

# セキュアLDAP(LDAPS)用のCUCMの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[LDAPS証明書の確認とインストール](#)

[セキュアLDAPディレクトリの設定](#)

[セキュアLDAP認証の設定](#)

[UCサービスのADへのセキュアな接続の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、非セキュアLDAP接続からセキュアLDAPS接続へのADへのCUCM接続を更新する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- AD LDAPサーバ
- CUCM LDAP の設定
- CUCM IM & Presenceサービス(IM/P)

### 使用するコンポーネント

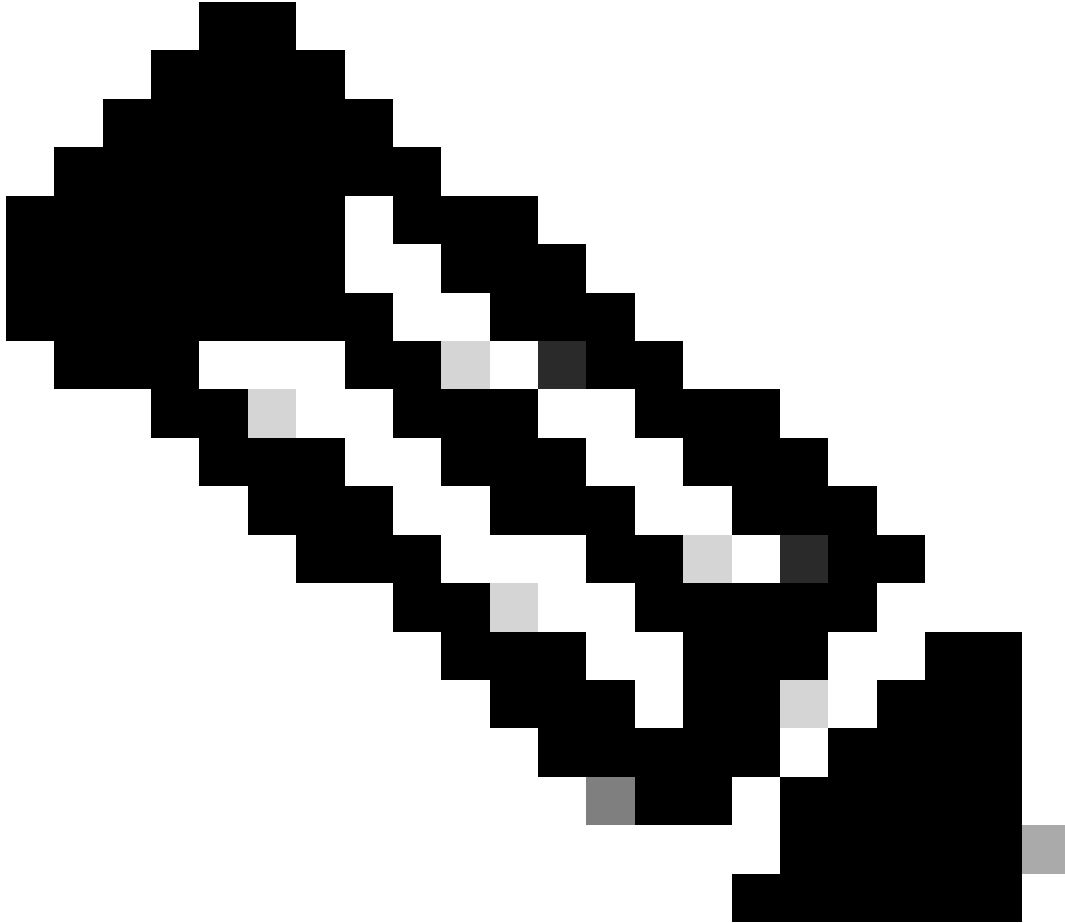
このドキュメントの情報は、CUCMリリース9.x以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

Lightweight Directory Access Protocol(LDAPS)用のAD Lightweight Directory Access Protocol(LDAP)の設定は、Active Directory(AD)管理者が行います。これには、LDAPS証明書の要件を満たすCA署名付き証明書のインストールが含まれます。

---



注：他のCisco Collaboration Applications: [Software Advisory: Secure LDAP Mandatory for Active Directory Connections](#)に対して、非セキュアLDAPからADへのセキュアLDAPS接続を更新するための情報については、このリンクを参照してください。

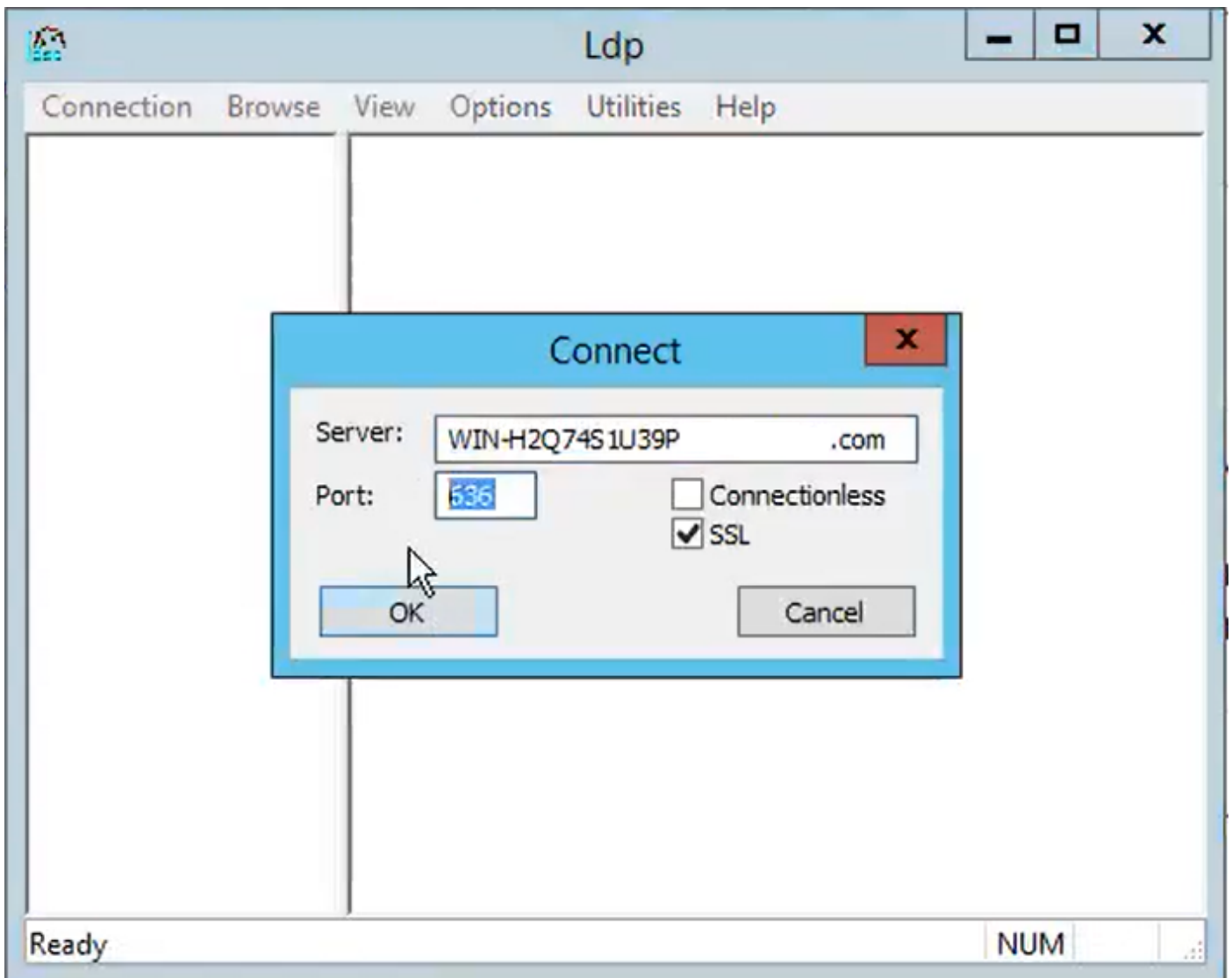
---

## LDAPS証明書の確認とインストール

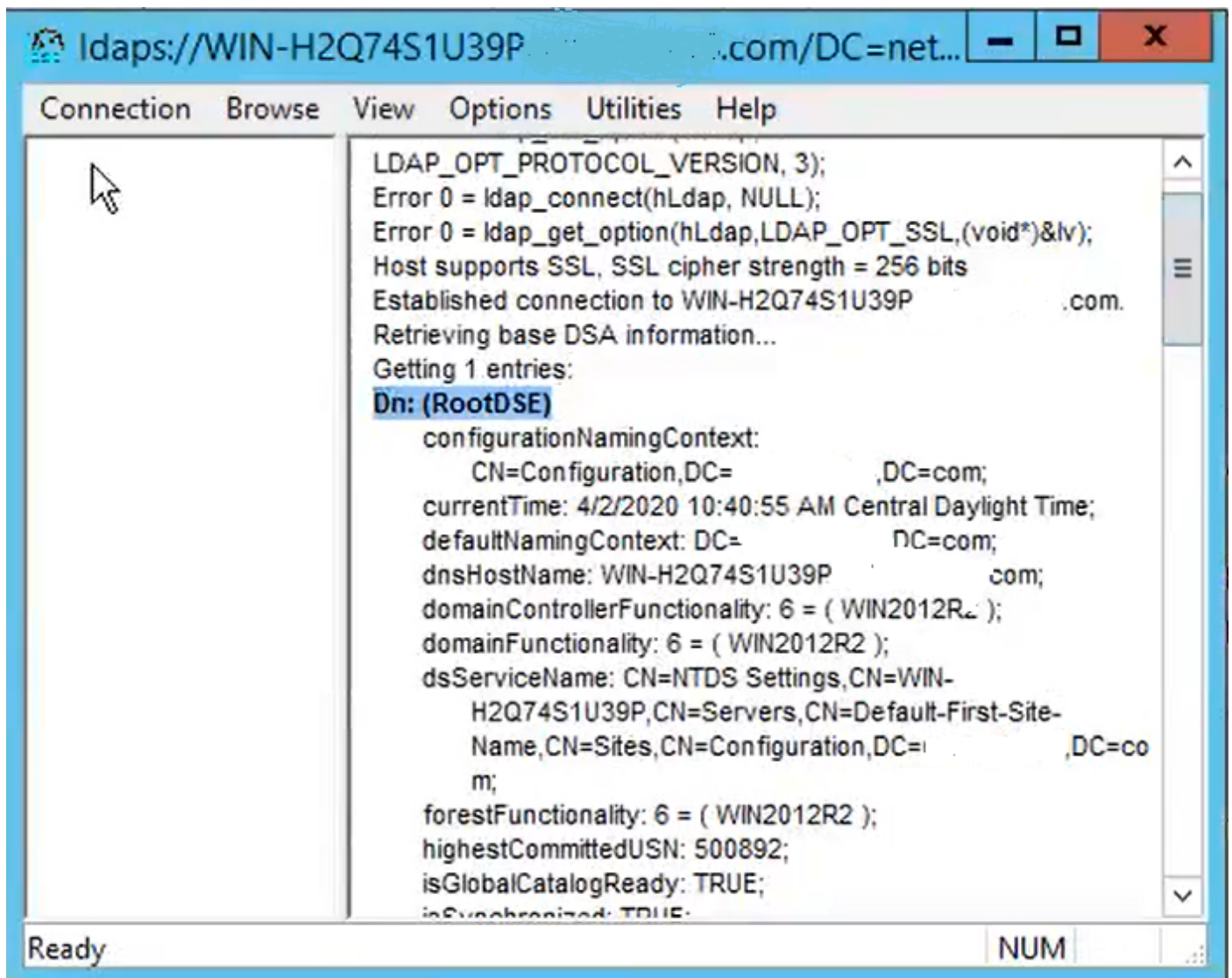
ステップ 1：LDAPS証明書がADサーバにアップロードされたら、ldp.exeツールを使用して、ADサーバでLDAPSが有効になっていることを確認します。

1. ADサーバでAD管理ツール(Ldp.exe)を起動します。
2. ConnectionメニューからConnectを選択します。
3. LDAPSサーバの完全修飾ドメイン名(FQDN)をサーバとして入力します。
4. ポート番号として636を入力します。

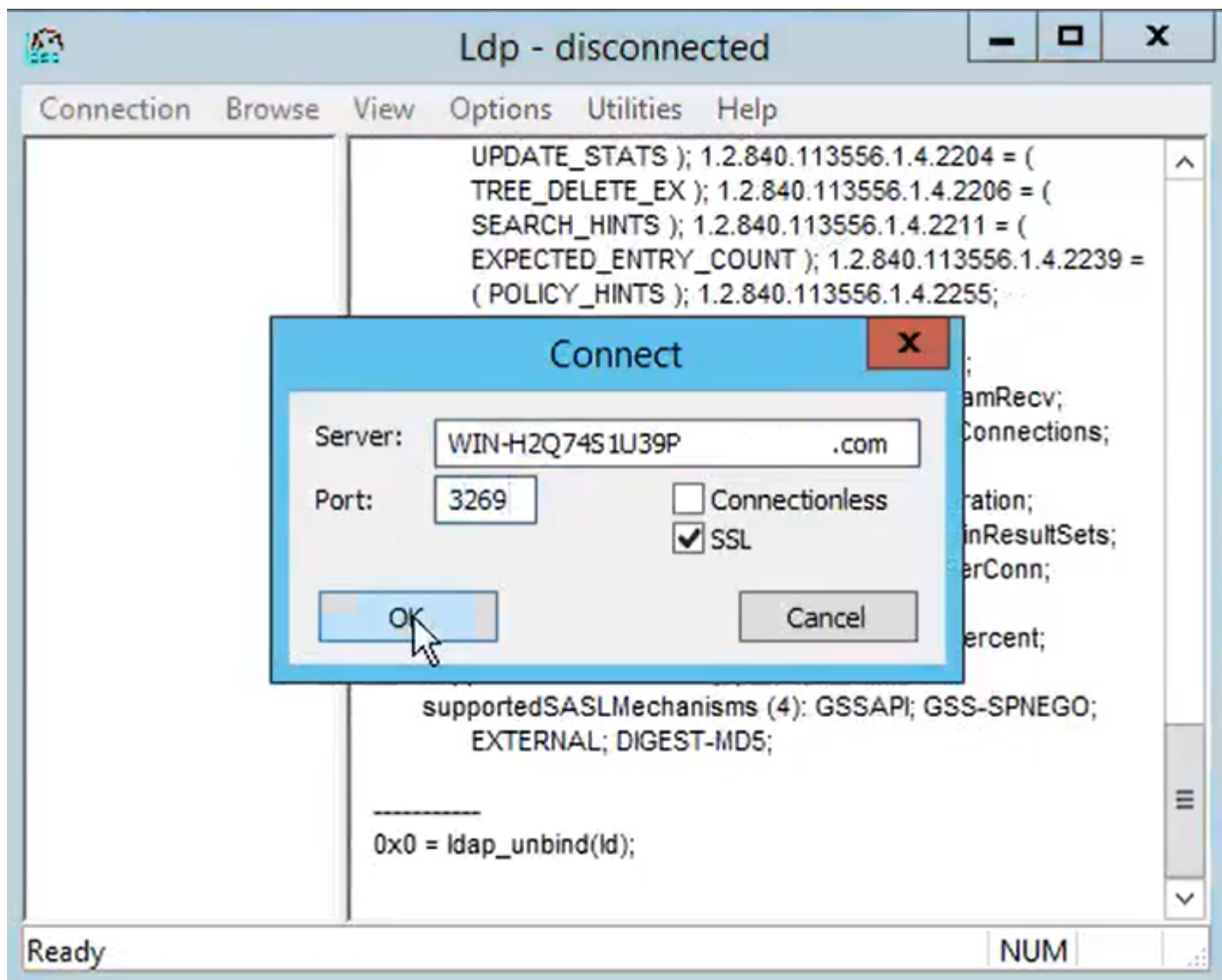
5. 図に示すように、OKをクリックします



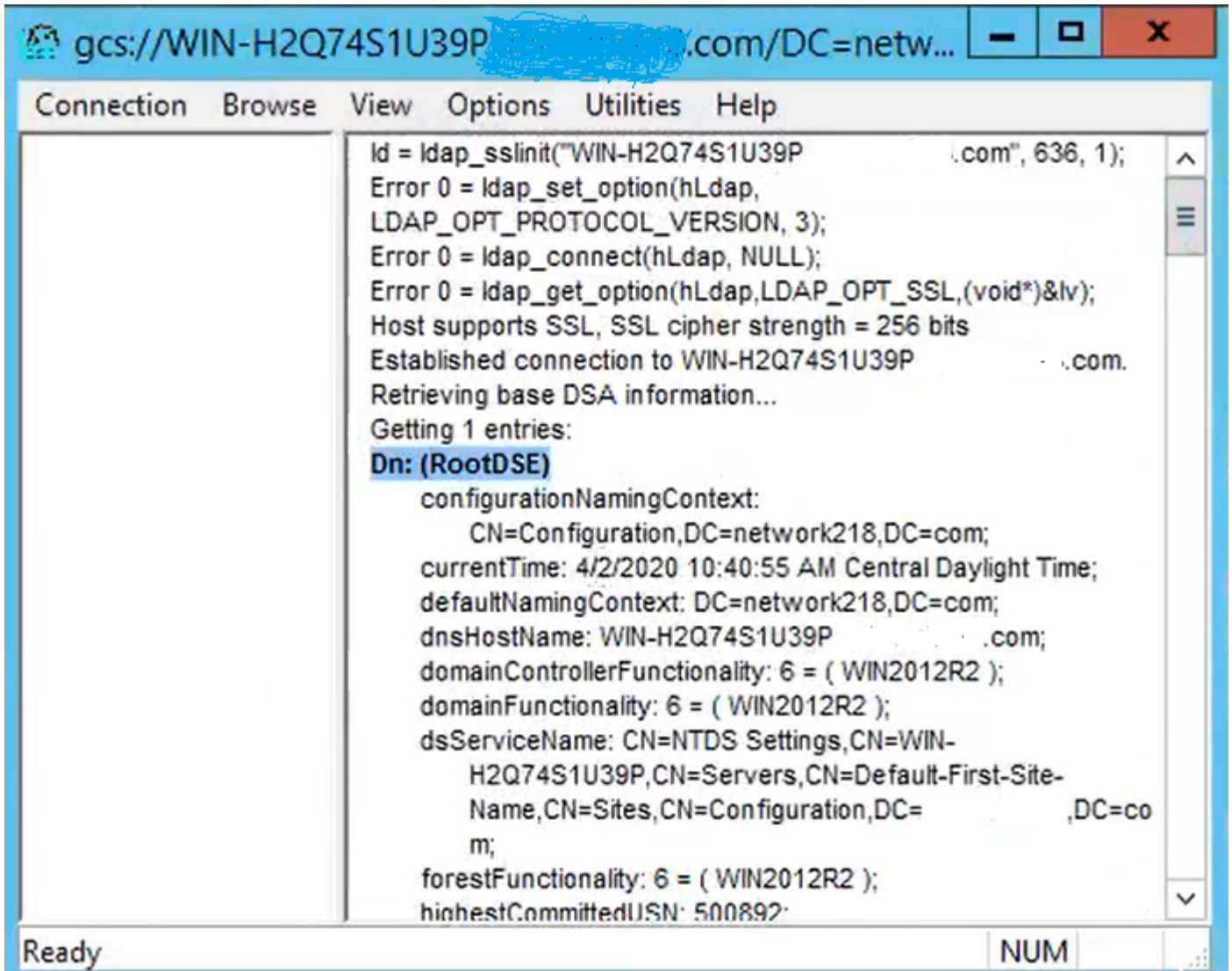
ポート636での接続が正常に行われると、図に示すように、右側のペインにRootDSE情報が出力されます。



図に示すように、ポート3269に対してこの手順を繰り返します。

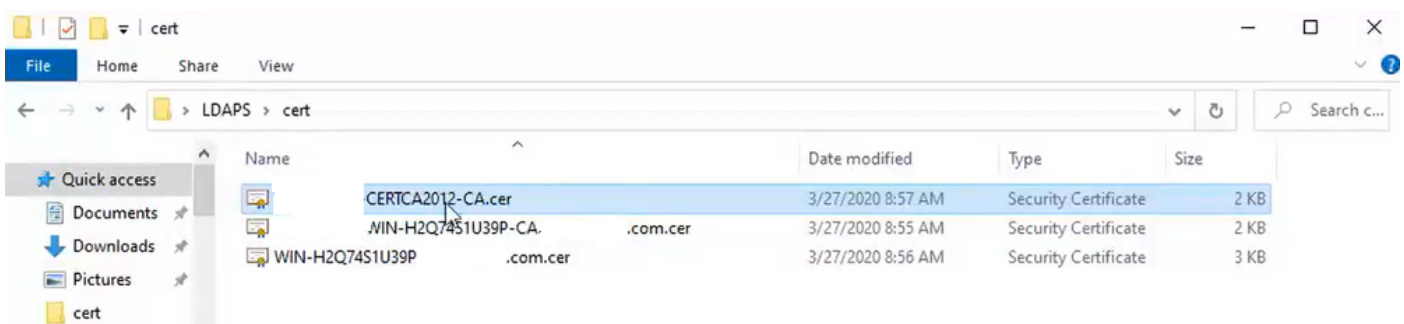


ポート3269での接続が正常に行われると、図に示すように、RootDSE情報が右側のペインに表示されます。

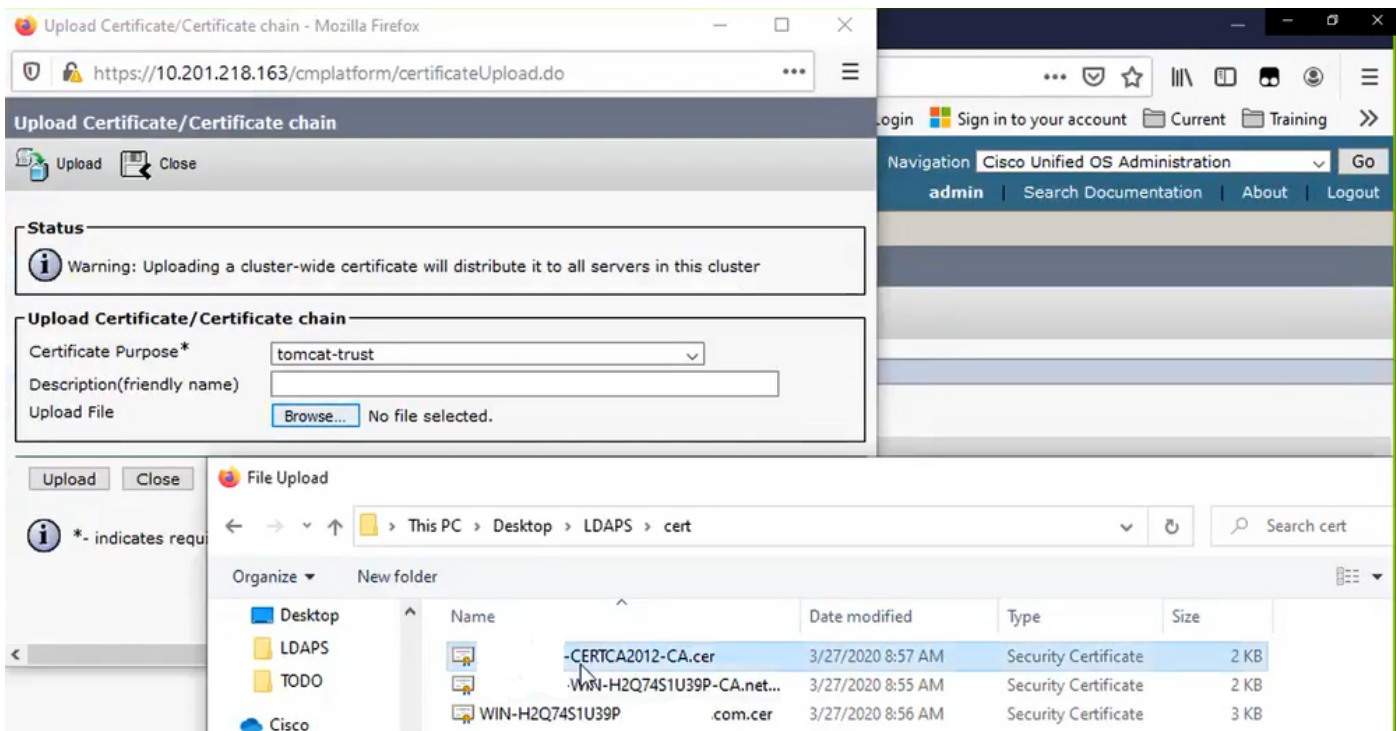


ステップ 2 : LDAPSサーバ証明書の一部であるルート証明書と中間証明書を取得し、これらを tomcat-trust証明書として各CUCMおよびIM/Pパブリッシャノードにインストールし、 CallManager-trustとしてCUCMパブリッシャにインストールします。

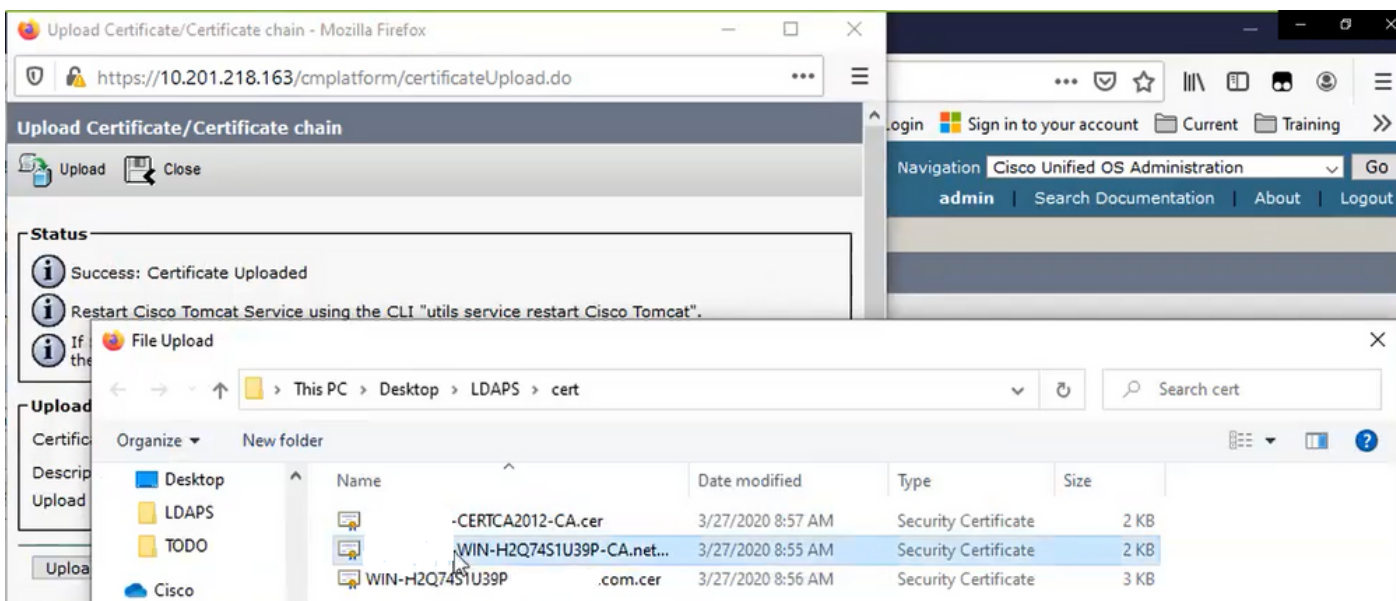
LDAPSサーバ証明書<hostname>.<Domain>.cerの一部であるルート証明書と中間証明書を図に示します。



CUCMパブリッシャのCisco Unified OS Administration > Security > Certificate Managementに移動します。ルート(root)をtomcat-trust ( 図を参照 ) およびCallManager-trust ( 図を参照 ) としてアップロードします。



intermediateをtomcat-trust ( 図を参照 ) およびCallManager-trust ( 図を参照 ) としてアップロードします。

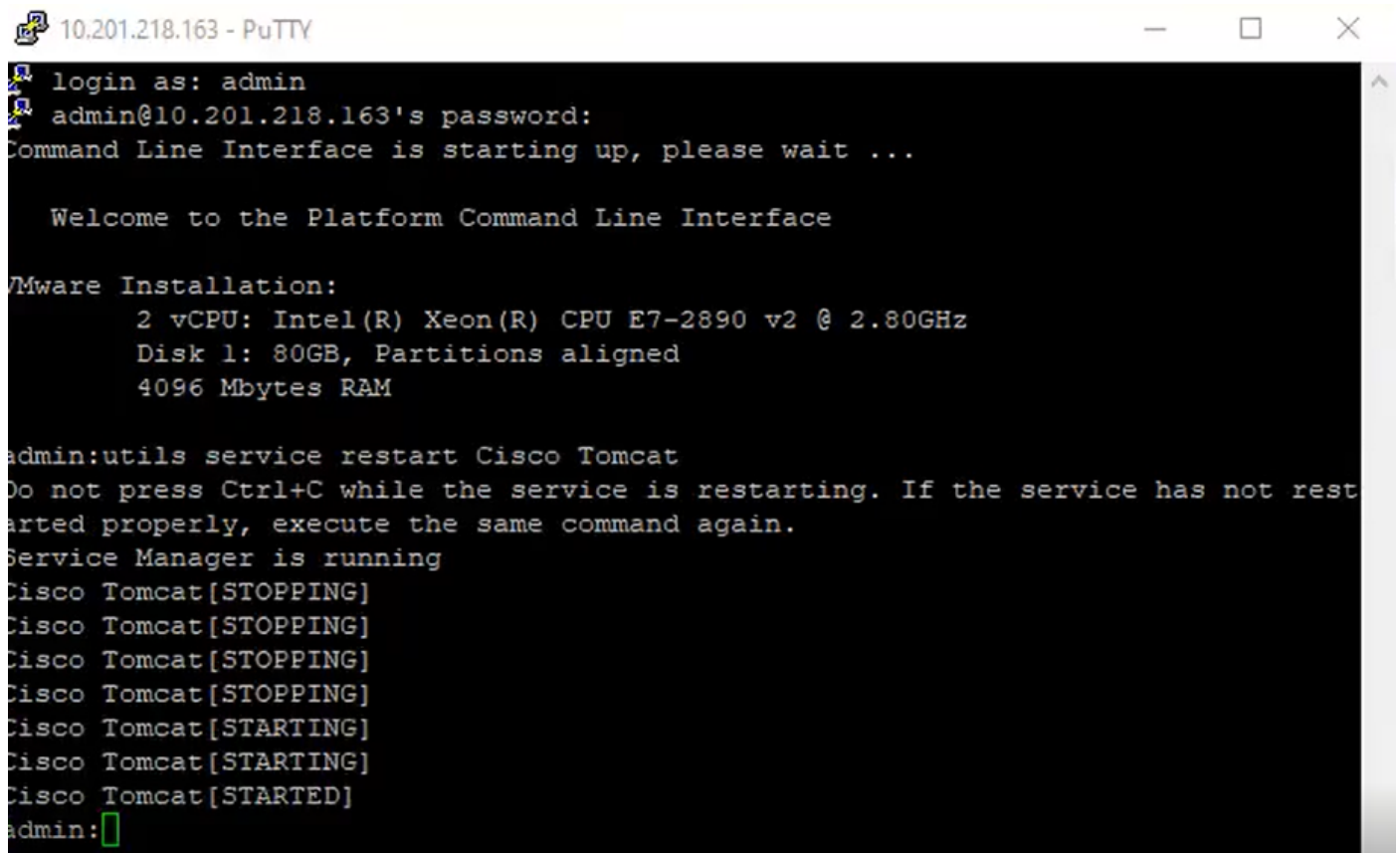


**注** : CUCMクラスタの一部であるIM/Pサーバがある場合、これらの証明書をこれらのIM/Pサーバにアップロードする必要があります。

**注** : 別の方法として、LDAPSサーバ証明書をtomcat-trustとしてインストールすることもできます。

ステップ 3 : クラスタ内の各ノード ( CUCMおよびIM/P ) のCLIからCisco Tomcatを再起動します。また、CUCMクラスタでは、パブリッシャノードでCisco DirSyncサービスが起動していることを確認します。

tomcatサービスを再起動するには、各ノードのCLIセッションを開き、図に示すようにコマンド  
utils service restart Cisco Tomcatを実行する必要があります。



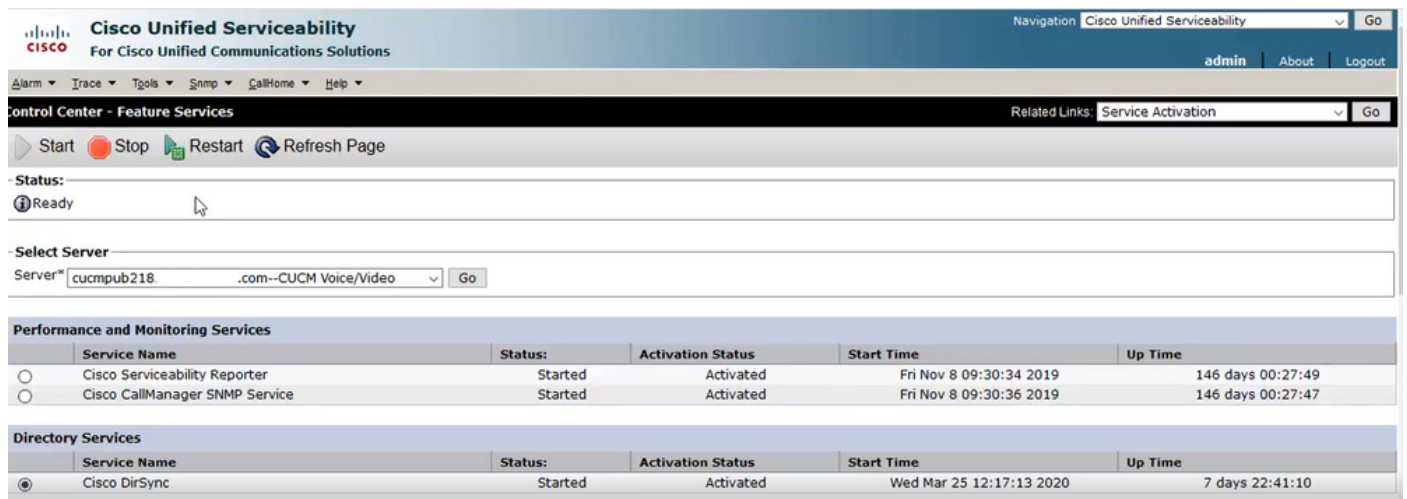
```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

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:
```

ステップ 4 : CUCMパブリッシャのCisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動し、Cisco DirSyncサービスがアクティブで開始されていることを確認し ( 図を参照 )、これが使用されている場合は各ノードでCisco CTIManagerサービスを再起動します ( 図を参照 )。



Cisco Unified Serviceability  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified Serviceability Go

admin About Logout

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

## セキュアLDAPディレクトリの設定

ステップ 1 : ポート636でのADへのLDAPS TLS接続を利用するために、CUCM LDAPディレクトリを設定します。



CUCM Administration > System > LDAP Directoryの順に移動します。LDAPサーバ情報のLDAPSサーバのFQDNまたはIPアドレスを入力します。図に示すように、LDAPSポートとして636を指定して、Use TLSのボックスにチェックマークを付けます。

The screenshot shows the Cisco Unified CM Administration interface for configuring an LDAP Directory. The page is titled "LDAP Directory" and includes a navigation menu at the top with options like "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is divided into two sections: "Group Information" and "LDAP Server Information".

**Group Information**

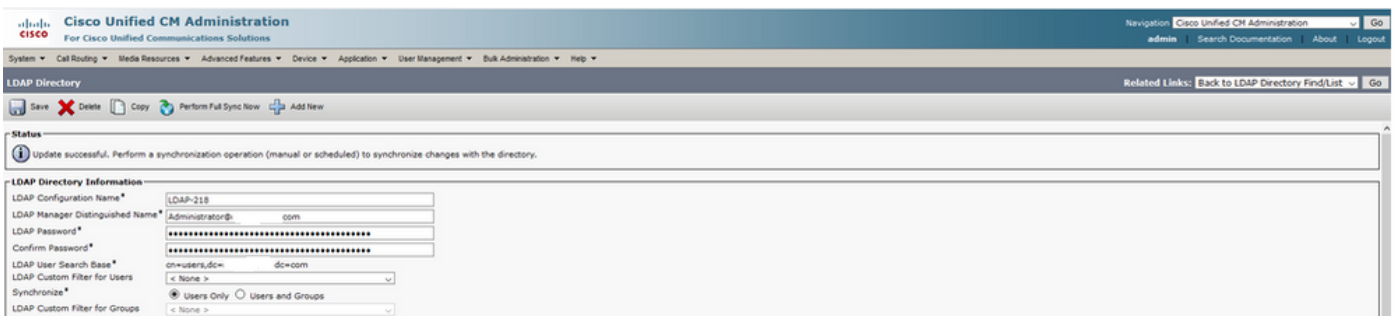
- User Rank\*: 1-Default User Rank
- Access Control Groups: A list box with "Add to Access Control Group" and "Remove from Access Control Group" buttons.
- Feature Group Template: < None >
- Warning: If no template is selected, the new line features below will not be active.
- Apply mask to synced telephone numbers to create a new line for inserted users
- Mask: [Text Input]
- Assign new line from the pool list if one was not created based on a synced LDAP telephone number
- Order: DN Pool Start [Text Input] DN Pool End [Text Input]
- Add DN Pool [Button]

**LDAP Server Information**

- Host Name or IP Address for Server\*: WIN-H2Q74S1U39R.com
- LDAP Port\*: 636
- Use TLS:
- Add Another Redundant LDAP Server [Button]

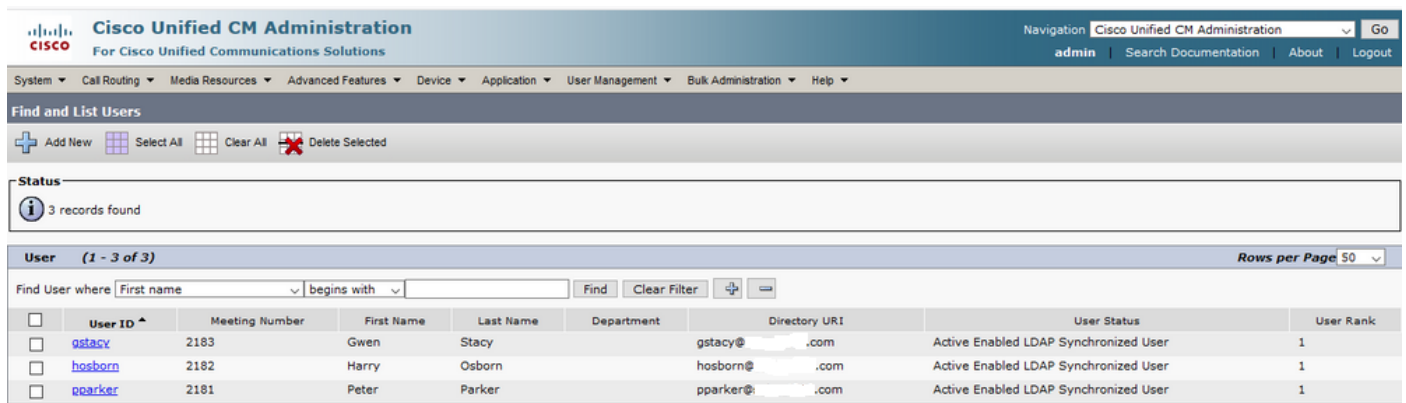
注：デフォルトでは、LDAPサーバ情報で設定されているバージョン10.5(2)SU2および9.1(2)SU3のFQDNが証明書のCommon Nameに照らしてチェックされた後、FQDNの代わりにIPアドレスが使用されている場合は、コマンドutils ldap config ipaddrを発行してFQDNからCNへの検証の適用を停止します。

ステップ 2：LDAPSの設定変更を完了するには、図に示すように、Perform Full Sync Nowをクリックします。



The screenshot shows the Cisco Unified CM Administration web interface. The page title is "LDAP Directory". At the top, there is a navigation menu with items like "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". Below the navigation, there are icons for "Save", "Delete", "Copy", "Perform Full Sync Now", and "Add New". A status message indicates a successful update. The main section is titled "LDAP Directory Information" and contains several fields: "LDAP Configuration Name" (LDAP-218), "LDAP Manager Distinguished Name" (Administrator@.com), "LDAP Password" (masked), "Confirm Password" (masked), "LDAP User Search Base" (ou=users,dc=,dc=com), "LDAP Custom Filter for Users" (None), "Synchronize" (Users Only selected), and "LDAP Custom Filter for Groups" (None). The "Perform Full Sync Now" button is highlighted with a red box.

ステップ 3 : CUCM Administration > User Management > End Userの順に移動し、図に示すようにエンドユーザが存在することを確認します。

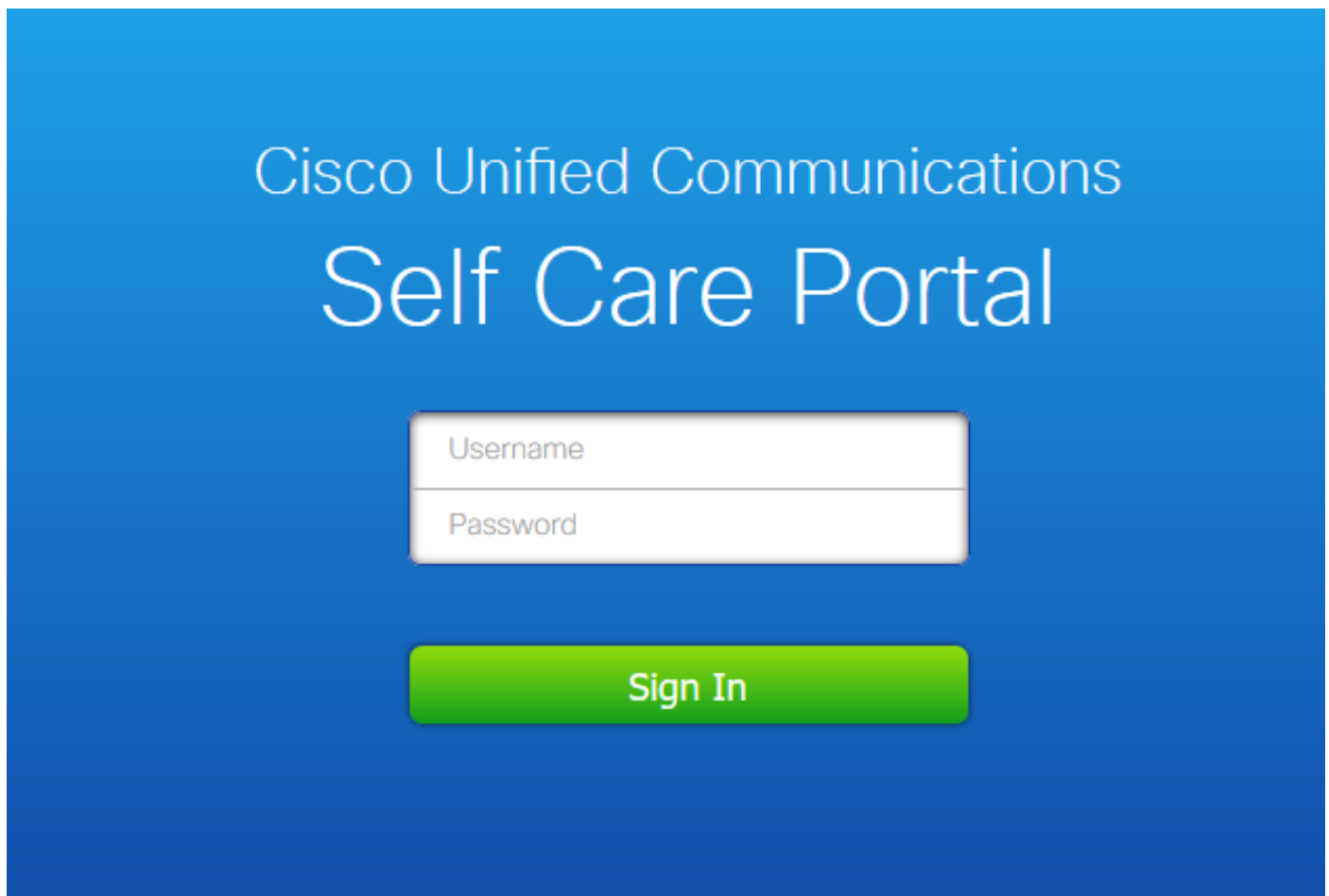


The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes 'Cisco Unified CM Administration' and 'For Cisco Unified Communications Solutions'. The main menu includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Find and List Users' section is active, showing '3 records found'. Below this is a table of users with columns for 'User ID', 'Meeting Number', 'First Name', 'Last Name', 'Department', 'Directory URI', 'User Status', and 'User Rank'.

<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

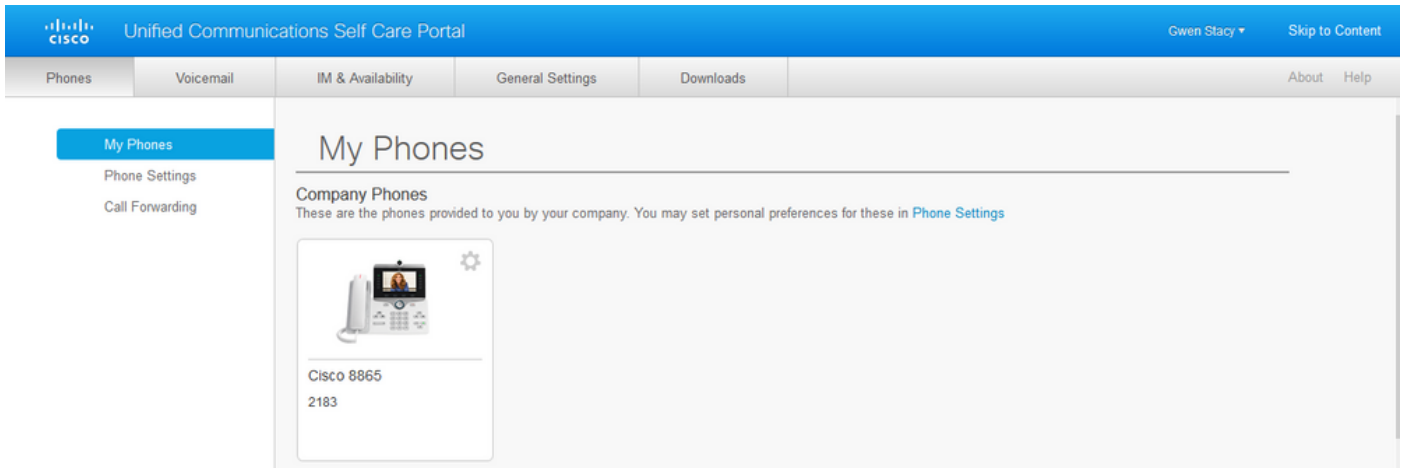
ステップ 4 : ユーザログインが成功したことを確認するために、ccmuserページ(<https://<ip address of cucm pub>/ccmuser>)に移動します。

CUCMバージョン12.0.1のccmuserページは次のようになります。



The screenshot shows the Cisco Unified Communications Self Care Portal login page. The background is blue with the text 'Cisco Unified Communications Self Care Portal' in white. Below the text is a login form with two input fields: 'Username' and 'Password'. A green 'Sign In' button is positioned below the form.

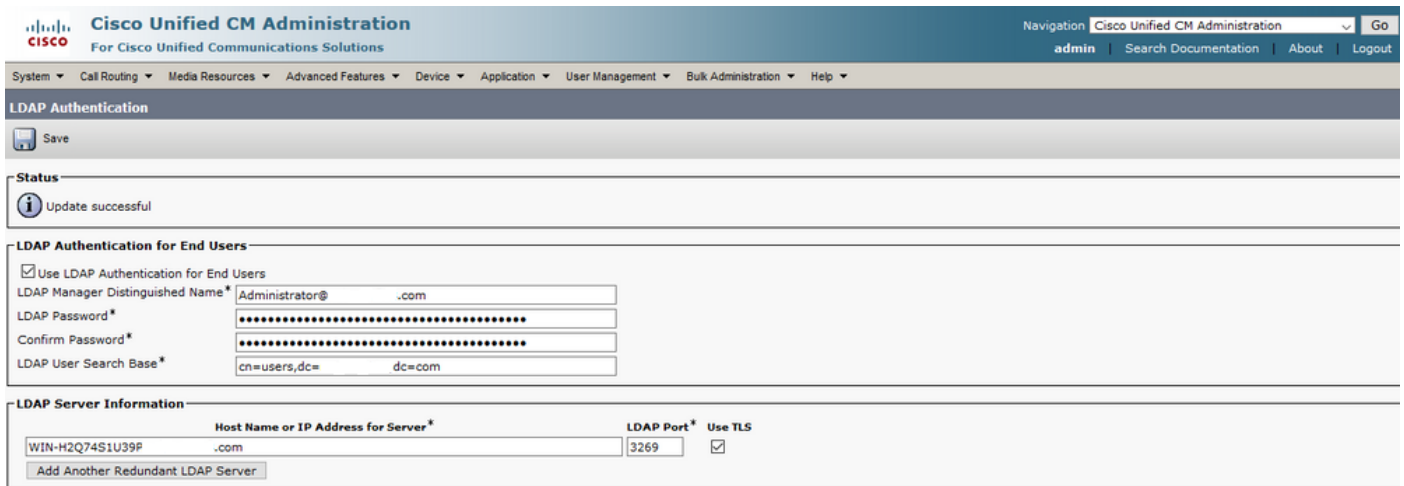
図に示すように、ユーザはLDAPクレデンシャルの入力後に正常にログインできます。



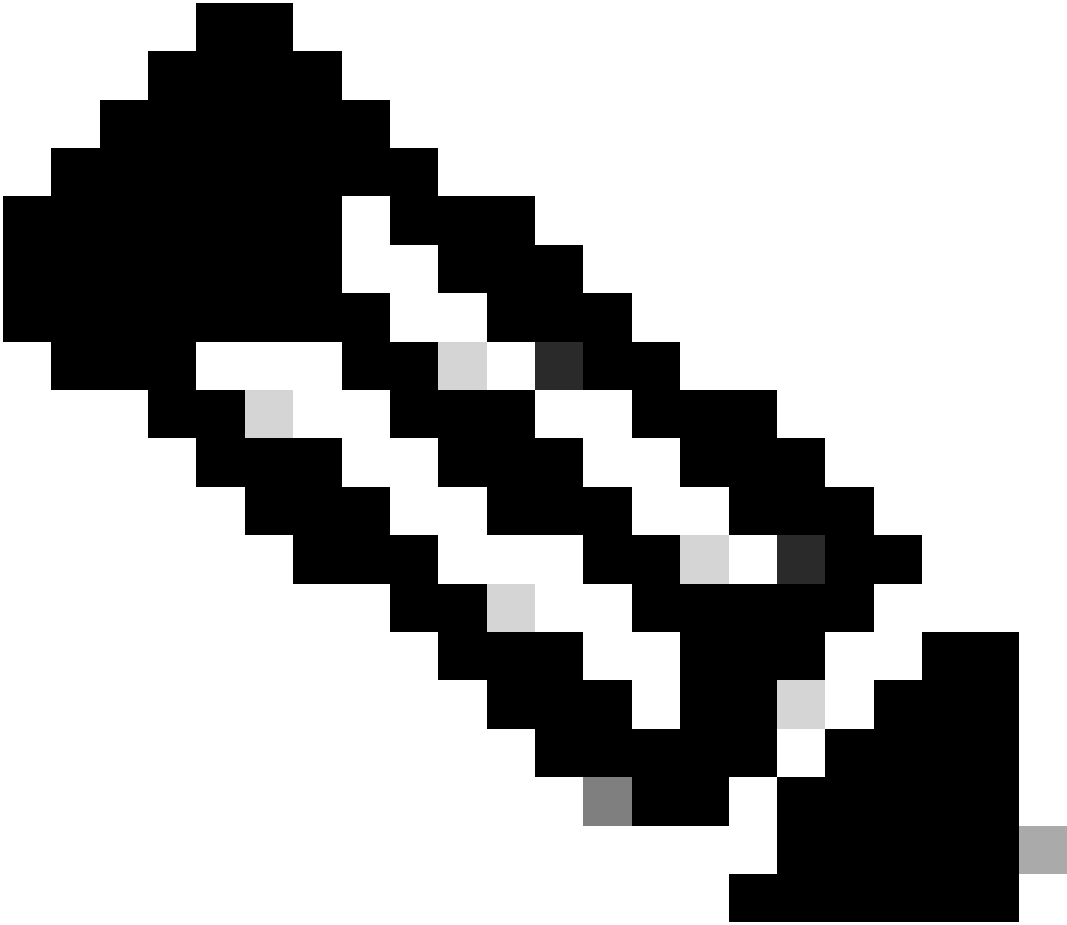
## セキュアLDAP認証の設定

ポート3269でのADへのLDAPS TLS接続を利用するために、CUCM LDAP認証を設定します。

CUCM Administration > System > LDAP Authenticationの順に移動します。LDAPサーバ情報のLDAPSサーバのFQDNを入力します。図に示すように、LDAPSポートとして3269を指定して、Use TLSのボックスにチェックマークを付けます。



---



注：Jabberクライアントを使用している場合は、LDAPS認証にポート3269を使用することをお勧めします。これは、グローバルカタログサーバへのセキュアな接続が指定されていないと、ログイン時にJabberがタイムアウトする可能性があるためです。

---

## UCサービスのADへのセキュアな接続の設定

LDAPを使用するUCサービスを保護する必要がある場合は、TLSでポート636または3269を使用するようにこれらのUCサービスを設定します。

CUCM administration > User Management > User Settings > UC Serviceの順に移動します。ADを指すディレクトリサービスを検索します。LDAPSサーバのFQDNをホスト名/IPアドレスとして入力します。図に示すように、ポートを636または3269、およびプロトコルTLSとして指定します

。

**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.

注：JabberクライアントがADへのLDAPS接続を確立できるようにするには、Jabberクライアントマシンの証明書管理信頼ストアにインストールされているCUCMにインストールされているtomcat-trust LDAPS証明書も、Jabberクライアントマシンに必要です。

## 確認

このセクションでは、設定が正常に動作していることを確認します。

TLS接続のためにLDAPサーバからCUCMに送信された実際のLDAPS証明書/証明書チェーンを確認するには、CUCMパケットキャプチャからLDAPS TLS証明書をエクスポートします。CUCMパケットキャプチャからTLS証明書をエクスポートする方法については、[CUCMパケットキャプチャからTLS証明書をエクスポートする方法](#)を参照してください。

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- LDAPS設定を確認できるビデオ([セキュアLDAPディレクトリおよび認証ウォークスルービデオ](#))へのアクセスを提供します。
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。