Genesys Administrator Extension Deployment Guide

Setting Up Genesys Administrator Extension

5/5/2025

Contents

- 1 Setting Up Genesys Administrator Extension
  - 1.1 Overview

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

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