تمكين الاتصال الآمن بين CMS و CUCM

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

التكوين

تمكين الاتصال الآمن بين خادم CMS و CUCM/IMP

تكوين CUCM المحدد لمشاركة التواجد بين WebApp وعميل Jabber

التحقق من الصحة

المقدمة

يوضح هذا المستند كيفية تمكين الاتصال بين خادم الاجتماعات (CMS) من Cisco ومدير الاتصالات الموحدة (CUCM).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- CMS الإصدار 3.8 والإصدارات الأحدث
- CUCM و IM&P
- Jabber

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- CMS، الإصدار 3.8
- CUCM و IM&P 14 SU (3)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

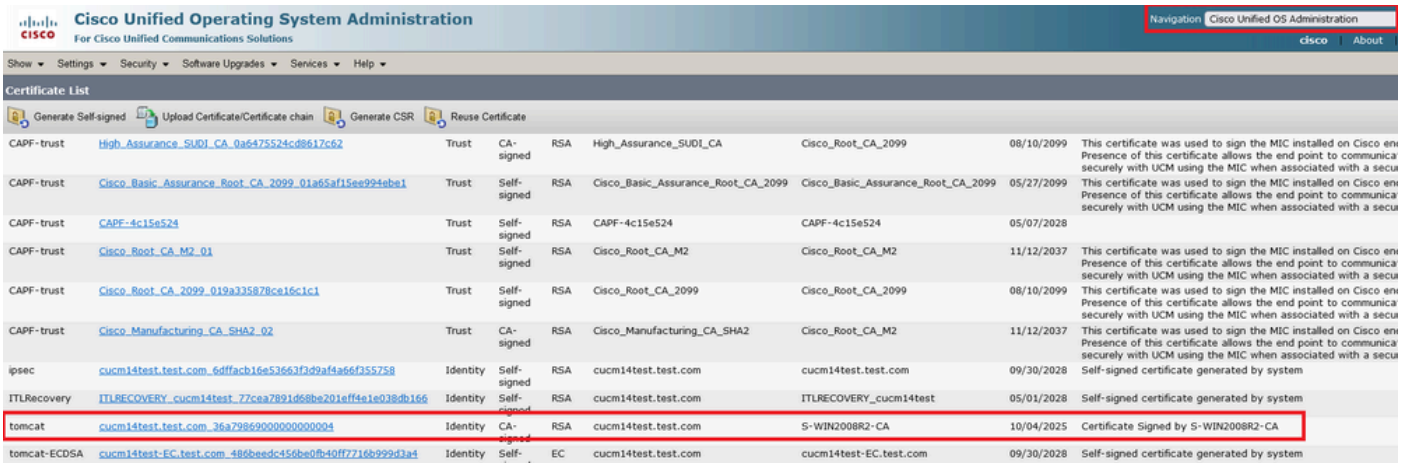
يوضح هذا المستند عملية إنشاء اتصال آمن بين CMS و CUCM لمشاركة وجود Jabber/Web

App. وهو يشرح الخطوات التفصيلية لتكوين حالة التحديث لمستخدمي Jabber واستكشاف أخطائها وإصلاحها أثناء إجتماعات تطبيق الويب على CMS. يمكن تكوين خادم الاجتماعات لتحديث حالة التواجد الخاصة بمستخدمي Jabber أثناء اشتراكهم في إجتماع Cisco Meeting Server Web App.

التكوين

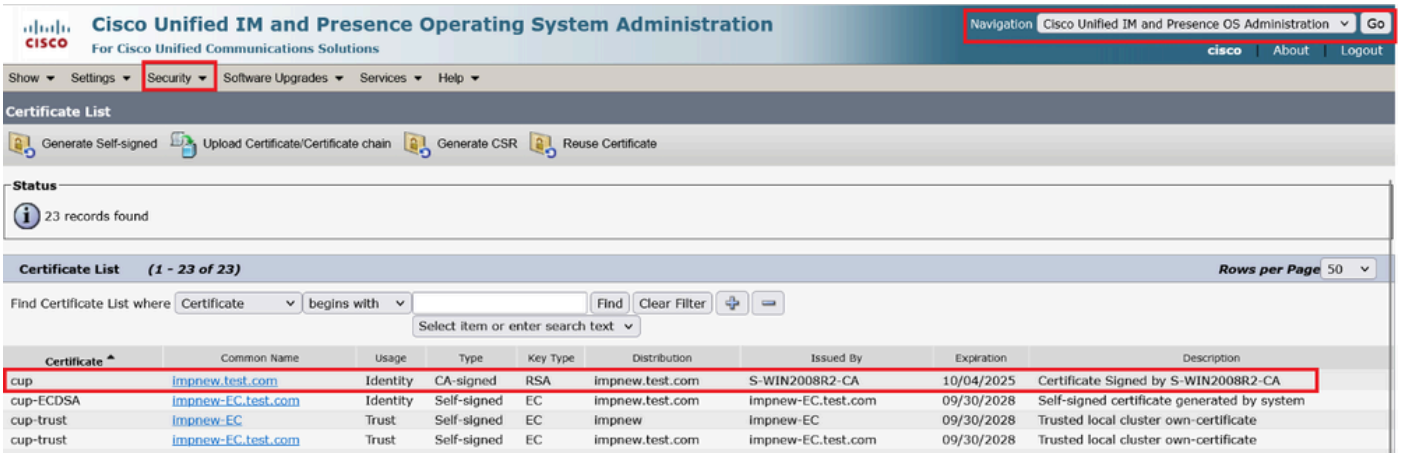
تمكين الاتصال الآمن بين خادم CMS و CUCM/IMP

قم بتسجيل الدخول إلى CUCM في صفحة إدارة OS، وتصفح إلى Security > Certificate Management، وتنزيل شهادة TOMCAT.



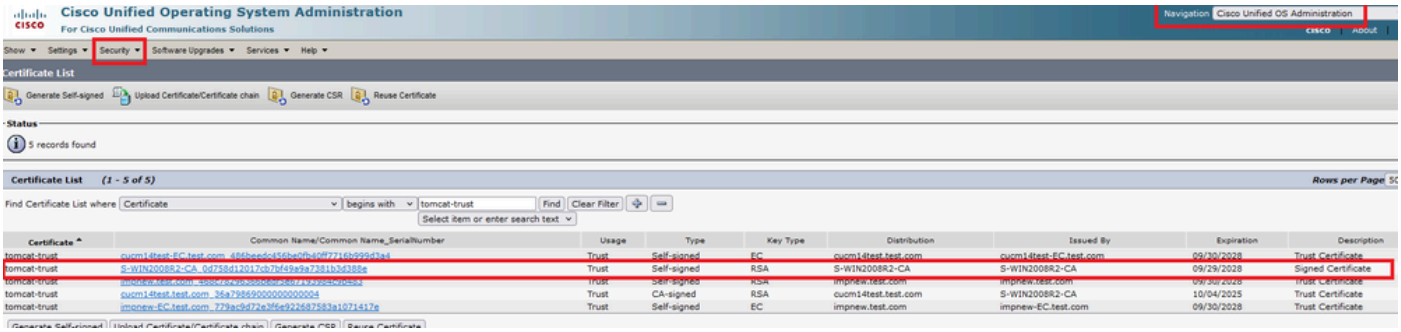
شهادة *CUCM Tomcat*

قم بتسجيل الدخول إلى خادم Cisco Unified Presence (CUPS) في صفحة إدارة OS، وتصفح إلى Security > Certificate Management، وتنزيل شهادة CUPS.

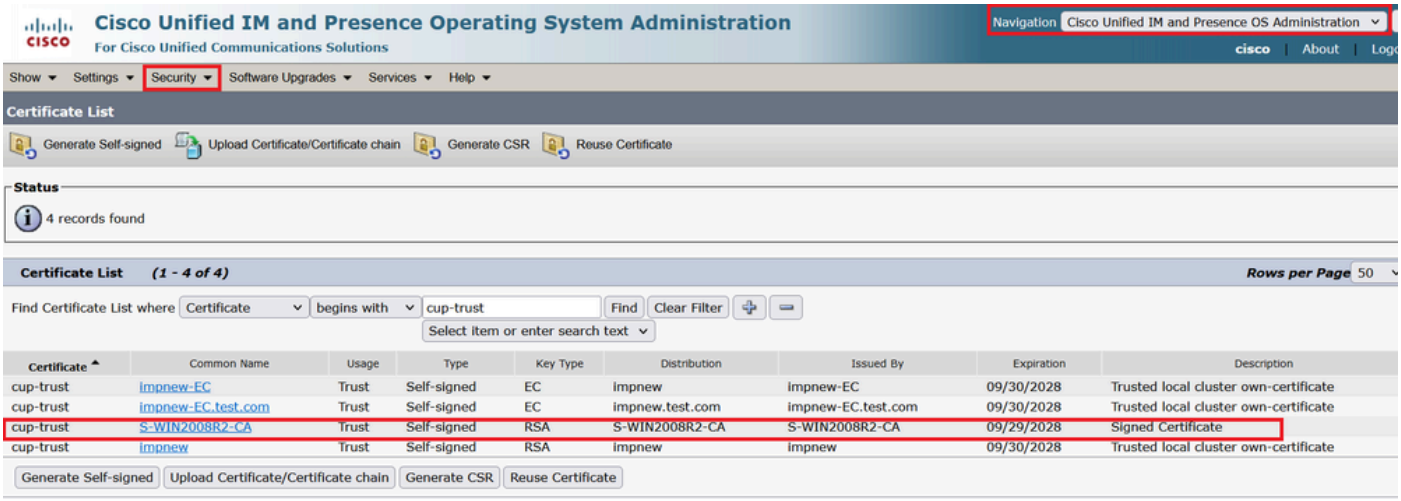


شهادة *Presence CUPS*

تنزيل "شهادة المرجع المصدق الجذر" التي وقعت على شهادة Tomcat و Cup.



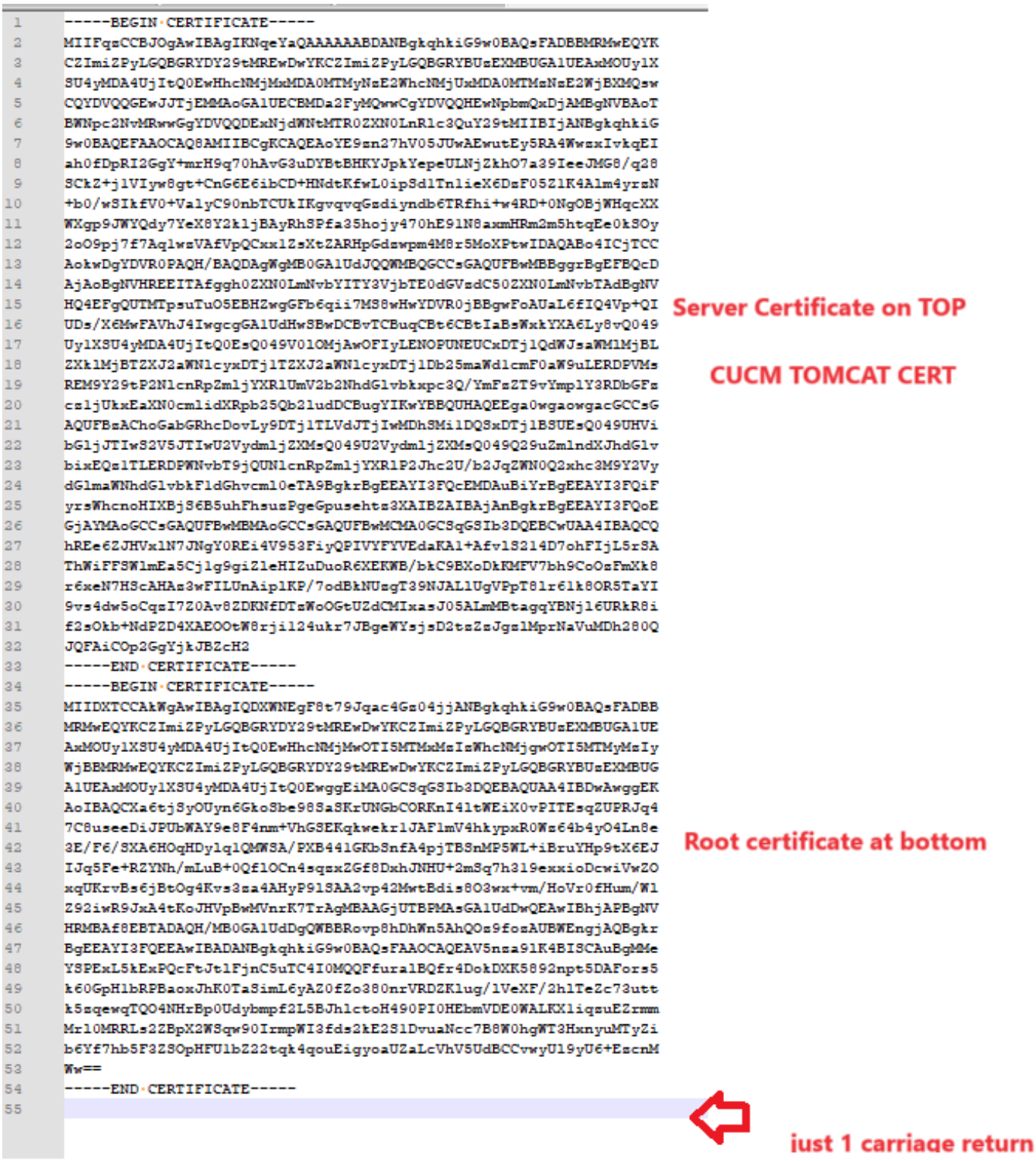
شهادة الجذر ل *Tomcat*



الشهادة الجذر ل *CUPS*

إنشاء حزمة شهادة من شهادات CUCM. حزمة شهادة تعني، وضع شهادة الخادم في الأعلى، والشهادة الوسيطة (أي) في المنتصف، وشهادة الجذر في الأسفل، متبوعة ب (1) رجوع عربة.

هنا عينة ل الحزمة شهادة:



حزمة شهادة *Tomcat*

قم بإنشاء حزمة ترخيص من شهادات CUPS. حزمة شهادة تعني، وضع شهادة الخادم في الأعلى، والشهادة الوسيطة (أي) في المنتصف، وشهادة الجذر في الأسفل، متبوعة ب (1) رجوع عربة.

```
-----BEGIN CERTIFICATE-----
MIIFqTCCBJGgAwIBAgIKNrMm8gAAAAAABTANBgkqhkiG9w0BAQsFADBBMRMwEQYK
CZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUGA1UEAxMOUyly
SU4yMDA4UjItQ0EwHhcNMjMxMDA0MTMzOTU0WhcNMjUxMDA0MTM0OTU0WjBjMQsw
CQYDVQQGEwJJTjEOMAwGA1UECBMFa2FybmExDDAKBgNVBAcTA2JnbDEOMAwGA1UE
ChMFY2lsY28xDDAKBgNVBAsTA2thcjEYMBYGA1UEAxMPaW1wbmV3LnRlc3QuY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkHb9jsWyhi6i4IkSx8hC
Z1U5LZHBQZ8RDQwlvT3CFGZut+dayK9KshYtsOAhRFwLPWgGtABJWMr98f+DM0RG
FsmCtNolZsEOq8QCR6b/kbQuC+6LhhgpIM8I44StLaAF4neZ/5dmCU9zJNCpnbpH
EbqbXKhW8V4ZBZeLP0T2zavk5V+vriGuMjV299vGrEu49kB0EN2M+mnfcnf2OxT5
wtFqCY9jijKSKC4Ocu6iJ88A7Hi/yJQJ1NeUmnLpGpF/HKUrc1u5pBdfiVlEXBkS
LX2bm49PFGRS0guxJZVC457vmAgACgKvwE5s3HvW1t3TplWE4AZtSn3s9tsYSOC7
bwIDAQABo4ICFzCCAhswHQYDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMA4G
A1UdDwEB/wQEAwIFoDAaBgNVHREEEzARgg9pbXBuZXcudGVzdC5jb20wHQYDVR0O
BBYEFOxvmV/jdcIDMEVOjsWR/yRAo9ktMB8GA1UdIwQYMBaAFGi+nyEOFafkCFA7
P1+jMBQFYSeCMIHIBgNVHR8EgcAwgb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPVMt
V01OMjAwOFIyLUNBLENOPVdJTjIwMDhSMixDTjlDRFAsQ049UHVibGljJTIwS2V5
JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1TLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnQwgboGCCsGAQUFBwEBBIGtMIGqMIGnBggrBgEF
BQcwAoaBmmxkYXA6Ly8vQ049U1lSU4yMDA4UjItQ0EsQ049QU1BLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9UyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWNlcnRp
ZmljYXRpb25BdXRob3JpdHkwPQYJKwYBBAGCNxUHBDAwLgYmKwYBBAGCNxUIhcq7
FoXJ6ByFwY0ugeboRYbLss4HhqbrHobc91wCAWQCAQIwJwYJKwYBBAGCNxUKBBow
GDAKBggrBgEFBQcDATAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAVJDy
3mMOFWgLW4hishn/XCPChLMPG54IE+EINTBqsoqxsv13XL1do0JjNAI7Xd+FoAGQ
UXRjRN3q326yiY5C2itTLe/aVpc1C5yN6krL/8PEnBnmopubQVdqRUCbn4r2liNV
sNcBrUeOY0Vr2/EVeBObVblDGowfrxMj59v40kl5wYc88h0bopL1I/Sc2mpw5m2Z
R5nyyxSXfjkMZSwvMnO+Sus7dbJu2zfI6sw0EhF12tRRQHCsq9n9uQD8UXCjQFdq
Y3A+LJGewlAuPt4+sqOxjYKYNP8m8+WIBIUEv+oXAoVbs8ffQFoPXYf/2mWrBJRP
2v/At0ns31UdcKFUPw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIQDXWNEgF8t79Jqac4Gs04jjANBgkqhkiG9w0BAQsFADBB
MRMwEQYKCZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUGA1UE
AxMOUylXSU4yMDA4UjItQ0EwHhcNMjMwOTI5MTMxMzIzWhcNMjgwOTI5MTMyMzIy
WjBBMRMwEQYKCZImiZPyLGQBGRYDY29tMREwDwYKCZImiZPyLGQBGRYBUzEXMBUG
A1UEAxMOUylXSU4yMDA4UjItQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCXa6tjSyOUyn6GkoSbe98SaSKrUNGbCORKnI4ltWEiX0vPITEsqZUPRJq4
7C8useeDiJPUbWAY9e8F4nm+VhGSEKqkwekrlJAFlmV4hkypxR0Wz64b4yO4Ln8e
3E/F6/SXA6HOqHDylqlQMWSA/PXB44lGKb3nfA4pjTBSnMP5WL+iBruYHp9tX6EJ
IJq5Fe+RZYNh/mLuB+0QflOCn4sqsxZGf8DxhJNHU+2m3q7h319exxioDcwiVwZO
xqUKrvBs6jBtOg4Kvs3sa4AHyP918AA2vp42MwtBdis8O3wx+vm/HoVr0fHum/W1
Z92iwR9JxA4tKoJHVpBwMVnrK7TrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBRovp8hDhWn5AhQOs9fosAUBWEngjAQBgkr
BgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAV5nsa9lK4BISCAuBgMMe
YSPExL5kExPQcFtJtlFjnC5uTC4I0MQQFfuralBQfr4DokDXK5892npt5DAFors5
k60GpH1bRPBaoxJhK0TaSimL6yAZ0fZo380nrVRDZKlug/1VeXF/2hlTeZc73utt
k5zqewqTQO4NHrBp0Udybmpf2L5BJhlctoH490PI0HEbmVDE0WALKXliqsuEZrmm
Mrl0MRRLs2ZBpX2WSqw90IrmpWI3fds2kE2S1DvuaNcc7B8W0hgWT3HxnyuMTyZi
b6Yf7hb5F3ZSOpHFU1bZ22tqk4qouEigyoaUZaLcVhV5UdBCCvwyUl9yU6+EscnM
Ww==
-----END CERTIFICATE-----
```

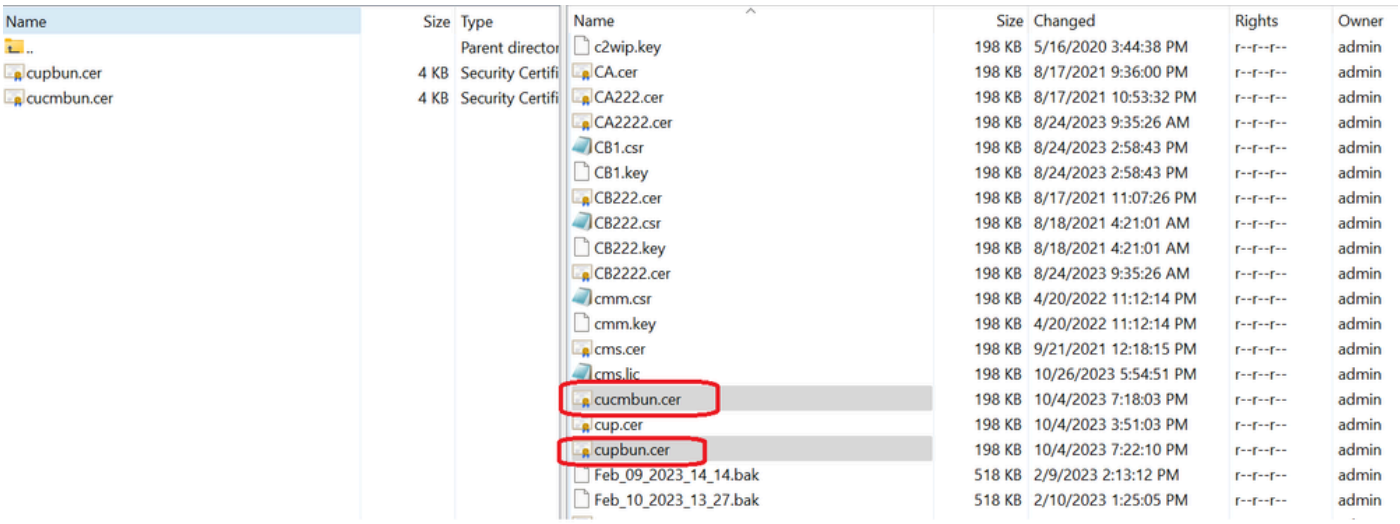
CUPS Certificate

Root Certificate

carriage return

حزمة شهادة *CUPS*

اضغط على شهادات الحزمة التي تم إنشاؤها سابقا إلى خادم CMS من خلال WinSCP.



نسخ حزمة الشهادات إلى *CMS*

تعيين شهادة حزمة TOMCAT على CallBridge باستخدام callbridge ucm certs <cert-bundle>.

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

كاليبريغدي سيرت تراست

تعيين شهادة مجموعة خوادم Cup على CallBridge باستخدام callbridge imps certs <cert-bundle>.

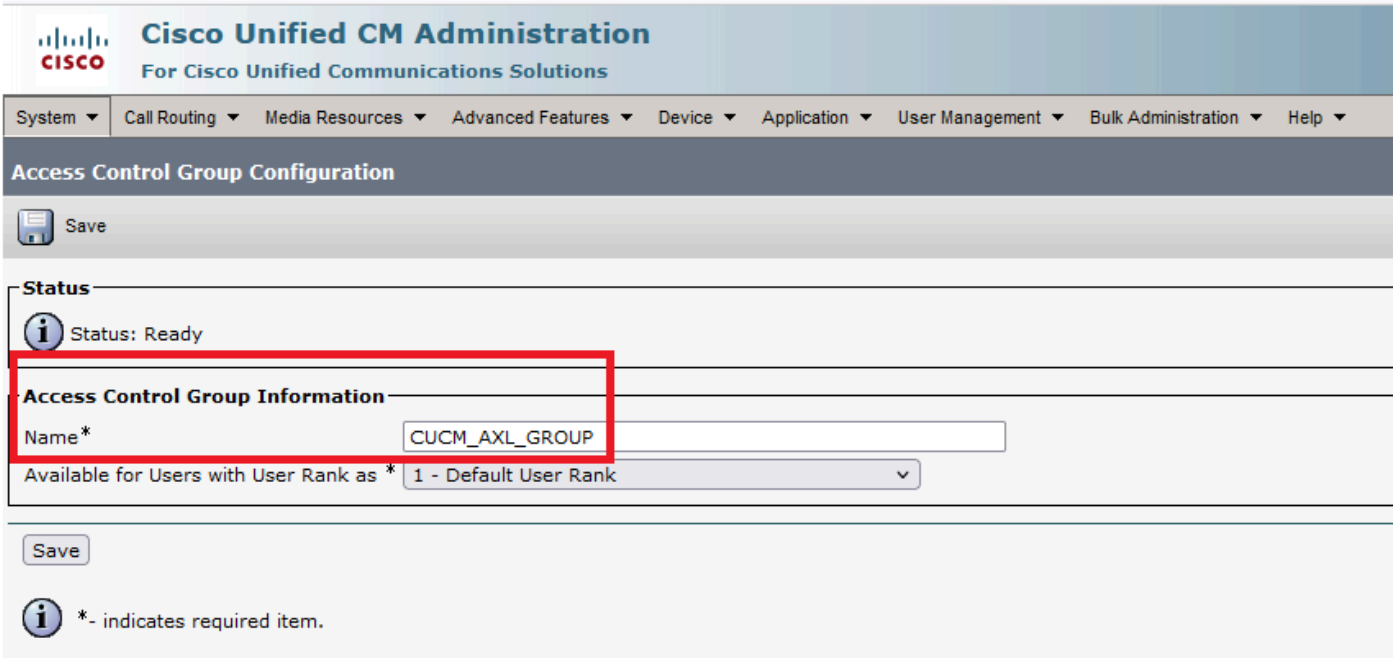
```
wb3>
wb3> callbridge imps certs cupbun.cer
wb3>
```

قم بتشغيلcallbridge الأمر للتحقق من تعيين حزم الشهادات.

```
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>
```

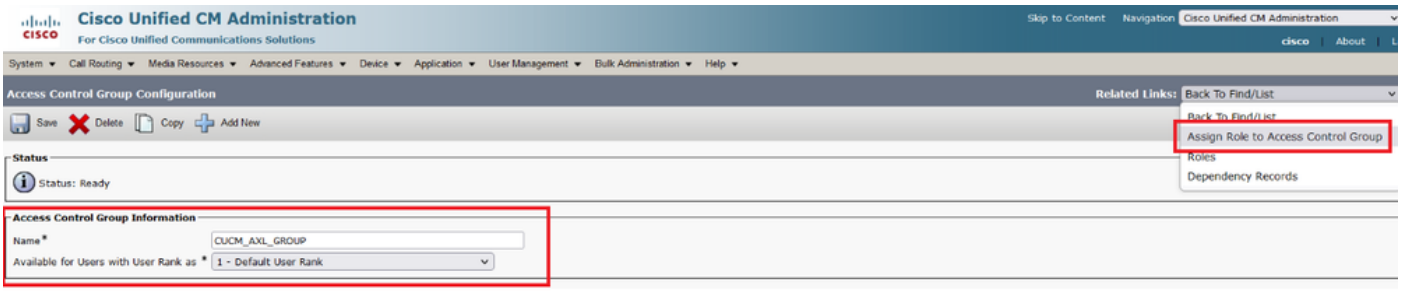
التحقق من شهادة الثقة في *CallBridge*

قم بتسجيل الدخول إلى CUCM كمسؤول CM، انتقل إلى User Management > User Settings > Access Control Group، وانقر Add New، وقم بإنشاء مجموعة تحكم في الوصول CUCM_AXL_Group.

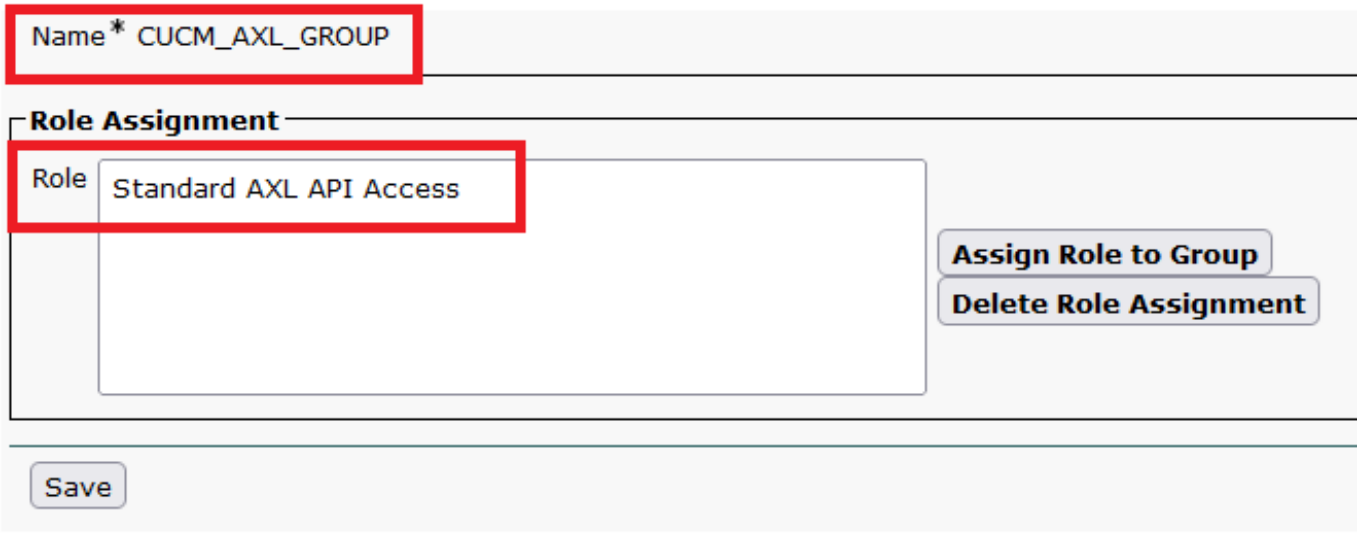


إنشاء مجموعة *AXL*

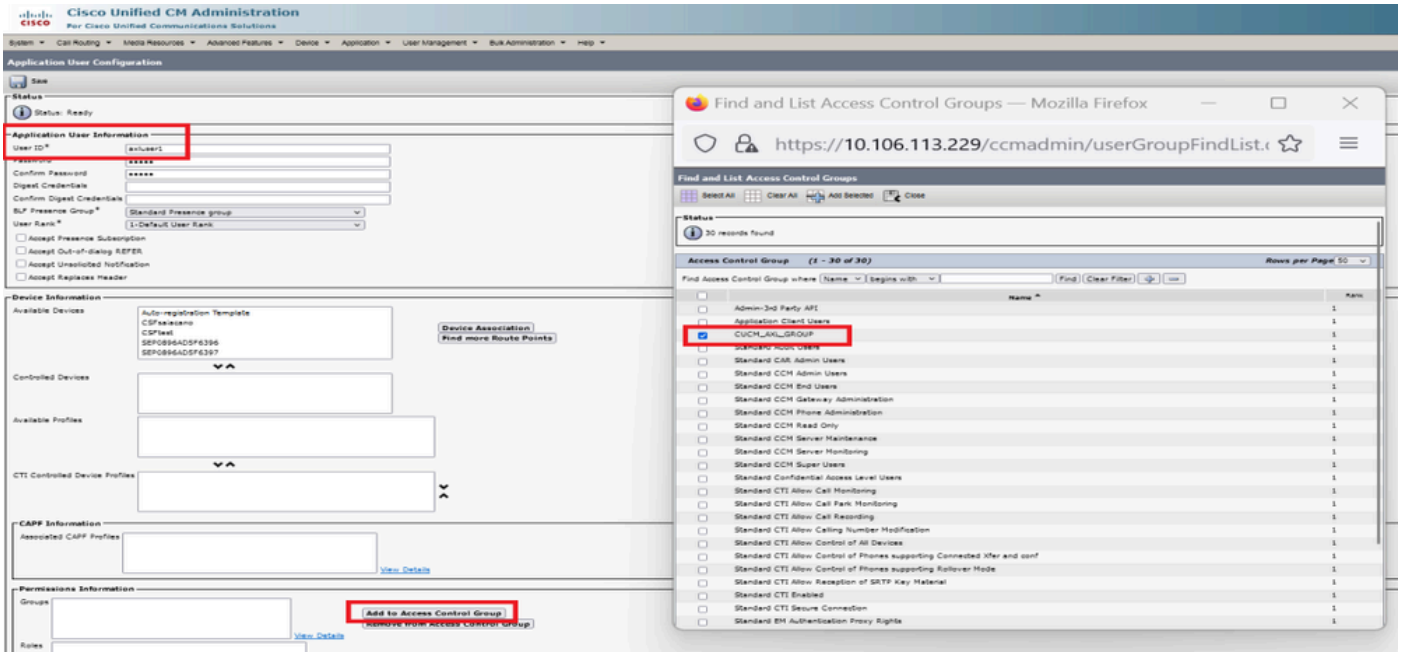
قم بتعيين الدور Standard AXL API Access إلى مجموعة التحكم في الوصول التي تم إنشاؤها مسبقا.



تعيين وصول واجهة برمجة التطبيقات إلى مجموعة *AXL*

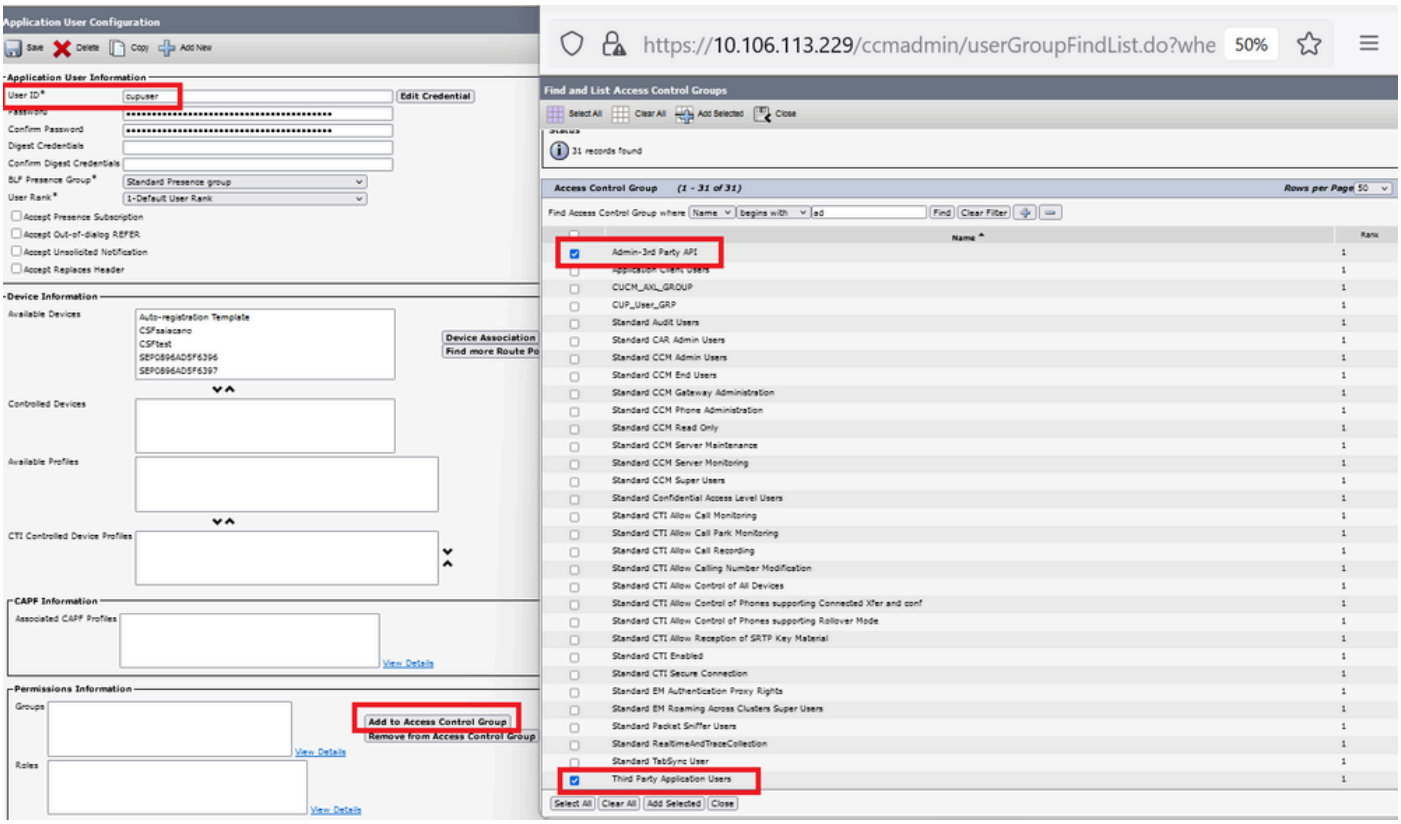


انتقل إلى User Management > Application User، وانقر فوق Add New، ثم قم بإنشاء مستخدم AXLuser للتطبيق. ثم قم بتعيين مجموعة التحكم في الوصول، التي تم إنشاؤها مسبقا.



إنشاء مستخدم وتعيين مجموعة *AXL*

قم بإنشاء مستخدم Cup وتعيين هذين الدورين: Third Party Application Users وAdmin-3rd Party API.

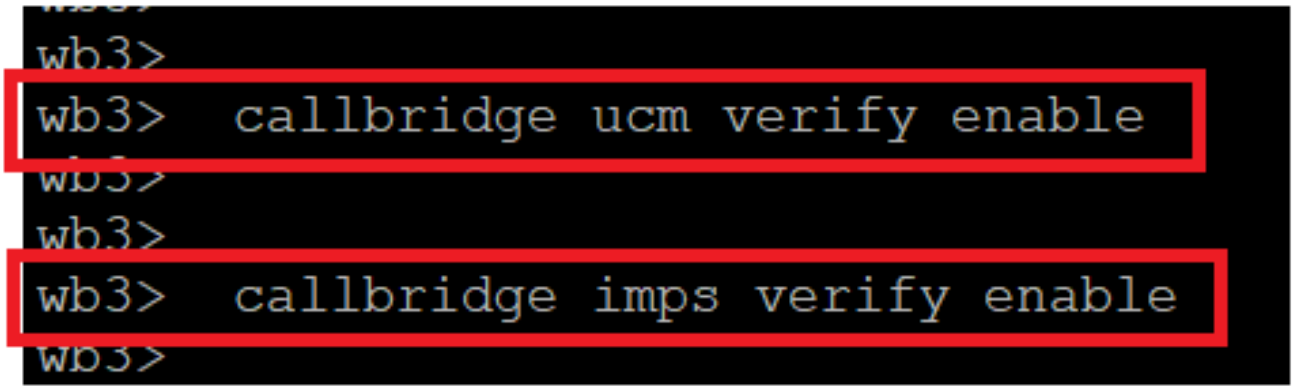


إنشاء مستخدم الكأس

تمكين التحقق من الشهادة لشهادة CUCM و Cisco Unified Communications Manager IM & Presence Service (IMPS) على CMS باستخدام:

callbridge ucm verify <enable/disable>

callbridge imps verify <enable/disable>



التحقق من *CallBridge* من *CUPS* و *CUCM*

تحقق من ذلك من خلال تشغيل callbridge الأمر.

```
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>
```

التحقق من أمر الاستدعاء

قم الآن بإضافة اسم المجال المؤهل بالكامل (FQDN) لـ CUCM و**AXL** و **CUPS** التي تم إنشاؤها سابقا على CMS باستخدام callbridge ucm add <hostname/IP> <axl_user> <presence_user>.

axl_user = مستخدم AXL على CUCM

presence_user = مستخدم CUP الذي تم إنشاؤه مسبقا

```
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>
```

إضافة *CUCM* إلى *CallBridge*

الآن، تحقق مما إذا كانت CMS تثق بخدمات CUCM بمساعدة:

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>
```

حالة *CallBridge AXL*

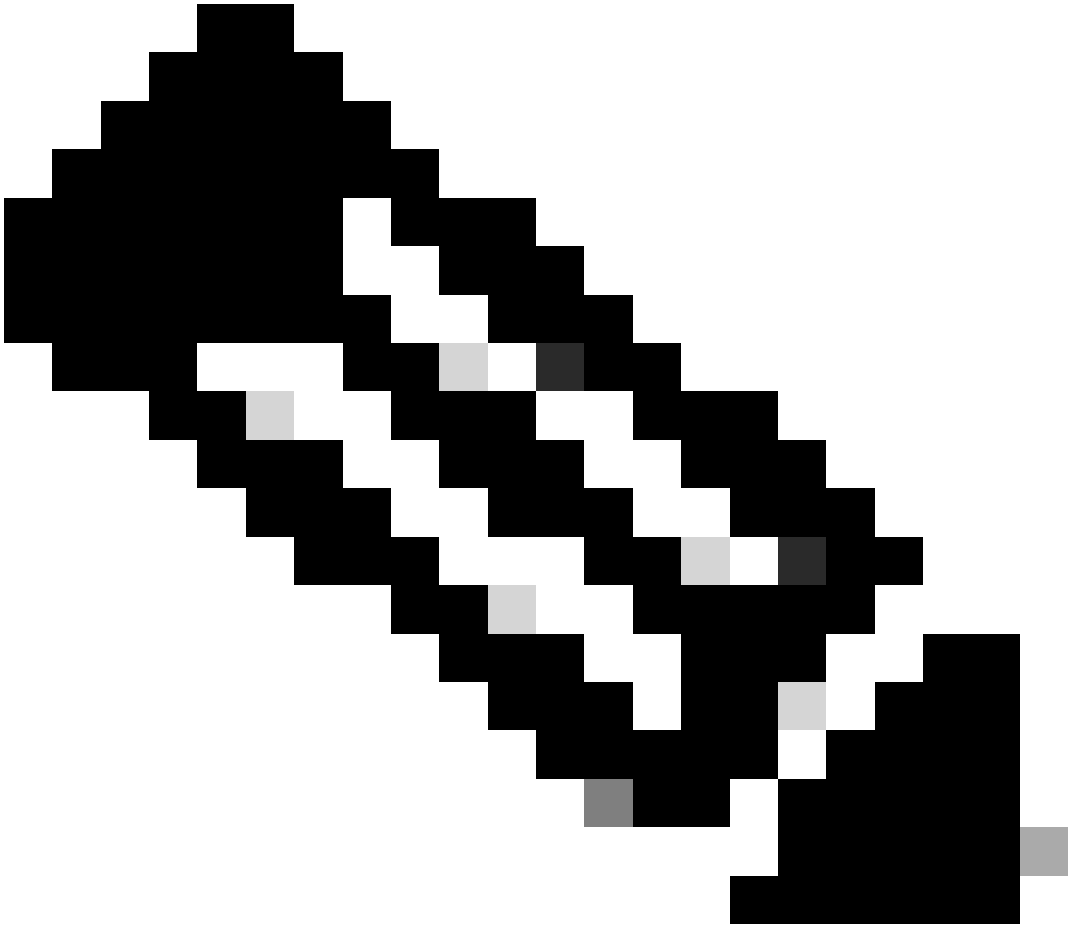
callbridge imps <hostname/IP> <presence_user> presence_service status

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>
```

حالة وجود *CallBridge*

تعني الخدمات المتوفرة أن CUCM و CMS يثقان ببعضهما البعض بالنسبة لخدمات AXL والحضور.



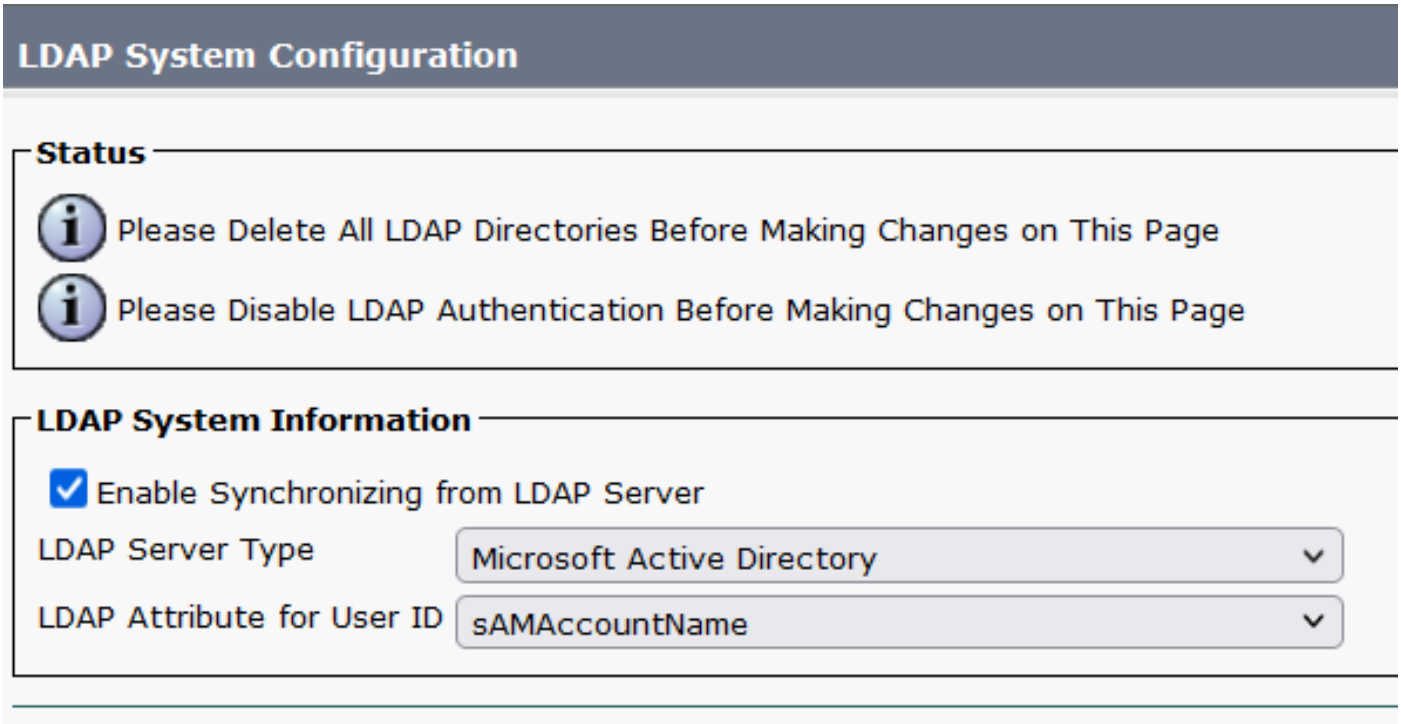
ملاحظة:

يحتوي CUCM على مستخدمي بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) الذين تمت مزامنتهم وتحديثهم أيضا على CUPS. يجب أن يكون لدى المستخدمين نفس معرف مستخدم تطبيق ويب و Jabber JID ويجب أن يتم تسجيلهم في تطبيق ويب بنفس معرف المستخدم، ليتم تحديث التواجد على Jabber.

تكوين CUCM المحدد لمشاركة التواجد بين WebApp وعميل Jabber

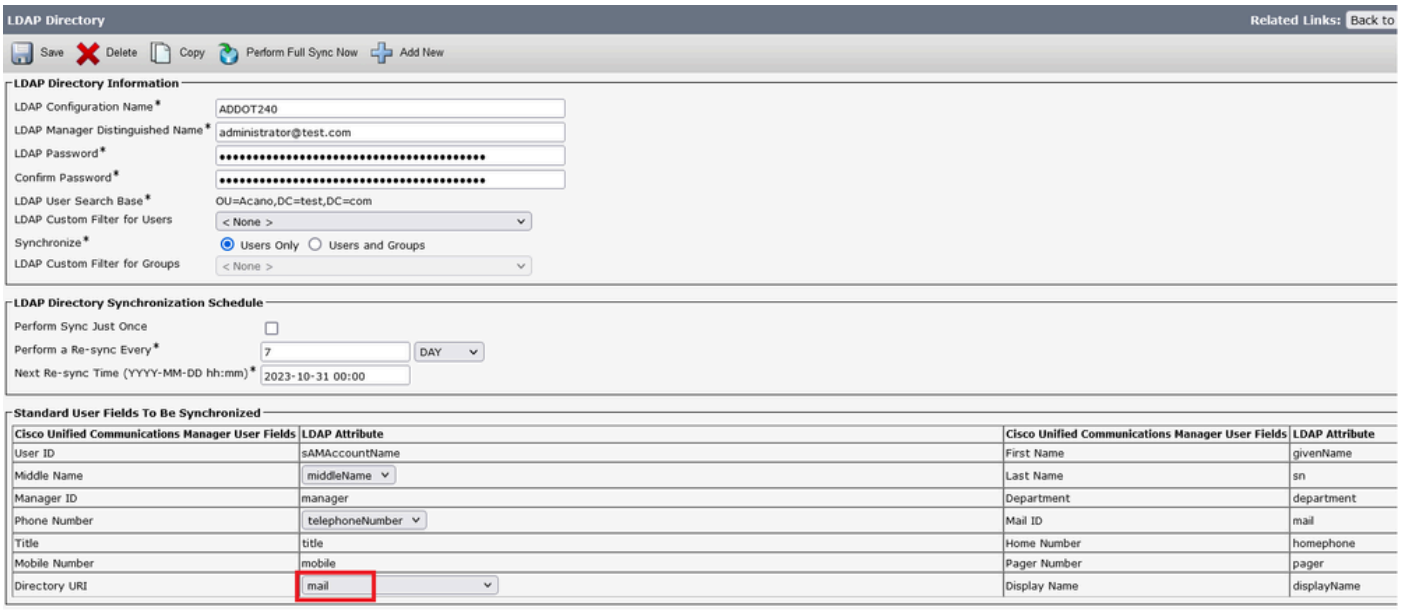
يجب أن يحتوي CUCM على بروتوكول LDAP تم تكوينه.

نظام LDAP:



تكوين *CUCM LDAP 1*

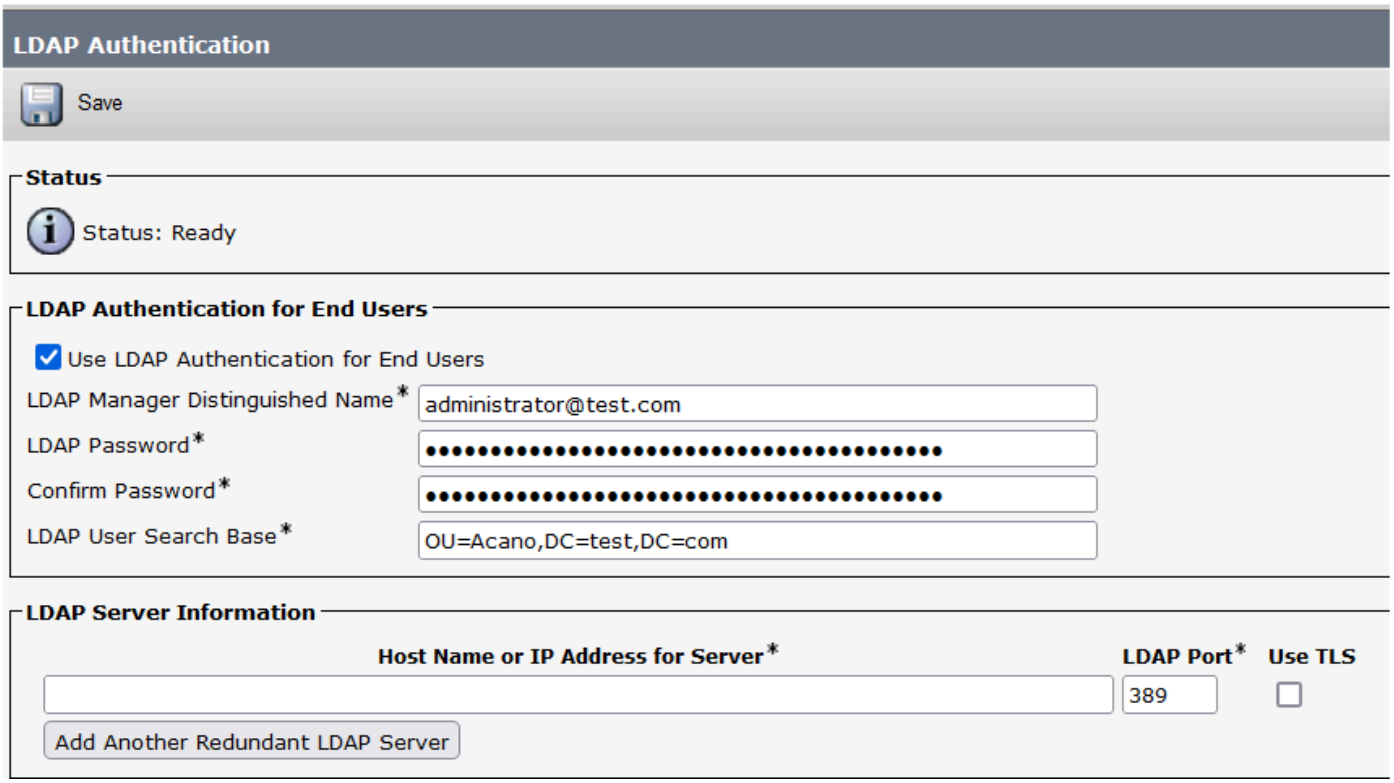
دليل LDAP:



تكوين CUCM LDAP 2

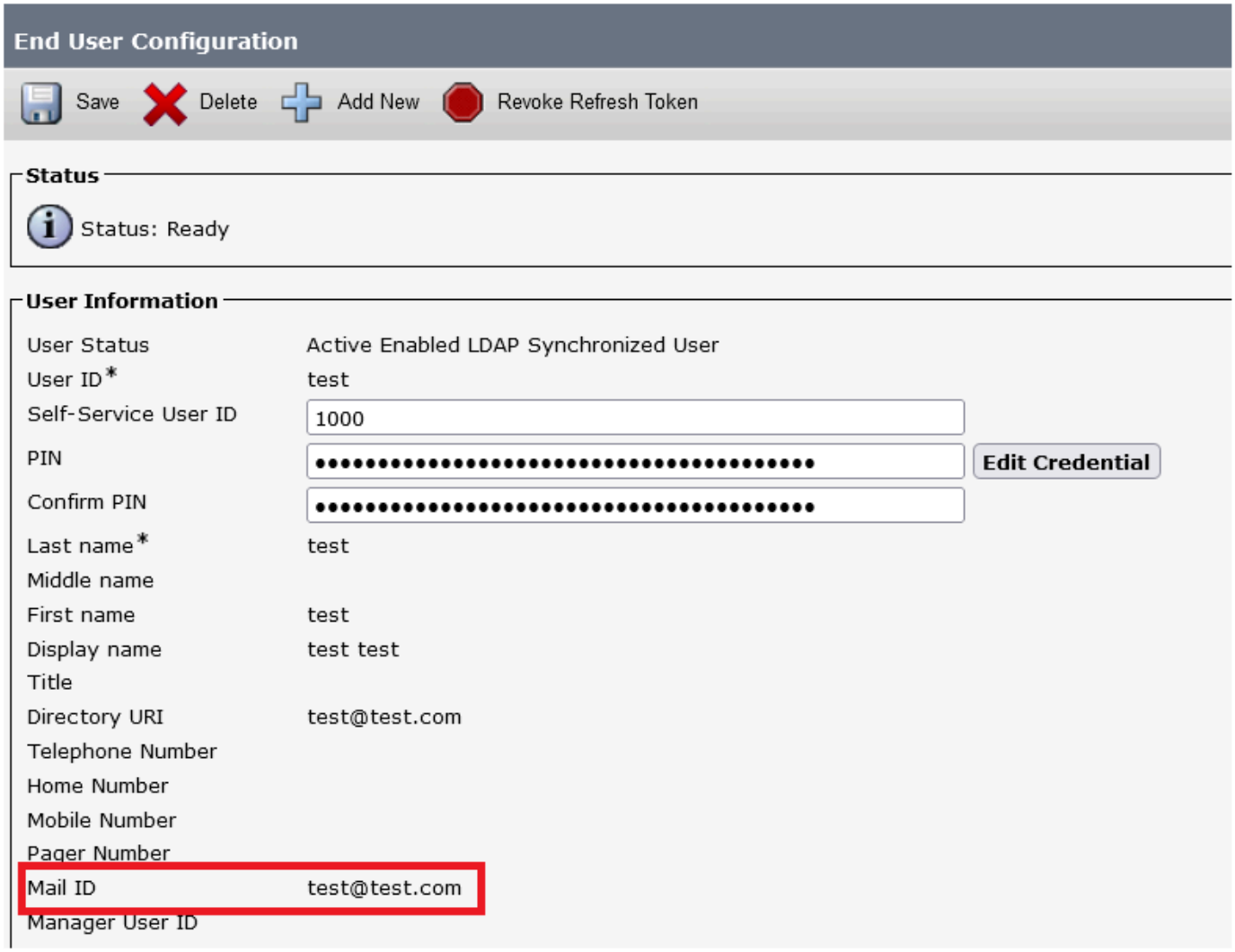
مصادقة LDAP:

تكوين CUCM LDAP 1 CUCM LDAP Configuration 1 CUCM LDAP Configuration 1



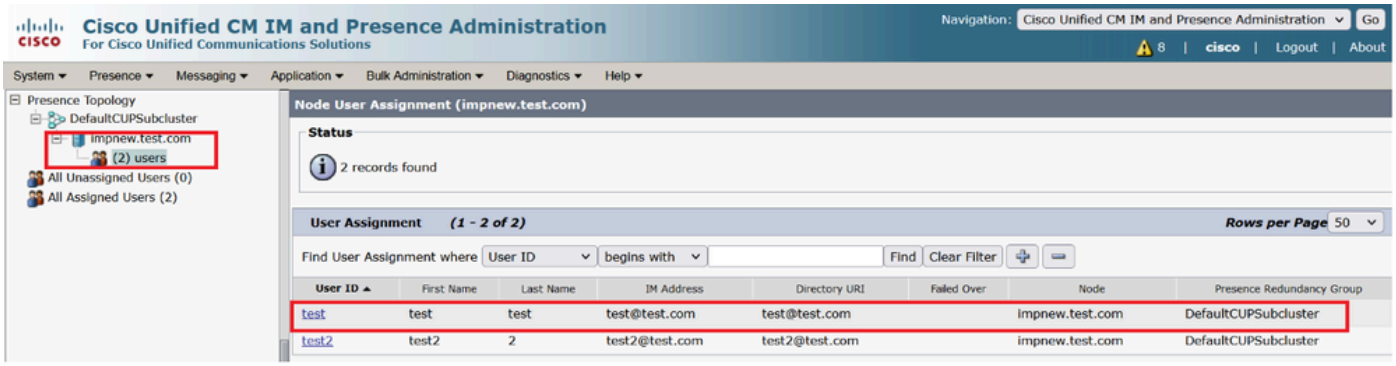
CUCM LDAP Configuration 3

المستخدمون الذين تم سحبهم من LDAP إلى CUCM مع تكوين معرف البريد:



مستخدمون في *CUCM*

تم تحديث مستخدم CUCM على خادم CUPS:



المستخدمون في *CUPS*

تم تكوين دليل LDAP نفسه أيضا على CMS. يتم سحب قاعدة بيانات المستخدم ومزامنتها على CMS.

مستخدمو CMS

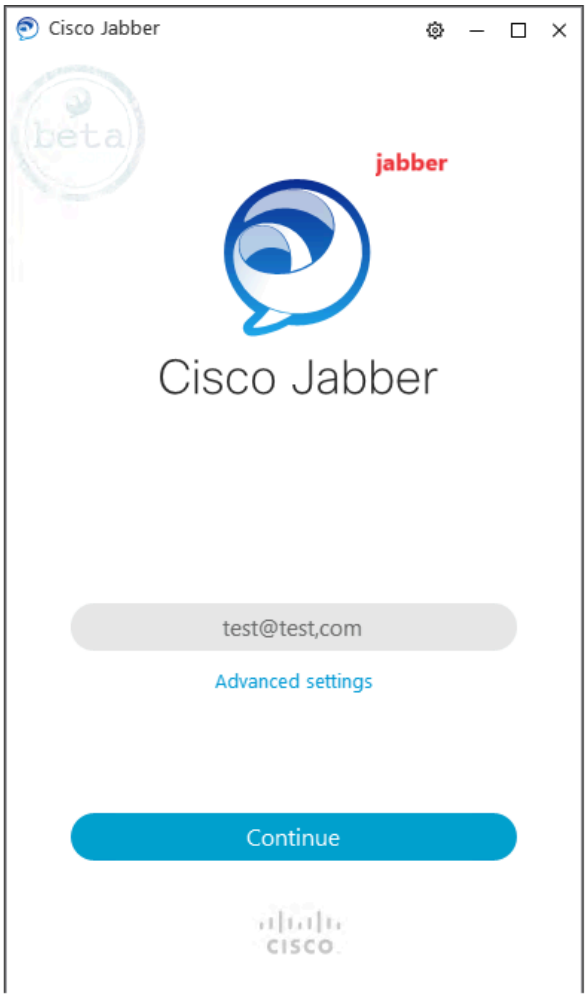
الآن، بما أنك قد قمت بالفعل بالتحقق من أن CMS يمكن أن تثق في CUCM، يمكنك متابعة إختبار التواجد.

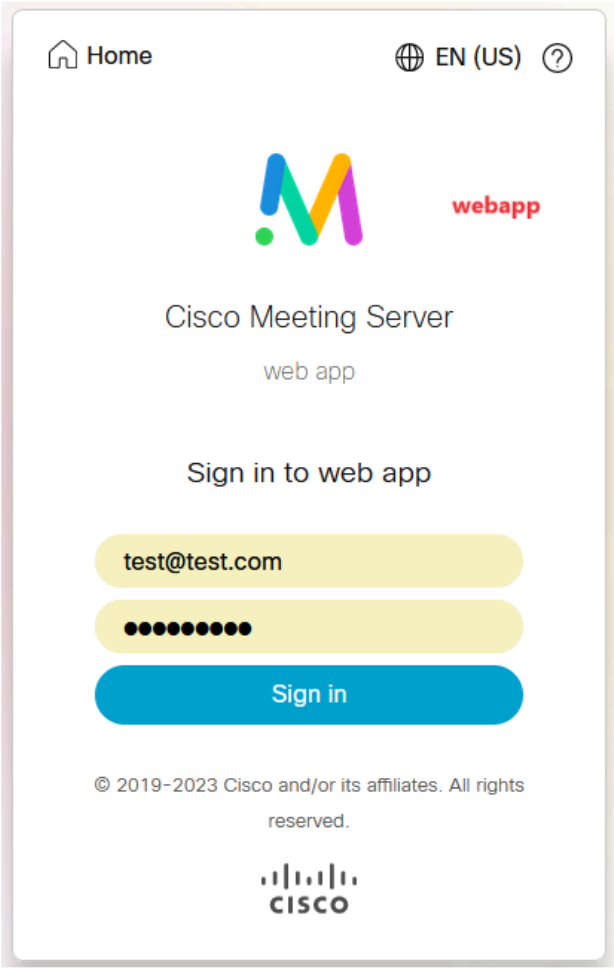
```
wb3>
wb3> callbridge ucm add <hostname/IP> <axl_user> <presence_user>
Only 1 UCM node is allowed. Delete existing UCM node to add a new UCM node.
wb3> callbridge ucm add cucm14test.test.com axluser cupuser
Enter axl user password:
Enter presence user password:
UCM node updated successfully. Restart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

إضافة كوؤس و CUCM إلى CMS

التحقق من الصحة

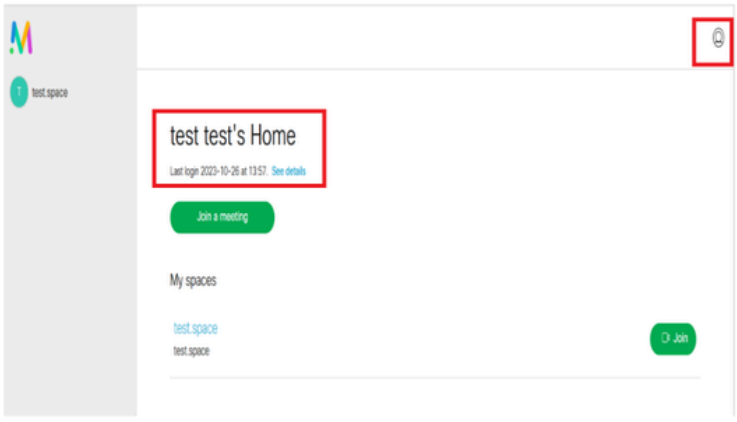
تم التوقيع على عميلين بنفس المستخدم (تمت المزامنة من نفس بروتوكول LDAP):

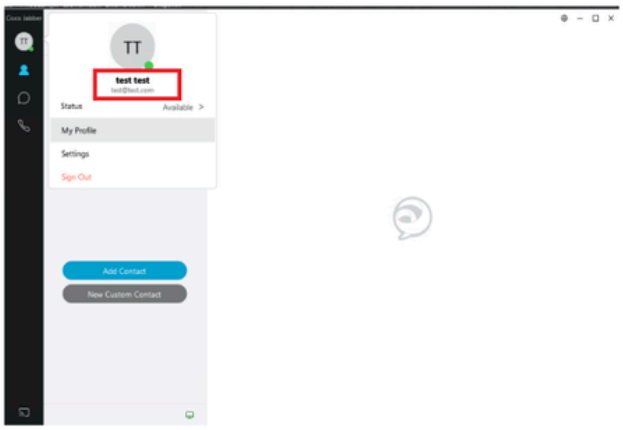




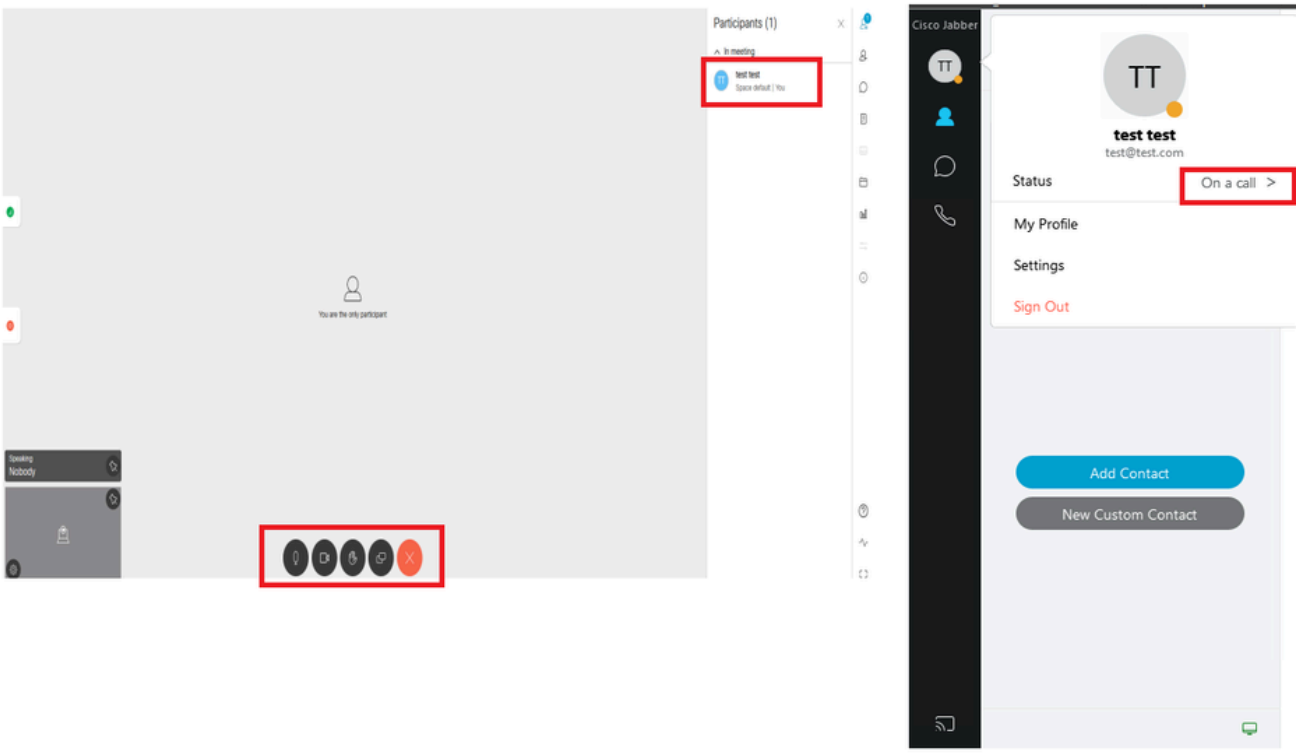
تسجيل دخول المستخدم في *Jabber* و *WebApp*

قام كل الزبونين بتسجيل الدخول إلى نفس المستخدم test@test.com.





التواجد في *Jabber* و *WebApp* قبل الاتصال



تغيير حالة التواجد عند الانضمام من تطبيق ويب

عندما يقوم مستخدم Jabber بتسجيل الدخول إلى تطبيق ويب والانضمام إلى إجتماع، يقوم خادم الاجتماعات بتحديث حالة Jabber إلى "في إجتماع، في مكالمة" ويرتد إلى حالته السابقة بعد أن ينهي المستخدم الاجتماع. على سبيل المثال، إذا كانت حالة المستخدم على Jabber تظهر "متوفر"، يتم تحديثها إلى "في إجتماع، في مكالمة" عندما تكون في إجتماع تطبيق ويب. بعد أن يغادر المستخدم الاجتماع، يتم تعيين حالة Jabber إلى "متوفر" مرة أخرى. إذا كان مستخدم Jabber في إجتماع/مكالمة أخرى أثناء الانضمام إلى إجتماع تطبيق ويب، فلن يقوم خادم الاجتماعات بتحديث حالة Jabber. إذا كان مستخدم Jabber قد قام بتعيين حالته إلى 'DND - عدم الإزعاج' قبل الانضمام إلى إجتماع تطبيق ويب، فإن خادم الاجتماعات لا يقوم بتحديث حالة Jabber. إذا قام المستخدم بتحديث حالة Jabber يدويا في أي وقت أثناء إجتماع تطبيق ويب، لا يتجاوز خادم الاجتماعات حالة المستخدم التي تم تحديثها يدويا.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).