

# 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.



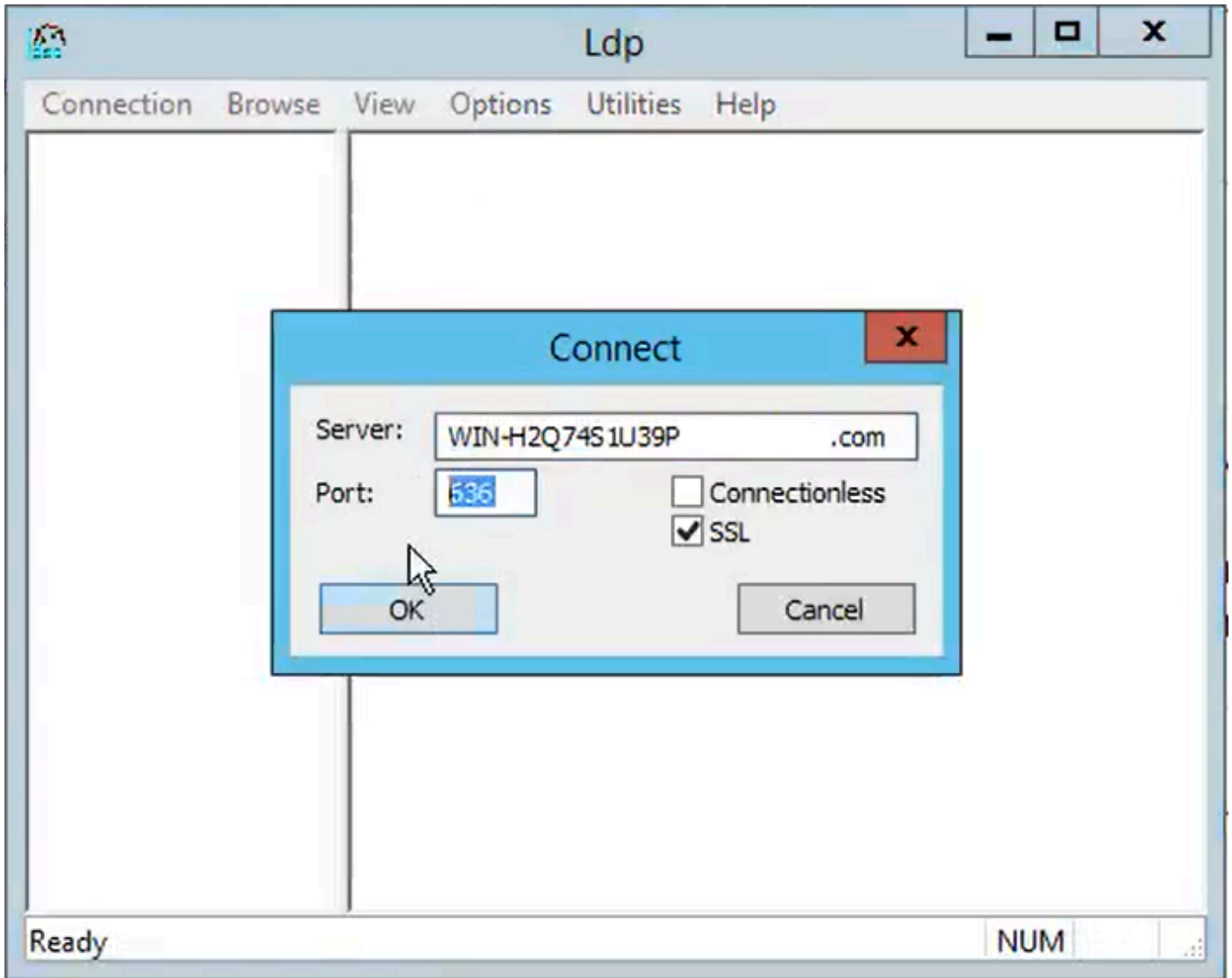
**Note:** See this link for information in order to update from non-secure LDAP to secure LDAPS connections to AD for other Cisco Collaboration Applications: [Software Advisory: Secure LDAP Mandatory for Active Directory Connections](#)

---

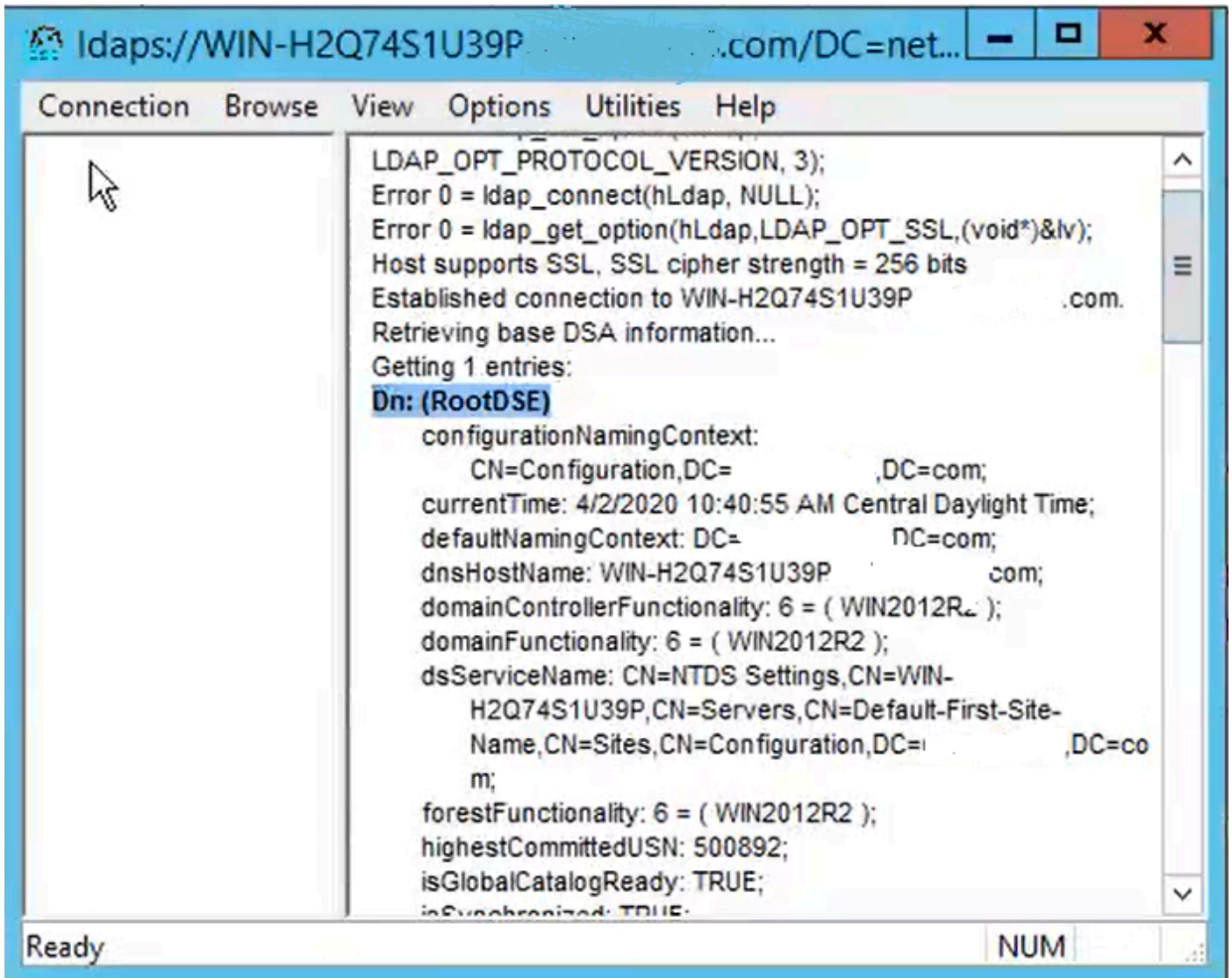
## Verify and Install LDAPS Certificates

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.

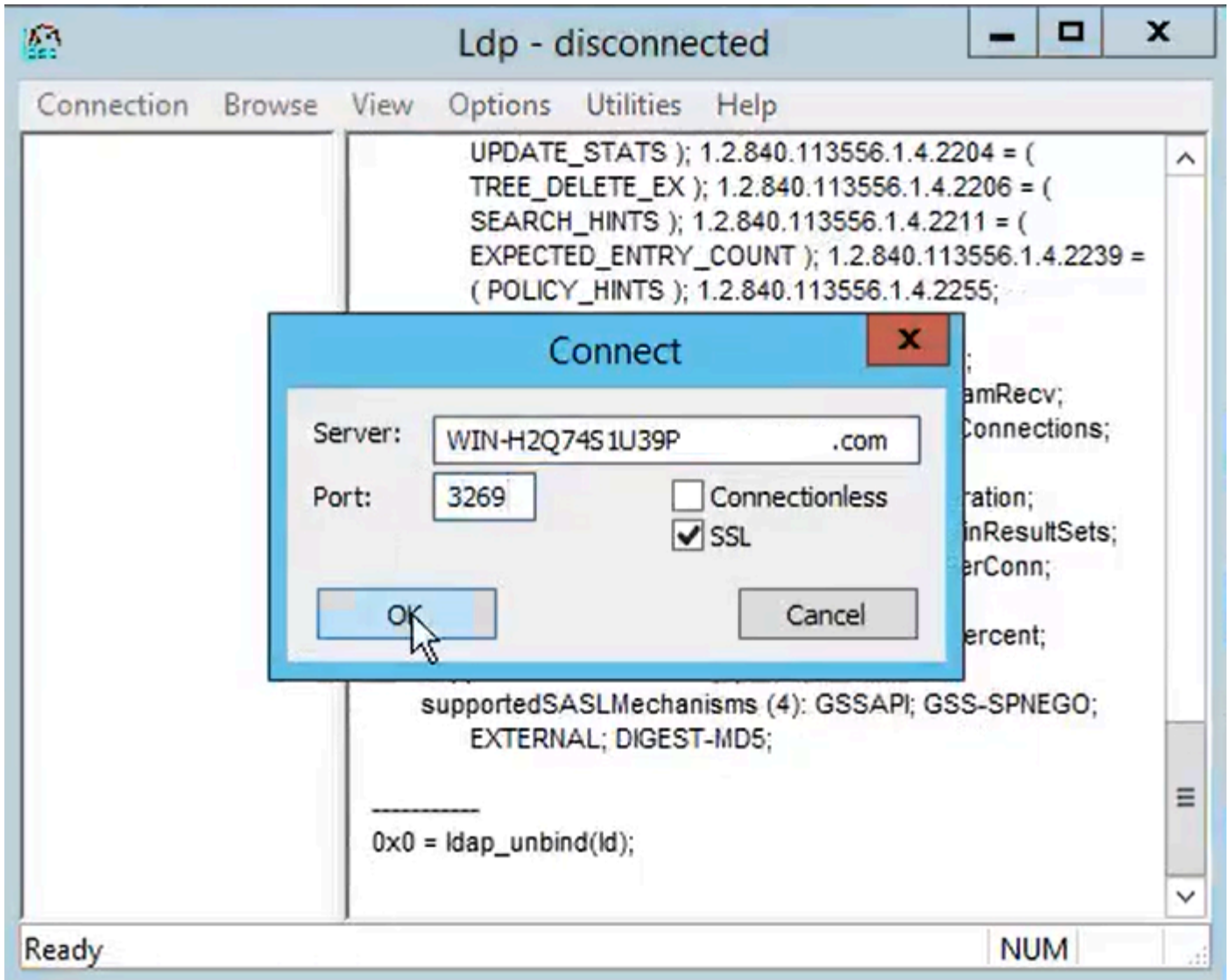
1. Start the **AD Administration Tool (Ldp.exe)** on the AD server.
2. On the **Connection** menu, select **Connect**.
3. Enter the **Fully Qualified Domain Name (FQDN)** of the LDAPS server as the server.
4. Enter **636** as the port number.
5. Click **OK**, as shown in the image



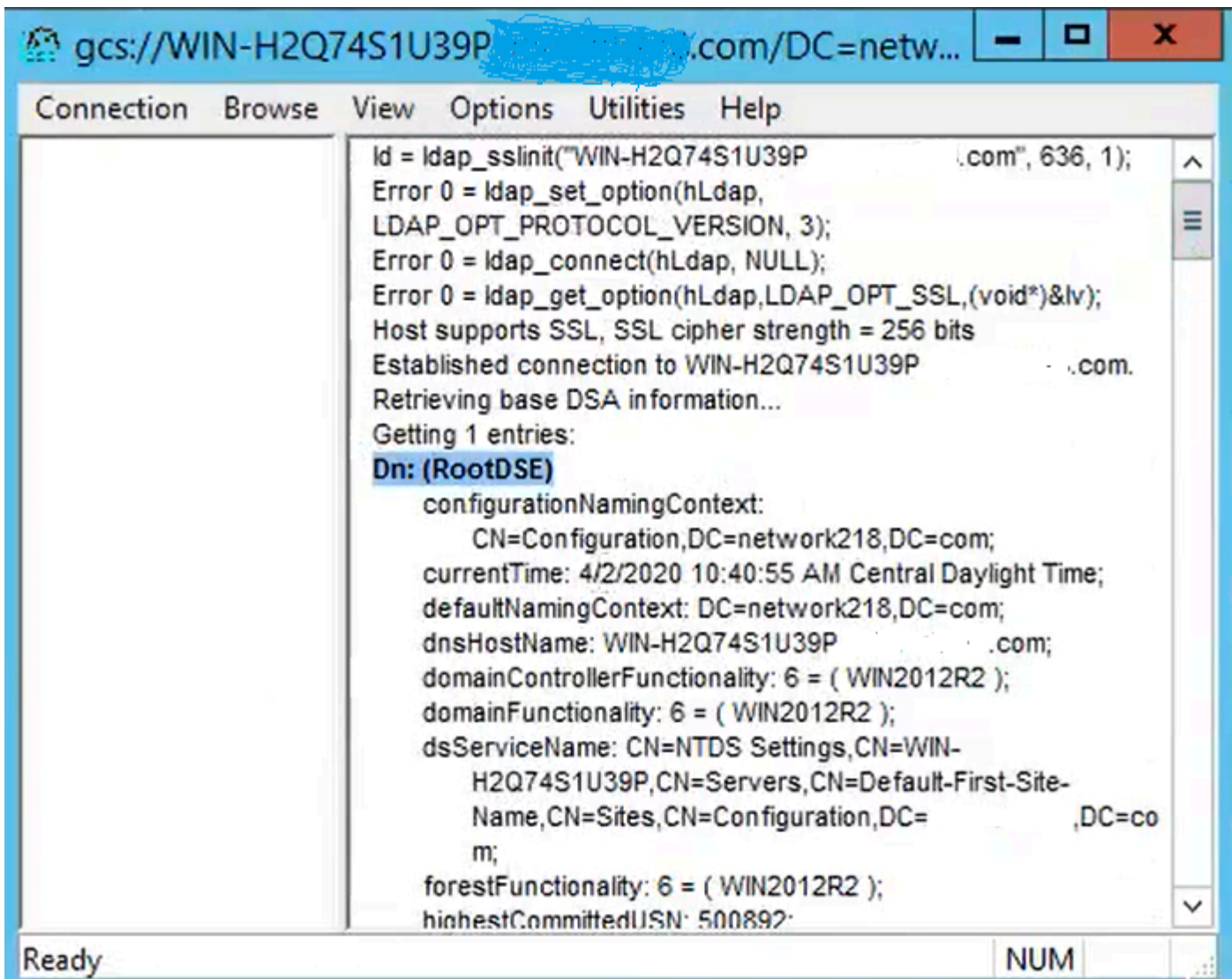
For a successful connection on port 636, RootDSE information prints out in the right pane, as shown in the image:



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

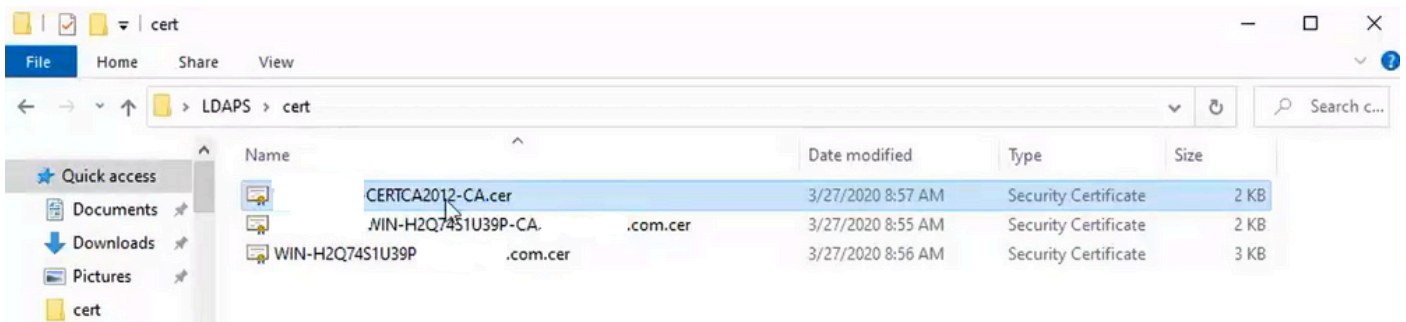


For a successful connection on port 3269, RootDSE information prints out in the right pane, as shown in the image:

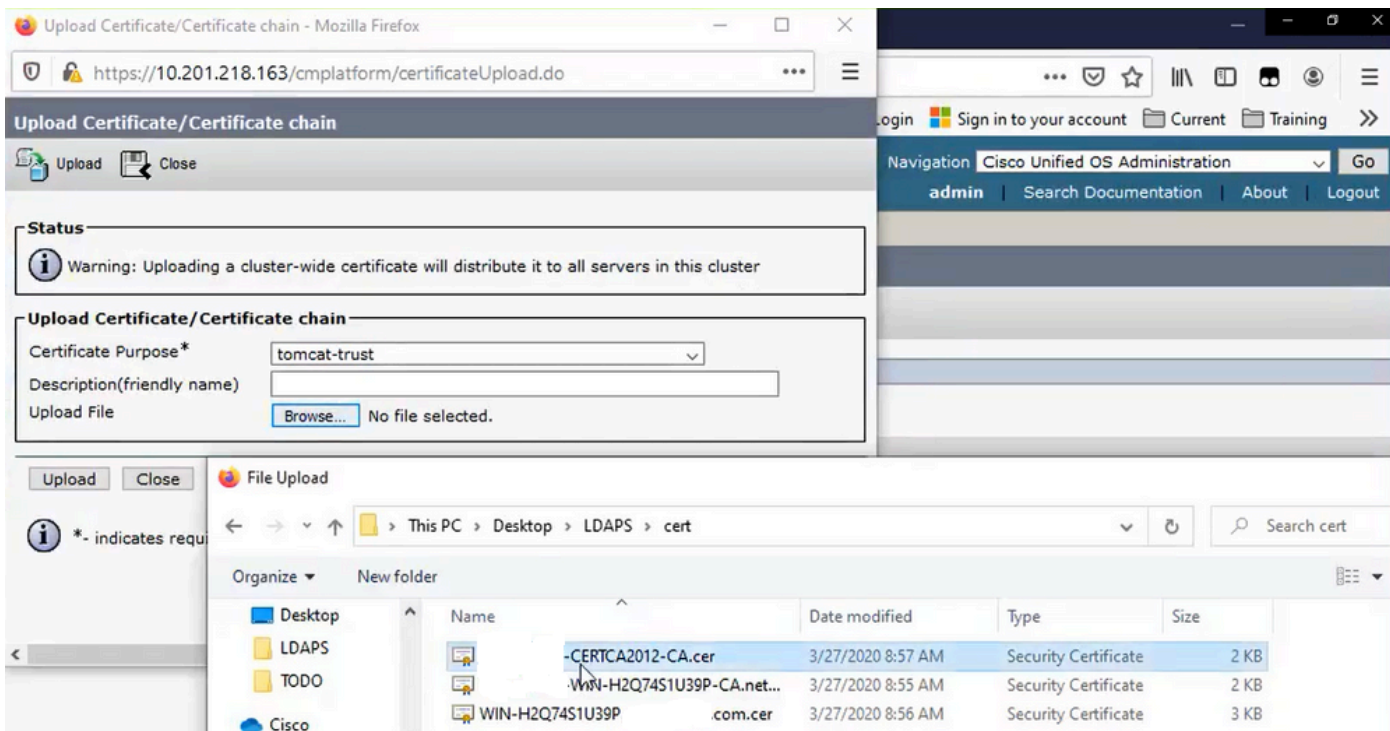


Step 2. Obtain the root and any intermediate certificates that are part of the LDAPS server certificate and install these as tomcat-trust certificates on each of the CUCM and IM/P publisher nodes and as CallManager-trust on the CUCM publisher.

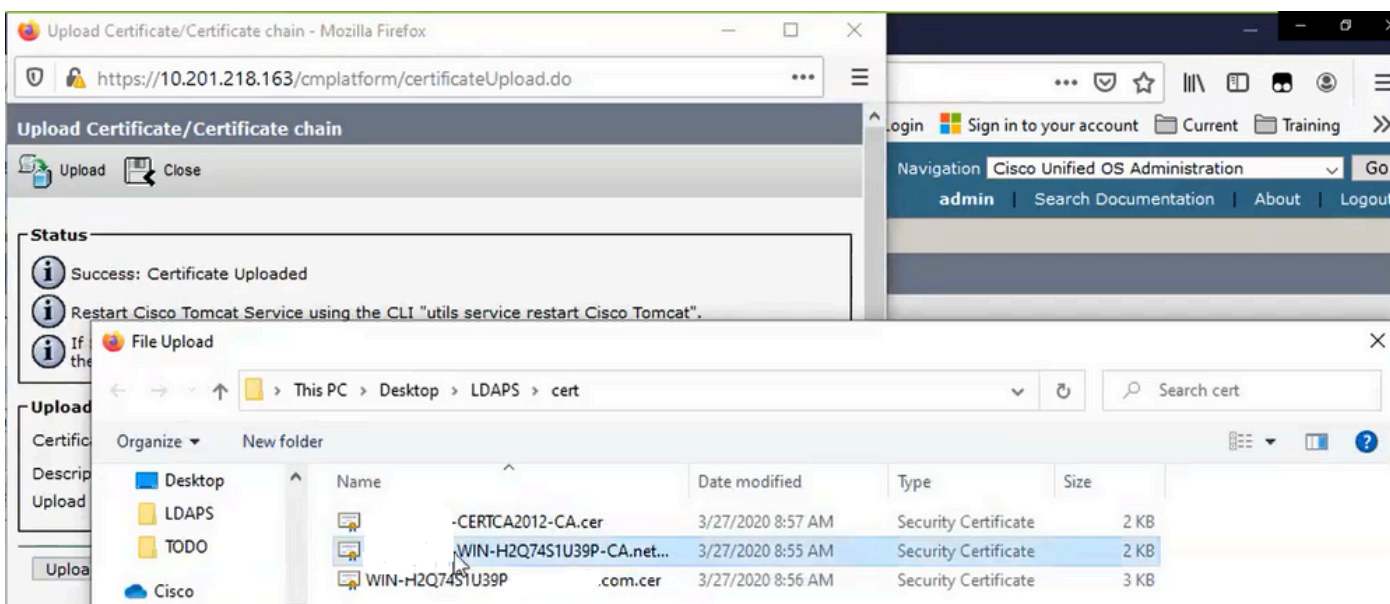
The root and intermediate certificates that are part of an LDAPS server certificate, <hostname>.<Domain>.cer, are shown in the image:



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

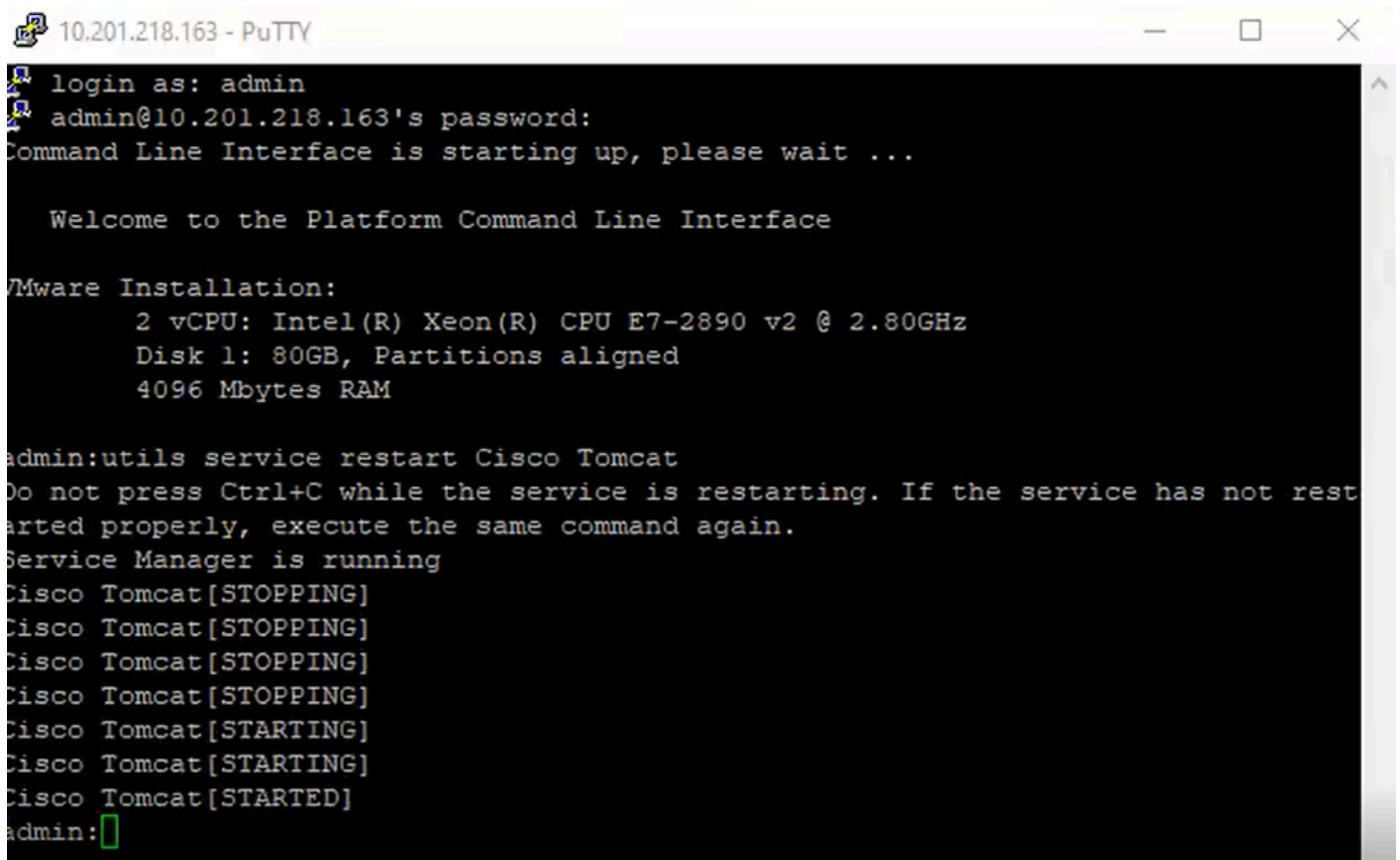


**Note:** If you have IM/P servers that are part of the CUCM cluster, you also need to upload these certificates to these IM/P servers.

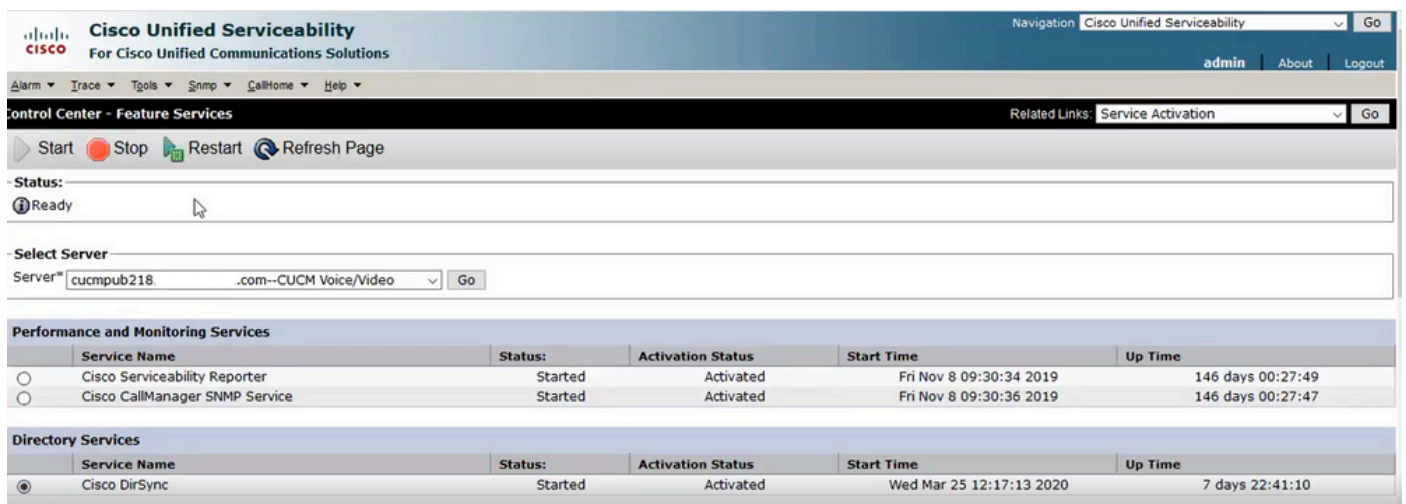
**Note:** As an alternative, you can install the LDAPS server certificate as tomcat-trust.

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:



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):



## Configure Secure LDAP Directory

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

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:

The screenshot shows the Cisco Unified CM Administration interface. The main navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', and 'Bulk Administration'. The current page is 'LDAP Directory'. The 'LDAP Server Information' section is expanded, showing the following fields:

- Host Name or IP Address for Server\*:** WIN-H2Q74S1U39P...
- LDAP Port\*:** 636
- Use TLS:**

Buttons for 'Add Another Redundant LDAP Server' and 'Add DN Pool' are visible. The 'Group Information' section above shows 'User Rank\*' set to '1-Default User Rank' and 'Access Control Groups' with 'Add to Access Control Group' and 'Remove from Access Control Group' buttons.



**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:

The screenshot shows the Cisco Unified CM Administration interface after a successful synchronization. The 'Status' section displays the message: 'Update successful. Perform a synchronization operation (manual or scheduled) to synchronize changes with the directory.' The 'LDAP Directory Information' section is expanded, showing the following fields:

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

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

**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

**Find and List Users**

+ Add New | Select All | Clear All | Delete Selected

**Status**  
3 records found

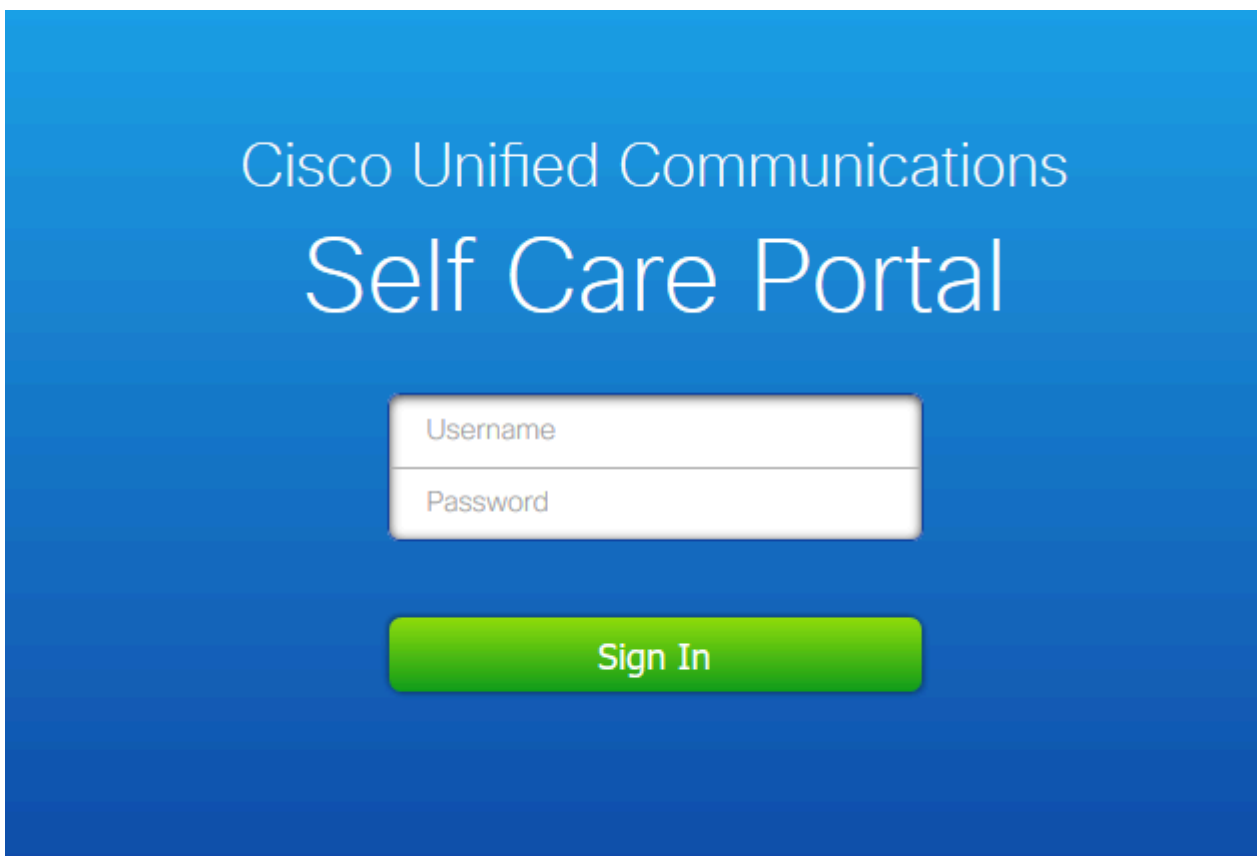
**User (1 - 3 of 3)** Rows per Page 50

Find User where First name begins with Find Clear Filter

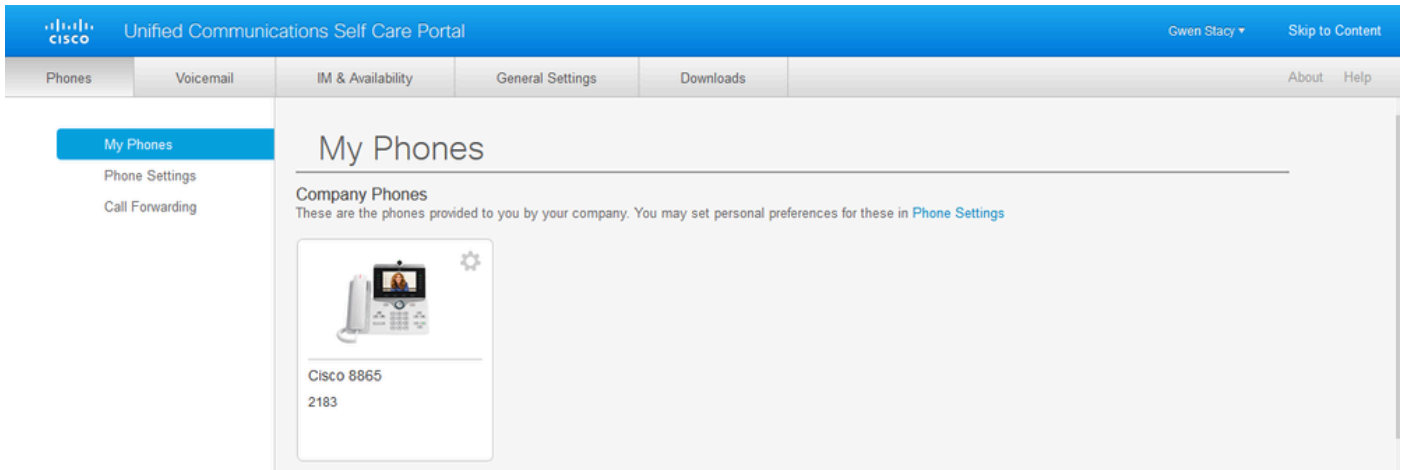
<input type="checkbox"/>	User ID ^	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
<input type="checkbox"/>	gstacy	2183	Gwen	Stacy		gstacy@.com	Active Enabled LDAP Synchronized User	1
<input type="checkbox"/>	hosborn	2182	Harry	Osborn		hosborn@.com	Active Enabled LDAP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

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:



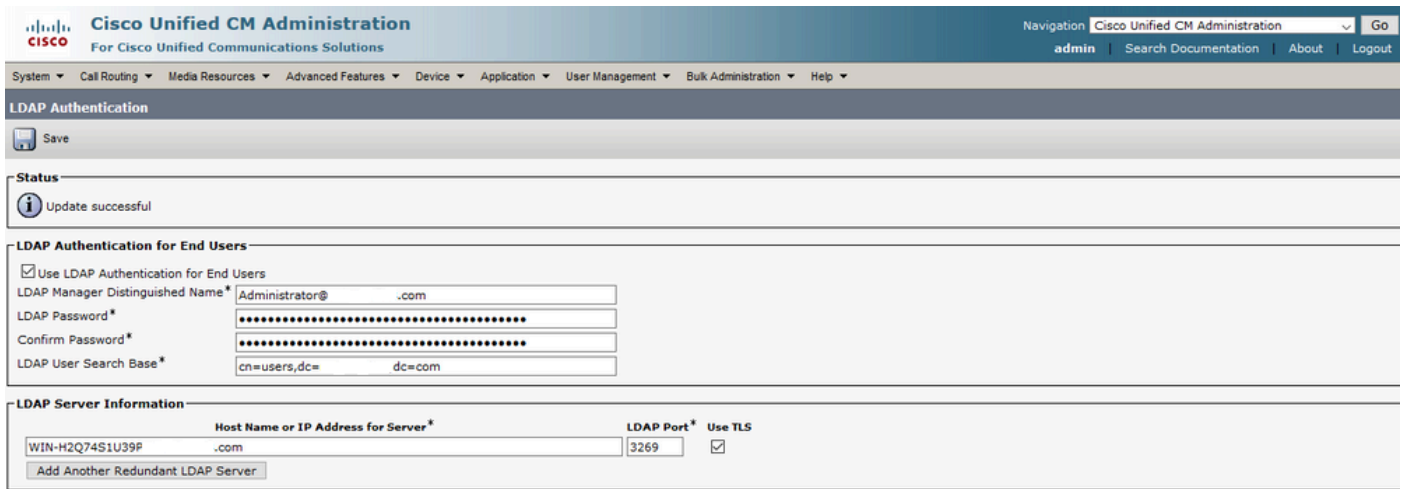
The user can successfully log in after LDAP credentials are entered, as shown in the image:



## 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:



**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:

The screenshot displays the Cisco Unified CM Administration interface for configuring a UC Service. The page title is "UC Service Configuration". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area shows a status message "Update successful" and a form for "UC Service Information". The form fields are: UC Service Type: Directory; Product Type\*: Directory; Name\*: Secure Directory; Description: (empty); Host Name/IP Address\*: WIN-H2Q74S1U39P.com; Port: 636; Protocol: TLS. Below the form are buttons for Save, Delete, Copy, Reset, Apply Config, and Add New. A note at the bottom left states "\* 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: [How to Export TLS Certificate from CUCM Packet Capture](#)

## 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: [Secure LDAP Directory and Authentication Walkthrough Video](#)
- [Technical Support & Documentation - Cisco Systems](#)