

Activer la communication sécurisée entre CMS et CUCM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Activation de la communication sécurisée entre CMS et le serveur CUCM/IMP](#)

[Configuration spécifique CUCM pour le partage de présence entre Webapp et Jabber Client](#)

[Vérifier](#)

Introduction

Ce document décrit comment activer la communication entre Cisco Meeting Server (CMS) et Cisco Unified Communications Manager (CUCM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CMS version 3.8 et ultérieure
- CUCM et IM&P
- Jabber

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMS version 3.8
- CUCM et 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit le processus d'établissement d'une communication sécurisée entre CMS et CUCM pour le partage de présence Jabber/Web app. Il explique en détail les étapes de configuration et de dépannage de l'état de mise à jour des utilisateurs Jabber pendant les téléconférences Web sur l'application sur le CMS. Le serveur de téléconférence peut être configuré afin de mettre à jour l'état de présence des utilisateurs Jabber lorsqu'ils sont engagés dans une téléconférence d'application Web Cisco Meeting Server.

Configurer

Activation de la communication sécurisée entre CMS et le serveur CUCM/IMP

Connectez-vous à CUCM sur la page d'administration du système d'exploitation, accédez à Security > Certificate Management et téléchargez le certificat 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
CAFF-trust	Cisco_Basic_Assurance_Root_CA_2099_01a65af15ee994e8e1	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
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
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
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
ipsec	cucm14test.test.com_6dffacfb16e53663f3d9af4a66335758	Identity	Self-signed	RSA	cucm14test.test.com	cucm14test.test.com	09/30/2028	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY_cucm14test_77caa7891d68be201eff4e1e038db166	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_496beedc456be08f40ff7716b999d3a4	Identity	Self-	EC	cucm14test.test.com	cucm14test-EC.test.com	09/30/2028	Self-signed certificate generated by system

Certificat CUCM Tomcat

Connectez-vous à Cisco Unified Presence Server (CUPS) sur la page d'administration du système d'exploitation, accédez à Security > Certificate Management, puis téléchargez le certificat 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

Certificat Presence CUPS

Téléchargez le certificat d'autorité de certification racine qui a signé le certificat Tomcat et 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)

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 488baed0456ba0b40f7716999d41a1	Trust	Self-signed	EC	cuom1dtest.test.com	cuom1dtest-EC.test.com	09/30/2028	Trust Certificate
tomcat-trust	S-WIN2008R2-CA_04738d12017d07d7f59a9a7381b2d388e	Trust	Self-signed	RSA	S-WIN2008R2-CA	S-WIN2008R2-CA	09/29/2028	Signed Certificate
tomcat-trust	impnew-impnew.com 38082a2e3808e92801a33095b05883	Trust	Self-signed	RSA	impnew.test.com	impnew-impnew.com	09/30/2028	Trust Certificate
tomcat-trust	cuom1dtest.test.com 26a7386920002000200204	Trust	CA-signed	RSA	cuom1dtest.test.com	S-WIN2008R2-CA	10/04/2025	Trust Certificate
tomcat-trust	impnew-EC.test.com 729a9d72e3fe922487583a1071417e	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

Certificat racine de 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)

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

Certificat racine pour CUPS

Créez un groupe de certificats de CUCM. Un certificat d'ensemble signifie, placer le certificat de serveur au-dessus, le certificat intermédiaire (n'importe lequel) au milieu et le certificat RACINE au bas, suivi d'un (1) retour chariot.

Voici un exemple de certificat BUNDLE :

```
1 -----BEGIN CERTIFICATE-----
2 MIIFqgCCBjOgAwIBAgIKNqYeYAAAAAABDANBqkqhkiG9w0BAQsFADBBMRMwEQYK
3 CZImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUGA1UEAxMOUy1X
4 SU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMyNzE2WncNMjUxMDA0MTMyNzE2WjBXMQsw
5 CQYDVQQGEwJlZEMMAQGA1UECMBDQ2FyMQswCgYDVQQHEwNpbmQxZjAMBGNVBAOT
6 BWNpc2NvMRswGgYDVQQDEkxjZWNTMTR0ZXN0LnRlc3QuY29tMIIBIjANBgkqhkiG
7 9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAoYE9an27hV05JUwAEwutEY5RA4WwaxIvkqEI
8 ah0fDpRI2GgY+mrH9q70hAvG3uDYBtBHKYJpkYepeULNjZkh07a39IeeJMG8/q28
9 SckZ+j1VIyw8gt+cnG6E6ibCD+HNdtKfwL0ipSdlTnlieX6DsF05Z1K4Alm4yrsN
10 +b0/wSikfV0+ValyC90nbTCUCIKGvqvqGadiyndb6TRfhi+w4RD+0NgOBjWHqcXX
11 WXgp9JWYQdy7YeX8Y2kljBAyRhSPfa35hojy470hE91N8axmHRm2m5htqeE0kSOy
12 2o09pj7f7Aq1wVAFvPQCxkl2sXtZARHpGdswpm4M8r5MoXPtWIDAQABo4ICjTCC
13 AokwDgYDVR0PAAQ/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
14 AjAoBgNVHREEITAfghh0ZXN0LmNvbYITy3VjbTE0dGVudC50ZXN0LmNvbTAdBgNV
15 HQEFQgQUTMTpsuTu05EBH2wgGf6qii7M38wHwYDVR0jBBgwFoAUA6L6fIQ4Vp+QI
16 UDz/X6MwFAVhJ4IwgcgGA1UdHwSBwDCBwTCBuqCBt6CBtIaBsWakYXA6Ly8vQ049
17 Uy1XSU4yMDA4UjItQ0EwQ049V01OMjAwOFIyLENOPUNEUCxDTj1lQdWJsaWMM1MjBL
18 ZXklMjBTZXJ2aWNlcykDTj1lTXJ2aWNlcyskDTj1lDb25maWdlcmF0aW9uLERDPVMS
19 REM9Y29tP2N1cnRpZmljYXRlUmV2b2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFs
20 csljUkxEXN0cmliidXRpb25Qb21udDCBugYIKwYBBQUHAQEEdga0wgaowgacGCCsG
21 AUFBAChOgabGRhcDovLy9DTj1lTLVdJTj1lMDhSMlDQ3sDTj1BSUESQ049UHVh
22 bGljJTlW2V5JTlW2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
23 bixEQslTLERDPWNvbT9jQUN1cnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M5Y2V5
24 dG1maWNhdGlvbkf1dGhvcml0eTA9BgkkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQcE
25 yrsWhcnoHIXEjS6B5uhFhsusPgeGpusehts3XAIBZAIbAjAnBgkkrBgEEAYI3FQcE
26 GjAYMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMCMAoGCCsG8Ib3DQEBcUAA4IBAQCQ
27 hREe6ZJHVx1N7JNgY0RE4V9S3FiyQPIVYFVEdaKAL+AfV1S214D7ohFIjL5rSA
28 ThWiFFS1w1eA5Cjlg9gi2leHI2uDuor6XEXKWB/bkC9BXoDkRMFV7bh9CoosFmXk8
29 r6xeN7H9cAHAs3wFILUnAip1KF/7odBkNUSgT39NJAL1UgVFPt81r6lk8OR5TAYI
30 9vs4dw5ocQzs7Z0Av8ZDRNFDTsWoOGtU2dCMIXasJ05ALmMBtagqYBNj16URkR8i
31 f2sOkb+NdPZD4XAE00tW8rji124ukr7JBgeWYsjsD2tsZsJgslMprNaVuMDh280Q
32 JQFAiCOp3GgYjkJBZcH2
33 -----END CERTIFICATE-----
34 -----BEGIN CERTIFICATE-----
35 MIIDXTCCAkwGwIBAgIQDXWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADBB
36 MRMwEQYKCC2ImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUGA1UE
37 AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMyNzE2WncNMjUxMDA0MTMyNzE2WjBXMQsw
38 WjBEMRMwEQYKCC2ImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUG
39 A1UEAxMOUy1XSU4yMDA4UjItQ0EwEwgEiMA0GC8qG8Ib3DQEBAAUAA4IBDwAwggEK
40 AoIBAQCXa6tjSyoUyn6GkoSbe98SasKRUNGbCORKni41tWEiX0vPITEsqZUPRJq4
41 7C8useeDiJFUBWAY9e8F4nm+VhGSEKqkwekrlJAF1mV4hkypkR0Wz64b4y04Ln8e
42 3E/F6/SXA6HOHQHdy1qlQMWSA/PXB441GKbSnfA4pjTB8nMP5WL+iBruYH9tX6EJ
43 IJq5Fe+RZYNH/mLuB+0Qf1OCn4sqsx2Gf8DxhJNHU+2m3q7h319exxioDcwiVwZO
44 xqUKrvBs6jBtOg4Kvs3sa4AHyP91SAA2vp42MwtBdis8O3wx+vm/HoVr0fHum/W1
45 Z92iwR9Jx44tKoJHVpBwMvnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjaPBGNV
46 HRMBAf8EBTADAQH/MB0GA1UdDgQWBBERovp8hDhWn5AhQ0s9fosAUBWEngjaQBgkr
47 BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEA5nsa91K4BISCAuBgMMe
48 YSPEXl5kEXPQcFtJt1FjnC5uTC4IOMQQFfuralBQfr4DokDXK5892npt5DAFors5
49 k60GpH1bRPBaoxJhR0Ta3imL6yAZ0f2o380nrVRDZKlug/1VeXF/2hlTeZc73utt
50 k5sqewqTQ04NHrBp0Udybmpf2L5BjhlctoH490PI0HEbmVDE0WALKXliqsuEzrmm
51 mrl0MRRlS2ZBpX2W3qw90IrmPW13fde2kE2S1DvuaNcc7B8W0hgWT3HnyuMTyZi
52 b6Yf7hb5F3Z3OpHFU1b222tqk4qouEigyaaUZaLcVhV5UdBCCvwyU19yU6+EscnM
53 Ww==
54 -----END CERTIFICATE-----
55
```

Server Certificate on TOP

CUCM TOMCAT CERT

Root certificate at bottom



just 1 carriage return

Ensemble de certificats Tomcat

Créer un ensemble de certificats de CUPS. Un certificat d'ensemble signifie, placer le certificat de serveur au-dessus, le certificat intermédiaire (n'importe lequel) au milieu et le certificat RACINE au bas, suivi d'un (1) retour chariot.

```
1 -----BEGIN CERTIFICATE-----
2 MIIFqTCCBjGgAwIBAgIKNrMm8gAAAAAABTANBgkqhkiG9w0BAQsFADEBMMRMEQYK
3 C2ImiZPyLQGBGRYDY29tMREwDwYKZC2ImiZPyLQGBGRYBUeEXMBUGA1UEAxMOUy1X
4 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
5 CQYDVQQGEwJlEOMAwGA1UECmFmZ2FybmExDDAKBgNVBAcTA2JnbDEOMAwGA1UE
6 CmFY21sY28xDDAKBgNVBAcTA2t0c3EYMBYGA1UEAxMPaW1wbmV3LnRlc3QuY29t
7 MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKHb9jzWYhi6i4IkSx8hC
8 Z1USLZHBQ28RDQw1vT3CFGZut+dayK9KshYtsOAhRfWLPWgGtABJWMr98f+DM0RG
9 FsmCtNo1ZsEOqSQCRC6b/kbQuC+6LhhgIM8I448tLaAF4neZ/5dmCUSzJNCpnbpH
10 EbqbXKkH8V42BZLeLP0T2savk5V+vriGuMjV299vGrEu49kB0EN2M+mnfcnf20xT5
11 wtFqCY9jijKSKC40cu6iJ88A7Hi/yJQJ1NeUmnLpGpF/HKUrclu5pBdfiV1EXBk8
12 LX2bm49PFGRS0guxJZVC457vmAgACgKvwE5s3HvW1t3Tp1WE4AZtSn3z9tsYSOC7
13 bwIDAQABO4ICfzCCAnsWHDYDVR01BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMA4G
14 A1UdDwEe/wQEAwIFoDAAEgNVHREEEzARgg9pbXBu2XcudGVsdC5jb20wHQYDVR0O
15 BBEYFOxvmV/jdcIDMEVOjzWR/yRAo9ktMB8GA1UdIwQYMBaAFGi+nyEOfafkCFA7
16 Pl+jMBQFYSeCMIHIBgNVHR8EgcAwgb0wgbqggbbeggb3GgbFsZGFwOi8vL0NOFVMe
17 V01OMjAwOFIyLUNBLENOFVdJTjIwMDhSMixDTj1DRFAzQ049UHVibGljJTJwS2Vt
18 JTIwU2VydmljZXMzQ049U2VydmljZXMzQ049Q29uZmlndXJhdGlvbixEQs1TLERD
19 FWNvbT9jZkxJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9
20 Y1JMRGlzdHJpYnV0aW9uUG9pbmQwgb0GCCsGAQUFBwEBB1IGtMIGqMIGnBggrBgEF
21 BQcwAoaBmmxkYXA6Ly8vQ049Uy1XSU4yMDA4UjItQ0EzQ049QU1BLENOFVBlYmcp
22 YyUyMEtleSUyMFN1cnZpY2VsLENOPVN1cnZpY2VsLENOPUNvbmZpZ2VYXRpb24s
23 REM9UyxEQs1jb20/Y0FDZkxJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNsPWN1cnRp
24 ZmljYXRpb25EeXRob3JpdHkwPQYJKwYBBAGCNxUHBDAAwLgYmKwYBBAGCNxUIhcq7
25 FoXJ6ByFwY0ugeboRyBLSz4HhqbRbHobc91wCAWQCAQIwJwYJKwYBBAGCNxUKBBow
26 GDAKBggrBgEFBQcDATAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAUJdy
27 3mM0FwGwLW4hiShn/XCPChLMPG54IE+EINTBqsoqxs12XLl1do0JjNAI7Xd+FoAGQ
28 UXRjRN3q326yiY5C2itLe/aVpclC5Yn6krL/8PEEnBmopubQVdqRUCbn4r21iNV
29 sNcBrUeOY0Vr2/EVeBObVh1DGowfrxMj59v40k15wYc88h0bopL1I/Sc2mpw5m2Z
30 R5nyyx3XfjkmZSwwMnO+Suz7dbJu2zfI6sw0EhF12tRRQHCsq9n9uQDSUXCjQFdq
31 Y3A+LJGawlAuPt4+sqOxjYKYNP8m8+WIBIUEv+oXAOVbz8ffQFoPKYf/ZmWxB-JRP
32 2v/At0ns31UdcKFUPw==
33 -----END CERTIFICATE-----
34 -----BEGIN CERTIFICATE-----
35 MIIDXTCCAkwgAwIBAgIQDXWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADEB
36 MRMwEQYKZC2ImiZPyLQGBGRYDY29tMREwDwYKZC2ImiZPyLQGBGRYBUeEXMBUGA1UE
37 AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
38 CQYDVQQGEwJlEOMAwGA1UECmFmZ2FybmExDDAKBgNVBAcTA2JnbDEOMAwGA1UE
39 CmFY21sY28xDDAKBgNVBAcTA2t0c3EYMBYGA1UEAxMPaW1wbmV3LnRlc3QuY29t
40 A1UEAxMOUy1XSU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
41 AoIBAQCXa6tj8yOUyn6GkoSbe98Sas3KrUNGBCORKnI41tWEiX0vPITEsqZUPRJq4
42 7C8useeDiJPUBWAY9e8F4nm+VhGSEKqkwekr1JAF1mV4hkypxR0Wz64b4yO4Ln8e
43 3E/F6/SXA6HOqHDylq1QWWSA/PXB441GKb8nfa4pjTBSnMP5WL+iBruYHp9tX6EJ
44 IJq5Fe+RZYnh/mLuB+0Qf1OCn4sqsqzGf8DxhJNHU+2m3q7h319exxioDcwiVwZO
45 xqUKRvBs6jBtOg4Kvs3sa4AHyP91SAA2vp42MwtBdis803wx+vm/HoVr0fHum/W1
46 Z92iwR9Jx4tK0JHVpBwMvnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAWIBhjaFBGjNV
47 HRMBAF8EBTADAQH/MB0GA1UdDgQWBBr0vp8hDhWn5AhQOz9fosAUBWEngjaQBgkr
48 BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAU5nsa91K4BISCAuBgmMe
49 YSPEXl5kExPQCfTJt1FjnCSuTC4IOMQQFfuralBQfr4DokDXK5892npt5DAFor5
50 k60GpHlBRPBAoxJhK0TaSimL6yAZ0fZ0380nrVRDZKlug/lVeXF/2h1TeZc73utt
51 k5sqewqTQO4NhrBp0Udybmf2L5BJh1ctoH490PIOHEbmVDE0WALEKXliqsuE2rmm
52 Mr10MRRLs22BpX2WSqw90IrmPWI3fds2kE2S1DvuaNcc7B8W0hgWT3HxnyuMTyZi
53 b6Yf7hb5F2ZSOpHFU1bZ22tqk4qouEigyoaUZaLcVhV5UdBCCvwyU19yU6+EscnM
54 Ww==
55 -----END CERTIFICATE-----
```

CUPS Certificate

Root Certificate



carriage return

Bundle de certificats CUPS

Transférez les certificats d'ensemble créés précédemment vers le serveur CMS via 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

Copie du lot de certificats dans CMS

Attribuez un certificat d'ensemble TOMCAT sur Callbridge à l'aide de `callbridge ucm certs <cert-bundle>`.

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

Cert Trust Callbridge

Attribuez un certificat d'ensemble de serveurs CUP sur Callbridge à l'aide de `callbridge imps certs <cert-bundle>`.

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

Exécutez cette `callbridge` commande afin de vérifier si les groupes de certificats sont attribués.

```
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>
```

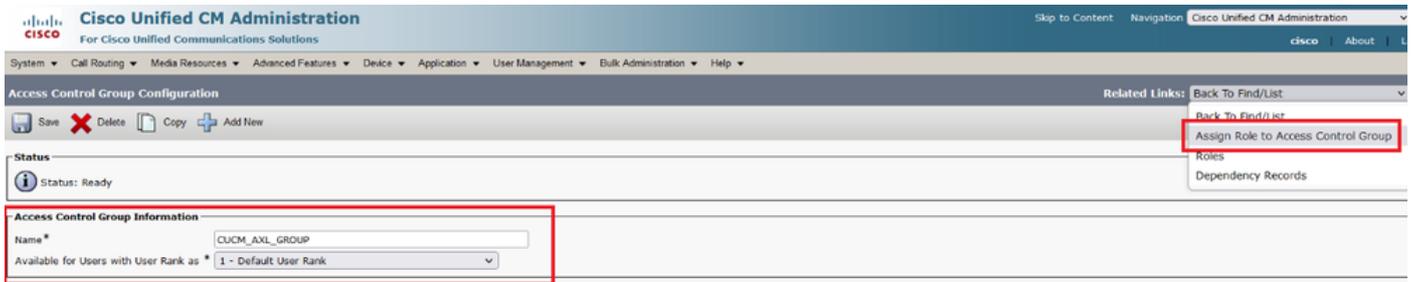
Vérification du certificat de confiance Callbridge

Connectez-vous à CUCM en tant qu'administrateur CM, accédez à User Management > User Settings > Access Control Group, cliquez sur Add New et créez un groupe de contrôle d'accès CUCM_AXL_Group.

The screenshot shows the Cisco Unified CM Administration web interface. The breadcrumb navigation is: System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help. The main heading is "Access Control Group Configuration". There is a "Save" button at the top left. The "Status" section shows "Status: Ready". The "Access Control Group Information" section is highlighted with a red box and contains the following fields: "Name*" with the value "CUCM_AXL_GROUP" and "Available for Users with User Rank as*" with a dropdown menu set to "1 - Default User Rank". There is another "Save" button at the bottom left. A note at the bottom states: "* - indicates required item."

Création du groupe AXL

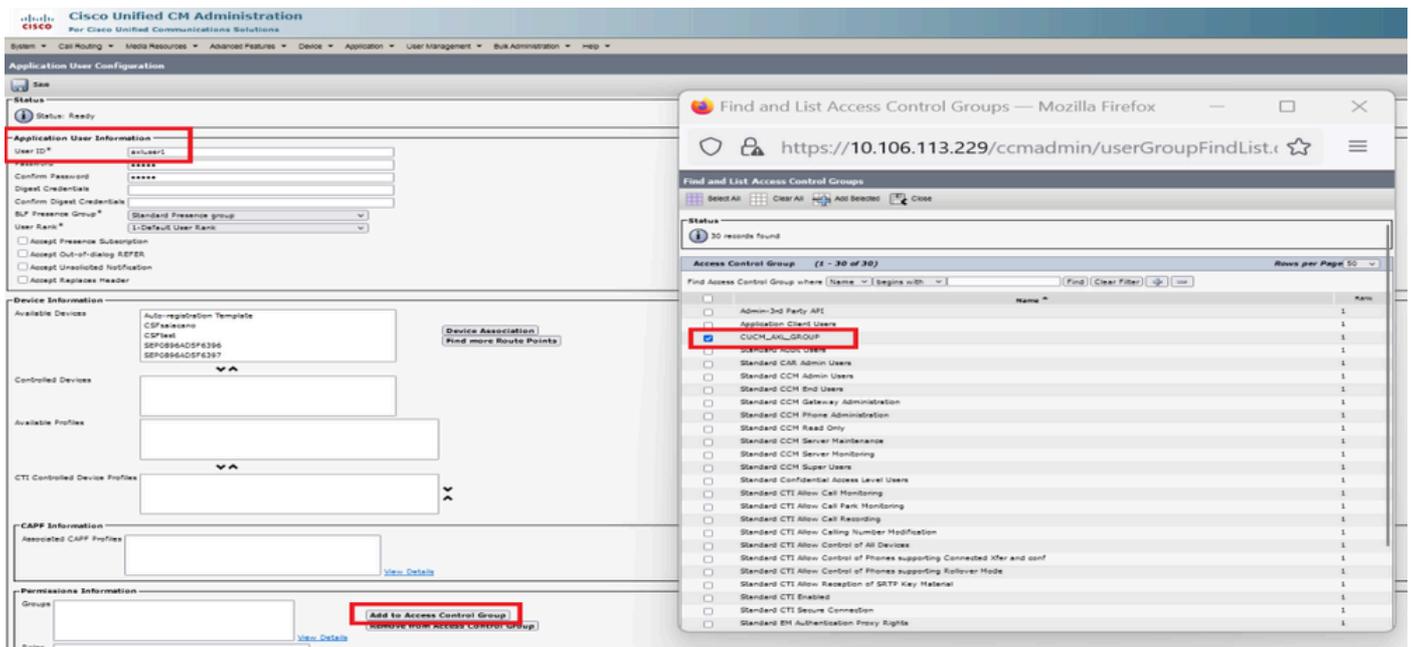
Attribuez le rôle Standard AXL API Access au groupe de contrôle d'accès créé précédemment.



Attribution d'un accès API au groupe AXL

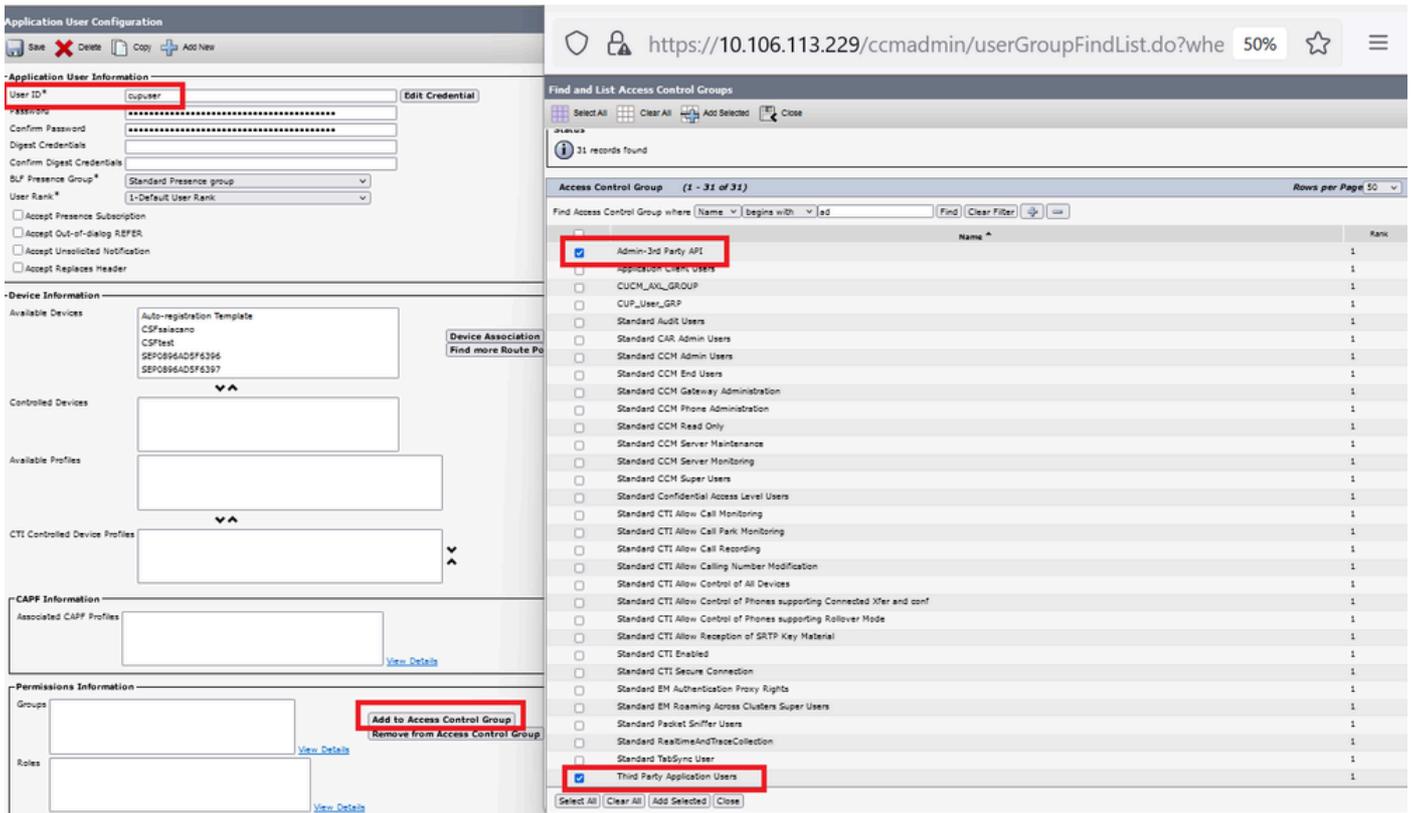


Accédez à User Management > Application User, cliquez sur Add New et créez un utilisateur d'application AXLUser. Attribuez ensuite le groupe de contrôle d'accès, créé précédemment.



Création d'un utilisateur et affectation d'un groupe AXL

Créez un utilisateur CUP et attribuez ces deux rôles : Third Party Application Users et Admin-3rd Party API.

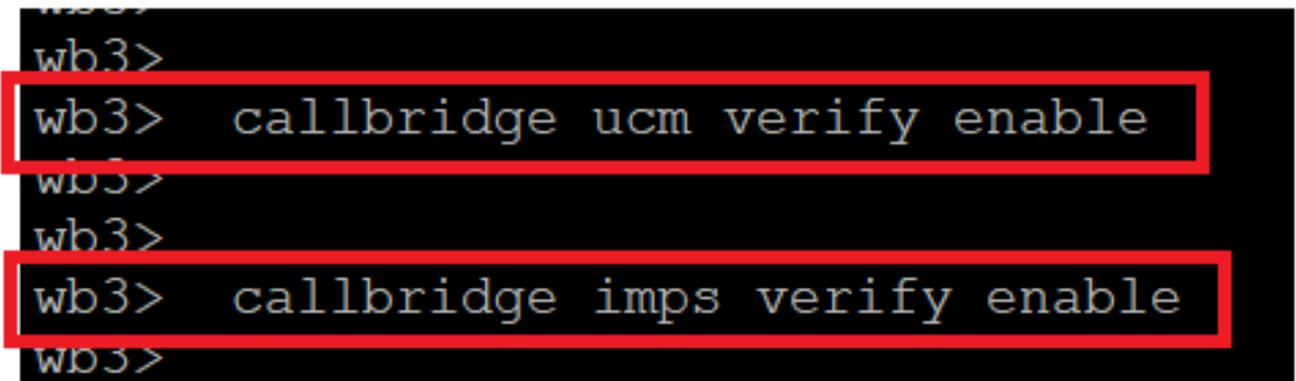


Création d'un utilisateur CUP

Activez la vérification de certificat pour le certificat CUCM et le certificat Cisco Unified Communications Manager IM & Presence Service (IMPS) sur le CMS à l'aide de :

callbridge ucm verify <enable/disable>

callbridge impv verify <enable/disable>



Callbridge vérifie le certificat CUCM et CUPS

Vérifiez-le en exécutant la commande callbridge.

```

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>

```

Vérification de la commande Callbridge

Ajoutez maintenant CUCM Fully Qualified Domain Name (FQDN) et l'utilisateur **AXL** et **CUPS** créés précédemment sur CMS à l'aide de `callbridge ucm add <hostname/IP> <axl_user> <presence_user>`.

`axl_user` = utilisateur AXL sur CUCM

`presence_user` = utilisateur CUP créé précédemment

```

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>

```

Ajout de CUCM à Callbridge

Maintenant, vérifiez si CMS fait confiance aux services CUCM à l'aide de :

`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>

```

État AXL de 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>
```

État de présence Callbridge

Les services disponibles signifient que CUCM et CMS se font mutuellement confiance pour les services AXL et Presence.

Remarque :

CUCM dispose d'utilisateurs LDAP (Lightweight Directory Access Protocol) synchronisés et également mis à jour sur le CUPS. Les utilisateurs doivent avoir le même ID utilisateur d'application Web et le même JID Jabber et doivent être connectés à l'application Web avec le même ID utilisateur pour que la présence soit mise à jour sur Jabber.

Configuration spécifique CUCM pour le partage de présence entre Webapp et Jabber Client

LDAP doit être configuré pour CUCM.

Système 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:

Configuration LDAP CUCM 1

Annuaire 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

Configuration LDAP CUCM 2

Authentication LDAP :

Configuration CUCM LDAP 1 Configuration CUCM LDAP 1 Configuration CUCM LDAP 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

Configuration CUCM LDAP 3

Utilisateurs extraits de LDAP dans CUCM avec ID de messagerie configuré :

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:

Utilisateurs dans CUCM

Utilisateur CUCM mis à jour sur le serveur CUPS :

Navigation: Cisco Unified CM IM and Presence Administration | Go

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 | Find | Clear Filter

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

Utilisateurs dans CUPS

Le même répertoire LDAP est également configuré sur le CMS. La base de données utilisateur est extraite et synchronisée sur 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
testz	testz@test.com	testz@test.com
user 1	user1@saml.com	user1@saml.com

Utilisateurs CMS

Maintenant, puisque vous avez déjà validé que CMS peut faire confiance à CUCM, vous pouvez continuer à tester la présence.

```

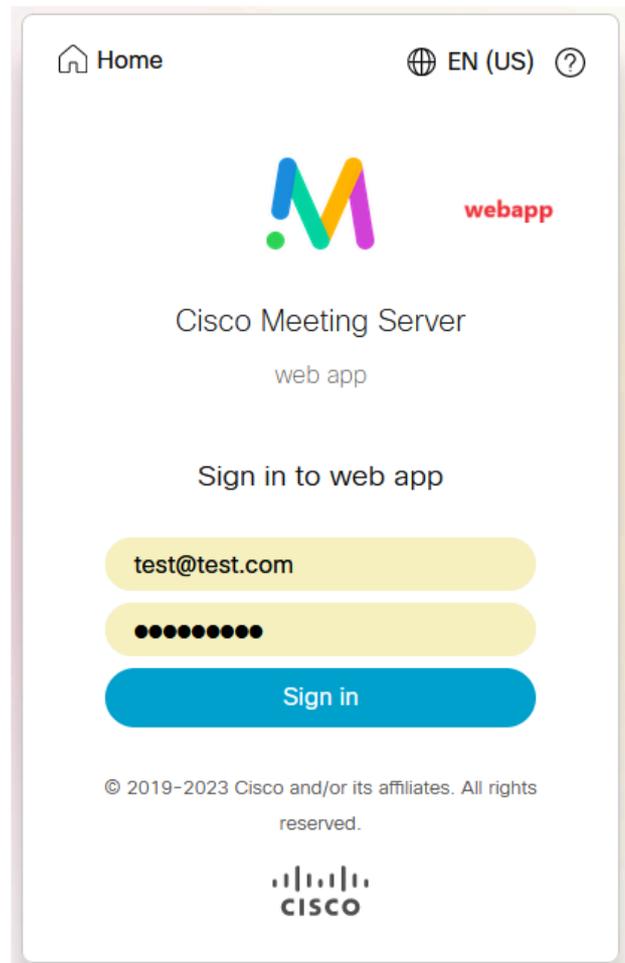
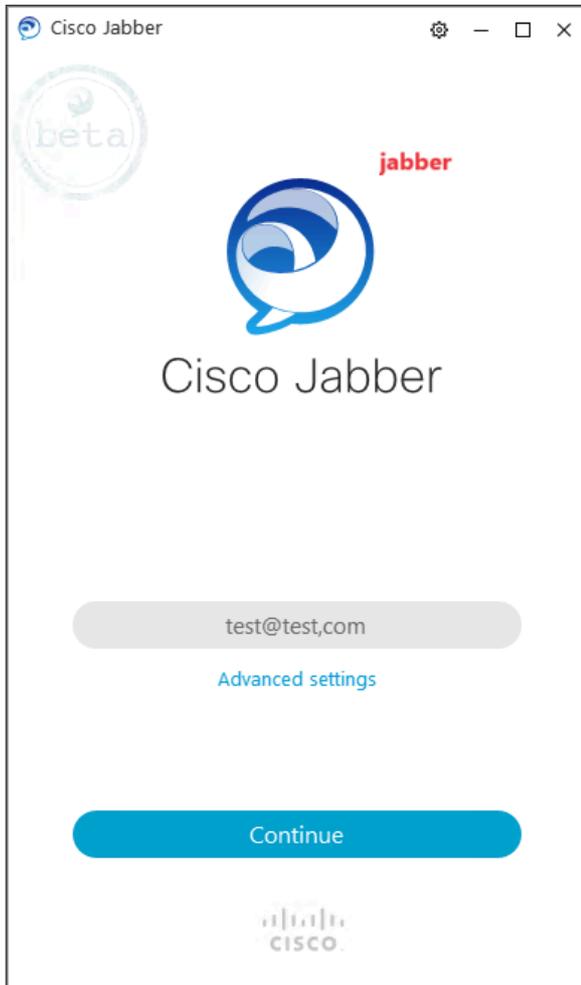
wb3>
wb3> callbridge ucm add <hostname/IP> <axl_user> <presence_user>
Only 1 UCM node is allowed. Delete existing UCM node to add a new UCM node.
wb3> callbridge ucm add cucml4test.test.com axluser cupuser
Enter axl user password:
Enter presence user password:
UCM node updated successfully. Restart the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

```

Ajout de CUPS et CUCM à CMS

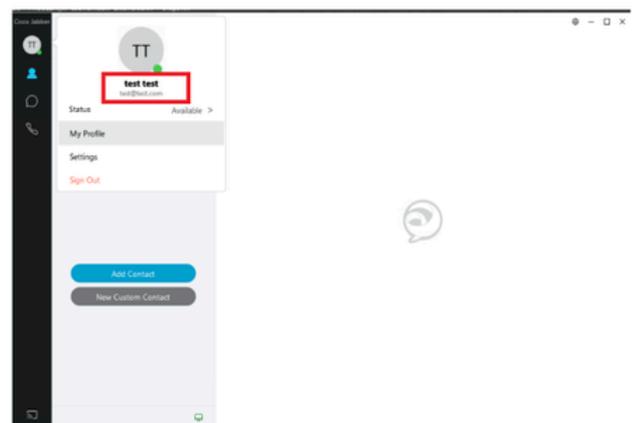
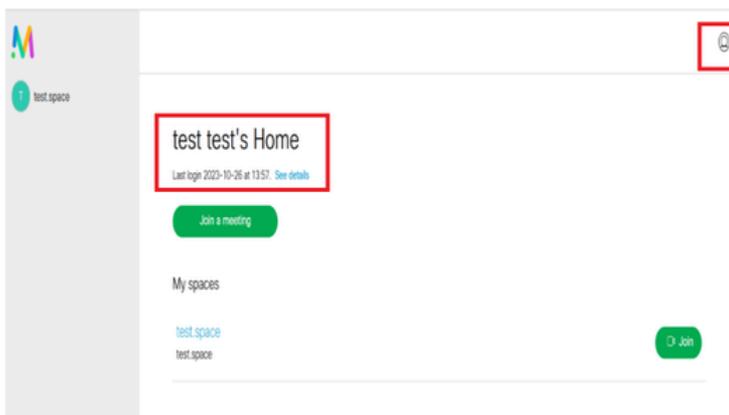
Vérifier

Connecté à deux clients avec le même utilisateur (synchronisé à partir du même LDAP) :

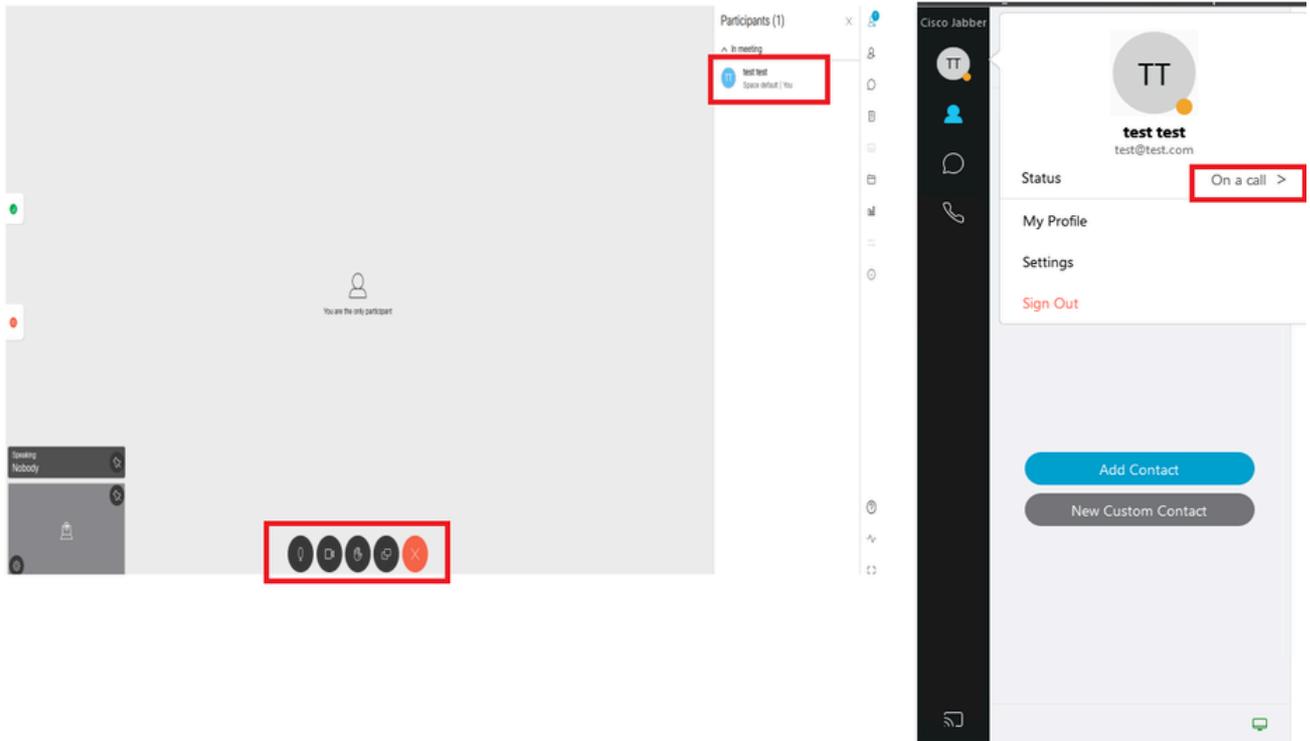


Connexion utilisateur dans Jabber et webapp

Les deux clients se sont connectés au même utilisateur test@test.com.



Présence dans Jabber et Webapp avant l'appel



L'état de présence change lorsque l'appel est joint depuis webapp

Lorsqu'un utilisateur Jabber se connecte à l'application Web et se connecte à une téléconférence, le serveur de téléconférence met à jour l'état Jabber en « En téléconférence, En appel » et revient à son état précédent une fois que l'utilisateur a terminé la téléconférence. Par exemple, si l'état de l'utilisateur sur Jabber est « Disponible », il est mis à jour en « En réunion, En appel » lors d'une téléconférence d'application Web. Une fois que l'utilisateur a quitté la téléconférence, l'état Jabber est de nouveau défini sur Disponible. Si l'utilisateur Jabber se trouve dans une autre téléconférence ou un autre appel alors qu'il se connecte à la téléconférence de l'application Web, Meeting Server ne met pas à jour l'état Jabber. Si l'utilisateur Jabber a défini son état sur « NPD - Ne pas déranger » avant de se connecter à la téléconférence de l'application Web, le serveur de téléconférence ne met pas à jour l'état Jabber. Si l'utilisateur met à jour manuellement l'état Jabber à tout moment pendant la téléconférence de l'application Web, le serveur de téléconférence ne remplace pas l'état utilisateur mis à jour manuellement.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.