

Configurazione di Cisco Meeting Server e delle conferenze ad hoc CUCM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione di CMS](#)

[Configurazione di CUCM](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare le conferenze ad hoc con Cisco Meeting Server (CMS) e Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione e configurazione CMS
- Registrazione endpoint CUCM e creazione trunk
- Certificati firmati

Componenti usati

- CUCM
- CMS Server 2.0.X e versioni successive
- I componenti Webadmin e Call Bridge devono essere già configurati nel CMS
- Record DNS (Domain Name System) interni per Call Bridge e Webadmin, risolvibili in indirizzo IP del server CMS
- Autorità di certificazione (CA) interna per firmare il certificato con l'utilizzo chiavi avanzato per l'autenticazione del server Web e del client Web
- Certificati firmati per la comunicazione Transport Layer Security (TLS)

Nota: I certificati autofirmati non sono supportati per questa distribuzione perché richiedono l'autenticazione del server Web e del client Web che non consente di aggiungere certificati autofirmati

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. Il documento può essere consultato per tutte le versioni software o hardware, ma è necessario soddisfare i requisiti minimi di versione.

Configurazione

Configurazione di CMS

Passaggio 1. Creare un account utente amministratore con privilegi API (Application Program Interface).

- Aprire una sessione SSH (Secure Shell) sul processore di gestione della scheda madre (MMP)
- Per aggiungere un account utente a livello di amministrazione, eseguire il comando **user add <nomeutente> <ruolo>**
- Immettere la password, come illustrato nell'immagine.

```
cb1> user add apiadmin admin
Please enter new password:
Please enter new password again:
Success
```

Passaggio 2. Generare i certificati.

- Eseguire il comando **pki csr <nome file> CN:<nome comune> subjectAltName:<nomi alternativi soggetto>**
- Utilizzare le informazioni in base alle proprie esigenze

Nome file certo

CN tptac9.com

NomeOggetto cmsadhoc.tptac9.com.10.106.81.32

- Non utilizzare caratteri jolly per generare il certificato. Un certificato con caratteri jolly non è supportato da CUCM
- Verificare che il certificato sia firmato con l'autenticazione server Web e client Web con utilizzo chiavi avanzato

Nota: Per utilizzare lo stesso certificato per tutti i servizi, il nome comune (CN) deve essere il nome di dominio e il nome degli altri servizi CMS deve essere incluso come nome alternativo soggetto (SAN). In questo caso anche l'indirizzo IP è firmato dal certificato e considerato attendibile da qualsiasi computer in cui sia installato il certificato radice.

Configurazione di CUCM

Passaggio 1. Caricare i certificati nell'archivio protetto di CUCM.

- Il certificato radice può essere scaricato dall'interfaccia Web interna di Certification Authority **Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [tptac9-WIN-TI6UAFTSEEV-CA-1] ▲
▼

Encoding method:

- DER
 Base 64

[Install CA certificate](#)


[Download CA certificate](#)

- Aggiungere il certificato del bridge di chiamate e il certificato del bundle (intermedio e radice) all'archivio di attendibilità di CallManager

Upload Certificate/Certificate chain



 Upload  Close

Status


 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*
Description(friendly name)
Upload File CA-cert.cer

 Upload  Close

Status

 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*
Description(friendly name)
Upload File certall.cer

Se si dispone di certificati separati per Call Bridge e Webadmin, assicurarsi di caricare:

- I certificati di Webadmin, Call Bridge e Root per l'archivio di attendibilità di Gestione chiamate in CUCM

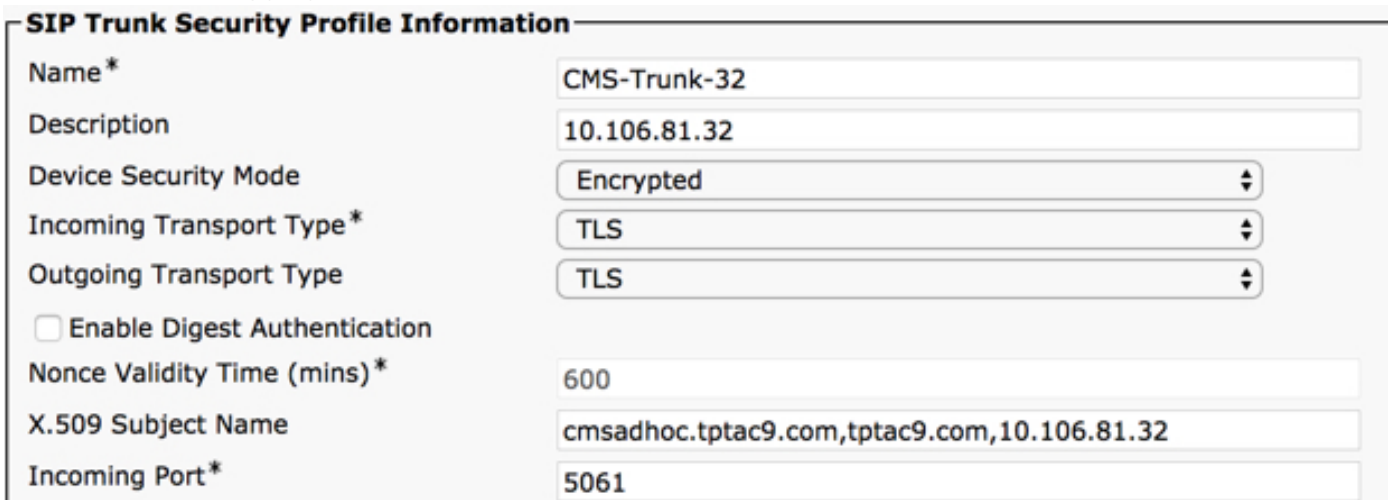
Nota: Il trunk SIP CUCM può essere creato come trunk SIP non protetto. In questo caso, non è necessario caricare il certificato del bridge di chiamate nell'archivio di trust CallManager, ma è necessario caricare il certificato radice che ha firmato il certificato webadmin nell'archivio di trust CallManager.

Passaggio 2. Configurare un profilo trunk SIP sicuro.

- Aprire l'interfaccia Web CUCM
- Selezionare **Sistema > Sicurezza > SIP Trunk Security Profile**
- Selezionare **Aggiungi nuovo**
- Immettere i valori con le informazioni corrette

Nome	Immettere un nome, ad esempio CMS-Trunk-32
Modalità di protezione del dispositivo	Seleziona crittografato
Tipo di trasporto in ingresso	Seleziona TLS
Tipo di trasporto in uscita	Seleziona TLS
Nome soggetto X.509	Immettere il CN del certificato del bridge di chiamate separando i nomi virgole
Porta in ingresso	Immettere la porta per la ricezione delle richieste TLS. Il valore predefinito è 5061

- Selezionare **Salva**



SIP Trunk Security Profile Information

Name*	CMS-Trunk-32
Description	10.106.81.32
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	cmsadhoc.tptac9.com,tptac9.com,10.106.81.32
Incoming Port*	5061

Passaggio 3. Creazione del trunk SIP

- Selezionare **Device > Trunk**
- Selezionare **Aggiungi nuovo**
- Selezionare **SIP Trunk** per il tipo di trunk
- Seleziona **successivo**
- Immettere i valori applicabili

Nome dispositivo	Immettere un nome per il trunk SIP, ad esempio CMS-Abhishek-32
Indirizzo di destinazione	Immettere l'indirizzo IP del CMS o il nome di dominio completo del bridge di chiamate ad esempio 10.106.81.32
Porta di destinazione	Immettere la porta su cui il CMS resta in ascolto delle comunicazioni TLS, ad esempio 5061
Profilo di sicurezza	Selezionare il profilo protetto creato al passaggio 2, CMS-Trunk-32

trunk SIP Profilo SIP

Seleziona profilo SIP standard per TelePresence Conferencing

SIP Information						
Destination						
<input type="checkbox"/> Destination Address is an SRV						
Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration	
1* 10.106.81.32		5061	up		Time Up: 0 day 0 hour minutes	
MTP Preferred Originating Codec*	711ulaw					
BLF Presence Group*	Standard Presence group					
SIP Trunk Security Profile*	CMS-Trunk-32					
Rerouting Calling Search Space	< None >					
Out-Of-Dialog Refer Calling Search Space	< None >					
SUBSCRIBE Calling Search Space	< None >					
SIP Profile*	Standard SIP Profile For TelePresence Conferencing					View Details
DTMF Signaling Method*	No Preference					

Passaggio 4. Creare il bridge per conferenze

- Selezionare **Risorse multimediali > Conference Bridge**
- Selezionare **Aggiungi nuovo**
- Selezionare **Cisco TelePresence Conductor** dal menu a discesa **Conference Bridge**

Nota: Da CUCM versione 11.5.1 SU3, l'opzione **Cisco Meeting Server** è disponibile per essere selezionata come **Conference Bridge Type** nel menu a discesa

- Inserisci le informazioni corrette

Nome bridge per conferenze

Descrizione

SIP Trunk

Sostituisci destinazione trunk SIP come indirizzo HTTP

Nome host/Indirizzo IP

Username

Password

Conferma password

Usa HTTPS

Porta HTTP

Immettere un nome per il dispositivo, ad esempio **CMS-Adh**

Immettere una descrizione per il bridge per conferenze, ad esempio **10.106.81.32**

Selezionare il trunk SIP creato nel passaggio 3, **CMS-Abhis**
32

Selezionare questa casella se è necessario un nome diverso

Immettere il nome host o l'indirizzo IP del CMS, ad esempio
10.106.81.32

Immettere l'utente creato in CMS con privilegi API, ad esem
admin

Immettere la password dell'utente API

Immettere la password un'altra volta

Selezionare la casella, necessaria per la connessione CMS

Immettere la porta CMS webadmin, ad esempio **443**

Conference Bridge Configuration
Relat

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Status

Status: Ready

Conference Bridge Information

Conference Bridge : CMS-Adhoc-32 (10.106.81.32)
 Registration: Registered with Cisco Unified Communications Manager CUCM115
 IPv4 Address: 10.106.81.32

Device Information

Conference Bridge Type* Cisco TelePresence Conductor
 Device is trusted
 Conference Bridge Name*
 Description
 Conference Bridge Prefix
 SIP Trunk*
 Allow Conference Bridge Control of the Call Security Icon

HTTP Interface Info

Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1

Username*
 Password*
 Confirm Password*
 Use HTTPS
 HTTP Port*

- Selezionare **Salva**

Nota: Per consentire connessioni sicure, è necessario includere il campo **Nome host (FQDN di CMS) e/o Indirizzo IP** nel certificato Webadmin, nel **nome comune** o nel campo **Nome alternativo soggetto**





- Dopo la creazione del bridge di conferenze, aprire la sezione **Cisco Unified Serviceability**
- Selezionare **Strumenti > Control Center - Servizi funzionalità**
- Dal menu a discesa, selezionare il nodo editore CUCM
- Selezionare **Vai**
- Selezionare il **servizio Cisco CallManager**
- Selezionare **Riavvia**

Attenzione: Quando il servizio CallManager viene riavviato, le chiamate connesse rimangono ma alcune funzionalità non sono disponibili durante il riavvio. Non sono possibili nuove chiamate. Il riavvio del servizio richiede circa 5-10 minuti, a seconda del carico di lavoro CUCM. Eseguire questa operazione con cautela e assicurarsi di eseguirla durante un intervento di manutenzione.


Passaggio 5. Il bridge CMS è stato registrato nel CUCM

- Vai a **Risorse multimediali > Gruppo risorse multimediali**
- Fare clic su **Aggiungi nuovo** per creare un nuovo gruppo di risorse multimediali e immettere un nome
- Spostare il bridge per conferenze (cms) in questo caso dalla casella **Risorse multimediali disponibili** alla casella **Risorse multimediali selezionate**
- Fare clic su **Salva**.

Media Resource Group Configuration

 Save
 Delete
 Copy
 Add New

Status

 Status: Ready

Media Resource Group Status

Media Resource Group: CMS MRG (used by 45 devices)

Media Resource Group Information

Name*

Description

Devices for this Group

Available Media Resources**

ANN_2
 CFB_2
 IVR_2
 MOH_2
 MTP_2

▼ ▲

Selected Media Resources*

cmslab1.acanotaclab.com (CFB)

Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)

Save Delete Copy Add New

Passo 6: aggiungere i gruppi di risorse multimediali (MRG) agli elenchi dei gruppi di risorse multimediali (MRGL)

- Vai a **Risorse multimediali > Elenco gruppi di risorse multimediali**
- Fare clic su **Aggiungi nuovo** per creare un nuovo elenco di gruppi di risorse multimediali e inserire un nome oppure selezionare un MRGL esistente e fare clic su di esso per modificarlo.
- Spostare uno o più gruppi di risorse multimediali creati dalla casella **Gruppi di risorse multimediali disponibili** ai **gruppi di risorse multimediali selezionati**
- Fare clic su **Salva**.

Media Resource Group List Configuration

Save Delete Copy Add New

Status
 Status: Ready

Media Resource Group List Status
 Media Resource Group List: CMS MRGL (used by 45 devices)

Media Resource Group List Information
 Name* CMS MRGL

Media Resource Groups for this List

Available Media Resource Groups
 CMS Cluster 1 MRGL
 CMS Cluster 2 MRGL
 CMS Cluster 3 MRGL
 CMS Cluster MRG
 softwareBridge

Selected Media Resource Groups
 CMS MRG

Save Delete Copy Add New

Passo 7: Aggiungere MRGL a un pool di dispositivi o a un dispositivo

A seconda dell'implementazione, è possibile configurare un pool di dispositivi e applicarlo agli endpoint oppure assegnare un singolo dispositivo (un endpoint) a un MRGL specifico. **Se un parametro MRGL viene applicato sia al pool di dispositivi che a un endpoint, le impostazioni dell'endpoint avranno la precedenza.**

- Vai a **Sistema >> Pool di dispositivi**
- Creare un nuovo pool di dispositivi o utilizzare un pool di dispositivi esistente. Fare clic su **Aggiungi nuovo**

Device Pool Configuration

Save

Status: Ready

Device Pool Information

Device Pool: New

Device Pool Settings

Device Pool Name*

Cisco Unified Communications Manager Group*

Calling Search Space for Auto-registration

Adjunct CSS

Reverted Call Focus Priority

Intercompany Media Services Enrolled Group

Roaming Sensitive Settings

Date/Time Group*

Region*

Media Resource Group List

Passaggio 8: Per aggiungere il pool di dispositivi all'endpoint e aggiungere MRGL all'endpoint

- Vai a **Dispositivo**> **Telefoni**
- Fare clic su **Trova** e selezionare il dispositivo su cui modificare le impostazioni del pool di dispositivi
- Applicare il pool di dispositivi e MRGL creati nei passi precedenti
- **Salvataggio, applicazione della configurazione e ripristino**

L'endpoint verrà riavviato e registrato

Phone Configuration

Save Delete Copy Reset Apply Config Add New

Modify Button Items

1 [Line \(1\) - 6000 \(no partition\)](#)

----- Unassigned Associated Items -----

2 [Line \(2\) - Add a new DN](#)

Product Type: Cisco Spark Room Kit
Device Protocol: SIP

Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager 10.104.215.207
IPv4 Address: [10.104.130.54](#)
Active Load ID: ce-9.3.1-61bfa3834f2-2018-05-04
Inactive Load ID: None
Download Status: None

Device Information

Device is Active
 Device is trusted

MAC Address*

Description

Device Pool* [View Details](#)

Common Device Configuration [View Details](#)

Phone Button Template*

Common Phone Profile* [View Details](#)

Calling Search Space


AAR Calling Search Space

Media Resource Group List

Passaggio 9: Configurazione su un endpoint

- **Accedere** alla **GUI Web** dell'endpoint
- Selezionare **Imposta > Configurazione > Conferenza > Modalità multipunto**
- Selezionare **CUCMMediaResourceGroupList**

Multipoint Mode

CUCMMediaResourceGroupList 

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

- Aprire l'interfaccia Web CUCM
- Selezionare **Dispositivo > Trunk**
- Selezionare il trunk SIP che punta a CMS
- Verificare che i trunk siano in stato **Full Service**
- Selezionare **Risorse multimediali > Conference Bridge**
- Selezionare il bridge per conferenze CMS
- Assicurarsi che sia registrato con CUCM

Effettua una chiamata ad hoc

- Chiamata dall'endpoint A registrata in CUCM (aggiunta MRGL) a un altro endpoint B
- Sull'endpoint A, fare clic su **Add**, quindi comporre EndpointC
- L'endpoint A verrà messo in attesa
- Fare clic su **Unisci**
- Verifica della connessione delle chiamate in CMS
- Aprire l'interfaccia Web CMS
- Selezionare **Stato > Chiamate**

Per il test, sono stati utilizzati 3 endpoint per conferenze audio/video ad-hoc

Status	Configuration	Logs
Active Calls		
Filter	<input type="text"/>	<input type="button" value="Set"/> Show only calls with alarms <input type="button" value="Set"/>
Conference: 001036010001 (3 active calls)		
<input type="checkbox"/>	SIP 6000@acanotaclab.com [less] (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.96 Mb/s
	outgoing media	OPUS, H.264, 1920 x 1080 29.9fps, 929 Kb/s
	additional protocols	unencrypted Active Control
	remote address	6000@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd1-cfd7680a@10.104.215.207
<input type="checkbox"/>	SIP abhi [less] (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.94 Mb/s
	outgoing media	AAC, H.264, 1920 x 1080 30.3fps, 1.33 Mb/s
	additional protocols	unencrypted Active Control
	remote address	2333@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd3-cfd7680a@10.104.215.207
<input type="checkbox"/>	SIP sakatuka [less] (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.94 Mb/s
	outgoing media	AAC, H.264, 1920 x 1080 29.9fps, 1.19 Mb/s
	additional protocols	unencrypted Active Control
	remote address	1105@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd2-cfd7680a@10.104.215.207

Risoluzione dei problemi

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