

Habilitar comunicação segura entre CMS e CUCM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Habilitando a comunicação segura entre o CMS e o servidor CUCM/IMP](#)

[Configuração específica de CUCM para compartilhamento de presença entre o Webapp e o cliente Jabber](#)

[Verificar](#)

Introdução

Este documento descreve como habilitar a comunicação entre o Cisco Meeting Server (CMS) e o Cisco Unified Communications Manager (CUCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CMS versão 3.8 e posterior
- CUCM e IM&P
- Jabber

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

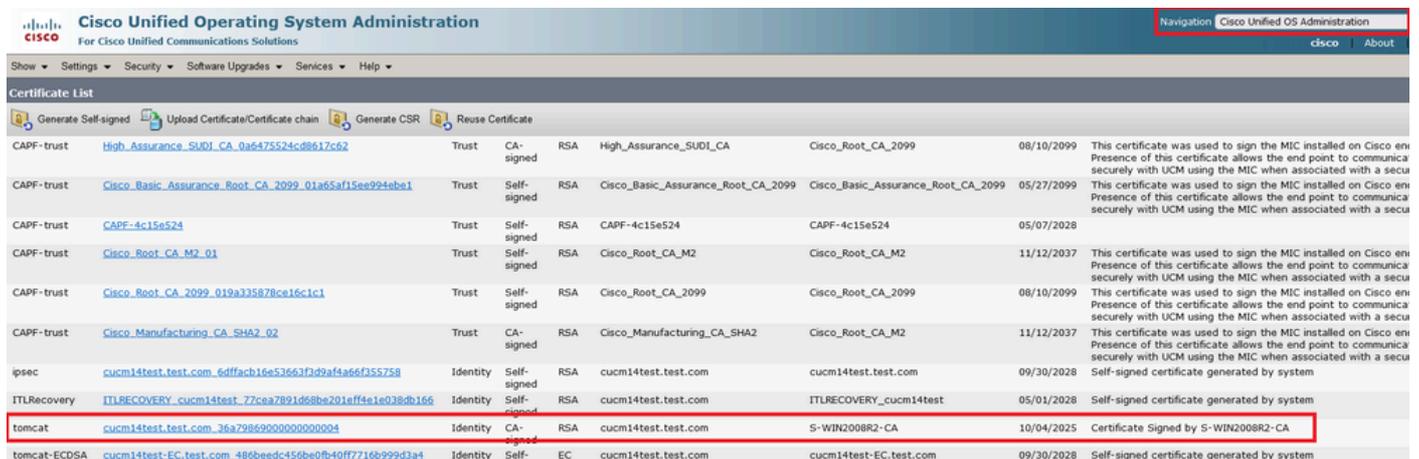
Informações de Apoio

Este documento descreve o processo de estabelecimento de comunicação segura entre o CMS e o CUCM para o compartilhamento de presença do Jabber/aplicativo Web. Ele explica as etapas detalhadas para configurar e solucionar problemas do status de atualização dos usuários Jabber durante as reuniões do aplicativo Web no CMS. O Servidor de Reunião pode ser configurado para atualizar o status de presença de usuários Jabber enquanto eles estão envolvidos em uma reunião do aplicativo Web do Cisco Meeting Server.

Configurar

Habilitando a comunicação segura entre o CMS e o servidor CUCM/IMP

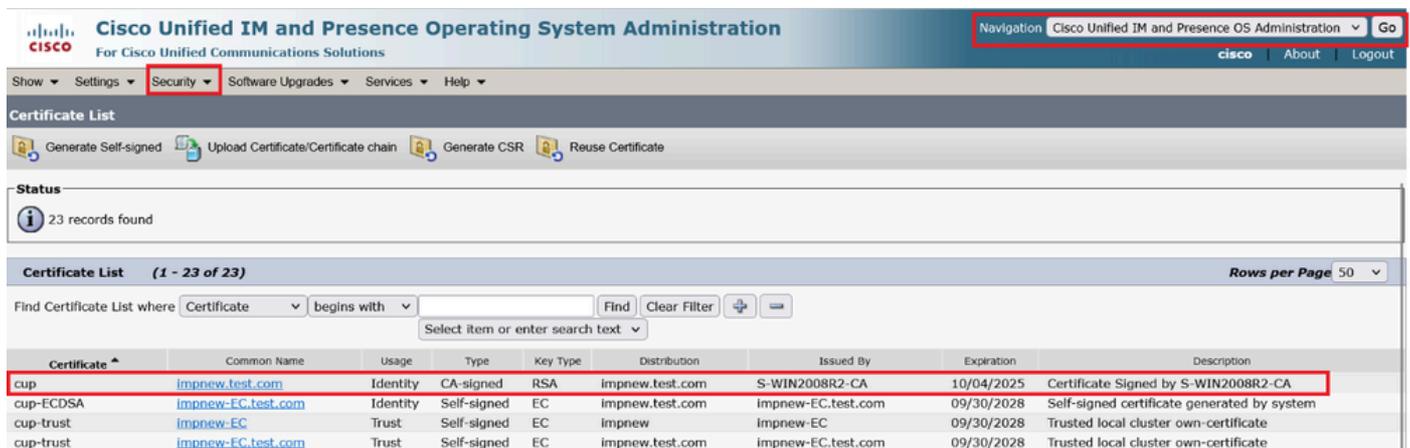
Faça login no CUCM na página de admin do SO, navegue para Security > Certificate Management e baixe o certificado TOMCAT.



Trust	Common Name	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
CAFF-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 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_6dffacfb16e53663f3d9af4a66335758	Identity	Self-signed	RSA	cucm14test.test.com	cucm14test.test.com	09/30/2028	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY_cucm14test_77c0a7891d68be201eff4e1e038db166	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_496beedc456be08d49ff7716b999d3a4	Identity	Self-	EC	cucm14test.test.com	cucm14test-EC.test.com	09/30/2028	Self-signed certificate generated by system

Certificado Tomcat CUCM

Faça login no Cisco Unified Presence Server (CUPS) na página de administração do SO, navegue para Security > Certificate Management e baixe o certificado 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

Certificado CUPS de presença

Faça o download do Certificado de CA RAIZ que assinou o certificado Tomcat e Cup.

Cisco Unified Operating System Administration

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_04738d12017d07d7f59a9a7381b03288e	Trust	Self-signed	RSA	S-WIN2008R2-CA	S-WIN2008R2-CA	09/29/2028	Signed Certificate
tomcat-trust	impnew-impnew.com 38082a2e380808e3807a33083d05883	Trust	Self-signed	RSA	impnew.test.com	impnew-impnew.com	09/30/2028	Trust Certificate
tomcat-trust	cuom1dtest.test.com 26a738692000200020024	Trust	CA-signed	RSA	cuom1dtest.test.com	S-WIN2008R2-CA	10/04/2025	Trust Certificate
tomcat-trust	impnew-EC.test.com 779a9d72e3fe922487583a1071417e	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

Certificado raiz de Tomcat

Cisco Unified IM and Presence Operating System Administration

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

Certificado raiz para CUPS

Crie um pacote de certificados de CUCM. Um certificado de pacote significa, colocando o certificado do servidor no topo, o certificado intermediário (qualquer um) no meio e o certificado de RAIZ na parte inferior, seguido de um (1) retorno de carro.

Aqui está um exemplo para o certificado BUNDLE:

```
1 -----BEGIN CERTIFICATE-----
2 MIIFqgCCBjOgAwIBAgIKNqYeYAAAAAABDANBqkqhkiG9w0BAQsFADBBMRMwEQQYK
3 CZImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUGA1UEAxMOUy1X
4 SU4yMDA4UjItQ0EwHhcNMjMxMjA0MTMyNzE2WncNMjUxMjA0MTMyNzE2WjBXMQsw
5 CQYDVQQGEwJlZEMMAQGA1UECMBDQ2FyMQwwCgYDVQQHEwNpbmQxZjAMBGNVBAOT
6 BWNpc2NvMRswGgYDVQQDEkxjZWNtMTR0ZXN0LnRlc3QuY29tMIIBIjANBgkqhkiG
7 9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAoYE9an27hV05JUwAEwutEY5RA4WwaxIvkqEI
8 ah0fDpRI2GgY+mrH9q70hAvG3uDYBtBHKYJpkYepeULNjZkh07a39IeeJMG8/q28
9 SckZ+j1VIyw8gt+cnG6E6ibCD+HNdtKfwL0ipSdlTnlieX6DsF05Z1K4Alm4yrsN
10 +b0/wSikfV0+ValyC90nbTCUCIKGvqvqGadiyndb6TRfhi+w4RD+0NgOBjWHqcXX
11 WXgp9JWYQdy7YeX8Y2kljBAyRhSPfa35hojy470hE91N8axmHRm2m5htqEe0kSOy
12 2o09pj7f7Aq1wVAfVpQCxkl2sXtZARHpGdswpm4M8r5MoXPtWIDAQABo4ICjTCC
13 AokwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQMBQGCCsGAQUFBwMBBggrBgEFBQcD
14 AjAoBgNVHREEITAfghh0ZXN0LmNvbYITy3VjbTE0dGVudC50ZXN0LmNvbTAdBgNV
15 HQ4EFgQUTMTpsuTu05EBH2wgGf6qii7M38wHwYDVR0jBBgwFoAUA6L6fIQ4Vp+QI
16 UDz/X6MwFAVhJ4IwgcgGA1UdHwSBwDCBwTCBuqCBt6CBtIaBsWakYXA6Ly8vQ049
17 Uy1XSU4yMDA4UjItQ0EwQ049V010MjAwOFIyLENOPUNEUCxDTj1lQdWJsaWMM1MjBL
18 ZXklMjBTZXJ2aWNlcysxDTj1lTXJ2aWNlcysxDTj1lDb25maWdlcmF0aW9uLERDPVMS
19 REM9Y29tP2N1cnRpZmljYXRlUmV2b2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz
20 csljUkxEXX0cmliidXRpb25Qb2ludDCBugYIKwYBBQUHAQEEdga0wgaowgacGCCsG
21 AQUFBsAChOGabGRhcDovLy9DTj1lTLVdJTj1lMDhSM1lDQ3xDTj1lBSUESQ049UHVl
22 bGljJTlW2V5JTlW2V5dmljZXMxQ049U2V5dmljZXMxQ049Q29uZmlndXJhdGlv
23 bixEQslTLERDPWNvbT9jQUN1cnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M5Y2V5
24 dG1maWNhdGlvbkf1dGhvcml0eTA9BgkkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQcE
25 yrsWhcnoHIXEjS6B5uhFhsusPgeGpusehts3XAIBZAIbAjAnBgkkrBgEEAYI3FQcE
26 GjAYMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMCMAoGCCsG8Ib3DQEBcUAA4IBAQCQ
27 hREe6ZJHVx1N7JNgY0RE4V9S3FiyQPIVYFVEdaKAL+AfvlS214D7ohFIjL5rSA
28 ThWiFFS1w1eA5Cjlg9gi2leHI2uDuor6XEXKWB/bkC9BXoDkRMFV7bh9CoosFmXk8
29 r6xeN7H9cAHAs3wFILUnAip1KF/7odBkNUSgT39NJAL1UgVFPt81r6lk8OR5TAYI
30 9vs4dw5ocQzs7Z0Av8ZDRNfDTsWoOGtU2dCMIXasJ05ALmMBtagqYBNj16URkR8i
31 f2sOkb+NdPZD4XAE00tW8rji124ukr7JBgeWYsjsD2tsZsJgslMprNaVuMDh280Q
32 JQFAiCOp2GgYjkJBZcH2
33 -----END CERTIFICATE-----
34 -----BEGIN CERTIFICATE-----
35 MIIDXTCCAkwGwIBAgIQDXWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADBB
36 MRMwEQQYKCC2ImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUGA1UE
37 AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjMxMjA0MTMyNzE2WncNMjUxMjA0MTMyNzE2WjBXMQsw
38 WjBEMRMwEQQYKCC2ImiZPyLQGBGRYDY29tMREwDwYKCC2ImiZPyLQGBGRYBUzEXMBUG
39 A1UEAxMOUy1XSU4yMDA4UjItQ0EwEwgEiMA0GC8qG8Ib3DQEBAAUAA4IBDwAwggEK
40 AoIBAQCXa6tjSyoUyn6GkoSbe98SasSKrUNGbcCORKni41tWEiX0vPITEsqZUPRJq4
41 7C8useeDiJFUBWAY9e8F4nm+VhGSEKqkwekrlJAF1mV4hkypkR0Ws64b4y04Ln8e
42 3E/F6/SXA6HOqHDylq1QMWSA/PXB441GKbSnfA4pjTBSnMP5WL+iBruYH9tX6EJ
43 IJq5Fe+RZYNH/mLuB+0Qf1OCn4sqsx2Gf8DxhJNHU+2m3q7h319exxioDcwiVwZO
44 xqUKrvBs6jBtOg4Kvs3sa4AHyP91SAA2vp42MwtBdis8O3wx+vm/HoVr0fHum/W1
45 Z92iwR9Jx44tKoJHVpBwMvnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNV
46 HRMBAf8EBTADAQH/MB0GA1UdDgQWBBERovp8hDhWn5AhQ0s9fosAUBWEngjAQBgkr
47 BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEA5nsa91K4BI3CAuBgMMe
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

Pacote de certificado Tomcat

Crie um pacote de certificados CUPS. Um certificado de pacote significa, colocando o certificado do servidor no topo, o certificado intermediário (qualquer um) no meio e o certificado de RAIZ na parte inferior, seguido de um (1) retorno de carro.

```
1 -----BEGIN CERTIFICATE-----
2 MIIFqTCCBjGgAwIBAgIKNrMm8gAAAAAABTANBgkqhkiG9w0BAQsFADEBMMRMwEQYK
3 CZImiZPyLgQBGRYDY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
4 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
5 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
6 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
7 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
8 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
9 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
10 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
11 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
12 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
13 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
14 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
15 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
16 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
17 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
18 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
19 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
20 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
21 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
22 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
23 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
24 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
25 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
26 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
27 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
28 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
29 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
30 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
31 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
32 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
33 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
34 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
35 -----END CERTIFICATE-----
```

CUPS Certificate

```
1 -----BEGIN CERTIFICATE-----
2 MIIDXTCCAkWgAwIBAgIQDKWNEgF8t79Jqac4Gz04jjANBgkqhkiG9w0BAQsFADEB
3 MRMwEQYKZCZImiZPyLgQBGRYDY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UE
4 AxMOUy1XSU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0Wj
5 BjMQswCQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
6 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
7 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
8 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
9 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
10 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
11 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
12 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
13 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
14 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
15 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
16 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
17 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
18 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
19 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
20 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
21 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
22 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
23 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
24 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
25 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
26 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
27 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
28 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
29 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
30 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
31 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
32 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
33 CQYDVQQGEwJlY29tMREwDwYKZCZImiZPyLgQBGRYBUeEXMBUGA1UEAxMOUy1X
34 SU4yMDA4UjItQ0EwHhcNMjM5MDA0MTMzOTU0WhcNMjUzMDA0MTMzOTU0WjBjMQsw
35 -----END CERTIFICATE-----
```

Root Certificate



carriage return

Pacote de certificado CUPS

Envie por push os certificados de pacote criados anteriormente para o servidor 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

Copiando o pacote de certificados para o CMS

Atribua o certificado de pacote TOMCAT no Callbridge usando `callbridge ucm certs <cert-bundle>`.

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

Callbridge cert trust

Atribua o certificado do pacote de servidor CUP no Callbridge usando `callbridge imps certs <cert-bundle>`.

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

Execute o `callbridge` comando para verificar se os pacotes de certificados estão atribuídos.

```
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>
```

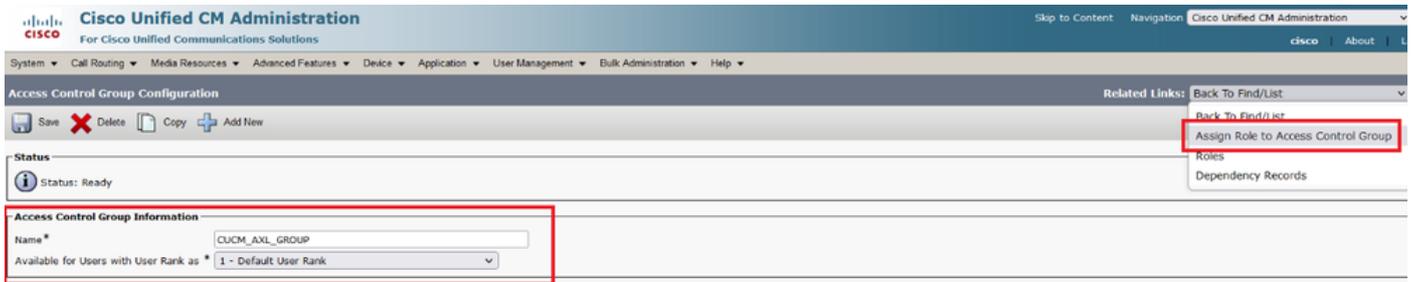
Verificação de certificado de confiança do Callbridge

Faça login no CUCM como Administrador do CM, navegue até User Management > User Settings > Access Control Group, clique em Add New e crie um Grupo de controle de acesso CUCM_AXL_Group.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Access Control Group Configuration'. Below this, there is a 'Save' button and a 'Status' section showing '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 of the form. A note at the bottom left states '* - indicates required item.'

Criando grupo AXL

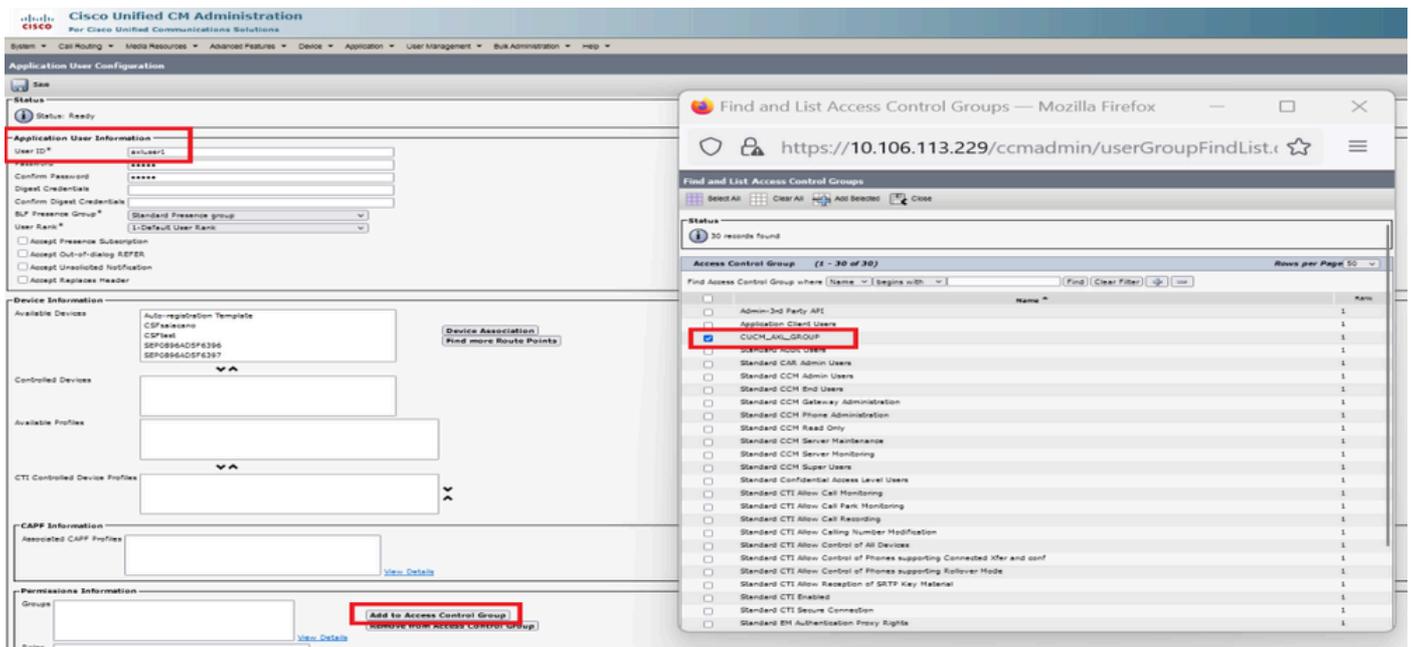
Atribua a função Standard AXL API Access ao Grupo de Controle de Acesso criado anteriormente.



Atribuição de acesso de API ao grupo AXL

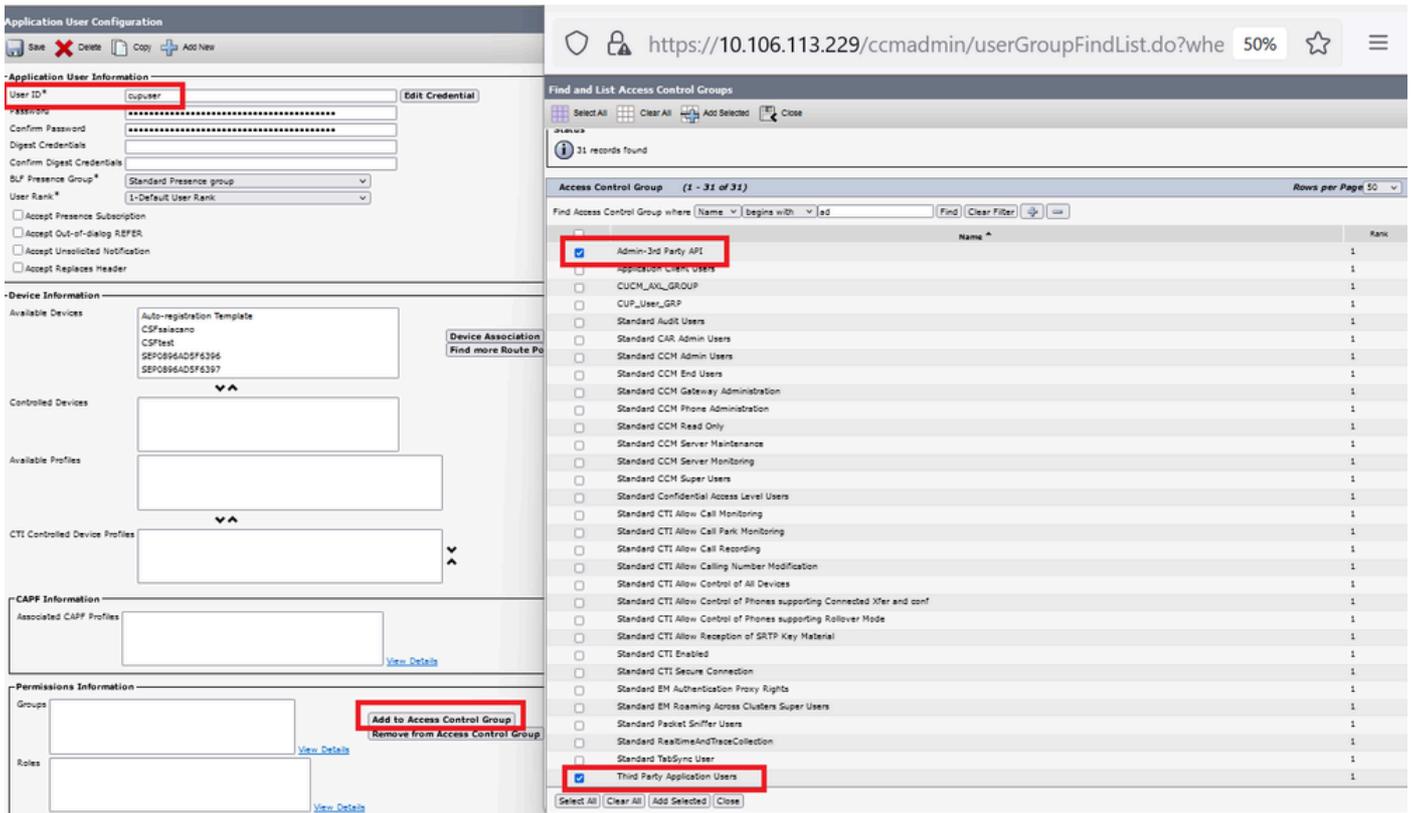


Navegue até User Management > Application User, clique em Add New e crie um Usuário de aplicativo AXLUser. Em seguida, atribua o grupo de controle de acesso, que foi criado anteriormente.



Criando um usuário e atribuindo um grupo AXL

Crie um usuário CUP e atribua estas duas funções: Third Party Application Users e Admin-3rd Party API.



Criando usuário CUP

Habilite a verificação de certificado para o CUCM e o certificado do Cisco Unified Communications Manager IM & Presence Service (IMPS) no CMS usando:

callbridge ucm verify <enable/disable>

callbridge impv verify <enable/disable>

```

wb3>
wb3> callbridge ucm verify enable
wb3>
wb3>
wb3> callbridge impv verify enable
wb3>
  
```

Verificação do certificado CUCM e CUPS pelo Callbridge

Verifique-o executando o comandocallbridge.

```

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>

```

Verificação de comando de ponte de chamada

Agora, adicione o CUCM Fully Qualified Domain Name (FQDN) e o usuário AXL e o CUPS criados anteriormente no CMS usando callbridge ucm add <hostname/IP> <axl_user> <presence_user>.

axl_user = usuário AXL no CUCM

presence_user = usuário do CUP criado anteriormente

```

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>

```

Adicionando CUCM ao Callbridge

Agora, verifique se o CMS confia nos serviços do CUCM com a ajuda de:

callbridge ucm <hostname/IP> axl_service status

callbridge ucm cucml4test.test.com axl_service status

```

wb3> callbridge ucm cucml4test.test.com axl_service status
Axl service available.
wb3>

```

status AXL do 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>
```

Status de presença do Callbridge

Os serviços disponíveis significam que o CUCM e o CMS confiam uns nos outros para os serviços AXL e Presence.

Note:

O CUCM tem usuários do protocolo LDAP sincronizados e também atualizados no CUPS. Os usuários devem ter a mesma ID de usuário do aplicativo Web e Jabber JID e devem estar conectados ao aplicativo Web com a mesma ID de usuário, para que a presença seja atualizada no Jabber.

Configuração específica de CUCM para compartilhamento de presença entre o Webapp e o cliente Jabber

O CUCM deve ter o LDAP configurado.

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

Configuração LDAP do CUCM 1

Diretório LDAP:

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

Save Delete Copy Perform Full Sync Now Add New

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

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)* 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

Configuração LDAP do CUCM 2

Autenticação LDAP:

Configuração LDAP do CUCM 1 Configuração LDAP do CUCM 1 Configuração LDAP do CUCM 1

LDAP Authentication

Save

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* 389

Use TLS

Configuração LDAP do CUCM 3

Usuários extraídos do LDAP para o CUCM com ID de e-mail configurada:

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:

Usuários no CUCM

Usuário do CUCM atualizado no servidor 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

Usuários no CUPS

O mesmo Diretório LDAP também é configurado no CMS. O banco de dados do usuário é recebido e sincronizado no 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

Usuários CMS

Agora, como você já validou que o CMS pode confiar no CUCM, você pode continuar com o teste de Presença.

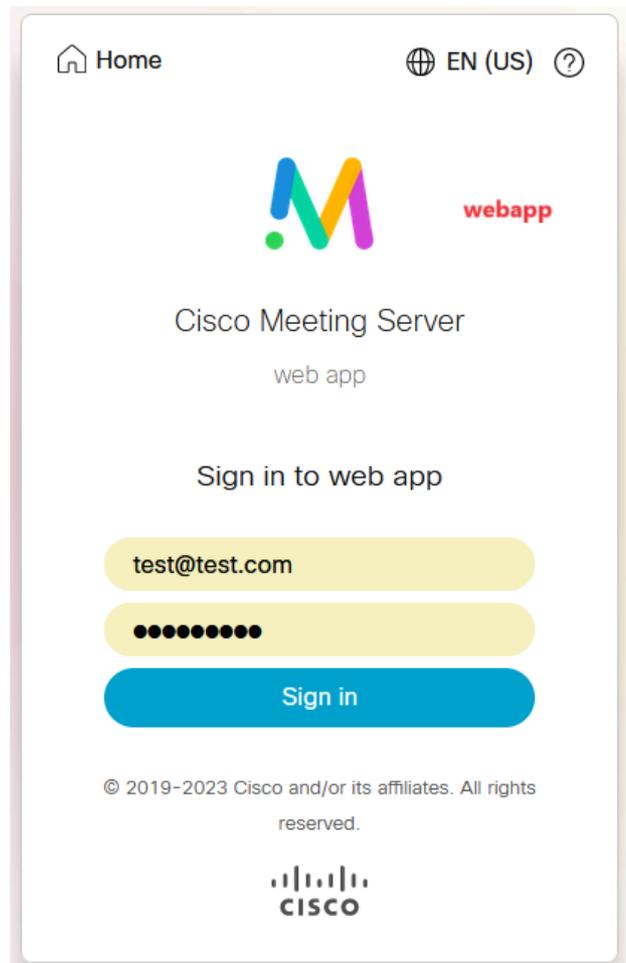
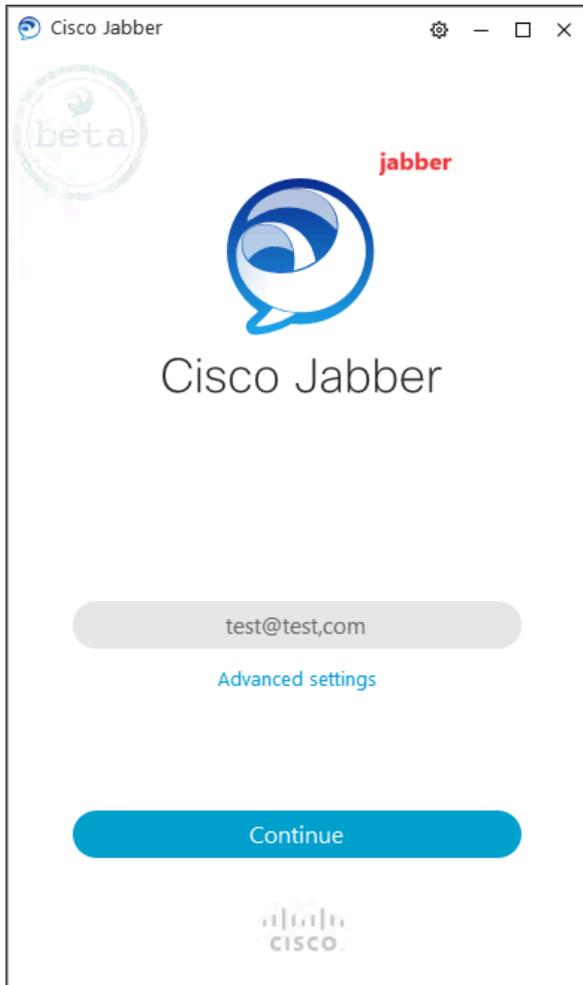
```

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> █
  
```

Adicionando CUPS e CUCM ao CMS

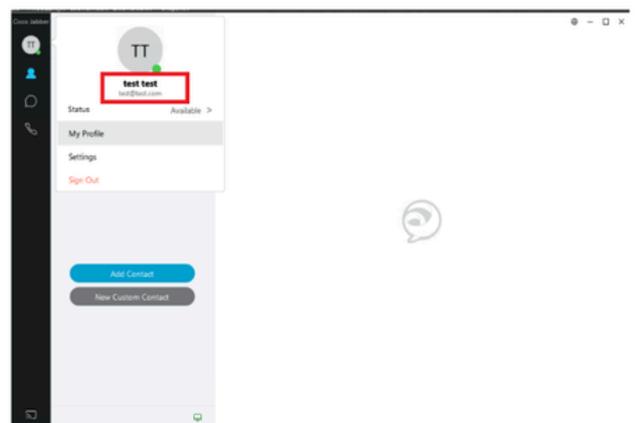
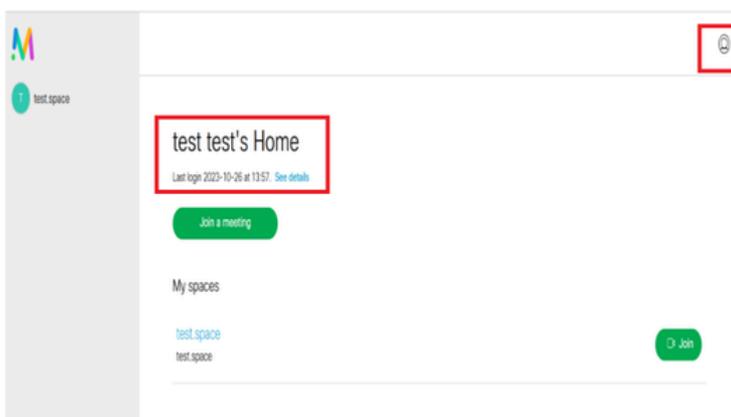
Verificar

Conectado em dois clientes com o mesmo usuário (sincronizado do mesmo LDAP):

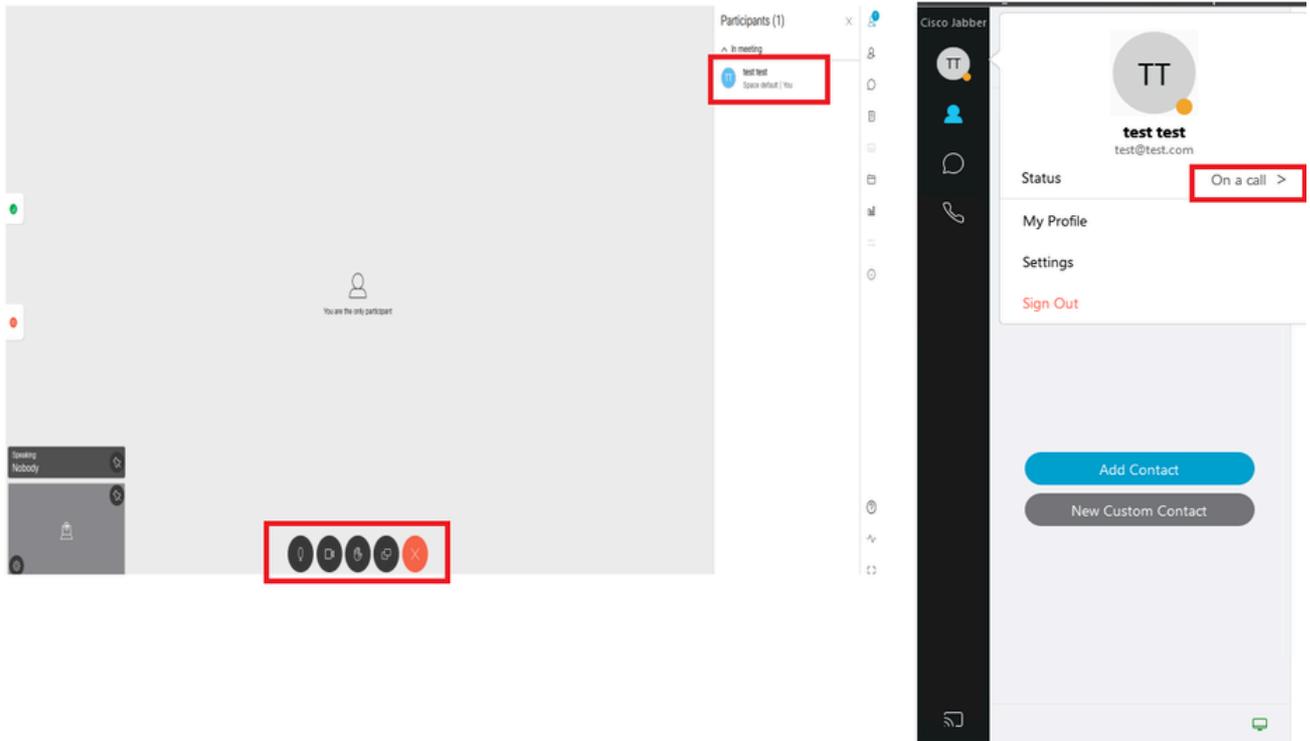


Login do usuário no Jabber e no webapp

Ambos os clientes entraram no mesmo usuário test@test.com.



Presença no Jabber e no Webapp antes da chamada



O status de presença muda quando a chamada ingressa do aplicativo Web

Quando um usuário do Jabber entra no aplicativo Web e ingressa em uma reunião, o Servidor de Reunião atualiza o status do Jabber para 'Em uma reunião, Em uma chamada' e reverte para o status anterior após o usuário terminar a reunião. Por exemplo, se o status do usuário no Jabber for 'Disponível', ele será atualizado para 'Em uma reunião, Em uma chamada' quando estiver em uma reunião do aplicativo Web. Depois que o usuário sai da reunião, o status do Jabber é definido como "Disponível" novamente. Se o usuário do Jabber estiver em outra reunião/chamada ao ingressar na reunião do aplicativo Web, o Servidor de Reunião não atualizará o status do Jabber. Se o usuário do Jabber tiver definido seu status como 'DND - Não perturbe' antes de ingressar na reunião do aplicativo Web, o Servidor de Reunião não atualizará o status do Jabber. Se o usuário atualizar o status do Jabber manualmente a qualquer momento durante a reunião do aplicativo Web, o Servidor de Reunião não substituirá o status do usuário atualizado manualmente.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.