

Configurazione e integrazione CMS singolo combinato

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio 1. Accedere a CMS](#)

[Passaggio 2. Modificare il nome host](#)

[Passaggio 3. Configurare le impostazioni di rete](#)

[Fase 4. Concessione della licenza al CMS](#)

[Passaggio 5. Generare e installare certificati](#)

[Passaggio 6. Record DNS](#)

[Passaggio 7. Configurazione del servizio](#)

[Passaggio 8. Integrare LDAP](#)

[Passaggio 9. Configurazione di CUCM](#)

[Verifica](#)

[Comunicazione Callbridge e XMPP](#)

[Sincronizzazione LDAP con CMS](#)

[Accesso a Webbridge](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare e integrare Cisco Meeting Server (CMS) Single Combined.

i servizi da configurare sono Call Bridge, Webadmin, Web Bridge, Extensible Messaging and Presence Protocol (XMPP) e Lightweight Directory Access Protocol (LDAP)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM)
- Active Directory (AD)
- CA (Certification Authority)
- Client SFTP (Secure File Transfer Protocol)
- Server DNS (Domain Name Service)

Componenti usati

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

- CMS versione 2.3.7
- CUCM versione 11.5.1
- Google Chrome versione 69.0.3497
- WinSCP versione 5.7.7
- Windows Server 2012

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.

Configurazione

Passaggio 1. Accedere a CMS

- La prima volta che si accede a CMS, viene visualizzato il messaggio di benvenuto nella schermata e viene richiesto di eseguire l'accesso
- Le credenziali predefinite sono:

Utente: admin

Password: admin

- Dopo aver immesso le credenziali, il server richiede una nuova password

```
Welcome to the CMS VM
acano login: admin
Please enter password:
Password has expired
Please enter new password:
Please enter new password again:
Failed logins since last successful login 0
acano>
acano> _
```

- Si consiglia di creare un nuovo utente admin. È buona norma nel caso si perda la password di un account.
- Immettere il comando: `utente add <nomeutente> admin`
- Immettere una nuova password e confermarla

```
CMS01> user add anmiron admin
Please enter new password:
Please enter new password again:
Success
CMS01>
```

Passaggio 2. Modificare il nome host

- Questa modifica è facoltativa
- Eseguire il comando `hostname <nome>`
- Riavvia il server
- Eseguire il comando `reboot`

```
acano> hostname CMS01
A reboot is required for the change to take effect
acano>
acano> reboot
Waiting for server to stop...
Waiting for server to stop...
Waiting for server to stop...
Waiting for server to stop...
Waiting for server to stop...
Rebooting...
```

Passaggio 3. Configurare le impostazioni di rete

- Per visualizzare le impostazioni correnti, eseguire il comando `ipv4 a`
- Aggiungi configurazione ipv4
- Eseguire il comando `ipv4 <interface> add <indirizzo_ip>/<subnetmask> <gateway>`

```
CMS01> ipv4 a add 172.16.85.8/27 172.16.85.1
Only interface enabled: setting gateway as default egress route
CMS01>
```

- Configurare il fuso orario
- Eseguire il comando `timezone <timezoneName>`
- Per visualizzare tutti i fusi orari disponibili, eseguire il comando `timezone list`
- Aggiunta di un server NTP (Network Time Protocol)
- Eseguire il comando `ntp server add <indirizzoip>`

```
CMS01> ntp server add 10.88.246.254
CMS01>
CMS01> timezone America/Mexico_City
Reboot the system to finish updating the timezone
CMS01>
CMS01> _
```

- Aggiungi server DNS
- Eseguire il comando `dns add forwardzone <dominio> <dnsip>`

```
CMS01> dns add forwardzone . 172.16.85.2
CMS01>
```

Nota: È possibile configurare un dominio specifico per la ricerca DNS, tuttavia se il DNS può risolvere qualsiasi dominio, utilizzare un punto come dominio

Fase 4. Concessione della licenza al CMS

- Per configurare i servizi CMS, è necessario installare una licenza
- Per generare e installare la licenza, è necessario l'indirizzo MAC (Media Access Control), in quanto le licenze verranno abbinate a tale indirizzo.
- Eseguire il comando **se**
- Copiare l'indirizzo **MAC**
- Per generare una licenza, contattare il rappresentante commerciale.

Nota: Il processo di generazione della licenza non rientra nell'ambito di questo documento.

```
CMS01> iface a
Mac address 00:50:56:96:CD:2A
Configured values:
Auto-negotiation:  default
Speed:             default
Duplex:           default
MTU:              1500
Observed values:
Speed:            10000
Duplex:          full
CMS01>
CMS01>
```

- Una volta ottenuto il file di licenza, rinominarlo in **cms.lic**
- Usare WinSCP o un altro client SFTP per caricare il file nel server CMS

Name	Size	Changed
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM
audit	10 KB	10/6/2018 4:48:03 PM
boot.json	10 KB	10/6/2018 3:59:11 PM
cms.lic	9 KB	10/6/2018 4:47:54 PM
live.json	9 KB	10/6/2018 4:47:54 PM
log	1,440 KB	10/6/2018 4:48:03 PM
logbundle.tar.gz	1 KB	10/6/2018 4:48:03 PM

- Una volta caricato il file, eseguire la **licenza** del comando
- Riavvia il server
- Eseguire il comando **reboot**

```
CMS01> license
Feature: callbridge status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: turn status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: webbridge status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: recording status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: personal status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: shared status: Activated expiry: 2019-Jan-04 (88 days remain)
CMS01>
CMS01> reboot
Waiting for server to stop...
```

Passaggio 5. Generare e installare certificati

- Genera una richiesta di firma del certificato (CSR) per callbridge, webadmin, webbridge e xmpp
- Eseguire il comando `pki csr <service> CN:<servicefqdn>` a tale scopo.

```
CMS01> pki csr callbridge CN:callbridge.anmiron.local
.....
.....
Created key file callbridge.key and CSR callbridge.csr
CSR file callbridge.csr ready for download via SFTP
CMS01>
CMS01> pki csr webadmin CN:cms01.anmiron.local
.....
.....
Created key file webadmin.key and CSR webadmin.csr
CSR file webadmin.csr ready for download via SFTP
CMS01> pki csr webbridge CN:webbridge.anmiron.local
.....
.....
Created key file webbridge.key and CSR webbridge.csr
CSR file webbridge.csr ready for download via SFTP
CMS01>
CMS01> pki csr xmpp CN:xmpp.anmiron.local
.....
...
Created key file xmpp.key and CSR xmpp.csr
CSR file xmpp.csr ready for download via SFTP
```

Nota: In questo esempio viene creato un singolo certificato per ogni server ed è possibile creare un certificato per tutti i servizi. Per ulteriori informazioni sulla creazione di certificati, vedere la [Guida alla creazione di certificati](#)

- Dopo l'esecuzione del comando vengono generati due file: `.csr` e un file `.key`, con il nome del servizio assegnato nei passaggi precedenti.
- Scaricare i file CSR dal server CMS. A tale scopo, utilizzare WinSCP o un altro client SFTP.

Name	Size	Changed
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM
audit	16 KB	10/6/2018 5:04:18 PM
boot.json	10 KB	10/6/2018 3:59:11 PM
callbridge.csr	26 KB	10/6/2018 4:51:02 PM
callbridge.key	26 KB	10/6/2018 4:51:02 PM
cms.lic	26 KB	10/6/2018 5:04:14 PM
live.json	26 KB	10/6/2018 5:04:14 PM
log	1,448 KB	10/6/2018 5:04:16 PM
loqbundle.tar.gz	1 KB	10/6/2018 5:04:19 PM
webadmin.csr	26 KB	10/6/2018 4:51:54 PM
webadmin.key	26 KB	10/6/2018 4:51:54 PM
webbridge.csr	26 KB	10/6/2018 4:54:38 PM
webbridge.key	26 KB	10/6/2018 4:54:38 PM
xmpp.csr	26 KB	10/6/2018 4:59:35 PM
xmpp.key	26 KB	10/6/2018 4:59:35 PM

- Firmare il CSR con un'autorità di certificazione
- Assicurarsi di utilizzare un modello che contenga l'**autenticazione client e server Web**
- Carica il certificato firmato nel server CMS
- Assicurarsi di caricare la **CA radice** e qualsiasi certificato **intermedio** che abbia firmato i certificati

Name	Size	Changed	Righ
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM	r--r-
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM	r--r-
audit	20 KB	10/6/2018 5:14:04 PM	r--r-
boot.json	10 KB	10/6/2018 3:59:11 PM	r--r-
callbridge.cer	37 KB	10/6/2018 5:12:20 PM	r--r-
callbridge.csr	37 KB	10/6/2018 4:51:02 PM	r--r-
callbridge.key	37 KB	10/6/2018 4:51:02 PM	r--r-
cms.lic	37 KB	10/6/2018 5:14:04 PM	r--r-
live.json	37 KB	10/6/2018 5:14:04 PM	r--r-
log	1,451 KB	10/6/2018 5:14:04 PM	r--r-
loqbundle.tar.gz	1 KB	10/6/2018 5:14:04 PM	r--r-
RootCA.cer	37 KB	10/6/2018 5:14:04 PM	r--r-
webadmin.cer	37 KB	10/6/2018 5:12:23 PM	r--r-
webadmin.csr	37 KB	10/6/2018 4:51:54 PM	r--r-
webadmin.key	37 KB	10/6/2018 4:51:54 PM	r--r-
webbridge.cer	37 KB	10/6/2018 5:12:26 PM	r--r-
webbridge.csr	37 KB	10/6/2018 4:54:38 PM	r--r-
webbridge.key	37 KB	10/6/2018 4:54:38 PM	r--r-
xmpp.cer	37 KB	10/6/2018 5:12:27 PM	r--r-
xmpp.csr	37 KB	10/6/2018 4:59:35 PM	r--r-
xmpp.key	37 KB	10/6/2018 4:59:35 PM	r--r-

- Per verificare che tutti i certificati siano elencati in CMS, eseguire il comando **pki list**

```
CMS01> pki list
User supplied certificates and keys:
callbridge.key
callbridge.csr
webadmin.key
webadmin.csr
webbridge.key
webbridge.csr
xmpp.key
xmpp.csr
callbridge.cer
webadmin.cer
webbridge.cer
xmpp.cer
RootCA.cer
CMS01>
```

Passaggio 6. Record DNS

- Creare i record Indirizzo DNS (A) per callbridge, xmpp, webadmin e webbridge
- Assicurarsi che tutti i record puntino all'indirizzo IP del CMS

callbridge	Host (A)	172.16.85.8	static
cms01	Host (A)	172.16.85.8	static
webbridge	Host (A)	172.16.85.8	static
xmpp	Host (A)	172.16.85.8	static

- Crea un record di servizio (SRV) per **client xmpp**
- Il formato del record del servizio è

Servizio client_xmpp

Protocollo _tcp

Port 5222

Destinazione Immettere il nome FQDN XMPP, ad esempio **xmpp.anmiron.local**

_xmpp-client	Service Location (SRV)	[10][10][5222] xmpp.anmiron.local.	static
--------------	------------------------	------------------------------------	--------

Passaggio 7. Configurazione del servizio

Configurare il callbridge:

- Immettere il comando **callbridge Listen <interface>**
- Immettere il comando **callbridge certs <callbridge-key-file> <file-crt> [<pacchetto-certificati>]**
- Il **file di chiave** è la chiave creata al momento della creazione del CSR
- Il **cert-bundle** è il bundle della **CA radice** e di qualsiasi altro certificato intermedio

```
CMS01> callbridge listen a
CMS01>
CMS01> callbridge certs callbridge.key callbridge.cer RootCA.cer
CMS01>
```

Nota: L'interfaccia di ascolto del bridge di chiamate non deve essere impostata su un'interfaccia configurata per l'utilizzo di Network Address Translation (NAT) su un altro indirizzo IP

Configurare webadmin:

- Eseguire il comando **webadmin Listen <interfaccia> <porta>**
- Eseguire il comando **webadmin certs <file-chiave> <file-crt> [<bundle-certificato>]**

```
CMS01> webadmin listen a 445
CMS01>
CMS01> webadmin certs webadmin.key webadmin.cer RootCA.cer
CMS01>
```

Nota: Se il webadmin e il webbridge sono configurati nello stesso server, devono essere configurati su interfacce diverse o essere in ascolto su porte diverse, il webbridge deve essere in ascolto sulla porta 443. Il webadmin è in genere configurato sulla porta 445.

Configurare XMPP:

- Eseguire il comando **xmpp Listen <elenco interfacce>**
- Eseguire il comando **xmpp domain <nome dominio>**
- Eseguire il comando **xmpp certs <file-chiave> <file-crt> [<bundle-crt>]**

```
CMS01> xmpp listen a
CMS01>
CMS01> xmpp domain anmiron.local
CMS01>
CMS01> xmpp certs xmpp.key xmpp.cer RootCA.cer
CMS01>
```

Nota: Il nome di dominio deve corrispondere al dominio in cui sono stati creati i record DNS.

Configurare webbridge:

- Eseguire il comando **webbridge Listen <interfaccia[:port]> whitelist>**
- Eseguire il comando **webbridge certs <file-chiave> <file-crt> [<bundle-crt>]**
- Eseguire il comando **webbridge trust <crt-bundle>**

```
CMS01> webbridge listen a
CMS01>
CMS01> webbridge certs webbridge.key webbridge.cer RootCA.cer
CMS01>
CMS01> webbridge trust callbridge.cer
CMS01>
```

Nota: Il trust **crt-bundle** è il certificato callbridge e deve essere aggiunto al webbridge per consentire al callbridge di considerare attendibile il webbridge. In questo modo verrà abilitata la funzionalità **Join come Guest**.

- Eseguire il comando **callbridge restart**
- Eseguire il comando **wbeadmin enable**
- Eseguire il comando **xmpp enable**
- Eseguire il comando **webbridge enable**

```

CMS01> callbridge restart
SUCCESS: listen interface configured
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
CMS01>
CMS01> webadmin enable
SUCCESS: TLS interface and port configured
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
CMS01>
CMS01> xmpp enable
SUCCESS: Callbridge activated
SUCCESS: Domain configured
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
SUCCESS: XMPP server enabled
CMS01>
CMS01> webbridge enable
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
SUCCESS: Webbridge enabled
CMS01>

```

Nota: Il server deve restituire **SUCCESS** per tutti i servizi. Se restituisce **FAILURE**, rivedere i passaggi precedenti e verificare che la configurazione sia corretta

Per consentire al bridge di chiamate di accedere al servizio XMPP in modo sicuro, è necessario fornire un **nome di componente** per il bridge di chiamate da utilizzare per l'autenticazione con il servizio XMPP.

- Eseguire il comando **xmpp callbridge add <nome componente>**
- Il risultato mostra un segreto, come mostrato nell'immagine

```

CMS01> xmpp callbridge add callbridge
Success          : true
Callbridge      : callbridge
Domain          : anmiron.local
Secret          : 6DwNANabpumutI4pAb1
CMS01>

```

- Copia il valore **Secret**
- Accesso all'interfaccia Web del CMS
- Selezionare **Configurazione > Generale**
- Immettere le informazioni

- Nome bridge di chiamate univoco** Immettere il nome del callbridge creato, ad esempio **callbridge**
- Dominio** Immettere il nome del dominio, ad esempio **anmiron.local**
- Indirizzo server** Impostare l'indirizzo IP del CMS, ad esempio **localhost:5223**
- Segreto condiviso** Immettere il segreto creato nel passaggio precedente, ad esempio **6DwNANabpumut14pAb1**

- Selezionare **Invia**

General configuration

XMPP server settings

Unique Call Bridge name:

Domain:

Server address:

Shared secret: [\[cancel\]](#)

Confirm shared secret:

- Crea una **regola di corrispondenza chiamate in arrivo** per le chiamate in arrivo
- Selezionare **Configurazione > Chiamate in arrivo**
- Immettere le informazioni

Dominio Immettere il nome di dominio del server CMS, ad esempio **anmiron.local**

Priority Immettere un valore per la priorità, ad esempio **0**

Spazi di destinazione Selezionare **sì**

Call matching

<input type="checkbox"/>	Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync	Targets Lync Simplejoin	Tenant	
<input type="checkbox"/>	anmiron.local	0	yes	yes	yes	no	no	no	[edit]
	<input type="text"/>	<input type="text" value="0"/>	yes ▾	yes ▾	yes ▾	no ▾	no ▾		<input type="button" value="Add New"/> <input type="button" value="Reset"/>

- Crea uno spazio per il test
- Selezionare **Configurazione > Spazi**
- Immettere le informazioni

Nome Immettere un nome per lo spazio, ad esempio **spacetest**

parte utente URI Immettere un URI per lo spazio da chiamare, ad esempio **spacetest**

ID chiamata Immetti l'ID chiamata per partecipare a questo Windows Live Spaces da webbridge, ad esempio **spacetest**

Codice di accesso Immettere un numero se si desidera consentire l'accesso allo spazio, se necessario

Space configuration

Filter:

<input type="checkbox"/>	Name	URI user part	Secondary URI user part	Additional access methods	Call ID	Passcode	Default layout	
<input type="checkbox"/>	spacetest	spacetest			spacetest		not set	[edit]

Nota: La **parte utente URI** è ciò che i chiamanti devono comporre nel dominio configurato nella **regola di corrispondenza chiamate in arrivo**, ad esempio il chiamante deve comporre **spacetest@anmiron.local**

- Selezionare **Configurazione > Generale > Impostazioni bridge Web**
- Immettere le informazioni

URI client account guest

Questa è l'interfaccia Web di webbridge, ad esempio <https://webbridge.anmiron.local>

Dominio JID account guest

Il dominio configurato in CMS, ad esempio `anmiron.local`

Accesso guest tramite collegamento ipertestuale

Selezione consentita

Web bridge settings

Guest account client URI	<input type="text" value="https://webbridge.anmiron.local"/>
Guest account JID domain	<input type="text" value="anmiron.local"/>
Guest access via ID and passcode	<input type="text" value="secure: require passcode to be supplied with ID"/>
Guest access via hyperlinks	<input type="text" value="allowed"/>
User sign in	<input type="text" value="allowed"/>
Joining scheduled Lync conferences by ID	<input type="text" value="not allowed"/>

Passaggio 8. Integrare LDAP

- Aprire l'interfaccia Web CMS
- Selezionare **Configurazione > Active Directory**
- Immettere le informazioni

Indirizzo	L'indirizzo IP del server LDAP, ad esempio 172.16.85.28
Port	Questo valore è 389 se si utilizza una connessione non protetta e 636 se è richiesta una connessione protetta
Username	Immettere un amministratore del server LDAP, ad esempio anmiron\administrator
Password	Immettere la password dell'utente amministratore
Nome distinto di base	Si tratta di un'impostazione di Active Directory, ad esempio CN=Users, DC=anmiron, DC=local
Filtro	Si tratta di un'impostazione di Active Directory, ad esempio (memberof=CN=CMS, CN=Users, DC=anmiron, DC=local)
Nome visualizzato	Modalità di visualizzazione del nome utente, ad esempio \$cn\$
Username	ID di accesso dell'utente, ad esempio \$sAMAccountName\$@anmiron.local
Nome spazio	Modalità di visualizzazione dello spazio, ad esempio \$sAMAccountName\$ Space
Parte utente URI spazio	URI da comporre, ad esempio \$sAMAccountName\$.call
ID chiamata spazio	ID chiamata da utilizzare da webbridge, ad esempio \$sAMAccountName\$.space

Active Directory Server Settings

Address	<input type="text" value="172.16.85.28"/>
Port	<input type="text" value="389"/>
Secure connection	<input type="checkbox"/>
Username	<input type="text" value="anmiron\administrator"/>
Password	<input type="password" value="....."/> [cancel]
Confirm password	<input type="password" value="....."/>

Import Settings

Base distinguished name	CN=Users,DC=anmiron,DC=local
Filter	(memberof=CN=CMS,CN=Users,DC=anmiron,DC=local)

Field Mapping Expressions

Display name	\$cn\$
Username	\$\$AMAccountName\$@anmiron.local
Space name	\$\$AMAccountName\$ Space
Space URI user part	\$\$AMAccountName\$.call
Space secondary URI user part	
Space call ID	\$\$AMAccountName\$.space

- Selezionare **Invia**
- Seleziona **Sincronizza**

Il nome distinto di base e il filtro sono impostazioni di Active Directory. In questo esempio vengono fornite informazioni di base per ottenere informazioni con l'Editor attributi in Active Directory. Per aprire Nell'Editor attributi, abilitare **Funzionalità avanzate** in Active Directory. Passare a **Utenti e computer > Visualizza** e selezionare **Caratteristiche avanzate**

- Per questo esempio viene creato un gruppo denominato **CMS**
- Aprire la funzionalità **Utenti e computer** in Active Directory
- Selezionare un **utente** a destra e aprire le proprietà
- Passare all'**Editor attributi**
- Nella colonna **Attributo** individuare il campo **distinguishedName**

The image shows two screenshots of the Active Directory console. The left screenshot shows the 'Users Properties' dialog box with the 'Attribute Editor' tab selected. The 'Attributes' list shows 'distinguishedName' with the value 'CN=Users,DC=anmiron,DC=local'. A 'String Attribute Editor' dialog box is overlaid on top, showing the 'Attribute: distinguishedName' and 'Value: CN=Users,DC=anmiron,DC=local'. The right screenshot shows the 'CMS Properties' dialog box with the 'Attribute Editor' tab selected. The 'Attributes' list shows 'distinguishedName' with the value 'CN=CMS,CN=Users,DC=anmiron,DC=local'. A 'String Attribute Editor' dialog box is overlaid on top, showing the 'Attribute: distinguishedName' and 'Value: CN=CMS,CN=Users,DC=anmiron,DC=local'. Both dialog boxes have 'Clear', 'OK', and 'Cancel' buttons.

Nota: Per ulteriori informazioni sui filtri LDAP, consultare la [Guida all'implementazione di CMS](#)

Passaggio 9. Configurazione di CUCM

- Aprire l'interfaccia Web di CUCM
- Selezionare **Dispositivo > Trunk**
- Selezionare **Aggiungi nuovo**
- Nel menu a discesa **Tipo di trunk** selezionare **SIP Trunk**
- Seleziona **successivo**

Trunk Information

Trunk Type*

Device Protocol*

Trunk Service Type*

- Immettere le informazioni

Nome dispositivo Immettere un nome per il trunk SIP, ad esempio **TrunkToCMS**

Indirizzo di destinazione Immettere l'indirizzo IP del CMS o il nome di dominio completo del bridge di chiamata ad esempio **172.16.85.8**

Porta di destinazione Immettere la porta di ascolto del CMS, ad esempio **5060**

Profilo di sicurezza trunk SIP Selezionare il profilo protetto, ad esempio **Profilo trunk SIP non protetto**

Profilo SIP Seleziona **profilo SIP standard per TelePresence Conferencing**

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="172.16.85.8"/>	<input type="text"/>	<input type="text" value="5060"/>

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

- Selezionare **Salva**
- Selezionare **Reset**
- Selezionare **Instradamento chiamate > Schema instradamento SIP > Aggiungi nuovo > Seleziona instradamento dominio**
- Immettere le informazioni

Modello IPv4 Immettere il dominio configurato per CMS, ad esempio **anmiron.local**

Elenco trunk/route SIP Selezionare il SIP Trunk creato in precedenza, **TrunktoCMS**

Pattern Definition

Pattern Usage: Domain Routing

IPv4 Pattern*:

IPv6 Pattern:

Description:

Route Partition:

SIP Trunk/Route List*: [\(Edit\)](#)

Block Pattern

- Selezionare **Salva**

Verifica

Comunicazione Callbridge e XMPP

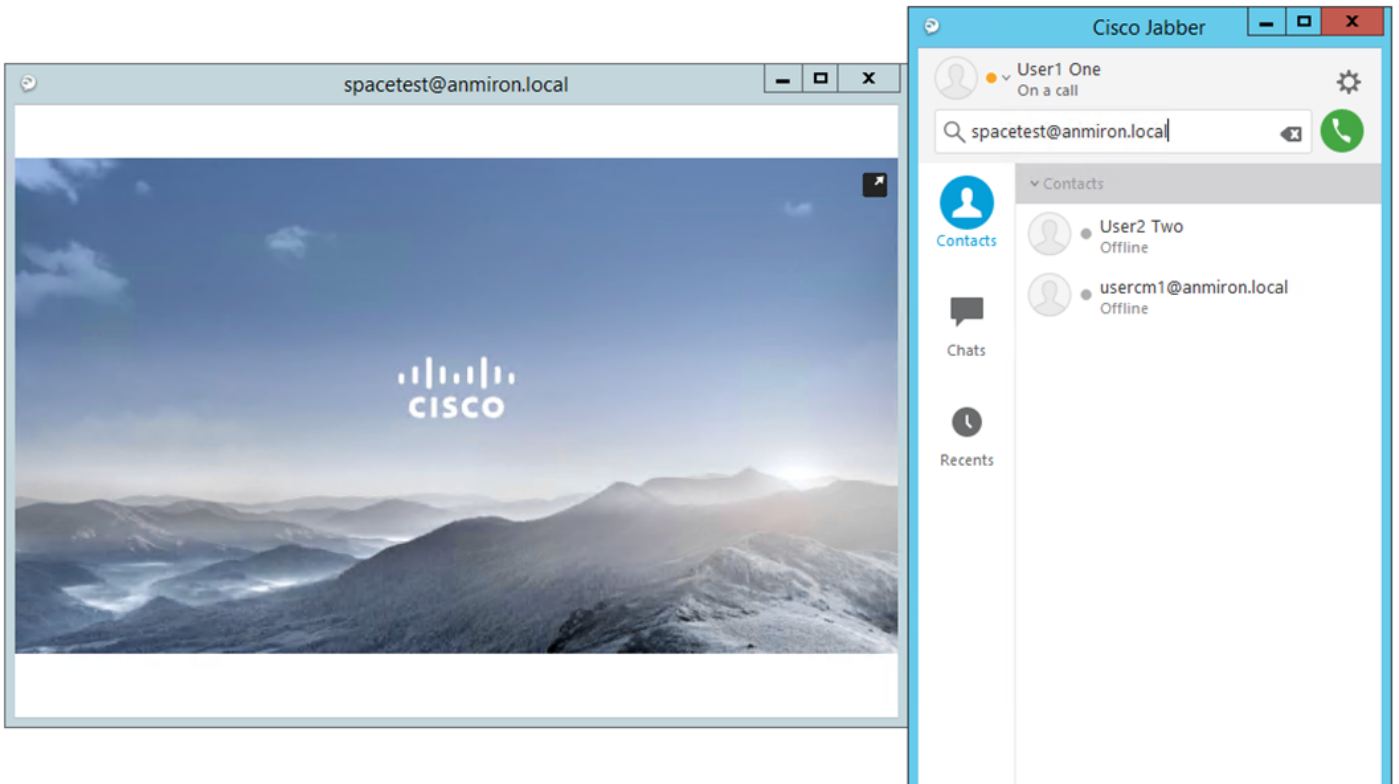
- Aprire l'interfaccia Web di CMS
- Selezionare **Stato > Generale**
- Lo stato della connessione XMPP deve essere connesso a localhost



System status

Uptime	12 minutes, 47 seconds
Build version	2.3.7
XMPP connection	connected to localhost (secure) for 55 seconds
Authentication service	registered for 54 seconds

- Effettua una chiamata da un dispositivo registrato su CUCM
- Comporre l'URI **spacetest@anmiron.local**



- Aprire l'interfaccia Web di CMS
- Selezionare **Stato > Chiamate**
- La chiamata deve essere visualizzata come **chiamata attiva**

Active Calls

Filter Show only calls with alarms

Conference: spacetest (1 active call)

<input type="checkbox"/>	SIP 30103@anmiron.local [more] (incoming, unencrypted)
--------------------------	------------------------------------------------------------------------

1

Sincronizzazione LDAP con CMS

- Aprire l'interfaccia Web CMS
- Passare a **Stato > Utenti**
- È necessario visualizzare l'elenco completo degli utenti

Users

Filter

Name	Email	XMPP ID
CMS User1	cmsuser1@anmiron.local	cmsuser1@anmiron.local
CMS User2	cmsuser2@anmiron.local	cmsuser2@anmiron.local

- Selezionare **Configurazione > Spazi**
- Assicurarsi che ogni utente disponga di un proprio spazio

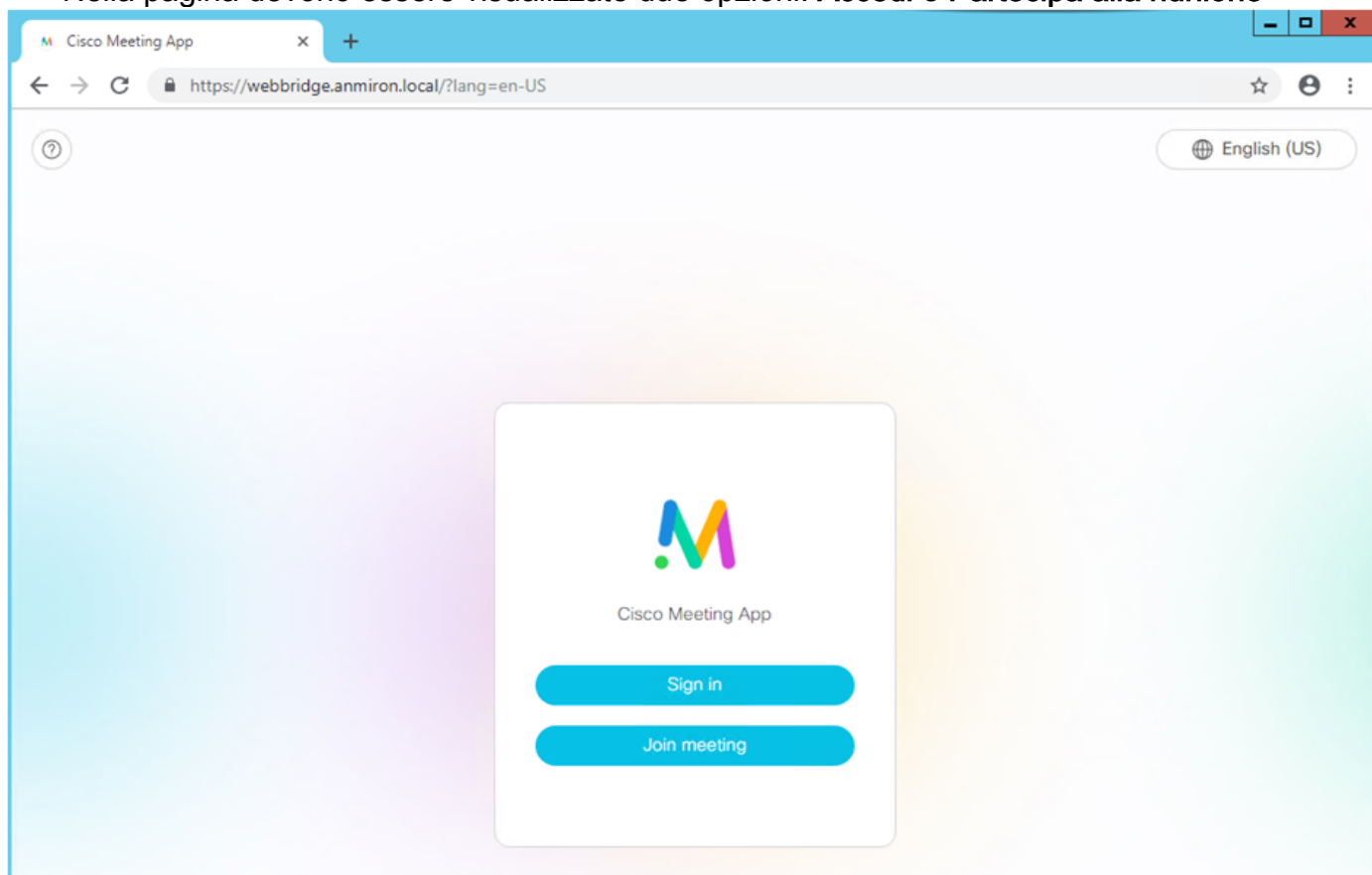
Space configuration

Name	URI user part	Secondary URI user part	Additional access methods	Call ID	Passcode	Default layout	
<input checked="" type="checkbox"/> cmsuser1 Space	cmsuser1.call			cmsuser1.space		not set	[edit]
<input type="checkbox"/> cmsuser2 Space	cmsuser2.call			cmsuser2.space		not set	[edit]
<input type="checkbox"/> spacetest	spacetest			spacetest		not set	[edit]
<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	not set	[Add New] [Reset]

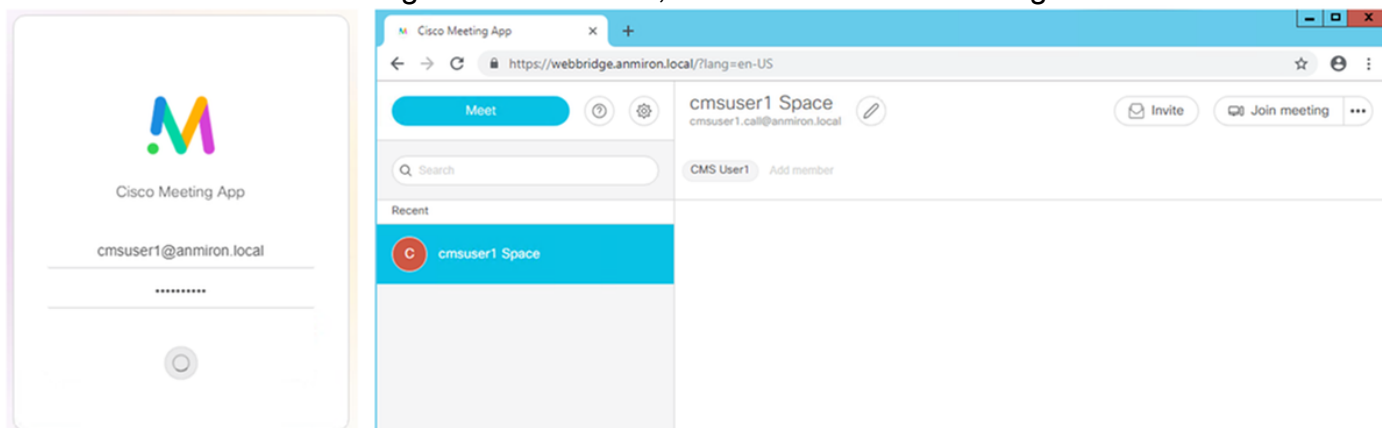
1
[Delete]

Accesso a Webbridge

- Utilizzare il browser Web per accedere alla pagina Web configurata per il servizio webbridge, <https://webbridge.anmiron.local>
- Nella pagina devono essere visualizzate due opzioni: **Accedi** e **Partecipa alla riunione**



- Gli utenti precedentemente integrati da AD devono essere in grado di eseguire l'accesso
- Seleziona **accesso**
- Immettere il **nome utente** e la **password**
- L'utente deve essere in grado di **accedere**, come mostrato nell'immagine



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.