Genesys Administrator Extension Deployment Guide

Deploying Genesys Administrator Extension

4/15/2025

Deploying Genesys Administrator Extension

The following table summarizes the steps necessary to perform the basic deployment of Genesys Administrator Extension. Before beginning your installation, make sure 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.

> **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 $).

Deploying Genesys Administrator Extension

1. Create and configure the configuration objects required for Genesys Administrator Extension.

Creating the necessary configuration objects for Genesys Administrator Extension

Purpose

To create the following configuration objects required by Genesys Administrator Extension:

- `Host` object for the computer on which Genesys Administrator Extension is to be installed (Step 1)
- `Host` object for the computer on which the database to be used by Genesys Administrator Extension will be located (Step 2)
- `Database Access Point` to provide database access to the database used by Genesys Administrator Extension (Step 3)
- `Application` object for Genesys Administrator Extension with a connection to Configuration Layer to retrieve configuration information (Step 4)
- `Application` object to provide the capability to log in to Genesys Administrator Extension (Step 5)

Important

- All tasks in this procedure are completed by using Genesys Administrator or a similar configuration utility to create the necessary configuration objects in the Configuration Database. This procedure assumes that you are using Genesys Administrator.
- In this procedure, use the instructions that are provided in Genesys Administrator 8.1 Help or the Framework 8.1 Deployment Guide, and add the object-specific configuration requirements listed here.

Prerequisites

- Management Framework 8.0.0 or higher is installed and running. You must have Configuration Server 8.0.300.42 or higher.
- If you are using Configuration Server 8.1.1 or higher, you must use Genesys Administrator 8.1.2 or higher, as previous versions do not support the GAX application type for configuring role privileges.
- Genesys Administrator 8.1 or higher is installed and running.

Start

1. Create and configure a `Host` object for the computer on which Genesys Administrator Extension will be installed, as follows:
   a. Use the instructions in Genesys Administrator 8.1 Help or the Framework 8.1 Deployment Guide to create and configure a `Host` object.
   b. On the `Configuration` tab, specify a Solution Control Server `Application` object.
   c. Click Save `&` `Close` to save the new object and its configuration.

4. Use the instructions in Genesys Administrator 8.1 Help or the Framework 8.1 Deployment Guide to create and configure a `Host` object for the computer on which the database to be used by Genesys Administrator Extension will be installed.

Important

When using Genesys Administrator in a load-balanced environment, make sure that all nodes have shared-access to the application metadata. See the Framework 8.1 Genesys Administrator Deployment Guide for details about how to set this up.

5. Use Genesys Administrator to create and configure a Database Access Point (DAP) `Application` object, which is necessary for connectivity to the database that will be used by Genesys Administrator

Extension, as follows:

a. Use the instructions in the Framework 8.1 Deployment Guide to create and configure a DAP Application object.

b. Open the Configuration tab.

c. In the Server Info section, enter the following information:

i. In the Tenants list, add the Environment Tenant.

ii. In the Host field, select the Host object on which the database is to be installed, and that was configured in Step 2. If you do not use a non-standard port, enter 1521 for an Oracle database, 1433 for a Microsoft SQL Server 2008 database, or 5432 for a PostgreSQL database.

c. In the DB Info section, enter the following:

i. In the Connection Type field, select JDBC.

ii. In the Role field, select Main.

iii. In the Debug field, select false.

iv. In the JDBC Query Timeout field, enter 15.

v. In the DBMS Type field, select Oracle for an Oracle database, mssql for a Microsoft SQL Server 2008 database, or postgre for a PostgreSQL database.

vi. In the Database Name field, enter the Solution name of the database instance.

vii. In the User Name field, enter the user name required to access the database.

viii. In the User Password field, enter the password required for the user name specified in the previous step to access the database.

ix. In the Case Conversion field, select any.

j. Open the Options tab and complete the following steps:

i. Create a new section called GAX.

ii. In this new section, add the configuration option role and set its value to main. This identifies this DAP as the one for the main database that is used by Genesys Administrator Extension.

c. Click Save & Close to save the new object and its configuration.

4. Create and configure a Server Application object for Genesys Administrator Extension, as follows:

a. Import the Application Template object for Genesys Administrator Extension. Refer to Genesys Administrator 8.1 Help for detailed instructions.

i. Upload one of the following files from the installation package, depending on which version of Management Framework you are running:

- For Configuration Server up to version 8.1.0: Genesys_Administrator_Extension_MF810_813.apd
- For Configuration Server from version 8.1.1 on: Genesys_Administrator_Extension_813.apd

- Import the XML metadata file, which contains the GAX privilege information and default settings, by clicking Import Metadata, then navigate to the folder in which the application template was deployed. There are two templates available, depending on which version of Management Framework you are running:

  - For Configuration Server up to version 8.1.0: Genesys_Administrator_Extension_MF810_813.xml

  - For Configuration Server from version 8.1.1 on: `Genesys_Administrator_Extension_813.xml`

- Click `Save & Close` to save the new object.
- Use the instructions in the Framework 8.1 Deployment Guide to create and configure an `Application` object by using the template imported in the previous step and on the `Host` object configured in Step 1. This new object will appear as being of type `Generic Genesys Server` if you are running Management Framework <=8.1.0 and of type `Genesys Administrator Server` if you are running Management Framework >8.1.0.
- Open the `Configuration` tab.
- In the `General` section, in the list of `Connections`, add connections to the following components:
  - Primary Solution Control Server
  - Main DAP (configured in Step 3)
  - Auditing DAP. This should be linked to the database where the auditing data will be written. The configuration (refer to Step 3) is the same as the Main DAP; however, the Role property of the Auditing DAP should be set to the value `auditing` instead of the value `main`.

    > **Important**
    >
    > Both the Auditing DAP and the LRM DAP are not mandatory for every installation. If you configure GAX to use auditing, then you must have a DAP configured. If you remove the LUR from the installation, the DAP is not required.

  - LRM DAP. This should be linked to the database that will hold the LRM data that is displayed by License Usage Reporting. The configuration (refer to Step 3) is the same as the Main DAP; however, the Role property of the LRM DAP should be set to the value `lrm` instead of the value `main`.

> **Important**
>
> In GAX 8.1.310 releases or higher, License Usage Reporting functionality is provided by the License Reporting Manager (LRM) plug-in for GAX.

- In the `Server Info` section, enter the following information:
  i. In the `Working Directory` field, enter the path to your working directory.
     - (Linux) For example: `/home/gcti/apache-tomcat-6.0.37/bin/`.
     - (Windows Server) For example: `C:\GCTI\Tomcat6_GAX_812\bin`
  ii. In the `Command Line` field, enter the following:
     - Linux:`./gax_startup.sh`
     - Windows Server:`.\gax_startup.bat`

iii. In the Command Line Arguments field, enter the following (all on one line):

```
-host <Configuration Server name or IP address> -port <Configuration Server port> -app <GAX
Generic Server Application name>
```

where the values in <brackets> are replaced by the values used by your deployment.

> **Important**
>
> **Limitation:**
>
> If Configuration Server has several independent ports configured, the port that GAX should use cannot be freely chosen if GAX is started by Management Framework tools such as Solution Control Server, Genesys Administrator, or Solution Control Interface. In that case GAX will always connect to the port that Solution Control Server uses to connect to Configuration Server.
>
> **Workaround:**
>
> If GAX should not use the same Configuration Server port as Solution Control Server, GAX should not be started by using Management Framework tools. GAX should only be started manually or as a service.

- Select the host object where GAX is to be deployed.
- Specify the listening port by entering 8080 (the typical value for Genesys; you can also specify another port) in the Listening Port field.

> **Important**
>
> Setting this port value does not change the port that is used by GAX; it is overridden by the Tomcat configuration.

- On the Options tab, verify or update the name of your client object (to be created in Step 5) given by the following option:

```
general.client_app_name=<name>
```

- Click Save & Close to save the new object and its configuration.

> **Important**
>
> The creation of a client is optional. The default client will be used in a standard installation, such as cases in which

> `general.client_app_name` is set to `default`. Perform the next step only if you need to allow access to GAX for users that should not be able to access Genesys Administrator.

- Create and configure an `Application` object to allow users to log in to Genesys Administrator Extension. The name of this object must be exactly the same as that specified in Step 4h above. All users must have Read and `Execute` permissions for this `Application` object.

  Use the instructions in the Framework 8.1 Deployment Guide to create and configure an `Application` object of type `Configuration Manager` based on the `Configuration Manager Application Template`.

  This object acts as a client application for the Genesys Administrator Extension server.

- Configure GAX logging by using the Genesys Log Wizard from Genesys Administrator or from the Genesys Solution Control Interface. The Log Wizard creates a set of configuration options in the `log` section of the GAX Server application object.

  (Optional) You can also create the log options manually by using the values in the table below.

GAX Logging value

Option	Description	Value	Required	Default
all	Defines the types of logging to be executed as a comma-separated list	stdout, <filename>	Yes	stdout
verbose	Defines the log level	all, trace, interaction, standard, none	No	standard
segment	Defines the maximum file size for file logging	<file size in KB>	No	""
expire	Number of backup log files to be maintained	<number of files >	No	""

- Set up a user on the host to create a new user named `gcti` and a group named `gcti`, which is the primary group for the new user and set `/bin/bash` as the default shell. This user will be used to run the Tomcat service and to run LCA (unless you have configured LCA to run under the root or another user). Refer to the Genesys Administrator 8.1 Help for information about creating a new group and a new user.

End

2. Set up the user on the Host machine.

Refer to the Genesys Administrator 8.1 Help for information about creating a new group and a new user.

3. Set up the host on which Genesys Administrator Extension server will run.

Setting up the host for Genesys Administrator Extension server

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

Start

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

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

      (Linux) Select the `.bin` package that does not have `rpm` in its name. That is, select `*.bin`. Do *not* select `*-rpm.bin`.

   b. (Linux) Put the downloaded file into the directory `/usr/lib/java`.
      i. Make the file executable by entering the following command:

         ```
         chmod +x <filename>.bin
         ```

      ii. Run the file to install Java, by entering the following command at the # prompt:

         ```
         ./<filename>.bin
         ```

      The contents will be installed in the same directory as the file.

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

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

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

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

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

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

End

4. Install Tomcat.

Installing Tomcat

Prerequisites

- JRE 6 is installed on your host and JRE_HOME is configured correctly.

Start

1. Download Tomcat 6.0.37 as a ZIP archive from the following location:

   `http://archive.apache.org/dist/tomcat/tomcat-6/v6.0.37/`

   > **Important**
   > You must use the ZIP archive to install Tomcat. GAX does not work properly if the Windows installer is used to install Tomcat.

2. (Linux) Open a terminal as the user `gcti` by entering the following command at the # prompt:

   ```
   su gcti
   ```

3. Extract the downloaded archive to the following directory:

- (Linux) `home/gcti/apache-tomcat-6.0.37`
- (Windows Server) `C:\GCTI\Apache Tomcat 6.0.37\`

> **Important**
> Ensure that the user on the host on which GAX Tomcat is running can read all files and execute all `*.bat` scripts (on Windows) or `*.sh` scripts (on Linux) in this directory.

- Set the environment variable:

- (Linux)
  i. Set the following environment variable for your host by inserting the following line into the `/etc/profile` file:

     ```
     CATALINA_HOME=/home/gcti/apache-tomcat-6.0.37
     ```

- (Windows)
  i. Navigate to Control Panel.
  ii. Double-click on System.
  iii. Click Advanced system settings.
  iv. Click Environment Variables.
  v. In the System variables section, set the system environment variable `CATALINA_HOME` to the path where your Tomcat instance is installed.

> **Important**
>
> `$CATALINA_HOME` refers to the installation directory for Tomcat.
>
> On Windows, it might be: `c:\Program Files\Apache Tomcat 6.0.37\.`
>
> On Linux, it might be: `/home/gcti/apache-tomcat-6.0.37/`

- In the file `/home/gcti/apache-tomcat-6.0.37/conf/tomcat-users.xml`, add the following line in the section `<tomcat-users>`:

  ```
  <user username="manager" password="<password>" roles="manager"/>
  ```

  where <password> is the password to access Tomcat.

- To test the installation:

  - Linux:

  i. Enter the following command at the # prompt:

     ```
     bin/startup.sh
     ```

  ii. Point your web browser to `http://<host>:8080`

  - Windows Server:

  i. Run the following file:

     ```
     C:\GCTI\Apache Tomcat 6.0.37\bin\startup.bat
     ```

  ii. Point your web browser to `http://<host>:8080`

- (Optional) (Linux) Since Tomcat log files do not rotate by default, set up Tomcat log file rotation by creating the file `/etc/logrotate.d/tomcat` as the root, containing the following lines:

  ```
  /home/gcti/apache-tomcat-6.0.37/logs/catalina.out {
  ```

```
copytruncate
daily
rotate 7
compress
missingok
size 256M
}
```

This also adds the file `catalina.out` to the system log daily rotation.

GAX does not write a lot of data to the catalina.out log file; however, it is good practice to enable log rotation to prevent long-term issues with the size of the log file.

> **Important**
>
> If you want detailed information about how to configure TLS/SSL for Tomcat connections, refer to the following website: http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html

End

(Optional) Configure Tomcat to enable HTTPS-Only mode.

Configuring Tomcat to enable HTTPS-Only mode

Purpose

- To set up Tomcat to work in HTTPS-only mode and thereby improve system security.

There are three general steps that are required to set up Tomcat to operate in HTTPS-only mode:

1. Generate the keystore file. This file contains the certificate. A certificate is required. The certificate can be either a certificate authorized by a Certificate Authority, which you have to import into your keystore file, or, a self-signed certificate that you create and use in the keystore file.

   The last approach is simpler in that it offers the same level of security; however, the end user must trust your GAX authority.

   No matter which authority is used, all information is encoded and transmitted by using the HTTPS protocol.

2. Configure the SSL connector in Tomcat.
3. Configure Tomcat to use HTTPS-only for the GAX application.

More detailed information about HTTPS setup, certificates and authorization is available in the Tomcat

6 SSL documentation:

http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html#Configuration

Prerequisites

- JRE 6 and Tomcat 6.0.xx are installed on the web host.

Start

1. Create a self-signed certificate, or import an existing certificate.

- To create and use a self-signed certificate, follow these steps:

i. To create a keystore, use the Keytool application (this is automatically installed with the JRE). Alternatively, you can use the OpenSSL application, as described in the Tomcat documentation.

ii. From the command line, navigate to the `JRE_HOME\bin` directory:

```
cd $JRE_HOME/bin/
```

iii. Execute the following, replacing all values of the placeholders, by using the same value for `<password_for_certificate>` and `<password_for_keystore_file>`.

```
keytool -genkeypair -alias tomcat -keypass
<password_for_certificate> -keystore
<keystore_file_location> -storepass
<password_for_keystore_file> -validity
<number_of_days_for_validity>
```

For example:

```
keytool -genkeypair -alias tomcat -keypass Genesys -keystore
/home/gcti/keystore.key -storepass genesys -validity 365
```

iv. At the prompts, provide the requested information about your certificate, including company, contact name, and so on. This information is displayed to users who attempt to access a secure page in your application.

> **Important**
>
> Enter the fully qualified domain name of the machine where your instance of Tomcat is running, as you are prompted for your first and last name.

The keystore file is created and it can be referenced by Tomcat.

- To import an existing certificate that is based on a certification request, follow these steps:

i. Create a local Certificate (refer to the previous bullet).

> **Important**
>
> In some cases you will have to enter the domain of your website (for example: `www.<example>.com`) in the `first- and lastname` field to create a working Certificate.

ii. Use the following command to create a Certification Request (CSR):

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr
 -keystore <your_keystore_filename> -keypass
 <password_for_certificate> -storepass
 <password_for_keystore_file>
```

The `certreq.csr` file is created. You can submit this certification request to a Certification Authority to obtain a certificate.

After you obtain the certificate signed by a Certification Authority, you can import it into your local keystore. Before you can import your certificate, you must import a Chain Certificate or a Root Certificate into your keystore.

iii. Use the following command to import the Chain Certificate into your keystore:

```
keytool -import -alias root -keystore
 <your_keystore_filename> -trustcacerts -file
 <filename_of_the_chain_certificate>
```

iv. Use the following command to import your Certificate:

```
keytool -import -alias tomcat -keystore
 <your_keystore_filename> -file
 <your_certificate_filename>
```

- Configure the SSL connector in Tomcat.

a. From the `conf` directory of your Tomcat installation, open the `server.xml` file in a text editor. If set, you can use the `CATALINA_HOME` variable:

```
    $CATALINA_HOME/conf/server.xml
```

b. Find in the file the following code for setting the SSL connector:

```
<!--
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
  -->
```

c. Uncomment this code and add the following line of code:

```
keystoreFile="<keystore_file_location>"
 keystorePass="<password_for_keystore_file>"
```

d. Replace the placeholders with the correct values from Step 1. For example:

```
<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" />
```

e. Restart your Tomcat server, and verify that is it listening on port 8443 (or whatever port you have specified) in HTTPS mode. The HTTP port 8080 remains open. Connections to that port are not redirected to the HTTPS port 8443.

- Configure Tomcat to accept HTTPS only:

a. From the same directory as the `server.xml` file in Step 2, open the Tomcat `web.xml` file in text editor.

b. Above the <web-app> tag, add the following code:

```
<display-name>Security Constraint</display-name>
   <web-resource-collection>
      <web-resource-name>Protected Area</web-resource-name>
      <!-- Define the context-relative URL(s) to be protected
-->
      <url-pattern>/*</url-pattern>
      <!-- If you list http methods, only those methods are
protected -->
   </web-resource-collection>
<user-data-constraint>
   <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

c. Restart Tomcat.

d. Confirm that HTTP requests are redirected to your HTTPS port by attempting to access the GAX application over HTTP by entering the following URL in a web browser window:

```
http://<yourhostname>:8080/gax
```

The browser should be redirected to your HTTPS connection:

```
https://<yourhostname>:8443/gax
```

End

5a. Install Genesys Administrator Extension server on a Linux host.

Installing Genesys Administrator Extension server on a Linux host

Prerequisites

- The `Application` object for Genesys Administrator Extension server exists (see Step 4 of Creating the necessary configuration objects for Genesys Administrator Extension).
- The environment variable for `JRE_HOME` has been configured (see Step 2 of Setting up the host for

Genesys Administrator Extension server).

Start

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

```
chmod 755 install.sh
```

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

```
./install.sh
```

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

4. Enter information as prompted by the installation file, as follows:
   a. Enter the name of this host machine, or press `Enter` to select the default.
   b. Enter the name of the host where Configuration Server is installed.
   c. Enter the port number used by Configuration Server.
   d. Enter the username and password used to access Configuration Server.
   e. Select `n` to not use Client Side Port Option (the listening port of the application; refer to Genesys 8.0 Security Deployment Guide).
   f. When prompted to select which application to install, enter the number associated with the Genesys Administrator Extension server object.

      The following prompt is displayed:

      ```
      "Press ENTER to confirm /opt/genesys/gax as the destination directory or enter a new one =>'
      ```

      You can specify the GAX_HOME folder here:

      ```
      GAX_HOME=/home/gcti/gax
      ```

      By default, the installation puts a `startup` and a `setenv` script in the Tomcat `bin/` directory and the Genesys Administrator Extension application in the Tomcat `webapps/` directory. Additional resources and the database creation script are installed in the folder given by the `GAX_HOME` environment variable (see Setting up the host for Genesys Administrator Extension server). Press `y` to accept this, or press `n` to cancel setup.

   g. Make the `setenv` script executable by entering the following command at the # prompt:

```
chmod 755 setenv.sh
```

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 `setnev.sh` file to a different value. If you enable TLS encryption, ensure that you make the following updates to the `setenv.sh` file. The `setenv.sh` file contains the following lines:

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

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

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

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

- To start GAX manually by using `gax_startup.sh`, you might have to modify this file by replacing the following line:

  ```
  export GAX_CMD_LINE_ARGS=$*
  ```

  with the following command (use arguments that match your system):

  ```
  GAX_CMD_LINE_ARGS="-host <configuration server host> -port <configuration server port> -app
   <application name>"

  export GAX_CMD_LINE_ARGS
  ```

End

5b. Install Genesys Administrator Extension server on a Windows Server 2008 host.

Installing Genesys Administrator Extension server on a Windows Server host

Prerequisites

- The `Application` object for Genesys Administrator Extension server exists (see Step 4 of Creating the necessary configuration objects for Genesys Administrator Extension).
- The environment variable for `JRE_HOME` has been configured (see Step 2 of Setting up the host for Genesys Administrator Extension server).

Start

1. Copy the IP to the host machine.
2. Run the installation file to extract and copy the necessary files by entering the following command:

   ```
   ./setup.exe
   ```

   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.

   If there is not an existing installation of GAX on the host, then you must specify the location of the Tomcat folder (refer to Installing Tomcat).
3. Enter information as prompted by the installation file, as follows:
   a. Enter the name of the host where Configuration Server is installed.
   b. Enter the port number used by Configuration Server.
   c. Enter the username and password used to access Configuration Server.

Important

- To start GAX manually by using `gax_startup.bat`, you might have to modify this file by replacing the following line:

  ```
  set GAX_CMD_LINE_ARGS=%*
  ```

  with the following command (use arguments that match your system):

  ```
  set GAX_CMD_LINE_ARGS=-host confserv -port 2020 -app gaxappobjname
  ```

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

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

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

End

6. Choose which GAX functionality is available on the host.

Choosing which GAX functionality is available on the host

Purpose

- To add or remove GAX internal modules to control which GAX functionality is available for users on a specific host.

You can install multiple instances of GAX on multiple hosts to support HA, load balancing, and the availability of functionality. Each deployment of GAX shares the same data resources, such as Configuration Server, the GAX database, audio resources, and so on.

The plug-in architecture of GAX enables you to add or remove modules to control the availability of functionality.

Start

1. Deploy GAX as described in Installing Genesys Administrator Extension server on a Linux host on each host (this procedure is performed on a Linux install, but works the same on Windows if you adjust the paths according to your installation).
2. Navigate to the following folder: `<Tomcat Home>/webapps/gax/WEB-INF/lib`
3. Remove the `gax-*.jar` files that contain the functionality that you want to restrict. For example, if you do not want the user on the host to deploy audio resources, remove the `gax-opm-arm*.jar` file.

> **Warning**
> Do not remove the `gax-core*.jar` and `gax-plugin-api*.jar` files. These files are required to run the core functionality of GAX. Also, do not remove any of the JAR files that do not begin with `gax-`.

4. Add any external plug-in `*.jar` files that will use the functionality of the plug-in by copying the `*.jar` file to the `<Tomcat Home>/webapps/gax/WEB-INF/lib` folder.

> **Important**
> You can choose to remove all of the standard GAX plug-in modules, except the core plug-ins, to run GAX with only the plug-in functionality.

5. Restart Tomcat after adding or removing plug-ins for changes to take effect.

End

7a. Set up the database for Oracle.

Setting up the Genesys Administrator Extension database (for Oracle)

Purpose

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

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

Start

1. Refer to the Oracle documentation to install the Oracle Database Management System on the host machine that corresponds to the `Host` object that you configured in Step 2 of the procedure Creating the necessary configuration objects for Genesys Administrator Extension.
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>;
```

3. Initialize the database by executing the following three scripts in the order below. The scripts are available in the following folder: `<installation folder>/resources/sql_scripts/oracle`

- `core_init_ora.sql`
- `opm_arm_init_ora.sql`
- `asd_init_ora.sql.`

> **Important**
>
> Error messages about unsuccessful execution of DROP statements might be displayed. Ignore these error messages. To verify that there are no real errors, execute the scripts twice. No errors should be displayed the second time.

- Connect the GAX Server application object to the DAP that you created in Step 3 of Creating the necessary

configuration objects for Genesys Administrator Extension.

End

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

7b. Set up the database for Microsoft SQL.

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

Purpose

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

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

Start

1. Refer to the Microsoft SQL Server 2008 R2 documentation to create the Microsoft SQL Server Database for GAX on the host machine that corresponds to the `Host` object that you configured in Step 2 of the procedure Creating the necessary configuration objects for Genesys Administrator Extension. You can create the login and database, then execute the database scripts for MSSQL Server by using SQL Server Management Studio.
2. Start SQL Server Management Studio.
3. Connect to Microsoft SQL Server 2008 as `sa`.
   - Server type: `Database Engine`
   - Server name: `Local`
   - Authentication: `SQL Server Authentication`
- Create a login and password for the GAX database. For example: `gax812admin` with the password `password`.
- Create the GAX database (for example, `gax812`) by using the login to make this login the owner of the database.

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

- Verify that you can connect to the database with the login that you created:
  - Server type: `Database Engine`
  - Server name: `Local`
  - Authentication: `SQL Server Authentication`
- Execute the following scripts in the order below, by using the Microsoft SQL Server 2008 Query Editor. The scripts are available in the following folder: `<installation folder>/resources/sql_scripts/mssql`
  a. `core_init_mssql.sql`
  b. `opm_arm_init_mssql.sql`
  c. `asd_init_mssql.sql`

> **Warning**
> The following fields must have a combined size of 900 bytes or less:
>
> - `asd_sd table (folder, version, svc_name, tenant_id)`
> - `asd_ip table (folder, nickname, os, tenant_id, version, localeid, buildnumber)`
>
> This constraint is indicated during execution of the `asd_init_mssql.sql` script with the following warning:
>
> `The maximum key length is 900 bytes.`
>
> Microsoft SQL Server cannot store indexes that have a size greater than 900 bytes.

Error messages might be displayed during script execution, because there are `DROP` statements in the script that might be trying to drop tables or constraints that do not exist.

You can verify that the errors do not exist by executing the scripts twice.

End

7c. Set up the database for PostgreSQL.

Setting up the Genesys Administrator Extension database (for PostgreSQL)

Purpose

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

> **Important**
>
> - This procedure applies only to GAX 8.1.310 releases or higher.
> - It is recommended to use PostgreSQL version 9.1.8.

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

Start

1. Refer to the PostgreSQL 9.1 documentation to create the PostgreSQL Database for GAX on the host machine that corresponds to the `Host` object that you configured in Step 2 of the procedure Creating the necessary configuration objects for Genesys Administrator Extension.

   Create the login account and database, then execute the database scripts for PostgreSQL by using pgAdmin.
2. Start pgAdmin.
3. Select the PostgreSQL 9.1 connection and connect to the PostgreSQL database with the following user name: `postgres`.

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

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

   For example: `gax813admin` with the password `password`.

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

   ```
   CREATE USER gax WITH PASSWORD 'gax813admin' CREATEDB;
   ```

5. Create the GAX database (for example, gax813) by using the login created in Step 4 to make this login the owner of the database.

```
create database gax813 owner gax;
```

6. Connect to the database with the login that you created in Step 4.
7. Execute the following scripts in the order below, by using pgAdmin. The scripts are available in the following folder:

```
<installation folder>/resources/sql_scripts/postgres
```

   a. `core_init_postgres.sql`
   b. `opm_arm_init_postgres.sql`
   c. `asd_init_postgres.sql`

End

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

Enabling UTF-8 character encoding (for Oracle)

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

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

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

```
SELECT * FROM NLS_DATABASE_PARAMETERS;
```

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

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

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

new character set.

Important

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

8. Configure Genesys Administrator Extension.

Configuring Genesys Administrator Extension

Purpose

- To set up role privileges and logging for Genesys Administrator Extension.

Start

1. Stop Tomcat, if it is running.
2. In Genesys Administrator, create at least one new `Role` object to provide access to the functionality in Genesys Administrator Extension. Follow the instructions in Genesys Administrator 8.1 Help.
   a. Define the privileges that are granted by the role on the `Role Privileges` tab.
   b. Assign the role to users and access groups on the `Members` tab as required.

   Refer to the Genesys 8.0 Security Deployment Guide for more information about roles and role privileges.

End

9. Start Genesys Administrator Extension.

Logging In

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

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

Logging in to Genesys Administrator Extension

Prerequisites

- Configuration DB Server and Configuration Server are installed and running.
- An instance of a Genesys Administrator Extension `Application` object, configured as a server in Step 4 of Creating the necessary configuration objects for Genesys Administrator Extension, is connected to Configuration Server and running.
- Your browser and its windows are set to a resolution of 1024x768 or greater. If you are working in 1024x768, maximize the browser.
- The user logging in must have Read permission to their own `User` object and Read and Execute permissions on the Genesys Administrator Extension client object. Refer to the Genesys 8.0 Security Deployment Guide for information about permissions. Genesys Administrator Extension respects read-write permissions that are set for Environments and Tenants. You can only access those objects that you have permission to see.

Start

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

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

   where <Host name> is the name of the computer on which you installed Genesys Administrator Extension. The port number is the port that was defined when setting up Tomcat in Installing Tomcat.

6. Log in to Genesys Administrator Extension with your assigned user name and password, and click `Log in`.

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

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

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

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

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

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

End