

1. On the host machine, open the *GAX_HOME* folder (the folder in which you installed GAX) and create a sub-folder called **saml**.
2. Open the **saml** folder and create a sub-folder called **sp**.
3. Access the metadata file from the IdP (identity provider). Open the gax.properties in the **GAX_HOME/conf** folder and set the following values:
   - saml = `true`
   - session_securecookies = `true`
   - cookie_samesite = `None`
   - Set the **saml_idp_metadata** option to one of the following:
     - *http://location*—The web location of the IdP metadata file.
     - *filename*—The path and file name of the IdP metadata file of the local machine.
4. Perform one of the following to download the Service Provider metadata file from GAX:
   - For GAX version 9.0.107.04 (or lower), use the following URL to download the metadata: *http://host:port/gax/saml/metadata*, where *host:port* is the IP name and port number for the GAX installation.
   - For GAX version 9.0.108.03 (or higher), use the following URL to download the metadata: *http://host:port/gax/saml2/service-provider-metadata/default*, where *host:port* is the IP name and port number for the GAX installation.

   > **Important**
   > - You must use the host name or IP address to access the metadata file. You cannot specify **localhost**.
   > - If you have already configured SSO and you are upgrading to GAX version 9.0.108.03 (or higher), do the SSO setup completely once again after the upgrade.

5. Copy the downloaded metadata file, **sp.xml**, to the following folder on the host machine:

GAX_HOME\saml\sp.

6. Upload the **sp.xml** metadata file to the IdP server. The following is an example of a typical location on the IdP server: */home/ubuntu/idp/metadata/my_sp.xml*.
7. Log in to the IdP server and edit the **conf/relying-party.xml** file by adding the following metadata provider:

```
   <metadata:MetadataProvider id="uniqueID"
xsi:type="metadata:FilesystemMetadataProvider"
       metadataFile="/home/ubuntu/idp/metadata/my_sp.xml"
   maxRefreshDelay="P1D" />
```

> **Important**
>
> You must use a unique ID for **metadata:MetadataProvider id**.

8. Restart the IdP server.
9. On the host machine, edit the gax.properties file in the *GAX_HOME* folder and specify options for the following properties:
   - `saml=true`
   - `saml_entityid`—Your unique ID for IdP. This is the same ID specified in **relying-party.xml**.
   - `saml_idp_metadata=saml/idp-metadata.xml`
   - `saml_landingpage`—The SSO landing page.

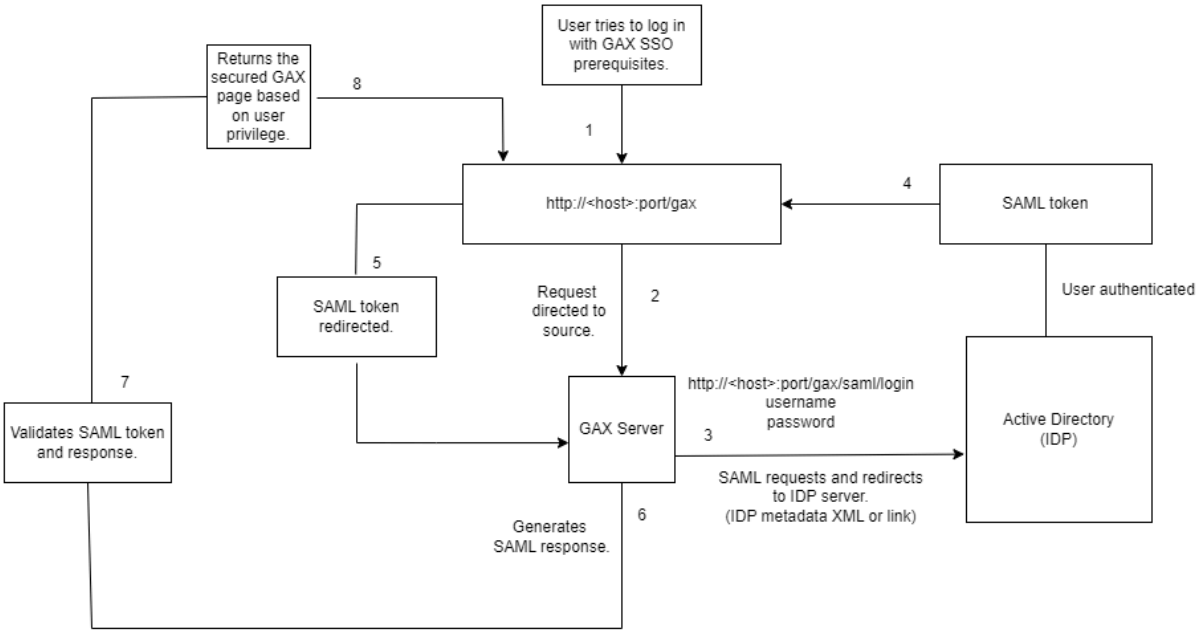
> **Important**
>
> The following options are not mandatory to enable SSO in GAX. However, if you prefer to use customized Java Keystore file instead of the default JKS, these options can be added to the gax.properties file.

   - `saml_jksfilelocation`—The location/path of the custom Java KeyStore (.jks) file. If this is not configured, the JKS file in the classpath is used.
   - `saml_jkspassword`—The custom KeyStore password. It is required when the `saml_jksfilelocation` option is set for a custom JKS file.
   - `saml_signingkeyname`—The custom key file name. It is required when the `saml_jksfilelocation` option is set for a custom JKS file.
   - `saml_signingkeypassword`—The custom key file password. It is recommended to set the same password as `saml_jkspassword` and it is an optional parameter.
10. Restart GAX.

Important

If SSO is enabled, but the metadata of the Service Provider (GAX) or IdP is incorrect, GAX logs the error and directs the user to the non-SAML login page.

The following diagram shows how a user is authenticated with SSO in GAX.



Including Additional JKS Parameters for SSO

If you want to use additional JKS parameters for SSO, follow the below procedure.

Procedure:

Steps

1. Create a backup of gax.properties file (`gax_bkp.properties`).
2. Empty the gax.properties file.
3. Start GAX. Access GAX in the same machine where it is installed using the url: http://localhost:8080/gax/
4. Log in as a root user. Password is not required for this login.

> **Important**
> Do not close the browser tab until all the parameters are added.

5. Access http://localhost:8080/gax/api/system/generategaxkey in another browser tab. This creates the `gax_store.txt` file in the `conf` folder.
6. Access the below APIs to add encrypted parameters in the gax.properties file:
   http://localhost:8080/gax/api/system/setsamljkspassword?password=<PASSWORD>
   http://localhost:8080/gax/api/system/setsamlsigningkeyname?name=<NAME>
   http://localhost:8080/gax/api/system/setsamlsigningkeypassword?password=<PASSWORD>
7. Add the existing parameters from the backup file `gax_bkp.properties` to gax.properties file and save it.
8. Now, follow the steps provided in the Enabling SSO section to enable the SSO feature.