Enable Secure Communication Between CMS and CUCM

Contents

Introduction

This document describes how to enable communication between the Cisco Meeting Server (CMS) and the Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CMS version 3.8 and later
- CUCM and IM&P
- Jabber

Components Used

The information in this document is based on these software and hardware versions:

- CMS version 3.8
- CUCM and IM&P 14 SU (3)

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.

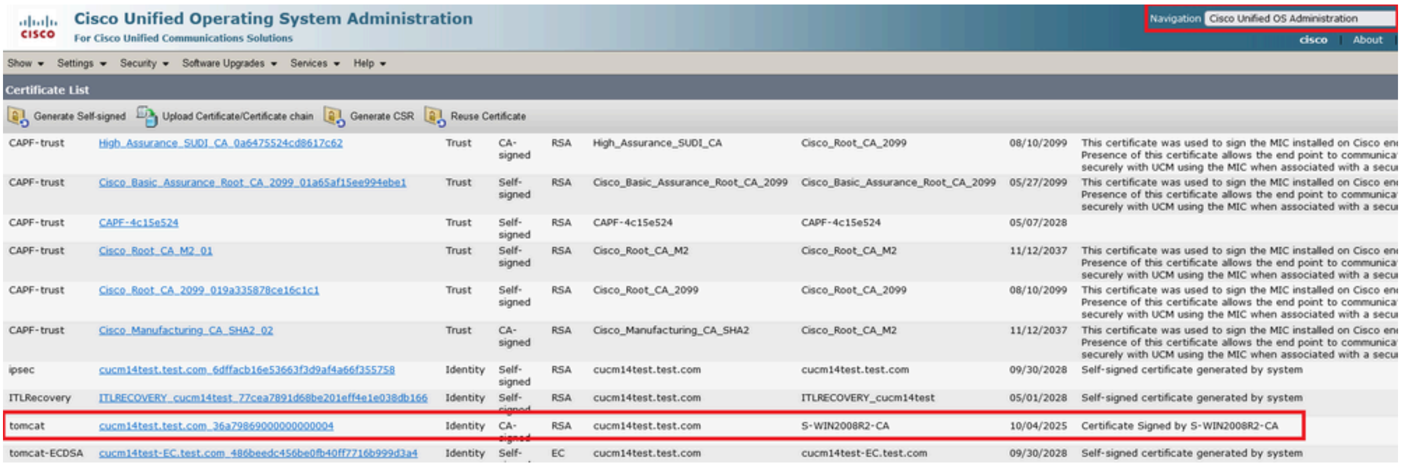
Background Information

This document outlines the process of establishing secure communication between CMS and CUCM for Jabber/Web app presence sharing. It explains the detailed steps for configuring and troubleshooting the updating status of Jabber users during web app meetings on the CMS. The Meeting Server can be configured in order to update the presence status of Jabber users while they are engaged in a Cisco Meeting Server web app meeting.

Configure

Enabling Secure Communication between CMS and CUCM/IMP Server

Log into CUCM on the OS admin page, navigate to Security > Certificate Management, and download the TOMCAT certificate.

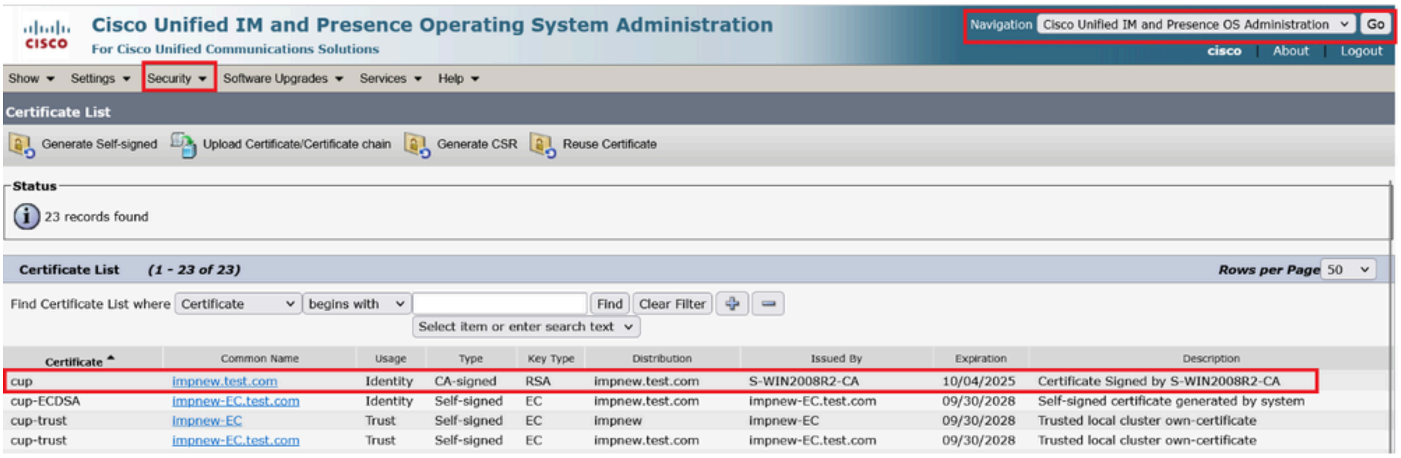


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration
cisco | About
Show Settings Security Software Upgrades Services Help
Certificate List
Generate Self-signed Upload Certificate/Certificate chain Generate CSR Reuse Certificate

CAPF-trust	High_Assurance_SUDI_CA_0a6475524cd8617c62	Trust	CA-signed	RSA	High_Assurance_SUDI_CA	Cisco_Root_CA_2099	08/10/2099	This certificate was used to sign the MIC installed on Cisco en Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAPF-trust	Cisco_Basic_Assurance_Root_CA_2099_01a65af15ee994ebe1	Trust	Self-signed	RSA	Cisco_Basic_Assurance_Root_CA_2099	Cisco_Basic_Assurance_Root_CA_2099	05/27/2099	This certificate was used to sign the MIC installed on Cisco en Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAPF-trust	CAPF-4c15e524	Trust	Self-signed	RSA	CAPF-4c15e524	CAPF-4c15e524	05/07/2028	
CAPF-trust	Cisco_Root_CA_M2_01	Trust	Self-signed	RSA	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco en Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAPF-trust	Cisco_Root_CA_2099_019a335878ce16c1c1	Trust	Self-signed	RSA	Cisco_Root_CA_2099	Cisco_Root_CA_2099	08/10/2099	This certificate was used to sign the MIC installed on Cisco en Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAPF-trust	Cisco_Manufacturing_CA_SHA2_02	Trust	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco en Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
ipsec	cucm14test.test.com_6dffacb16e53663f3d9af4a66f355758	Identity	Self-signed	RSA	cucm14test.test.com	cucm14test.test.com	09/30/2028	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY_cucm14test_77cea7891d68be201eff4e1e038db166	Identity	Self-signed	RSA	cucm14test.test.com	ITLRECOVERY_cucm14test	05/01/2028	Self-signed certificate generated by system
tomcat	cucm14test.test.com_36a79869000000000004	Identity	CA-signed	RSA	cucm14test.test.com	S-WIN2008R2-CA	10/04/2025	Certificate Signed by S-WIN2008R2-CA
tomcat-ECDSA	cucm14test-EC.test.com_486beedc456be0fb40ff7716b999d3a4	Identity	Self-	EC	cucm14test.test.com	cucm14test-EC.test.com	09/30/2028	Self-signed certificate generated by system

CUCM Tomcat Certificate

Log into the Cisco Unified Presence Server (CUPS) on the OS admin page, navigate to Security > Certificate Management, and download the CUPS certificate.



Cisco Unified IM and Presence Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified IM and Presence OS Administration
Go
cisco | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate List
Generate Self-signed Upload Certificate/Certificate chain Generate CSR Reuse Certificate
Status

23 records found

Certificate List (1 - 23 of 23)

Rows per Page 50

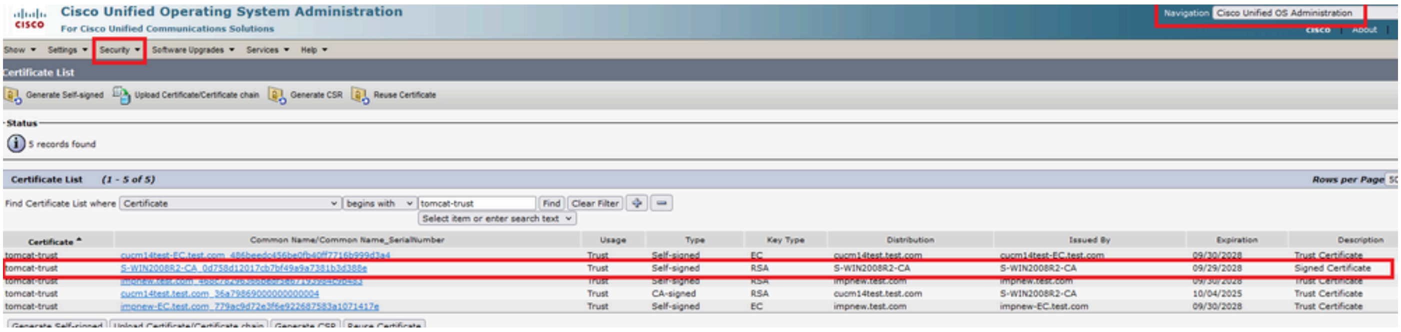
Find Certificate List where Certificate begins with Find Clear Filter

Select item or enter search text

Certificate	Common Name	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
cup	impnew.test.com	Identity	CA-signed	RSA	impnew.test.com	S-WIN2008R2-CA	10/04/2025	Certificate Signed by S-WIN2008R2-CA
cup-ECDSA	impnew-EC.test.com	Identity	Self-signed	EC	impnew.test.com	impnew-EC.test.com	09/30/2028	Self-signed certificate generated by system
cup-trust	impnew-EC	Trust	Self-signed	EC	impnew	impnew-EC	09/30/2028	Trusted local cluster own-certificate
cup-trust	impnew-EC.test.com	Trust	Self-signed	EC	impnew.test.com	impnew-EC.test.com	09/30/2028	Trusted local cluster own-certificate

Presence CUPS certificate

Download the ROOT CA Certificate which signed the Tomcat and Cup certificate.


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration
cisco | About |
Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Reuse Certificate

Certificate List

Status

5 records found

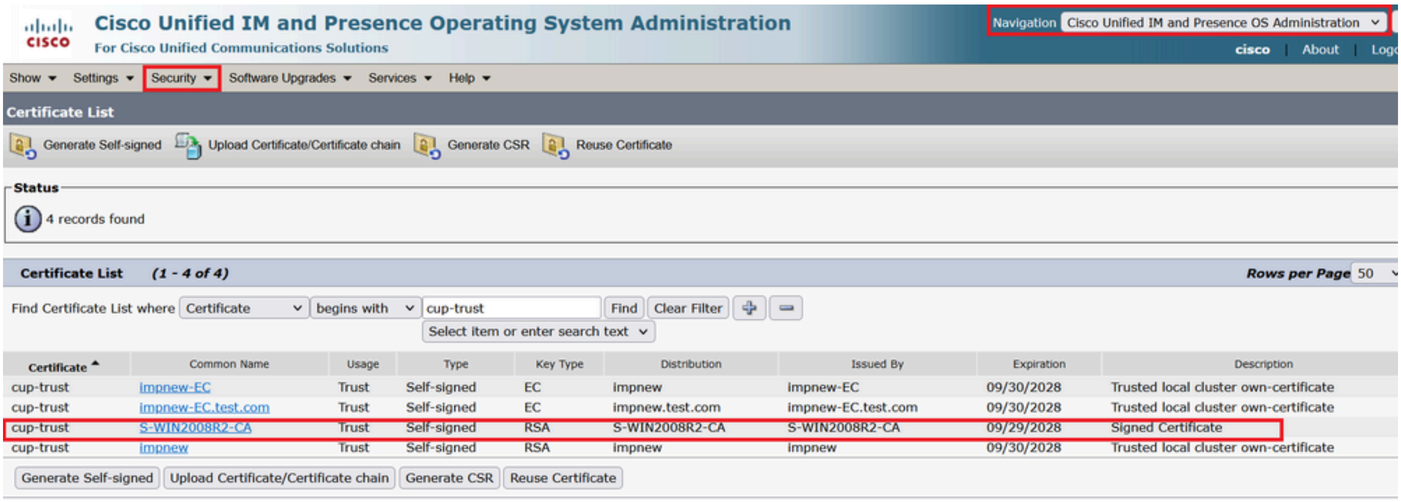
Certificate List (1 - 5 of 5) Rows per Page 50

Find Certificate List where Certificate begins with tomcat-trust Find Clear Filter
Select item or enter search text

Certificate ▲	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat-trust	cucm14test-EC.test.com_486beedc456be0fb40ff7716b999d3a4	Trust	Self-signed	EC	cucm14test.test.com	cucm14test-EC.test.com	09/30/2028	Trust Certificate
tomcat-trust	S-WIN2008R2-CA_0d758d12017cb7bf49a9a7381b3d388e	Trust	Self-signed	RSA	S-WIN2008R2-CA	S-WIN2008R2-CA	09/29/2028	Signed Certificate
tomcat-trust	impnew.test.com_[illegible]	Trust	Self-signed	RSA	impnew.test.com	impnew.test.com	09/30/2028	Trust Certificate
tomcat-trust	cucm14test.test.com_36a79869000000000004	Trust	CA-signed	RSA	cucm14test.test.com	S-WIN2008R2-CA	10/04/2025	Trust Certificate
tomcat-trust	impnew-EC.test.com_779ac9d72e3f6e922687583a1071417e	Trust	Self-signed	EC	impnew.test.com	impnew-EC.test.com	09/30/2028	Trust Certificate

Generate Self-signed | Upload Certificate/Certificate chain | Generate CSR | Reuse Certificate

Root certificate of Tomcat


Cisco Unified IM and Presence Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified IM and Presence OS Administration
cisco | About | Logo
Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Reuse Certificate

Certificate List

Status

4 records found

Certificate List (1 - 4 of 4) Rows per Page 50

Find Certificate List where Certificate begins with cup-trust Find Clear Filter
Select item or enter search text

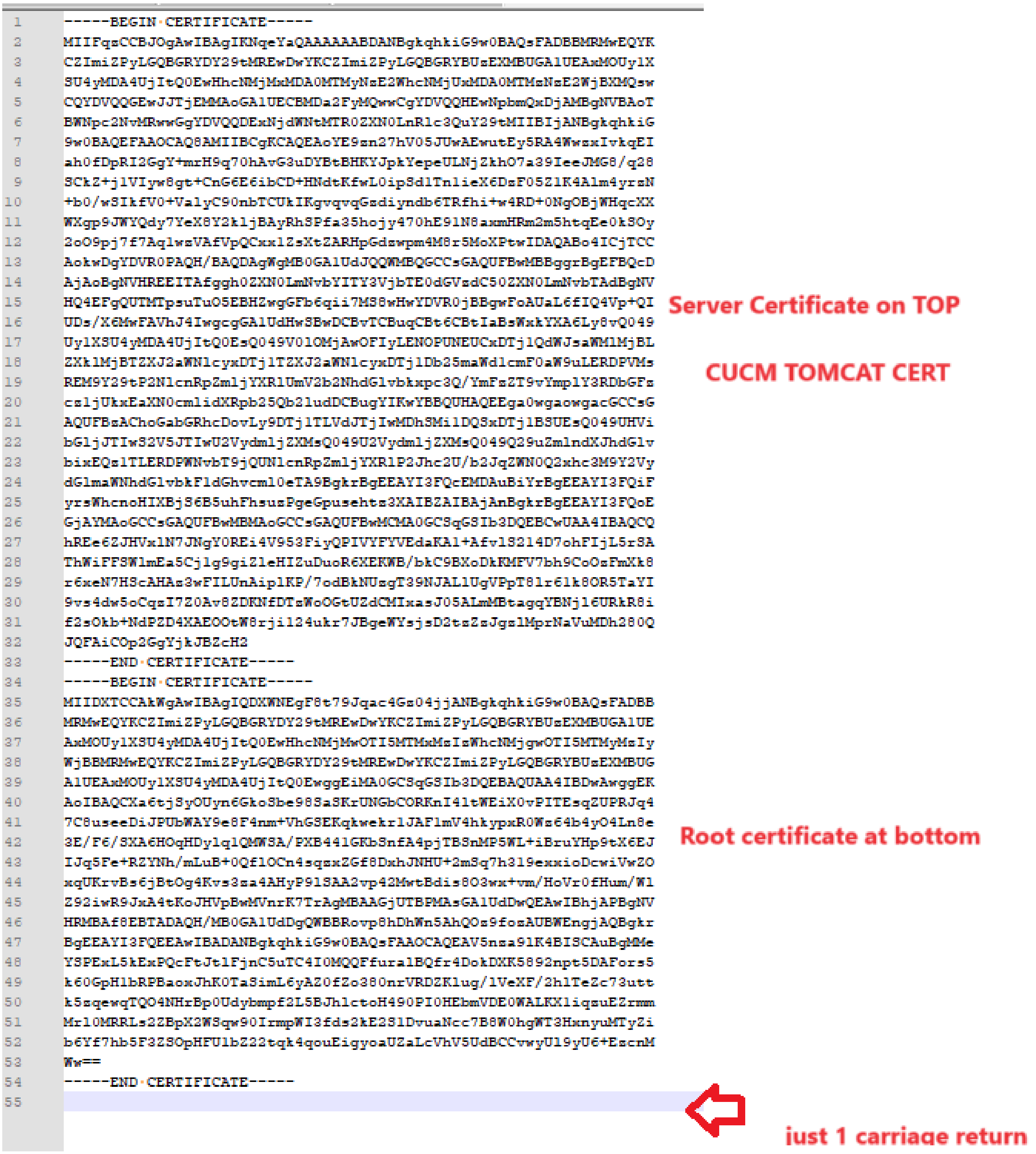
Certificate ▲	Common Name	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
cup-trust	impnew-EC	Trust	Self-signed	EC	impnew	impnew-EC	09/30/2028	Trusted local cluster own-certificate
cup-trust	impnew-EC.test.com	Trust	Self-signed	EC	impnew.test.com	impnew-EC.test.com	09/30/2028	Trusted local cluster own-certificate
cup-trust	S-WIN2008R2-CA	Trust	Self-signed	RSA	S-WIN2008R2-CA	S-WIN2008R2-CA	09/29/2028	Signed Certificate
cup-trust	impnew	Trust	Self-signed	RSA	impnew	impnew	09/30/2028	Trusted local cluster own-certificate

Generate Self-signed | Upload Certificate/Certificate chain | Generate CSR | Reuse Certificate

Root certificate for CUPS

Create a certificate bundle of CUCM certificates. A bundle certificate means, placing the Server certificate on top, the intermediate certificate (any) in the middle, and the ROOT certificate at the bottom, followed by one (1) carriage return.

Here is a sample for the BUNDLE certificate:



```
-----BEGIN CERTIFICATE-----
MIIFqzCCBJOgAwIBAgIKNqeYaQAAAAAABDANBgkqhkiG9w0BAQsFADBBMRMwEQYK
CZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUGA1UEAxMOUy1X
SU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMyNzE2WhcNMjUxMDA0MTMzNzE2WjBXMQsw
CQYDVQQGEwJJTjEMMAoGA1UECBMDa2FyMQwwCgYDVQQHEwNpbmQxDjAMBgNVBAoT
BWNpc2NvMRwwGgYDVQQDExNjdWNtMTR0ZXN0LnRlc3QuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoYE9zn27hV05JUwAEwutEy5RA4WwzxIvkqEI
ah0fDpRI2GgY+mrH9q70hAvG3uDYBtBHKYJpkYepeULNjZkhO7a39IeeJMG8/q28
SCkZ+j1VIyw8gt+CnG6E6ibCD+HNdtKfwL0ipSd1TnlieX6DzF05Z1K4Alm4yrzN
+b0/wSIkfV0+ValyC90nbTCUkIKgvqvqGzdiyndb6TRfhi+w4RD+0NgOBjWHqcXX
WXgp9JWYQdy7YeX8Y2kljBAyRhSPfa35hojy470hE91N8axmHRm2m5htqEe0kSOy
2oO9pj7f7AqlwzVAfVpQCxxlZsXtZARHpGdzwpm4M8r5MoXPtwIDAQABo4ICjTCC
AokwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
AjAoBgNVHREEITAfggh0ZXN0LmNvbYITY3VjbTE0dGVzdC50ZXN0LmNvbTAdBgNV
HQ4EFgQUTMTpsuTuO5EBHZwgGFb6qii7M38wHwYDVR0jBBgwFoAUaL6fIQ4Vp+QI
UDs/X6MwFAVhJ4IwgcgGA1UdHwSBwDCBvTCBuqCBt6CBtIaBsWxkYXA6Ly8vQ049
Uy1XSU4yMDA4UjItQ0EsQ049V01OMjAwOFIyLENOPUNEUCxDTj1QdWJsaWM1MjBL
ZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPVMs
REM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz
czljUkxEaXN0cmlidXRpb25Qb2ludDCBugYIKwYBBQUHAQEEga0wgaowgacGCCsG
AQUFBzAChoGabGRhcDovLy9DTj1TLVdJTjIwMDhSMi1DQSxDTj1BSUEsQ049UHVi
bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
bixEQz1TLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2Vy
dGlmaWNhdGlvbkF1dGhvcml0eTA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiF
yrsWhcnoHIXBjS6B5uhFhsuzPgeGpusehtz3XAIBZAIBAjAnBgkrBgEEAYI3FQoE
GjAYMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4IBAQCQ
hREe6ZJHVxlN7JNgY0REi4V953FiyQPIVYFYVEdaKA1+Afvl3214D7ohFIjL5rSA
ThWiFFSWlmEa5Cjlg9giZleHIZuDuoR6XEKWB/bkC9BXoDkKMFV7bh9CoOzFmXk8
r6xeN7HScAHAz3wFILUnAiplKP/7odBkNUzgT39NJAL1UgVPpT8lr6lk8OR5TaYI
9vs4dw5oCqzI7Z0Av8ZDKNfDTzWoOGtUZdCMIxasJ05ALmMBtaggYBNj16URkR8i
f2sOkb+NdPZD4XAEOOtW8rji124ukr7JBgeWYsjsD2tsZsJgz1MprNaVuMDh280Q
JQFAiCOp2GgYjkJBZcH2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIQDXWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADBB
MRMwEQYKCZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUGA1UE
AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjMwOTI5MTMxMzIzWhcNMjgwOTI5MTMyMzIy
WjBBMRMwEQYKCZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUG
A1UEAxMOUy1XSU4yMDA4UjItQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCXa6tjSyOUyn6GkoSbe98SaSKrUNGbCORKnI41tWEiX0vPITEsqZUPRJq4
7C8uzeeDiJPUbWAY9e8F4nm+VhGSEKqkwekr1JAFlmV4hkypxR0Wz64b4yO4Ln8e
3E/F6/SXA6HOqHDy1q1QMWSA/PXB441GKbSnfA4pjTBSnMP5WL+iBruYHp9tX6EJ
IJq5Fe+RZYNh/mLuB+0Qf1OCn4sqzxZGf8DxhJNHU+2mSq7h319exxioDcwiVwZO
xqUKrvBs6jBtOg4Kvs3za4AHyP91SAA2vp42MwtBdis8O3wx+vm/HoVr0fHum/W1
Z92iwR9JxA4tKoJHVpBwMVnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBRovp8hDhWn5AhQOz9fozAUBWEngjAQBgkr
BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAV5nza91K4BISCAuBgMMe
YSPExL5kExPQcFtJtlFjnC5uTC4I0MQQFfuralBQfr4DokDXK5892npt5DAFors5
k60GpH1bRPBaoxJhK0TaSimL6yAZ0fZo380nrVRDZKlug/lVeXF/2hlTeZc73utt
k5zqewqTQO4NHrBp0UdybmpfZL5BJhlctoH490PI0HEbmVDE0WALKXliqzuEZrmm
Mrl0MRRLs22BpX2WSqw90IrmpWI3fds2kE231DvuaNcc7B8W0hgWT3HxnyuMTyZi
b6Yf7hb5F3ZSOpHFUlbZ22tqk4qouEigyoaUZaLcVhV5UdBCCvwyUl9yU6+EscnM
Ww==
-----END CERTIFICATE-----
```

Server Certificate on TOP

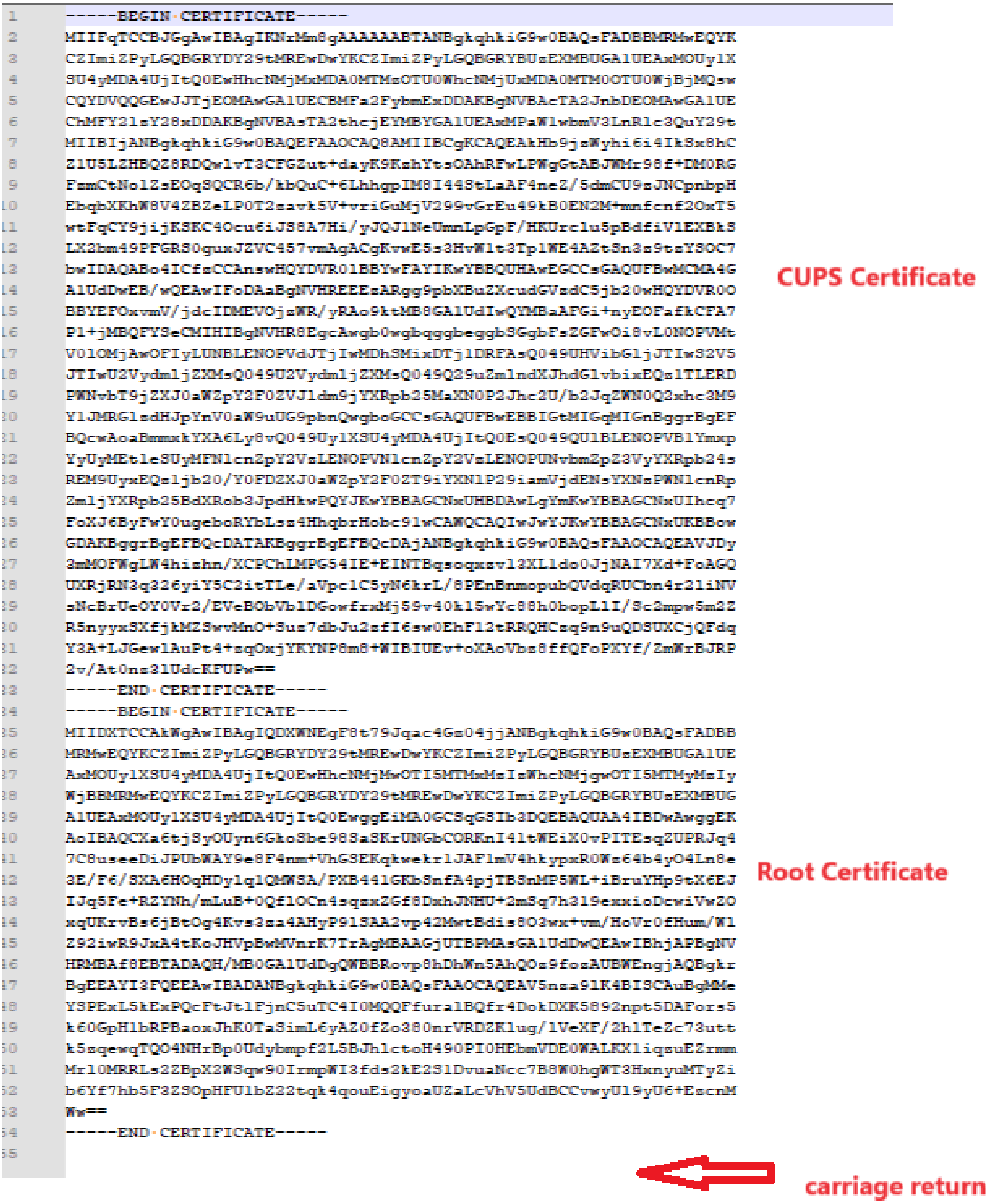
CUCM TOMCAT CERT

Root certificate at bottom

just 1 carriage return

Tomcat certificate bundle

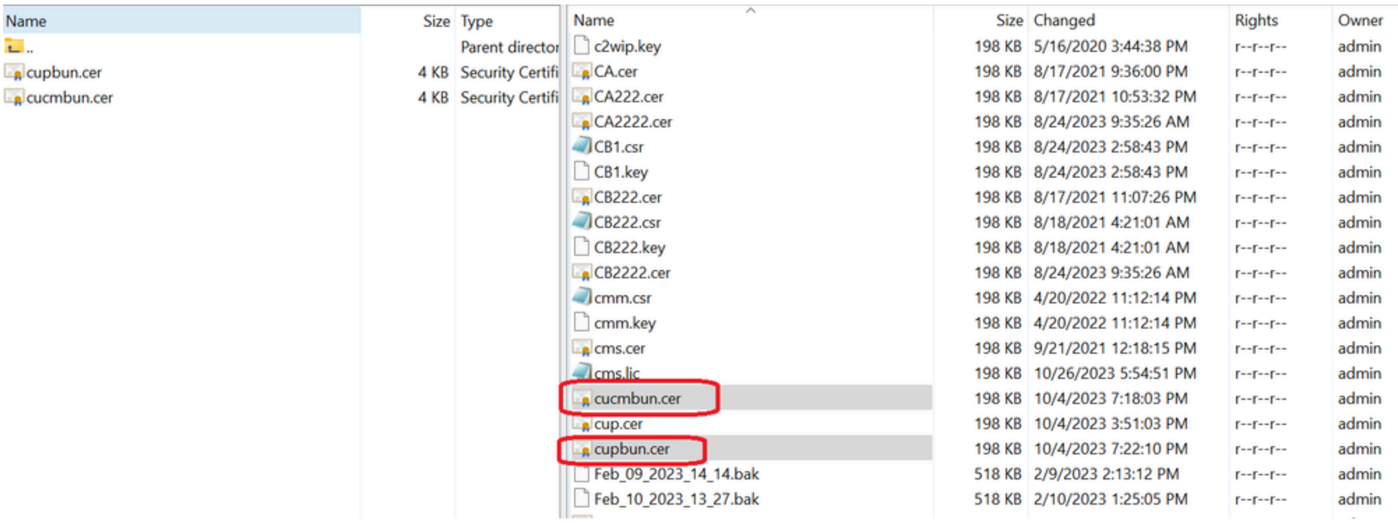
Create a certificate bundle of CUPS certificates. A Bundle certificate means, placing the Server certificate on top, the intermediate certificate (any) in the middle, and the ROOT certificate at the bottom, followed by one (1) carriage return.



```
-----BEGIN CERTIFICATE-----
MIIFqTCCBJGgAwIBAgIKNrMm8gAAAAAABTANBgkqhkiG9w0BAQsFADBBMRMwEQYK
CZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUGA1UEAxMOUy1X
SU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMzOTU0WhcNMjUxMDA0MTM0OTU0WjBjMQsw
CQYDVQQGEwJJTjEOMAwGA1UECBMFa2FybmExDDAKBgNVBAcTA2JnbDEOMAwGA1UE
ChMFY21zY28xDDAKBgNVBAsTA2thcjEYMBYGA1UEAxMPaW1wbmV3LnRlc3QuY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkHb9jzWyhi6i4Ik3x8hC
Z1U5LZHBQZ8RDQwlvT3CFGZut+dayK9KzhYtsOAhRFwLPWgGtABJWMr98f+DM0RG
FsmCtNo1ZsEOq3QCR6b/kbQuC+6LhhgpIM8I443tLaAF4neZ/5dmCU9zJNCpnbpH
EbqbXKhW8V42BZeLP0T2savk5V+vriGuMjV299vGrEu49kB0EN2M+mnfcnf2OxT5
wtFqCY9jijKSKC4Ocu6iJ38A7Hi/yJQJ1NeUmnLpGpF/HKUrclu5pBdfiV1EXBk3
LX2bm49PFGR30guxJZVC457vmAgACgKvwE5s3HvW1t3Tp1WE4AZt3n3s9tsYSOC7
bwIDAQABo4ICfzCCAnswHQYDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMA4G
A1UdDwEB/wQEAwIFoDAaBgNVHREEEzARgg9pbXBuZXcudGVzdC5jb20wHQYDVR0O
BBYEFOxvmV/jdcIDMEVOjzWR/yRAo9ktMB8GA1UdIwQYMBaAFGi+nyEOFafkCFA7
P1+jMBQFY3eCMIHIBgNVHR8EgcAwgb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPVMt
V01OMjAwOFIyLUNBLENOPVdJTjIwMDh3MixDTj1DRFAsQ049UHVibGljJTIwS2V5
JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1TLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnQwgboGCCsGAQUFBwEBBIGtMIGqMIGnBggrBgEF
BQcwAoaBmmxkYXA6Ly8vQ049Uy1XSU4yMDA4UjItQ0EsQ049QU1BLENOPVB1Ymxp
YyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cm2pY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9UyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRp
ZmljYXRpb25BdXRob3JpdHkwPQYJKwYBBAGCNxUHBDAwLgYmKwYBBAGCNxUIhcq7
FoXJ6ByFwY0ugeboRYbLss4HhqbrHobc91wCAWQCAQIwJwYJKwYBBAGCNxUKBBow
GDAKBggrBgEFBQcDATAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAVJDy
3mMOFWgLW4hishn/XCPChLMPG54IE+EINTBqsoqxsv13XL1do0JjNAI7Xd+FoAGQ
UXRjRN3q326yiY5C2itTLe/aVpc1C5yN6krL/8PEnBnmopubQVdqRUCbm4r21iNV
sNcBrUeOY0Vr2/EVeBObVb1DGowfrxMj59v40k15wYc88h0bopL1I/Sc2mpw5m2Z
R5nyyx3XfjkMZ3wvMnO+3uz7dbJu2sfI6sw0EhF12tRRQHCzq9m9uQDSUXCjQFdq
Y3A+LJGew1AuPt4+sqOxjYKYNP8m8+WIBIUEv+oXAoVbs8ffQFoPXYf/ZmWrBJRP
2v/At0ns31UdcKFUPw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIQDXWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADBB
MRMwEQYKCZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUGA1UE
AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjMwOTI5MTMxMzIzWhcNMjgwOTI5MTMyMzIy
WjBBMRMwEQYKCZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUG
A1UEAxMOUy1XSU4yMDA4UjItQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCXa6tj3yOUyn6GkoSbe983aSKrUNGbCORKnI41tWEiX0vPITEsqZUPRJq4
7C8useeDiJPUbWAY9e8F4nm+VhG3EKqkwekr1JAF1mV4hkypxR0Wz64b4yO4Ln8e
3E/F6/SXA6HOqHDy1q1QMWSA/PXB441GKb3nfA4pjTB3nMP5WL+iBruYHp9tX6EJ
IJq5Fe+RZYNh/mLuB+0Qf1OCm4sqsxZGf8DxhJNHU+2m3q7h319exxioDcwiVwZO
xqUKrvBs6jBtOg4Kvs3za4AHyP913AA2vp42MwtBdis8O3wx+vm/HoVr0fHum/W1
Z92iwR9JxA4tKoJHVpBwMVnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBRovp8hDhWn5AhQOz9fozAUBWEngjAQBgkr
BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAV5nza91K4BI3CAuBgMMe
Y3PExL5kExPQcFtJt1FjnC5uTC4I0MQQFfura1BQfr4DokDXK5892npt5DAFors5
k60GpH1bRPBaoxJhK0TaSimL6yAZ0fZo380nrVRDZKlug/1VeXF/2h1TeZc73utt
k5sqewqTQO4NHrBp0UdybmpfZL5BJh1ctoH490PI0HEbmVDE0WALKX1iqzuEZrmm
Mr10MRRLs2ZBpX2W3qw90IrmpWI3fds2kE231DvuaNcc7B8W0hgWT3HxnyuMTyZi
b6Yf7hb5F3Z3OpHFU1bZ22tqk4qouEigyoaUZaLcVhV5UdBCCvwyU19yU6+EzcnM
Ww==
-----END CERTIFICATE-----
```

CUPS certificate bundle

Push the bundle certificates created earlier to the CMS server via WinSCP.

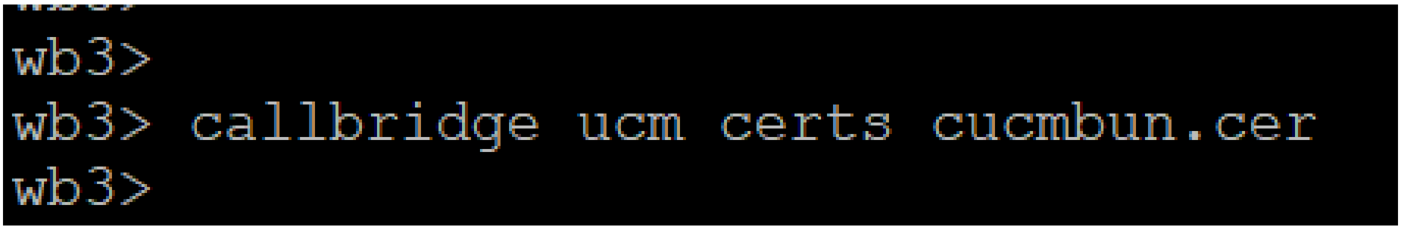


Name	Size	Type
..		Parent director
cupbun.cer	4 KB	Security Certifi
cucmbun.cer	4 KB	Security Certifi

Name	Size	Changed	Rights	Owner
c2wip.key	198 KB	5/16/2020 3:44:38 PM	r--r--r--	admin
CA.cer	198 KB	8/17/2021 9:36:00 PM	r--r--r--	admin
CA222.cer	198 KB	8/17/2021 10:53:32 PM	r--r--r--	admin
CA2222.cer	198 KB	8/24/2023 9:35:26 AM	r--r--r--	admin
CB1.csr	198 KB	8/24/2023 2:58:43 PM	r--r--r--	admin
CB1.key	198 KB	8/24/2023 2:58:43 PM	r--r--r--	admin
CB222.cer	198 KB	8/17/2021 11:07:26 PM	r--r--r--	admin
CB222.csr	198 KB	8/18/2021 4:21:01 AM	r--r--r--	admin
CB222.key	198 KB	8/18/2021 4:21:01 AM	r--r--r--	admin
CB2222.cer	198 KB	8/24/2023 9:35:26 AM	r--r--r--	admin
cmm.csr	198 KB	4/20/2022 11:12:14 PM	r--r--r--	admin
cmm.key	198 KB	4/20/2022 11:12:14 PM	r--r--r--	admin
cms.cer	198 KB	9/21/2021 12:18:15 PM	r--r--r--	admin
cms.lic	198 KB	10/26/2023 5:54:51 PM	r--r--r--	admin
cucmbun.cer	198 KB	10/4/2023 7:18:03 PM	r--r--r--	admin
cup.cer	198 KB	10/4/2023 3:51:03 PM	r--r--r--	admin
cupbun.cer	198 KB	10/4/2023 7:22:10 PM	r--r--r--	admin
Feb_09_2023_14_14.bak	518 KB	2/9/2023 2:13:12 PM	r--r--r--	admin
Feb_10_2023_13_27.bak	518 KB	2/10/2023 1:25:05 PM	r--r--r--	admin

Copying Certificates Bundle to CMS

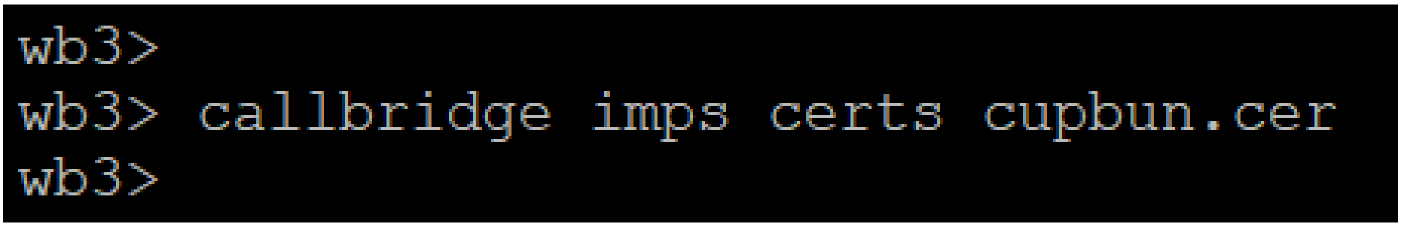
Assign TOMCAT bundle certificate on Callbridge using callbridge ucm certs <cert-bundle>.



```
wb3>
wb3> callbridge ucm certs cucmbun.cer
wb3>
```

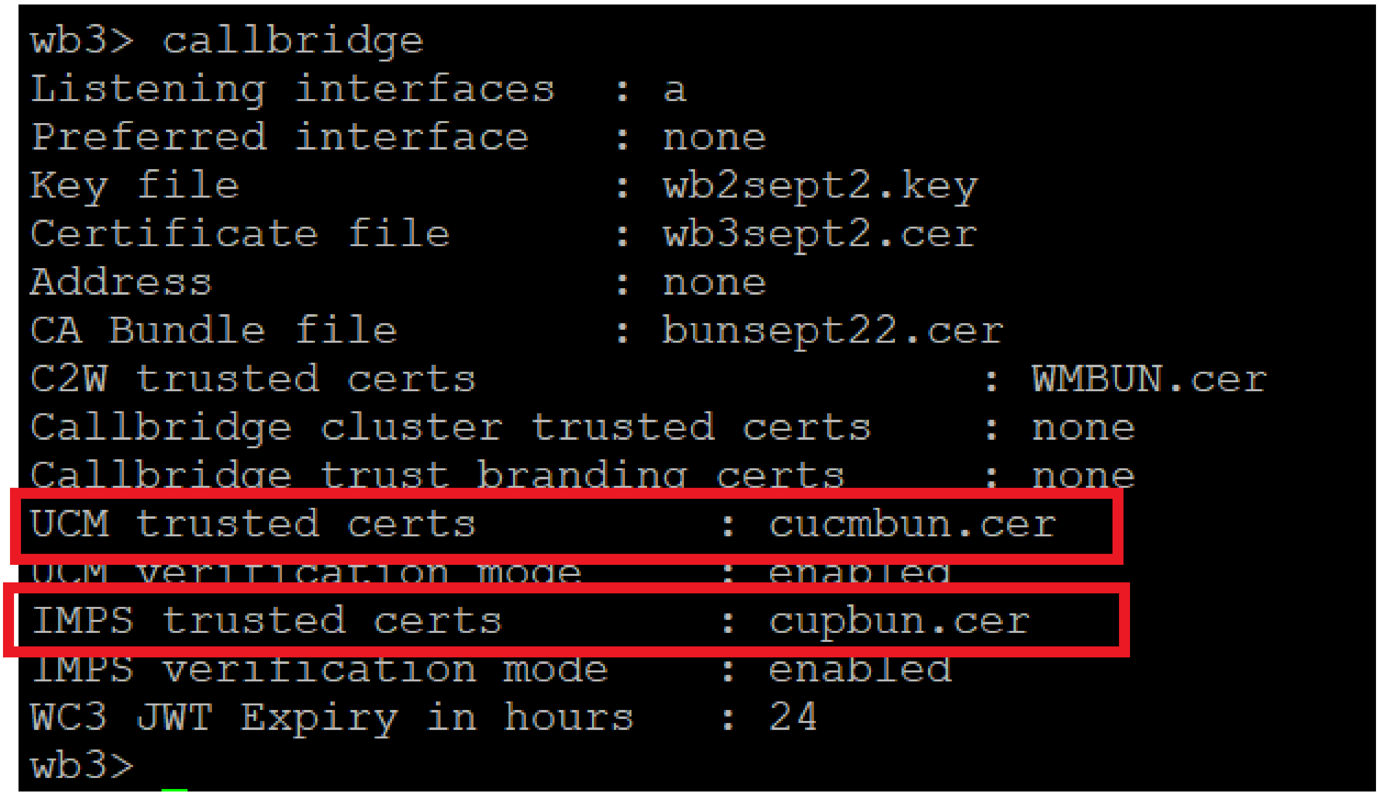
Callbrigde cert trust

Assign CUP server bundle certificate on Callbridge using callbridge imps certs <cert-bundle>.



```
wb3>
wb3> callbridge imps certs cupbun.cer
wb3>
```

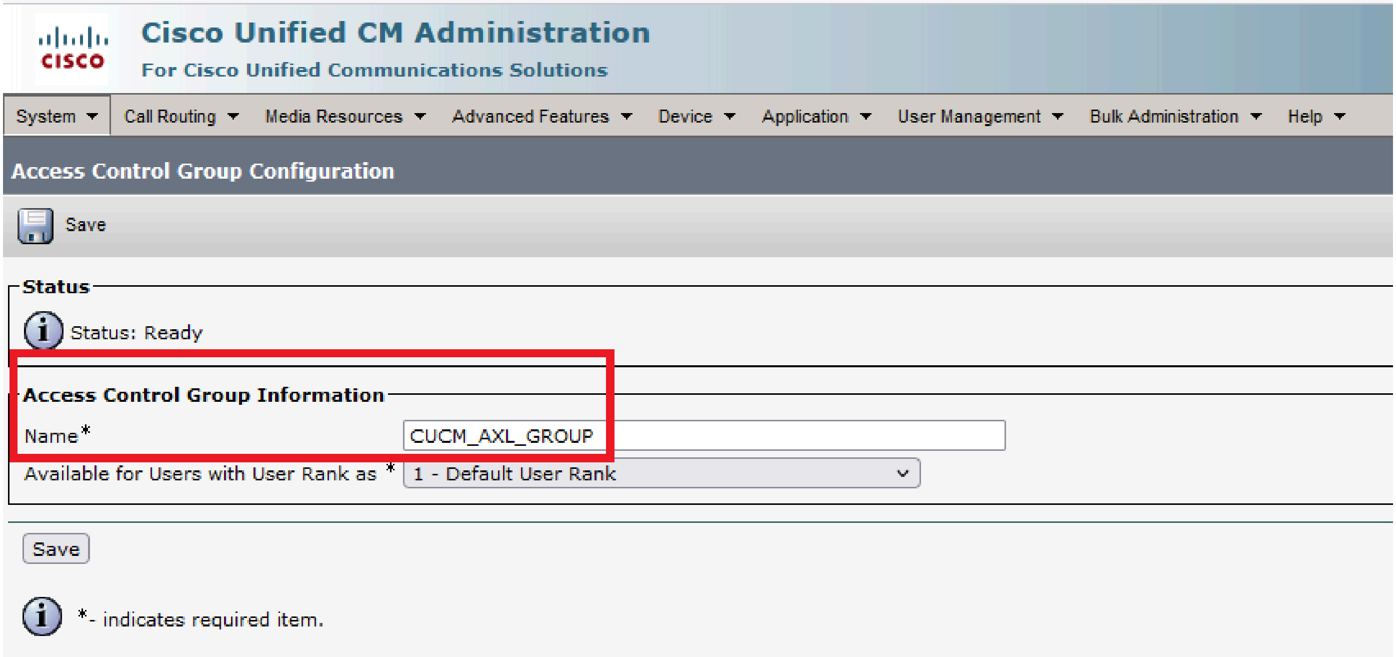
Run thecallbridge command in order to check if the certificate bundles are assigned.



```
wb3> callbridge
Listening interfaces     : a
Preferred interface      : none
Key file                 : wb2sept2.key
Certificate file         : wb3sept2.cer
Address                  : none
CA Bundle file           : bunsept22.cer
C2W trusted certs                             : WMBUN.cer
Callbridge cluster trusted certs              : none
Callbridge trust branding certs               : none
UCM trusted certs                : cucmbun.cer
UCM verification mode            : enabled
IMPS trusted certs               : cupbun.cer
IMPS verification mode           : enabled
WC3 JWT Expiry in hours          : 24
wb3>
```

Callbridge trust cert check

Log into CUCM as CM Administrator, navigate to User Management > User Settings > Access Control Group, click Add New and create an Access control Group CUCM_AXL_Group.



Access Control Group Configuration

Save

Status

Status: Ready

Access Control Group Information

Name* CUCM_AXL_GROUP

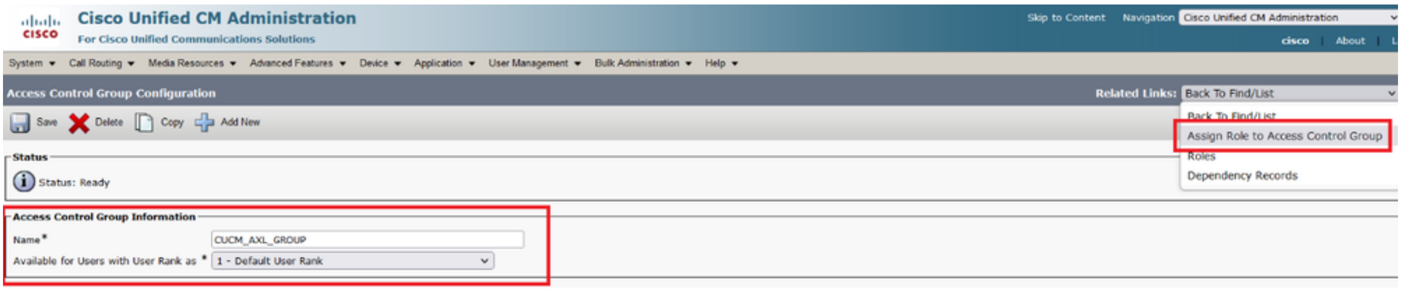
Available for Users with User Rank as * 1 - Default User Rank

Save

*- indicates required item.

Creating AXL group

Assign the role Standard AXL API Access to the Access Control Group created earlier.



Access Control Group Configuration

Status: Ready

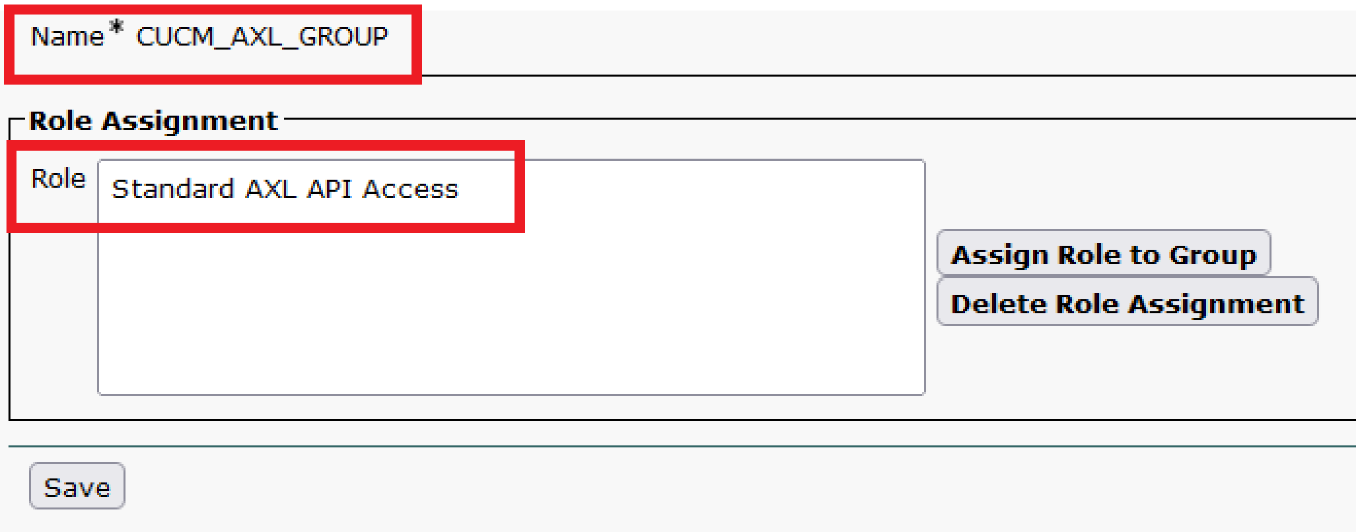
Access Control Group Information

Name* CUCM_AXL_GROUP

Available for Users with User Rank as * 1 - Default User Rank

Related Links: Back To Find/List

Assigning API access to AXL group

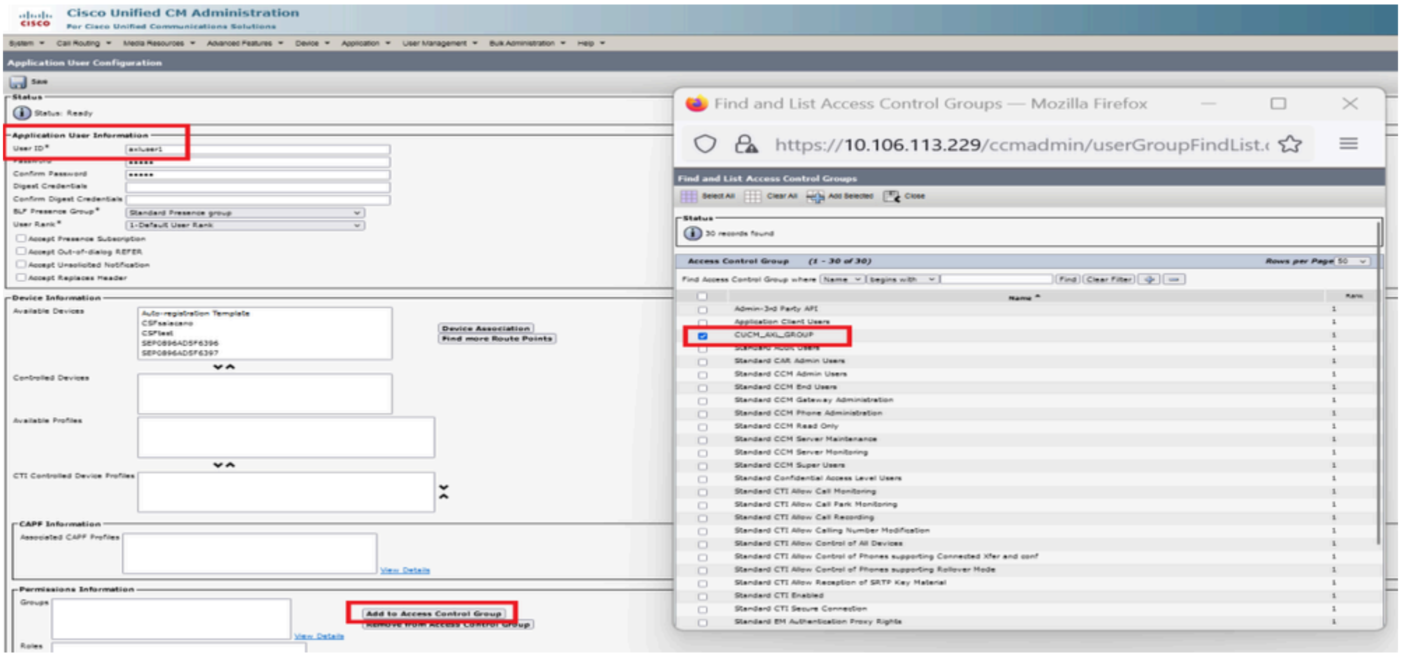


Name* CUCM_AXL_GROUP

Role Assignment

Role Standard AXL API Access

Navigate to User Management > Application User, click Add New and create an Application User AXLuser. Then, assign the access control group, which was created earlier.



Application User Configuration

Status: Ready

Application User Information

User ID* axluser1

Password *****

Confirm Password *****

Digest Credentials

Confirm Digest Credentials

BLF Presence Group* Standard Presence group

User Rank* 1-Default User Rank

□ Accept Presence Subscription

□ Accept Out-of-dialog REFER

□ Accept Unsolicited Notification

□ Accept Replaces Header

Device Information

Available Devices: Auto-registration Template, CSFsalesano, CSFtest, SEP0896AD5F6396, SEP0896AD5F6397

Find and List Access Control Groups — Mozilla Firefox

https://10.106.113.229/ccmadmin/userGroupFindList.

Status: 30 records found

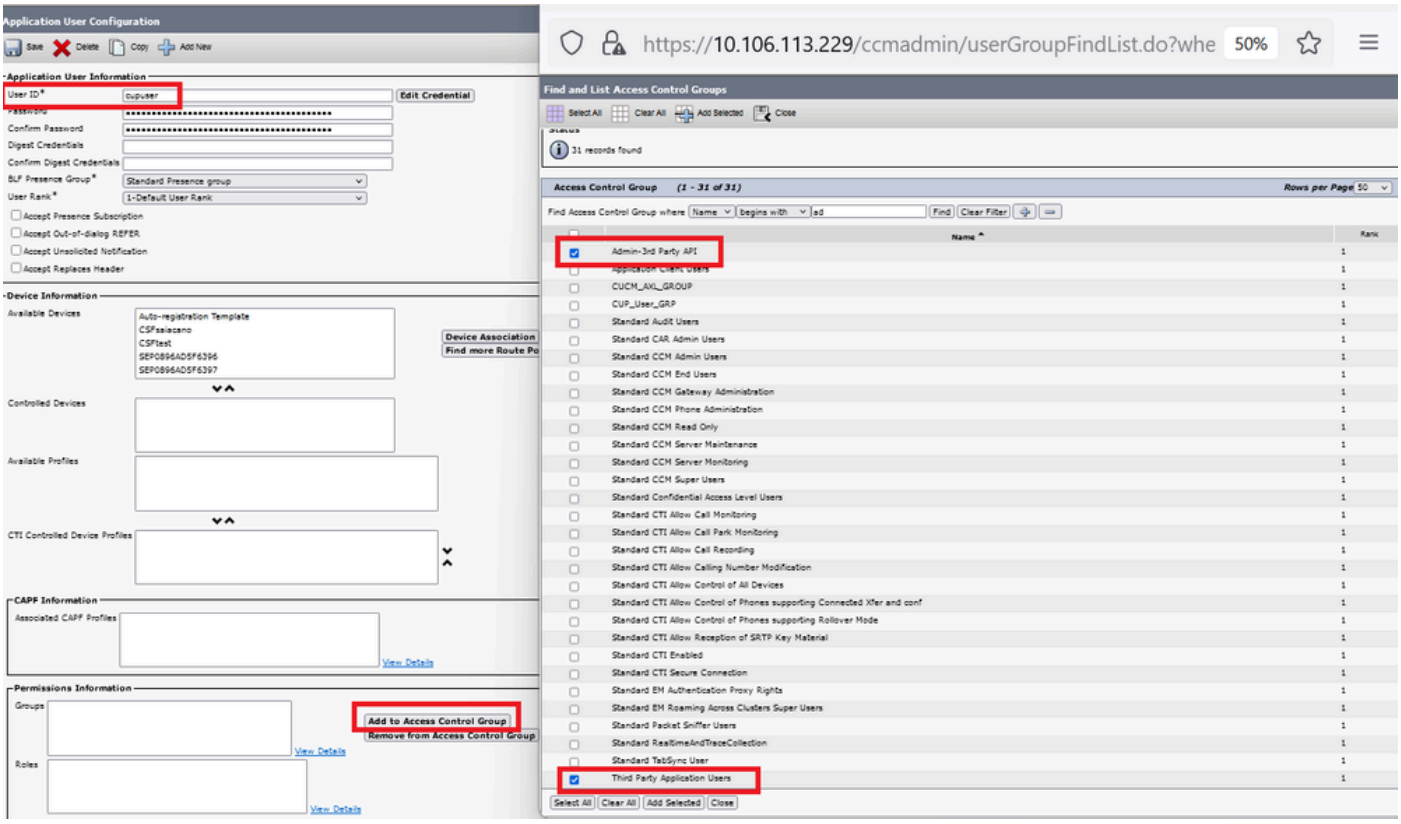
Access Control Group (1 - 30 of 30)

Find Access Control Group where Name begins with

	Name	Rank
□	Admin-3rd Party API	1
□	Application Client Users	1
☑	CUCM_AXL_GROUP	1
□	Standard Audit Users	1
□	Standard CAR Admin Users	1
□	Standard CCM Admin Users	1
□	Standard CCM End Users	1
□	Standard CCM Gateway Administration	1
□	Standard CCM Phone Administration	1
□	Standard CCM Read Only	1
□	Standard CCM Server Maintenance	1
□	Standard CCM Server Monitoring	1
□	Standard CCM Super Users	1
□	Standard Confidential Access Level Users	1
□	Standard CTI Allow Call Monitoring	1
□	Standard CTI Allow Call Park Monitoring	1
□	Standard CTI Allow Call Recording	1
□	Standard CTI Allow Calling Number Modification	1
□	Standard CTI Allow Control of All Devices	1
□	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	1
□	Standard CTI Allow Control of Phones supporting Rollover Mode	1
□	Standard CTI Allow Reception of SRTP Key Material	1
□	Standard CTI Enabled	1
□	Standard CTI Secure Connection	1
□	Standard EM Authentication Proxy Rights	1

Creating a user and assigning AXL group

Create a CUP user and assign these two roles: Third Party Application Users and Admin-3rd Party API.



Application User Configuration

Application User Information

User ID*	cupuser
Password	**
Confirm Password	**
Digest Credentials	
Confirm Digest Credentials	
BLF Presence Group*	Standard Presence group
User Rank*	1-Default User Rank

□ Accept Presence Subscription
□ Accept Out-of-dialog REFER
□ Accept Unsolicited Notification
□ Accept Replaces Header

Device Information

Available Devices: Auto-registration Template
CSFsaiacano
CSFtest
SEP0896AD5F6396
SEP0896AD5F6397

Controlled Devices

Available Profiles

CTI Controlled Device Profiles

CAPF Information

Associated CAPF Profiles

Permissions Information

Groups

Roles

https://10.106.113.229/ccmadmin/userGroupFindList.do?whe 50%

Find and List Access Control Groups

Status

31 records found

Access Control Group (1 - 31 of 31) Rows per Page 50

Find Access Control Group where Name begins with ad

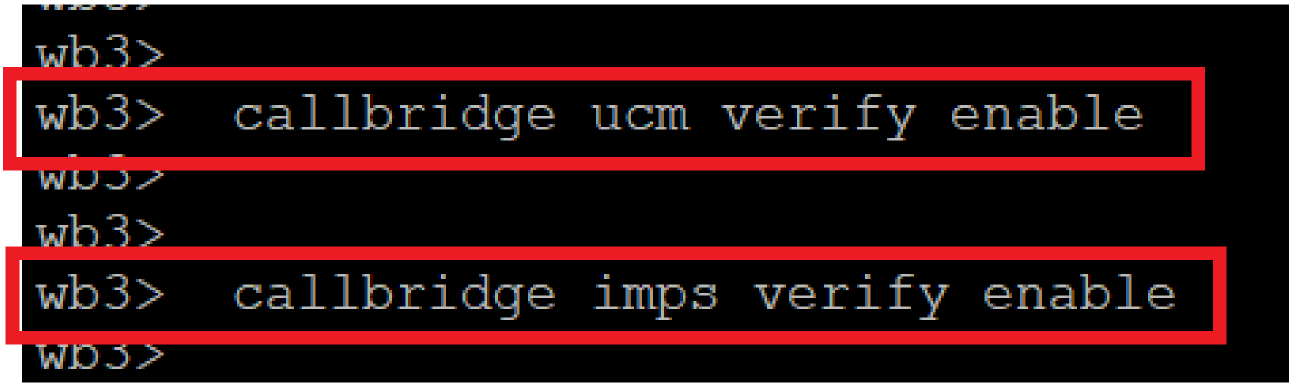
□	Name ▲	Rank
☑	Admin-3rd Party API	1
□	Application Client Users	1
□	CUCM_AXL_GROUP	1
□	CUP_User_GRP	1
□	Standard Audit Users	1
□	Standard CAR Admin Users	1
□	Standard CCM Admin Users	1
□	Standard CCM End Users	1
□	Standard CCM Gateway Administration	1
□	Standard CCM Phone Administration	1
□	Standard CCM Read Only	1
□	Standard CCM Server Maintenance	1
□	Standard CCM Server Monitoring	1
□	Standard CCM Super Users	1
□	Standard Confidential Access Level Users	1
□	Standard CTI Allow Call Monitoring	1
□	Standard CTI Allow Call Park Monitoring	1
□	Standard CTI Allow Call Recording	1
□	Standard CTI Allow Calling Number Modification	1
□	Standard CTI Allow Control of All Devices	1
□	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	1
□	Standard CTI Allow Control of Phones supporting Rollover Mode	1
□	Standard CTI Allow Reception of SRTP Key Material	1
□	Standard CTI Enabled	1
□	Standard CTI Secure Connection	1
□	Standard EM Authentication Proxy Rights	1
□	Standard EM Roaming Across Clusters Super Users	1
□	Standard Packet Sniffer Users	1
□	Standard RealtimeAndTraceCollection	1
□	Standard TabSync User	1
☑	Third Party Application Users	1

Creating CUP user

Enable certificate verification for the CUCM and Cisco Unified Communications Manager IM & Presence Service (IMPS) certificate on the CMS using:

```
callbridge ucm verify <enable/disable>
```

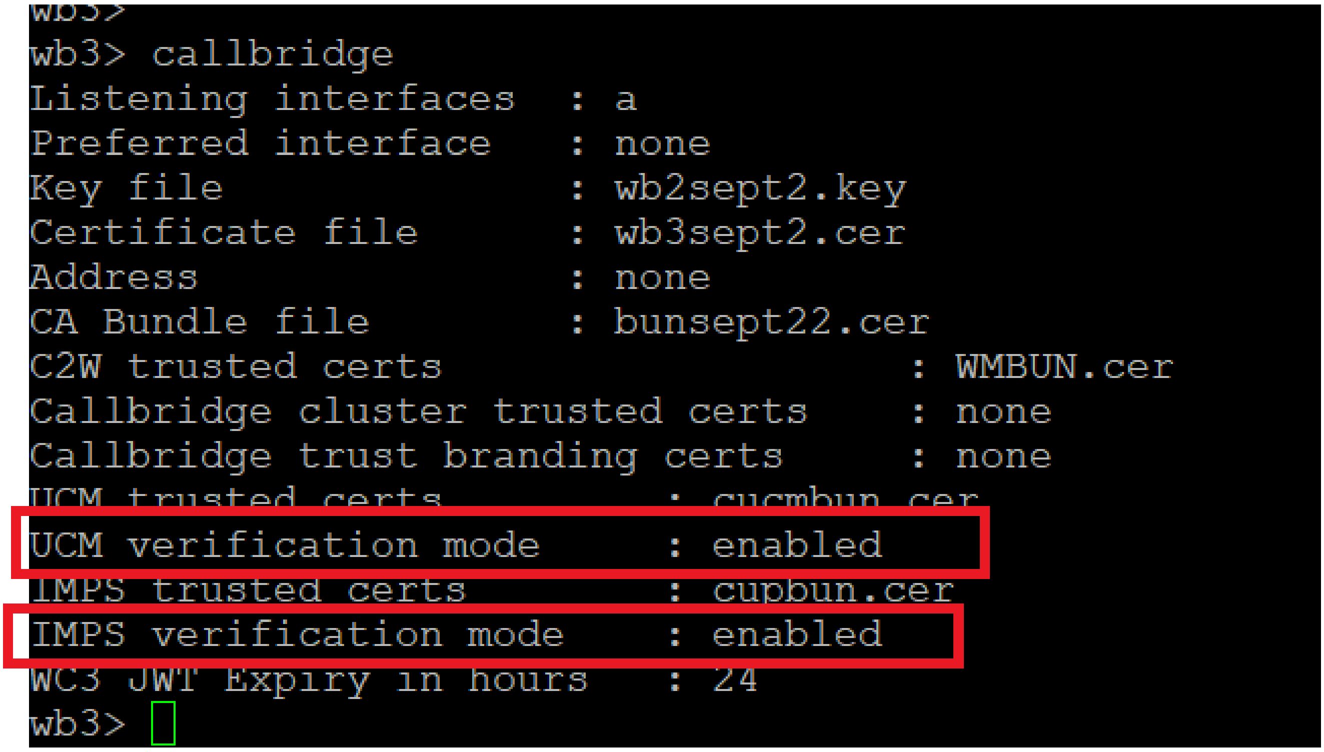
```
callbridge imps verify <enable/disable>
```



```
wb3>
wb3>  callbridge ucm verify enable
wb3>
wb3>
wb3>  callbridge imps verify enable
wb3>
```

Callbridge verify CUCM and CUPS cert

Verify it by running the `callbridge` command.



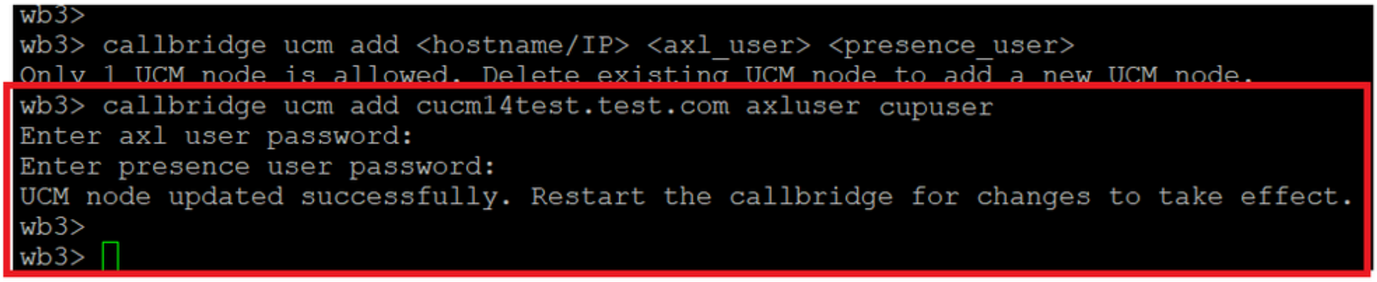
```
wb3>
wb3> callbridge
Listening interfaces     : a
Preferred interface      : none
Key file                 : wb2sept2.key
Certificate file         : wb3sept2.cer
Address                  : none
CA Bundle file           : bunsept22.cer
C2W trusted certs                            : WMBUN.cer
Callbridge cluster trusted certs             : none
Callbridge trust branding certs              : none
UCM trusted certs                : cucmbun.cer
UCM verification mode            : enabled
IMPS trusted certs               : cupbun.cer
IMPS verification mode           : enabled
WC3 JWT Expiry in hours          : 24
wb3>
```

Callbrdge command check

Now add CUCM Fully Qualified Domain Name (FQDN) and the User **AXL** and **CUPS** created earlier on CMS using callbridge ucm add <hostname/IP> <axl_user> <presence_user>.

axl_user = AXL user on CUCM

presence_user = CUP user created earlier



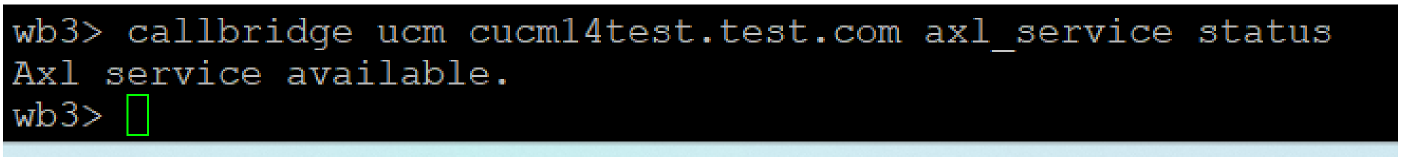
```
wb3>
wb3> callbridge ucm add <hostname/IP> <axl_user> <presence_user>
Only 1 UCM node is allowed. Delete existing UCM node to add a new UCM node.
wb3> callbridge ucm add cucm14test.test.com axluser cupuser
Enter axl user password:
Enter presence user password:
UCM node updated successfully. Restart the callbridge for changes to take effect.
wb3>
wb3>
```

Adding CUCM to Callbridge

Now, verify if CMS trusts CUCM services with the help of:

callbridge ucm <hostname/IP> axl_service status

callbridge ucm cucm14test.test.com axl_service status

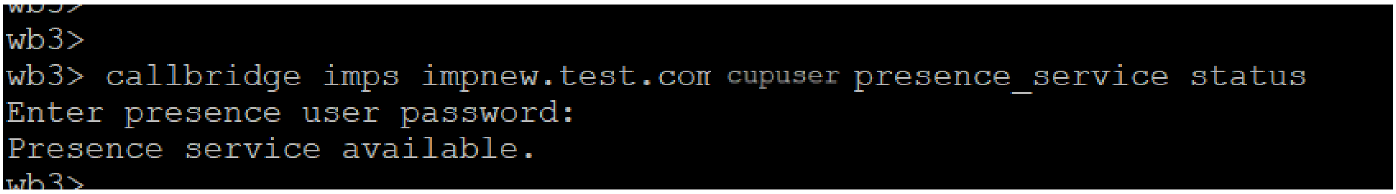


```
wb3> callbridge ucm cucm14test.test.com axl_service status
Axl service available.
wb3>
```

Callbridge AXL status

callbridge imps <hostname/IP> <presence_user> presence_service status

wb3> callbridge imps impnew.test.com cisco presence_service status



```
wb3>
wb3>
wb3> callbridge imps impnew.test.com cupuser presence_service status
Enter presence user password:
Presence service available.
wb3>
```

Callbridge presence status

Services available means CUCM and CMS trust each other for AXL and Presence services.

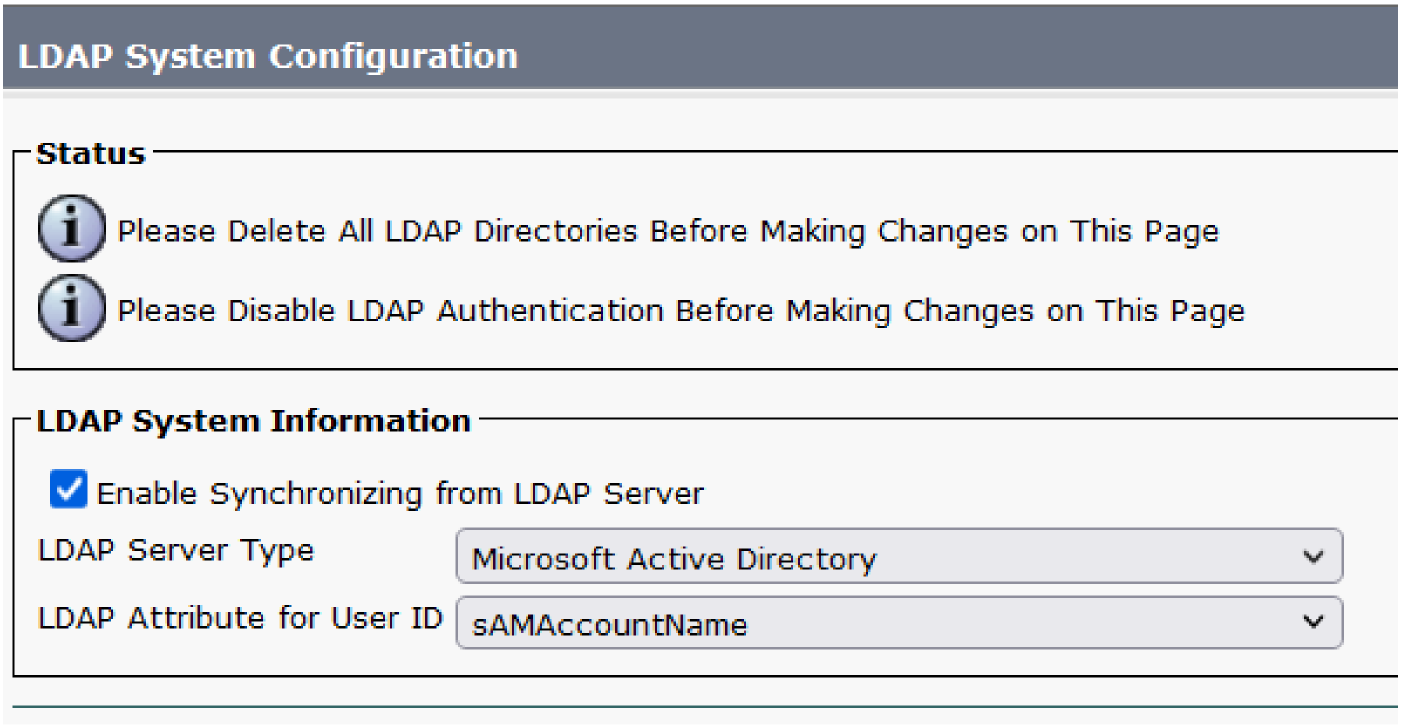
Note:
CUCM has Lightweight Directory Access Protocol (LDAP) users synced and also updated on the CUPS. The users must have the same web app user ID and Jabber JID and must be signed into the web app with the same user ID, for presence to be updated on Jabber.

CUCM Specific Configuration for Presence Sharing between Webapp and Jabber

Client

CUCM must have LDAP configured.

LDAP System:



LDAP System Configuration

Status

Please Delete All LDAP Directories Before Making Changes on This Page

Please Disable LDAP Authentication Before Making Changes on This Page

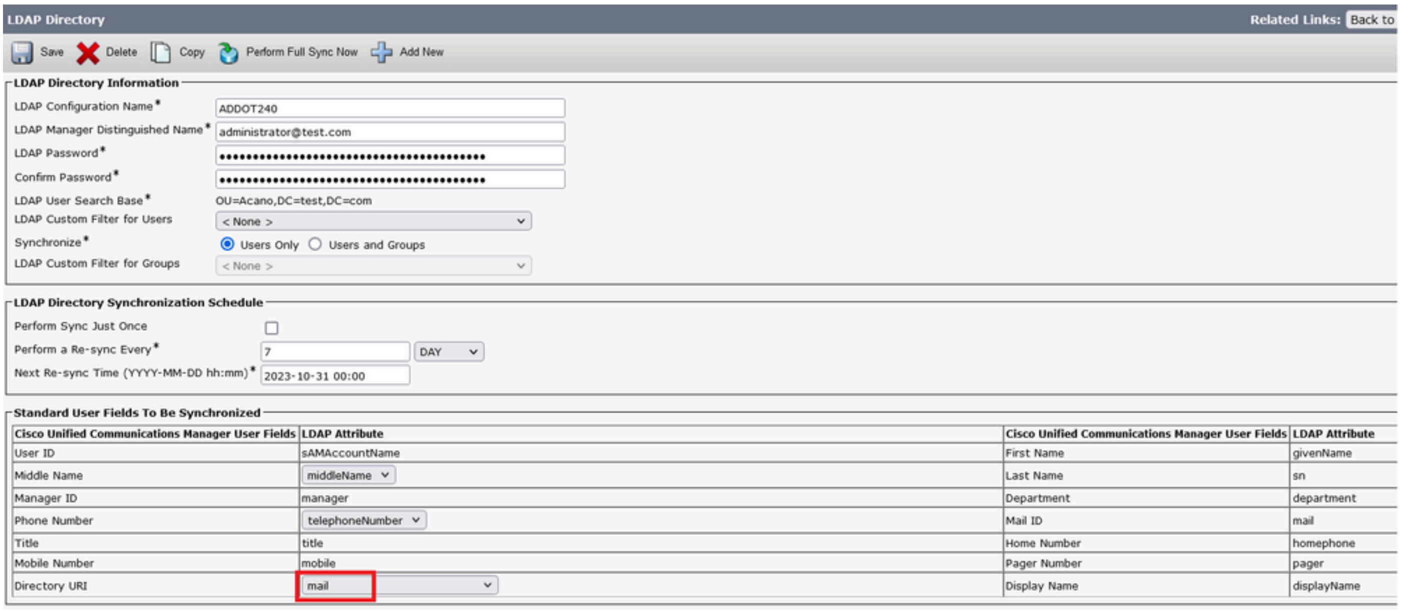
LDAP System Information

☑ Enable Synchronizing from LDAP Server

LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

CUCM LDAP configuration 1

LDAP Directory:



LDAP Directory Information

LDAP Configuration Name*	ADDOT240
LDAP Manager Distinguished Name*	administrator@test.com
LDAP Password*	•••••••••••••••••••••••••••••••••••••••
Confirm Password*	•••••••••••••••••••••••••••••••••••••••
LDAP User Search Base*	OU=Acano,DC=test,DC=com
LDAP Custom Filter for Users	< None >
Synchronize*	● Users Only ○ Users and Groups
LDAP Custom Filter for Groups	< None >

LDAP Directory Synchronization Schedule

Perform Sync Just Once	□
Perform a Re-sync Every*	7 DAY
Next Re-sync Time (YYYY-MM-DD hh:mm)*	2023-10-31 00:00

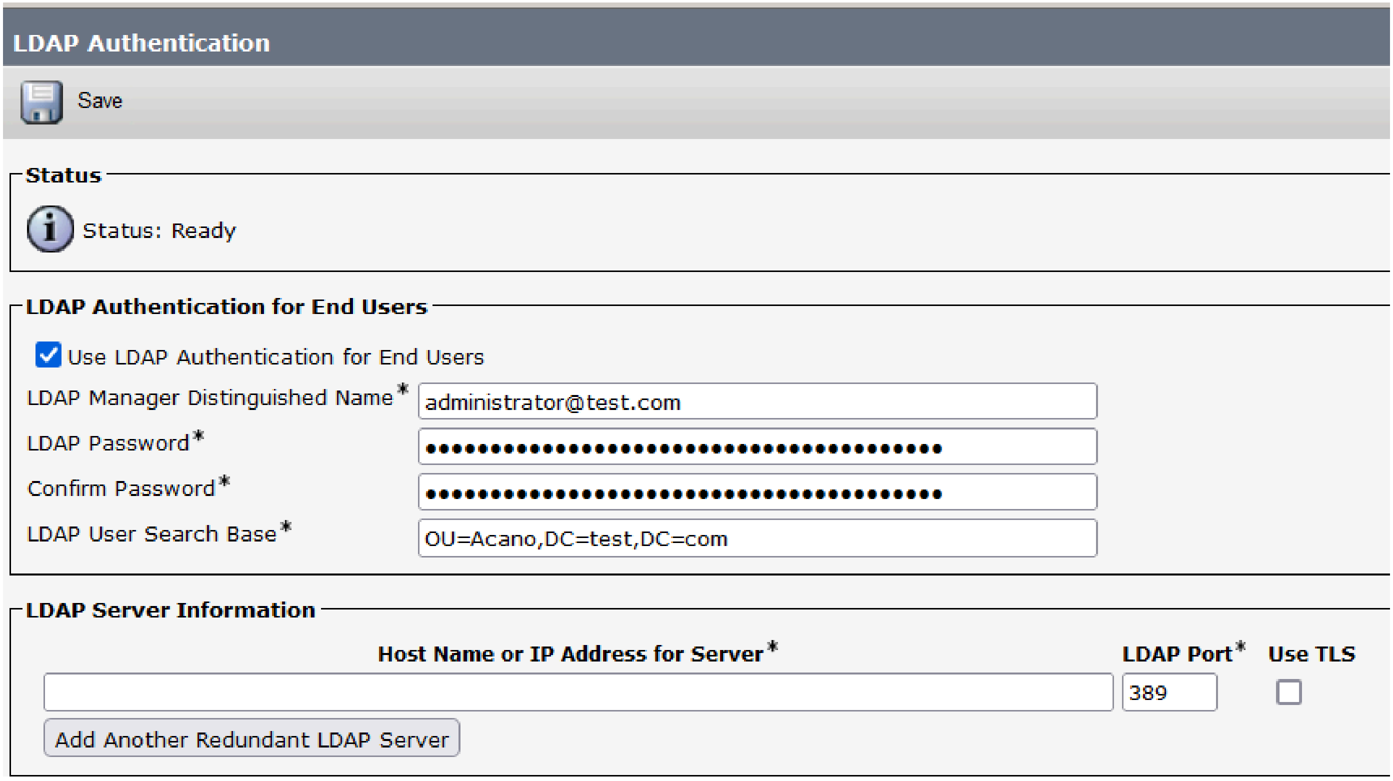
Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail
Title	title	Home Number	homephone
Mobile Number	mobile	Pager Number	pager
Directory URI	mail	Display Name	displayName

CUCM LDAP configuration 2

LDAP Authentication:

CUCM LDAP configuration 1 CUCM LDAP configuration 1 CUCM LDAP configuration 1



Status

Status: Ready

LDAP Authentication for End Users

☑ Use LDAP Authentication for End Users

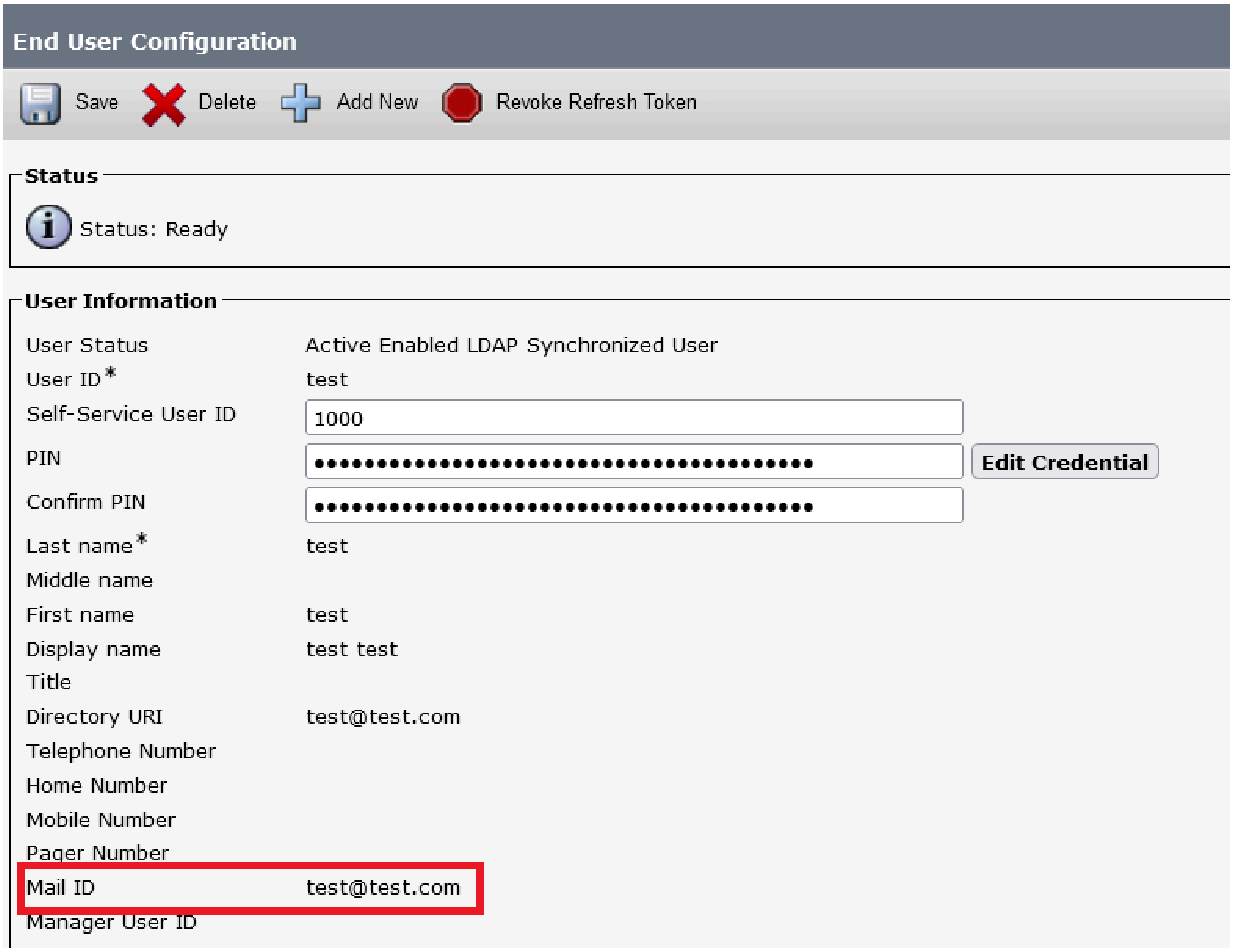
LDAP Manager Distinguished Name*	administrator@test.com
LDAP Password*	••
Confirm Password*	••
LDAP User Search Base*	OU=Acano,DC=test,DC=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
	389	□

CUCM LDAP configuration 3

Users pulled from LDAP into CUCM with Mail-ID configured:



Status

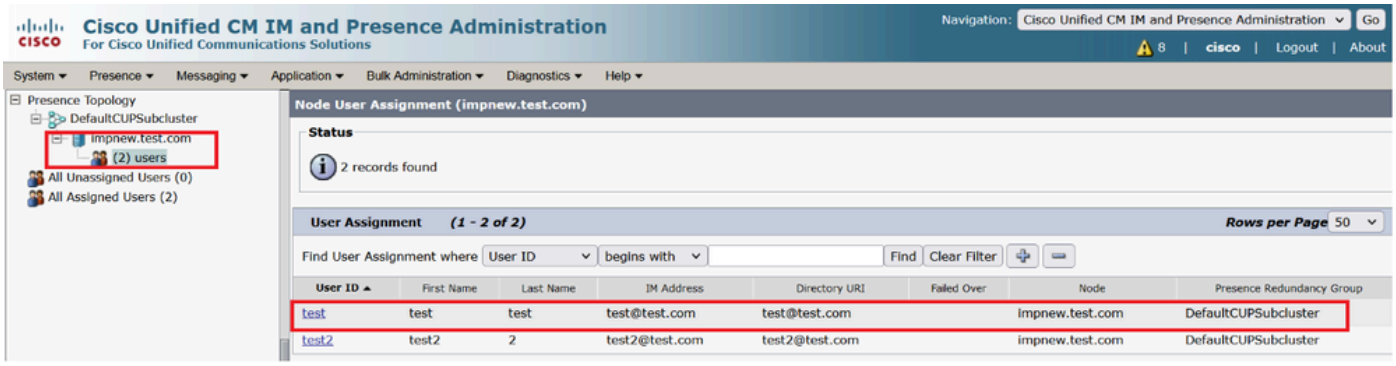
Status: Ready

User Information

User Status	Active Enabled LDAP Synchronized User
User ID*	test
Self-Service User ID	1000
PIN	●●
Confirm PIN	●●
Last name*	test
Middle name	
First name	test
Display name	test test
Title	
Directory URI	test@test.com
Telephone Number	
Home Number	
Mobile Number	
Pager Number	
Mail ID	test@test.com
Manager User ID	

Users in CUCM

CUCM user updated on CUPS server:



Node User Assignment (impnew.test.com)

Status

2 records found

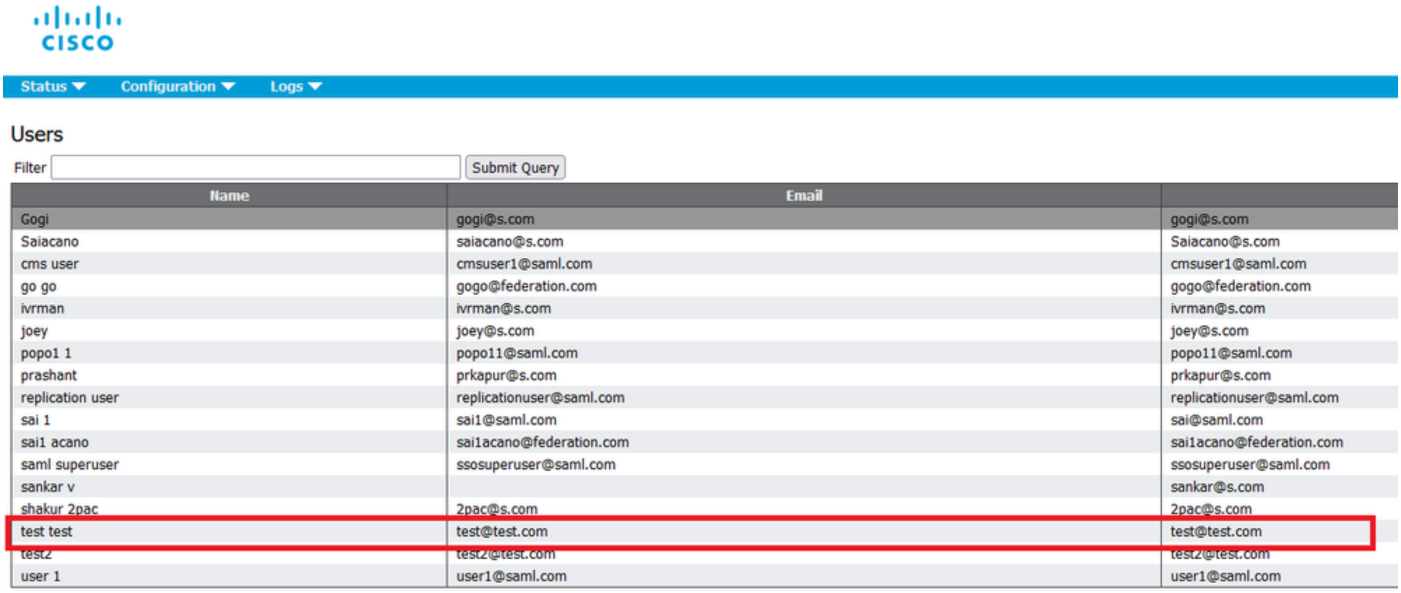
User Assignment ***(1 - 2 of 2)*** ***Rows per Page*** 50

Find User Assignment where User ID begins with

User ID ▲	First Name	Last Name	IM Address	Directory URI	Failed Over	Node	Presence Redundancy Group
test	test	test	test@test.com	test@test.com		impnew.test.com	DefaultCUPSubcluster
test2	test2	2	test2@test.com	test2@test.com		impnew.test.com	DefaultCUPSubcluster

Users in CUPS

The same LDAP Directory is also configured on the CMS. The user database is pulled and synced on CMS.



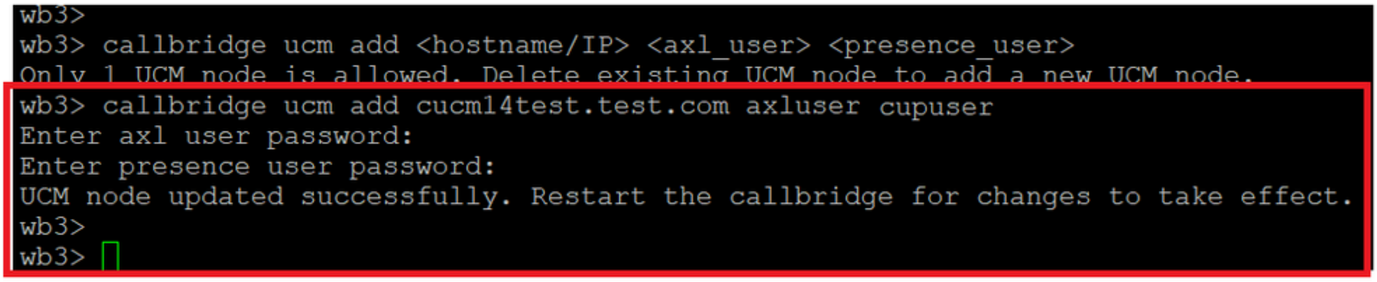
Users

Filter [ ] Submit Query

Name	Email	
Gogi	gogi@s.com	gogi@s.com
Saiacano	saiacano@s.com	Saiacano@s.com
cms user	cmsuser1@saml.com	cmsuser1@saml.com
go go	gogo@federation.com	gogo@federation.com
ivrman	ivrman@s.com	ivrman@s.com
joey	joey@s.com	joey@s.com
popo1 1	popo11@saml.com	popo11@saml.com
prashant	prkapur@s.com	prkapur@s.com
replication user	replicationuser@saml.com	replicationuser@saml.com
sai 1	sai1@saml.com	sai@saml.com
sai1 acano	sai1acano@federation.com	sai1acano@federation.com
saml superuser	ssosuperuser@saml.com	ssosuperuser@saml.com
sankar v		sankar@s.com
shakur 2pac	2pac@s.com	2pac@s.com
test test	test@test.com	test@test.com
test2	test2@test.com	test2@test.com
user 1	user1@saml.com	user1@saml.com

CMS users

Now, since you have already validated that CMS can trust CUCM, you can proceed with testing Presence.

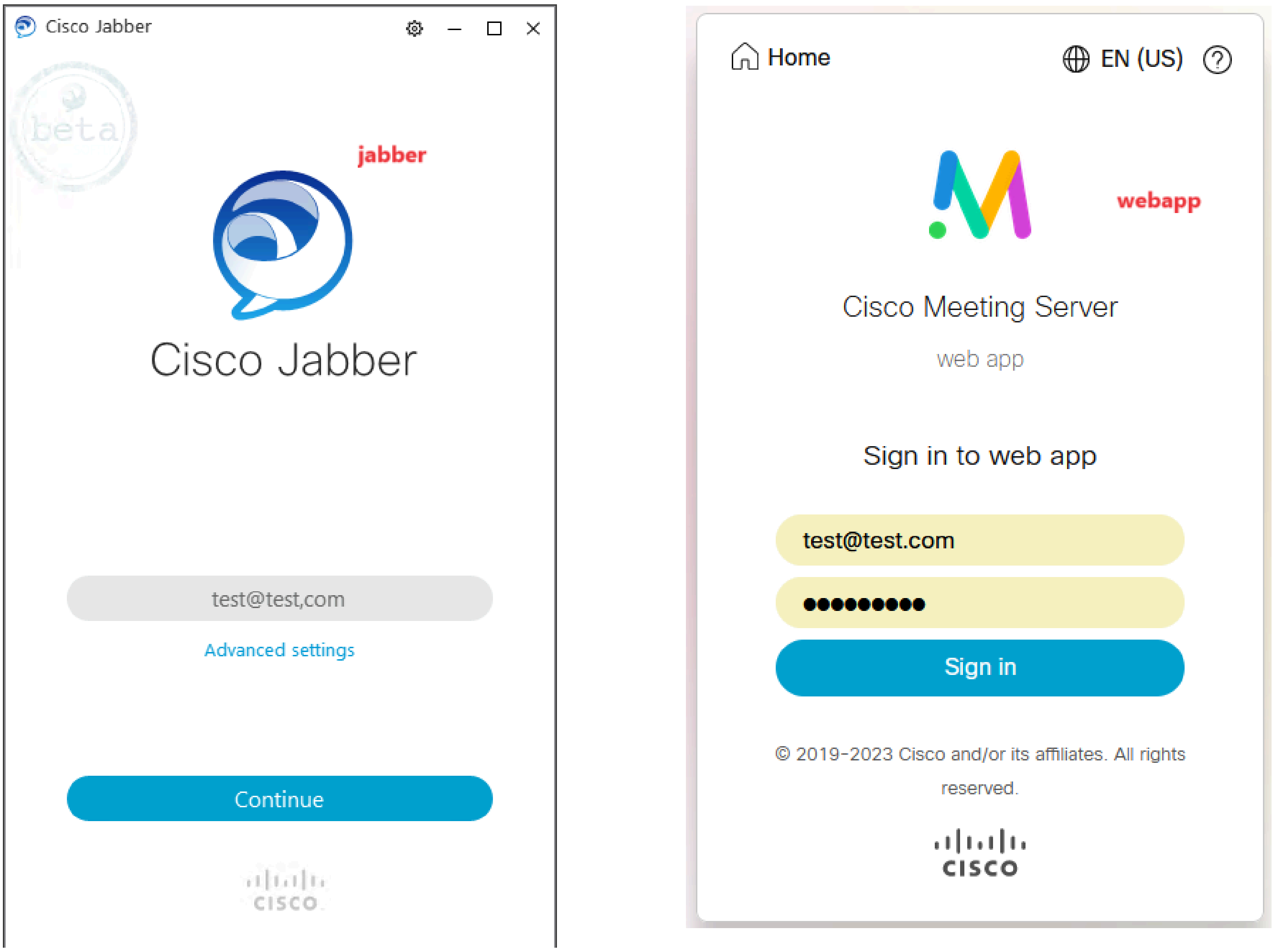


```
wb3>
wb3> callbridge ucm add <hostname/IP> <axl_user> <presence_user>
Only 1 UCM node is allowed. Delete existing UCM node to add a new UCM node.
wb3> callbridge ucm add cucm14test.test.com axluser cupuser
Enter axl user password:
Enter presence user password:
UCM node updated successfully. Restart the callbridge for changes to take effect.
wb3>
wb3>
```

Adding CUPS and CUCM to CMS

Verify

Signed on two clients with the same user (synced from the same LDAP):



test@test,com

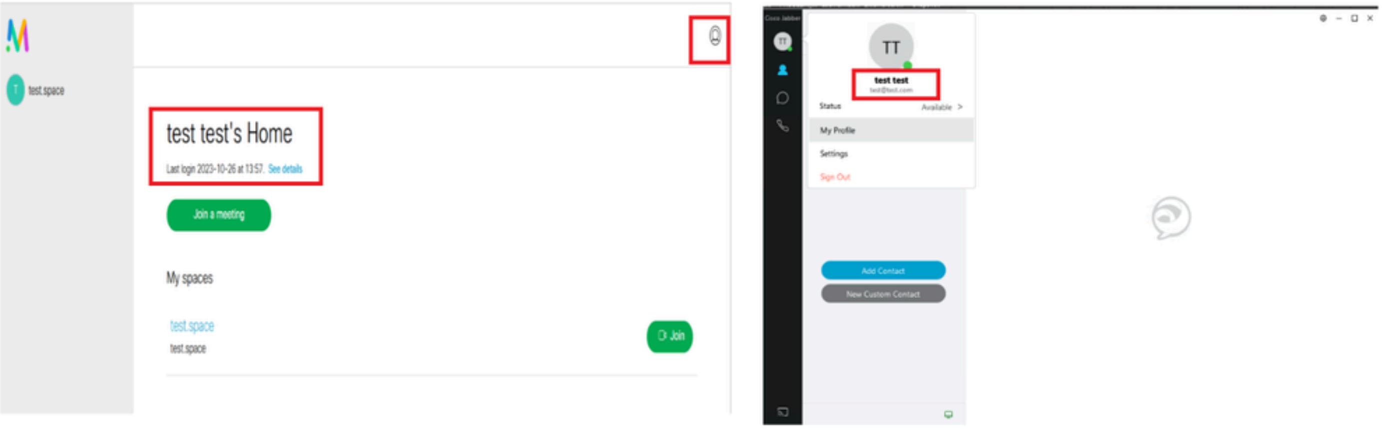
test@test.com

●●●●●●●●●

© 2019-2023 Cisco and/or its affiliates. All rights reserved.

User login in Jabber and webapp

Both clients signed into the same user test@test.com.



test test's Home

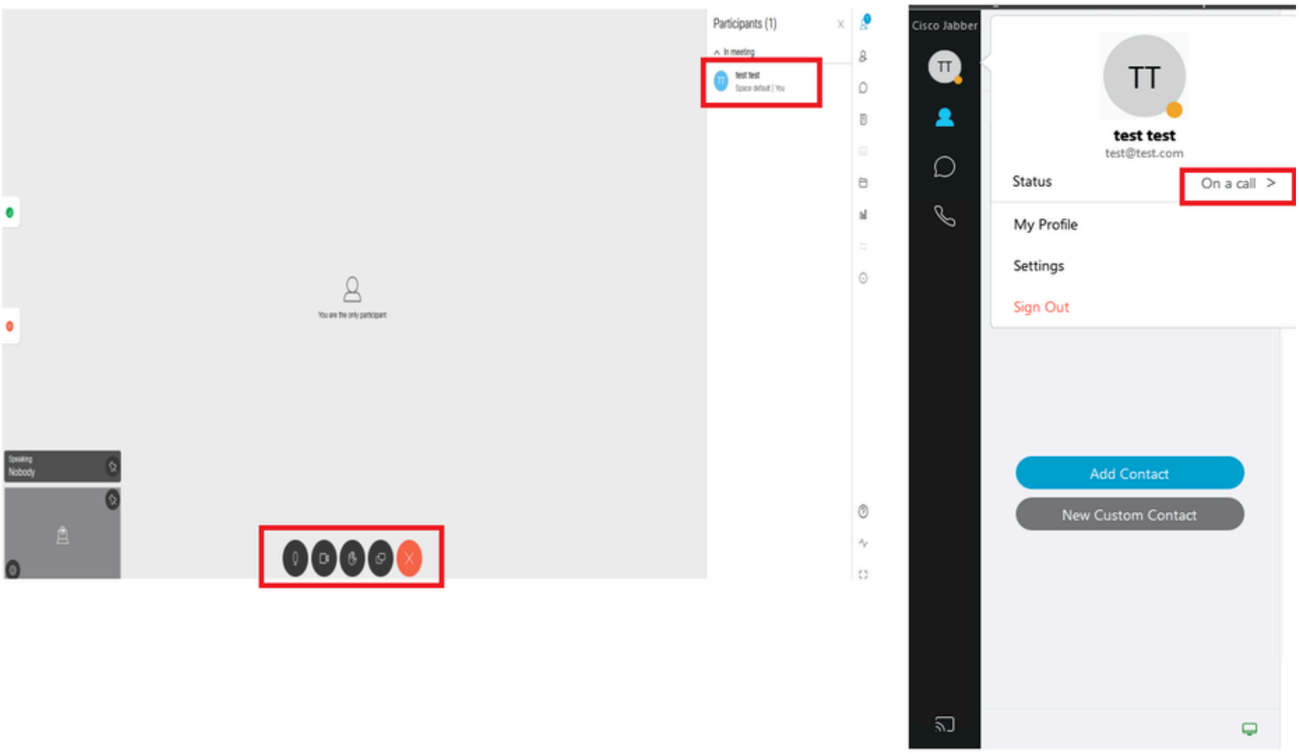
Last login 2023-10-26 at 13:57. See details

test.space
test.space

test test
test@test.com

Status Available >

Presence in Jabber and Webapp before call



Presence status changes when call is joined from webapp

When a Jabber user signs into the web app and joins a meeting, the Meeting Server updates the Jabber status to ‘In a meeting, In a call’ and reverts to its previous status after the user ends the meeting. For example, if the status of the user on Jabber is showing ‘Available’, it is updated to ‘In a meeting, In a call’ when in a web app meeting. After the user leaves the meeting, the Jabber status is set to ‘Available’ again. If the Jabber user is in another meeting/call while joining the web app meeting, the Meeting Server does not update the Jabber status. If the Jabber user has set their status to 'DND - Do not disturb' before joining the web app meeting, the Meeting Server does not update the Jabber status. If the user updates the Jabber status manually anytime during the web app meeting, the Meeting Server does not override the manually updated user status.