Genesys Intelligent Automation Reference Guide

User Authentication and Authorization

4/13/2025

User Authentication and Authorization

This section describes how Genesys Intelligent Automation ensures that only authenticated and authorized users access Intelligent Automation environment specifically, and the Genesys software environment generally.

For more information about user authentication and authorization, refer to the User Authentication and User Authorization section of the *Genesys Security Deployment Guide*.

Internal and External Users

There are two types of users in Intelligent Automation:

- Internal users: Created and managed in Intelligent Automation. See the Users page in Intelligent Automation Help. These users are not subject to an external authentication engine; all authentication is done by Intelligent Automation. All authorization is implemented through Roles.
- External users: Created and managed in Genesys Configuration Server. Authentication is done internally by Configuration Server and sometimes by an external authentication engine, such as LDAP (Lightweight Directory Access Protocol), and RADIUS (Remote Authentication Dial In User Service). Authorization is done in Configuration Server. External users are supported starting in release 9.0.004.00.

The two user types mean that when creating a new user, the administrator must first decide whether to create the user in Intelligent Automation or in Configuration Server.

Prerequisites for external users

If you are working with external users, you must do the following:

1. Enable Intelligent Automation to work with external users.
2. Configure Intelligent Automation access to Configuration Server.
3. Import a Solution Package Definition (SPD) file containing all role privileges, into the Genesys Configuration Database.
4. Link tenant IDs in the Configuration Database to Intelligent Automation companies. Identify a *default* company for those users that might not belong to a tenant.

Important

When configuring custom roles, ensure that the name for a custom role in the SPD file matches the name created in the **Administration > Roles** option. See Roles in Intelligent Automation and Roles tab in

> Administration for more information.

Configure working with external users

To configure Intelligent Automation to work with external users, set the parameter **Login.ExternalAuthentication.Mode** to `ConfigServer` in the **Default Server Settings** tab under **Administration** in the Intelligent Automation interface:

Login.ExternalAuthentication.Mode	ConfigServer

The default value of this parameter is None, meaning that external users cannot log in to Intelligent Automation.

Configure access to Configuration Server

To configure Intelligent Automation to work with external users, Intelligent Automation must call upon Configuration Server to, among other things, validate the user. Therefore, you must provide the information required to access Configuration Server in the **Default Server Settings** tab, as follows:

GenesysSDK.ConfigServer.ClientApplicationName	default
GenesysSDK.ConfigServer.LoginAsApplication	false
GenesysSDK.ConfigServer.Password	password
GenesysSDK.ConfigServer.Server.Host	
GenesysSDK.ConfigServer.Server.Port	2020
GenesysSDK.ConfigServer.Username	default

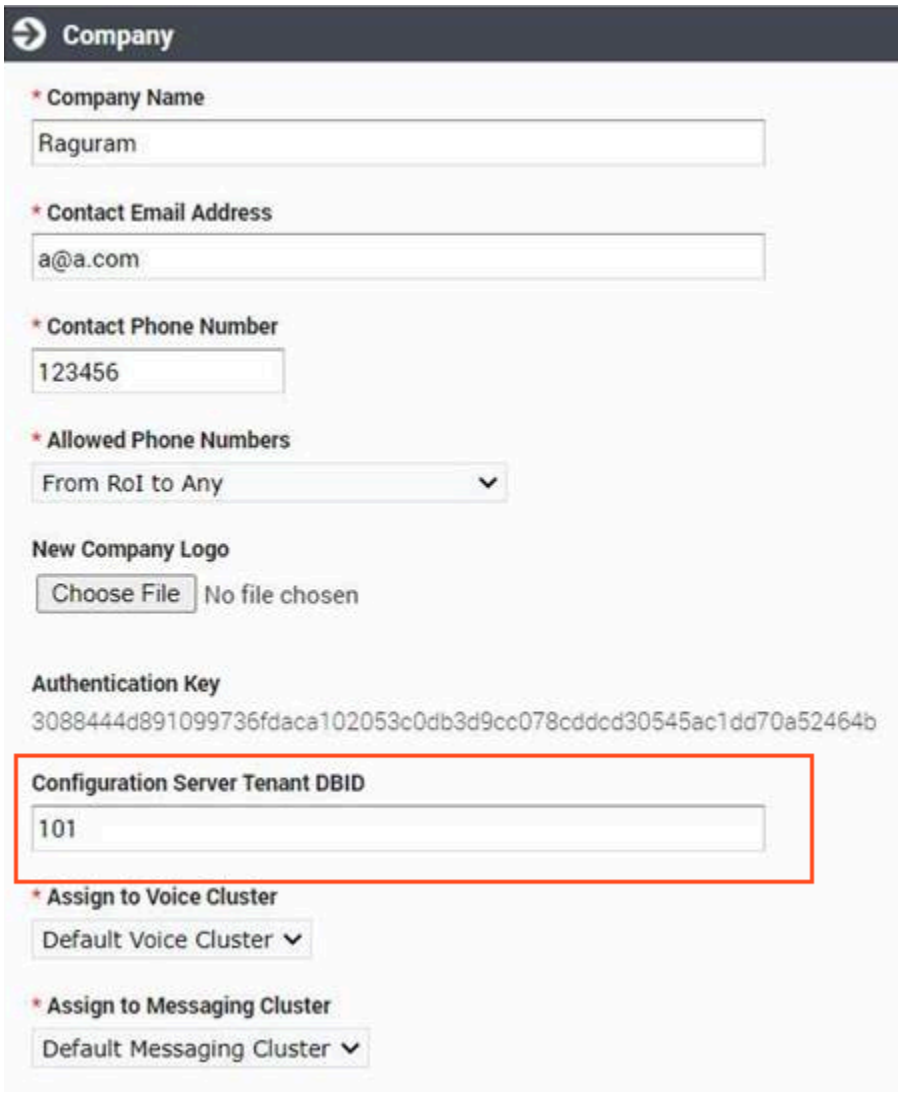
Import SPD file into Configuration Database

A Solution Package Definition (SPD) file contains all role privileges for the associated solution. Without it, validated external users would be logged in with no permissions or roles. An SPD file called **IA_SPD_Roles.xml** is provided to you by Intelligent Automation if you choose to manage external users via Configuration Server. It must be imported into the Genesys Configuration Database. For information about installing the SPD file, see Solution Deployment or the Genesys Administrator Extension Developer's Guide.

Linking tenant IDs to Intelligent Automation companies

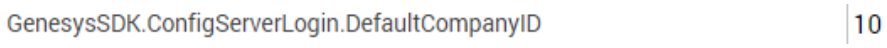
Each Intelligent Automation company should be linked to a tenant in the Configuration Database by specifying the DBID of that Tenant in the **Configuration Server Tenant (DBID)** field when configuring the company. When an external user logs into Intelligent Automation, the company

corresponding to the user's Tenant is loaded for that user.



> **Important**
>
> This field will not appear unless the **Login.ExternalAuthenticationMode** server setting is set to `ConfigServer`.

If a company is not linked to a particular tenant, or the tenant does not exist, you can specify a *default* company in the **GenesysSDK.ConfigServerLogin.DefaultCompanyID** parameter under **Administration** > **Default Server Settings**.



If a default company is not specified, any login by an external user without a linked tenant ID is rejected.

> **Important**
>
> If the external user belongs to the environment tenant, Intelligent Automation will use the **GenesysSDK.ConfigServerLogin.DefaultCompanyID** option to determine the default company ID to be loaded.

Standard Responses

When a user runs a callflow app to fetch the standard response from UCS, Intelligent Automation will look for the company TenantID configured in the **Configuration Server Tenant (DBID)** field first. If this field is empty, the value of the default company ID configured in the DefaultCompanyID (**Administration** > **Default Server Settings**).

If both TenantId and defaultID are not configured, then IA would assume the default tenantID as Environment (TenantID : 1)

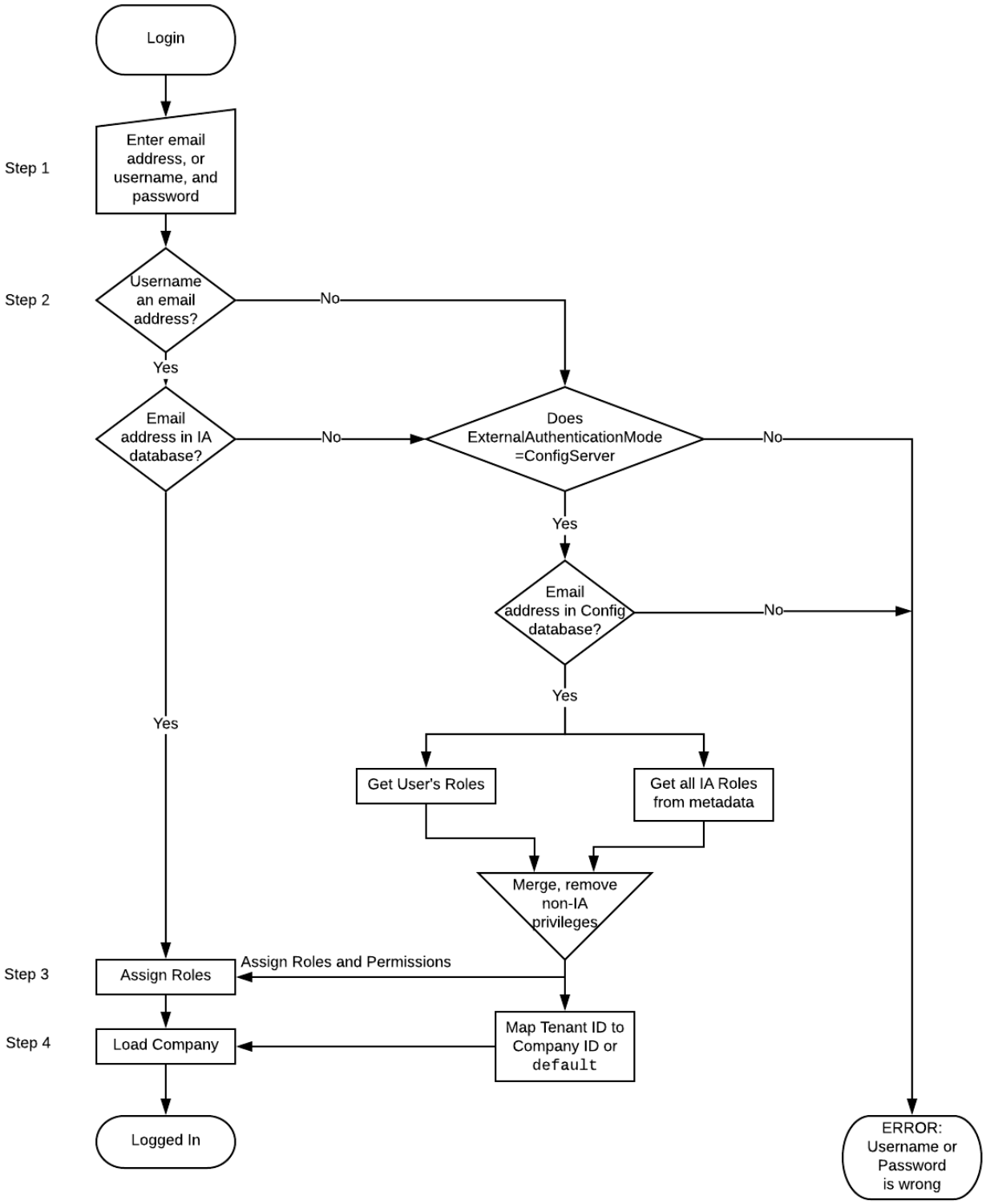
At login

At login, the following high-level actions occur:

1. The user enters their username and password. For internal users, the username is their email address. For external users, the username is their Configuration Server username.
2. The user is authenticated, or validated, by having their user's credentials compared to internally-stored credentials in the application's database.
3. Permissions and roles are assigned to the user, based on the information in their respective database. Permissions define what the user can see, while roles define what the user can do to those items it can see.
4. The company associated with the user is loaded. For external users, the company is based on the Tenant ID with which the user is associated or the **GenesysSDK.ConfigServerLogin.DefaultCompanyID** parameter if no association of the default company is found.

With these four steps completed, the user is now in the Dashboard of the Intelligent Automation interface, ready to start working.

The following flow chart illustrates the login process:


Login
Step 1
Enter email address, or username, and password
Step 2
Username an email address?
No
Yes
Email address in IA database?
No
Does ExternalAuthenticationMode =ConfigServer
No
Yes
Email address in Config database?
No
Yes
Yes
Get User's Roles
Get all IA Roles from metadata
Merge, remove non-IA privileges
Step 3
Assign Roles
Assign Roles and Permissions
Step 4
Load Company
Map Tenant ID to Company ID or default
Logged In
ERROR: Username or Password is wrong

Changing passwords for external users

Passwords for external users can be changed in Intelligent Automation. The process of managing them is completely transparent to the Intelligent Automation user.

> **Important**
>
> Passwords can be changed only for external users who are configured in Configuration Server.

If **Change password at next login** is checked in the external user's profile in Configuration Server when the external user logs in to Intelligent Automation, the user is prompted to change their password in the same way as for an internal user. See How do I change my password. The password is changed in Configuration Server automatically and **Change password at next login** is cleared in the external user's profile.