

# LDAPS(Secure LDAP)용 CUCM 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[LDAPS 인증서 확인 및 설치](#)

[보안 LDAP 디렉터리 구성](#)

[보안 LDAP 인증 구성](#)

[UC 서비스의 AD에 대한 보안 연결 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

---

## 소개

이 문서에서는 비보안 LDAP 연결에서 보안 LDAPS 연결로 AD에 대한 CUCM 연결을 업데이트하는 절차에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AD LDAP 서버
- CUCM LDAP 컨피그레이션
- CUCM IM & Presence Service(IM/P)

### 사용되는 구성 요소

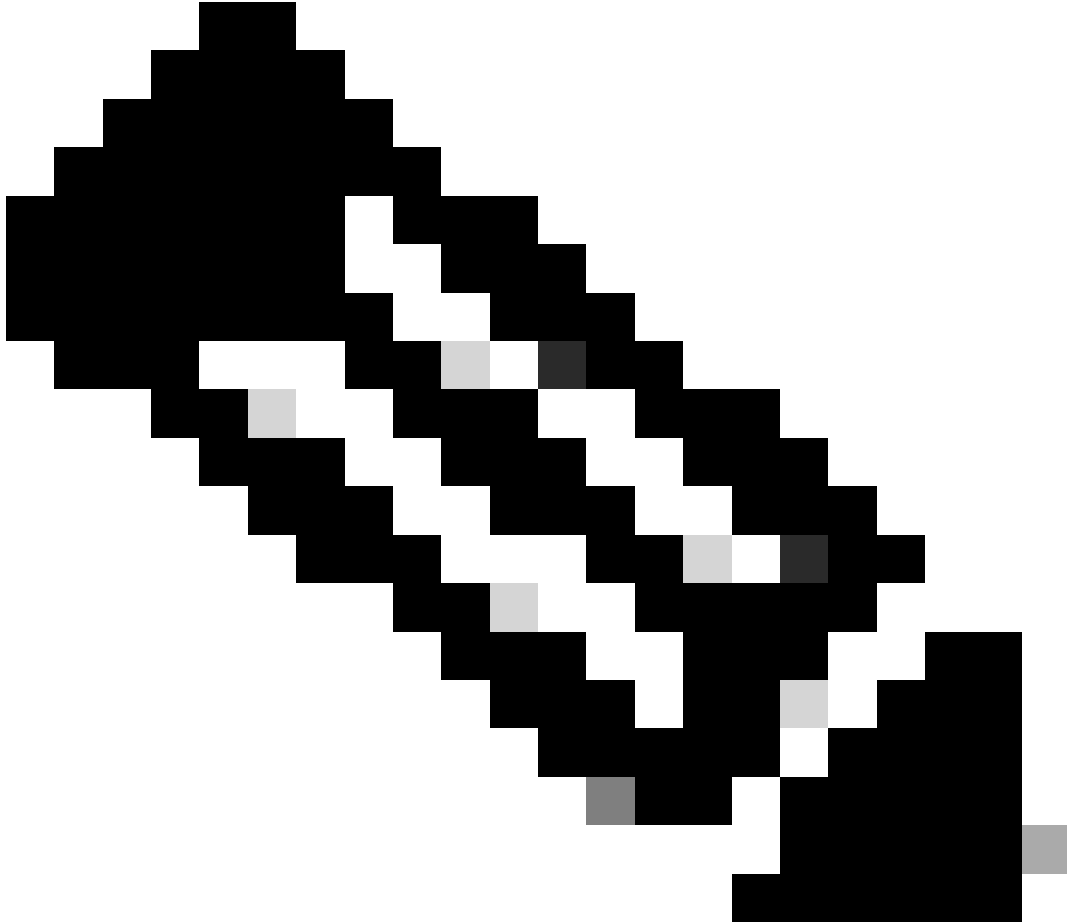
이 문서의 정보는 CUCM 릴리스 9.x 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

LDAP(Lightweight Directory Access Protocol)용 AD LDAP(Lightweight Directory Access Protocol)를 구성하는 것은 AD(Active Directory) 관리자의 책임입니다. 여기에는 LDAPS 인증서의 요구 사항을 충족하는 CA 서명 인증서 설치가 포함됩니다.

---



참고: 비보안 LDAP에서 다른 Cisco Collaboration 애플리케이션의 AD로 LDAPS 연결을 보호하도록 업데이트하려면 이 링크를 참조하십시오. [소프트웨어 권고: Active Directory 연결에 필요한 보안 LDAP](#)

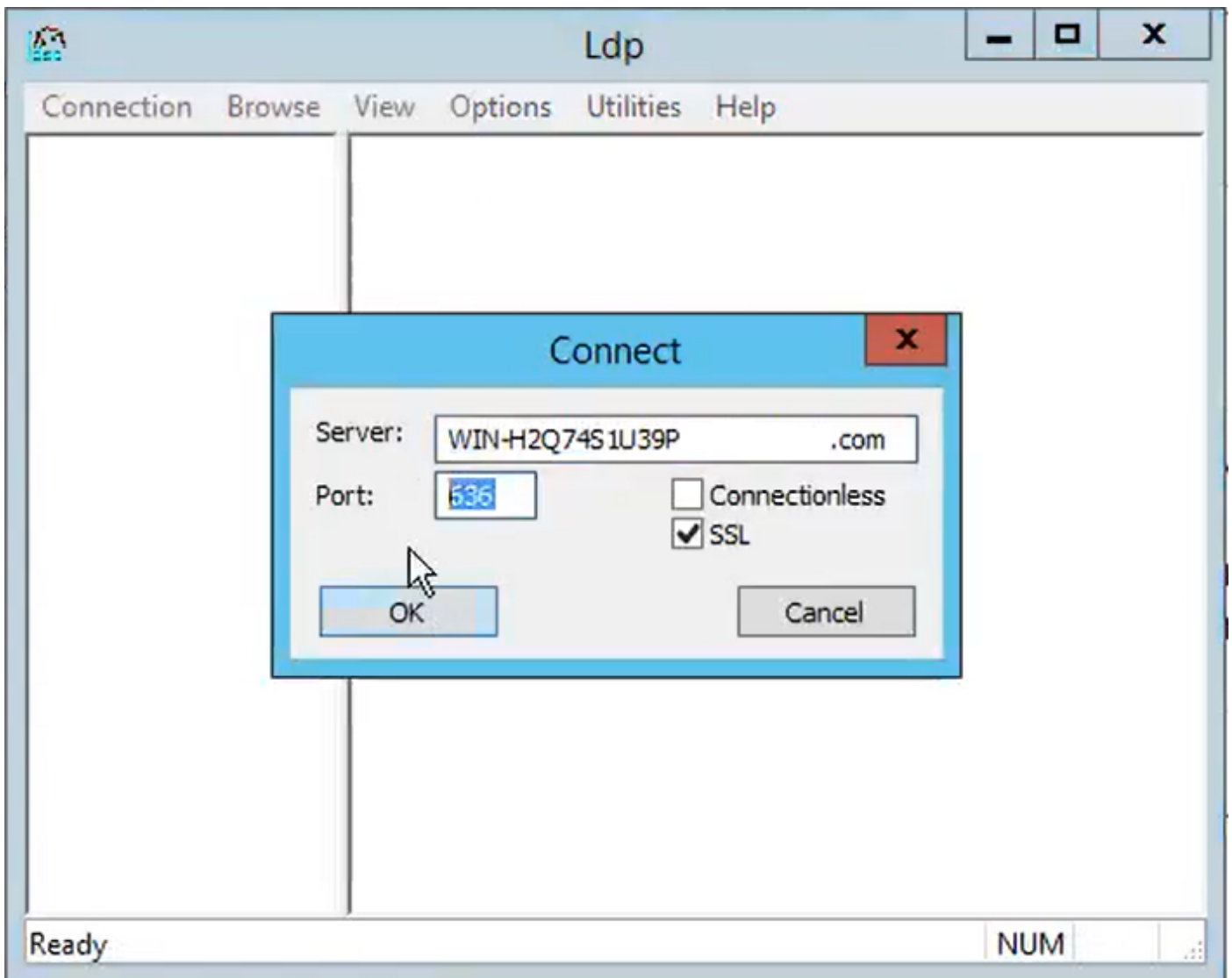
---

## LDAPS 인증서 확인 및 설치

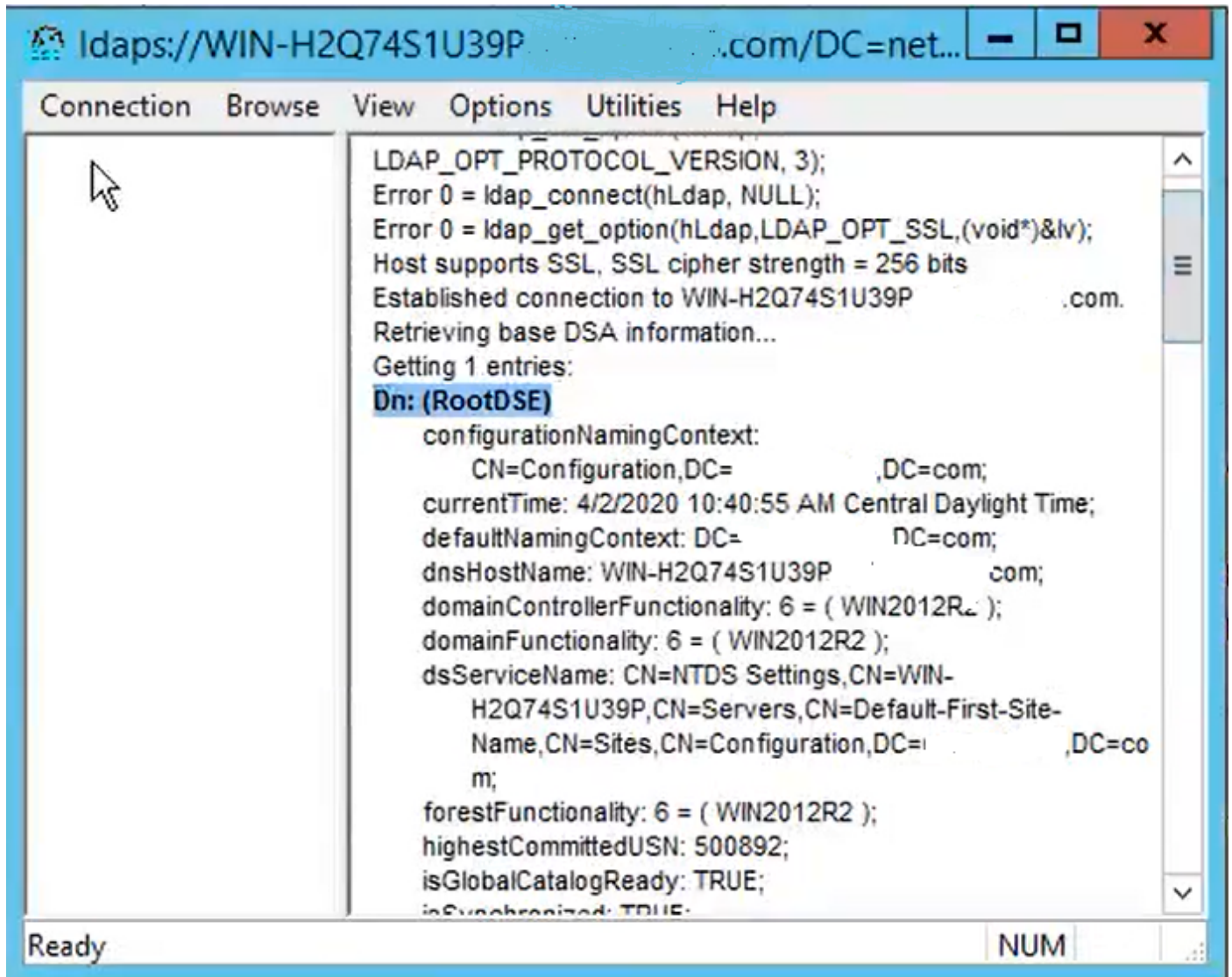
1단계. LDAPS 인증서가 AD 서버에 업로드된 후 AD 서버에서 ldp.exe 도구를 사용하여 LDAPS가 활성화되어 있는지 확인합니다.

1. AD 서버에서 AD 관리 도구(Ldp.exe)를 시작합니다.
2. 연결 메뉴에서 연결을 선택합니다.
3. LDAPS 서버의 FQDN(Fully Qualified Domain Name)을 서버로 입력합니다.
4. 포트 번호로 636을 입력합니다.

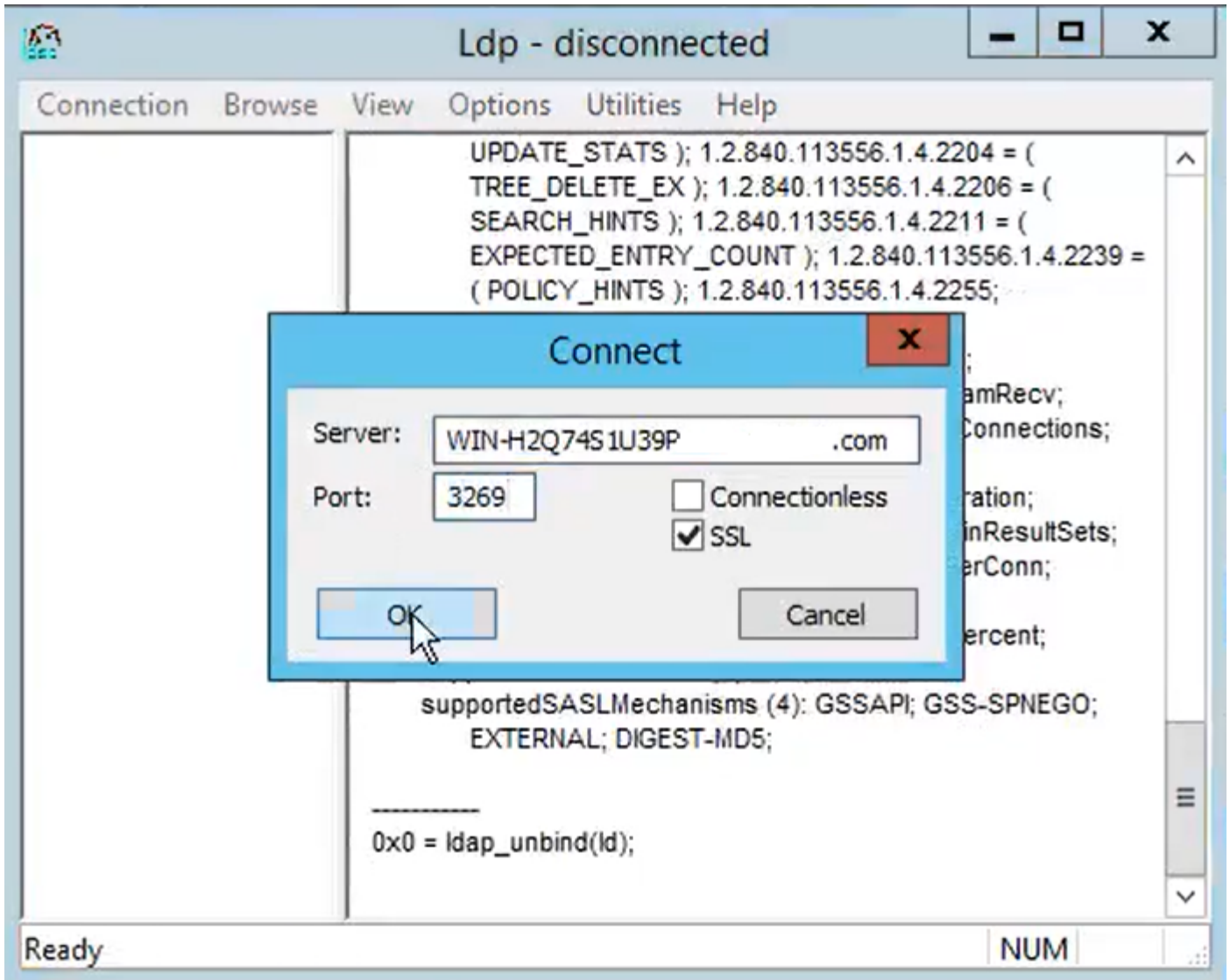
5. 그림과 같이 OK(확인)를 클릭합니다



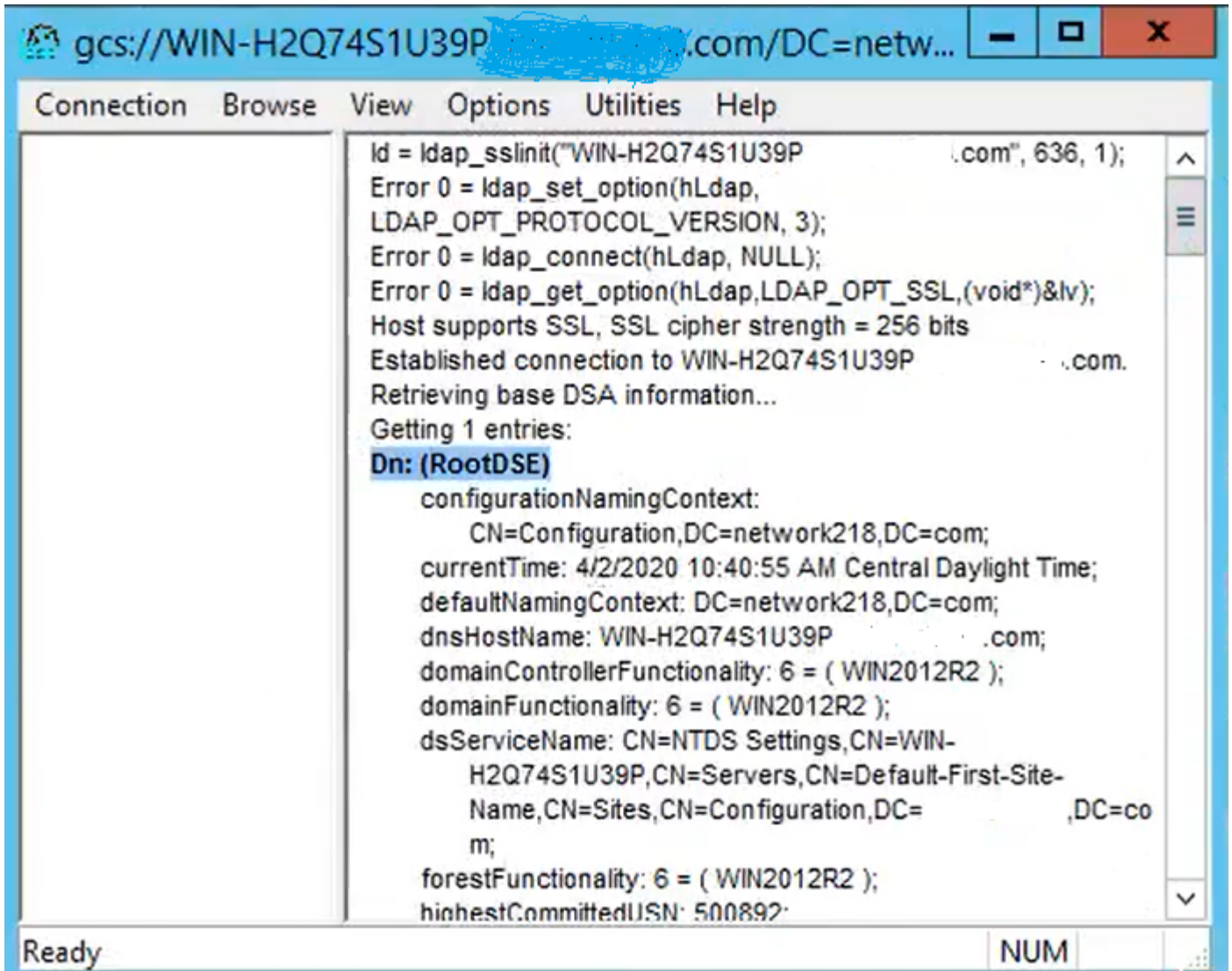
포트 636에서 성공적으로 연결하려면 그림과 같이 RootDSE 정보가 오른쪽 창에 출력됩니다.



이미지에 표시된 대로 포트 3269에 대해 절차를 반복합니다.

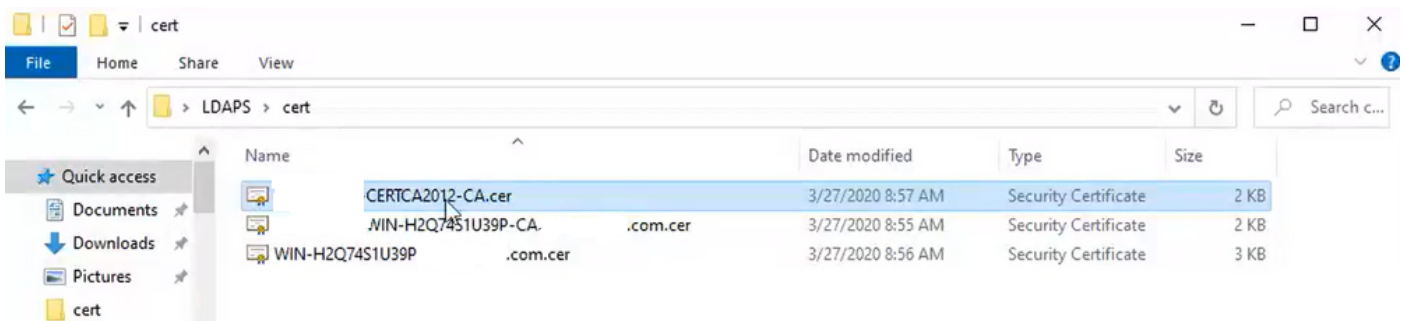


포트 3269에서 성공적으로 연결하려면 그림과 같이 RootDSE 정보가 오른쪽 창에 출력됩니다.



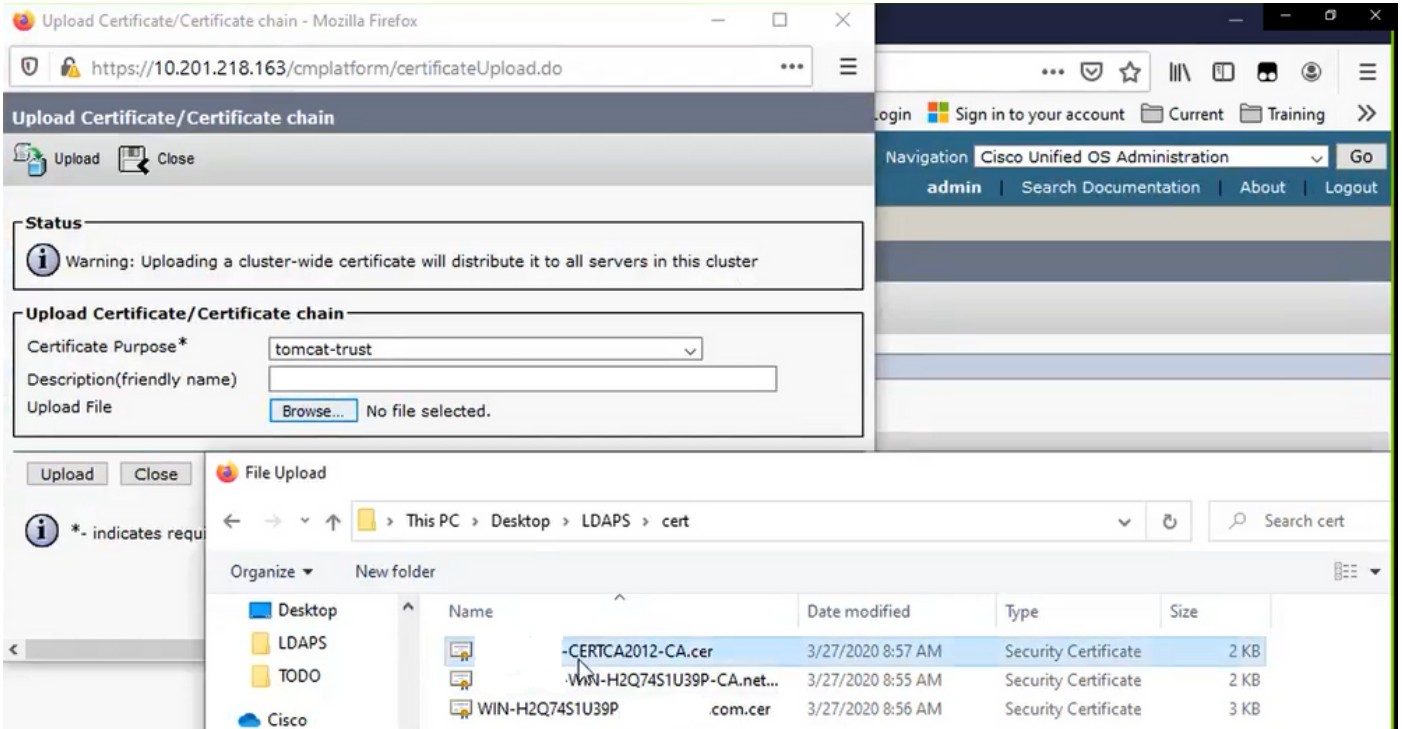
2단계. LDAPS 서버 인증서의 일부인 루트 및 중간 인증서를 가져오고 이를 각 CUCM 및 IM/P 게시자 노드에 tomcat-trust 인증서로, CUCM 게시자에 CallManager-trust로 설치합니다.

LDAPS 서버 인증서의 일부인 루트 및 중간 인증서인 <hostname>.<Domain>.cer이 이미지에 표시됩니다.

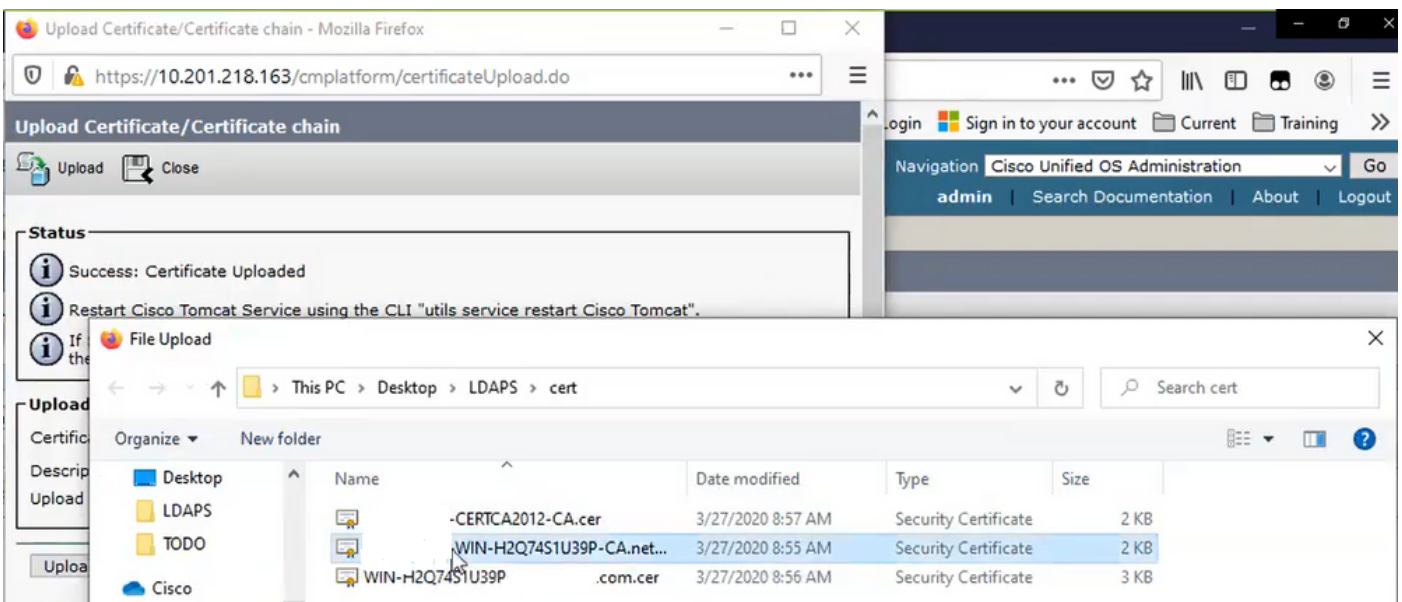


CUCM publisher(CUCM 게시자) Cisco Unified OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리)로 이동합니다. 루트를 tomcat-trust(이미지에 표시된 대로) 및 CallManager-trust(표시되지 않음)로 업로드합니다.





중간을 tomcat-trust(이미지에 표시된 대로) 및 CallManager-trust(표시되지 않음)로 업로드합니다.



**참고:** CUCM 클러스터의 일부인 IM/P 서버가 있는 경우 이러한 인증서를 이 IM/P 서버에 업로드해야 합니다.

**참고:** 대안으로 LDAPS 서버 인증서를 tomcat-trust로 설치할 수 있습니다.

3단계. 클러스터의 각 노드(CUCM 및 IM/P)의 CLI에서 Cisco Tomcat을 다시 시작합니다. 또한 CUCM 클러스터의 경우 게시자 노드에서 Cisco DirSync 서비스가 시작되었는지 확인합니다.

Tomcat 서비스를 재시작하려면 각 노드에 대해 CLI 세션을 열고 그림과 같이 `utils service restart Cisco Tomcat` 명령을 실행해야 합니다.

```

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

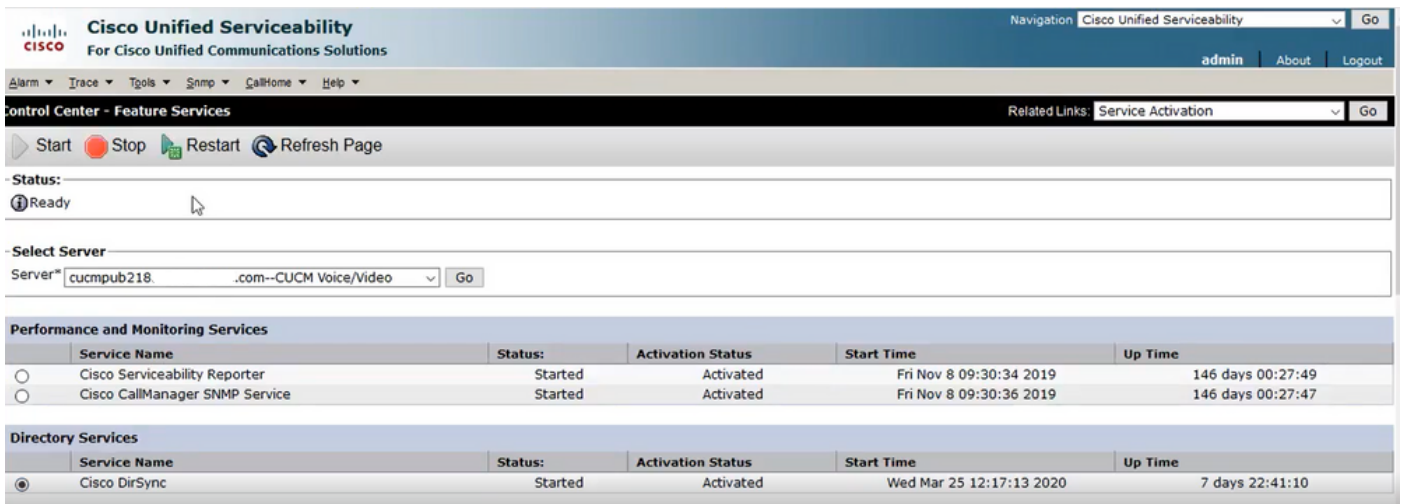
Welcome to the Platform Command Line Interface

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:

```

4단계. CUCM publisher(CUCM 게시자) Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동하여 Cisco DirSync 서비스가 활성화 및 시작되었는지 확인하고(이미지에 표시된 것처럼), 이 서비스가 사용되는 경우(표시되지 않음) 각 노드에서 Cisco CTIManager 서비스를 다시 시작합니다.



## 보안 LDAP 디렉터리 구성

1단계. 포트 636에서 AD에 대한 LDAPS TLS 연결을 활용하려면 CUCM LDAP 디렉토리를 구성합니다.

CUCM Administration(CUCM 관리) > System(시스템) > LDAP Directory(LDAP 디렉토리)로 이동합니다. LDAP 서버 정보에 대한 LDAPS 서버의 FQDN 또는 IP 주소를 입력합니다. 이미지에 표시된

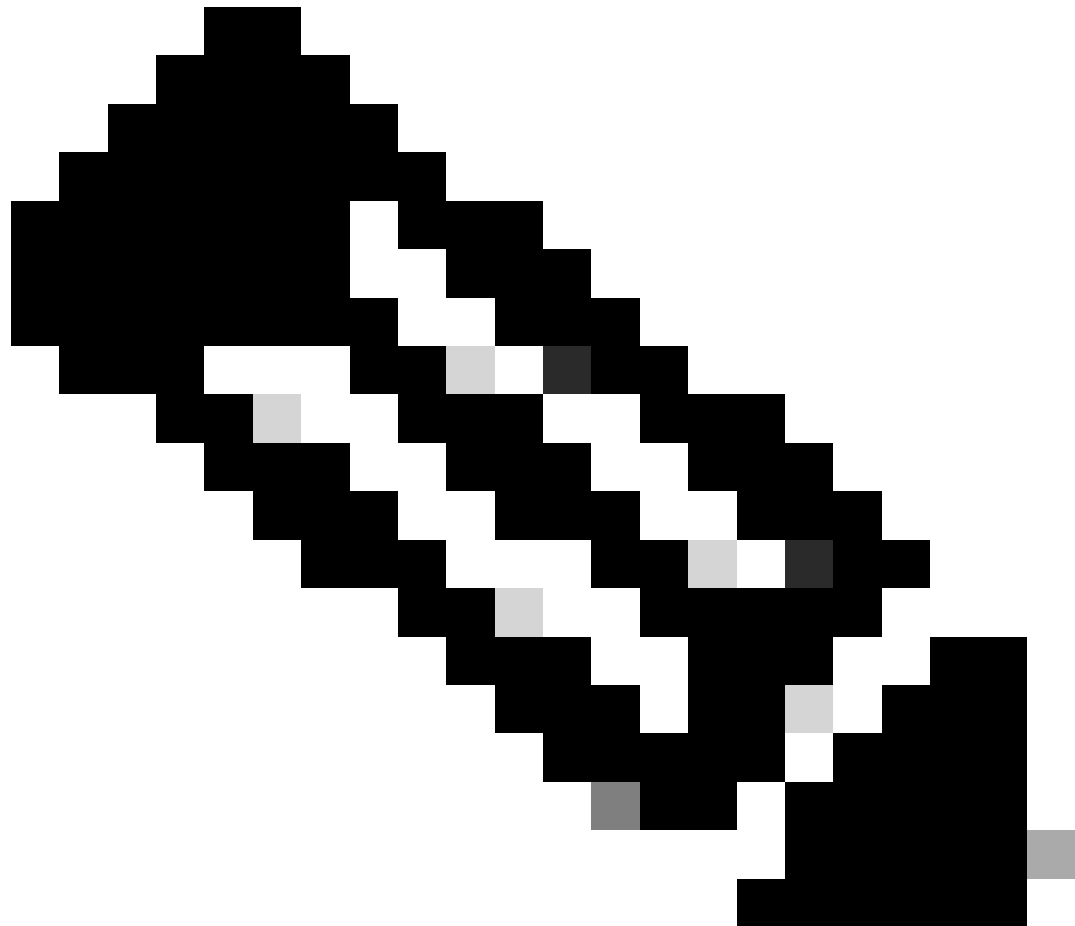


대로 LDAPS 포트 636을 지정하고 Use TLS(TLS 사용) 확인란을 선택합니다.

The screenshot shows the Cisco Unified CM Administration interface for LDAP Directory configuration. The 'LDAP Server Information' section is highlighted, showing the following fields:

- Host Name or IP Address for Server\*: WIN-H2Q7451U39P... .com
- LDAP Port\*: 636
- Use TLS:

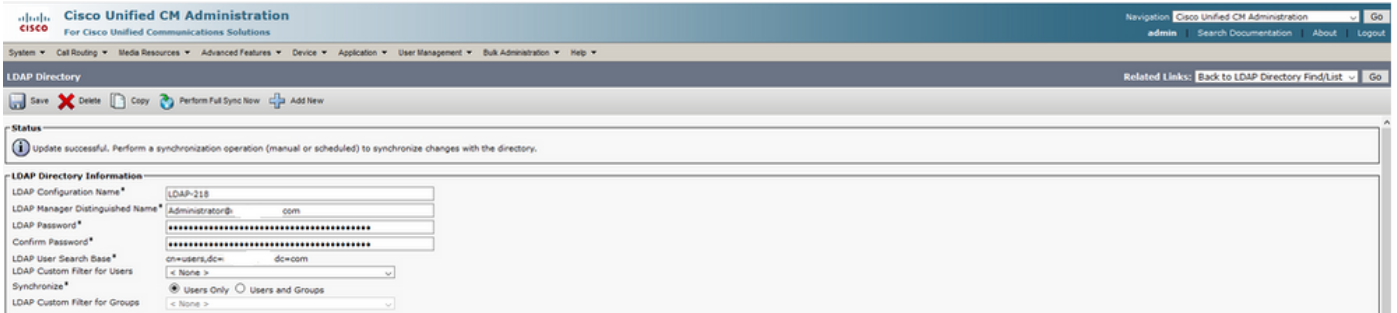
Buttons for 'Add Another Redundant LDAP Server' and 'Add DN Pool' are also visible.



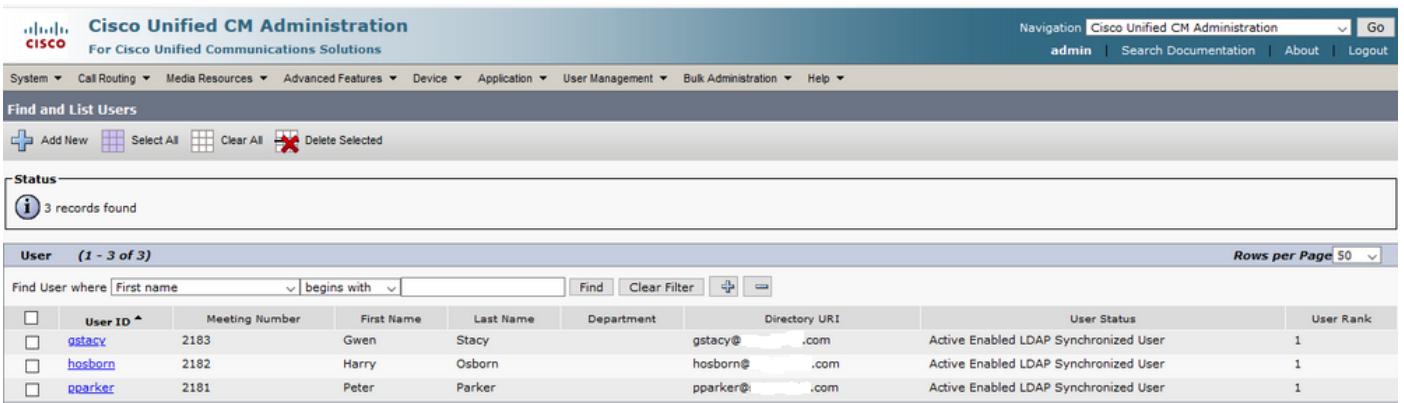
참고: 기본적으로 LDAP 서버 정보에 구성된 버전 10.5(2)SU2 및 9.1(2)SU3 FQDN을 인증

서의 일반 이름에 대해 확인한 후, FQDN 대신 IP 주소를 사용하는 경우 ldap config ipaddr 명령을 실행하여 FQDN의 CN 확인 적용을 중지합니다.

2단계. LDAPS에 대한 컨피그레이션 변경을 완료하려면 다음 이미지에 표시된 대로 Perform Full Sync Now(지금 전체 동기화 수행)를 클릭합니다.



3단계. CUCM Administration(CUCM 관리) > User Management(사용자 관리) > End User(최종 사용자)로 이동하고 이미지에 표시된 대로 최종 사용자가 있는지 확인합니다.



4단계. 사용자 로그인에 성공적인지 확인하기 위해 ccmuser 페이지(<https://<cucm pub>/ccmuser>의 ip 주소)로 이동합니다.

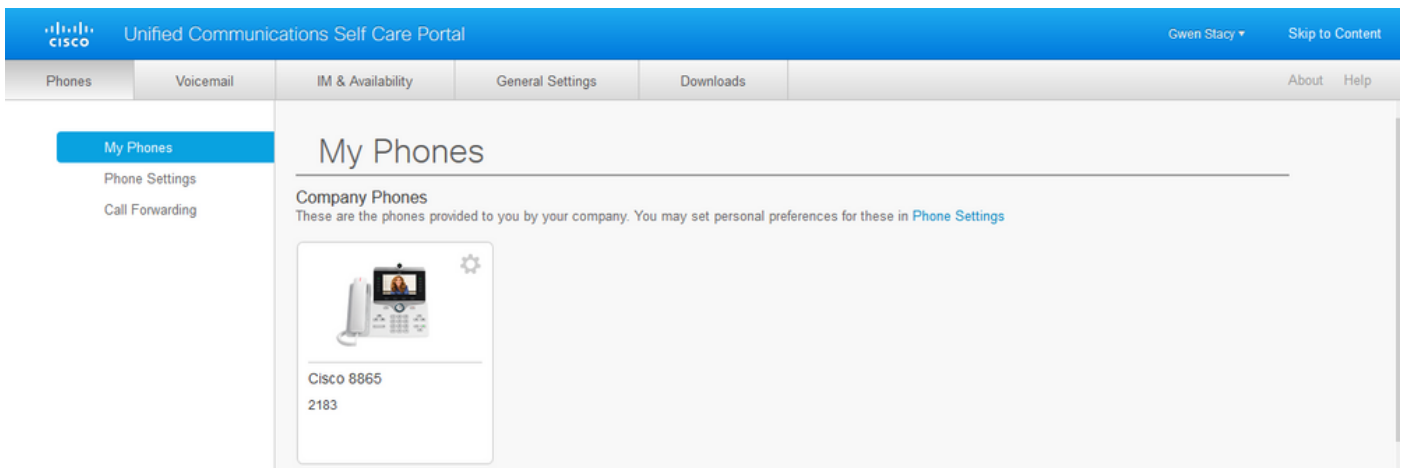
CUCM 버전 12.0.1의 ccmuser 페이지는 다음과 같습니다.

# Cisco Unified Communications Self Care Portal

Username
Password

Sign In

사용자는 그림과 같이 LDAP 자격 증명을 입력한 후 성공적으로 로그인할 수 있습니다.



## 보안 LDAP 인증 구성

포트 3269에서 AD에 대한 LDAPS TLS 연결을 활용하려면 CUCM LDAP 인증을 구성합니다.

CUCM Administration(CUCM 관리) > System(시스템) > LDAP Authentication(LDAP 인증)으로 이동합니다. LDAP 서버 정보에 대한 LDAPS 서버의 FQDN을 입력합니다. 이미지에 표시된 대로 LDAPS 포트 3269를 지정하고 Use TLS(TLS 사용) 확인란을 선택합니다.

**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\* .....

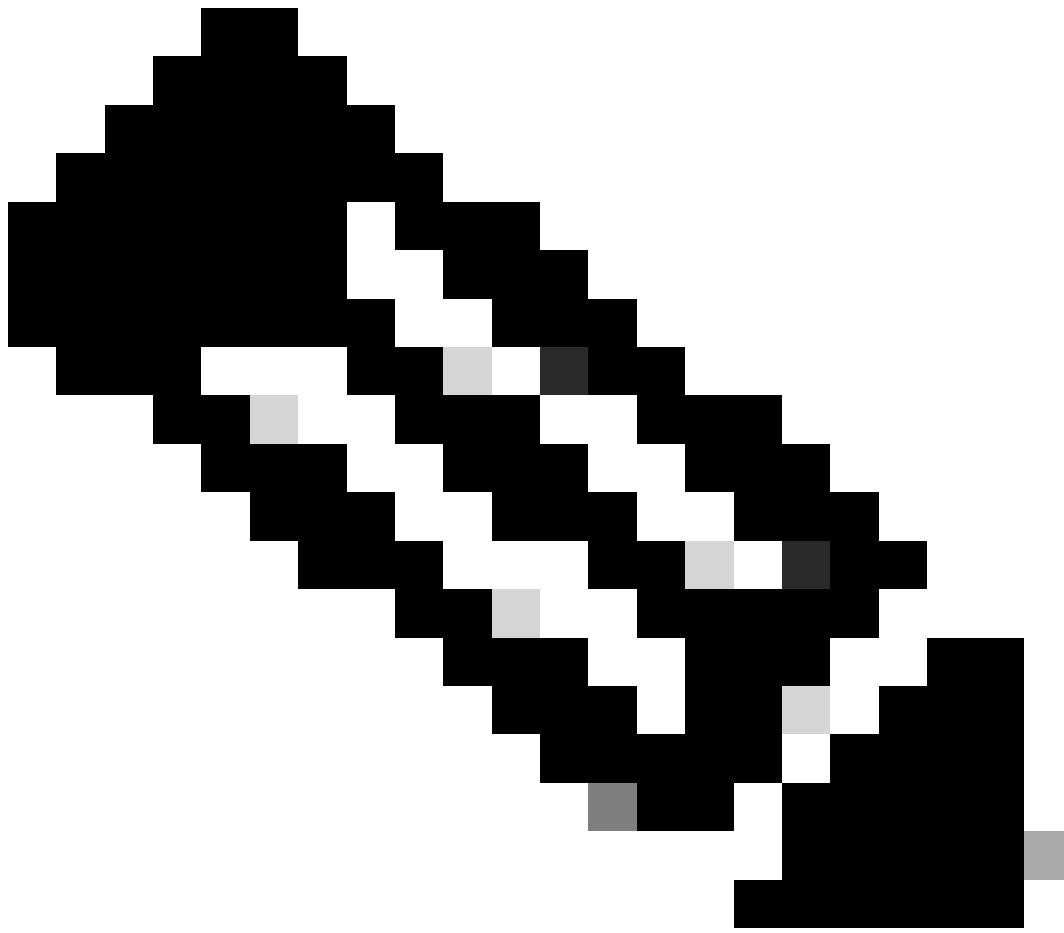
Confirm Password\* .....

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

**LDAP Server Information**

Host Name or IP Address for Server*	LDAP Port*	Use TLS
WIN-H2Q74S1U39P .com	3269	<input checked="" type="checkbox"/>

Add Another Redundant LDAP Server



참고: Jabber 클라이언트가 있는 경우 전역 카탈로그 서버에 대한 보안 연결을 지정하지 않으면 로그인에 대한 Jabber 시간 초과가 발생할 수 있으므로 LDAPS 인증에 포트 3269를 사용하는 것이 좋습니다.

# UC 서비스의 AD에 대한 보안 연결 구성

LDAP를 활용하는 UC 서비스를 보호해야 하는 경우 TLS를 사용하는 포트 636 또는 3269를 활용하도록 이러한 UC 서비스를 구성합니다.

CUCM administration(CUCM 관리) > User Management(사용자 관리) > User Settings(사용자 설정) > UC Service(UC 서비스)로 이동합니다. AD를 가리키는 디렉터리 서비스를 찾습니다. LDAPS 서버의 FQDN을 호스트 이름/IP 주소로 입력합니다. 이미지에 표시된 대로 636 또는 3269와 프로토콜 TLS로 포트를 지정합니다.

The screenshot shows the Cisco Unified CM Administration web interface. The page title is "Cisco Unified CM Administration" with the tagline "For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The current page is "UC Service Configuration".

At the top right, there is a "Navigation" dropdown set to "Cisco Unified CM Administration" and a "Go" button. Below it, there are links for "admin", "Search Documentation", "About", and "Logout".

The main content area has a "UC Service Configuration" header with a "Related Links: Back To Find/List" dropdown and a "Go" button. Below this is a toolbar with icons for "Save", "Delete", "Copy", "Reset", "Apply Config", and "Add New".

The "Status" section shows an "Update successful" message.

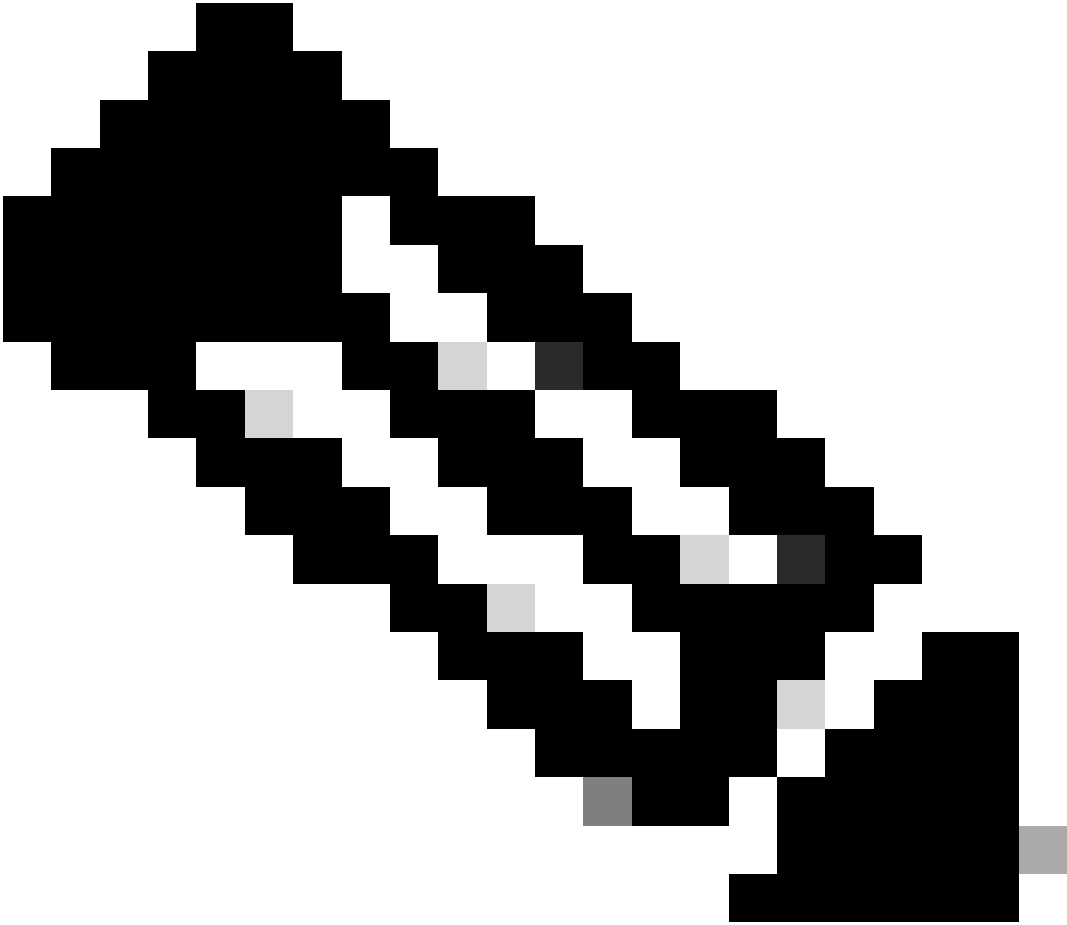
The "UC Service Information" section contains the following fields:

- UC Service Type: Directory
- Product Type\*: Directory
- Name\*: Secure Directory
- Description: (empty)
- Host Name/IP Address\*: WIN-H2Q74S1U39P .com
- Port: 636
- Protocol: TLS

At the bottom of the form, there is another toolbar with buttons for "Save", "Delete", "Copy", "Reset", "Apply Config", and "Add New". A note at the bottom left states: "i \* indicates required item."



---



참고: Jabber 클라이언트가 AD에 대한 LDAPS 연결을 설정할 수 있도록 Jabber 클라이언트 머신의 인증서 관리 신뢰 저장소에 설치된 CUCM에 설치된 tomcat-trust LDAPS 인증서가 Jabber 클라이언트 머신에 있어야 합니다.

---

## 다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

TLS 연결을 위해 LDAP 서버에서 CUCM으로 전송된 실제 LDAPS 인증서/인증서 체인을 확인하려면 CUCM 패킷 캡처에서 LDAPS TLS 인증서를 내보냅니다. 이 링크는 CUCM 패킷 캡처에서 TLS 인증서를 내보내는 방법에 대한 정보를 제공합니다. CUCM 패킷 [캡처에서 TLS 인증서를 내보내는 방법](#)

## 문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

## 관련 정보

- 이 링크를 클릭하면 LDAPS 구성: [Secure LDAP Directory and Authentication\(LDAP 디렉토리 보안 및 인증\) 연습 비디오를 안내하는 비디오에 액세스할 수 있습니다.](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.