Developer's Guide

Role-Based Access Control

12/12/2025

Contents

Role-Based Access Control

This page describes how you can implement the role-based access in the Context Services.

Configuration

Through Configuration Manager or Genesys Administrator, you can define roles for your application built on top of the Context Services. To do this, you assign one or more roles to your users when creating your application's configuration in the Context Services. You are responsible for creating and defining these roles, where each role is a collection of Genesys Administrator Tasks associated with permissions.

<tabber> Context Services=

Rights for Context Services

Tasks related to Service management are available in GMS and may require specific permission set up in Genesys Administrator.

Starting 8.5.0, privileges are simplified.

Name	Description
Administrator	Specifies write access to all CS APIs.
Supervisor	Specifies read access to all CS APIs.

The following table details the relationship between requests and privileges.

Privileges required per API operations:

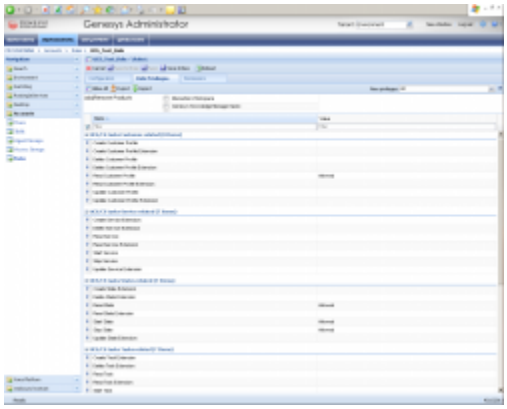
HTTP Operation	Required Permissions
PUT	Administrator
POST	Administrator
GET	Administrator or Supervisor
DELETE	Administrator

Click here to learn how to create roles and assign privileges.

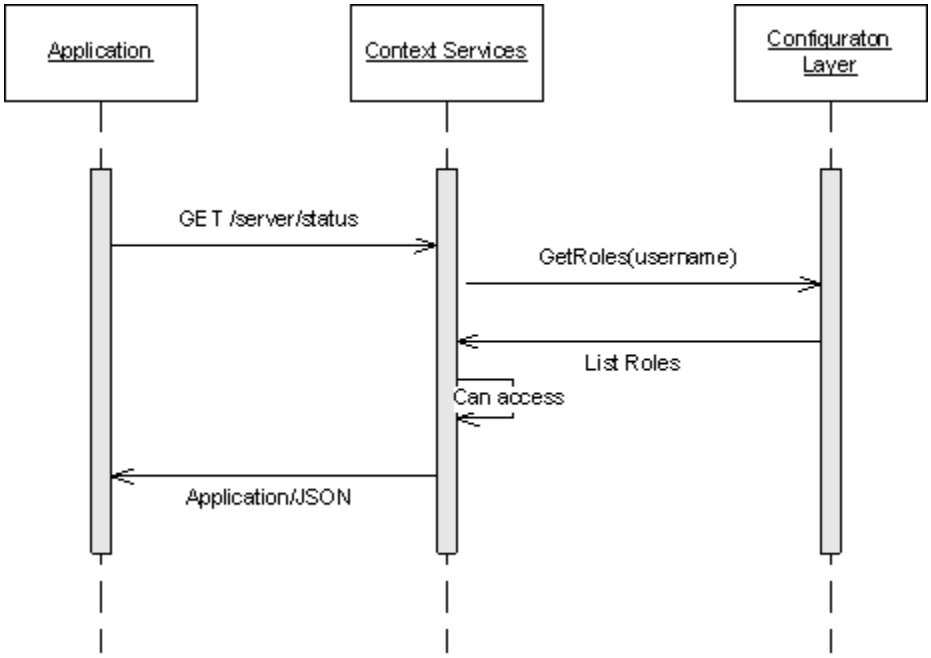
|-| Rights for Customer Profiles=

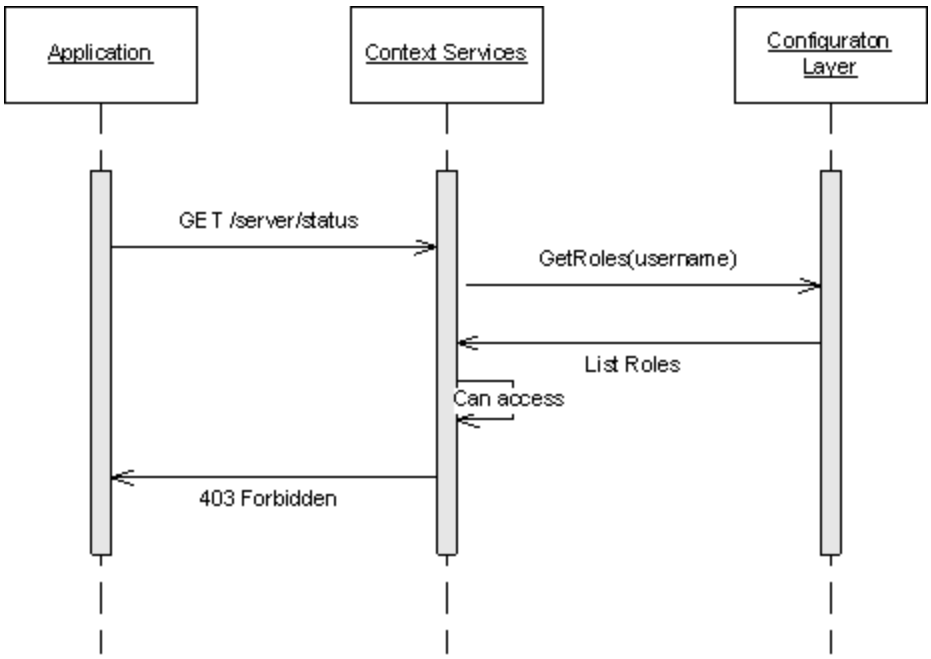
Genesys Administrator Tasks for Customer Profiles in UCS

Tasks related to Customer management are available in UCS and require specific permission set up in Genesys Administrator.



Once authenticated, if the `use-role` option is set to `true` in the configuration (see the options defined in [authentication] Section) then the Universal Contact Server checks that each operation is allowed. If not, `Error 403 forbidden` is returned.





Mapping Genesys Administrator Task with Context Services

Operations can require that one or more Genesys Administrator Tasks are allowed, according to the type of data that the request modifies. If your application's role does not allow all of the rights required for a given operation, then the operation does not proceed.

For example, consider that your application performs a Create Customer Profile operation with extensions. If your application's role allows `UCS.Customer.createProfile` but not `UCS.Customer.createProfileExtension` then the profile is not created. Your application instead receives a `HTTP 403 Forbidden error`.

Operation	Genesys Administrator Tasks
Profile Operations	
Create Customer Profile POST /profiles	• UCS.Customer.createProfile • UCS.Customer.createProfileExtension (if extensions)
Delete Customer Profile DELETE /profiles/${customer_id}	• UCS.Customer.deleteCustomerProfile

Operation	Genesys Administrator Tasks
Delete Record From Profile Extension PUT /profiles/${customer_id}/extensions/${ext_name}/by/unique	• UCS.Customer.deleteProfileExtension
Identify Customer GET /profiles	• UCS.Customer.readCustomerProfile • UCS.Customer.readProfileExtension (if `include_extensions` is specified in the query)
Insert Extension Records POST /profiles/${customer_id}/extensions	• UCS.Customer.createProfileExtension
Bulk Profile Import POST /profiles/import	• UCS.Customer.executeBulkImport • UCS.Customer.createProfile • UCS.Customer.createProfileExtension
Query Customer Profile GET /profiles/${customer_id}	• UCS.Customer.readCustomerProfile • UCS.Customer.readProfileExtension (if extensions)
Update Customer Profile PUT /profiles/${customer_id}	• UCS.Customer.updateCustomerProfile • UCS.Customer.updateProfileExtension (if extensions)
Merge Customer Profile PUT /profiles/${customer_id}/merge/${src_id}/	• UCS.Customer.mergeCustomerProfile
Update Record In Profile Extension PUT /profiles/${customer_id}/extensions/${ext_name}/by/unique	• UCS.Customer.updateProfileExtension
Schema Operations	
Create Profile Extension Schema POST /metadata/profiles/extensions	• UCS.SchemaMgt.createProfileExtensionSchema
Create Identification Key POST /metadata/identification-keys	• UCS.SchemaMgt.createIdKeys
Get Identification Keys GET /metadata/identification-keys	• UCS.SchemaMgt.readIdKeys
Query Profile Schema GET /metadata/profiles/	• UCS.SchemaMgt.readProfileExtensionSchema
Query Profile Extension Schema	UCS.SchemaMgt.readProfileExtensionSchema

Operation	Genesys Administrator Tasks
GET /metadata/profiles/extensions	
Query Business Attribute Schema GET /metadata/business-attributes/${business-attribute-name}	• UCS.SchemaMgt.readBusinessAttributes
Get Metadata Cache GET /metadata/cache	• UCS.SchemaMgt.handleMetadata
Change Metadata Cache PUT /metadata/cache	• UCS.SchemaMgt.handleMetadata
Get Metadata GET ${contenttype}} /metadata	• UCS.SchemaMgt.handleMetadata
Delete Metadata Profile Extensions DELETE /metadata/profiles/extensions/${extension-name}	• UCS.SchemaMgt.deleteProfileExtensionSchema
Delete Metadata Identification Keys DELETE /metadata/identification-keys/${id_key-name}	• UCS.SchemaMgt.deleteIdKeys
Interaction Operations	
Query Interactions GET /customers/${customer_id}/interactions GET /services/${service_id}/interactions GET /interactions/${interaction_id}	• UCS.SchemaMgt.readInteraction