Customized Organizational Unit for LDAP Integration Between Call Manager and Active Directory

Contents

Introduction Prerequisites Requirements Components Used Configure Configuration on AD server Configuration on CUCM Verify Troubleshoot

Introduction

This document describes the procedure to create a new customized Organizational Unit (OU) for special users when you have a primary OU.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Active Directory (AD) server.

Components Used

The information in this document is based on Cisco Unified Call Manager (CUCM) Release 10.5.2.13900-12.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Configuration on AD server

Step 1. Create a new OU.

Right-click the primary OU and choose New > Organizational Unit.



Step 2. Check the newly created OU. (In this example, the newly created OU is "CIsco_TAC.")



Step 3. Add users in the new OU.

Right-click the new OU and choose **New > User**.



Step 4. Create a user who will bridge the gap between the AD server and CUCM.

Right-click **Users** and choose **New > User**.

📔 Active Directory Users and Computers 📃 🔲 🗙									
File Action View Help									
📃 Active Directory Users and Comput 🛛 🔊	lame	Туре	Description						
 Active Directory Users and Comput Saved Queries ramebala.com Builtin Cisco_ICM Computers Domain Controllers ForeignSecurityPrincipals ForeignSecurityPrincipals Managed Service Accounts sachin User Cisc Delegate Control Find New All Tasks View Refresh Export List Properties Help 	Administrator Administrator Allowed RODC Password Res ccm admin Cert Publishers Denied RODC Password Res Donain RODC Password Res Donain GOC Password Res Donain Computers Domain Computers Domain Computers Domain Computers Domain Guests Computer Contact Group InetOrgPerson msImaging-PSPs MSMQ Queue Alias Printer User Shared Folder	Type User security Group - Domain Local User Security Group - Domain Local plicati Security Group - Domain Local Security Group - Global Security Group - Universal rs Security Group - Domain Local ver Security Group - Domain Local ers Security Group - Domain Local security Group - Domain Local Security Group - Global	Description Built-in account for admini Members in this group can Members of this group can DNS Administrators Group DNS clients who are permi Designated administrators All domain controllers in th All domain users Designated administrators Members of this group are All domain tusers Designated administrators Members of this group can Members in this group can Members of this group can Built-in account for guest Members of this group can Designated administrators						
Create a new object									

The new user is created. This user must be a member of **domain admin**.

ccm admin Properties			? ×				
Dial-in Environment	Sessions	Remot	e control				
Remote Desktop Services Profile	Personal Virtu	ial Desktop	СОМ+				
General Address Account Profile	Telephones	Organization	Member Of				
<u>U</u> ser logon name:							
cadmin	@ramebala.com	n	•				
User logon name (pre- <u>W</u> indows 2000):						
RAMEBALA	cadmin						
Logon Hours Log On <u>T</u> o							
Unlock account							
Account <u>o</u> ptions:							
User must change password at	next logon		-				
User cannot change password							
Password never expires							
Store password using reversible	encryption		_				
CAccount expires							
Ne <u>v</u> er							
◯ End of: Saturday , August 06, 2016 🔽							
ОК	Cancel	Apply	Help				

Step 5. Right-click User > Properties.

On the Properties dialog, select the **Member Of** tab.

On the Member Of tab, click Add.

ccm admin Properties	? ×
Dial-in Environment Remote Desktop Services Profile General Address Account Pr	Sessions Remote control Personal Virtual Desktop COM+ ofile Telephones Organization Member Of
Member of:	actory Domain Services Folder
Domain Admins ramebala.c	com/Users
A <u>d</u> d <u>R</u> emove	
Primary group: Domain Admi	ns
Set Primary Group There i you ha applica	s no need to change Primary group unless ve Macintosh clients or POSIX-compliant tions.
ОК	Cancel Apply Help

Step 6. For the "object names to select," enter "domain admin" and click Check Names.

Select Groups	? ×
<u>S</u> elect this object type:	
Groups or Built-in security principals	Object Types
From this location:	
ramebala.com	Locations
Enter the object names to select (<u>examples</u>):	
domain admin	Check Names
Advanced OK	Cancel

Step 7. Select Domain Admins and click Set Primary Group; then remove Domain Users.

ccmadmin cucm Properties ? 🔀							
Dial-in Environment Sessions Remote control Remote Desktop Services Profile Personal Virtual Desktop COM+ General Address Account Profile Telephones Organization Member Of							
Member of:							
Name Active Directory Domain Services Folder							
Domain Admins ramebala.com/Users Domain Users ramebala.com/Users							
A <u>d</u> d <u>R</u> emove							
Primary group: Domain Admins <u>Set Primary Group</u> There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.							
OK Cancel Apply Help							

Step 8. Right-click the new OU (Cisco_TAC in this example) and choose Properties.



Step 9. On the Properties dialog, select the Managed By tab and click Change.

Cisco_TAC Properties		? ×
General Managed By	СОМ+	
Name:		
[Change Prop	oerties Clear
Office:		
Street:		 ▼
City:		
State/province:		
Country/region:		
Telephone number:		
Fax number:		
	ОК	Cancel <u>Apply</u>

Step 10. Enter the object name to select (the user name created to bridge the AD server and CUCM in step 4) and then click **Check Names.**

Select User, Contact, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
ramebala.com	Locations
Enter the object name to select (<u>examples</u>):	
ccmadmin cucm (ccmadmin@ramebala.com)	Check Names
Advanced	OK Cancel

Configuration on CUCM

Step 11. Go to **System > LDAP > LDAP System**.

Server		M Administration		Na	vigation Cisco Unified CM A	dministrat	ion 🔻 G
Cisco Unified CM		inications Solutions		ccmadmin	Search Documentation	Abou	t Logo
Cisco Unified CM Group		rces · Advanced Features · Device	✓ Application ✓ User Management ✓ Bulk Administration ✓ Help ✓				
Presence Redundancy Groups	1						
Phone NTP Reference	1						
Date/Time Group	ļ	en 47 day(s) without a s	uccessful backup. Please verify backup configuration.				
BLF Presence Group					-		
Region Information	•	Administration				1 1 1	
Device Pool	ľ				1	14.	7
Device Mobility	•	12					非上
DHCP	•	tel(R) Xeon(R) CPU X7560 @ 2.	27GHz, disk 1: 110Gbytes, 4096Mbytes RAM, Partitions aligned				4
LDAP	•	LDAP System					1
SAML Single Sign-On		LDAP Directory					
Cross-Origin Resource Sharing		LDAP Authentication					
(CORS)		LDAP Custom Filter	8 AM UTC, to node 10.106.99.195, from 10.196.120.81 using HTTPS				
Location into	۲ų	nc	J				

Step 12. Select the checkbox labeled Enable Synchronizing from LDAP Server.

System •	Call Routing	Media Resources 🔻	Advanced Features 🔻	Device - Application	▼ User Management ▼	Bulk Administration 💌	Help 🔻	
	DAP System Configuration							
- Status								
(i) Ple	ase Delete All LD	AP Directories Before	Making Changes on Th	nis Page				
	ase Disable I DAP	Authentication Befor	e Making Changes on 1	This Page				
			e Hulding changes on i					
	system Informat	ion						
🗹 Ena	ble Synchronizing	from LDAP Server						
LDAP S	erver Type	Microsoft Active D	irectory	-				
LDAP A	ttribute for User I	D sAMAccountName		•				
(i) *	indicates require	d item.						

Step 13. Go to **System > LDAP > LDAP Directory**.

	Server	M Administration			Navigation Ci	sco Unified CM Administration 👻
	Cisco Unified CM	unications Solutions			ccmadmin Search	Documentation About Lo
	Cisco Unified CM Group	Irces - Advanced Features - Device	■ Application ■ User Management	 Bulk Administration Help 		
	Presence Redundancy Groups					
	Phone NTP Reference					
	Date/Time Group	ear All 🙀 Delete Selected				
	BLF Presence Group					
	Region Information					
	Device Pool					
	Device Mobility					
	DHCB					Rows per Page 50
_	DHCP		bh 👻	Clear Filter		
	LDAP •	LDAP System	rind rind			
	SAML Single Sign-On	LDAP Directory	LDAP Distinguished Name	LDAP User Search Base	2	LDAP Server Hosts(s)
	Cross-Origin Resource Sharing	LDAP Authentication	amebala.com	OU=sachin,DC=ramebala,DC=com		10.106.122.160
	(CORS)	LDAR Custom Filter				
	Location Info	Lover ousion ritter				

Step 14. Click Add new.

System ▼ Call Routing ▼ Media Reso	Durces Advanced Features	Device •	Application <	User Management <	Bulk Administration <	Help 🔻
LDAP Directory						
Save						
- Status						
(i) Status: Ready						
-LDAP Directory Information						
LDAP Configuration Name*	TAC_LDAP					
LDAP Manager Distinguished Name st	cadmin@ramebala.com					
LDAP Password*	•••••					
Confirm Password*	•••••					
LDAP User Search Base*	OU=Cisco_TAC,DC=ramebala,E	DC=com				
LDAP Custom Filter	< None >		-			

Note:

LDAP Configuration Name: This value is any name of an LDAP Configuration. **LDAP Manager Distinguished Name**: This value should be the user name of the AD and CUCM bridge user.

LDAP Password: This value is the password of the bridge user created in step 4.

LDAP User Search Base: To find this value, follow this procedure on the AD server:

A) Right-click on the OU and select **Properties**.

Active Directory Users and Computers										
File Action View Help										
← ⇒ 2 📰 🔏 🖹 🗙 🖻 Q 📾 🛛 🖬 🖏 🖄 🍞 🛛 🤽										
Active Directory Users and Compu	Name Type	Description								
 ★ Saved Queries ★ Builtin ★ Builtin ★ Cisco_ICM ★ Compt ★ Compt ★ Compt ★ Compt ★ Domain ★ Nanac All Tasks ★ Manac ★ Nanac ★ New All Tasks ★ Wiew ★ Syster ★ Wiew ★ Delete Rename Refresh Export List Properties Help 	There are no items to show in this view.									
	Image: A state of the state									
Opens the properties dialog box for the	current selection.									

B) On the Properties dialog, select the **Attribute Editor** tab and find the "distinguishedName" value.

Ciso	:o_TAC Properties	? ×
Ġ	eneral Managed By C	Ibject Security COM+ Attribute Editor
	Attribute	Value
	с	<not set=""></not>
	cn	<not set=""></not>
	со	<not set=""></not>
	countryCode	<not set=""></not>
	defaultGroup	<not set=""></not>
	description	<not set=""></not>
	desktopProfile	<not set=""></not>
	destinationIndicator	<not set=""></not>
	displayName	<not set=""></not>
	displauNamePrintable	(not set)
	distinguishedName	OU=Cisco_TAC,DC=ramebala,DC=com
	Conolgnataro	- and tools
	dSCorePropagationD	7/7/2016 2:12:25 AM Pacific Daylight Time;
	extensionName	<not set=""></not>
	· · · <u>-</u> · · · · ·	
	<u>, </u>	
	View	Filter
	OK	Cancel Apply Help

Step 15. Here, keep the LDAP Server IP address and Port.

	LDAP Port * Use TLS
10.106.122.160	389

Step 16. Click Save.

Step 17. Click Perform Full Sync Now.



Verify

In order to verify the user on CUCM, navigate to **User Management > End User**.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.