Configure CUCM for Secure LDAP (LDAPS)

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Verify and Install LDAPS Certificates
Configure Secure LDAP Directory
Configure Secure LDAP Authentication
Configure Secure Connections to AD for UC Services
Verify
Troubleshoot
Related Information

Introduction

This document describes the procedure to update CUCM connections to AD from a non-secure LDAP connection to a secure LDAPS connection.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AD LDAP Server
- CUCM LDAP Configuration
- CUCM IM & Presence Service (IM/P)

Components Used

The information in this document is based on CUCM release 9.x and higher.

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, ensure that you understand the potential impact of any command.

Background Information

It is the responsibility of the Active Directory (AD) Administrator to configure AD Lightweight Directory Access Protocol (LDAP) for Lightweight Directory Access Protocol (LDAPS). This includes the installation of CA-signed certificates that meet the requirement of an LDAPS certificate.



Note: See this link for information in order to update from non-secure LDAP to secure LDAPS connections to AD for other Cisco Collaboration Applications: <u>Software Advisory: Secure LDAP</u> <u>Mandatory for Active Directory Connections</u>

Verify and Install LDAPS Certificates

Step 1. After the LDAPS certificate has been uploaded to the AD server, verify that LDAPS is enabled on the AD server with the **ldp.exe** tool.

- 1. Start the AD Administration Tool (Ldp.exe) on the AD server.
- 2. On the Connection menu, select **Connect**.
- 3. Enter the Fully Qualified Domain Name (FQDN) of the LDAPS server as the server.
- 4. Enter **636** as the port number.
- 5. Click **OK**, as shown in the image

	Ldp		- 0	x
Connection Browse	View Options Utilities	Help		
	Connect	X	1	
	Connect			
Se	rver: WIN-H2Q74S1U39P	.com		
Po	rt:	Connectionless		
		Count		
	OK	Cancel		
Ready			NUM	

For a successful connection on port 636, RootDSE information prints out in the right pane, as shown in the image:

😭 Idaps://W	IN-H2C	74S1U3	9P		.com/D	C=net	-		x
Connection B	Browse	View Op	tions	Utilities	Help				
		LDAP_OF Error 0 = Error 0 = Host sup Establish Retrieving Getting 1 Dn: (Roo confi C curre defau dnsH doma doma dsSe H fores highe isGlo	port_PRO Idap_c Idap_g ports S ed com base entries tDSE) guration N=Con entTime utNamin ostNamin ostNamin costNamin inContri inFunc inFunc inFunc instCom balCata	nNamingCon figuration,D ame: WIN-H2C rollerFunction ame: CN=NT S1U39P,CN= N=Sites,CN ionality: 6 = mittedUSN: 5 alogReady: 2 and TDUE	RSION, 3); ap, NULL); Ldap,LDAP_ her strength VIN-H2Q74S ation DC= 0:40:55 AM DC= 0:40:55 AM DC= 0:40:50 AM DC= 0:50 AM	OPT_SSL, n = 256 bits 1U39P ,DC=cor Central Da DC=cor WIN2012R R2); ,CN=WIN- =Default-Fi on,DC=r 2);	(void*) m; ylight com 2);)&lv); .com. Time; ; ; ; ; ;	< III >
Ready							NU	M	at

Repeat the procedure for port 3269, as shown in the image:



For a successful connection on port 3269, RootDSE information prints out in the right pane, as shown in the image:

gcs://WIN-H2Q	74S1U39P .com/DC=netw ×
Connection Browse	View Options Utilities Help
	Id = Idap_sslinit("WIN-H2Q74S1U39P .com", 636, 1); Error 0 = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3); Error 0 = Idap_connect(hLdap, NULL); Error 0 = Idap_get_option(hLdap,LDAP_OPT_SSL,(void*)&Iv); Host supports SSL, SSL cipher strength = 256 bits Established connection to WIN-H2Q74S1U39P .com. Retrieving base DSA information Getting 1 entries: Dn: (RootDSE) configurationNamingContext: CN=Configuration,DC=network218,DC=com; currentTime: 4/2/2020 10:40:55 AM Central Daylight Time; defaultNamingContext: CN=Configuration,DC=network218,DC=com; dumainControllerFunctionality: 6 = (WIN2012R2); domainFunctionality: 6 = (WIN2012R2); domainFunctionality: 6 = (WIN2012R2); h2Q74S1U39P,CN=Servers,CN=Default-First-Site- Name,CN=Sites,CN=Configuration,DC= m; forestFunctionality: 6 = (WIN2012R2); highestCommittedUSN: 500892'
Ready	NUM

Step 2. Obtain the root and any intermediate certificates that are part of the LDAPS server certificate and install these as tomcat-trust certificates on each of the CUCM and IM/P publisher nodes and as CallManager-trust on the CUCM publisher.

The root and intermediate certificates that are part of an LDAPS server certificate, <hostname>.<Domain>.cer, are shown in the image:

nome	Share	View							~
÷ → • ↑ 📙	> LD	APS → cert					5 v	8	Search c
1 0 ith man	^	Name	^		Date modified	Туре	Size		
			CERTCA2012-CA.cer		3/27/2020 8:57 AM	Security Certificate		2 KB	
Documents	× -		WIN-H2Q7451U39P-CA.	.com.cer	3/27/2020 8:55 AM	Security Certificate		2 KB	
Downloads	Я	WIN-H2C	74S1U39P .com.cer		3/27/2020 8:56 AM	Security Certificate		3 KB	

Navigate to CUCM publisher **Cisco Unified OS Administration > Security > Certificate Management**. Upload root as **tomcat-trust** (as shown in the image) and as **CallManager-trust** (not shown):

🙆 Upload Certificate/Certi	ficate chain - Mozilla Firefox	_				-	- a ×
🔽 🖗 https://10.201.	218.163/cmplatform/certi	ficateUpload.do	=		⊠ ☆	III\ 🗉 🖬	
Upload Certificate/Cer	tificate chain			.ogin 🚦 Sign	in to your account	Current 🗎 Tra	aining >>
Upload 🖳 Close				Navigation data	Cisco Unified OS Adm	inistration ntation About	GO GO
Status Warning: Uploading Upload Certificate/Ce Certificate Purpose* Description(friendly nam Upload File	a cluster-wide certificate w ertificate chain tomcat-trust Browse No file so File Upload	ill distribute it to all servers in this cluster					
i) *- indicates requi	\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This	PC > Desktop > LDAPS > cert			~	ڻ ب Se	arch cert
	Organize 👻 New folder	t					-
	Desktop ^	Name	Date mo	dified	Туре	Size	
<	LDAPS	-CERTCA2012-CA.cer	3/27/202	0 8:57 AM	Security Certificate	2 KB	
	TODO	-WN-H2Q74S1U39P-CA.ne	t 3/27/202	20 8:55 AM	Security Certificate	2 KB	
	Cisco	WIN-H2Q74S1U39P .com.cd	er 3/27/202	20 8:56 AM	Security Certificate	3 KB	

Upload intermediate as tomcat-trust (as shown in the image) and as CallManager-trust (not shown):

ፅ Upload C	Certificate/Certificat	e chain - I	Mozilla Firefox		- [I X					ø >
🛈 🔒 ht	ttps://10.201.218	8.163/cm	platform/certif	icateUpload.do		≡		🛛 t			۰ =
Upload Cer	rtificate/Certifi	cate cha	in			^	.ogin 🚦 Sign in to	your account	Current	🛅 Trai	ining 🚿
Upload	Close						Navigation <mark>Cisco</mark> admin S	Unified OS A Gearch Docun	dministration nentation	About	✓ Go Logout
Status i Succe i Resta i If	ess: Certificate Up art Cisco Tomcat S) File Upload	loaded ervice us	sing the CLI "uti	ls service restart Cisco Tor	mcat".			-	-		×
the	← → ∽ ↑	> This	PC > Desktop	> LDAPS > cert			~	Q O	Search cert		
Certific	Organize - N	lew folder								E 🕶 🛛	. 0
Descrip	E Desktop	^	Name	^	Date modifie	ed	Туре	Size			
Upload	LDAPS			-CERTCA2012-CA.cer	3/27/2020 8:	57 AM	Security Certificate	2 K	В		
	TODO			WIN-H2Q74S1U39P-CA.net	3/27/2020 8:	55 AM	Security Certificate	2 K	В		
Uploa	Cisco		WIN-H2Q7	4ร์โป39P .com.ce	r 3/27/2020 8:	56 AM	Security Certificate	3 K	В		

Note: If you have IM/P servers that are part of the CUCM cluster, you also need to upload these certificates to these IM/P servers.

Note: As an alternative, you can install the LDAPS server certificate as tomcat-trust.

Step 3. Restart Cisco Tomcat from the CLI of each node (CUCM and IM/P) in clusters. Additionally, for the CUCM cluster, verify that the Cisco DirSync service on the publisher node is started.

In order to Restart the Tomcat service, you need to open a CLI session for each node and run the command **utils service restart Cisco Tomcat**, as shown in the image:

P 10.201.218.163 - PuTTY	-		\times
<pre>login as: admin admin@10.201.218.163's password: Command Line Interface is starting up, please wait</pre>			^
Welcome to the Platform Command Line Interface			
<pre>/Mware Installation: 2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz Disk 1: 80GB, Partitions aligned 4096 Mbytes RAM</pre>			
admin:utils service restart Cisco Tomcat Do not press Ctrl+C while the service is restarting. If the service arted properly, execute the same command again. Service Manager is running Cisco Tomcat[STOPPING] Cisco Tomcat[STOPPING] Cisco Tomcat[STOPPING] Cisco Tomcat[STOPPING] Cisco Tomcat[STARTING] Cisco Tomcat[STARTING]	e has	not	rest
Cisco Tomcat[STARTED] admin:			

Step 4. Navigate to CUCM publisher **Cisco Unified Serviceability > Tools > Control Center - Feature Services**, verify that the **Cisco DirSync** service is activated and started (as shown in the image), and restart the **Cisco CTIManager** service on each node if this is used (not shown):

abab	Cisco Unified Serviceability			Navigation C	isco Unified Serviceability 🗸 🗸	Go
cisco	For Cisco Unified Communications Solutions				admin About Lo	gout
Alarm 🔻	Irace - Tgols - Snmp - CallHome - Help -					
Control C	Center - Feature Services			Related Links:	Service Activation 🗸 🗸	Go
Sta	rt 🛑 Stop , Restart 🔇 Refresh Page					
Status:						_
() Read	ly D					
Select	Server					
Server*	cucmpub218comCUCM Voice/Video v	Go				
Perform	nance and Monitoring Services					
	Service Name	Status:	Activation Status	Start Time	Up Time	
0	Cisco Serviceability Reporter	Started	Activated	Fri Nov 8 09:30:34 2019	146 days 00:27:49	
0	Cisco CallManager SNMP Service	Started	Activated	Fri Nov 8 09:30:36 2019	146 days 00:27:47	
Directo	ry Services					
	Service Name	Status:	Activation Status	Start Time	Up Time	
۲	Cisco DirSync	Started	Activated	Wed Mar 25 12:17:13 2020	7 days 22:41:10	

Configure Secure LDAP Directory

Step 1. Configure the CUCM LDAP Directory in order to utilize LDAPS TLS connection to AD on port 636.

Navigate to **CUCM Administration > System > LDAP Directory**. Type the FQDN or the IP address of the LDAPS server for LDAP Server Information. Specify the LDAPS port of **636** and check the box for **Use TLS**, as shown in the image:

aluda Cisco Unified CM Administration	Navigation Cisco Unified CM Administration 🗸 Go
CISCO For Cisco Unified Communications Solutions	admin Search Documentation About Logo
System 🔻 Call Routing 👻 Media Resources 👻 Advanced Features 🗶 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻	
LDAP Directory	Related Links: Back to LDAP Directory Find/List 🗸 Go
🔚 Save 💥 Delete 🗈 Copy 🏷 Perform Full Sync Now 🖧 Add New	
- Group Information	
User Rank* I_Dofault Liser Pank	
Access Control Groups	
Add to Access Control Group	
Remove from Access Control Group	
2	
Feature Group Template < None >	
Warning: If no template is selected, the new line features below will not be active.	
Apply mask to synced telephone numbers to create a new line for inserted users	
Mask	
Assign new line from the goal list if one was not created based on a sweed LDAR telephone symbol	
Assign new me rom the poor list if one was not created based on a synced LOAP telephone number	
Order DN Pool Start DN Pool End	
Add DN Pool	
-LDAP Server Information	
Host Name or IP Address for Server" LDAP Port" Use TLS	
WIN-H2Q/451039Rcom 636	
Add Another Redundant LDAP Server	



Note: By default, after versions 10.5(2)SU2 and 9.1(2)SU3 FQDN configured in LDAP Server Information are checked against the Common Name of the certificate, in case the IP address is used instead of the FQDN, the command **utils ldap config ipaddr** is issued to stop the enforcement of

FQDN to CN verification.

Step 2. In order to complete the configuration change to LDAPS, click **Perform Full Sync Now**, as shown in the image:

Julia Cisco Unified	CM Administration	Navigation Cisco Unified CM Administration 🗸 160								
CISCO For Cisco Unified Con	nmunications Solutions	admin Search Documentation About Logout								
System • Call Routing • Media Resou	arces • Advanced Features • Device • Application • User Man	spenent ♥ Bulk Administration ♥ Help ♥								
LDAP Directory Related Links: Elsk to LDAP Directory And Link - 3										
🔜 Save 🗶 Delete 🗋 Copy 👔	🕐 Perform Full Sync Now 🖓 Add New									
c Status										
0	Aarus									
Update successful. Perform a s	ynchronization operation (manual or scheduled) to synchronize ch	anges with the directory.								
LDAP Directory Information										
LDAP Configuration Name*	LDAP-218									
LDAP Manager Distinguished Name*	Administrator@i com									
LDAP Password*										
Confirm Password*										
LDAP User Search Base*	cn+users,dc+ dc+com									
LDAP Custom Filter for Users	< None > v									
Synchronize*	Users Only Users and Groups									
LDAP Custom Filter for Groups	< None >									
1										

Step 3. Navigate to **CUCM Administration > User Management > End User** and verify that end-users are present, as shown in the image:

cisco	Cisco Unified CM Administration Navigation Go Cisco Unified CM Administration Go Go Cisco Unified Communications Solutions admin Search Documentation About Logour											
System -	System 🔻 Cal Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻											
Find and	Find and List Users											
🕂 Add	👍 Add New 🏢 Select All 🔛 Clear All 💥 Delete Selected											
Status -	Status (i) 3 records found											
User	(1 - 3 of 3)								Rows per Pag	ge 50 🗸		
Find Use	r where First na	me v be	egins with 🗸		Find Clear Fi	lter 🕂 🛥						
	User ID *	Meeting Number	First Name	Last Name	Department	Director	y URI	User Status	U	lser Rank		
	gstacy	2183	Gwen	Stacy		gstacy@	com	Active Enabled LDAP Synchronized User	1			
	hosborn	2182	Harry	Osborn		hosborn@	.com	Active Enabled LDAP Synchronized User	1			
	pparker	2181	Peter	Parker		pparker@:	.com	Active Enabled LDAP Synchronized User	1			

Step 4. Navigate to **ccmuser** page (**https://<ip address of cucm pub>/ccmuser**) in order to verify that the user log in is successful.

The ccmuser page for CUCM version 12.0.1 looks like this:

Cisco Unified Communications
Self Care Portal
Username

	Username	
	Password	
(Sign In)

The user can successfully log in after LDAP credentials are entered, as shown in the image:

cisco Unified Communications Self Care Portal	Skip to Content
Phones Voicemail IM & Availability General Settings Downloads	About Help
My Phones My Phones Phone Settings Call Forwarding Call Forwarding Company Phones These are the phones provided to you by your company. You may set personal preferences for these in Phone Settings Cisco 8865 2183	_

Configure Secure LDAP Authentication

Configure CUCM LDAP Authentication in order to utilize LDAPS TLS connection to AD on port 3269.

Navigate to **CUCM Administration > System > LDAP Authentication**. Type the FQDN of the LDAPS server for LDAP Server Information. Specify the LDAPS port of **3269** and check the box for **Use TLS**, as shown in the image:

ululu Cisco Unified	CM Administration		Navigation Cisco Unified CM Administration	√ Go
For Cisco Unified Co	mmunications Solutions		admin Search Documentation About	Logout
System - Call Routing - Media Reso	ources - Advanced Features - Device - Application - User Ma	nagement 👻 Bulk Administration 👻 Help 👻		
LDAP Authentication				
Save				
Status				
(i) Update successful				
LDAP Authentication for End Us	iers			
Use LDAP Authentication for En	d Users			
LDAP Manager Distinguished Name	* Administrator@ .com			
LDAP Password*		1		
Confirm Password*	••••••	1		
LDAP User Search Base*	cn=users,dc= dc=com			
LDAP Server Information				
н	ost Name or IP Address for Server*	LDAP Port* Use TLS		
WIN-H2Q74S1U39P	om	3269		
Add Another Redundant LDAP S	erver			



Note: If you have Jabber clients, it is recommended to use port 3269 for LDAPS Authentication, since Jabber timeout for log in can occur if a secure connection to the global catalog server is not specified.

Configure Secure Connections to AD for UC Services

If you need to secure UC services that utilize LDAP, configure these UC services to utilize port 636 or 3269 with TLS.

Navigate to **CUCM administration > User Management > User Settings > UC Service**. Find Directory Service that points to AD. Type the FQDN of the LDAPS server as the Host Name/IP Address. Specify the port as **636** or **3269** and **protocol TLS**, as shown in the image:

Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration V G0 admin Search Documentation About Logout			
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help				
UC Service Configuration	Related Links: Back To Find/List 🧹 Go			
🔚 Save 🗶 Delete 🗈 Copy 🍄 Reset 🧷 Apply Config 🕂 Add New				
r Status -				
Update successful				
r UC Service Information				
UC Service Type: Directory				
Product Type* Directory				
Name* Secure Directory				
Description				
Host Name/IP Address* WIN-H2Q74S1U39P .com				
Port 636				
Protocol TLS V				
Save Delete Copy Reset Apply Config Add New				
(i) *- indicates required item.				



Note: The Jabber client machines also need to have the tomcat-trust LDAPS certificates that were installed on CUCM installed in the certificate management trust store of the Jabber client machine in order to allow the Jabber client to establish an LDAPS connection to AD.

Verify

Use this section to confirm that your configuration works properly.

In order to verify the actual LDAPS certificate/certificate chain sent from the LDAP server to CUCM for the TLS connection, export the LDAPS TLS Certificate from a CUCM packet capture. This link provides information on how to export a TLS certificate from a CUCM packet capture: <u>How to Export TLS</u> <u>Certificate from CUCM Packet Capture</u>

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.

Related Information

- This link provides access to a video that walks through the LDAPS configurations: <u>Secure LDAP</u> <u>Directory and Authentication Walkthrough Video</u>
- <u>Technical Support & Documentation Cisco Systems</u>