Genesys Administrator Extension Migration Guide

Prerequisites

4/21/2025

Contents

Prerequisites

Before upgrading Genesys Administrator Extension, you must ensure that your system meets the prerequisites described in this section.

Management Framework

You must be running Management Framework 8.1.0 or later to support GAX.

If you are currently running a release of Management Framework earlier than 8.1.0, refer to Management Framework documentation to upgrade to the required release of Management Framework.

Computing Environment Prerequisites

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

- Red Hat Enterprise Linux 5.5 (64-bit) - Enterprise Edition, with Updates from RHN enabled
- Red Hat Enterprise Linux 6.0 (64-bit) - Enterprise Edition, with Updates from RHN enabled
- Red Hat Enterprise Linux 7.0 (64-bit) - Enterprise Edition, with Updates from RHN enabled

Or,

- Windows Server 2008 R2, with 64-bit applications running natively on a 64-bit operating system
- Windows Server 2012, with 64-bit applications running natively on a 64-bit operating system

The computer must also run the following:

- Java 8 Runtime (JRE) from Oracle. See the Genesys Administrator Extension Deployment Guide for information about obtaining and installing Java, if necessary.

> **Important**
>
> JDK 1.8 is mandatory to install GAX 9.0.x. For more information on recommended JDK versions, see the *Supported Operating Environment Guide* for Genesys Administrator Extension.

Starting in GAX 8.1.4, GAX uses an embedded Jetty instance as the web application server; as a result, Tomcat is no longer a prerequisite to use GAX. For those who choose to use Tomcat instead of

Jetty, GAX requires Tomcat 6.0.37 (or a later version from the Tomcat 6.0.x branch) or Tomcat versions 7 or 8. Refer to Genesys Administrator Extension Migration Guide for additional information. For information on how to deploy GAX into Tomcat 8, see Deploying GAX into Tomcat 8.

In addition, each module of Genesys Administrator Extension might have additional prerequisites. Refer to the Genesys Administrator Extension Deployment Guide for more information.

Browser Requirements

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

- Microsoft Internet Explorer 9.x, 10.x, 11.x
- Mozilla Firefox 17 or higher
- Safari 6, 7, or 8, on Macintosh systems
- Chrome

Genesys Administrator Extension supports all major browsers, but it is optimized for Chrome. If you use Microsoft Internet Explorer or Safari, refer to the Genesys Administrator Extension Deployment Guide 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.

Required Permissions and Role Privileges

Genesys Administrator Extension uses a permission-based mechanism and a role-based access control system to protect your data. After installing (but before using) Genesys Administrator Extension, ensure that all GAX users have the necessary access permissions and role privileges to do their work.

At a minimum, each GAX user requires the following permissions to log in to GAX:

- Read permission for his or her own object, preferably for the main folder in which he or she resides (for example, the Persons folder).
- Read permission for the tenant to which he or she belongs to.
- Read and Execute permission for the Configuration Server application object, usually named **default**.

There are no role privileges required to log in to GAX. However, without any role privileges, a user is unable to see anything in GAX after he or she has logged in. You must assign to the user specific role privileges to access and work with configuration objects and to perform GAX-specific functions. Refer to product-specific documentation for role privileges specific to the product. For GAX functions, refer to the chapter "Role Privileges" in the *Genesys Administrator Extension Deployment Guide*.

Note: When upgrading the GAX template and metadata, new and changed role privileges are

automatically updated in the system. Be sure to review the role assignments in your upgraded configuration to ensure that they are appropriate, modifying them as necessary with the updated privileges.

Deploying Multiple Instances of GAX with Shared Resources

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

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

Minimum Required Firewall Permissions and Settings for GAX Deployment

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

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

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

> **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 have the following permissions:

- Write permission on the log file folder
- Read/Write access to the folder configured for ARM (Audio Resource Management)

Enabling UTF-8 Encoding (for Oracle Databases)

Genesys Administrator Extension optionally supports UTF-8 character encoding for Oracle databases. This functionality requires Configuration Server 8.1.2 or later. For more information, refer to the Genesys Administrator Extension Deployment Guide.

Deploying GAX into Tomcat 8

This section provides information on how to deploy GAX into Tomcat 8. Note that Tomcat 8 runs only with JDK 1.7. For more information on recommended JDK versions, see the *Supported Operating Environment Guide* for Genesys Administrator Extension.

1. Create a **conf** folder under the **<TOMCAT_HOME>/bin directory**.
2. Within the **conf** directory, create **gax.properties**.
3. Open **<TOMCAT_HOME>/conf/tomcat-users.xml**.
4. Add the following users and roles in **<TOMCAT_HOME>/conf/tomcat-users.xml** under the **<tomcat-users>** tag.

```
<role rolename="manager" />
<role rolename="manager-gui"/>
<role rolename="manager-script" />
<role rolename="manager-status" />
<user username="manager" password="password" roles="manager"/>
<user username="manager" password="password" roles="manager-gui"/>
```

Configuring Tomcat server.xml

Open **<TOMCAT_HOME>/conf/server.xml** and configure the following connector and comment the existing connector if it is configured.

For non-SSL GAX

```
<Connector port="8080" protocol="org.apache.coyote.http11.Http11Protocol"
connectionTimeout="20000" redirectPort="8443" URIEncoding="UTF-8" />
```

For SSL GAX

Ensure to set GAX in SSL mode as instructed in the Configuring System Security page, before you proceed further.

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150" scheme="https"
secure="true" sslProtocol="TLS" keystoreFile="<keystore_file_path>"
keystorePass="<keystore_password>" clientAuth="false" />
```

Deploying And Starting GAX

Important

Tomcat server has WAR file size maximum limitation of 50MB which is defined in the **<$tomcat_dir>\webapps\manager\WEB-INF\web.xml** file. Before deploying GAX WAR into Tomcat server as a 'manager' user, increase the WAR size limit by replacing the below content in the **<$tomcat_server>/webapps\manager\WEB-INF\web.xml** file.

```
<multipart-config>
<max-file-size>92428800</max-file-size>
<max-request-size>92428800</max-request-size>
<file-size-threshold>0</file-size-threshold>
</multipart-config>
```

1. Start Tomcat by running **startup.bat** under **<TOMCAT_HOME>/bin**.
2. Go to http://*hostname* (for SSL: https://*hostname*).
3. Click the **Manager App** and log in as manager.
4. Scroll down and click **Deploy** and browse **gax.war**.
5. Click **Deploy**.
   After the GAX WAR is deployed, GAX is displayed in the list.
6. After installing GAX, copy the **log4j2.xml** file from **<$tomcat_DIR>/webapps/gax/WEB-INF/classes/log4j2.xml** to the **<$tomcat_DIR>/bin/conf/log4j2.xml** folder.
7. Restart Tomcat.
8. Log in to GAX.