

Konfigurieren von CUCM für Secure LDAP (LDAPS)

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Überprüfen und Installieren von LDAPS-Zertifikaten](#)

[Sicheres LDAP-Verzeichnis konfigurieren](#)

[Konfigurieren der sicheren LDAP-Authentifizierung](#)

[Konfigurieren sicherer Verbindungen zu AD für UC-Dienste](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird das Verfahren zum Aktualisieren von CUCM-Verbindungen zu AD von einer nicht sicheren LDAP-Verbindung zu einer sicheren LDAPS-Verbindung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- AD LDAP-Server
- CUCM-LDAP-Konfiguration
- CUCM IM und Presence-Service (IM/P)

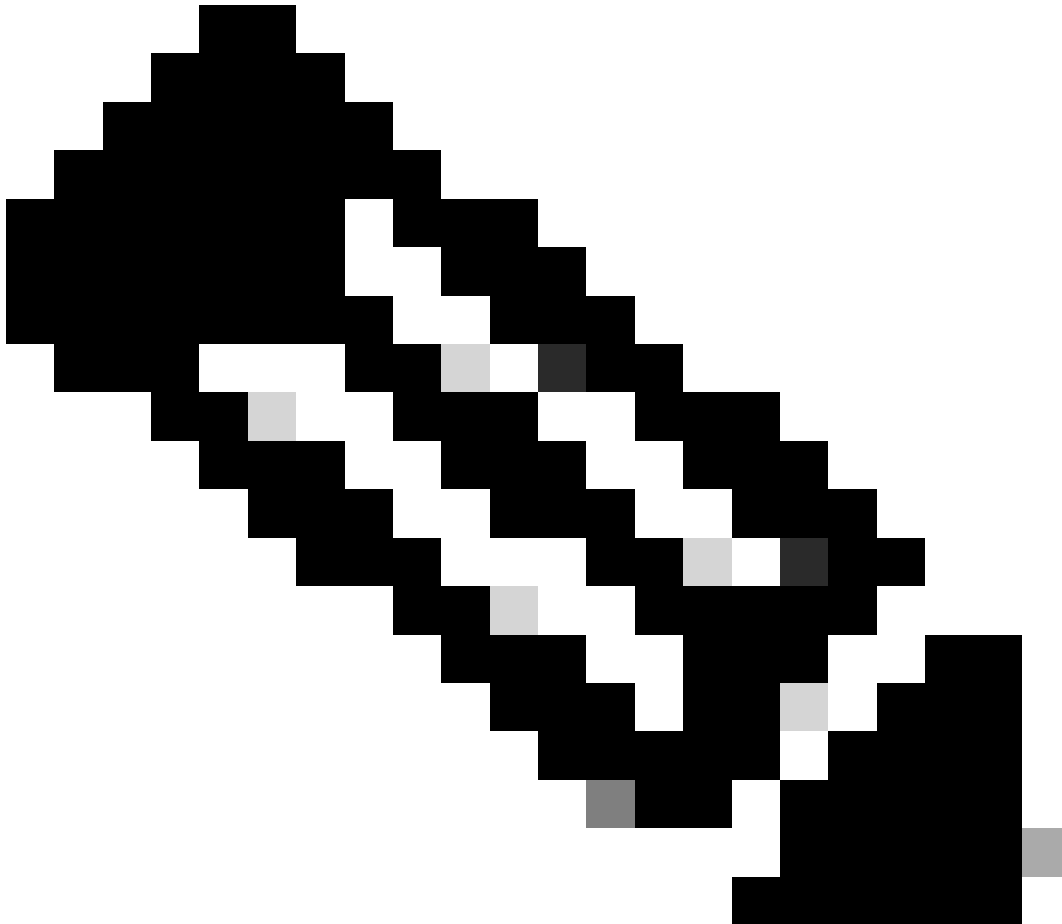
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CUCM Version 9.x und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Es obliegt dem Active Directory (AD)-Administrator, das AD Lightweight Directory Access Protocol (LDAP) für Lightweight Directory Access Protocol (LDAPS) zu konfigurieren. Dazu gehört die Installation von CA-signierten Zertifikaten, die die Anforderungen eines LDAPS-Zertifikats erfüllen.

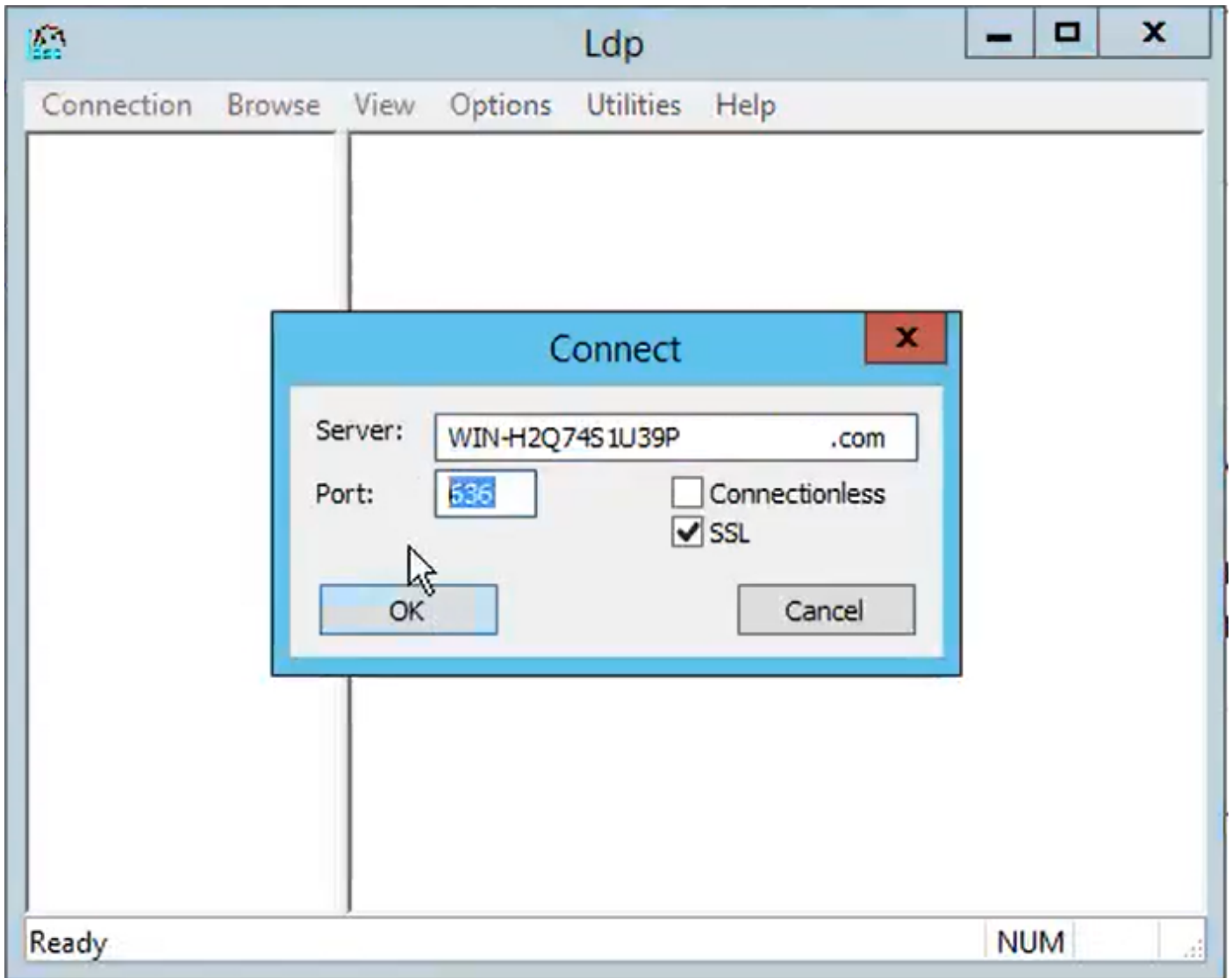


Hinweis: Unter diesem Link finden Sie Informationen zum Update von einem nicht sicheren LDAP auf eine sichere LDAPS-Verbindung mit AD für andere Cisco Collaboration-Anwendungen: [Softwareankündigung: Sicheres LDAP erforderlich für Active Directory-Verbindungen](#)

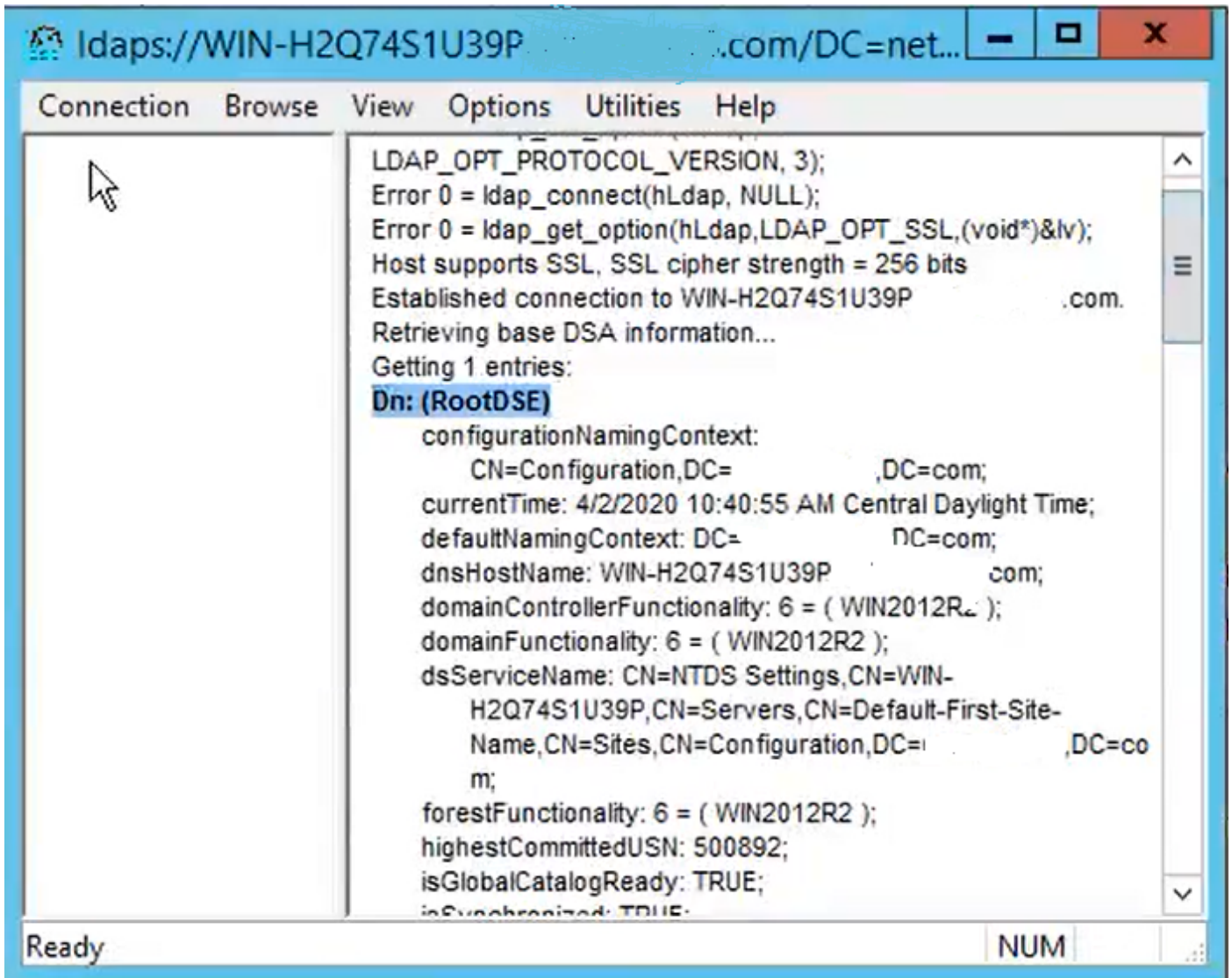
Überprüfen und Installieren von LDAPS-Zertifikaten

Schritt 1: Nachdem das LDAPS-Zertifikat auf den AD-Server hochgeladen wurde, überprüfen Sie, ob LDAPS auf dem AD-Server mit dem Tool ldp.exe aktiviert ist.

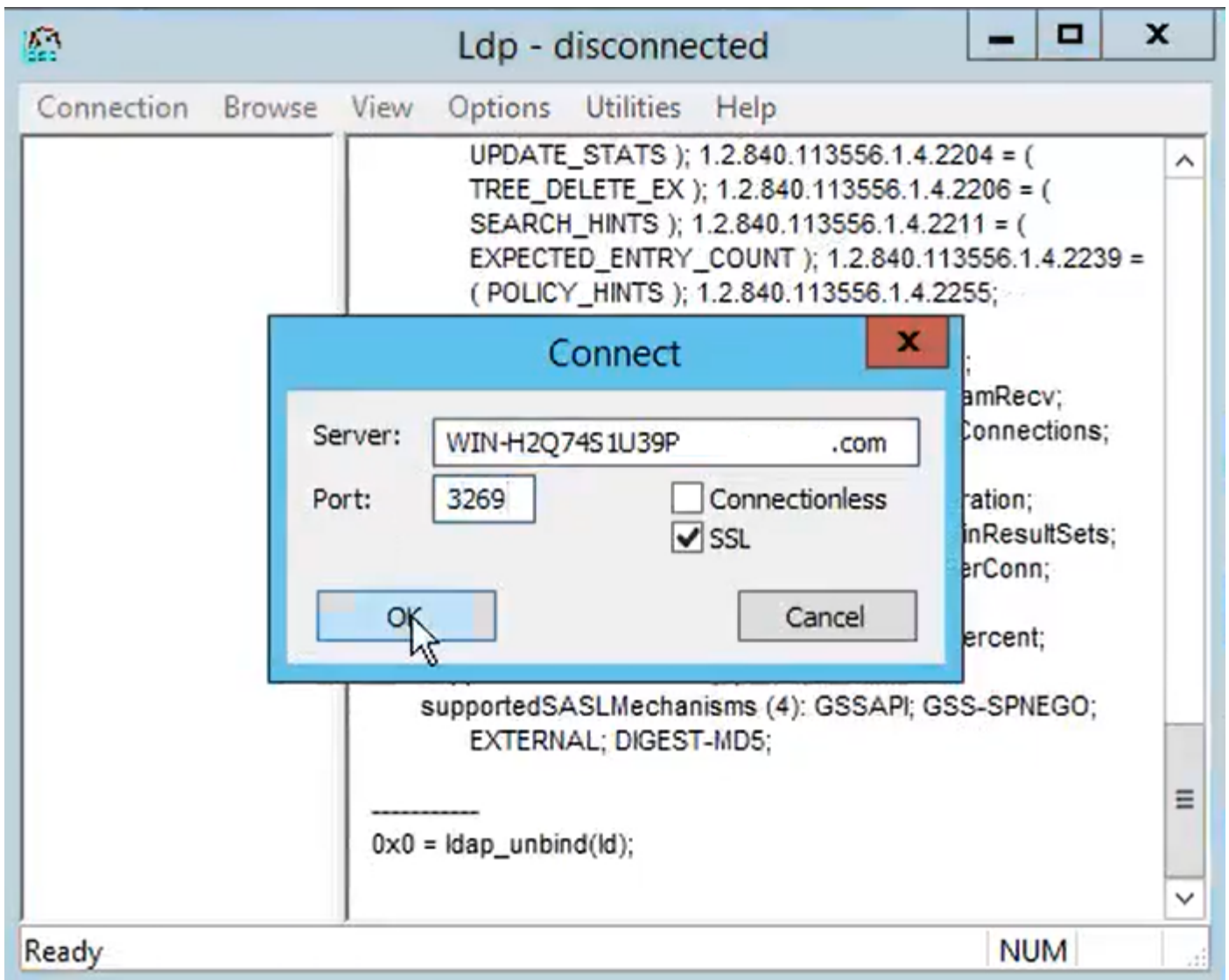
1. Starten Sie das AD-Verwaltungstool (Ldp.exe) auf dem AD-Server.
2. Wählen Sie im Menü Verbindung die Option Verbinden aus.
3. Geben Sie den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des LDAPS-Servers als Server ein.
4. Geben Sie 636 als Portnummer ein.
5. Klicken Sie auf OK, wie in der Abbildung dargestellt.



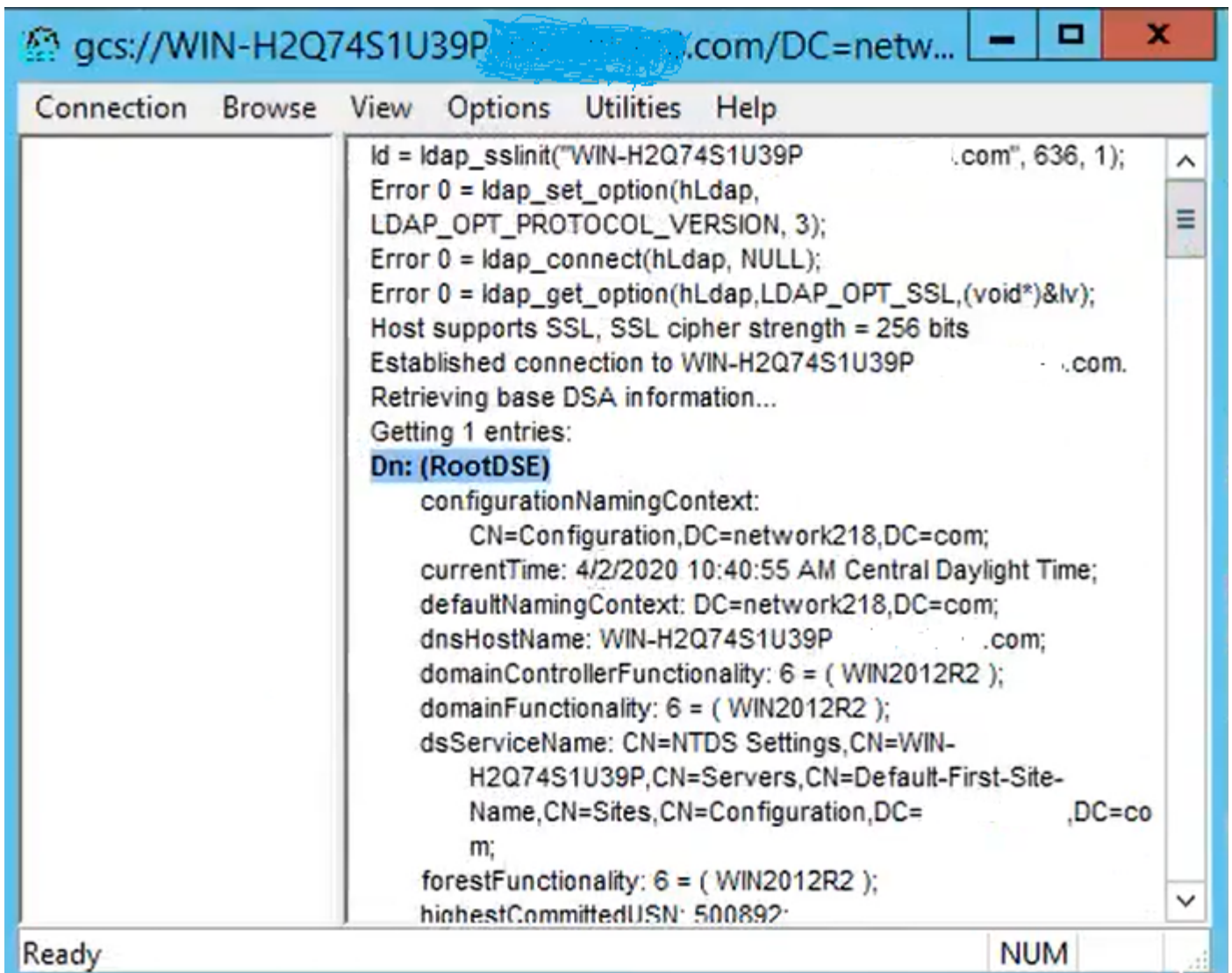
Für eine erfolgreiche Verbindung an Port 636 werden die RootDSE-Informationen im rechten Bereich ausgegeben, wie in der Abbildung dargestellt:



Wiederholen Sie den Vorgang für Port 3269, wie in der Abbildung dargestellt:

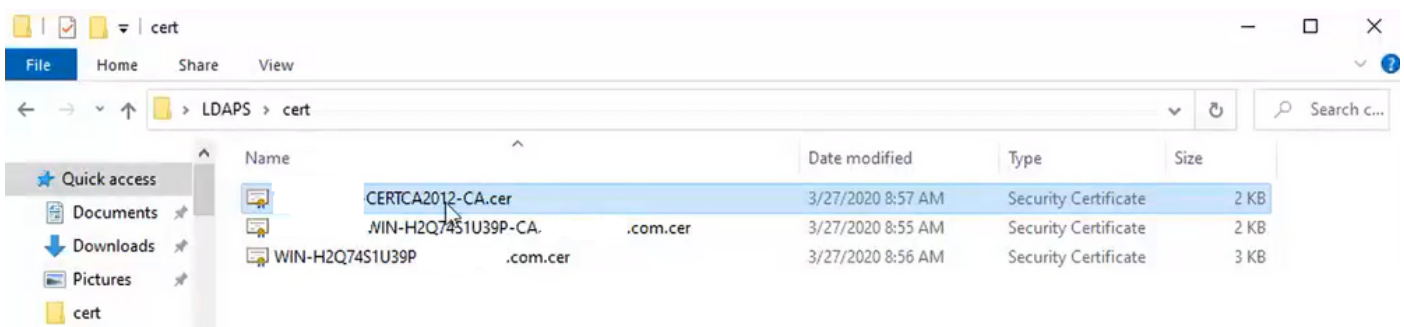


Für eine erfolgreiche Verbindung an Port 3269 werden die RootDSE-Informationen im rechten Bereich ausgegeben, wie in der Abbildung dargestellt:

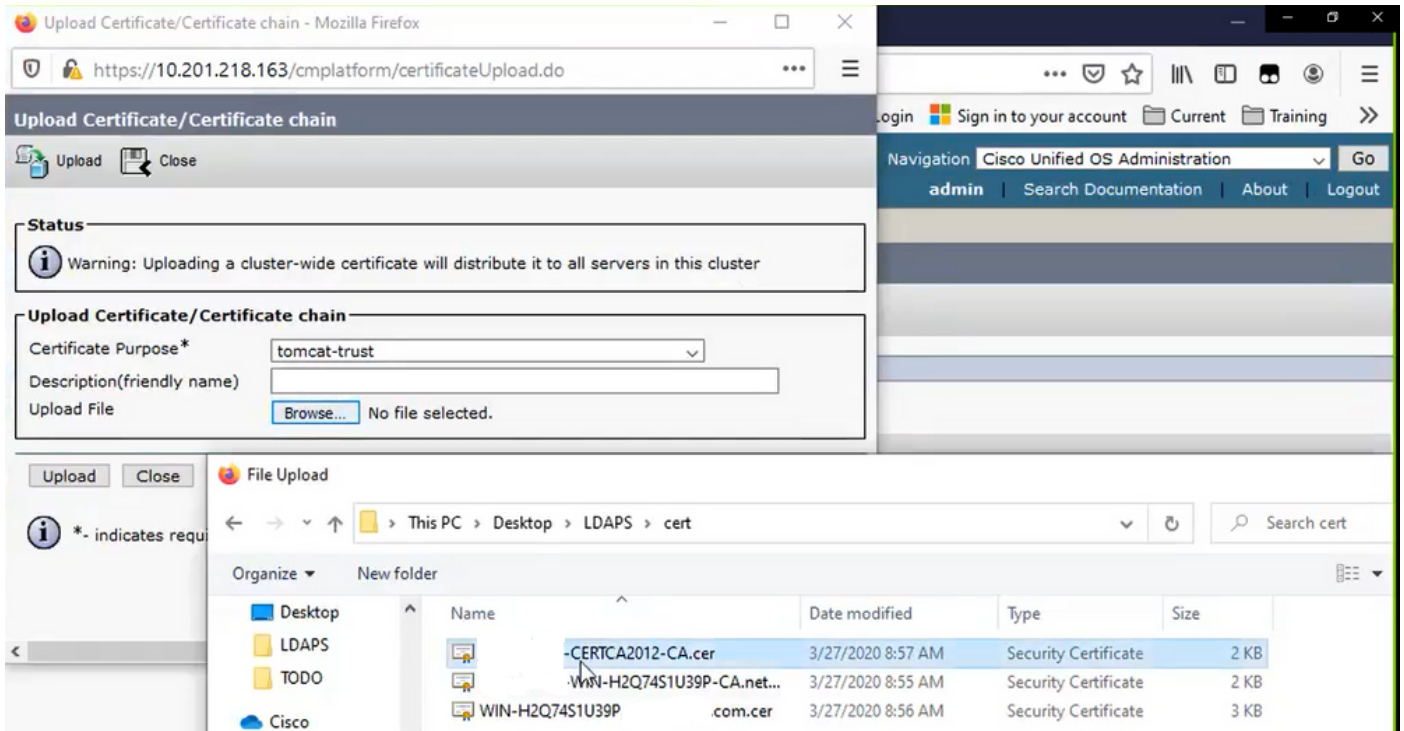


Schritt 2: Rufen Sie das Root- und alle Zwischenzertifikate ab, die Teil des LDAPS-Serverzertifikats sind, und installieren Sie diese als so genannte "tomcat-trust"-Zertifikate auf jedem CUCM- und IM/P-Publisher-Knoten sowie als "CallManager-trust" auf dem CUCM-Publisher.

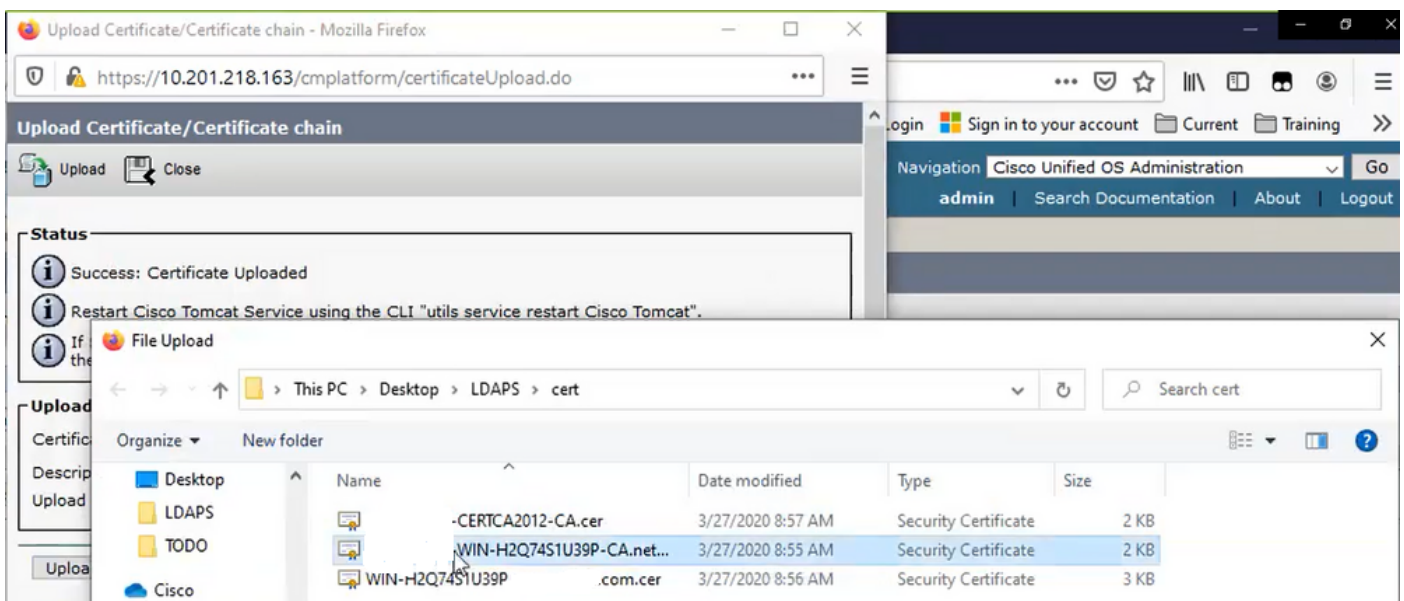
Die Stamm- und Zwischenzertifikate, die Teil eines LDAPS-Serverzertifikats sind, <hostname>.cer, werden im folgenden Bild angezeigt:




Navigieren Sie zu CUCM Publisher Cisco Unified OS Administration > Security > Certificate Management. Laden Sie den Stamm als tomcat-trust (wie im Bild gezeigt) und als CallManager-trust (nicht gezeigt) hoch:



Zwischenprodukt als tomcat-trust (wie im Bild gezeigt) und als CallManager-trust (nicht gezeigt) hochladen:

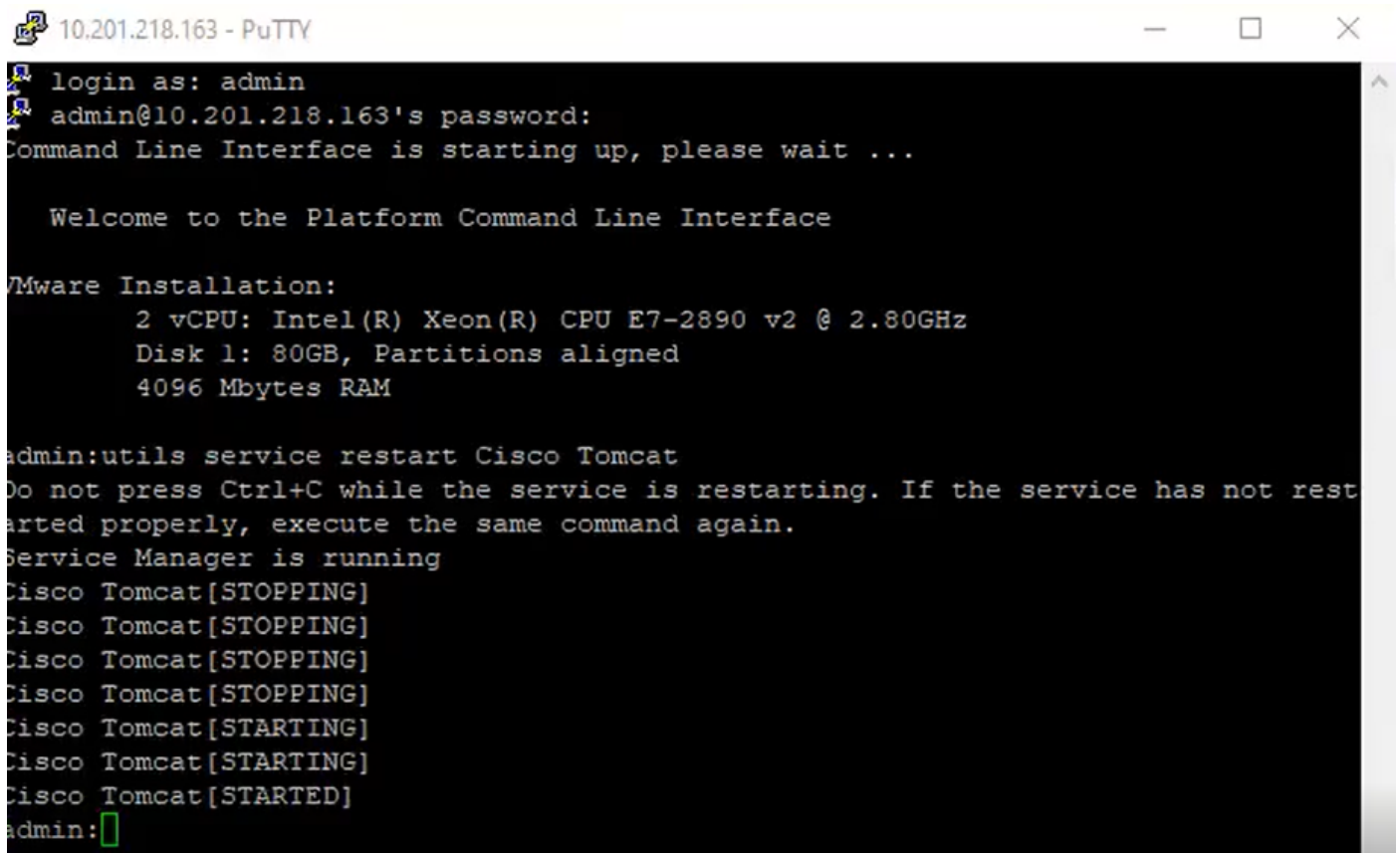


 Hinweis: Wenn IM/P-Server Teil des CUCM-Clusters sind, müssen Sie diese Zertifikate auch auf diese IM/P-Server hochladen.

 Hinweis: Alternativ können Sie das LDAPS-Serverzertifikat als tomcat-trust installieren.

Schritt 3: Starten Sie Cisco Tomcat über die CLI der einzelnen Knoten (CUCM und IM/P) in den Clustern neu. Überprüfen Sie außerdem für das CUCM-Cluster, ob der Cisco DirSync-Dienst auf dem Publisher-Knoten gestartet wurde.

Um den Tomcat-Dienst neu zu starten, müssen Sie eine CLI-Sitzung für jeden Knoten öffnen und den Befehl `utils service restart Cisco Tomcat` ausführen, wie im Bild gezeigt:



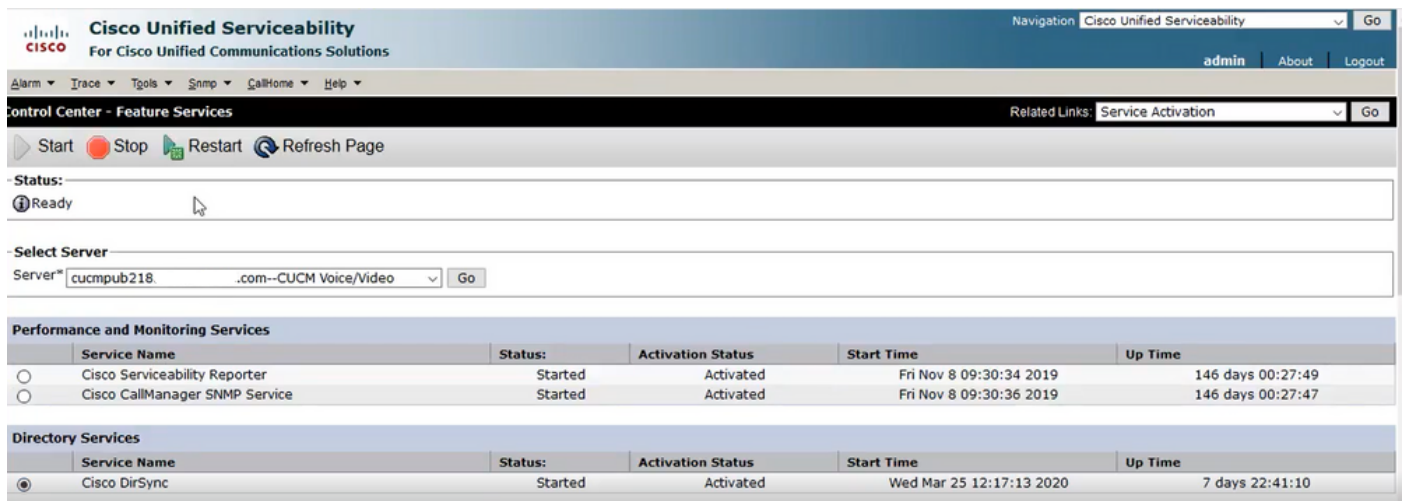
```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

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:
```

Schritt 4: Navigieren Sie zum CUCM-Publisher Cisco Unified Serviceability > Tools > Control Center - Feature Services, überprüfen Sie, ob der Cisco DirSync-Service aktiviert und gestartet wurde (wie im Bild gezeigt), und starten Sie den Cisco CTIManager-Service auf jedem Knoten neu, falls dieser verwendet wird (nicht dargestellt):



Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Navigation: Cisco Unified Serviceability Go

admin About Logout

Alarm Trace Tools Snmp CallHome Help

Control Center - Feature Services Related Links: Service Activation Go

Start Stop Restart Refresh Page

Status: Ready

Select Server
Server: cucmpub218 .com--CUCM Voice/Video Go

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

Sicheres LDAP-Verzeichnis konfigurieren

Schritt 1: Konfigurieren Sie das CUCM-LDAP-Verzeichnis, um die LDAPS-TLS-Verbindung mit AD auf Port 636 zu verwenden.

Navigieren Sie zu CUCM Administration > System > LDAP Directory. Geben Sie den FQDN oder die IP-Adresse des LDAP-Servers für LDAP-Serverinformationen ein. Geben Sie den LDAPS-Port 636 an, und aktivieren Sie das Kontrollkästchen TLS verwenden, wie im Bild gezeigt:

The screenshot shows the Cisco Unified CM Administration interface for the LDAP Directory configuration. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration For Cisco Unified Communications Solutions", and navigation links for "admin", "Search Documentation", "About", and "Logout". Below the navigation bar, there are tabs for "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is titled "LDAP Directory" and includes a "Related Links" section with a "Back to LDAP Directory Find/List" link and a "Go" button. The configuration is organized into two sections:

- Group Information:** This section contains several fields and options:
 - User Rank*:** A dropdown menu set to "1-Default User Rank".
 - Access Control Groups:** An empty list with "Add to Access Control Group" and "Remove from Access Control Group" buttons.
 - Feature Group Template:** A dropdown menu set to "< None >". A warning message below it states: "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:** This option includes a "Mask" input field.
 - Assign new line from the pool list if one was not created based on a synced LDAP telephone number.**
 - Order:** A table with columns "DN Pool Start" and "DN Pool End", each with an empty input field and an "Add DN Pool" button below.
- LDAP Server Information:** This section contains:
 - Host Name or IP Address for Server*:** An input field containing "WIN-H2Q74S1U39P...com".
 - LDAP Port*:** An input field containing "636".
 - Use TLS**
 - Add Another Redundant LDAP Server** button.



Hinweis: Wenn die in den LDAP-Serverinformationen konfigurierten FQDN-Versionen 10.5(2)SU2 und 9.1(2)SU3 mit dem allgemeinen Namen des Zertifikats abgeglichen wurden, wird standardmäßig der Befehl `utils ldap config ipaddr` ausgegeben, um die Durchsetzung von FQDN zur CN-Überprüfung zu beenden, wenn die IP-Adresse anstelle des FQDN verwendet wird.

Schritt 2: Um die Konfigurationsänderung in LDAPS abzuschließen, klicken Sie auf **Perform Full Sync Now** (Vollständige Synchronisierung jetzt durchführen), wie im Bild gezeigt:

The screenshot shows the Cisco Unified CM Administration interface for LDAP Directory configuration. The page title is "LDAP Directory". At the top, there is a navigation bar with "Cisco Unified CM Administration" and "admin". Below the navigation bar, there is a breadcrumb trail: "System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help".

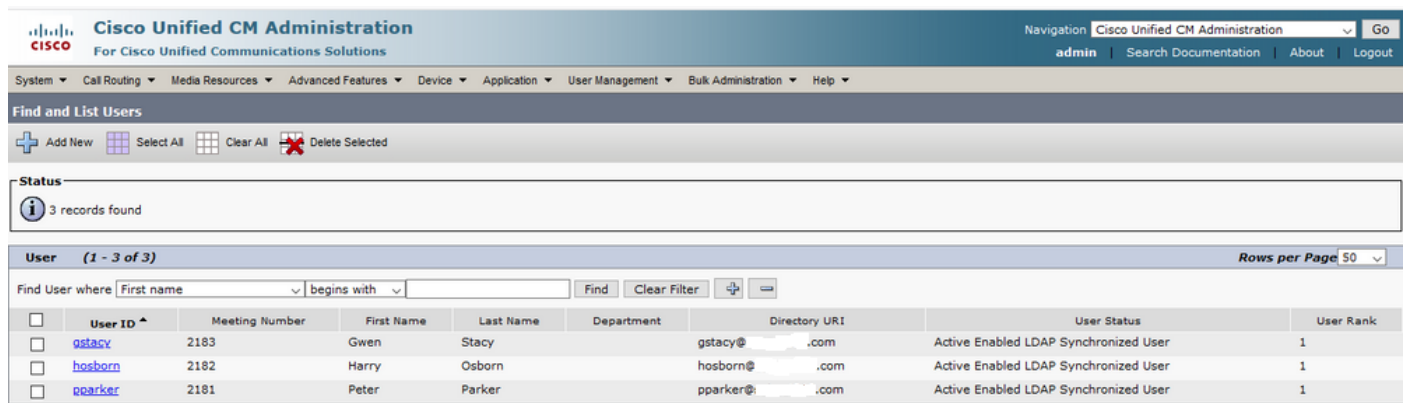
The main content area is titled "LDAP Directory" and includes a "Related Links" section with "Back to LDAP Directory Find/List". Below this, there is a "Status" section with a message: "Update successful. Perform a synchronization operation (manual or scheduled) to synchronize changes with the directory.".

The "LDAP Directory Information" section contains the following fields:

- LDAP Configuration Name*: LDAP-218
- LDAP Manager Distinguished Name*: Administrator@.com
- LDAP Password*: [Redacted]
- Confirm Password*: [Redacted]
- LDAP User Search Base*: cn=users,dc=,dc=com
- LDAP Custom Filter for Users: < None >
- Synchronize*: Users Only Users and Groups
- LDAP Custom Filter for Groups: < None >

At the bottom of the form, there is a "Perform Full Sync Now" button, which is highlighted in the image.

Schritt 3: Navigieren Sie zu CUCM Administration > User Management > End User, und überprüfen Sie, ob Endbenutzer vorhanden sind, wie in der Abbildung dargestellt:

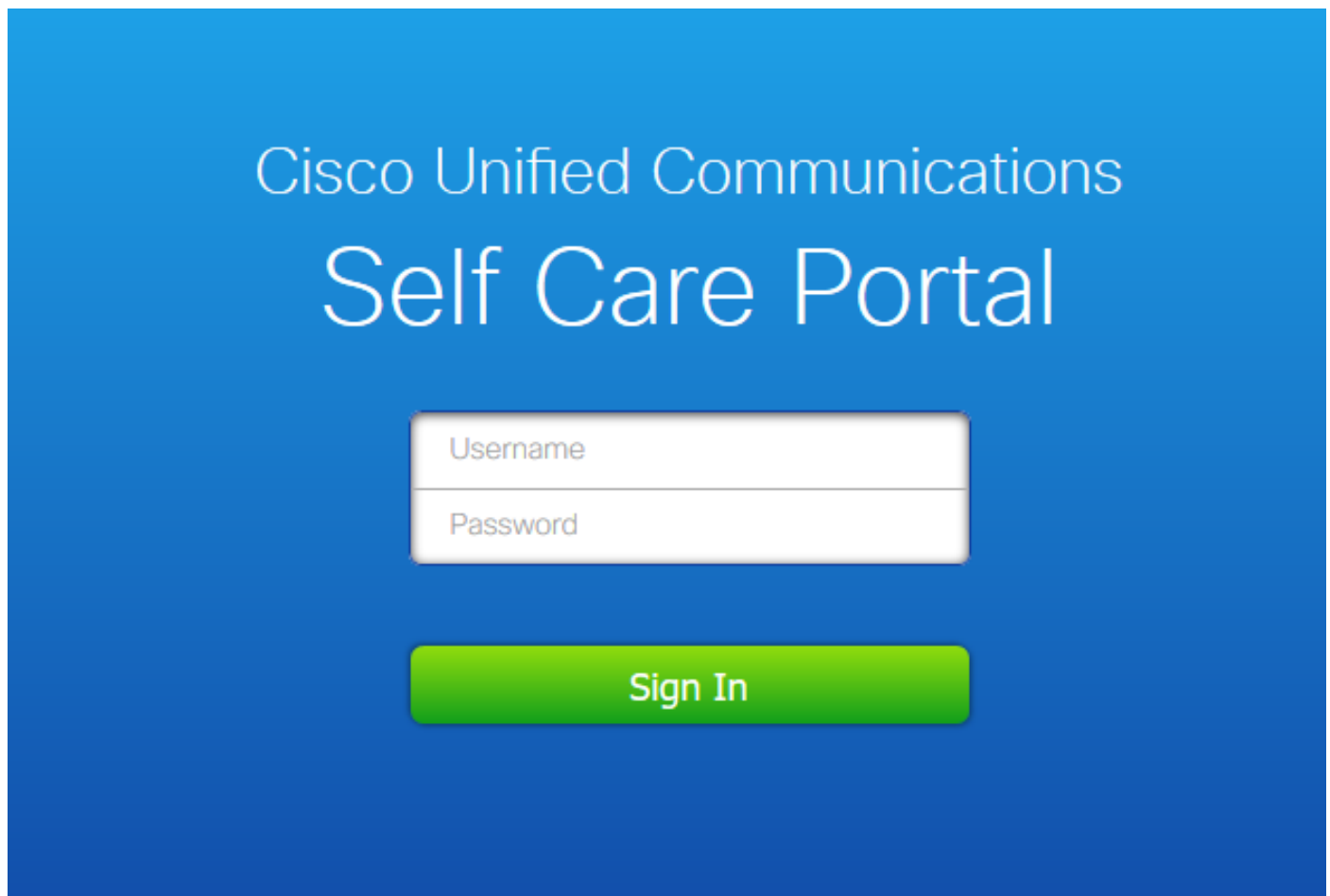


The screenshot shows the Cisco Unified CM Administration interface. The main content area is titled 'Find and List Users'. Below this title, there are buttons for 'Add New', 'Select All', 'Clear All', and 'Delete Selected'. A status bar indicates '3 records found'. Below the status bar, there is a search filter section with a dropdown for 'Find User where' and a 'Find' button. The main table displays the following data:

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

Schritt 4: Navigieren Sie zur Seite ccmuser (<https://<ip address of cucm pub>/ccmuser>), um sicherzustellen, dass sich der Benutzer erfolgreich angemeldet hat.

Die Seite "ccmuser" für CUCM-Version 12.0.1 sieht wie folgt aus:



Der Benutzer kann sich erfolgreich anmelden, nachdem die LDAP-Anmeldeinformationen eingegeben wurden, wie im folgenden Bild gezeigt:

The screenshot shows the 'My Phones' section of the Cisco Unified Communications Self Care Portal. The page title is 'My Phones' and it is under the 'Company Phones' section. Below the title, there is a description: 'These are the phones provided to you by your company. You may set personal preferences for these in [Phone Settings](#)'. A single phone is listed in a card format: 'Cisco 8865' and '2183'. The card includes an image of the phone and a settings gear icon.

Konfigurieren der sicheren LDAP-Authentifizierung

Konfigurieren Sie die CUCM-LDAP-Authentifizierung, um die LDAPS-TLS-Verbindung mit AD auf Port 3269 zu verwenden.

Navigieren Sie zu CUCM Administration > System > LDAP Authentication. Geben Sie den FQDN des LDAP-Servers für LDAP-Serverinformationen ein. Geben Sie den LDAPS-Port 3269 an, und aktivieren Sie das Kontrollkästchen TLS verwenden, wie im Bild gezeigt:

The screenshot shows the 'LDAP Authentication' configuration page in Cisco Unified CM Administration. The page has a navigation bar at the top with 'Cisco Unified CM Administration' and 'For Cisco Unified Communications Solutions'. Below the navigation bar, there is a 'Save' button and a 'Status' section indicating 'Update successful'. The main configuration area is divided into two sections: 'LDAP Authentication for End Users' and 'LDAP Server Information'. In the 'LDAP Authentication for End Users' section, the 'Use LDAP Authentication for End Users' checkbox is checked. The 'LDAP Manager Distinguished Name' field contains 'Administrator@.com'. The 'LDAP Password' and 'Confirm Password' fields are masked with dots. The 'LDAP User Search Base' field contains 'cn=users,dc=.dc=com'. In the 'LDAP Server Information' section, the 'Host Name or IP Address for Server' field contains 'WIN-H2Q74S1U39F.com'. The 'LDAP Port' field contains '3269'. The 'Use TLS' checkbox is checked. There is an 'Add Another Redundant LDAP Server' button at the bottom of the section.



Hinweis: Wenn Sie Jabber-Clients haben, wird empfohlen, Port 3269 für die LDAPS-Authentifizierung zu verwenden, da ein Jabber-Timeout für die Anmeldung auftreten kann, wenn keine sichere Verbindung zum globalen Katalogserver angegeben ist.

Konfigurieren sicherer Verbindungen zu AD für UC-Dienste

Wenn Sie UC-Dienste sichern müssen, die LDAP verwenden, konfigurieren Sie diese UC-Dienste so, dass sie Port 636 oder 3269 mit TLS verwenden.

Navigieren Sie zu CUCM Administration > User Management > User Settings > UC Service. Suchen nach Verzeichnisdienst, der auf AD verweist. Geben Sie den FQDN des LDAPS-Servers als Hostnamen/IP-Adresse ein. Geben Sie den Port als 636 oder 3269 und das Protokoll TLS an, wie im Bild gezeigt:

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

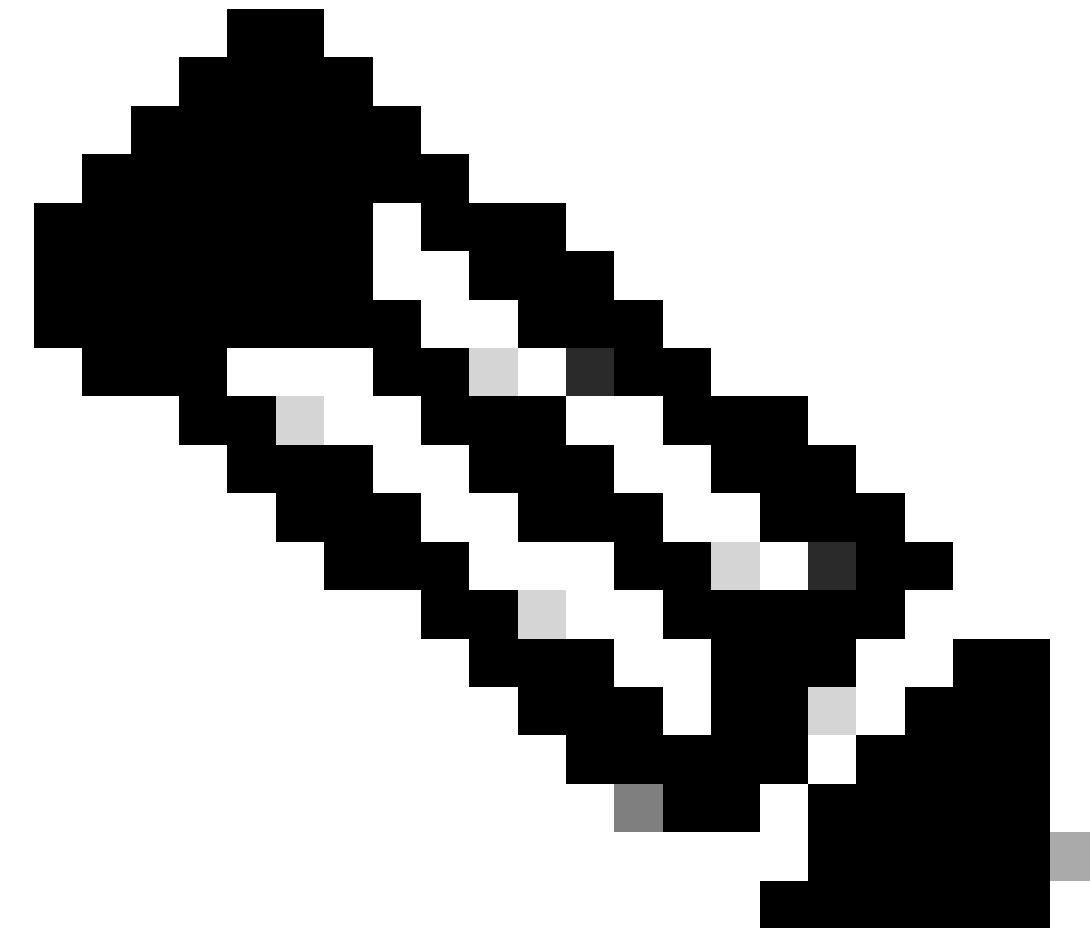
Status
Update successful

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.



Hinweis: Auf den Jabber-Client-Computern müssen auch die auf dem CUCM installierten Tomcat-Trust-LDAPS-Zertifikate im Zertifikatmanagement-Trust-Speicher des Jabber-Client-Computers installiert sein, damit der Jabber-Client eine LDAPS-Verbindung mit AD herstellen kann.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Exportieren Sie das LDAPS TLS-Zertifikat aus einer CUCM-Paketerfassung, um die tatsächliche LDAPS-Zertifikat-/Zertifikatskette zu überprüfen, die vom LDAP-Server an den CUCM für die TLS-Verbindung gesendet wurde. Dieser Link enthält Informationen zum Exportieren eines TLS-Zertifikats aus einer CUCM-Paketerfassung: [So exportieren Sie ein TLS-Zertifikat aus der CUCM-Paketerfassung](#)

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

- Dieser Link bietet Zugriff auf ein Video, das die LDAP-Konfigurationen durchgeht: [Secure LDAP Directory und Authentication Walkthrough Video](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.