

GENESYS

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.

User's Guide

Multiple UCS Instances in Single Tenant

5/13/2025

Multiple UCS Instances in Single Tenant

Purpose: describe a solution that enables multiple independent UCS instances to be deployed in a single tenant, based on the Access Group mechanism available in Configuration Server.

Contents

- 1 Multiple UCS Instances in Single Tenant
 - 1.1 Overview
 - 1.2 Configuration Procedure
 - 1.3 Adjustments
 - 1.4 Use with Other Genesys Applications
 - 1.5 Limitations

Overview

This solution uses access rights to restrict UCS instances from seeing objects that do not belong to them. Genesys components that access the Configuration Server database typically use the system account to access Configuration objects, granting the components global visibility. However, it is possible to use another account simply by changing the logon as option on the Security tab of the relevant Application object. One reason to use this solution relates to standard responses: If you have multiple UCS instances in a single tenant without restricted access, each instance will have access to the standard response library managed by the other instances. And if a UCS instance has access to a standard response library that it does not manage, it will keep deleting the standard responses from the Configuration Server database. The result will be that all instances will be repeatedly deleting other standard response libraries and re-creating their own. There is no need to use this configuration if you do not use standard responses and don't mind the UCS instances sharing each other's Contact and Interaction attributes. And of course these issues do not arise when the UCS instances are in different tenants. Different access groups represent different lines of business (LOB). This example uses two LOBs, e-mail, and chat.

Configuration Procedure

Airroiders	contents of /configuration/Environment/Access Groups
Configuration Configuration Access Groups Administrators EVERYONE Super Administrators SYSTEM Users Action Codes	Name Enter text here Image: Administrators Image: EVERYONE Image: Super Administrators Image: System Image: System Image: Users
Agent Groups Alarm Conditions Application Templates Applications Desktops/GIS/AIL Management Framework Multimedia Outbound Real-time/Reporting Routing	New Access Group (0) [suite76:2020] Properties General Annex Image: State Enabled
Figure 2: Creating Access Groups	

1. Create an access group for each Line of Business (LOB).

2. Create a user for each of the access groups: right-click the access group, then select New > Person.

All Folders			Contents of '/Configu
Configuration Co	ators E <u>N</u> ew		UserName A Enter text h Y Person Shortcut to Person
⁴ New Person () (0) [suite76:202	0] Proper	ties X
General Ranks Mem	ber Of Annex	c	
Erst:			_
<u>L</u> ast:			•
<u>T</u> enant:	A Environ	ment	- 3
Employee ID:	lob-email-use	r	
E- <u>M</u> ail:			_
Internal Authentication	lob-email-use	r.	
Enter Password:			<u> </u>
<u>R</u> e-enter Password:			
External Authentication External User ID:			_
	✓ State Enal	bled	🔲 is Agent
Г ОК	Cancel	M <u>a</u> ke Ne	ew Help

Figure 3: Creating a Person

- 3. Configure each access group's permission to access configuration objects:
 - 1. Right-click the tenant.
 - 2. On the Security tab, click Permissions.
 - 3. In the resulting Object Permission dialog, click Add...
 - 4. In the resulting Add dialog, click Add and select Full Control.

Do this for Environment and all defined Tenants (multi-tenant environment), or for Environment and Resources (single-tenant). The figure below shows the process for the Environment tenant.

All Folders		Contents of VConfigu	ration/Environment/A	ccess Groups/lob-e	mail	
	guration	UserName 🔺	First Name	Last Name	Employee ID	Agent
	vironment	Enter text h 🝸	Enter text h 🍸	Enter text h 🍸	Enter te 🍸	Enter te
🗆 🖂	Access Groups	🔒 lob-email-user			lob-email-user	False
	Administrators	<u> </u>				
4	Environment (1) [suite76:2020]	Properties	×			
	General Annex Security					
	·		1			
	Permissions		Add			
	View or set permission in	nformation on the	Add			
	selected item(s).		List Nam	nes From: 🛕 Enviro	oment	
(Permissions	<u>N</u> ames:			
🗉 🚺	Object Permission	_		ERYONE		
□ 🗍			SY:			
	Object: Tenant "Environment	."		ninistrators		
	Replace Permissions Recursively		kilob-			
	Name A	Access		oer Administrators		
	SYSTEM	Special Access(R	(X) 🔊 🔊 🔊 🔊	#15		
	Environment \default	Full Control				
	Environment Administrators	Full Control	(w <u>U</u> sers Me	mbers
. E (Environment\Super Administrators Environment\Users		~ (Add Shor		mbers
		Special Access(R	Add Nan			2
	1					_
			Environr	mentVob-chat;Enviror	iment Vob-email;)
	Type of A	Access: Full Control				
	OK L Com		Barr			
E E	OK Cano	cel <u>A</u> dd				
	IVKS			Access: Full Control		
岸	Objective Tables					1
	Persons			ОК	Cancel	
l 🚬	Diana Casura	1				
Figure 4: Sett	ing Tenant Permissions					

4. On the Security tab of the UCS Application, set the Log On As option to associate this UCS with one of the created users, and hence with an access group.

UCS_Email (General Connections	Tenants		operties ver Info Security	Start Info Depender		Co-Bro	Gerver fication Server owsing Server	7.5.0 7.5.0 7.6.0		True True True
Permissions	View or set permis selected item(s).	ssion infor	mation on th	ne	<u>N</u> an	ies:	A Environment			•
Log On As			<u>P</u> em	issions		default (default d lob-chat-user () lob-email-user () vide (vide)	_			
© <u>S</u> YSTE				- <u>1</u>		Add	Show Users	<u>M</u> ember	s <u>S</u> e	earch
					A <u>d</u> d	Name: Envir	OK	-user Cancel	<u>H</u> elp	
р ок	Cance	el l	M <u>a</u> ke New	Help						

Figure 5: Setting the Log On As Account

The UCS is now able to access only the objects for which the access group has permissions.

5. Set permissions for attributes:

Contact and Interaction Attributes are created in the Configuration Server database before being propagated to UCS. Therefore, in order to restrict a given attribute to one of the LOBs, you must specify permissions manually in the Configuration Server database.

- 1. Right-click the desired Attribute Value.
- 2. On the Security tab, click Permissions.
- 3. In the resulting Object Permission dialog, click the various LOB groups and select the desired permissions.

The figure below shows the customerId contact attribute being restricted to the Chat LOB.

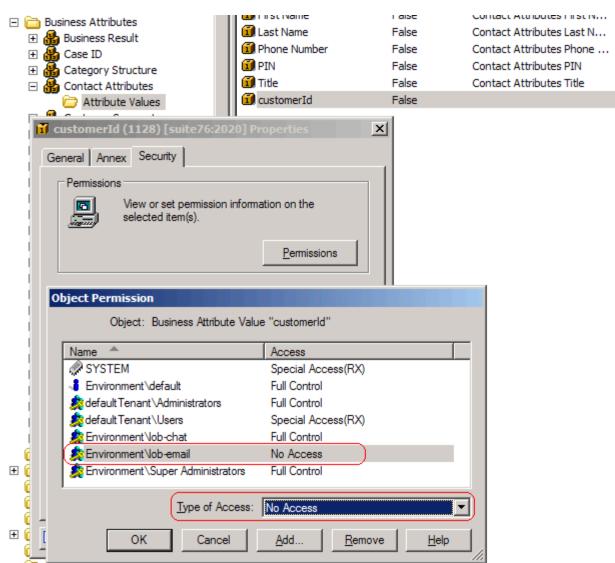


Figure 6: LOB-Specific Contact Attributes

The e-mail UCS will now behave as if customerId does not exist.

Important

Genesys recommends doing this before starting the e-mail UCS, to keep attribute metadata from being prematurely propagated.

6. To avoid having to perform the task in the previous step multiple times, you can group attributes in a folder and set permissions on the folder, as shown in the figure below. #:When an attribute is moved to the folder, it inherits the permissions.

🕀 🧯	Ь	Case	e ID		Display N	lame 📥	D	efault 🛛	1	Description	
🕀 🧯	Ь	Cate	egory Structure		Enter tex	(t here	7 E	inter te	7 E	Enter text	here
Ξ 👌	Ь	Cont	tact Attributes	ľ	🗊 custo	merId	F	alse			
E	-		Attribute Values								
			📄 chat-specific 🌖								
🕀 🗄	Ь	Cust	tomer Segment								
± 🧯	þ	DO	bject Permission)	<1
• (-	Ohiosti Esl								
± (¢١-		Object: Fold	per chat-sp	ecific						
± (ſ	G	Replace Permissio	ons Recursi	vely						
± (H	-				-		-			
± (Name 🚔			Access		Propa	agate	_	
± (SYSTEM			Special Acces	s(RX)		✓		
± (📲 Environment \def	ault		Full Control			✓		
± (🛕 default Tenant 🖓	dministrator	s	Full Control			✓		
± (🏂 default Tenant \U	sers		Special Access	s(RX)		✓		
± (Environment \Bus	siness Unit	Chat	Full Control			✓		
± ((Environment\Bus			No Access				Ţ	
± ((<u></u>								
± (т.,	an of Acres	No Asses	_			-	
± (<u>T</u> Y	pe or Acce	ess: No Acces	5			-	
± (~ .	1	1.1	-	1	1	
± (ОК	Cancel	<u>A</u> dd		<u>R</u> emove		<u>H</u> elp	
🗄 🚺											11.

Figure 7: Chat-Specific Contact Attributes

7. Further configuration of UCS Application objects.



1. Set No Access permissions on the UCS application for all LOBs other than the one that this UCS is dedicated to. These permissions will be copied to all new objects created by this UCS in the Configuration Server database.

UCS_chat (186) [suite76:2020] Properties		×	
General Tenants Server Info	Start Info		
Connections Options Annex Security	Dependenc	y I	
□ Permissions			
View or set permission information on the selected item(s).	_		
signing concernent (c).	^u	bject Permission	
Permis	sions	Object: Application "UCS_chat	
		Name 🔺	Access
⊢ Log On As		@ EVERYONE	Special Access(RX)
Log on As		SYSTEM	Special Access(RX)
C SYSTEM Account		Environment \default	Full Control
S STSTEM Account		Revironment Administrators	Full Control
<u>T</u> his Account: EnvironmentVob-chat		Environment Vob-chat	Full Control
	≤	Environment Nob-email	No Access
		Environment\Super Administrators	Full Control
		🙊 Environment \Users	Special Access(RX)
		Type of Access:	No Access
		OK Cancel	<u>A</u> dd <u>R</u> em
	_		
OK Cancel Make New	Help		

Figure 8: UCS Application Permissions

2. In the UCS settings section, set the auto-propagate-rights option to true.

General	Tenants	Server Info	Start Info
Connections	Options Annex	Security	Dependenc
settings) 🗙 🕞 🔗	Pa 69
Name 🔶	-	Value	^
Enter text her			A
abc allow-addi		"TRUE"	
abc allow-miss	-	"TRUE"	
	nb-records-per-task	"1000"	
abc archiving-	•	"4"	
abe auto-propa		"true" "FALSE"	
abc convert-id		"TRUE"	
abc enable-rep abc fieldcode-f	-	TRUE	
abchide-attac		"TRUE"	
•		"TRUE"	
abelog-db-flov		"TRUE"	
abc log-memor		"2000"	
•	a-create-full-interaction		
<u> </u>	ribute-lookup-strategy	"TRUE"	
uue primary-au ₄	nouterookup-sirategy	THUE	- D
•]			
Гок		1	
	Cancel	Make New	Help

Figure 9: UCS Options

From this point on, any new root category (as well as child categories or standard response) and screening rules will inherit the access permissions of the UCS application that created them.

Adjustments

This section describes some adjustments that may be required for Knowledge Manager objects (categories, standard responses, field codes, screening rules, training objects, and models).

Migration

If Knowledge Manager objects already exist in the Configuration Server database, you must use the following migration procedure:

- 1. Back up the UCS and Configuration Server databases.
- 2. Use Knowledge Manager to export all objects for each LOB to a file. Importing and exporting is described in "Importing and Exporting" in the "Knowledge Management: Basics" chapter of the

eServices User's Guide.

- 3. Use Knowledge Manager to delete all Knowledge Manager objects for each LOB.
- 4. Check that all Knowledge Manager objects have been removed from the Configuration Server database.
- 5. Upgrade all UCS database instances and specify permissions as outlined in Configuration Procedure.
- 6. Use Knowledge Manager to import all objects for each LOB, being sure to not select the option to generate new IDs for any LOB that previously synchronized with the Configuration Server database (since these IDs may already be used in strategies).
- 7. Wait for Knowledge Manager data to be synchronized.

Categories, standard responses, and field codes can have the same names in both LOBs, but not the same IDs. However, root categories and screening rules must have different names. IDs of these objects must be different as they are used as Configuration Server database object names.

Copying Knowledge Manager Data from One LOB to Another

Copying Knowledge Manager objects from one LOB to another can give rise to an issue with duplicated IDs. To avoid this you must rename the root category. This cannot be done in Knowledge Manager; instead you must manually edit the exported file, as in the following procedure. To copy Knowledge Manager data from one LOB to another:

- 1. Back up the UCS and Configuration Server databases.
- 2. Ensure that the target UCS is not able to write to the Configuration Server database.
- 3. Export the desired Knowledge Manager objects from the source UCS.
- 4. Rename the exported .kme file to a .zip file and extract the content, preserving the folder structure.
- 5. Open the category-sre folder and rename the folders that it contains. These folders are the root categories.
- 6. Compress the category-sre, field-codes and screening-rules files back to .zip files.
- 7. Rename the .zip file to .kme file.
- 8. Import the data into the target UCS, being sure to select Preserve uniqueness of objects by creation of new UCS IDs.
- 9. If you imported screening rules, you must now rename them.
- 10. Stop UCS, then set options and access rights as described in Configuration Procedure.
- 11. Start UCS and wait for Knowledge Manager to be synchronized to the Configuration Server database.

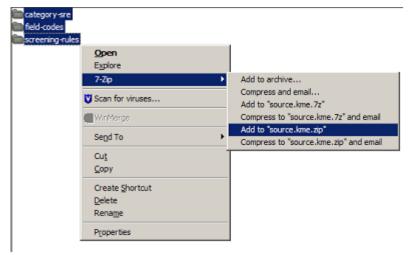


Figure 10: Knowledge Manager Folders Must be at the Root of the Zip File

Use with Other Genesys Applications

Access groups offer a generic ability to restrict access by other Genesys applications to the Configuration Server database. Consider, for example, Interaction Routing Designer (IRD). If IRD uses the default system account for logging into the Configuration Server database, it will have access to categories and screening rules for all LOBs. In this situation the strategy developer must keep track of which objects belong to which LOB. Otherwise, he or she runs the risk of creating strategies that request rendering of a standard response that does not exist in that UCS. This is why Genesys has recommended the use of a LOB-specific naming convention on root categories and screening rules. However, if IRD logs in using the lob-email-user account, it will only have access to objects relevant to the email LOB.

Limitations

- If IRD does not log in with a limited user, it will have access to standard responses that belong to other UCS, which makes it easy to create invalid strategies, as described in the preceding section.
- It is preferable to use one Universal Routing Server and one Interaction Server per business unit in order to prevent interactions from switching from one LOB to another.
- The solution described here makes it difficult to have multiple users to manage different objects in the Configuration Server database, such as when there is one user account per real person. It is preferable to have exactly one account for each LOB.
- All UCS instances access the same Business Attributes. This makes it difficult to define different Contact Attributes, Interaction Attributes, Media, Languages, and so on in different UCS instances. The only solution is to manually apply the access limitation to each created object.
- Applications (whether desktops or servers) that are not connected to Configuration Server using limited user(s) will see standard responses that are not usable by connected UCS instances. While Genesys applications can be configured to prevent this, that configuration must be done manually. It is preferable to use UCS as source for standard response titles anyway.