Esempio di configurazione per l'integrazione SIP sicura tra CUCM e CUC basata sulla crittografia di nuova generazione (NGE)

Sommario

Introduzione

In questo documento viene descritta la configurazione e la verifica della connessione SIP protetta tra Cisco Unified Communications Manager (CUCM) e il server Cisco Unity Connection (CUC) tramite crittografia di nuova generazione.

La sicurezza di nuova generazione sull'interfaccia SIP impedisce all'interfaccia SIP di utilizzare le cifrature Suite B basate sui protocolli TLS 1.2, SHA-2 e AES256. Consente le varie combinazioni di cifrari in base all'ordine di priorità dei cifrari RSA o ECDSA. Durante la comunicazione tra Unity Connection e Cisco Unified CM, sia la cifratura che i certificati di terze parti vengono verificati a entrambe le estremità. Di seguito viene riportata la configurazione per il supporto della crittografia

di nuova generazione.

Se si intende utilizzare i certificati firmati da un'Autorità di certificazione di terze parti, iniziare con la firma dei certificati alla fine della sezione di configurazione (Configurazione - Firma dei certificati basati su chiave CE da parte di un'Autorità di certificazione di terze parti)

Prerequisiti

Requisiti

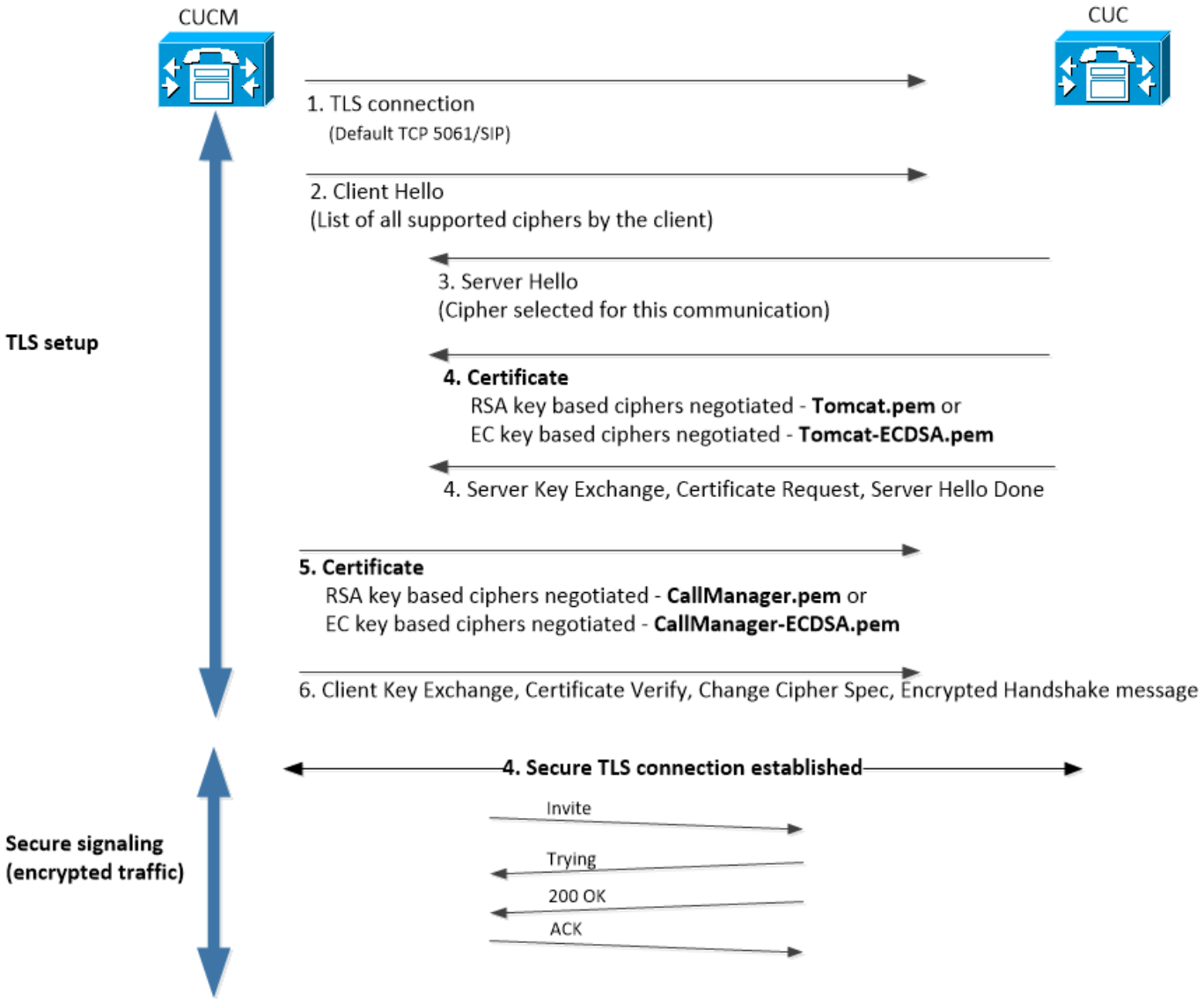
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

CUCM versione 11.0 e successive in modalità mista
CUC versione 11.0 e successive

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.

Esempio di rete

Questo diagramma spiega brevemente il processo che consente di stabilire una connessione sicura tra CUCM e CUC una volta attivato il supporto della crittografia di nuova generazione:



Requisiti del certificato

Questi sono i requisiti per lo scambio dei certificati dopo che il supporto della crittografia di nuova generazione è stato abilitato su Cisco Unity Connection.

- **Negoziazione delle cifrature basate su chiavi RSA**

certificato CUCM utilizzato	Certificato CUC utilizzato	Certificati da caricare in CUCM	Certificati da caricare in CU
CallManager.pem (autofirmato)	Tomcat.pem (autofirmato)	Tomcat.pem da caricare in CUCM > CallManager-trust	Nessuna.
CallManager.pem (firmato da CA)	Tomcat.pem (firmato dalla CA)	Certificato[*1] CA radice e intermedia CUC da caricare in CUCM > CallManager-trust	Certificato CA radice e intermedia CUCM[*2] da cari in CUC > CallManager-trust
CallManager.pem (firmato da CA)	Tomcat.pem (autofirmato)	Tomcat.pem da caricare in CUCM > CallManager-trust	Caricamento del certificato radice e intermedia CUCM i CUC > CallManager-trust.
CallManager.pem (autofirmato)	Tomcat.pem (firmato dalla CA)	Certificato CA radice e intermedia CUC da caricare in	Nessuna.

CUCM > CallManager-trust

[*1]Il certificato CA radice e intermedia CUC si riferisce al certificato CA che ha firmato il certificato Unity Connection Tomcat (Tomcat.pem).

[*2]Il certificato della CA radice e intermedia CUCM si riferisce al certificato della CA che ha firmato il certificato del CallManager CUCM (Callmanager.pem).

- **Crittografia basata su chiavi EC negoziata**

certificato CUCM utilizzato	Certificato CUC utilizzato	Certificati da caricare in CUCM	Certificati da caricare in CUC
CallManager-ECDSA.pem (autofirmato)	Tomcat-ECDSA.pem (autofirmato)	Tomcat-ECDSA.pem da caricare in CUCM > CallManager-trust	Nessuna.
CallManager-ECDSA.pem (firmato da CA)	Tomcat-ECDSA.pem (CA firmato)	Certificato[*1] CA radice e intermedia CUC da caricare in CUCM > CallManager-trust	Certificato CA radice e intermedia CUCM[*2] da caricare in CUC > CallManager-trust.
CallManager-ECDSA.pem (firmato da CA)	Tomcat-ECDSA.pem (autofirmato)	Tomcat-ECDSA.pem da caricare in CUCM > CallManager-trust.	Caricamento del certificato CA radice e intermedia CUCM in CUC > CallManager-trust.
CallManager-ECDSA.pem (autofirmato)	Tomcat-ECDSA.pem (CA firmato)	Certificato CA radice e intermedia CUC da caricare in CUCM > CallManager-trust	Nessuna.

[*1] Il certificato CA radice e intermedia CUC si riferisce al certificato CA che ha firmato il certificato Tomcat basato sulla connessione Unity EC (Tomcat-ECDSA.pem).

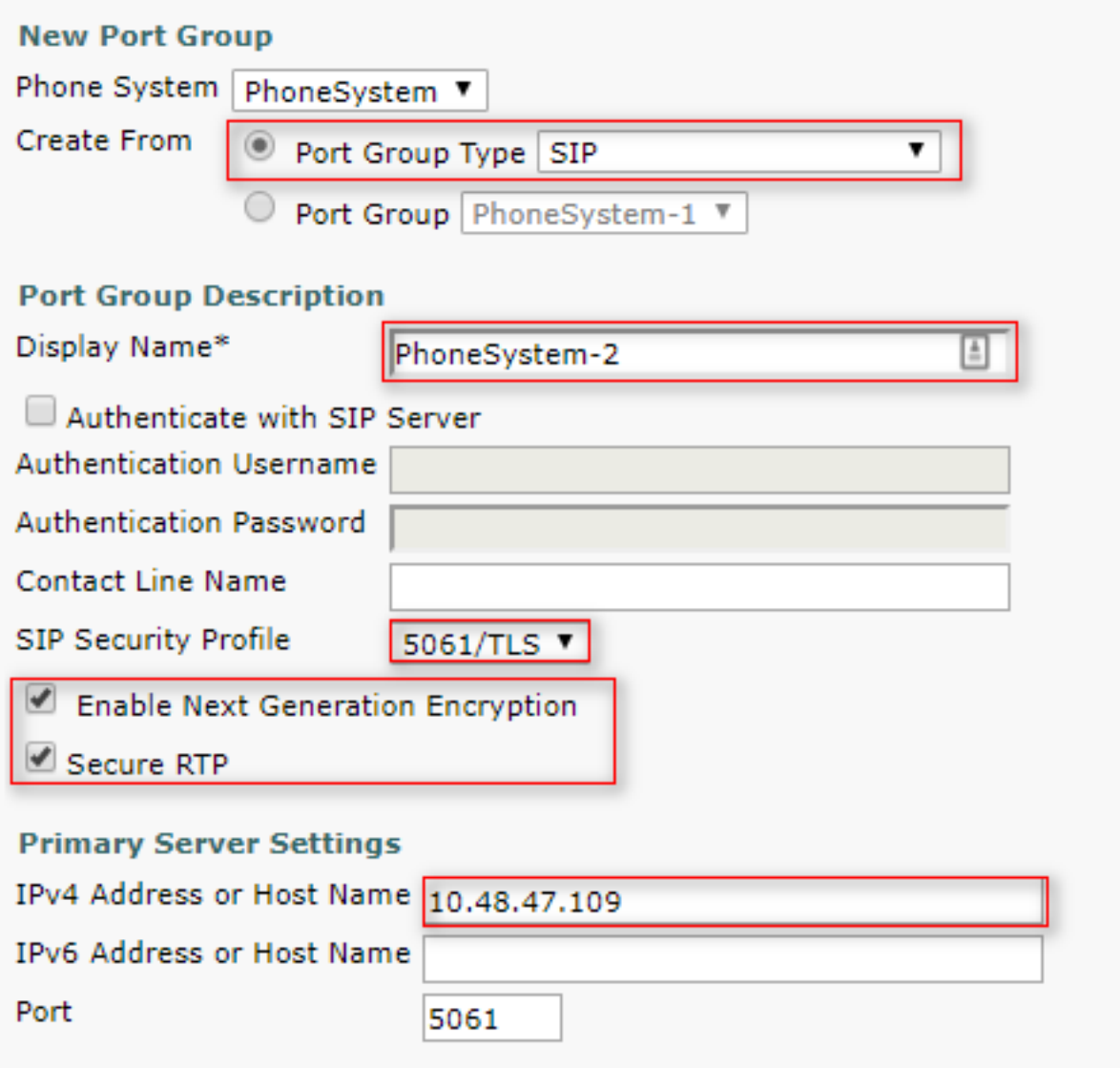
[*2] Il certificato CA radice e intermedia CUCM si riferisce al certificato CA che ha firmato il certificato CUCM CallManager (CallManager-ECDSA.pem).

1. **Nota:** Il certificato Tomcat-ECDSA.pem è chiamato CallManager-ECDSA.pem nelle versioni 11.0.1 di CUC. Dalla CUC 11.5.x il certificato è stato rinominato Tomcat-ECDSA.pem.

Configurazione - Cisco Unity Connection (CUC)

1. Aggiungere un nuovo gruppo di porte

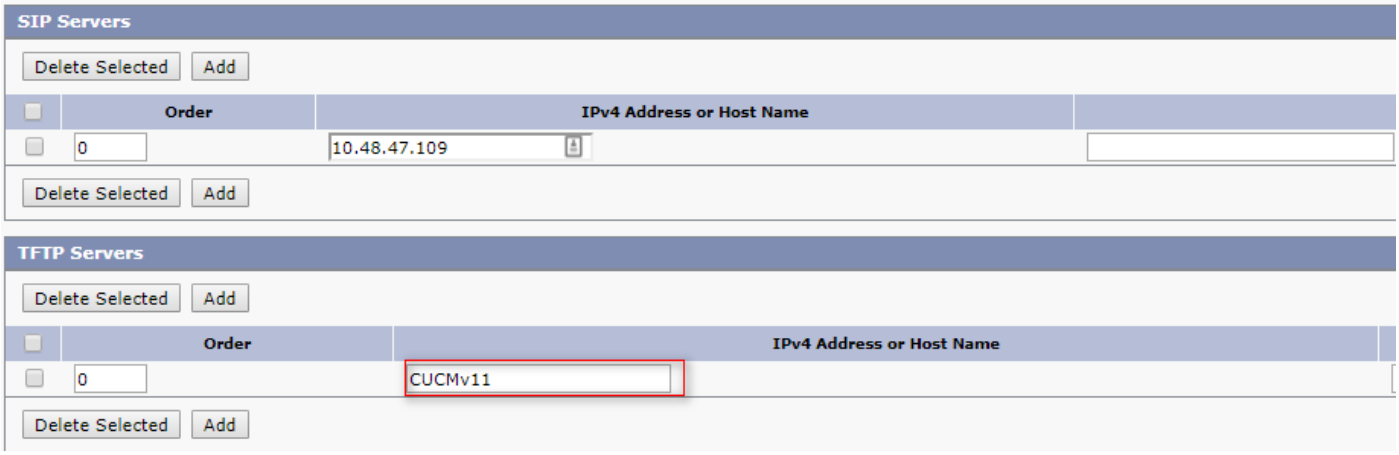
Passare alla pagina Amministrazione di Cisco Unity Connection > Integrazione telefonia > Gruppo di porte e fare clic su Aggiungi nuovo. Selezionare la casella di controllo Enable Next-Generation Encryption (Abilita crittografia di nuova generazione).



1. **Nota**:il certificato Cisco Tomcat di Unity Connection verrà utilizzato durante l'handshake SSL quando la casella di controllo Abilita crittografia di nuova generazione è abilitata.
   · Nel caso in cui la cifratura ECDSA venga negoziata, il certificato ECDSA basato su chiave EC viene utilizzato nell'handshake SSL.
   · Nel caso in cui la cifratura basata su RSA venga negoziata, il certificato tomcat basato su chiave RSA viene utilizzato nell'handshake SSL.

2. Aggiungere il riferimento al server TFTP

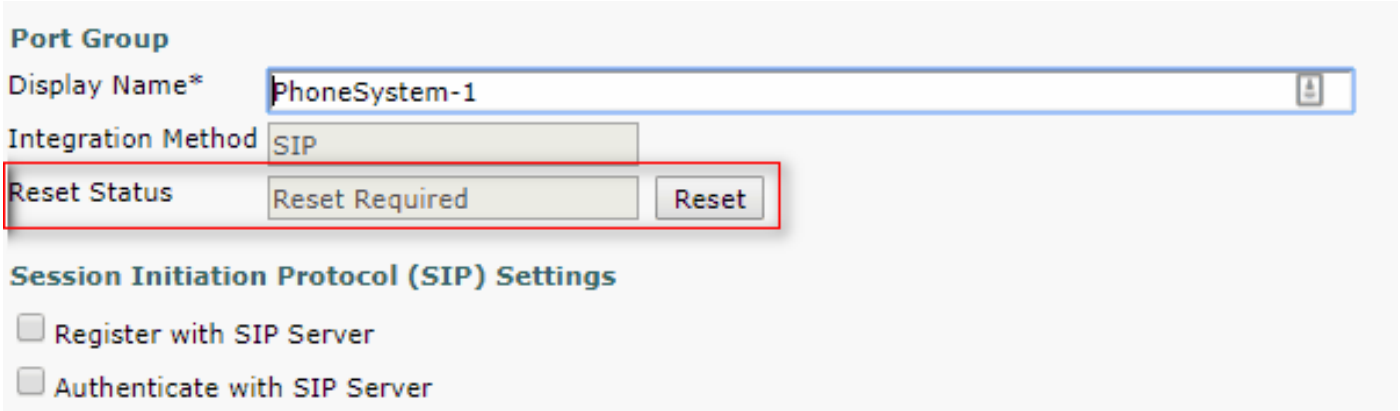
Nella pagina Informazioni di base gruppo porte, passare a Modifica > Server e aggiungere il nome di dominio completo (FQDN) del server TFTP del cluster CUCM. Il nome FQDN/nome host del server TFTP deve corrispondere al nome comune (CN) del certificato di CallManager. L'indirizzo IP del server non funzionerà e non sarà possibile scaricare il file ITL. Il nome DNS deve pertanto essere risolvibile tramite il server DNS configurato.



Riavviare Connection Conversation Manager su ogni nodo passando a Cisco Unity Connection Serviceability > Strumenti > Gestione servizi. Questa operazione è obbligatoria per rendere effettiva la configurazione.

1. **Nota:** Unity connection scarica il file ITL (ITLfile.tlv) dal protocollo TFTP di CUCM utilizzando il protocollo https su una porta protetta 6972 (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM deve essere in modalità mista poiché CUC sta cercando il certificato di funzione "CCM+TFTP" dal file ITL.

Tornare alla pagina di configurazione Integrazione telefonia > Gruppo di porte > Nozioni fondamentali sul gruppo di porte e reimpostare il gruppo di porte appena aggiunto.



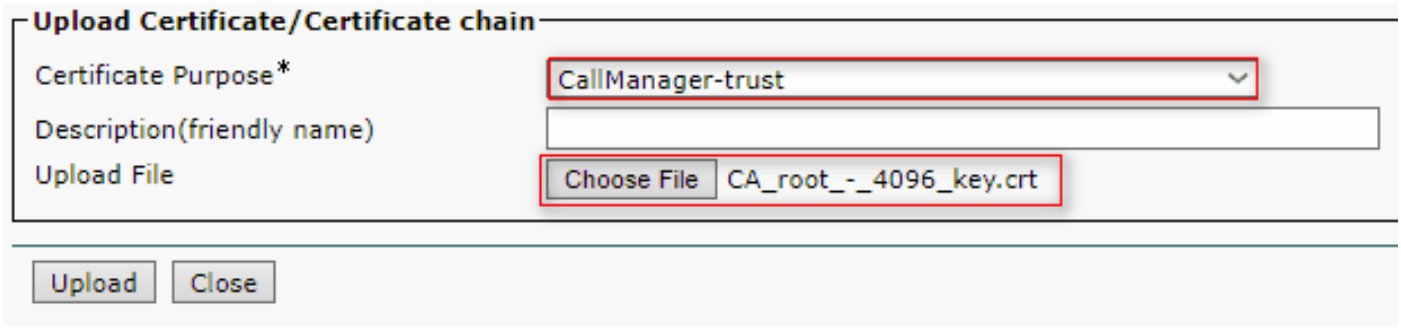
1. **Nota:** Ogni volta che il gruppo di porte viene reimpostato, il server CUC aggiorna il file ITL memorizzato localmente connettendosi al server CUCM.

3. Aggiungi porte della casella vocale

Tornare a Integrazione telefonia > Porta e fare clic su Aggiungi nuova per aggiungere una porta al gruppo di porte appena creato.

4. Caricare il certificato radice e intermedio CUCM della CA di terze parti

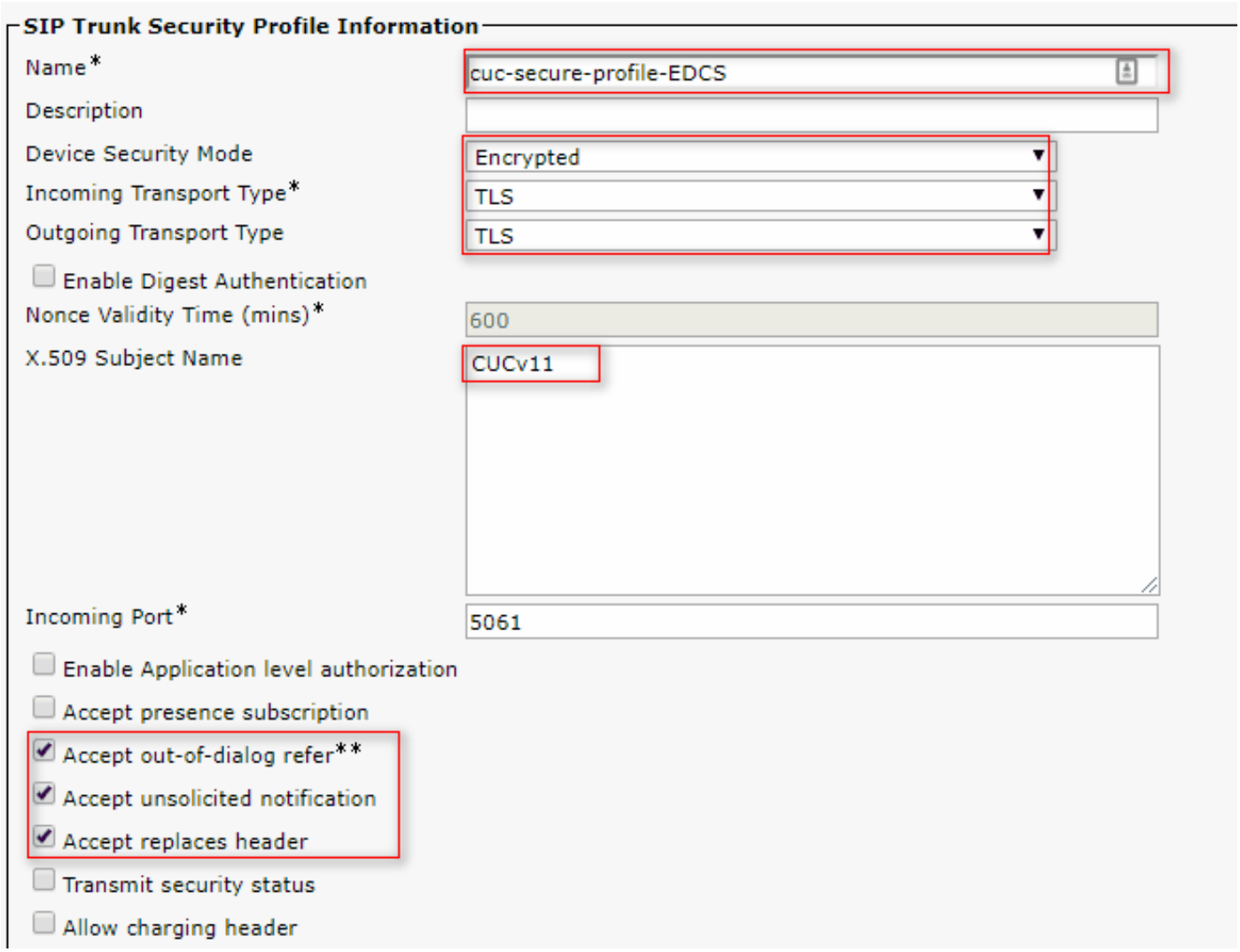
In caso di certificati di terze parti, è necessario caricare il certificato radice e intermedio dell'Autorità di certificazione di terze parti su CallManager-trust of Unity Connection. Questa operazione è necessaria solo se l'autorità di certificazione di terze parti ha firmato il certificato del gestore delle chiamate. Per eseguire questa azione, selezionare Cisco Unified OS Administration > Security > Certificate Management (Amministrazione sistema operativo unificato Cisco > Protezione > Gestione certificati) e fare clic su Upload Certificate (Carica certificato).



Configurazione - Cisco Unified CM (CUCM)

1. Creare un profilo di sicurezza trunk SIP

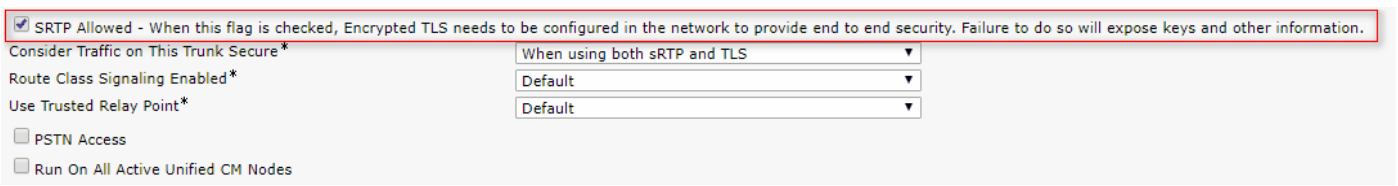
Passare a Amministrazione CUCM > Sistema > Protezione > SIP Trunk Security Profile e aggiungere un nuovo profilo. Il nome soggetto X.509 deve corrispondere al nome di dominio completo (FQDN) del server CUC.

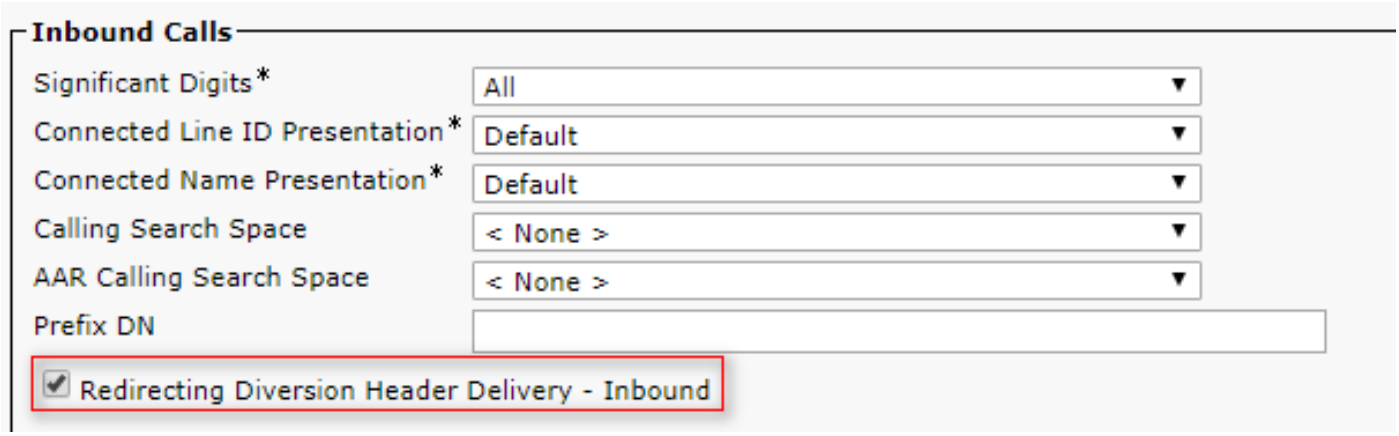


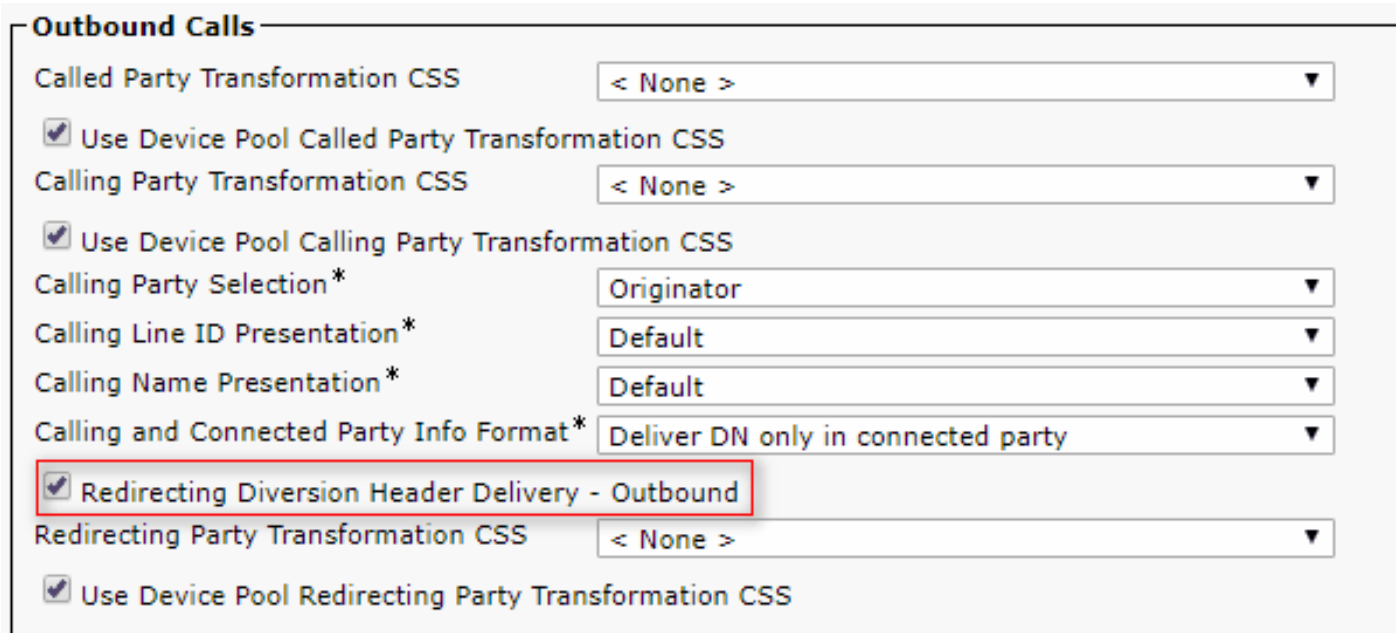
1. **Nota**: il comando CLI "show cert own tomcat/tomcat.pem" può visualizzare il certificato tomcat basato sulla chiave RSA su Unity Connection. Il CN deve corrispondere al nome soggetto X.509 configurato su CUCM. Il CN è uguale a FQDN/Nome host del server Unity. Il certificato basato su chiave EC contiene il nome FQDN/host nel campo Nome alternativo soggetto (SAN).

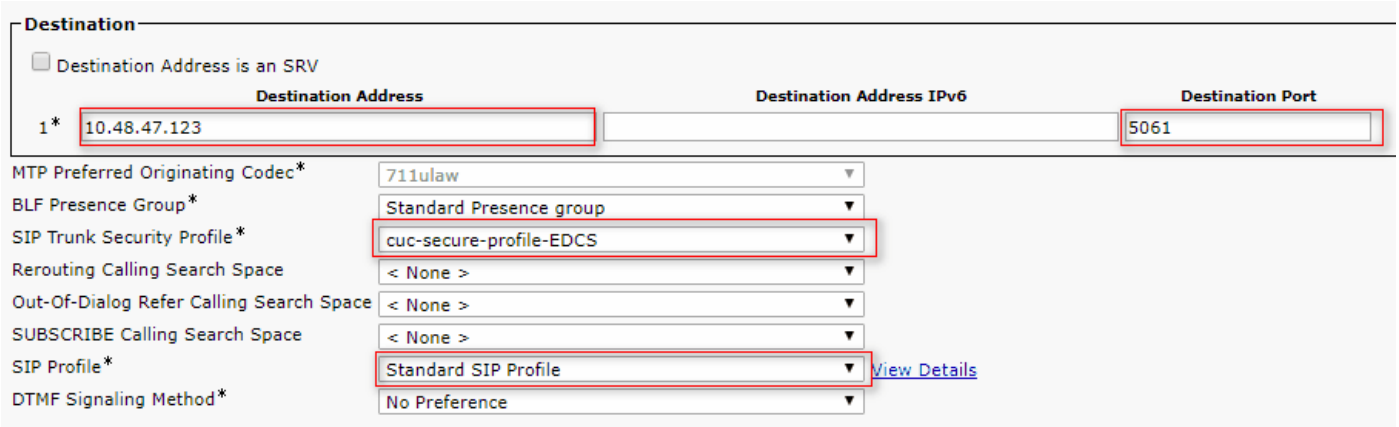
2. Creare un trunk SIP sicuro

Passare a Dispositivo > Trunk > Fare clic e aggiungere un nuovo trunk SIP standard che verrà utilizzato per l'integrazione protetta con Unity Connection.





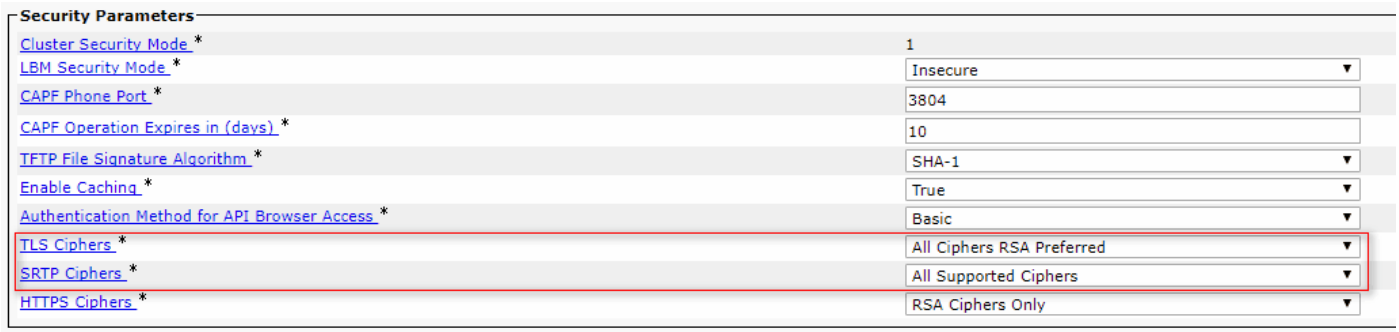




3. Configurare i cifrari TLS e SRTP

1. **Nota:** La negoziazione tra Unity Connection e Cisco Unified Communications Manager dipende dalla configurazione della cifratura TLS con le seguenti condizioni: Quando Unity Connection opera come server, la negoziazione della cifratura TLS si basa sulla preferenza selezionata da Cisco Unified CM.Se viene negoziata la cifratura basata su ECDSA, nell'handshake SSL vengono utilizzati i certificati ECDSA basati su chiave EC.Se la cifratura basata su RSA viene negoziata, i certificati tomcat basati su chiave RSA vengono utilizzati nell'handshake SSL.Quando Unity Connection opera come client, la negoziazione della cifratura TLS si basa sulla preferenza selezionata da Unity Connection.

Passare a Cisco Unified CM > Systems > Enterprise Parameters (Cisco Unified CM > Sistemi > Parametri aziendali) e selezionare l'opzione di cifratura appropriata dall'elenco a discesa TLS e Cifratura SRTP da.



Riavviare il servizio Cisco Call Manager su ciascun nodo passando alla pagina Cisco Unified Serviceability, Strumenti > Control Center-Feature Services e selezionare Cisco Call Manager in CM Services

Passare alla pagina Amministrazione di Cisco Unity Connection > Impostazioni di sistema > Configurazioni generali e selezionare l'opzione di cifratura appropriata dall'elenco a discesa TLS and SRTP Ciphers from.

Riavviare Connection Conversation Manager su ogni nodo passando a Cisco Unity Connection Serviceability > Strumenti > Gestione servizi.

Opzioni crittografia TLS con ordine di priorità

Opzioni crittografia TLS	Crittografia TLS in ordine di priorità
Massima affidabilità - Solo AES-256 SHA-384: Preferenza RSA	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Solo AES-256 SHA-384: Preferito ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH

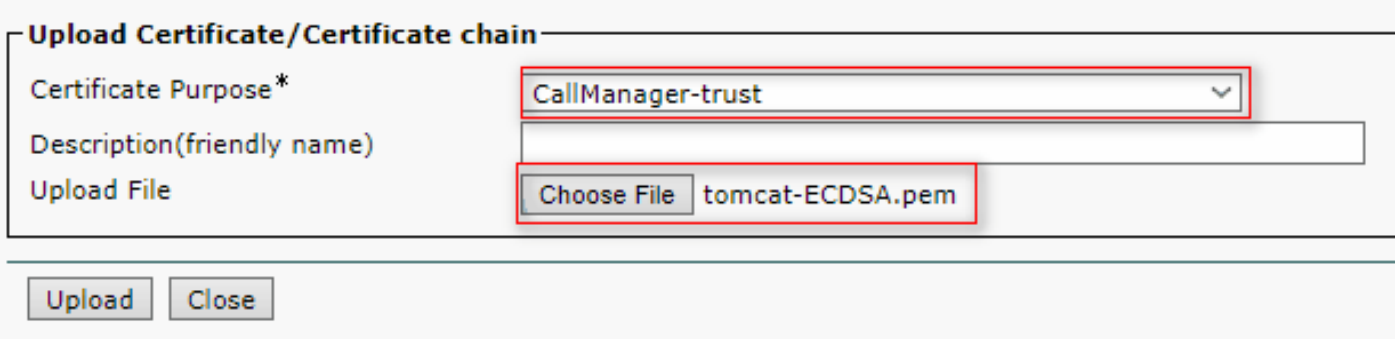
Medio-AES-256 AES-128 Only: Preferenza RSA	4 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_RSA_WITH_AES_128_CBC_SHA
Medio-AES-256 AES-128 Only: Preferito ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_RSA_WITH_AES_128_CBC_SHA
Tutti i cifrari RSA preferiti (predefinito)	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_RSA_WITH_AES_128_CBC_SHA
Tutti i cifrari ECDSA preferiti	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_RSA_WITH_AES_128_CBC_SHA

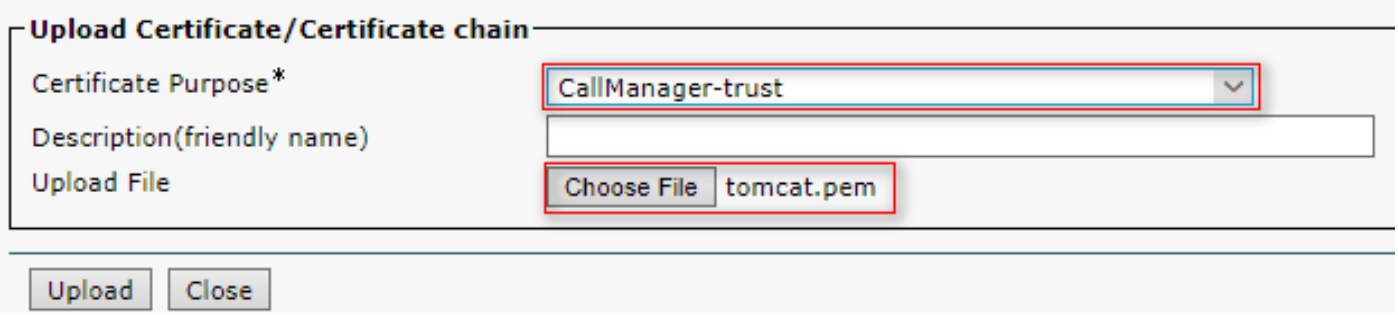
Opzioni crittografia SRTP in ordine di priorità

Opzione crittografia SRTP	SRTP in ordine di priorità
Tutti i cifrari AES-256, AES-128 supportati	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1 _32
AEAD AES-256, cifrari basati su AES-28 GCM	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
Solo cifrari AEAD AES256 basati su GCM	• AEAD_AES_256_GCM

4. Caricamento dei certificati CUC Tomcat (basati su RSA e EC)

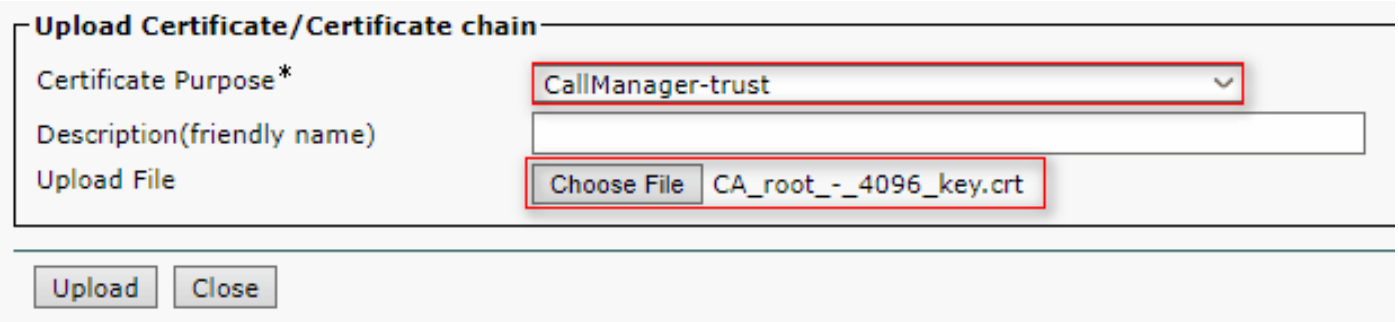
Passare a Amministrazione sistema operativo > Sicurezza > Gestione certificati e caricare entrambi i certificati CUC Tomcat (basati su RSA e EC) nell'archivio di attendibilità di CallManager.





1. **Nota**: il caricamento di entrambi i certificati Unity Tomcat non è obbligatorio se i cifrari ECDSA vengono negoziati solo. In tal caso è sufficiente il certificato CE Tomcat.

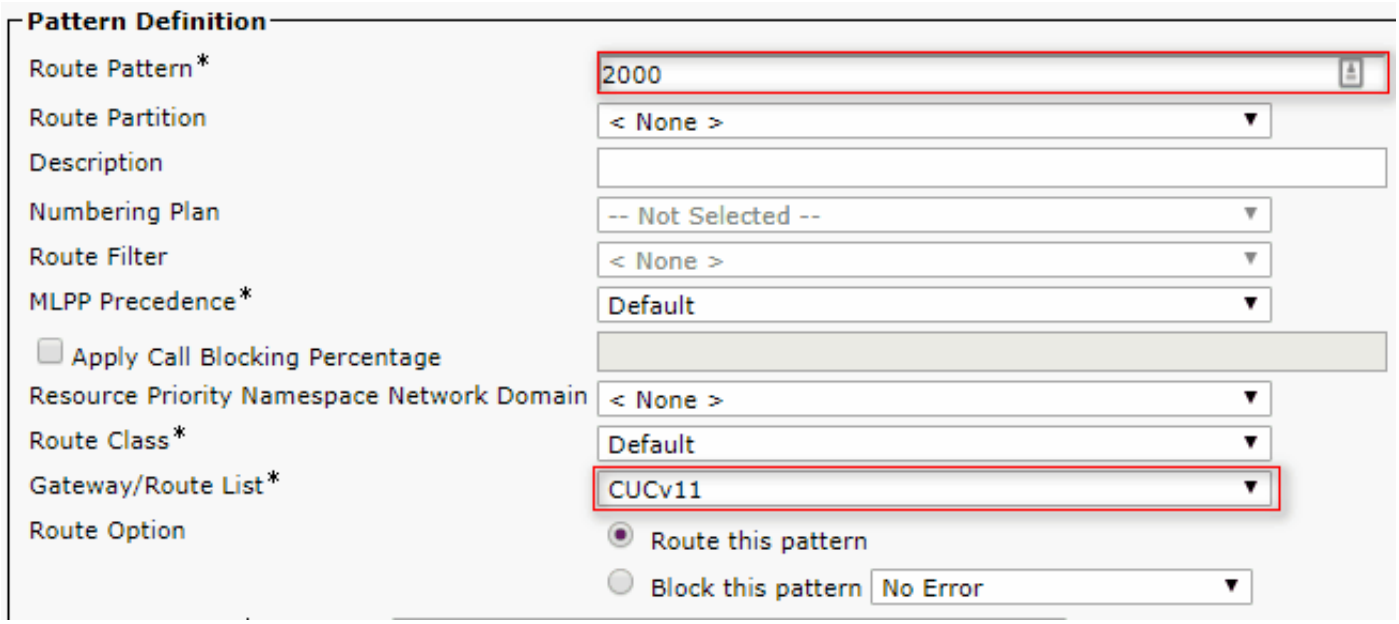
In caso di certificati di terze parti, è necessario caricare il certificato radice e il certificato intermedio dell'Autorità di certificazione di terze parti. Questa operazione è necessaria solo se l'autorità di certificazione di terze parti ha firmato il certificato Unity Tomcat.



Riavviare il processo Cisco Call Manager su tutti i nodi per applicare le modifiche.

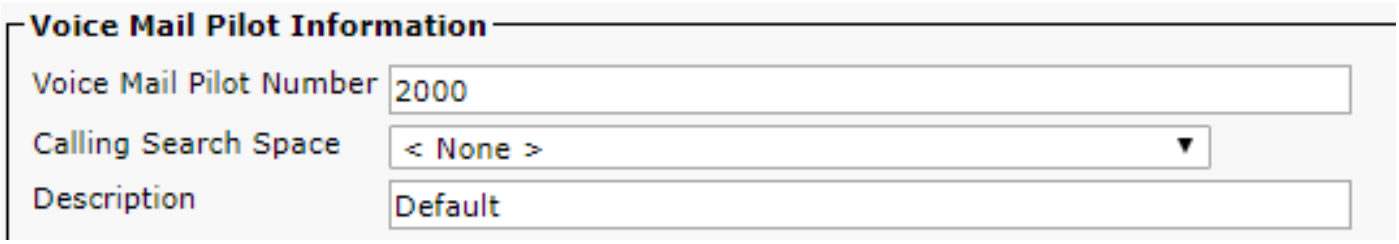
5. Creare un modello di instradamento

Configurare un modello di route che punti al trunk configurato passando a Instradamento chiamate > Instradamento/Ricerca > Modello di route. L'estensione immessa come numero di serie del percorso può essere utilizzata come pilota della segreteria telefonica.

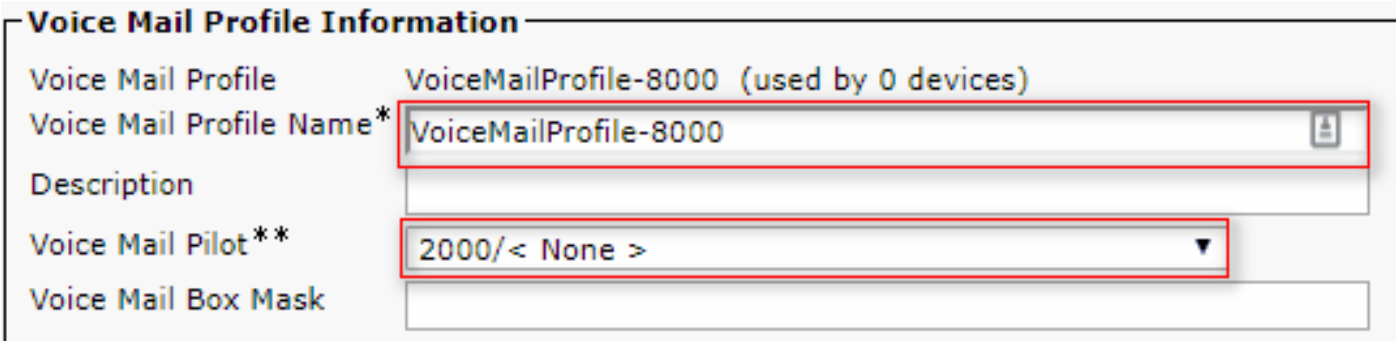


6. Creare il Programma pilota per la segreteria telefonica, il Profilo della segreteria telefonica e assegnarlo ai DN

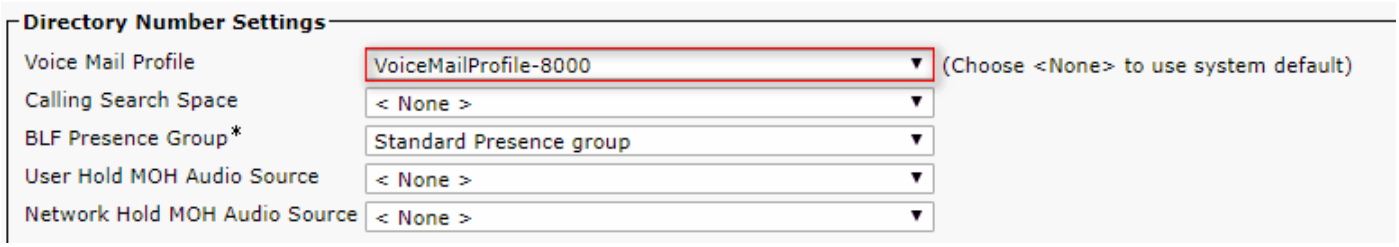
Creare un progetto pilota per la casella vocale per l'integrazione andando a Caratteristiche avanzate > Casella vocale > Programma pilota casella vocale.



Crea un profilo di segreteria telefonica per collegare tutte le impostazioni > Funzionalità avanzate > Segreteria telefonica > Profilo segreteria telefonica



Assegnare il nuovo profilo di segreteria telefonica ai DN destinati a utilizzare l'integrazione protetta passando a Instradamento chiamate > Numero directory



Configurazione - Firma dei certificati basati su chiave CE da parte di CA di terze parti (facoltativo)

I certificati potrebbero essere firmati da una CA di terze parti prima di configurare l'integrazione protetta tra i sistemi. Per firmare i certificati su entrambi i sistemi, procedere come segue.

Cisco Unity Connection

1. Genera richiesta di firma certificato (CSR) per CUC Tomcat-ECDSA e il certificato deve essere firmato da un'autorità di certificazione di terze parti
2. La CA fornisce il certificato di identità (certificato firmato dalla CA) e il certificato CA (certificato radice della CA) che devono essere caricati come segue:
   Carica il certificato radice CA nell'archivio di attendibilità tomcat
   Carica certificato di identità nell'archivio Tomcat-EDCS
3. Riavvia Gestione conversazioni su CUC

Cisco Unified CM

1. Generare CSR per CUCM CallManager-ECDSA e far firmare il certificato dall'autorità di certificazione di terze parti
2. La CA fornisce il certificato di identità (certificato firmato dalla CA) e il certificato CA (certificato radice della CA) che devono essere caricati come segue:
   Carica il certificato radice CA nell'archivio callmanager-trust
   Carica certificato di identità nell'archivio callmanager-EDCS
3. Riavviare i servizi CCM e TFTP Cisco su ciascun nodo

Lo stesso processo verrà utilizzato per firmare i certificati basati su chiavi RSA in cui CSR viene generato per il certificato CUC Tomcat e il certificato CallManager e caricato rispettivamente nell'archivio Tomcat e nell'archivio Callmanager.

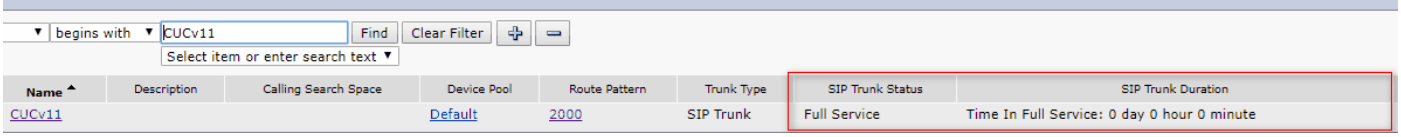
Verifica

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

Verifica Secure SIP Trunk

Premere il pulsante della casella vocale sul telefono per chiamare la casella vocale. Se l'estensione dell'utente non è configurata nel sistema Unity Connection, è necessario ascoltare il messaggio di apertura.

In alternativa, è possibile abilitare le opzioni SIP keepalive per monitorare lo stato del trunk SIP. È possibile abilitare questa opzione nel profilo SIP assegnato al trunk SIP. Una volta abilitato, è possibile monitorare lo stato del trunk SIP tramite Periferica > Trunk come mostrato di seguito:



Verifica chiamata Secure RTP

Verificare se l'icona del lucchetto è presente nelle chiamate a Unity Connection. Significa che il flusso RTP è crittografato (per funzionare, il profilo di sicurezza del dispositivo deve essere protetto), come mostrato in questa immagine

Informazioni correlate

- Guida all'integrazione SIP per Cisco Unity Connection versione 11.x