

# CUCM configureren voor beveiligde LDAP (LDAPS)

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[LDAPS-certificaten controleren en installeren](#)

[Secure LDAP-map configureren](#)

[Secure LDAP-verificatie configureren](#)

[Beveiligde verbindingen met AD configureren voor UCS-services](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

---

## Inleiding

In dit document wordt de procedure beschreven om CUCM-verbindingen naar AD van een niet-beveiligde LDAP-verbinding naar een beveiligde LDAPS-verbinding bij te werken.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AD LDAP-server
- CUCM LDAP-configuratie
- CUCM IM & Presence Service (IM/P)

### Gebruikte componenten

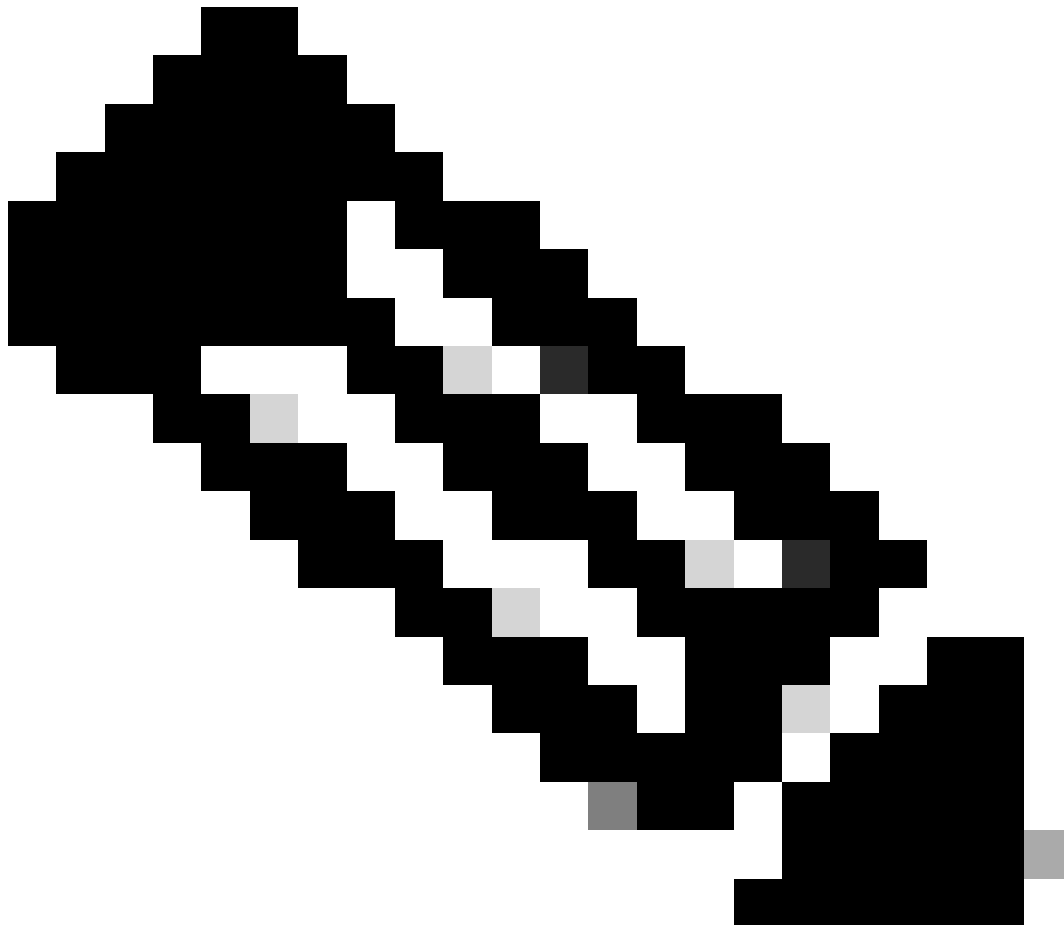
De informatie in dit document is gebaseerd op CUCM release 9.x en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Het is de verantwoordelijkheid van de beheerder van Active Directory (AD) om AD Lichtgewicht Directory Access Protocol (LDAP) te configureren voor Lichtgewicht Directory Access Protocol (LDAPS). Dit omvat de installatie van CA-ondertekende certificaten die voldoen aan de eis van een LDAPS-certificaat.

---



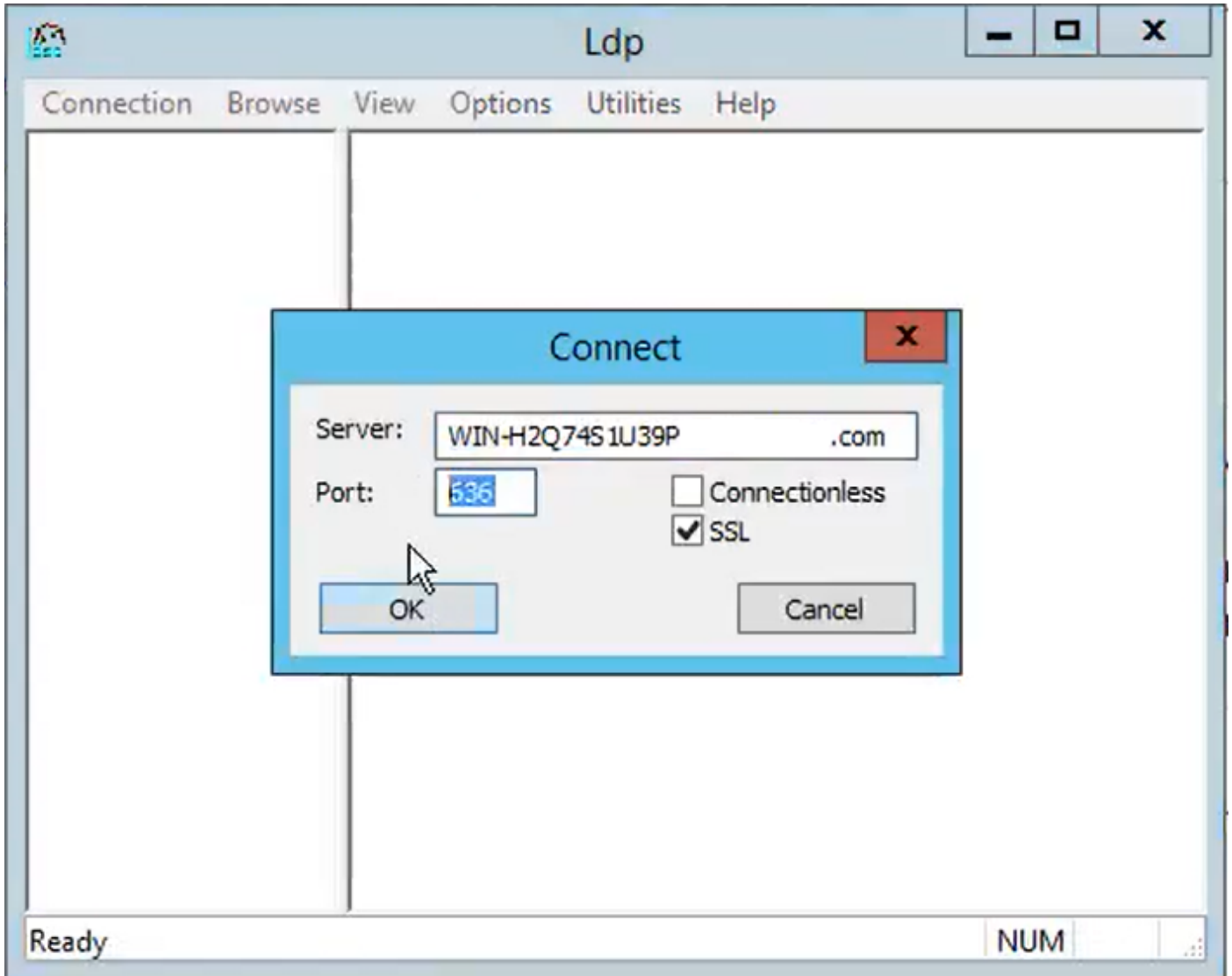
Opmerking: Raadpleeg deze link voor informatie over het bijwerken van niet-beveiligde LDAP om LDAPS-verbindingen naar AD te beveiligen voor andere Cisco Collaboration Application: [Software Advisory: Secure LDAP verplicht voor Active Directory Connections](#)

---

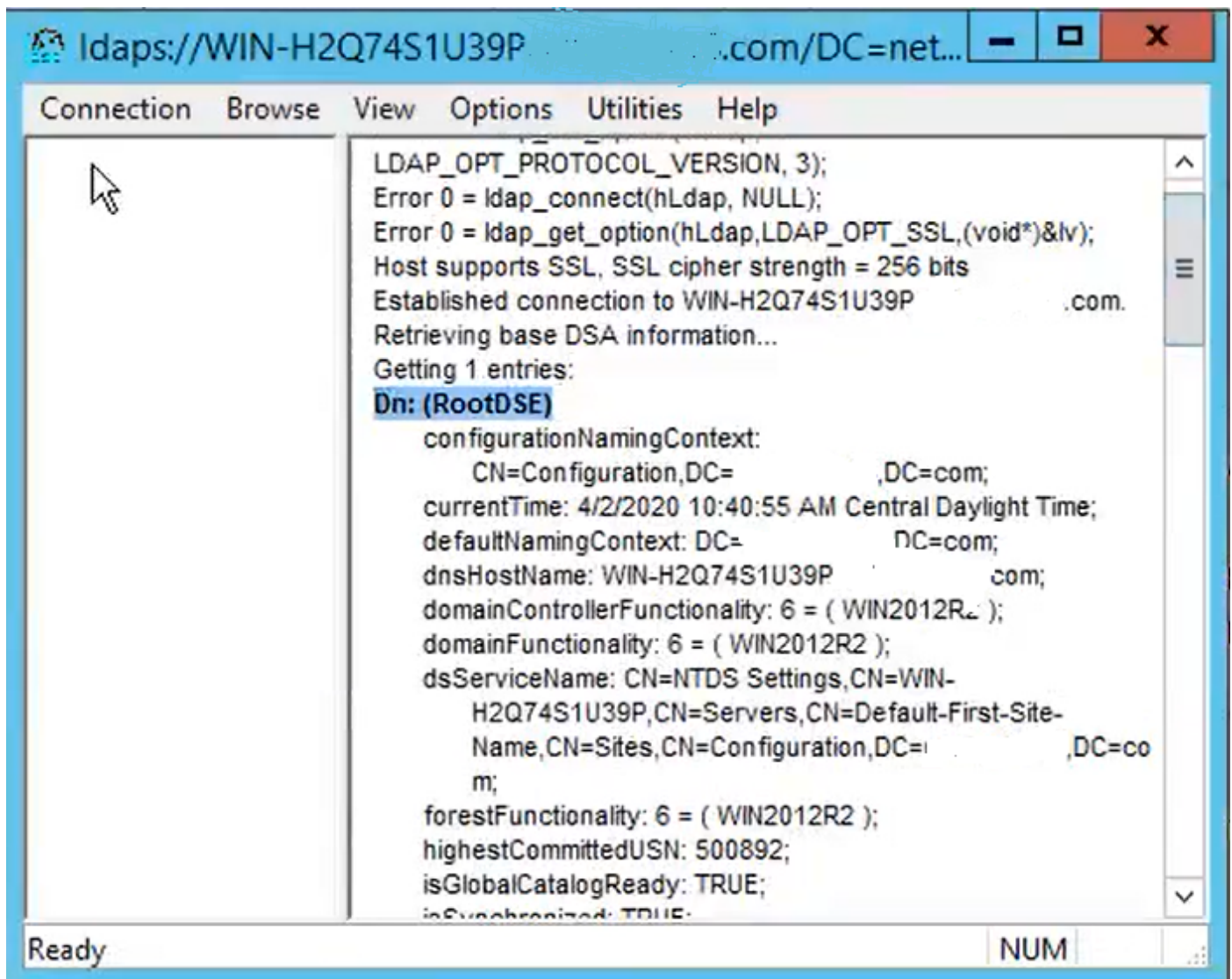
## LDAPS-certificaten controleren en installeren

Stap 1. Nadat het LDAPS-certificaat naar de AD-server is geüpload, controleert u of LDAPS op de AD-server is ingeschakeld met de tool ldp.exe.

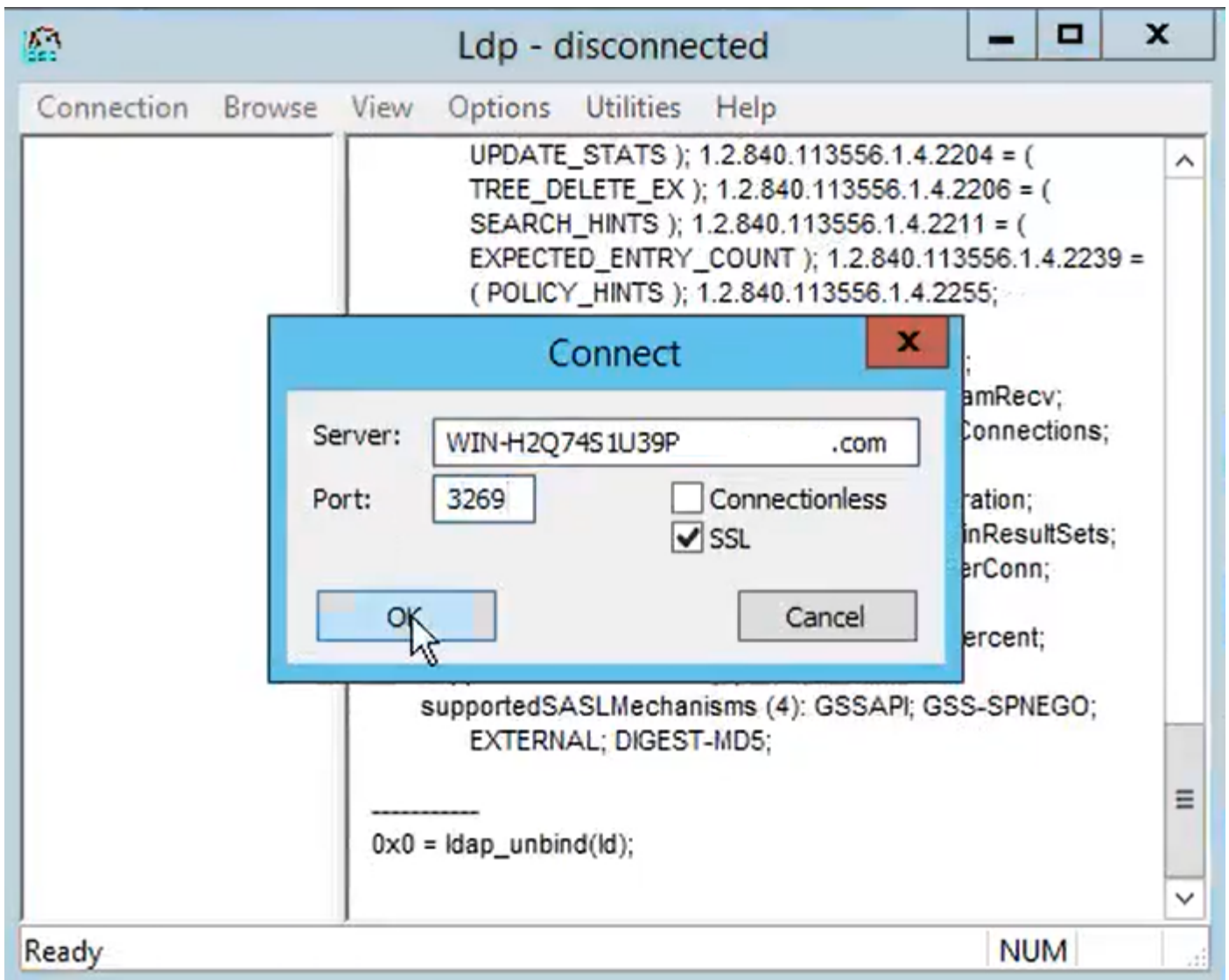
1. Start het AD-beheerprogramma (Ldp.exe) op de AD-server.
2. Selecteer in het menu Verbinding de optie Verbinden.
3. Voer de volledig gekwalificeerde domeinnaam (FQDN) van de LDAPS-server in als server.
4. Voer 636 in als poortnummer.
5. Klik op OK zoals in de afbeelding.



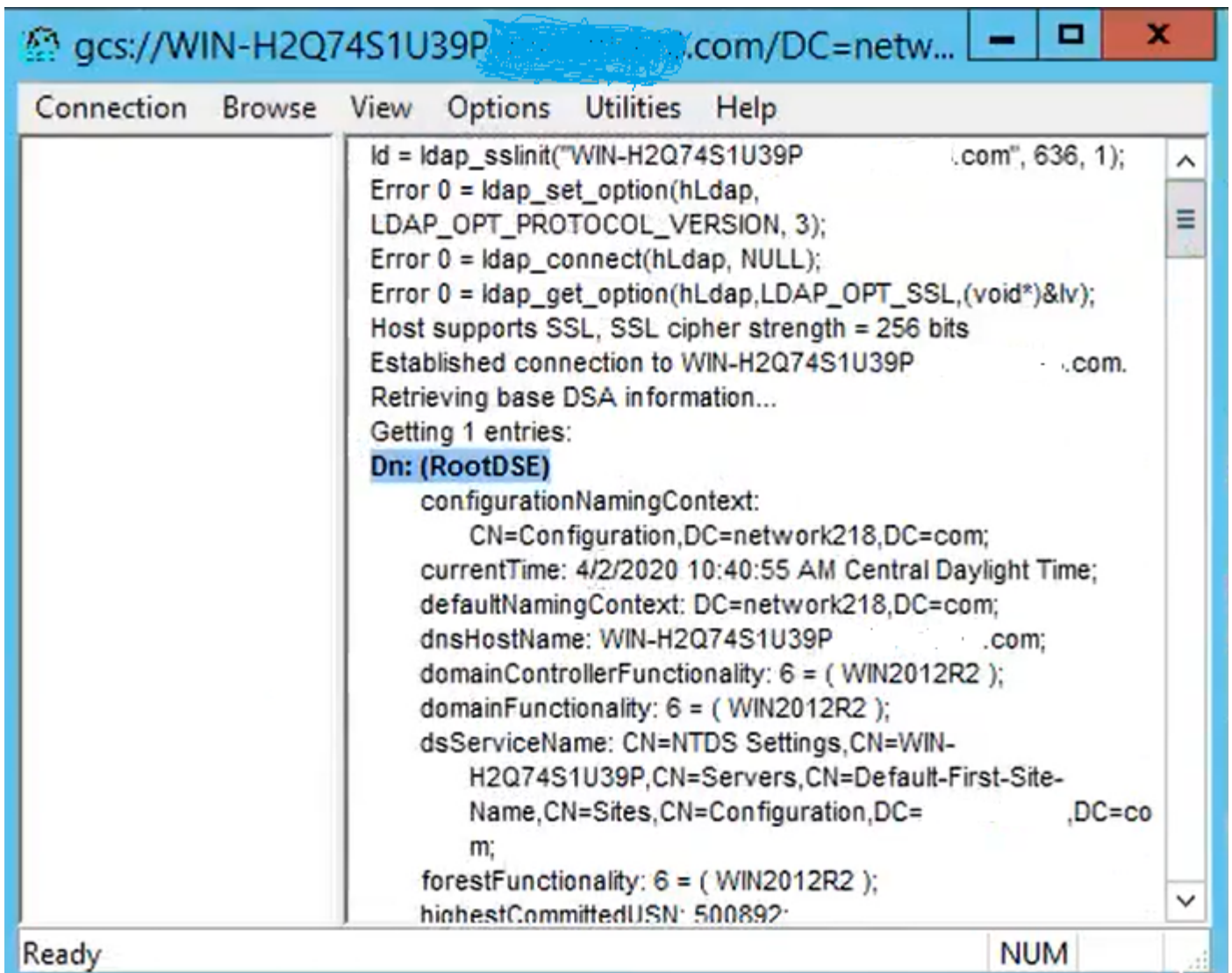
Voor een succesvolle verbinding op poort 636 wordt RootDSE-informatie in het rechter deelvenster afgedrukt, zoals in de afbeelding:



Herhaal de procedure voor poort 3269, zoals in de afbeelding:

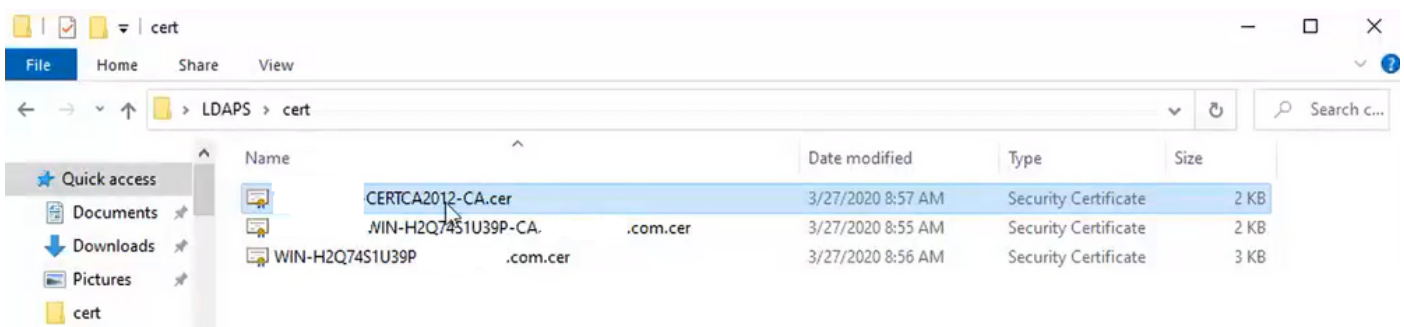


Voor een succesvolle verbinding op poort 3269, wordt de RootDSE-informatie in het rechterdeelvenster afgedrukt, zoals in de afbeelding:

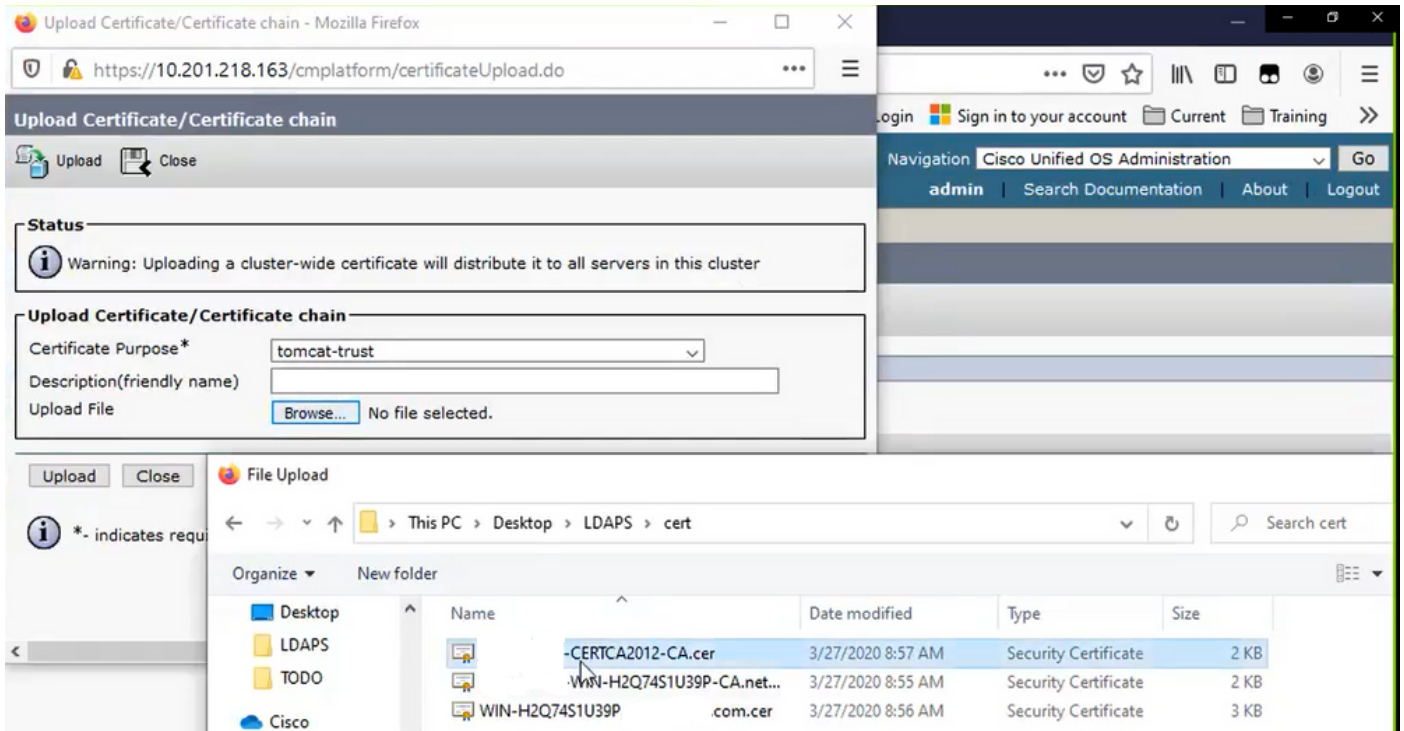


Stap 2. Verkrijg de wortel en om het even welke middencertificaten die deel van het LDAPS servercertificaat uitmaken en installeer deze als tomcat-trust certificaten op elk van de de uitgeversknooppunten van CUCM en IM/P en als CallManager-vertrouwen op de uitgever van CUCM.

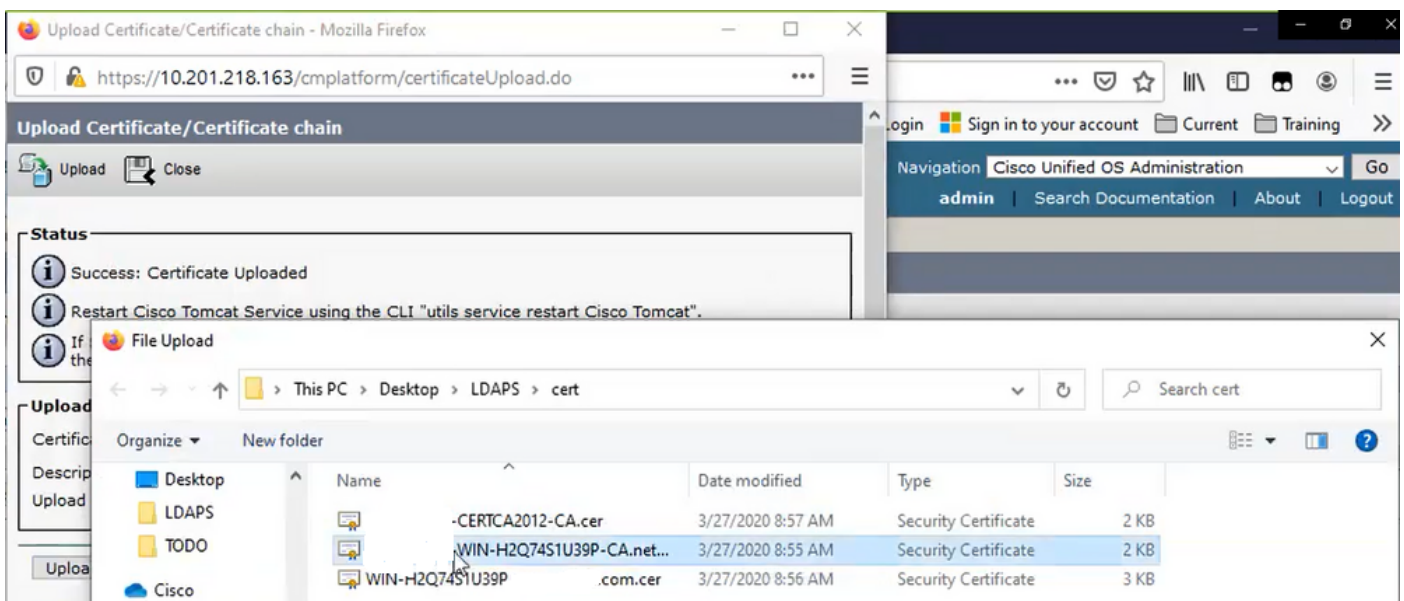
De basiscertificaten en tussentijdse certificaten die deel uitmaken van een LDAPS-servercertificaat, <hostname>.<Domain>.cer, worden in de afbeelding weergegeven:




Navigeer naar CUCM-uitgever Cisco Unified OS-beheer > Beveiliging > Certificaatbeheer. Upload root als tomcat-trust (zoals in de afbeelding) en als CallManager-trust (niet getoond):



Tussenpersoon uploaden als tomcat-trust (zoals in de afbeelding) en als CallManager-trust (niet weergegeven):

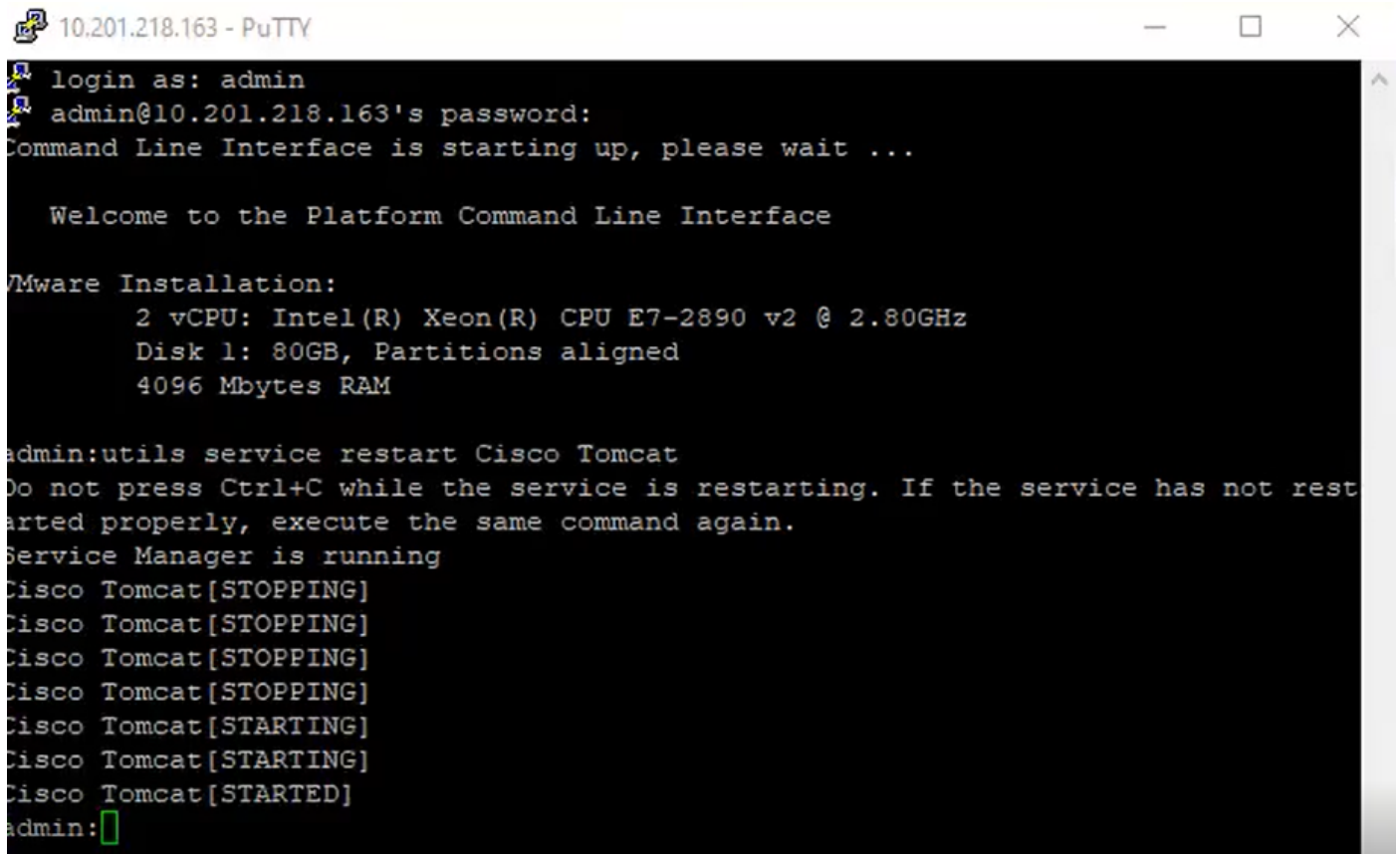


 Opmerking: als u IM/P-servers hebt die deel uitmaken van het CUCM-cluster, moet u deze certificaten ook uploaden naar deze IM/P-servers.

 Opmerking: Als alternatief kunt u het LDAPS-servercertificaat installeren als tomcat-trust.

Stap 3. Start Cisco Tomcat opnieuw vanaf de CLI van elk knooppunt (CUCM en IM/P) in clusters. Controleer voor het CUCM-cluster bovendien dat de Cisco DirSync-service op het uitverknooppunt is gestart.

Om de Tomcat-service te kunnen herstarten, moet u voor elke knooppunt een CLI-sessie openen en de Opnieuw opstarten van de service commando's uitvoeren op Cisco Tomcat, zoals in de afbeelding:



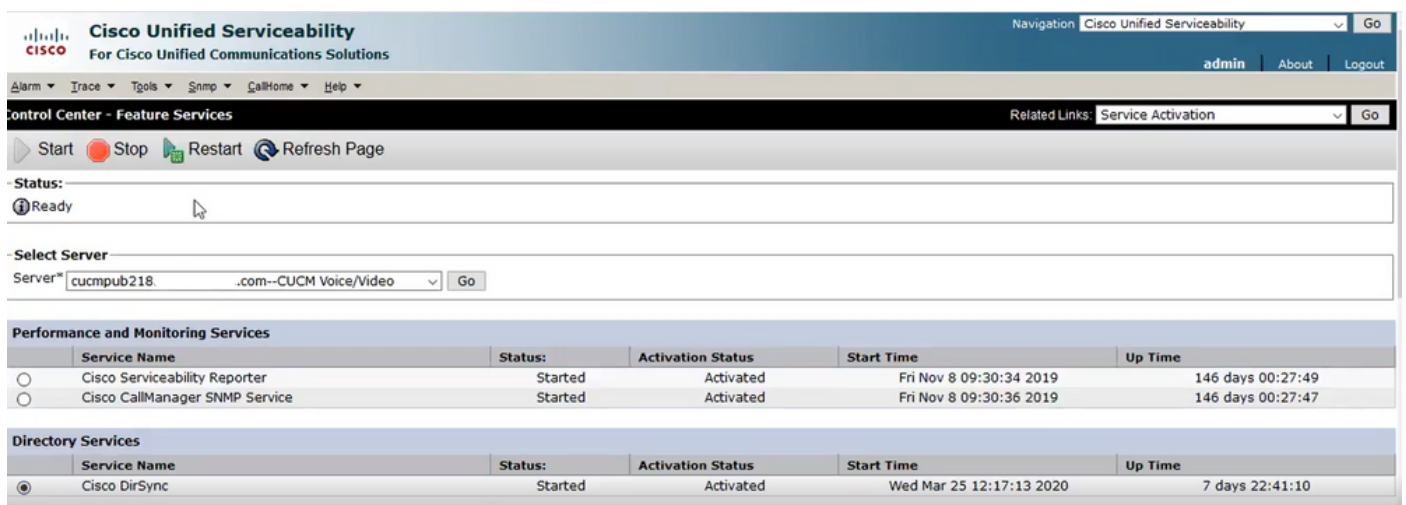
```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
  2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz
  Disk 1: 80GB, Partitions aligned
  4096 Mbytes RAM

admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
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]
Cisco Tomcat[STARTED]
admin:
```

Stap 4. Navigeer naar de CUCM-uitgever Cisco Unified Serviceability > Tools > Control Center - Feature Services, controleer of de Cisco DirSync-service is geactiveerd en gestart (zoals in de afbeelding) en start de Cisco CTIM Manager-service op elk knooppunt opnieuw als deze wordt gebruikt (niet weergegeven):



Performance and Monitoring Services						
Service Name	Status	Activation Status	Start Time	Up Time		
<input type="radio"/> Cisco Serviceability Reporter	Started	Activated	Fri Nov 8 09:30:34 2019	146 days 00:27:49		
<input type="radio"/> Cisco CallManager SNMP Service	Started	Activated	Fri Nov 8 09:30:36 2019	146 days 00:27:47		

Directory Services					
Service Name	Status	Activation Status	Start Time	Up Time	
<input checked="" type="radio"/> Cisco DirSync	Started	Activated	Wed Mar 25 12:17:13 2020	7 days 22:41:10	

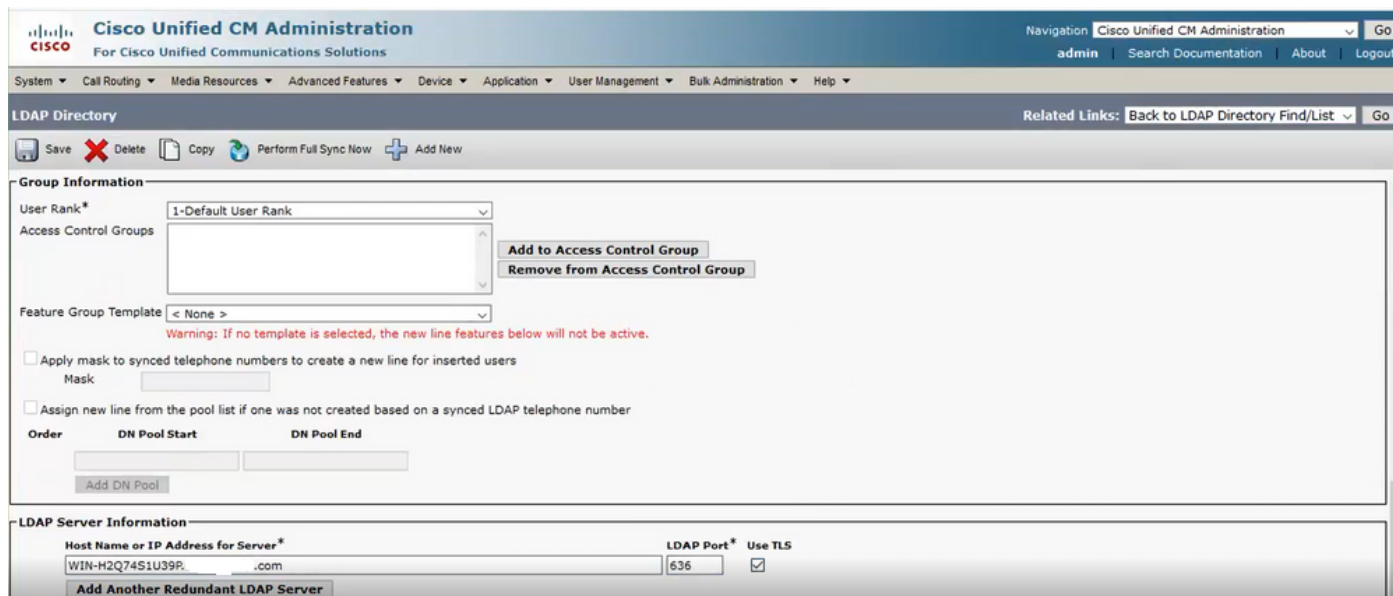
## Secure LDAP-map configureren

Stap 1. Configureer de CUCM LDAP Directory om de LDAPS TLS-verbinding met AD op poort



636 te gebruiken.

Ga naar CUCM Administration > System > LDAP Directory. Typ de FQDN of het IP-adres van de LDAPS-server voor LDAP Server-informatie. Specificeer de LDAPS-poort van 636 en controleer het vakje voor TLS gebruiken, zoals in de afbeelding:

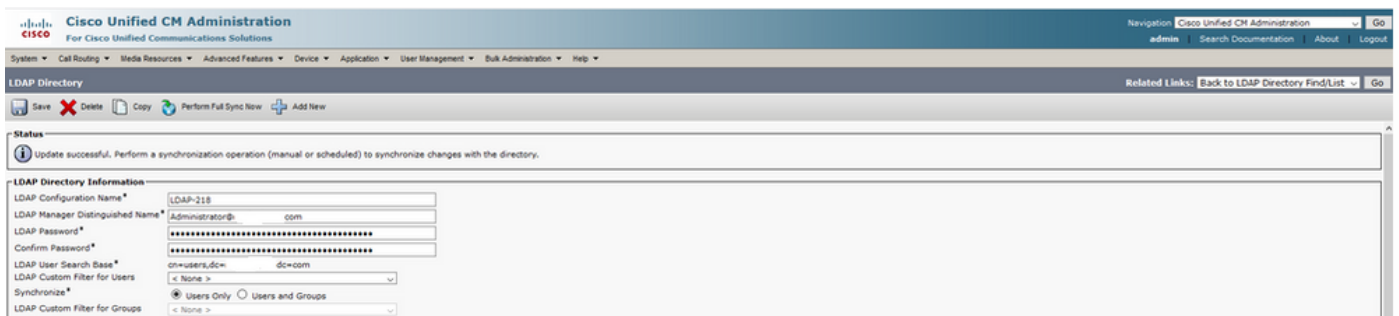


---

Opmerking: standaard worden de versies 10.5(2)SU2 en 9.1(2)SU3 FQDN geconfigureerd in LDAP Server Information gecontroleerd aan de algemene naam van het certificaat, als het IP-adres wordt gebruikt in plaats van de FQDN, de opdracht utils ldap config ipaddr wordt uitgegeven om de handhaving van FQDN naar CN verificatie te stoppen.

---

Stap 2. Klik op Full Sync Now uitvoeren om de configuratiewijziging in LDAPS te voltooien, zoals in het afbeelding wordt getoond:

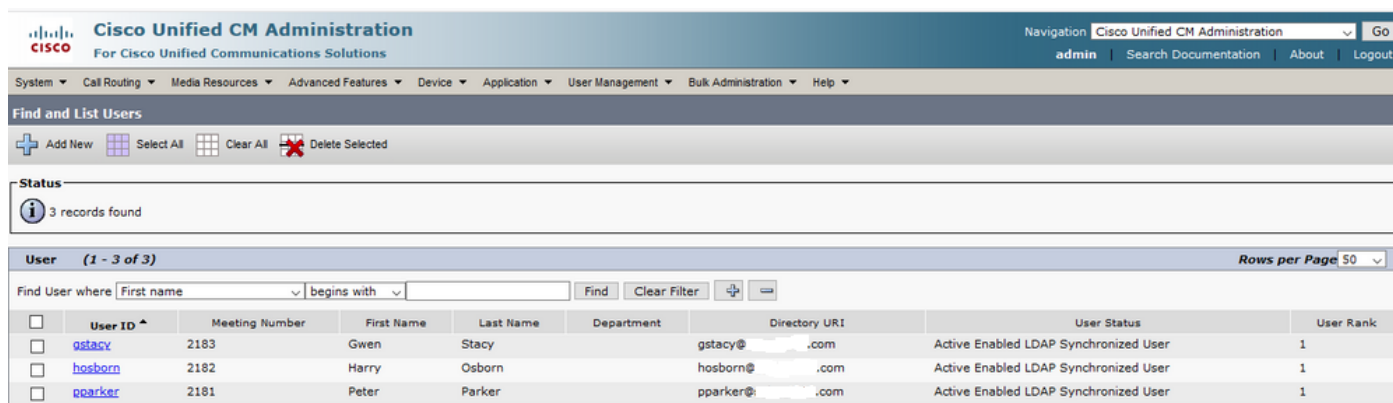


The screenshot shows the Cisco Unified CM Administration web interface. The page title is "LDAP Directory". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Bulk Administration. The main content area displays the "LDAP Directory Information" configuration form. The form fields are as follows:

Field	Value
LDAP Configuration Name*	LDAP-218
LDAP Manager Distinguished Name*	Administrator@com
LDAP Password*	*****
Confirm Password*	*****
LDAP User Search Base*	ou=users,dc=com
LDAP Custom Filter for Users	< None >
Synchronize*	<input checked="" type="radio"/> Users Only <input type="radio"/> Users and Groups
LDAP Custom Filter for Groups	< None >

At the top of the form, there is a status message: "Update successful. Perform a synchronization operation (manual or scheduled) to synchronize changes with the directory." Below the form, there are buttons for "Save", "Delete", "Copy", "Perform Full Sync Now", and "Add New".

Stap 3. Ga naar CUCM-beheer > Gebruikersbeheer > Eindgebruiker en controleer of de eindgebruikers aanwezig zijn, zoals in de afbeelding wordt getoond:

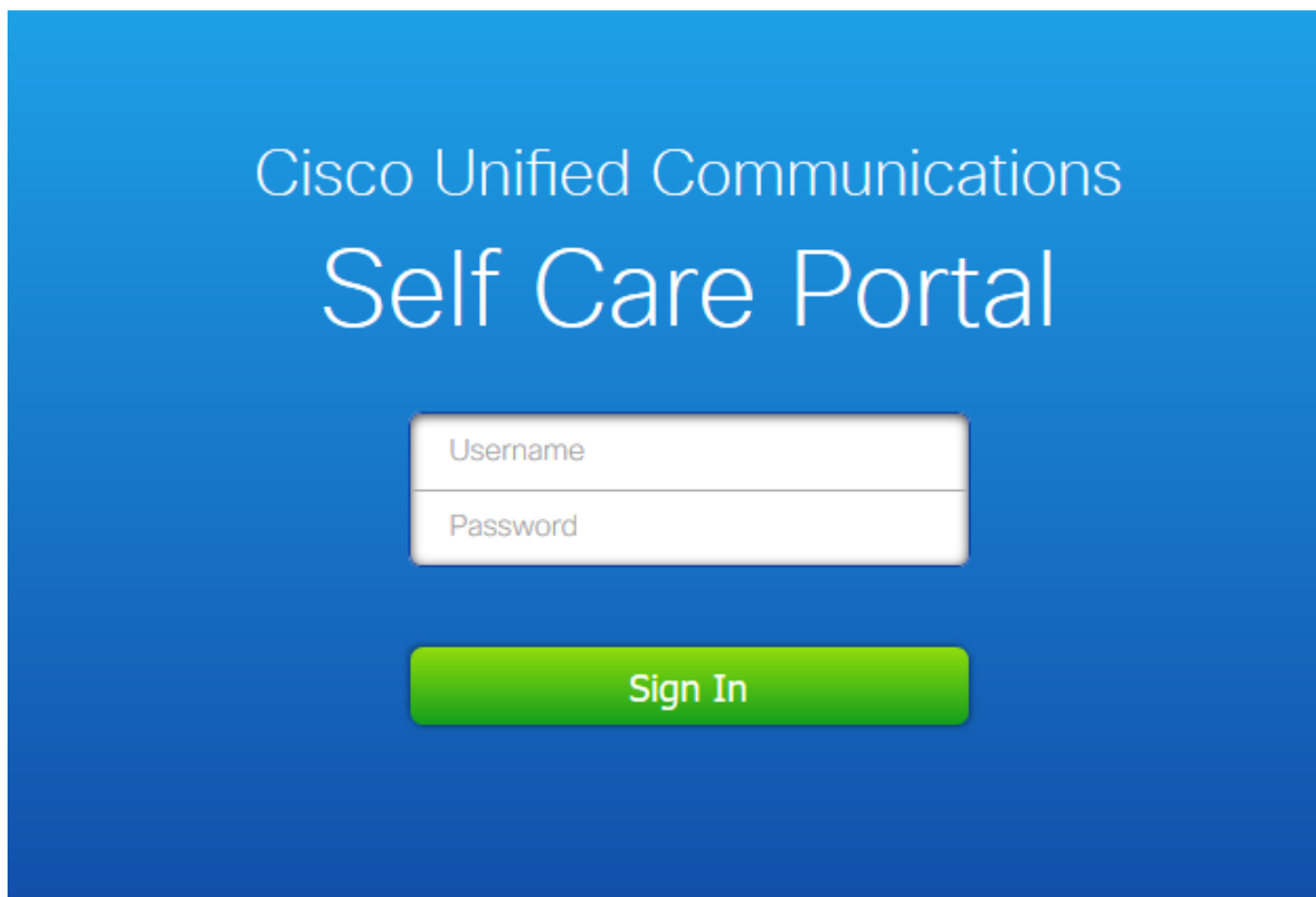


The screenshot shows the Cisco Unified CM Administration interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below this is a menu bar with options like System, Call Routing, Media Resources, etc. The main content area is titled "Find and List Users" and includes a status bar indicating "3 records found". Below the status bar is a table with columns for User ID, Meeting Number, First Name, Last Name, Department, Directory URI, User Status, and User Rank. The table contains three rows of user data.

<input type="checkbox"/>	User ID ^	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
<input type="checkbox"/>	<a href="#">gstacy</a>	2183	Gwen	Stacy		gstacy@...com	Active Enabled LDAP Synchronized User	1
<input type="checkbox"/>	<a href="#">hosborn</a>	2182	Harry	Osborn		hosborn@...com	Active Enabled LDAP Synchronized User	1
<input type="checkbox"/>	<a href="#">pparker</a>	2181	Peter	Parker		pparker@...com	Active Enabled LDAP Synchronized User	1

Stap 4. Navigeer naar de ccmuser pagina (<https://<ip adres of cucm pub>/ccmuser>) om te verifiëren dat de gebruiker inloggen succesvol is.

De commuser pagina voor CUCM versie 12.0.1 ziet er als volgt uit:



De gebruiker kan met succes inloggen nadat LDAP-referenties zijn ingevoerd, zoals in de afbeelding:

Unified Communications Self Care Portal

Gwen Stacy Skip to Content


Phones Voicemail IM & Availability General Settings Downloads About Help

My Phones

Phone Settings  
Call Forwarding

## My Phones

**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

## Secure LDAP-verificatie configureren

Configureer CUCM LDAP-verificatie om de LDAPS TLS-verbinding met AD op poort 3269 te gebruiken.

Ga naar CUCM Administration > System > LDAP-verificatie. Typ de FQDN van de LDAPS-server voor LDAP-serverinformatie. Specificeer de LDAPS-poort van 3269 en controleer het vakje voor TLS gebruiken, zoals in de afbeelding:

Cisco Unified CM Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

admin Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

### LDAP Authentication

Save

**Status**  
Update successful

**LDAP Authentication for End Users**

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name\* Administrator@ .com

LDAP Password\* .....

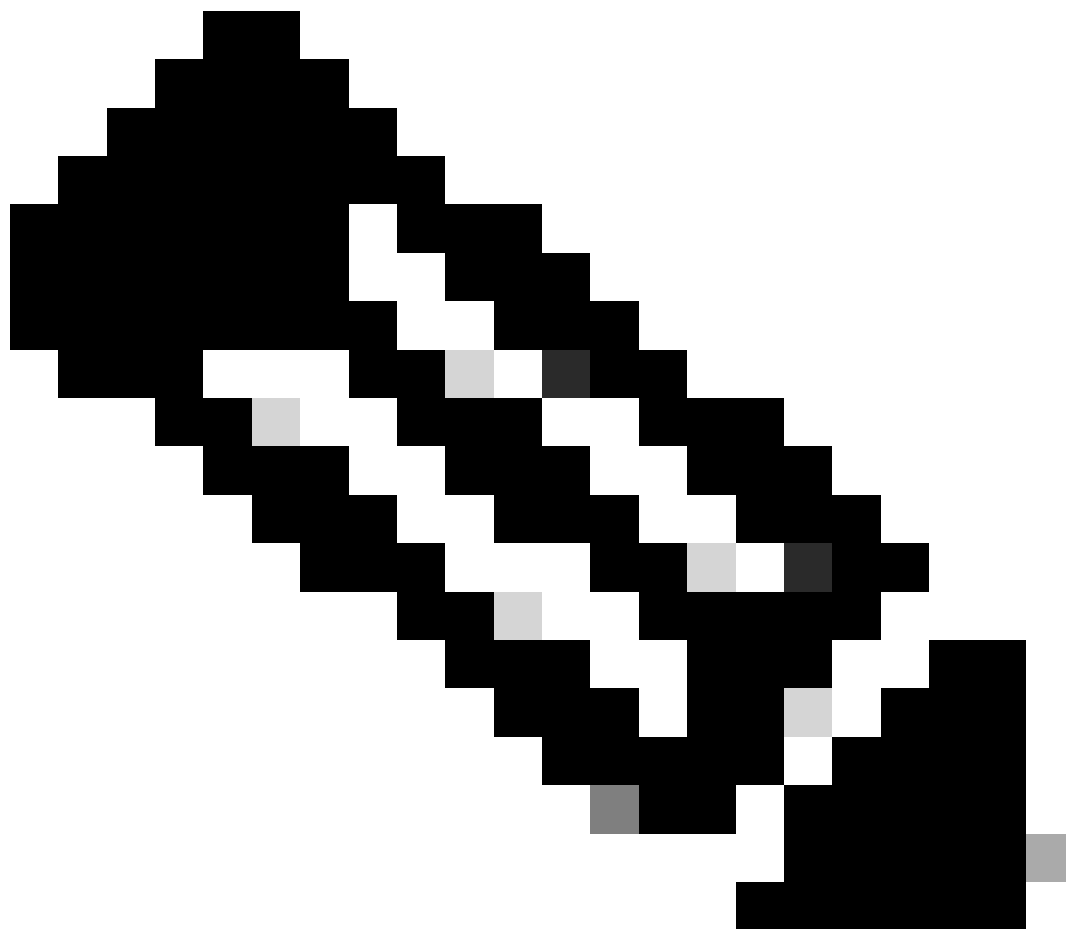
Confirm Password\* .....

LDAP User Search Base\* cn=users,dc= dc=com

**LDAP Server Information**

Host Name or IP Address for Server*	LDAP Port*	Use TLS
WIN-H2Q74S1U39F.com	3269	<input checked="" type="checkbox"/>

Add Another Redundant LDAP Server



Opmerking: Als u Jabber-clients hebt, wordt aanbevolen om poort 3269 te gebruiken voor LDAPS-verificatie, omdat Jabber-time-out voor inloggen kan optreden als er geen beveiligde verbinding met de wereldwijde catalogusserver is opgegeven.

---

## Beveiligde verbindingen met AD configureren voor UCS-services

Als u UC-services moet beveiligen die LDAP gebruiken, configureer dan deze UC-services om poort 636 of 3269 met TLS te gebruiken.

Ga naar CUCM-beheer > Gebruikersbeheer > Gebruikersinstellingen > UCS-service. Zoek Directory Service die verwijst naar AD. Typ de FQDN van de LDAPS-server als hostnaam/IP-adres. Specificeer de poort als 636 of 3269 en protocol TLS, zoals in de afbeelding:

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go  
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

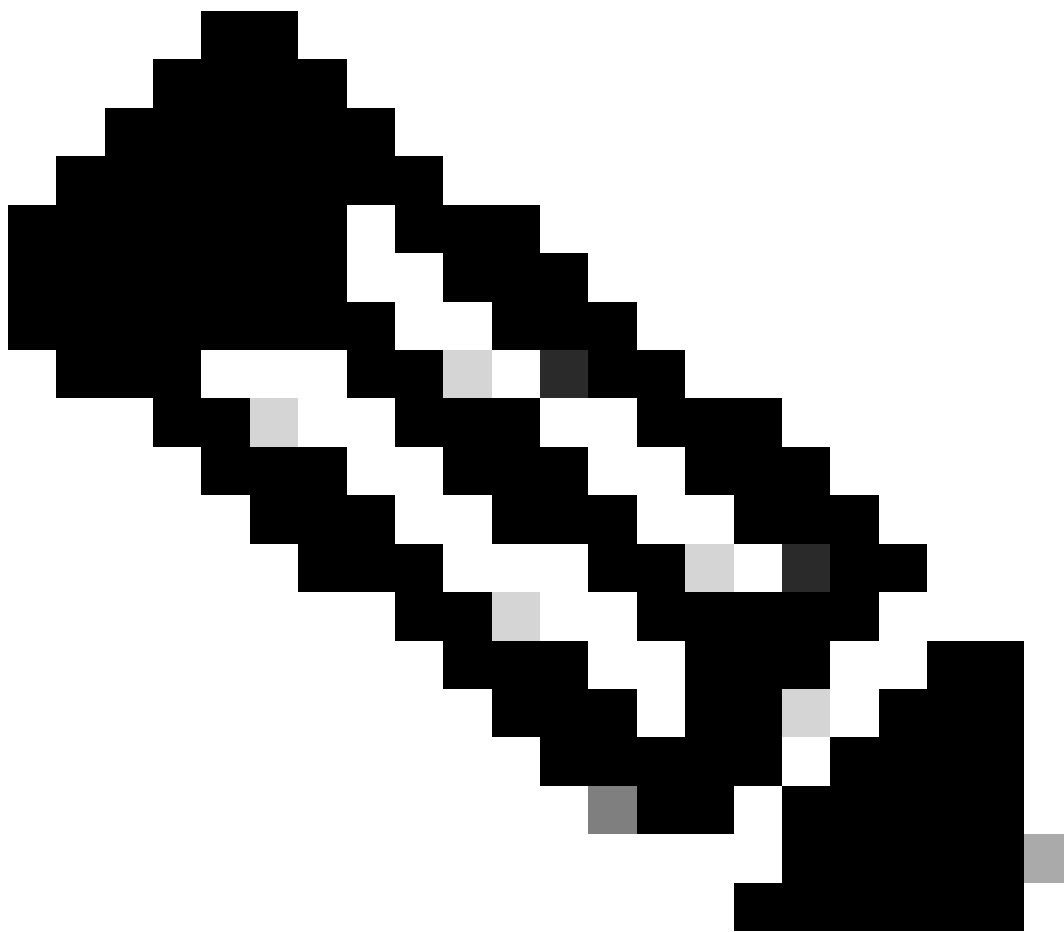
**Status**  
Update successful

**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

Save | Delete | Copy | Reset | Apply Config | Add New

\*. indicates required item.



Opmerking: de Jabber-clientmachines moeten ook de Tomcat-trust LDAPS-certificaten die op CUCM zijn geïnstalleerd, hebben geïnstalleerd in de certificaatbeheertrustwinkel van de Jabber-clientmachine om de Jabber-client in staat te stellen een LDAPS-verbinding met AD tot stand te brengen.

## Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Om de eigenlijke LDAPS-certificaatketen die van de LDAP-server naar CUCM is verzonden voor de TLS-verbinding te verifiëren, exporteert u het LDAPS TLS-certificaat vanuit een CUCM-pakketopname. Deze link geeft informatie over het exporteren van een TLS-certificaat vanuit een CUCM-pakketopname: [Hoe TLS-certificaat exporteren vanuit CUCM Packet Capture](#)

## Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

## Gerelateerde informatie

- Deze link geeft toegang tot een video die door de configuraties van LDAPS loopt: [Secure LDAP Directory en Authenticatie Walkthrough Video](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.