

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

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.

Important

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, email and chat.

Configuration Procedure

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.



,	🖳 New Person () (0) [:	suite76:2020] Properties	×						
	General Ranks Member Of Annex								
	Eirst:								
	Last:	_							
	<u>T</u> enant:	🛦 Environment 💌 🥵							
	<u>E</u> mployee ID:	lob-email-user							
	E- <u>M</u> ail:	•							
	☐Internal Authentication <u>U</u> ser Name:	lob-email-user							
	Enter Password:								
	<u>R</u> e-enter Password:								
	External Authentication								
	External User ID:	▼							
		✓ State Enabled							
	ОК	Cancel Make New Help							

Figure 3: Creating a Person

- 3. Configure each access group's permission to access configuration objects:
 - a. Right-click the tenant.
 - b. On the Security tab, click Permissions.
 - c. In the resulting Object Permission dialog, click Add...
 - d. 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.

-			1 1		
All Folders	Contents of '/Configu	uration/Environment/A	ccess Groups/lob-er	mail	
Configuration	UserName 🔺	First Name	Last Name	Employee ID	Agent
🖃 \land Environment	Enter text h 🍸	Enter text h 🍸	Enter text h 🍸	Enter te 🍸	Enter te
Access Groups	🔒 lob-email-user			lob-email-user	False
Administrators	1	111			
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: 🛕 Enviror	nment	
	D · · ·	Names:	,		
	Permissions				
Object Permission					
Ohiosta Tasant "Facing and		Ada			
Object: Tenant Environment		se Aun	chat		
Replace Permissions Recursively		solot-	email		
Name 🔺	Access	Sur Sur	er Administrators		
SYSTEM	Special Access(F		ers		
Environment \default	Full Control				
Senvironment Administrators	Full Control				
Environment\Super Administrators	Full Control		Add Show	w <u>U</u> sers <u>M</u> e	mbers
Environment \Users	Special Access(F	RX) (XX)			
		Add Nam	nes:		
		Environr	nent\lob-chat;Environ	ment Vob-email;	
Type of A	Access: Full Control		-		
🕀 🚺 🔿 🕀 🖓	cel <u>A</u> dd	<u>R</u> emi			
		Type of	Access: Full Control		•
TVRS 1			<u></u>		
Dependence Contraction Contrac	1		OK	Cancel	<u>H</u> elp
Persons					
Figure 4: Setting 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.

General Tenants Server Info Start Info Connections Options Annex Security Depender	Chat Server 7.5.0 True Classification Server 7.5.0 True Co-Browsing Server 7.6.000.01 True				
View or set permission information on the selected item(s).	List Names From: Environment Names: default (default default) lob-chat-user ()				
Permissions					
Log On As	vide (vide)				
This Account:	Add Show Users Members Search				
	Add Name: Environment Vob-email-user				
	OK Cancel <u>H</u> elp				
OK Cancel Make 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.
 - a. Right-click the desired Attribute Value.
 - b. On the Security tab, click Permissions.
 - c. 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.

Business Attributes		1 disc	Contact Attributes First N
🕀 👪 Business Result	🔟 Last Name	False	Contact Attributes Last N
🕀 🦝 Case ID	🗊 Phone Number	False	Contact Attributes Phone
🕀 🦝 Category Structure	🗊 PIN	False	Contact Attributes PIN
Contact Attributes	🗊 Title	False	Contact Attributes Title
Attribute Values	🗊 customerId	False	
🖬 customerId (1128) [suite76:202	20] Properties	×	
C I A Security			
General Annex Security		1	
Permissions		a 11	
View or set permission	information on the		
selected item(s).			
<u>seen</u> y			
	Permissions		
Object Permission			
Object: Business Attribut	- Malue "eveteenedd"		
Object: Business Attribute	e value customend		
Name 📤	Access		
SYSTEM	Special Access(RX)		
Environment\default	Full Control		
default Tenant \Administrators	Full Control		
	Special Access(RX)		
	opeoidi / loocooli / log		
Environment\lob-chat	Full Control		
Environment Vob-chat	Full Control		
Environment Vob-chat Environment Vob-email	Full Control No Access)	
Environment Vob-chat Environment Vob-email Environment \Super Administrat	Full Control No Access ors Full Control)	
Environment Vob-chat Environment Vob-email Environment \Super Administrat	Full Control No Access ors Full Control)	
Environment Vob-chat Environment Vob-email Environment \Super Administrat	Full Control No Access ors Full Control)	
Environment Vob-chat	Full Control No Access ors Full Control cess: No Access)	

Figure 6: LOB-Specific Contact Attributes

The email UCS will now behave as if customerId does not exist.

Important

Genesys recommends doing this before starting the email 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.

🕀 🥵 Cas	e ID 🔺	Display N	ame 🐣	Def	ault	Description	
🗉 灥 Cat	egory Structure	Enter tex	t here	T Ente	er te 🍸	Enter text h	iere
🖃 🏪 Con	tact Attributes	🗊 custor	merId	Fals	e		
Ξ 🧰	Attribute Values						
_ (🔁 chat-specific)						
🕀 🔒 Cus	tomer Segment						
🗉 🍪 🗖 🗖	biect Permission					×	a
• 📇 🗖						_	-
🗄 (🚧 👘	Object: Folder "chat-s	pecific"					
± (👝	Replace Permissions Recurs	ivelv					
± (,		
± (Name 🚔		Access		Propagate	▲	
± (SYSTEM		Special Access(RX)	✓		
± (📲 Environment \default		Full Control		✓		
± (🏚 default Tenant \Administrato	rs	Full Control		✓		
± (& default Tenant \Users		Special Access(RX)	✓		
± (🚯 Environment \Business Unit	Chat	Full Control		~		
± (Environment \Business Unit	Email	No Access		v	Ţ	
± ((<u></u>		
± (т						
± (<u>ц</u>	/pe or Acce	ess: TNO Access			<u> </u>	
± (I	1	1 .	1		
± (OK	Cancel	<u>A</u> dd	<u><u>R</u>e</u>	move	Help	
± (

Figure 7: Chat-Specific Contact Attributes

7. Further configuration of UCS Application objects.

Important

Both Primary and Backup UCS must have the same configuration options and permission settings.

a. 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 (1	86) [suite76:2020] Pi	operties	×	
Connections	Ontions Anney	Security Depend		
Permissions	View or set permission inf	omation on the		
size Til	selected item(s).		Object Permission	
		<u>P</u> emissions	Object: Application "UCS_cha	st"
			Name A	Access
			EVERYONE	Special Access(RX)
Log on no			SYSTEM	Special Access(RX)
O SYSTE	M Account		Environment \default	Full Control
				Full Control
This Account: Environment Vob-chat			A Environment Vob-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> emove
С ок	Cancel	M <u>a</u> ke New He	elp	

Figure 8: UCS Application Permissions

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

General	Tenants	Se	ver Info	Start Info
Connections	Options /	nnex	Security	Dependenc
settings	- D		× 🔜 d	» 🔉 🕑
Name 🔺		1	/alue	
Enter text here	÷	78	Enter text her	e 🍸
be allow-addit	ional-column		TRUE"	
allow-missi	ng-index		TRUE"	
archiving-r	b-records-per-ta	sk "	1000"	
archiving-t	ask-pool-size		4"	
auto-propa	gate-rights	•1	true"	
abc convert-idr	n-to-unicode		FALSE"	
abc enable-rep	orting		TRUE"	
abcfieldcode-f	ormat-locale			
be hide-attack	ned-data		TRUE"	
abc log-db-flow	rate		TRUE"	
abclog-memory	/-usage		TRUE"	
abc max-select	-count		2000"	
abc openmedia	-create-full-inter	action "	FALSE"	
obs primary-attr	ibute-lookup-stra	ategy "	TRUE"	-
4				•
	_			

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.
- 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.

Important

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 $\ensuremath{\mathsf{File}}$

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.