



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

Setting Up Genesys Administrator Extension

5/4/2025

Setting Up Genesys Administrator Extension


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

This chapter contains the following sections:

- [Overview](#)
- [Deploying Genesys Administrator Extension](#)
- [Prerequisites for Genesys Administrator Extension Modules](#)
- [Configuring System Security](#)
- [Configuring the Auditing Feature](#)
- [Managing GAX Compatible Plug-ins](#)
- [Upgrading GAX](#)
- [Customizing the GAX Homepage](#)
- [Cleaning the GAX Database After a Tenant is Deleted](#)

Overview


Genesys Administrator Extension is deployed on 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.


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

Prerequisites

Before you deploy Genesys Administrator Extension, you should review the planning information in the [Framework 8.1 Deployment Guide](#). This will help you to deploy Genesys Administrator and other components of the Framework in a manner that is most appropriate to your situation.

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

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

 **Note:** To avoid issues with role assignments, you should upgrade the application, metadata, and the roles to the new type when you migrate to GAX 8.1.2 or perform a fresh install (see [Upgrading to the latest Genesys Administrator Extension for Management Framework 8.1.1 or higher](#))

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

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

Or,

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


- Java 6 Runtime (JRE) from Oracle. See the [Setting up the host for Genesys Administrator Extension server](#) for information about obtaining and installing Java, if necessary.
- Tomcat 6.0.37 from Apache. When setting up Tomcat, Genesys strongly recommends that you enable gzip compression for responses. Follow the procedure [Installing Tomcat](#).

In addition, each module of Genesys Administrator Extension might have additional prerequisites. Refer to [Prerequisites for Genesys Administrator Extension Modules](#) 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 8.x or 9.x
- Mozilla Firefox 5 or higher
- Safari 5 or higher
- Chrome 8 or higher

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

Genesys Administrator Extension is designed to be viewed at a minimum screen resolution of 1024x768, although higher resolutions are recommended. If you are working in 1024x768 mode, maximize your browser to ensure that you can see all of the interface. In addition, all windows of the browser must be set to a resolution of 1024x768 or greater.



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

Required Permissions and Role Privileges

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

- A tenant user must have write (Update) permission on his or her User object to set and save his or her user preferences in Genesys Administrator Extension.
- To log in to Genesys Administrator Extension, a user must have Read permission on his or her User object, Read and Execute permissions on his or her Tenant object, and Read and Execute permissions on the Genesys Administrator Extension client Application object. These permissions are usually assigned by adding the users to access groups.

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

Deploying Multiple Instances of GAX with Shared Resources

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

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

Minimum Required Firewall Permissions and Settings for GAX Deployment

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

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

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

Minimum Required File System Permissions and Settings for GAX Deployment

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

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



Note: If Tomcat was extracted from the .tar file, the operating system user would already have these permissions.