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.

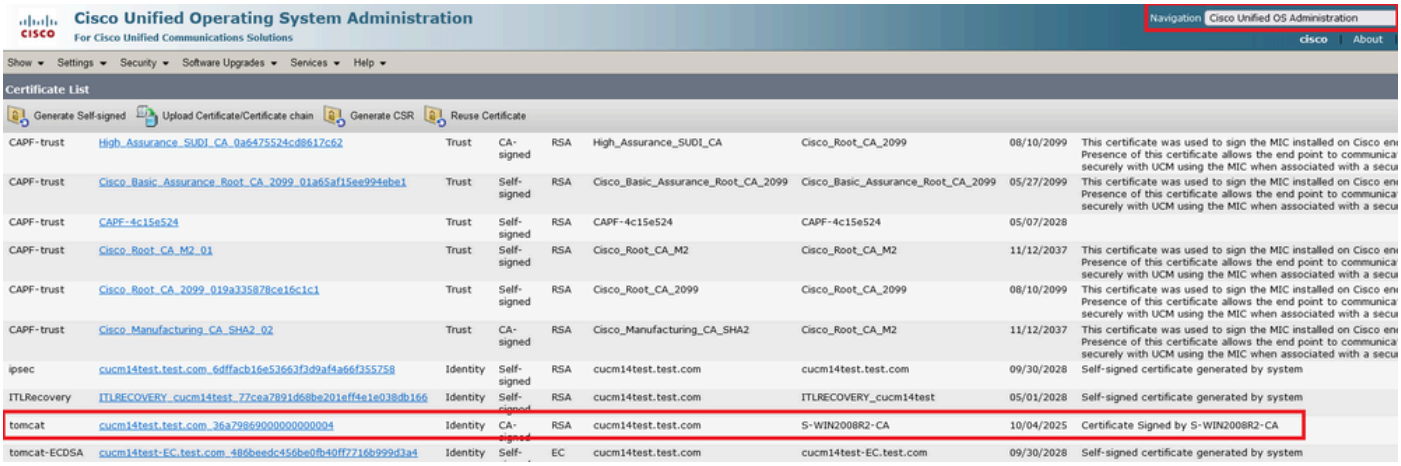
Premesse

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

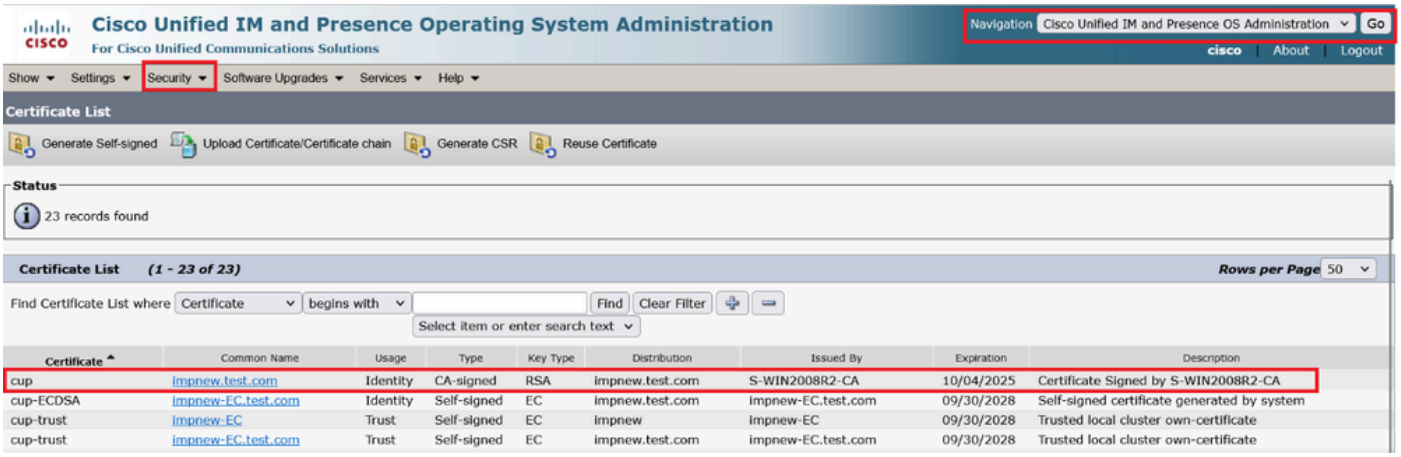
Comunicazione sicura tra CMS e server CUCM/IMP

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



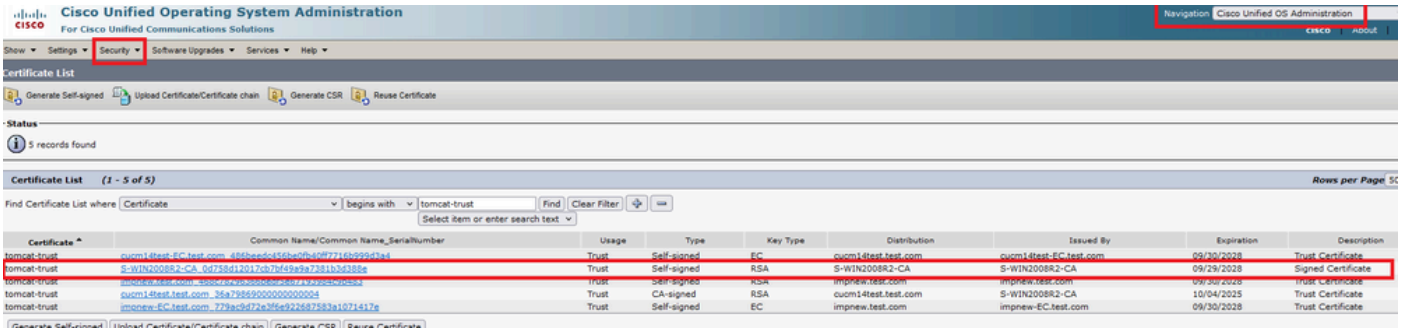
Certificato Tomcat CUCM

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

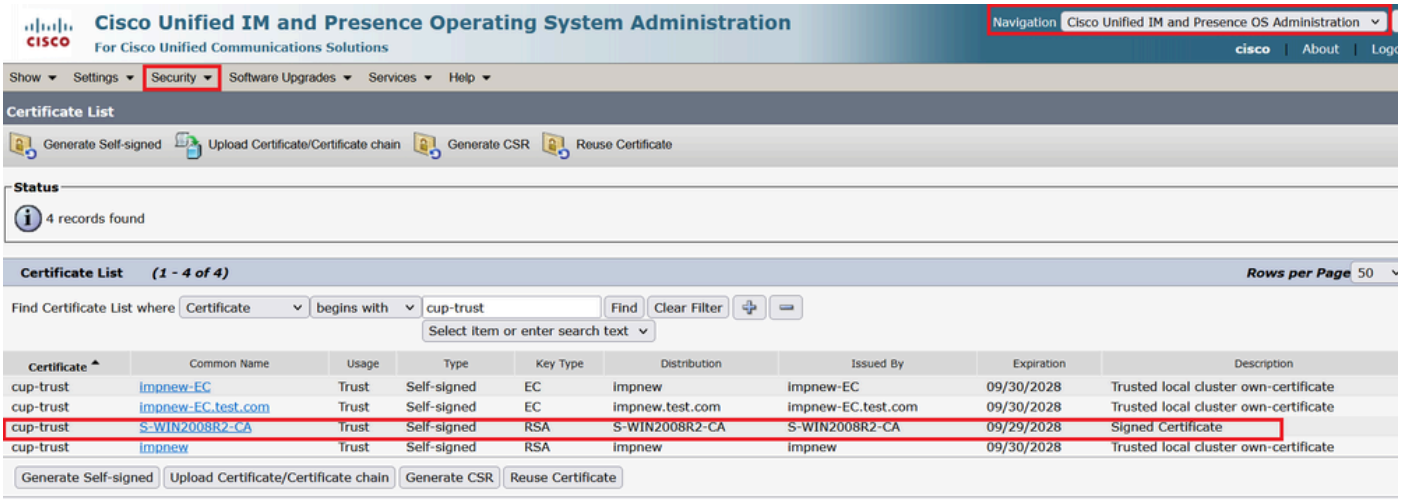


Certificato Presence CUPS

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



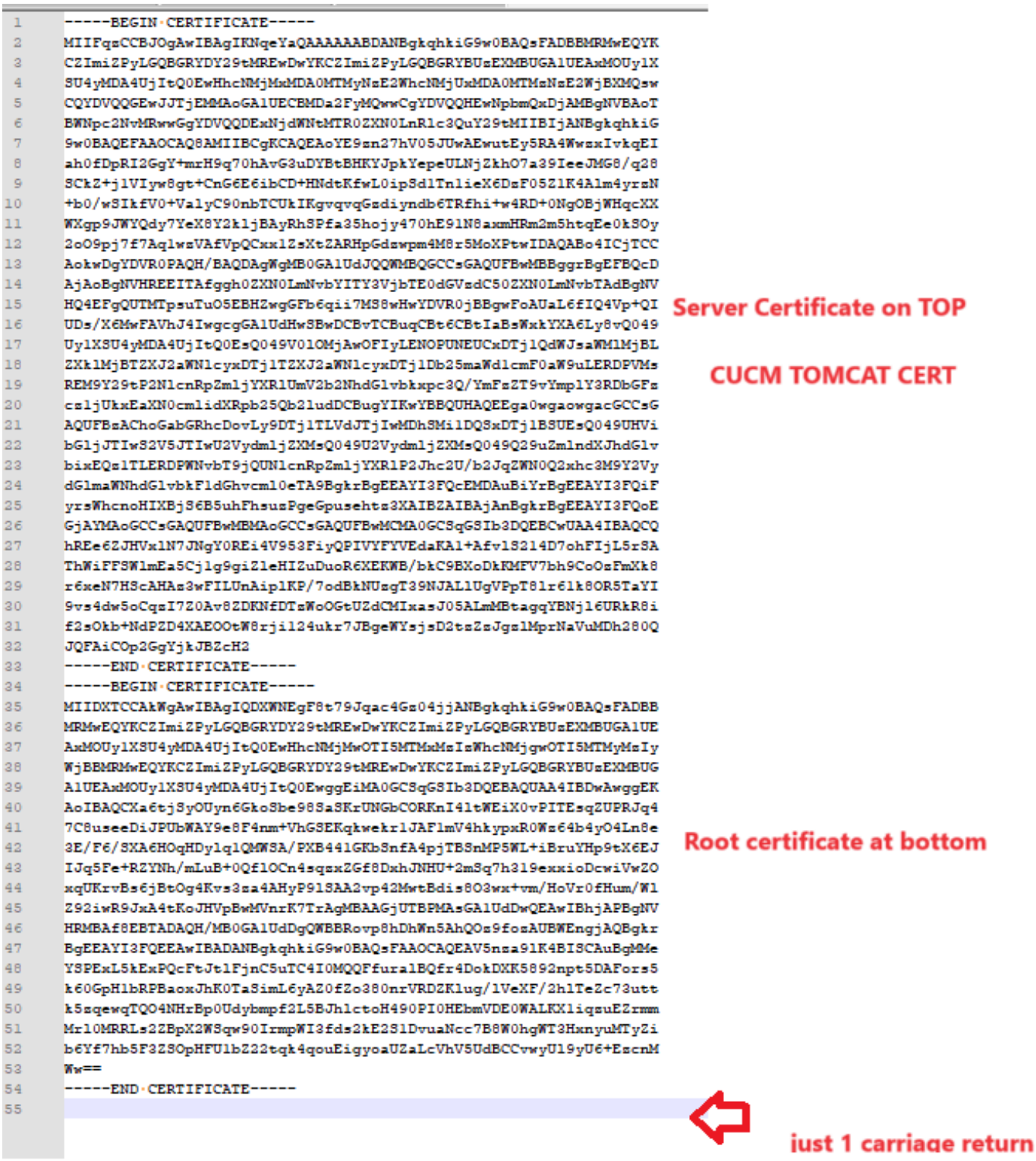
Certificato radice di Tomcat



Certificato radice per CUPS

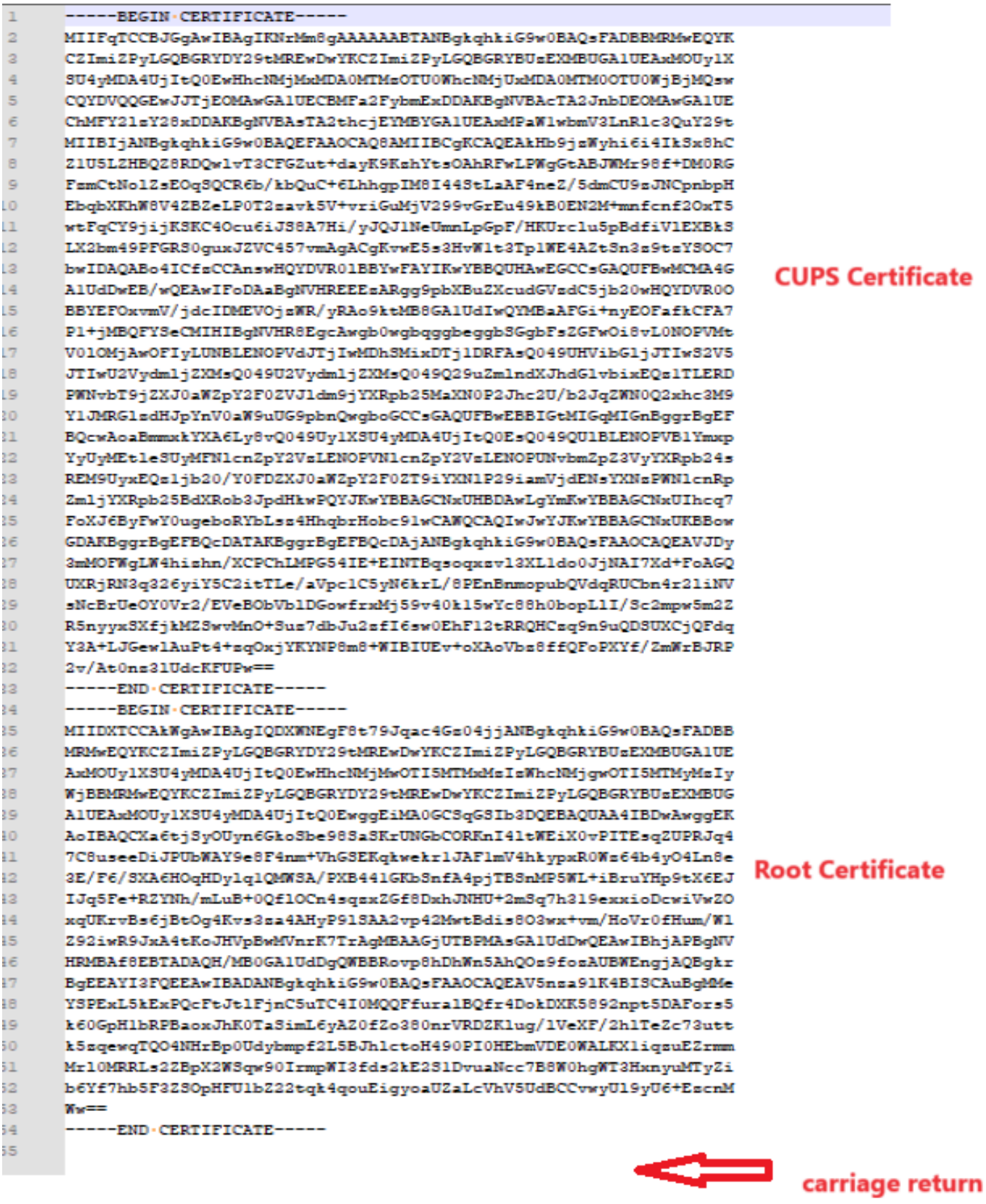
Crea un bundle di certificati CUCM. Per certificato bundle si intende l'inserimento del certificato del server nella parte superiore, del certificato intermedio (qualsiasi) nella parte centrale e del certificato ROOT nella parte inferiore, seguito da un (1) ritorno a capo.

Di seguito è riportato un esempio per il certificato BUNDLE:



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.



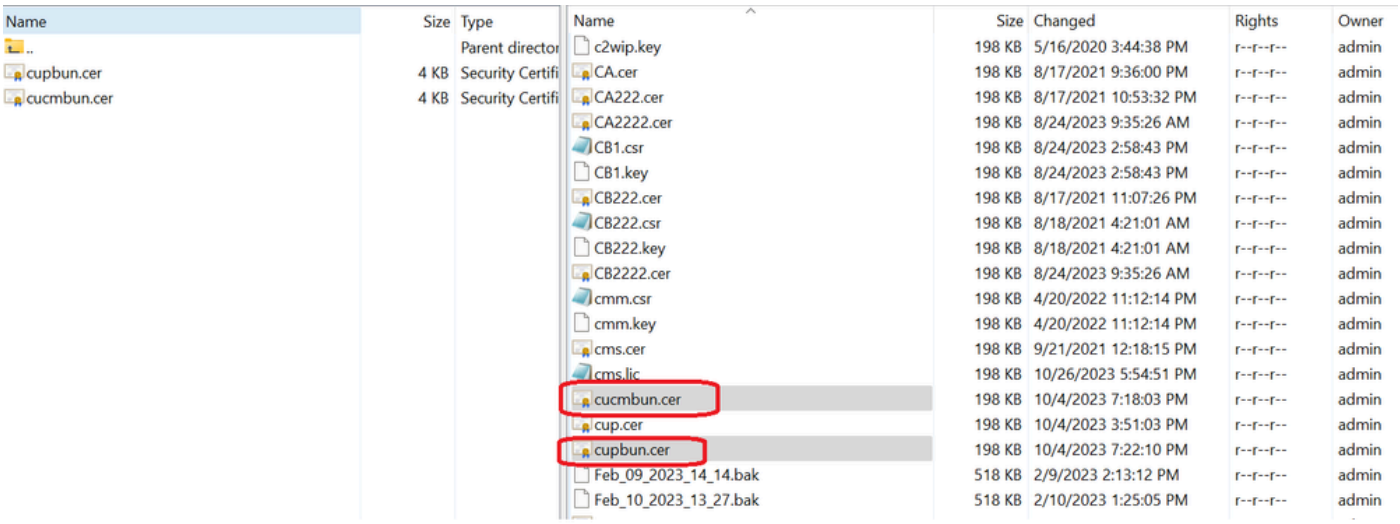
CUPS Certificate

Root Certificate

carriage return

Pacchetto certificati CUPS

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



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

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

Copia del bundle di certificati nel CMS

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

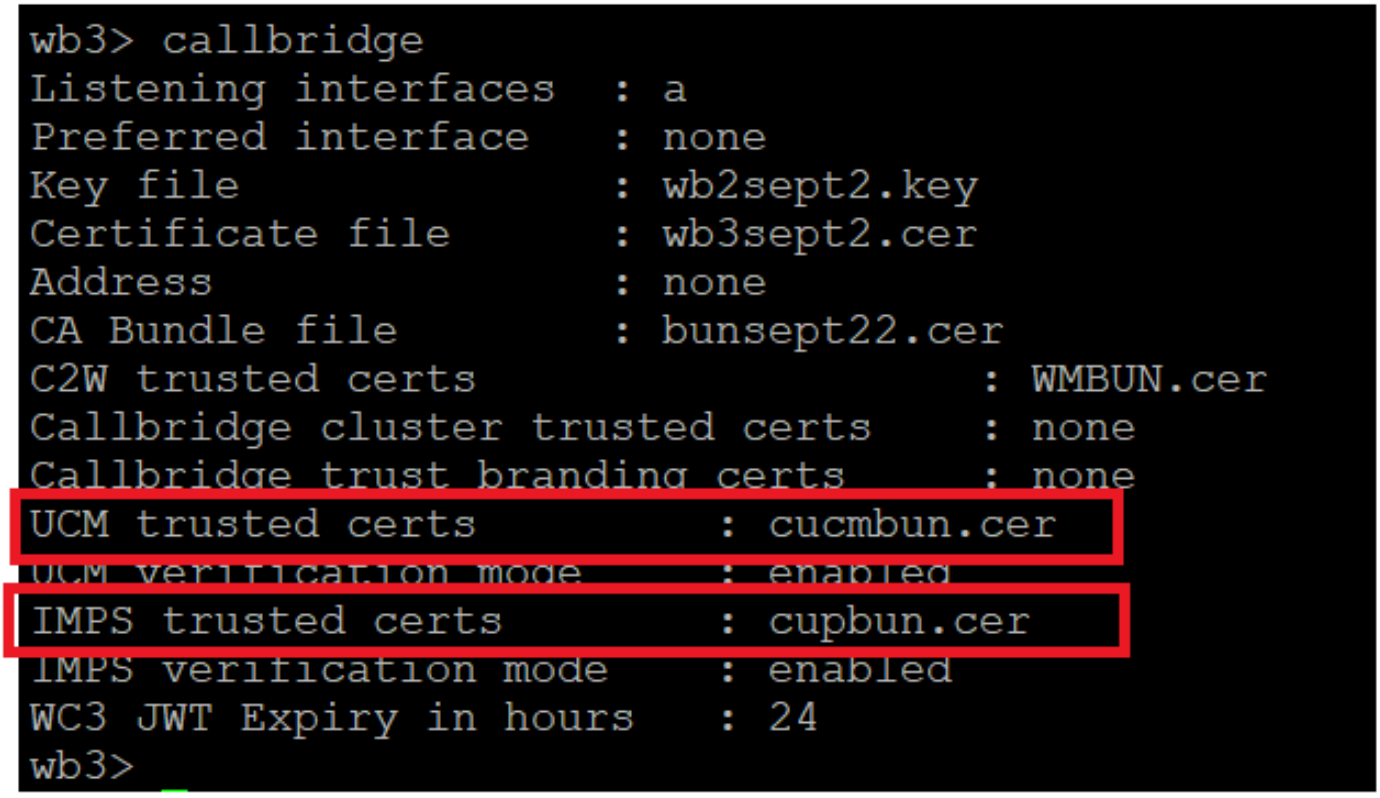
```
wb3>
wb3> callbridge ucm certs cucmbun.cer
wb3>
```

Trust certificato Callbridge

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

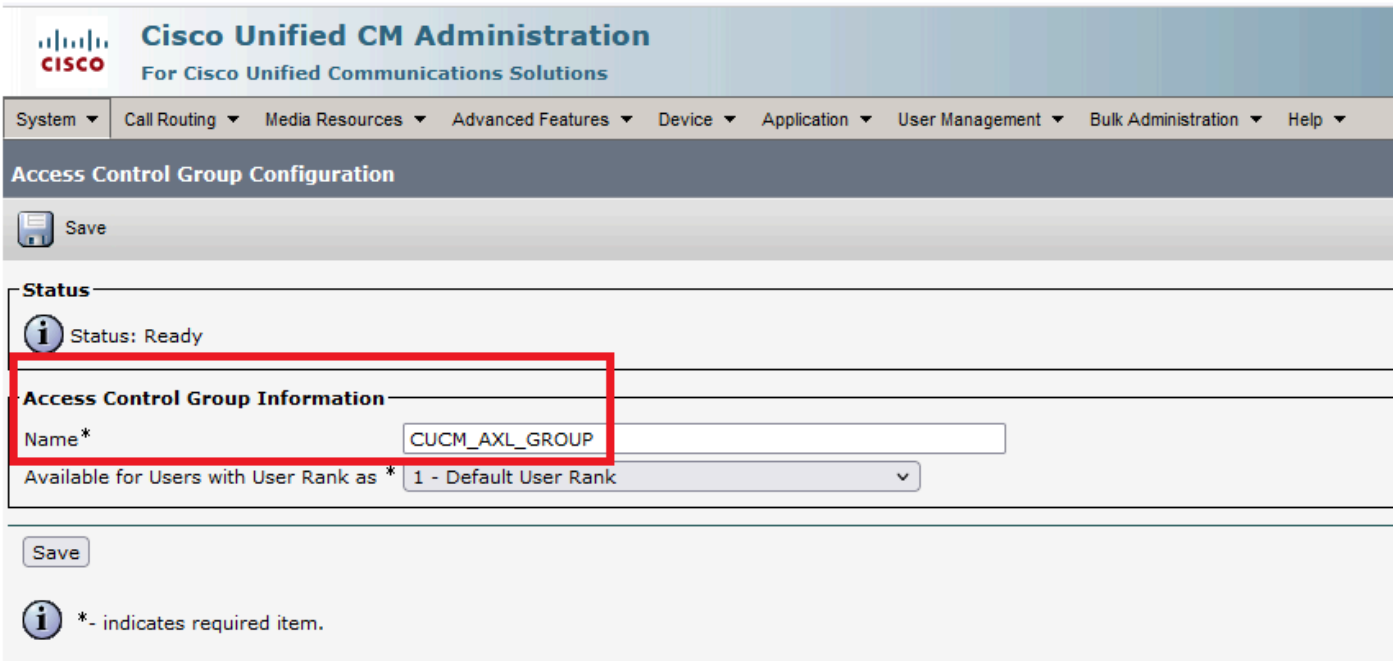
```
wb3>
wb3> callbridge imps certs cupbun.cer
wb3>
```

Eseguire ilcallbridge comando per verificare se i bundle di certificati sono assegnati.



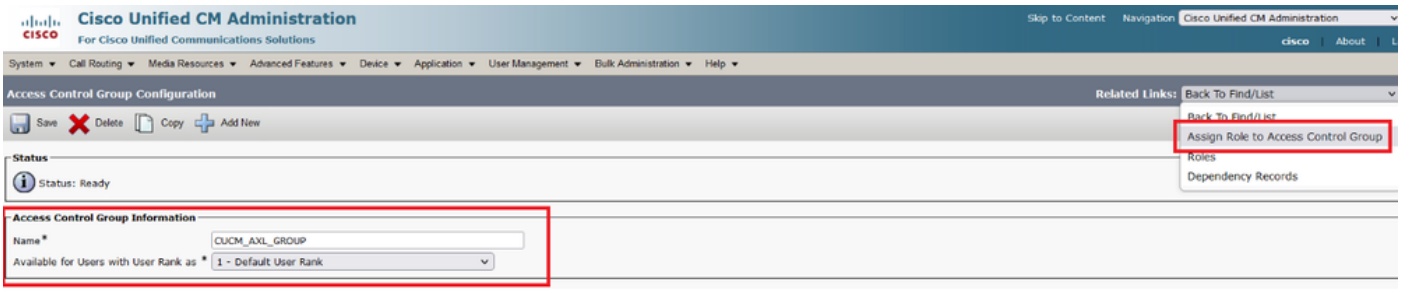
Controllo certificato trust Callbridge

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.

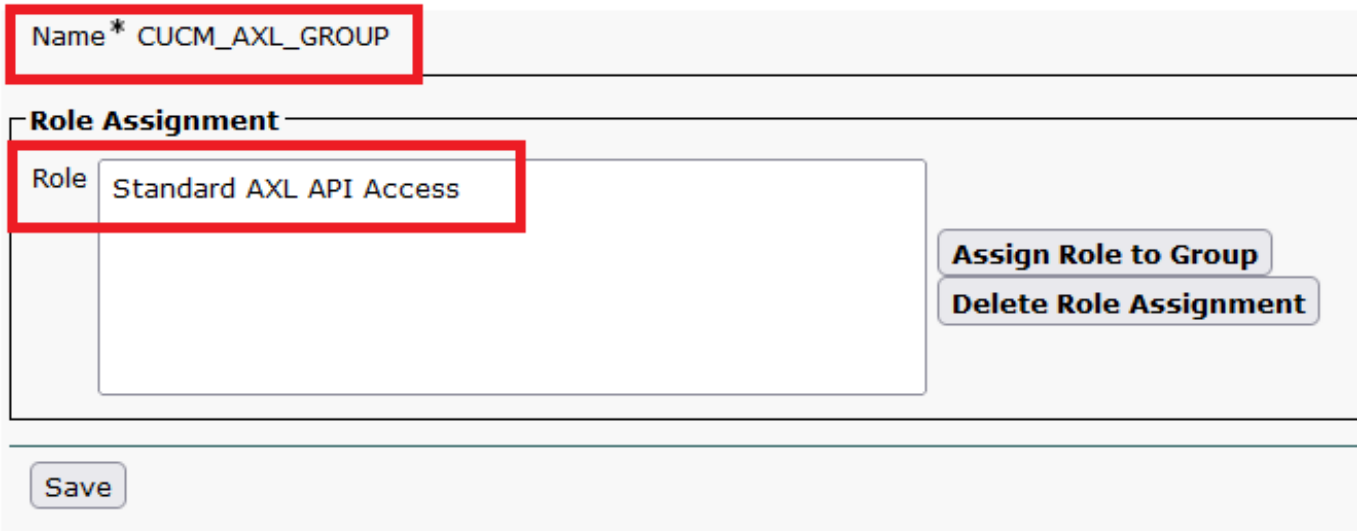


Creazione di un gruppo AXL

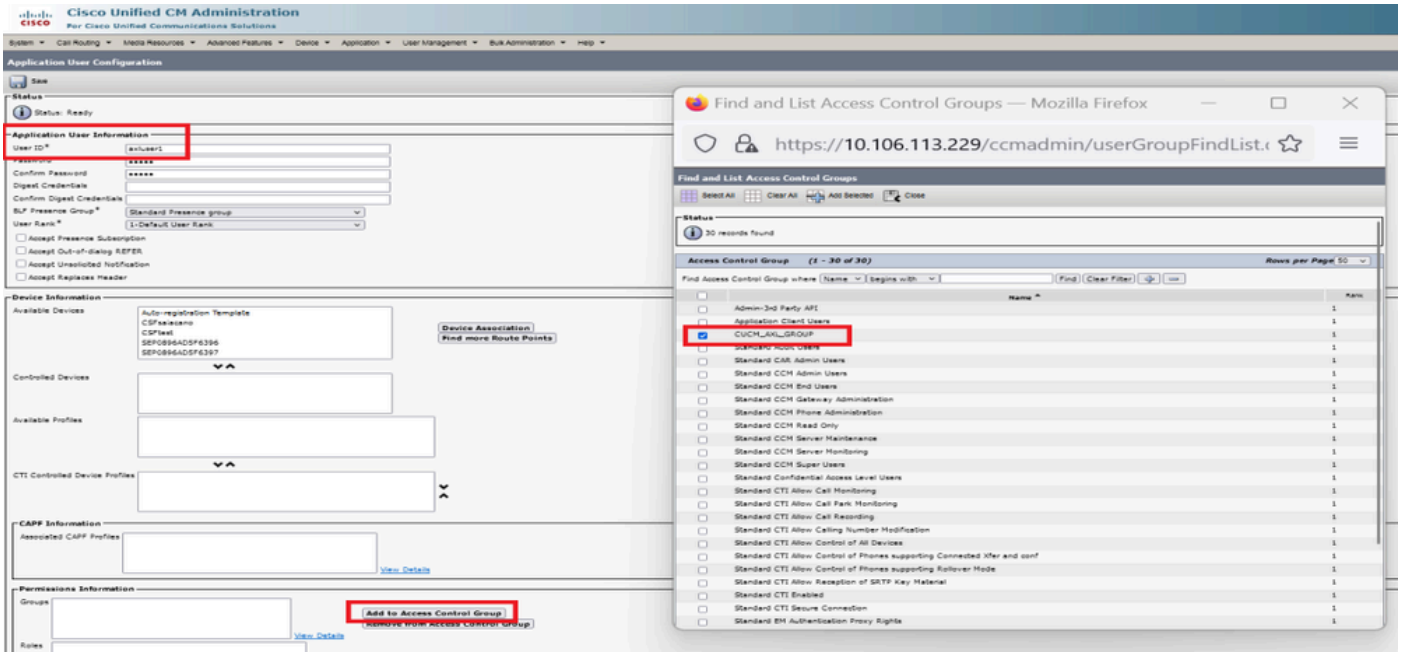
Assegnare il ruolo Standard AXL API Access al gruppo di controllo di accesso creato in precedenza.



Assegnazione dell'accesso API al gruppo AXL

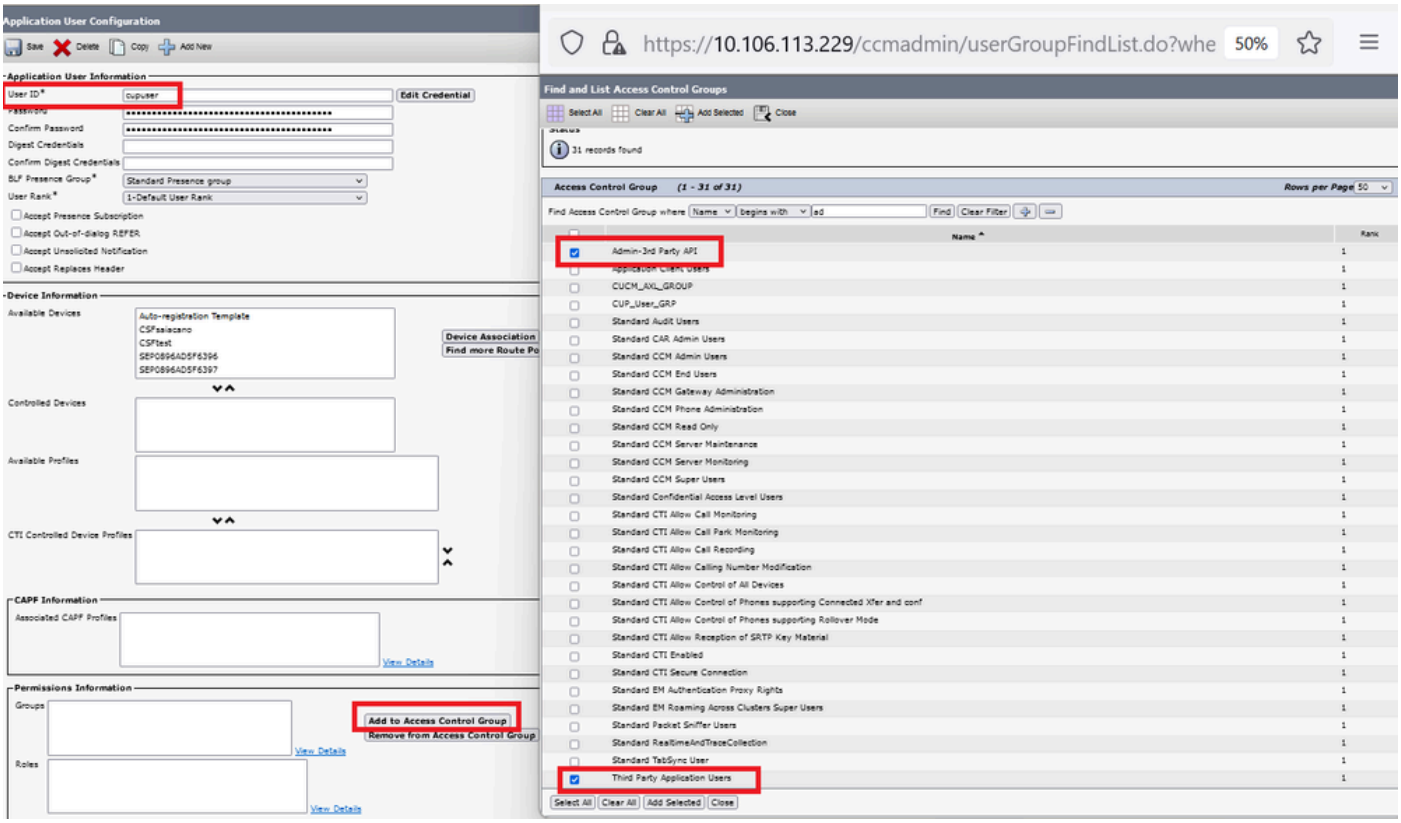


Passare aUser Management > Application User, fare clic su Add New e creare un utente applicazione AXLuser. Assegnare quindi il gruppo di controllo di accesso creato in precedenza.



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.

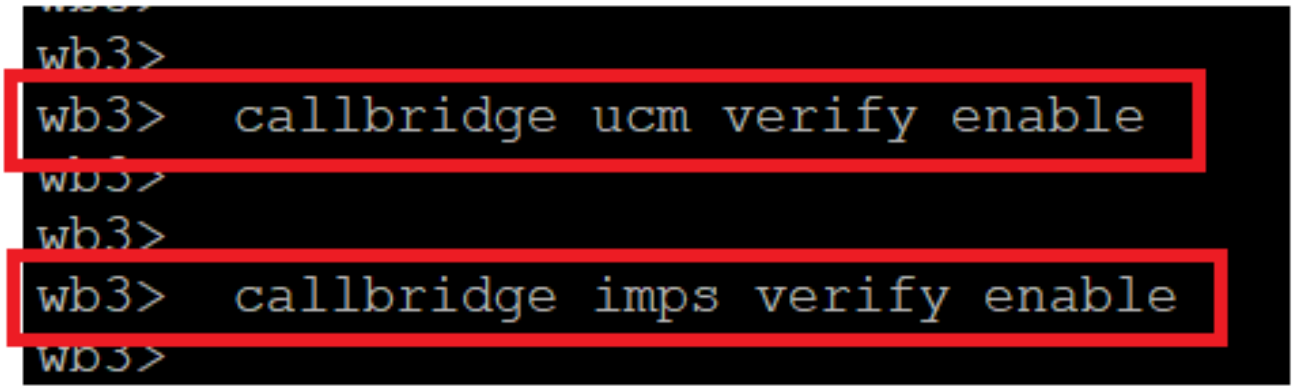


Creazione utente CUP

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

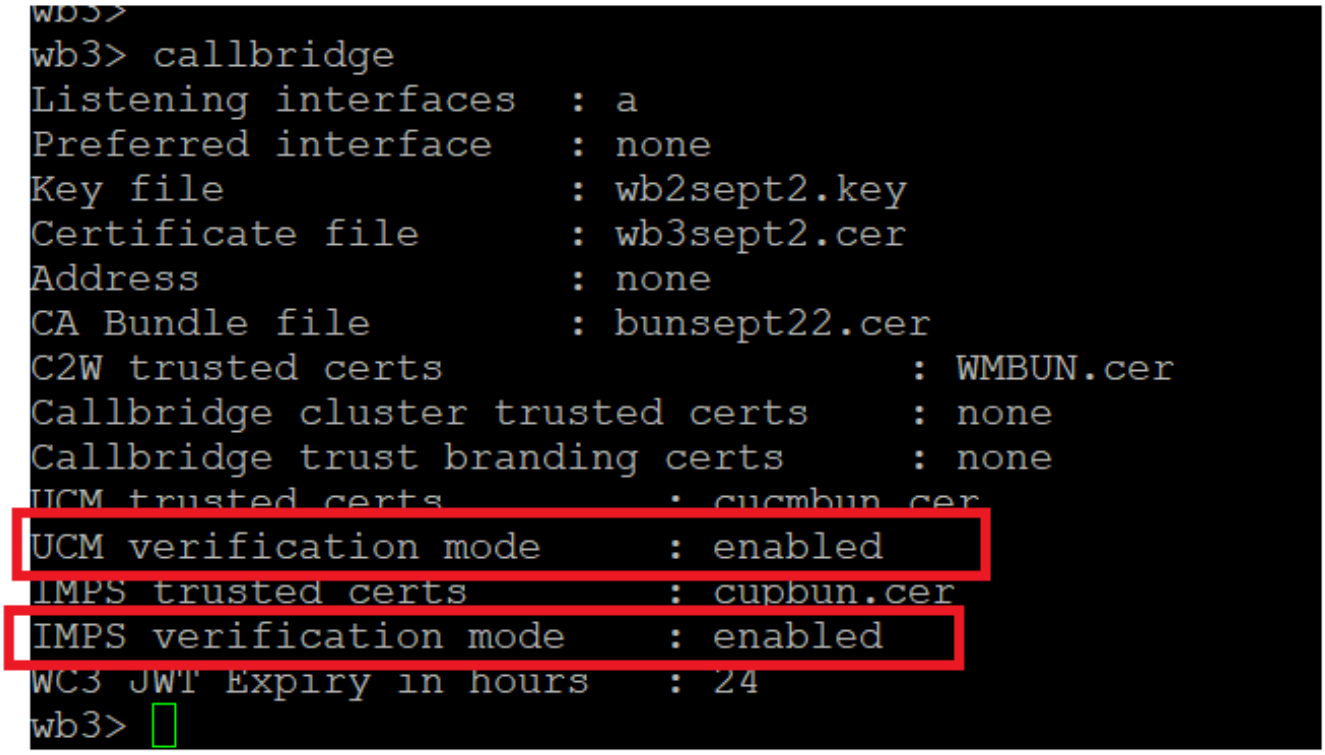
callbridge ucm verify <enable/disable>

callbridge imps verify <enable/disable>



Callbridge verifica i certificati CUCM e CUPS

Verificarlo eseguendo il callbridge comando.

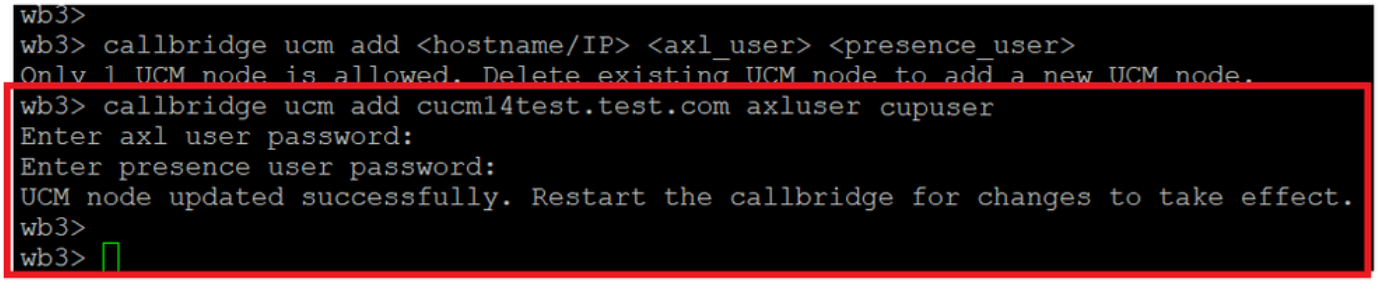


Controllo dei comandi di Callbridge

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

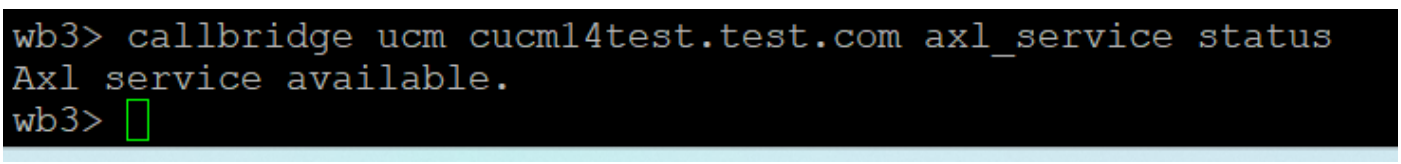


Aggiunta di CUCM a Callbridge

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



Stato AXL Callbridge

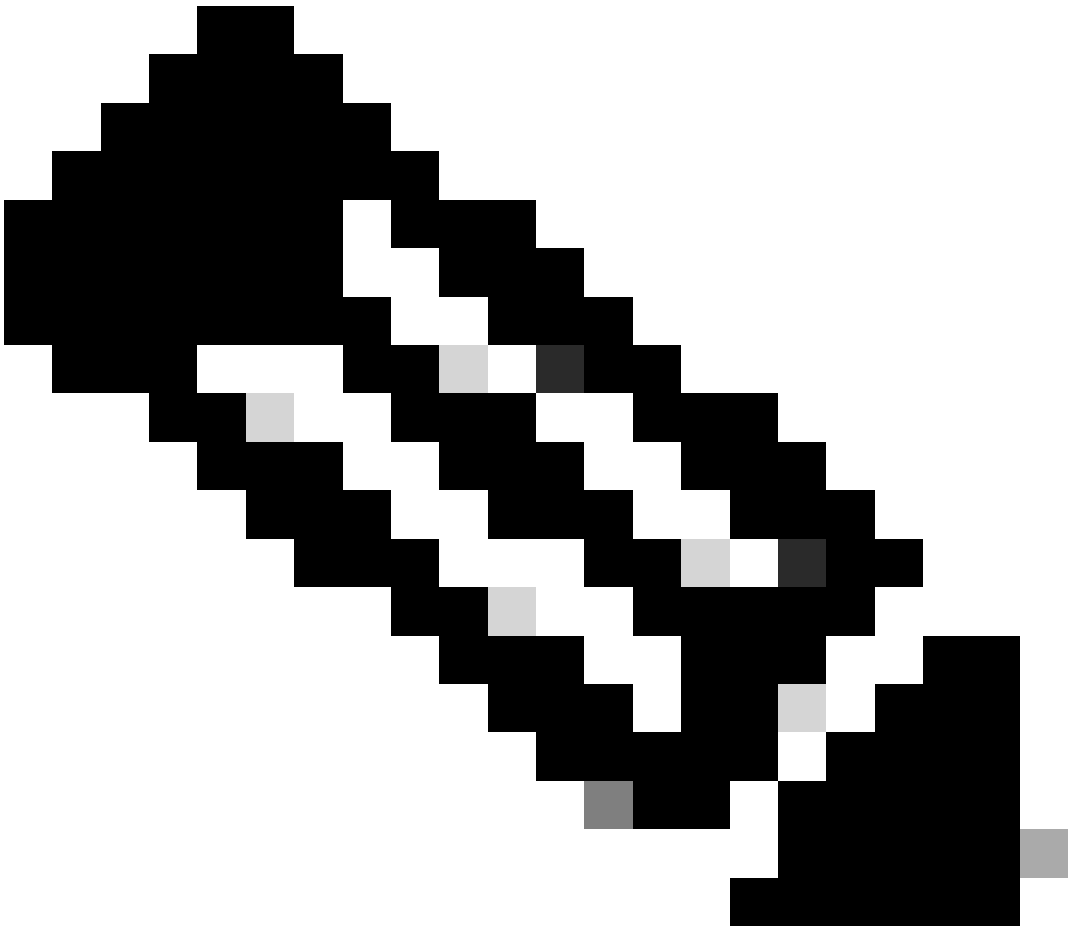
callbridge imps <hostname/IP> <presence_user> presence_service status

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

```
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.



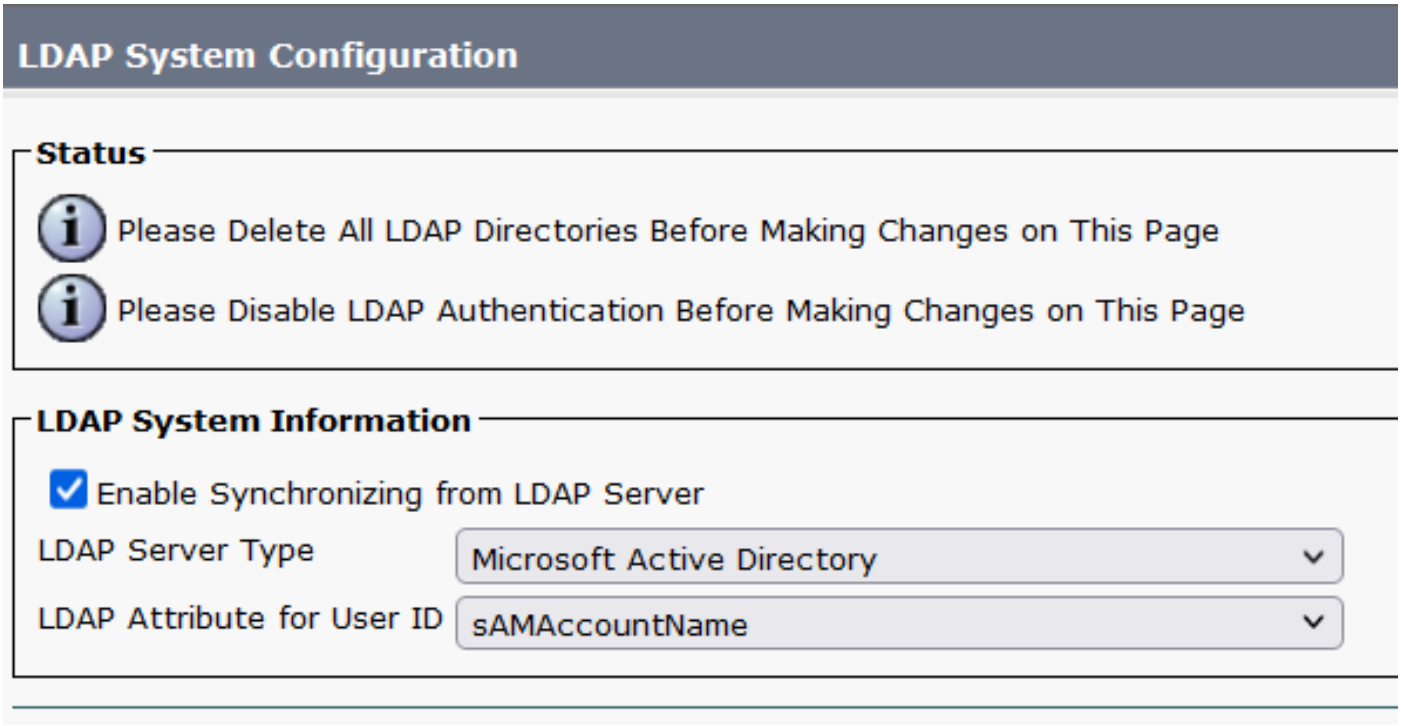
Nota:

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

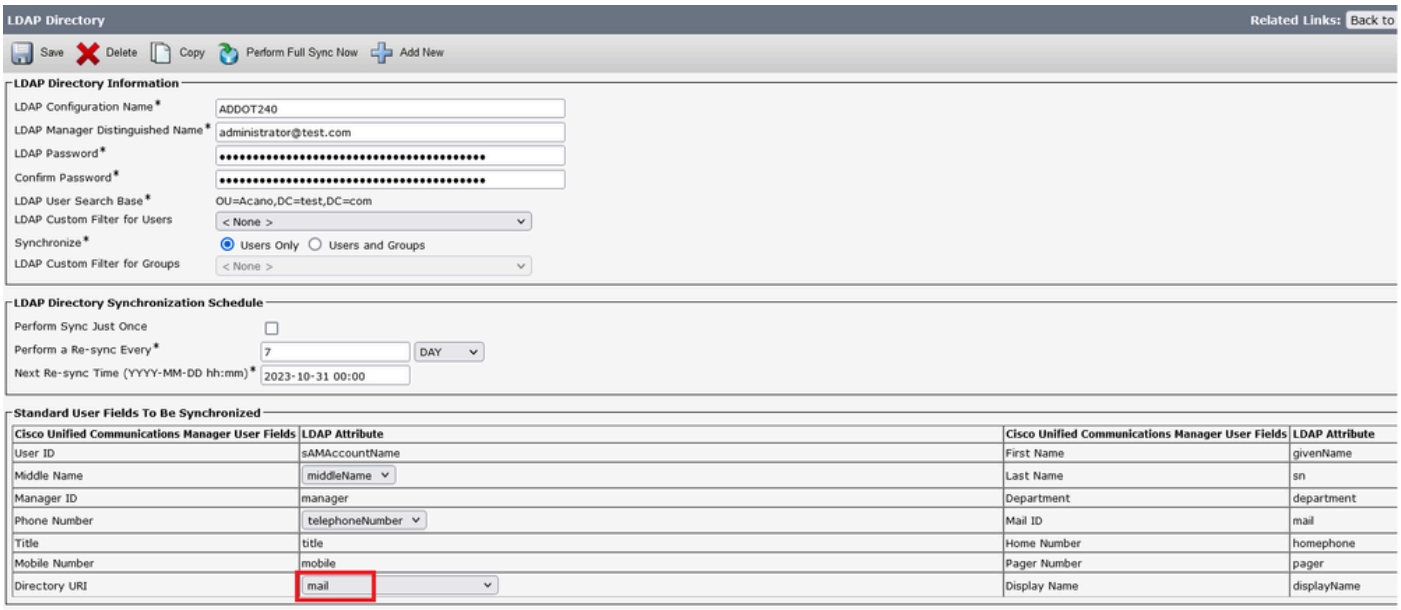
Per CUCM deve essere configurato LDAP.

Sistema LDAP:



Configurazione LDAP CUCM 1

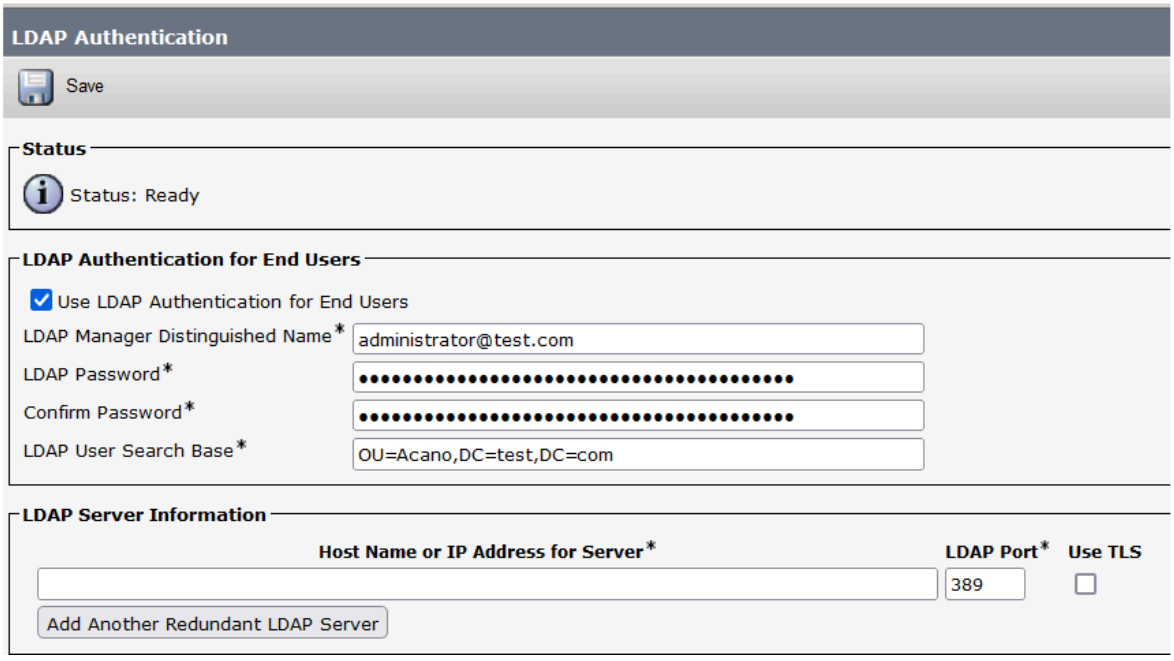
Directory LDAP:



Configurazione LDAP CUCM 2

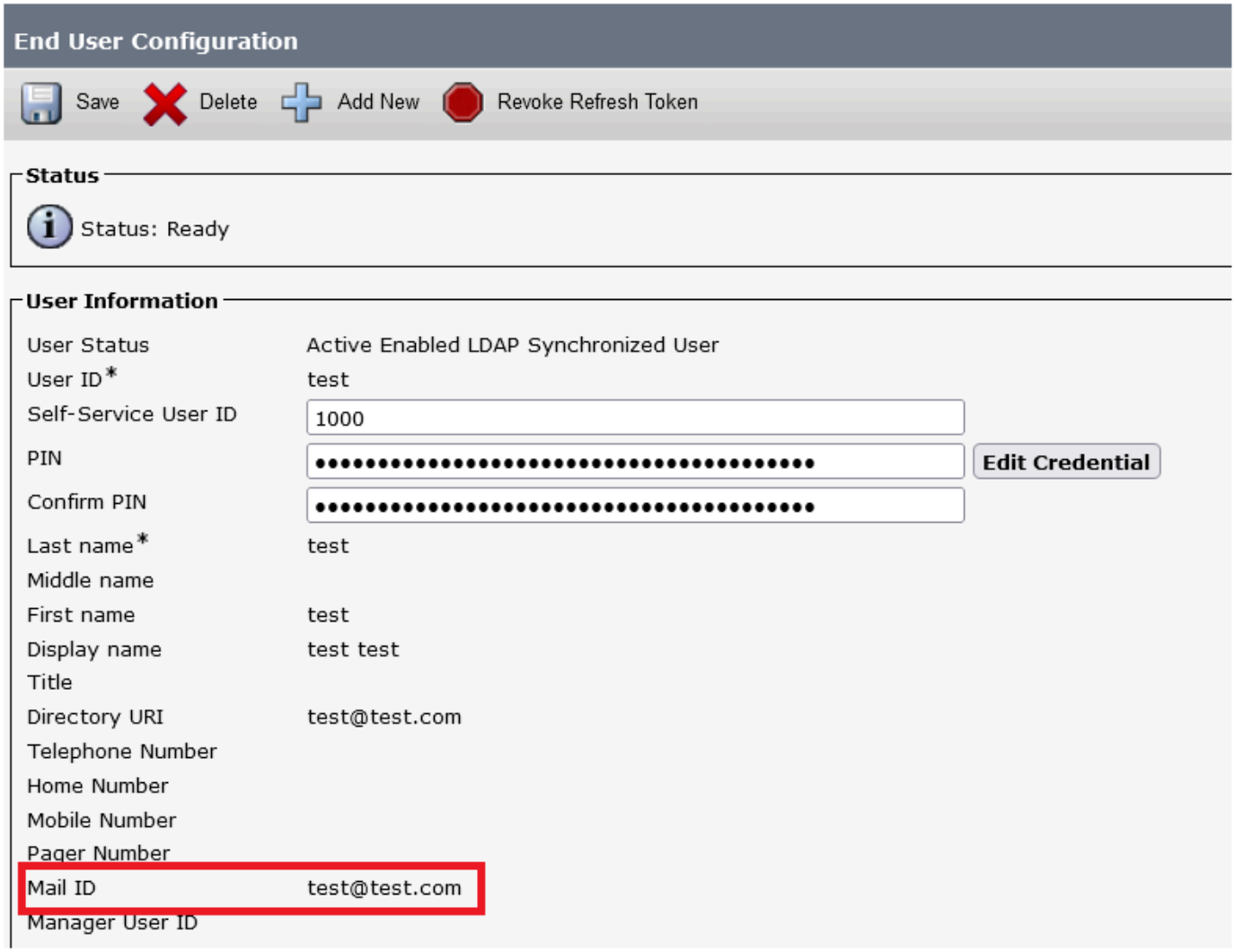
Autenticazione LDAP

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



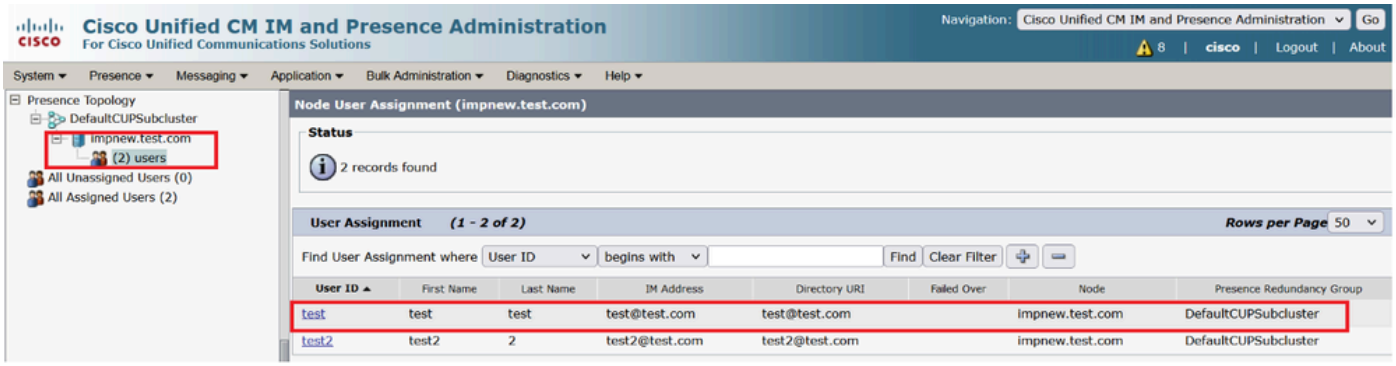
Configurazione LDAP CUCM 3

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



Utenti in CUCM

Utente CUCM aggiornato sul server CUPS:



Utenti in CUPS

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

Status Configuration Logs

Users

Filter Submit Query

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

Utenti CMS

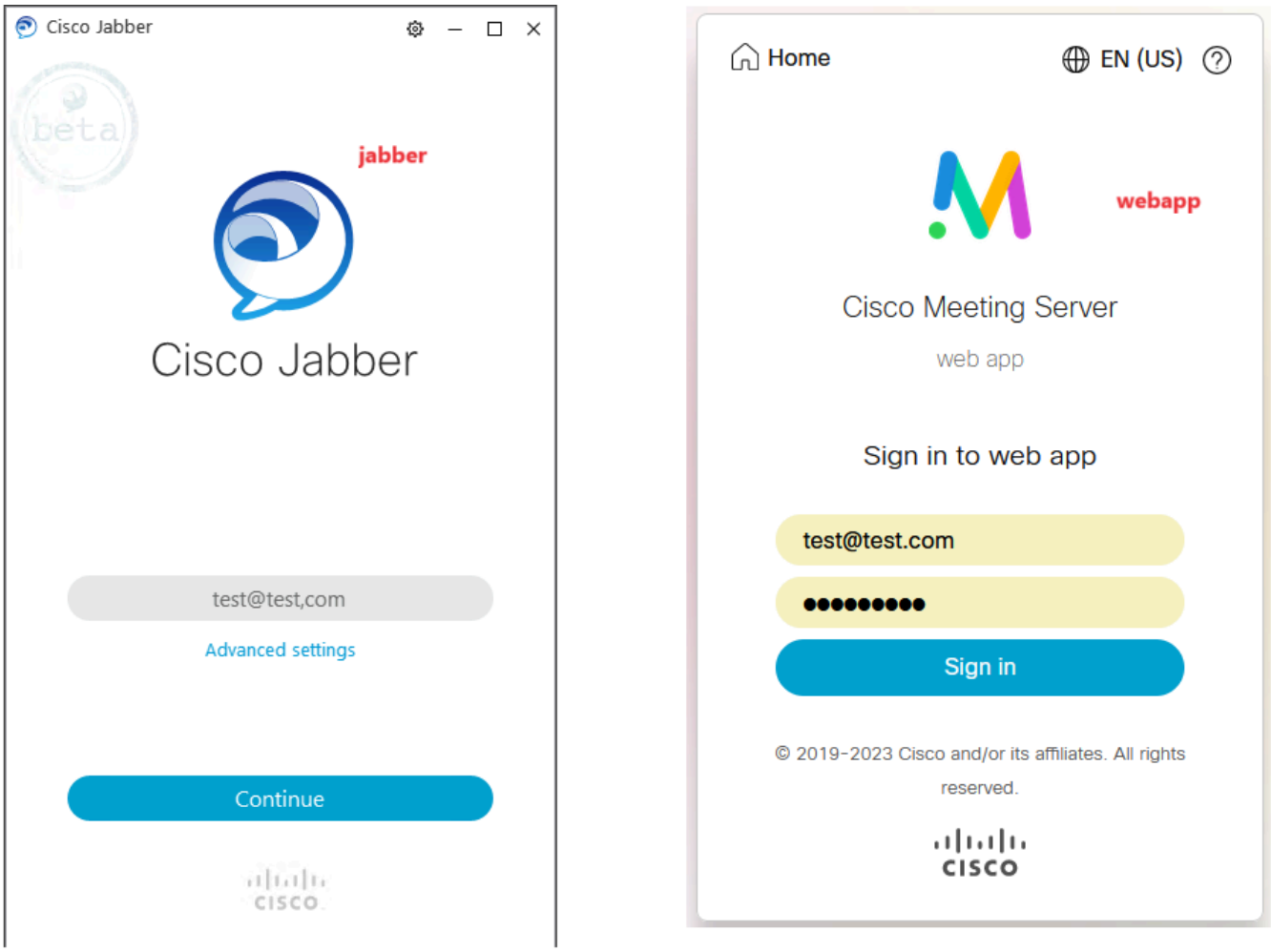
Ora, poiché è già stato verificato che il sistema CMS può considerare attendibile CUCM, è possibile procedere con il test della presenza.

```
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 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 CUPS e CUCM a CMS

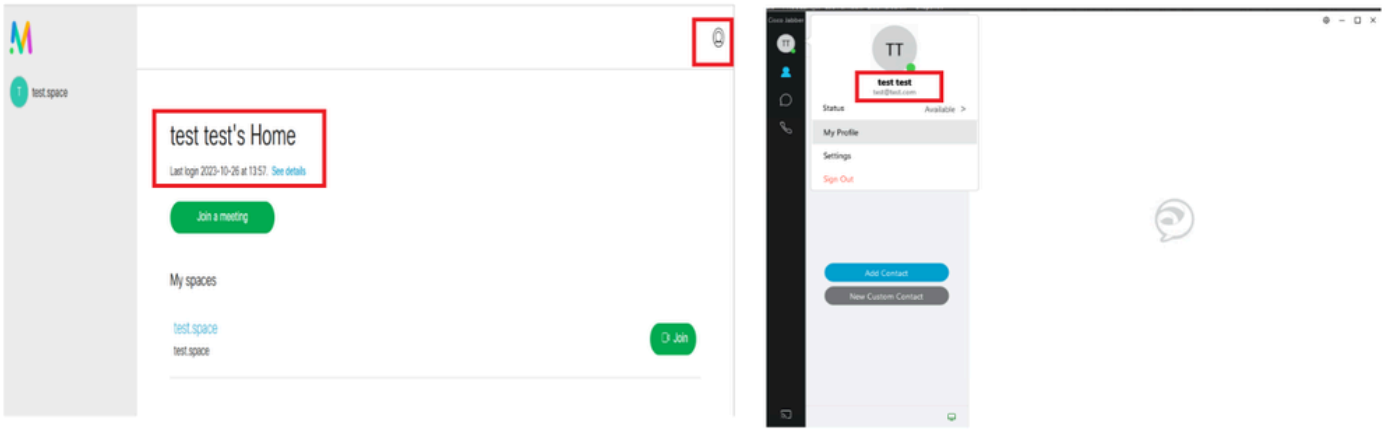
Verifica

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

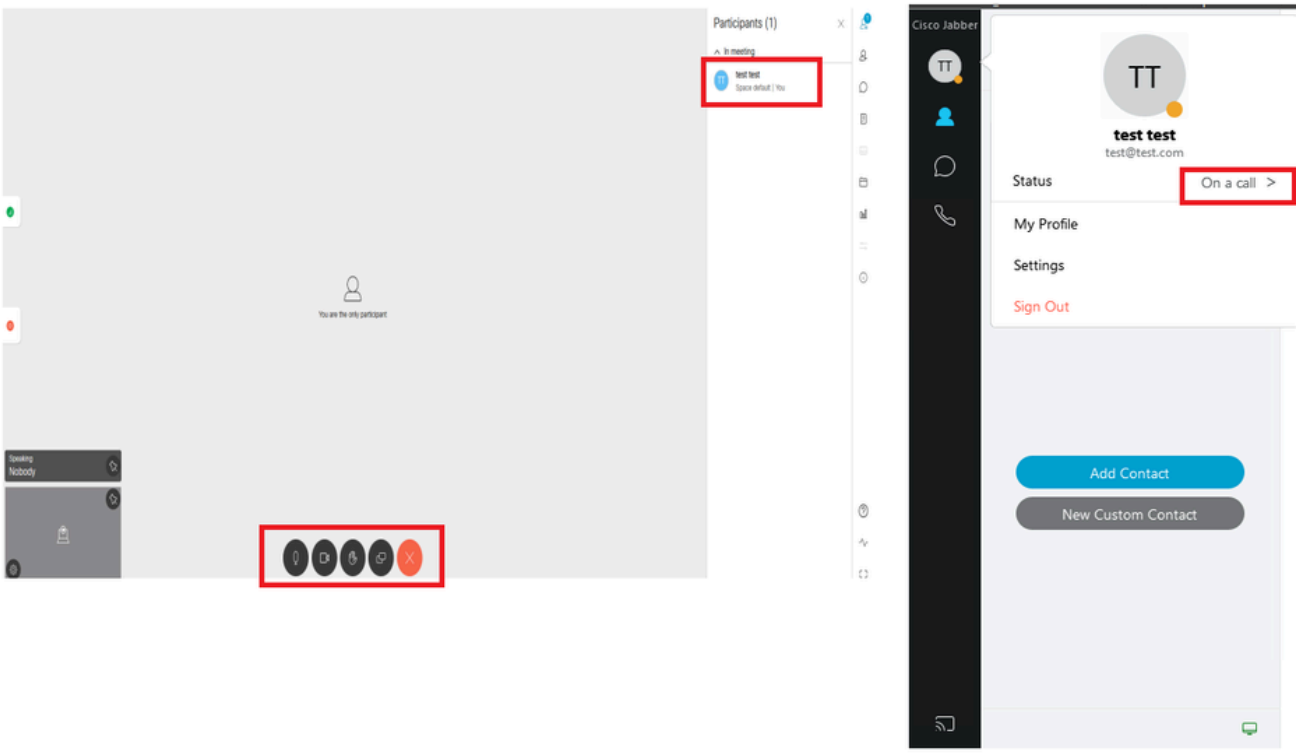


Accesso utente in Jabber e webapp

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).