

Abilitare la comunicazione sicura tra CMS e CUCM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Comunicazione sicura tra CMS e server CUCM/IMP](#)

[Configurazione specifica CUCM per la condivisione della presenza tra Webapp e client Jabber](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come abilitare la comunicazione tra Cisco Meeting Server (CMS) e Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CMS versione 3.8 e successive
- CUCM e IM&P
- Jabber

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CMS versione 3.8
- CUCM e IM&P 14 SU (3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritto il processo per stabilire una comunicazione sicura tra CMS e CUCM per la condivisione della presenza di Jabber/app Web. Illustra i passaggi dettagliati per la configurazione e la risoluzione dei problemi relativi all'aggiornamento dello stato degli utenti Jabber durante le riunioni dell'app Web sul CMS. È possibile configurare Meeting Server per aggiornare lo stato della presenza degli utenti Jabber durante una riunione con l'app Web Cisco Meeting Server.

Configurazione

Comunicazione sicura tra CMS e server CUCM/IMP

Accedere a CUCM nella pagina di amministrazione del sistema operativo, selezionare Security > Certificate Management e scaricare il certificato TOMCAT.

Trust	Common Name	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
CAFF-trust	High_Assurance_SUDI_CA_0a6475524c08617c62	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 eni Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAFF-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 eni Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAFF-trust	CAFF-4c15e524	Trust	Self-signed	RSA	CAFF-4c15e524	CAFF-4c15e524	05/07/2028	
CAFF-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 eni Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAFF-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 eni Presence of this certificate allows the end point to communica securely with UCM using the MIC when associated with a secu
CAFF-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 eni 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_6dffacb16e53663f3d9af4a66355758	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_36a79869500000000004	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_496beedc456be08f49ff7716b999d3a4	Identity	Self-	EC	cucm14test.test.com	cucm14test-EC.test.com	09/30/2028	Self-signed certificate generated by system

Certificato Tomcat CUCM

Accedere a Cisco Unified Presence Server (CUPS) nella pagina di amministrazione del sistema operativo, individuare Security > Certificate Management e scaricare il certificato CUPS.

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

Certificato Presence CUPS

Scaricare il certificato CA ROOT che ha firmato il certificato Tomcat and Cup.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration

Show Settings Security Software Upgrades Services Help

Certificate List

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

Status
3 records found

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

Find Certificate List where Certificate begins with tomcat-trust Find Clear Filter

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat-trust	cuom1dtest-EC.test.com_486baed6456ba0b40f7716999d41a1	Trust	Self-signed	EC	cuom1dtest.test.com	cuom1dtest-EC.test.com	09/30/2028	Trust Certificate
tomcat-trust	S-WIN2008R2-CA_04736d12017d7d7f59a9a7381b2d328e	Trust	Self-signed	RSA	S-WIN2008R2-CA	S-WIN2008R2-CA	09/29/2028	Signed Certificate
tomcat-trust	impnew-EC.test.com_38082a29e3808e93801a3392820583	Trust	Self-signed	RSA	impnew.test.com	impnew-EC.test.com	09/30/2028	Trust Certificate
tomcat-trust	cuom1dtest.test.com_26a7366300000000000024	Trust	CA-signed	RSA	cuom1dtest.test.com	S-WIN2008R2-CA	10/04/2025	Trust Certificate
tomcat-trust	impnew-EC.test.com_779a9d72e3fe922d87583a1071417e	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

Certificato radice di Tomcat

Cisco Unified IM and Presence Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified IM and Presence OS Administration

Show Settings Security Software Upgrades Services Help

Certificate List

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

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

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

Certificato radice per CUPS

Crea un bundle di certificati CUCM. Per certificato bundle si intende l'inserimento del certificato del server nella parte superiore, del certificato intermedio (qualsiasi) nella parte centrale e del certificato ROOT nella parte inferiore, seguito da un (1) ritorno a capo.

Di seguito è riportato un esempio per il certificato BUNDLE:

```
1 -----BEGIN CERTIFICATE-----
2 MIIFqgCCBjOgAwIBAgIKNqYeYAAAAAABDANBqkqhkiG9w0BAQsFADBBMRMwEQQYK
3 CZImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUGA1UEAxMOUy1X
4 SU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMyNzE2WncNMjUxMDA0MTMzNzE2WjBXMQsw
5 CQYDVQQGEwJlZEMMAQGA1UECMBDQ2FyMQwwCgYDVQQHEwNpbmQxZjAMBGNVBAOT
6 BWNpc2NvMRswGgYDVQQDEkNjZW50MTR0ZDZlLnRlc3QuY29tMIIBIjANBgkqhkiG
7 9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoYE9an27hV05JUwAEwutEy5RA4WwaxIvkqEI
8 ah0fDpRI2GgY+mrH9q70hAvG3uDYBtBHKYJpkYepeULNjZkh07a39IeeJMG8/q28
9 SckZ+j1VIyw8gt+cnG6E6ibCD+HNdtKfwL0ipSdlTnlieX6DsF05Z1K4Alm4yrsN
10 +b0/wSikfV0+ValyC90nbTCUCIKGvqvqGsdidb6TRfhi+w4RD+0NgOBjWHqcXX
11 WXgp9JWYQdy7YeX8Y2kljBAyRhSPfa35hojy470hE91N8axmHRm2m5htqeE0kSOy
12 2o09pj7f7Aq1wVAfVpQCxx12sXtZARHpGdswpm4M8r5MoXptwIDAQABo4ICjTCC
13 AokwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
14 AjAoBgNVHREEITAfgh0ZKN0LmNvbYITy3VjbTE0dGVudC50ZKN0LmNvbTAdBgNV
15 HQ4EFgQUTMTpsuTu05EBH2wgGFb6qii7M38wHwYDVR0jBBgwFoAUA6L6fIQ4Vp+QI
16 UDz/X6MwFAVhJ4IwgcgGA1UdHwSBwDCBwTCBuqCBt6CBtIaBsWakYXA6Ly8vQ049
17 Uy1XSU4yMDA4UjItQ0EwS049V010MjAwOFIyLENOPUNEUCxDTj1lQdWJsaWMM1MjBL
18 ZXk1MjBTZXJ2aWwN1cYkDTj1lTXJ2aWwN1cYkDTj1lDb25maWdlcmF0aW9uLERDPVMS
19 REM9Y29tP2N1cnRpZmljYXRlUmV2b2b2NhdG1vbkkxc3Q/YmFzZT9vYmplY3RDDBGFs
20 csljUkxEXX0cmliidXRpb25Qb2ludDCBugYIKwYBBQUHAQEEdga0wgaowgacGCCsG
21 AUFBAChOgabGRhcDovLy9DTj1lTLVdJTj1lMDhSM1lDQ3xDTj1lBSUESQ049UHVl
22 bGljJTlW2V5JTlW2V5dmljZXMzQ049U2V5dmljZXMzQ049Q29uZmlndXJhdG1v
23 bixEQslTLERDPWNvbT9jQUN1cnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M5Y2V5
24 dG1maWwNhdG1vbkkf1dGhvcml0eTA9BgkkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQcE
25 yrsWhcnoHIXEjS6B5uhFhsusPgeGpusehts3XAIBZAIbAjAnBgkkrBgEEAYI3FQcE
26 GjAYMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMCMAoGCCsG8Ib3DQEBcUAA4IBAQCQ
27 hREe6ZJHVx1N7JNgY0RE4V9S3FiyQPIVYFVEdaKAL+AfV1S214D7ohFIjL5rSA
28 ThWiFFS1w1eA5Cjlg9gi2leHI2uDuor6XEXKWB/bkC9BXoDkRMFV7bh9CoosFmXk8
29 r6xEn7H9cAHAs3wFILUnAip1KF/7odBkNUSgT39NJAL1UgVFPt81r6lk8OR5TAYI
30 9vs4dw5ocQzs1720Av8ZDKNFDTsWoOGtU2dCMIXasJ05ALmMBtagqYBNj16URkR8i
31 f2sOkb+NdPZD4XAE00tW8rji124ukr7JBgeWYsjsD2tsZsJgslMprNaVuMDh280Q
32 JQFAiCOp3GgYjkJBZcH2
33 -----END CERTIFICATE-----
34 -----BEGIN CERTIFICATE-----
35 MIIDXTCCAkWgAwIBAgIQDXWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADBB
36 MRMwEQQYKCC2ImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUGA1UE
37 AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMyNzE2WncNMjUxMDA0MTMzNzE2WjBXMQsw
38 WjBEMRMwEQQYKCC2ImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUG
39 A1UEAxMOUy1XSU4yMDA4UjItQ0EwEwgEiMA0GC8qG8Ib3DQEBQUAA4IBDwAwggEK
40 AoIBAQCXa6tjSyoUyn6GkoSbe98SasKRUNGbCORKnI41tWEiX0vPITEsqZUPRJq4
41 7C8useeDiJFUBWAY9e8F4nm+VhGSEKqkwekrlJAF1mV4hkypkR0Wz64b4y04Ln8e
42 3E/F6/SXA6HOHQHdy1qlQMWSA/PXB441GKbSnfA4pjTB8nMP5WL+iBruYH9tX6EJ
43 IJq5Fe+RZYNH/mLuB+0Qf1OCn4sqsx2Gf8DxhJNHU+2m3q7h319exxioDcwiVwZO
44 xqUKrvBs6jBtOg4Kvs3sa4AHyP91SAA2vp42MwtBdis803wx+vm/HoVr0fHum/W1
45 Z92iwR9Jx44tKoJHVpBwMvnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjaPBGNV
46 HRMBAf8EBTADAQH/MB0GA1UdDgQWBBERovp8hDhWn5AhQ0s9fosAUBWEngjaQBgkr
47 BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEA5nsa91K4BISCAuBgMMe
48 YSPEXl5kEXPQcFtJt1FjnC5uTC4IOMQQFfuralBQfr4DokDXK5892npt5DAFors5
49 k60GpH1bRPBaoxJhR0Ta3imL6yAZ0f2o380nrVRDZKlug/1VeXF/2hlTeZc73utt
50 k5sqewqTQ04NHrBp0Udybmpf2L5BjhlctoH490PI0HEBmVDE0WALKXliqsuEzrmm
51 mrl0MRRlS2ZBpX2W3qw90IrmPW13fde2kE2S1DvuaNcc7B8W0hgWT3HnyuMTyZi
52 b6Yf7hb5F3Z3OpHFU1b222tqk4qouEigyoaUZaLcVhV5UdBCCvwyU19yU6+EscnM
53 Ww==
54 -----END CERTIFICATE-----
55
```

Server Certificate on TOP

CUCM TOMCAT CERT

Root certificate at bottom



just 1 carriage return

Pacchetto di certificati Tomcat

Crea un bundle di certificati CUPS. Per certificato bundle si intende l'inserimento del certificato del server nella parte superiore, del certificato intermedio (qualsiasi) nella parte centrale e del certificato ROOT nella parte inferiore, seguito da un (1) ritorno a capo.

```
1 -----BEGIN CERTIFICATE-----
2 MIIFqTCCBjGgAwIBAgIKNrMm8gAAAAAABTANBgkqhkiG9w0BAQsFADEBMMRMwEQYK
3 CZImiZPyLQGBGRYDY29tMREwDwYKZCZImiZPyLQGBGRYBUzEXMBUGA1UEAxMOUy1X
4 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
5 CQYDVQQGEwJlTjEOMAwGA1UECBMFA2FybmExDDAKBgNVBAcTA2JnbDEOMAwGA1UE
6 CmFY21sY28xDDAKBgNVBAcTA2t0c3EYMBYGA1UEAxMFAW1wbmV3LnRlc3QuY29t
7 MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKHb9jzWYhi6i4IkSx8hC
8 Z1USLZHBQ28RDQw1vT3CFGZut+dayK9KshYtsOAhRFwLFPwGtABJWMz98f+DM0RG
9 FsmCtNo1ZsEOqSQCRC6b/kbQuC+6LhhgIM8I448tLaAF4neZ/5dmCUSzJNCpnbpH
10 EbqbXKkH8W42BZLeLP0T2savr5V+vriGuMjV299vGrEu49kB0EN2M+mnfcnf2OxT5
11 wtFqCY9jijKSKC40cu6iJ88A7Hi/yJQJ1NeUmnLpGpF/HKUrclu5pBdfiV1EXBkS
12 LX2bm49PFGRS0guxJZVC457vmAgACgKvwE5s3HvW1t3Tp1WE4AZtSn3z9tsYSOC7
13 bwIDAQABO4ICfsCCAnsWQYDVR01BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMA4G
14 AlUdDwEB/wQEAwIFoDAAEgNVHREEEzARgg9pbXBu2XcudGVsdC5jb20wHQYDVR0O
15 BBEYF0xvmV/jdcIDMEVOjzWR/yRAo9ktMB8GA1UdIwYQYBaAFGi+nyEOfafkCFA7
16 Pl+jMBQFYSeCMIHIBgNVHR8EgcAwgb0wgbqggbbeggb3GgbFsZGFwOi8vL0NOFVME
17 V01OMjAwOFIyLUNBLENOFVdJTjIwMDhSMixDTj1DRFAzQ049UHVibGljJTJwS2Vt
18 JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQs1TLERD
19 FWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9
20 Y1JMRGlzdHJpYnV0aW9uUG9pbmQwgb0GCCsGAQUFBwEBB1IGtMIGqMIGnBggrBgEF
21 BQcwAoaBmmxkYXA6Ly8vQ049Uy1XSU4yMDA4UjItQ0EzQ049QU1BLENOFVBlYmcp
22 YyUyMEtleSUyMFN1cnZpY2VsLENOPVN1cnZpY2VsLENOPUNvbmZpZ3VYXRpb24s
23 REM9UyxEQs1jb20/Y0FDZKJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNsPWN1cnRp
24 ZmljYXRpb25EeXR0b3JpdHkxPQYJKwYBBAGCNxUHBDAAwLgYmKwYBBAGCNxUIhcq7
25 FoXJ6ByFwY0ugeboRYbLs4HhqbRbHobc91wCAWQCAQIwJwYJKwYBBAGCNxUKBBow
26 GDAKBggrBgEFBQcDATAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAUJdy
27 3mMOfWgLN4hiShn/XCPChLMPG54IE+EINTBqsoqxs12XLl1do0JjNAI7Xd+PoAGQ
28 UXRjRN3q326yiY5C2itTLe/vAplC5yN6krL/8PEEnBmopubQVdqRUCbn4r21iNV
29 sNcBrUeOY0Vr2/EVeBObVh1DGowfrxMj59v40k15wYc88h0bopL1I/Sc2mpw5m2Z
30 R5nyyx3XfjkmZSwwMnO+Suz7dbJu2zfI6sw0EhF12tRRQHCsq9n9uQDSUXCjQFdq
31 Y3A+LJGawlAuPt4+sqOxjYKYNP8m8+WIBIUEv+oXAOvbs8ffQFoPKYf/ZmWxBJRP
32 2v/At0ns31UdcKFUPw==
33 -----END CERTIFICATE-----
34 -----BEGIN CERTIFICATE-----
35 MIIDXTCCAkwgAwIBAgIQDKWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADEB
36 MRMwEQYKZCZImiZPyLQGBGRYDY29tMREwDwYKZCZImiZPyLQGBGRYBUzEXMBUGA1UE
37 AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
38 CQYDVQQGEwJlTjEOMAwGA1UECBMFA2FybmExDDAKBgNVBAcTA2JnbDEOMAwGA1UE
39 CmFY21sY28xDDAKBgNVBAcTA2t0c3EYMBYGA1UEAxMFAW1wbmV3LnRlc3QuY29t
40 A1UEAxMOUy1XSU4yMDA4UjItQ0EwEwgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
41 AoIBAQCXA6tjSyOUyn6GkoSbe98SasKrUNGBCORKnI41tWEiX0vPITEsqZUPRJq4
42 7C8useeDiJPUBWAY9e8F4nm+VhGSEKqkwekr1JAF1mV4hkypxR0Wz64b4yO4Ln8e
43 3E/F6/SXA6HOqHDylq1QWWSA/PXB441GKb8nfa4pjTBSnMP5WL+iBruYHp9tX6EJ
44 IJq5Fe+RZYnh/mLUB+0Qf1OCn4sqsqzGf8DxhJNHU+2m3q7h319exxioDcwiVwZO
45 xqUKRvBs6jBtOg4Kvs3sa4AHyP91SAA2vp42MwtBdis803wx+vm/HoVr0fHum/W1
46 Z92iwR9Jx4tKkoJHVpEwMvnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBqNV
47 HRMBAF8EBTADAQH/MB0GA1UdDgQWBBRovp8hDhWn5AhQOz9fosAUBWEngjAQBgkr
48 BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAU5nsa91K4BISCAuBqMMe
49 YSPEXl5kExPQCfTJt1FjnCSuTC4IOMQQPfuralBQfr4DokDXK5892npt5DAFor5
50 k60GpHlRPFBAoxJhK0TaSimL6yAZ0fZo380nrVRDZKlug/lVeXF/2h1TeZc73utt
51 k5sqewqTQ04NhrBp0Udybmf2L5BJh1ctoH490PIOHEbmVDE0WALEXliqsuE2rmm
52 Mr10MRRls22BpX2WSqw90IrmPWI3fds2kE2S1DvuaNcc7B8W0hgWT3HxnyuMTyZi
53 b6Yf7hb5F2ZSOpHFU1b222tqk4qouEigyoaUZaLcVhV5UdBCCvwyU19yU6+EscnM
54 Ww==
55 -----END CERTIFICATE-----
```

CUPS Certificate

Root Certificate



carriage return

Pacchetto certificati CUPS

Eseguire il push dei certificati bundle creati in precedenza nel server CMS tramite WinSCP.

Name	Size	Type	Name	Size	Changed	Rights	Owner
..		Parent director	c2wip.key	198 KB	5/16/2020 3:44:38 PM	r--r--r--	admin
cupbun.cer	4 KB	Security Certifi	CA.cer	198 KB	8/17/2021 9:36:00 PM	r--r--r--	admin
cucmbun.cer	4 KB	Security Certifi	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

Copia del bundle di certificati nel CMS

Assegnare il certificato del bundle TOMCAT su Callbridge utilizzando `callbridge ucm certs <cert-bundle>`.

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

Trust certificato Callbridge

Assegna certificato bundle server CUP su Callbridge tramite `callbridge imps certs <cert-bundle>`.

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

Eseguire il `callbridge` comando per verificare se i bundle di certificati sono assegnati.

```

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>

```

Controllo certificato trust Callbridge

Accedere a CUCM come amministratore CM, passare a User Management > User Settings > Access Control Group, fare clic su Add New e creare un gruppo di controllo di accesso CUCM_AXL_Group.

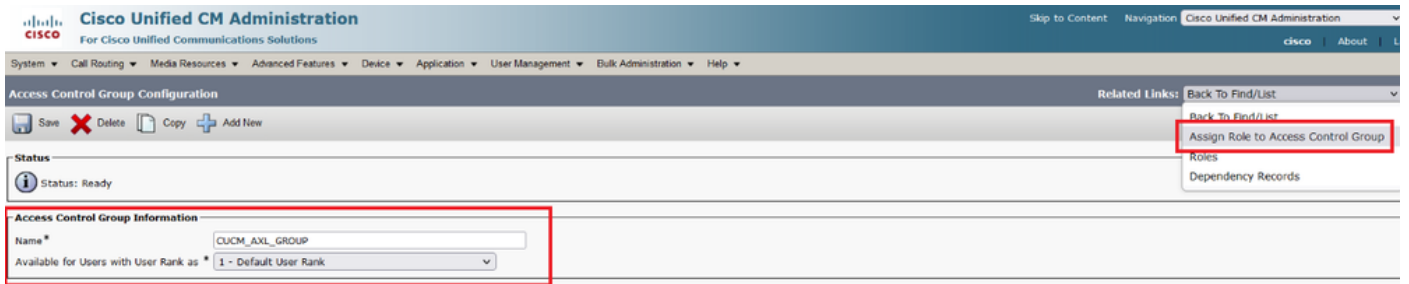
The screenshot shows the Cisco Unified CM Administration web interface. The page title is "Access Control Group Configuration". The "Status" section shows "Status: Ready". The "Access Control Group Information" section is highlighted with a red box and contains the following fields:

- Name***: CUCM_AXL_GROUP
- Available for Users with User Rank as***: 1 - Default User Rank

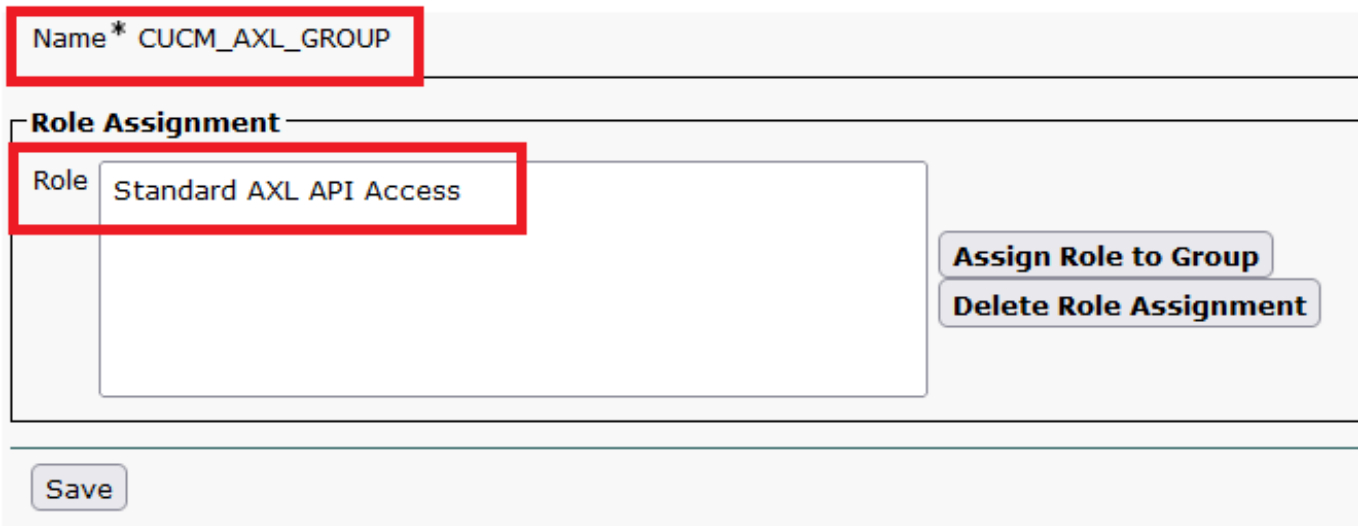
There is a "Save" button at the bottom left of the configuration area. A note at the bottom indicates that an asterisk (*) indicates a required item.

Creazione di un gruppo AXL

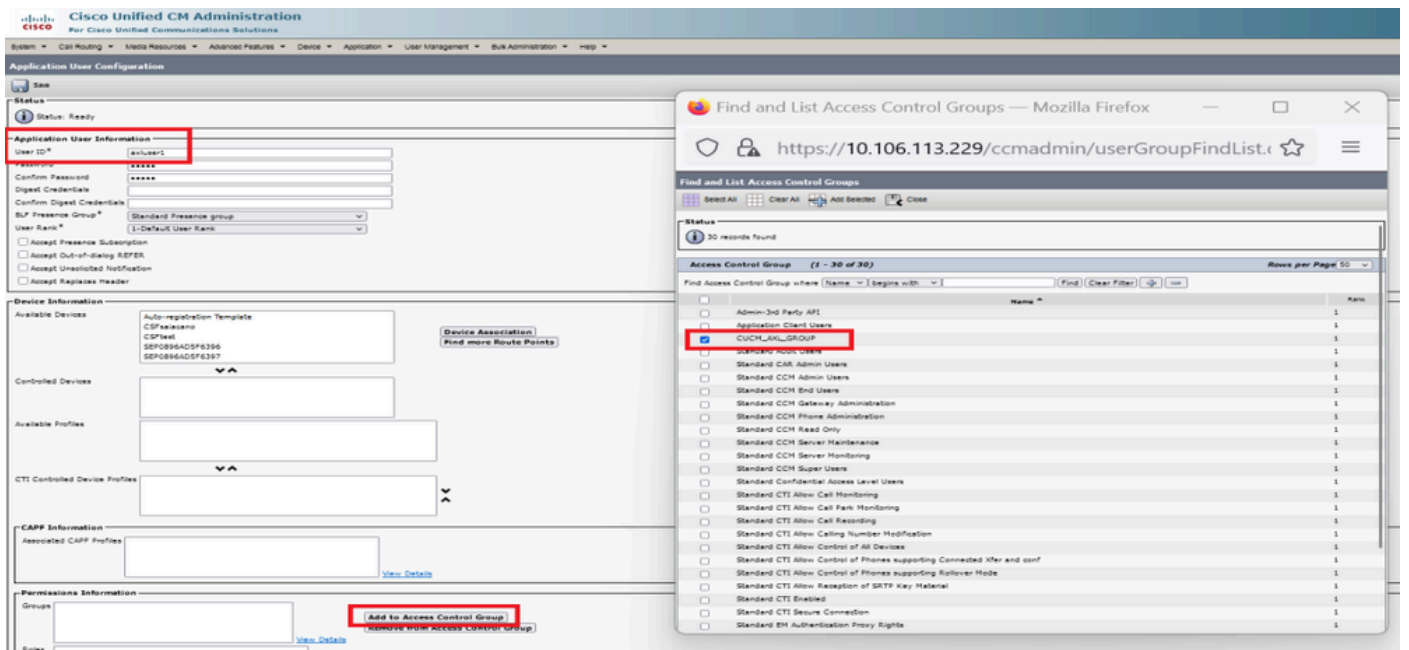
Assegnare il ruolo Standard AXL API Access al gruppo di controllo di accesso creato in precedenza.



Assegnazione dell'accesso API al gruppo AXL

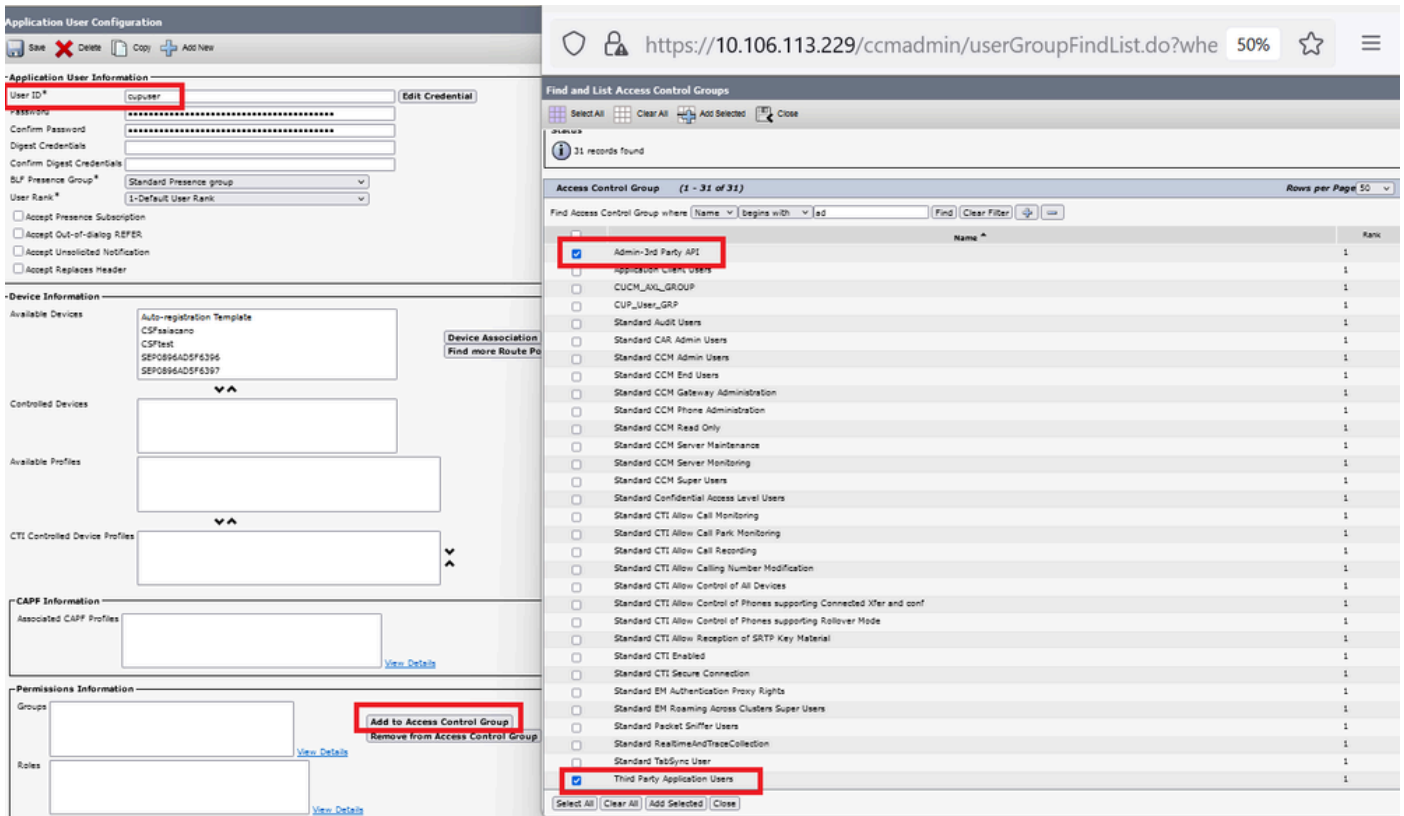


Passare a User Management > Application User, fare clic su Add New e creare un utente applicazione AXLUser. Assegnare quindi il gruppo di controllo di accesso creato in precedenza.



Creazione di un utente e assegnazione di un gruppo AXL

Creare un utente CUP e assegnare i due ruoli seguenti: Third Party Application Users e Admin-3rd Party API.

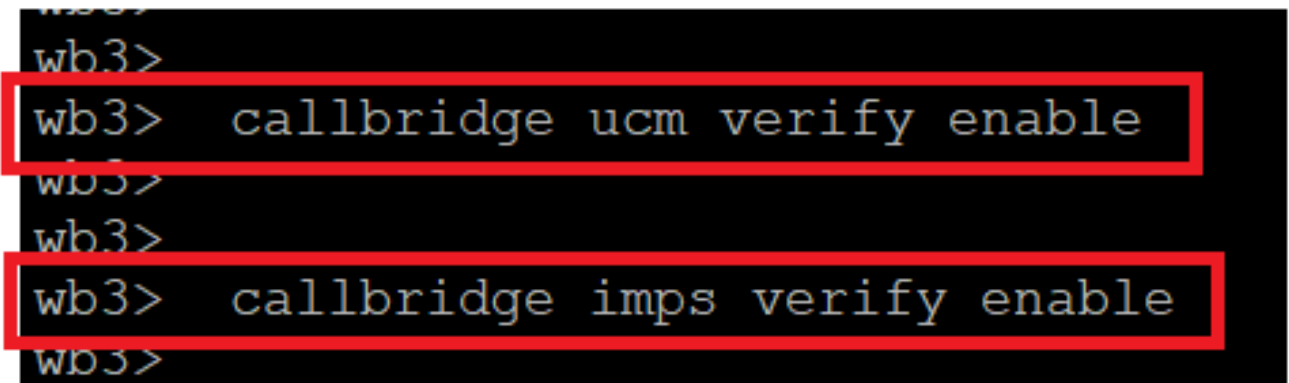


Creazione utente CUP

Abitare la verifica dei certificati per i certificati CUCM e Cisco Unified Communications Manager IM & Presence Service (IMPS) sul CMS utilizzando:

callbridge ucm verify <enable/disable>

callbridge impv verify <enable/disable>



Callbridge verifica i certificati CUCM e CUPS

Verificarlo eseguendo il callbridge comando.

```

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>

```

Controllo dei comandi di Callbridge

Aggiungere ora il nome di dominio completo (FQDN) CUCM e l'utente **AXL** e **CUPS** creati in precedenza su CMS using callbridge ucm add <hostname/IP> <axl_user> <presence_user>.

axl_user = utente AXL su CUCM

presence_user = Utente CUP creato in precedenza

```

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>

```

Aggiunta di CUCM a Callbridge

Ora, verificare se CMS considera attendibili i servizi CUCM con l'aiuto di:

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>

```

Stato AXL Callbridge

```
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>
```

Stato presenza Callbridge

I servizi disponibili consentono a CUCM e CMS di considerarsi reciprocamente attendibili per i servizi AXL e Presence.

Nota:

CUCM ha utenti Lightweight Directory Access Protocol (LDAP) sincronizzati e anche aggiornati su CUPS. Gli utenti devono avere lo stesso ID utente dell'app Web e Jabber JID e devono essere connessi all'app Web con lo stesso ID utente, per poter aggiornare la presenza in Jabber.



Configurazione specifica CUCM per la condivisione della presenza tra Webapp e client Jabber

Per CUCM deve essere configurato LDAP.

Sistema LDAP:

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
- LDAP Attribute for User ID

Configurazione LDAP CUCM 1

Directory LDAP:

LDAP Directory Related Links: [Back to](#)

LDAP Directory Information

LDAP Configuration Name*
 LDAP Manager Distinguished Name*
 LDAP Password*
 Confirm Password*
 LDAP User Search Base*
 LDAP Custom Filter for Users
 Synchronize* Users Only Users and Groups
 LDAP Custom Filter for Groups

LDAP Directory Synchronization Schedule

Perform Sync Just Once
 Perform a Re-sync Every* DAY
 Next Re-sync Time (YYYY-MM-DD hh:mm)*

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

Configurazione LDAP CUCM 2

Autenticazione LDAP

Configurazione LDAP CUCM 1 Configurazione LDAP CUCM 1 Configurazione LDAP CUCM 1

LDAP Authentication

Status

Status: Ready

LDAP Authentication for End Users

Use LDAP Authentication for End Users
 LDAP Manager Distinguished Name*
 LDAP Password*
 Confirm Password*
 LDAP User Search Base*

LDAP Server Information

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

Configurazione LDAP CUCM 3

Utenti estratti da LDAP in CUCM con Mail-ID configurato:

End User Configuration

Save
 Delete
 Add New
 Revoke Refresh Token

Status

Status: Ready

User Information

User Status: Active Enabled LDAP Synchronized User
 User ID*: test
 Self-Service User ID:
 PIN: [Edit Credential](#)
 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:

Utenti in CUCM

Utente CUCM aggiornato sul server CUPS:

Navigation: Cisco Unified CM IM and Presence Administration

System Presence Messaging Application Bulk Administration Diagnostics Help

Presence Topology

- DefaultCUPSSubcluster
 - impnew.test.com (2) users
- All Unassigned Users (0)
- All Assigned Users (2)

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	DefaultCUPSSubcluster
test2	test2	2	test2@test.com	test2@test.com		impnew.test.com	DefaultCUPSSubcluster

Utenti in CUPS

La stessa directory LDAP è configurata anche nel CMS. Il database utenti viene estratto e sincronizzato su CMS.

Users

Filter

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
testz	testz@test.com	testz@test.com
user 1	user1@saml.com	user1@saml.com

Utenti CMS

Ora, poiché è già stato verificato che il sistema CMS può considerare attendibile CUCM, è possibile procedere con il test della presenza.

```

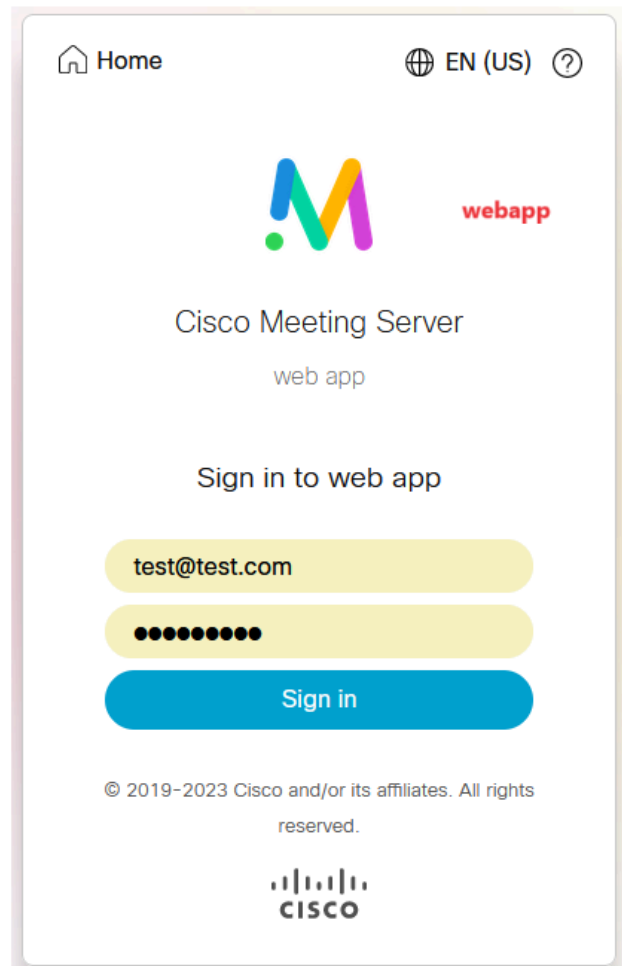
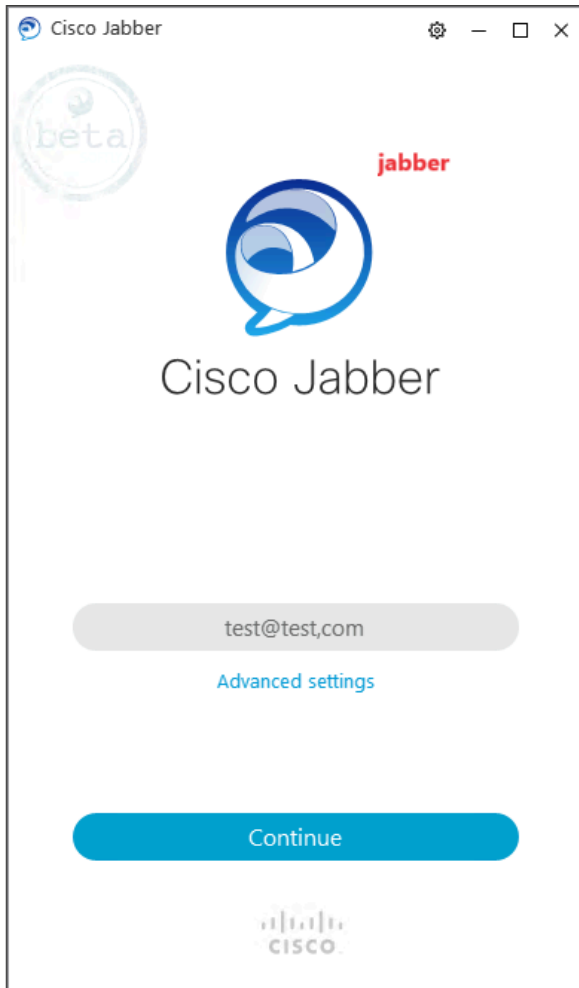
wb3>
wb3> callbridge ucm add <hostname/IP> <axl_user> <presence_user>
Only 1 UCM node is allowed. Delete existing UCM node to add a new UCM node.
wb3> callbridge ucm add cucml4test.test.com axluser cupuser
Enter axl user password:
Enter presence user password:
UCM node updated successfully. Restart the callbridge for changes to take effect.
wb3>
wb3> █

```

Aggiunta di CUPS e CUCM a CMS

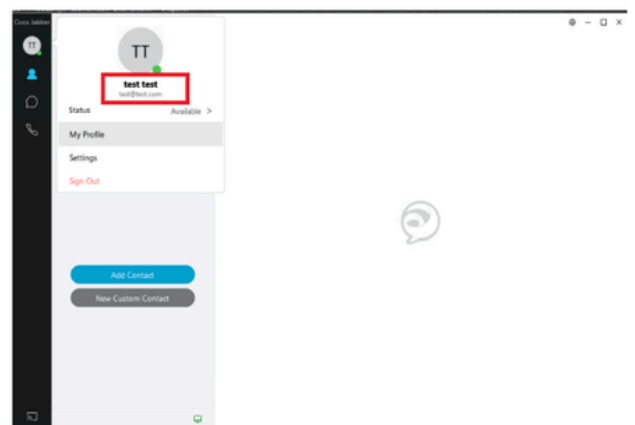
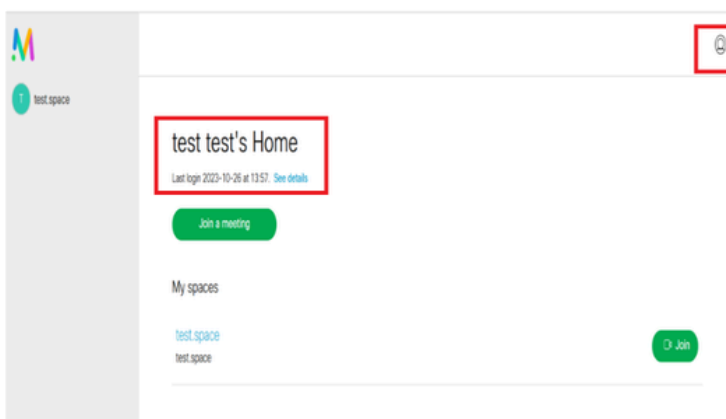
Verifica

Firmato su due client con lo stesso utente (sincronizzato dallo stesso LDAP):

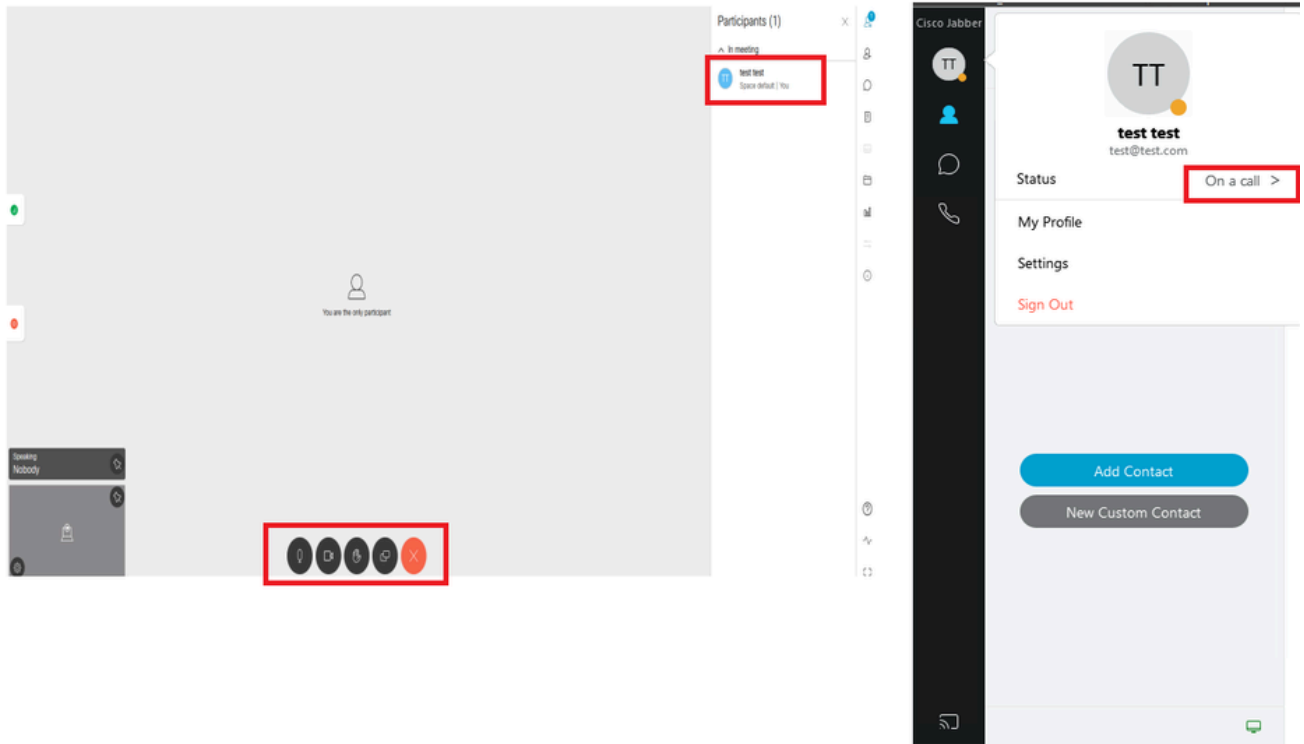


Accesso utente in Jabber e webapp

Entrambi i client hanno eseguito l'accesso allo stesso utente test@test.com.



Presenza in Jabber e Webapp prima della chiamata



Lo stato della presenza cambia quando la chiamata viene aggiunta da webapp

Quando un utente Jabber accede all'app Web e si unisce a una riunione, il server di riunione aggiorna lo stato di Jabber su 'In una riunione, In una chiamata' e torna allo stato precedente dopo che l'utente ha terminato la riunione. Ad esempio, se lo stato dell'utente su Jabber mostra 'Disponibile', viene aggiornato a 'In riunione, In chiamata' quando si è in riunione con un'app Web. Quando l'utente abbandona la riunione, lo stato di Jabber viene impostato nuovamente su 'Disponibile'. Se l'utente Jabber partecipa a un'altra riunione/chiamata mentre partecipa alla riunione dell'app Web, il Meeting Server non aggiorna lo stato di Jabber. Se l'utente Jabber ha impostato il proprio stato su 'DND - Non disturbare' prima di partecipare alla riunione dell'app Web, Meeting Server non aggiorna lo stato di Jabber. Se l'utente aggiorna manualmente lo stato di Jabber in qualsiasi momento durante la riunione dell'app Web, Meeting Server non ignora lo stato dell'utente aggiornato manualmente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).