Configurazione e risoluzione dei problemi di integrazione sicura tra CUCM e CUC

Sommario

Introduzione

Questo documento descrive la configurazione, la verifica e la risoluzione dei problemi di connessione sicura tra Cisco Unified Communications Manager (CUCM) e il server Cisco Unity Connection (CUC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CUCM.

Per ulteriori informazioni, consultare la guida alla sicurezza di Cisco Unified Communications Manager.

Nota: Per garantire il corretto funzionamento dell'integrazione protetta, è necessario impostare la modalità mista.

È necessario abilitare la crittografia per Unity Connection 11.5(1) SU3 e versioni successive.

Comando CLI "utils cuc encryption <enable/disable>"

Componenti usati

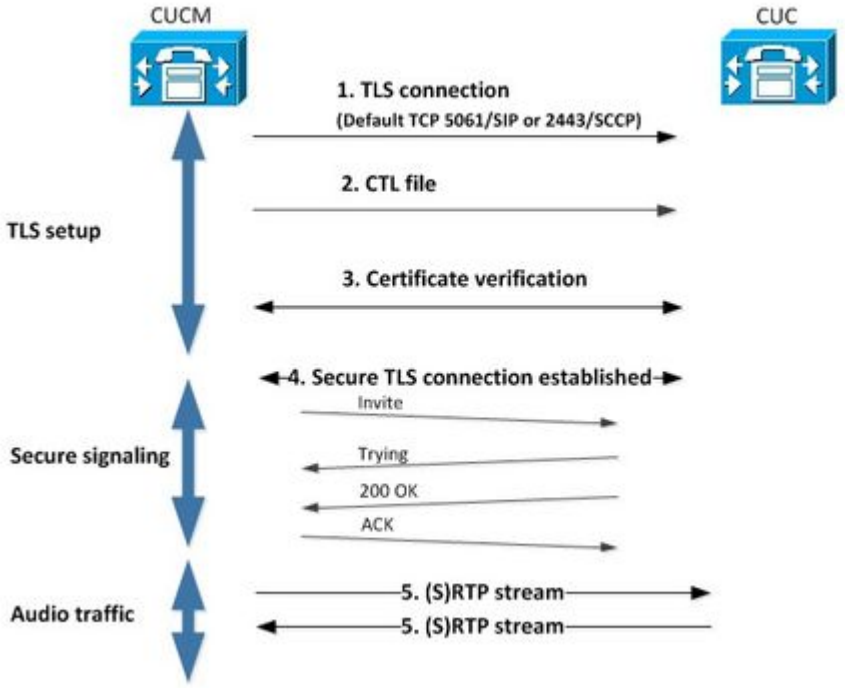
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM versione 10.5.2.1900-3.
- CUC versione 10.5.2.1900-3.

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.

Diagramma

Questo diagramma spiega brevemente il processo che consente di stabilire una connessione sicura tra CUCM e CUC:



1. Call Manager imposta una connessione TLS (Transport Layer Security) sicura al server CUC sulla porta 2443 Skinny Call Control Protocol (SCCP) o 5061 Session Initiation Protocol based (SIP) sul protocollo utilizzato per l'integrazione.

2. Il server CUC scarica il file dell'elenco di certificati attendibili (CTL) dal server TFTP (processo occasionale), estrae il certificato CallManager.pem e lo memorizza.

3. Il server CUCM offre il certificato Callmanager.pem verificato rispetto al certificato CallManager.pem ottenuto nel passaggio precedente. È inoltre in corso la verifica del certificato CUC rispetto a un certificato radice CUC archiviato in CUCM. Notare che il certificato radice deve essere caricato in CUCM dall'amministratore.

4. Se la verifica dei certificati ha esito positivo, viene stabilita una connessione TLS sicura. Questa connessione viene utilizzata per scambiare una segnalazione SCCP o SIP crittografata.

5. Il traffico audio può essere scambiato come Real-time Transport Protocol (RTP) o come SRTP.

Nota: Quando si stabilisce una comunicazione TLS, CUCM e CUC utilizzano l'autenticazione reciproca TLS. Per ulteriori informazioni, fare riferimento alla RFC 5630.

Configurazione - Secure SIP Trunk

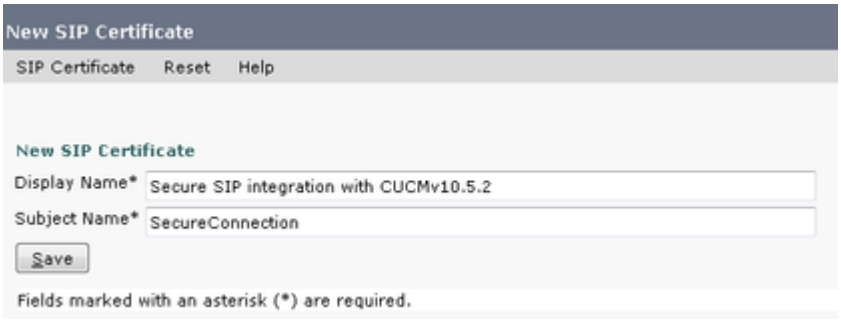
Configura CUC

1. Aggiungi certificato SIP

Selezionare Amministrazione CUC > Integrazioni telefonia > Protezione > Certificato SIP > Aggiungi nuovo

- Nome visualizzato: <qualsiasi nome significativo>
- Nome soggetto: <qualsiasi nome, ad esempio SecureConnection>

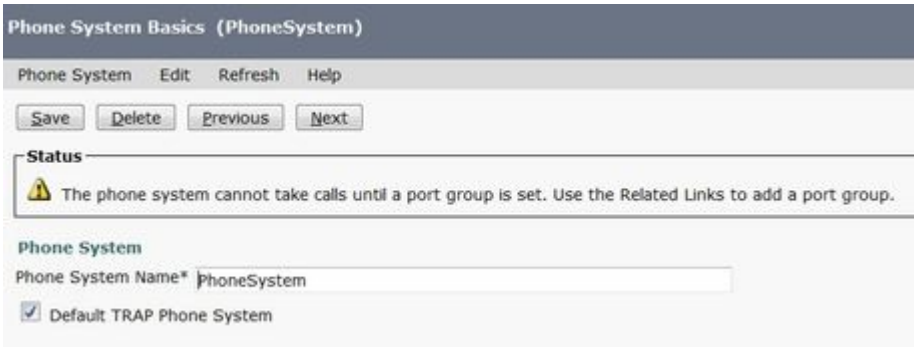
Nota: il nome soggetto deve corrispondere al nome soggetto X.509 nel profilo di sicurezza trunk SIP (configurato nel passaggio 1 della configurazione CUCM più avanti in questo documento).



Nota: Il certificato viene generato e firmato dal certificato radice CUC.

2. Creare un nuovo sistema telefonico o modificarne uno predefinito

Passare a Integrazione telefonia > Sistema telefonico. È possibile utilizzare il sistema telefonico esistente o crearne uno nuovo.

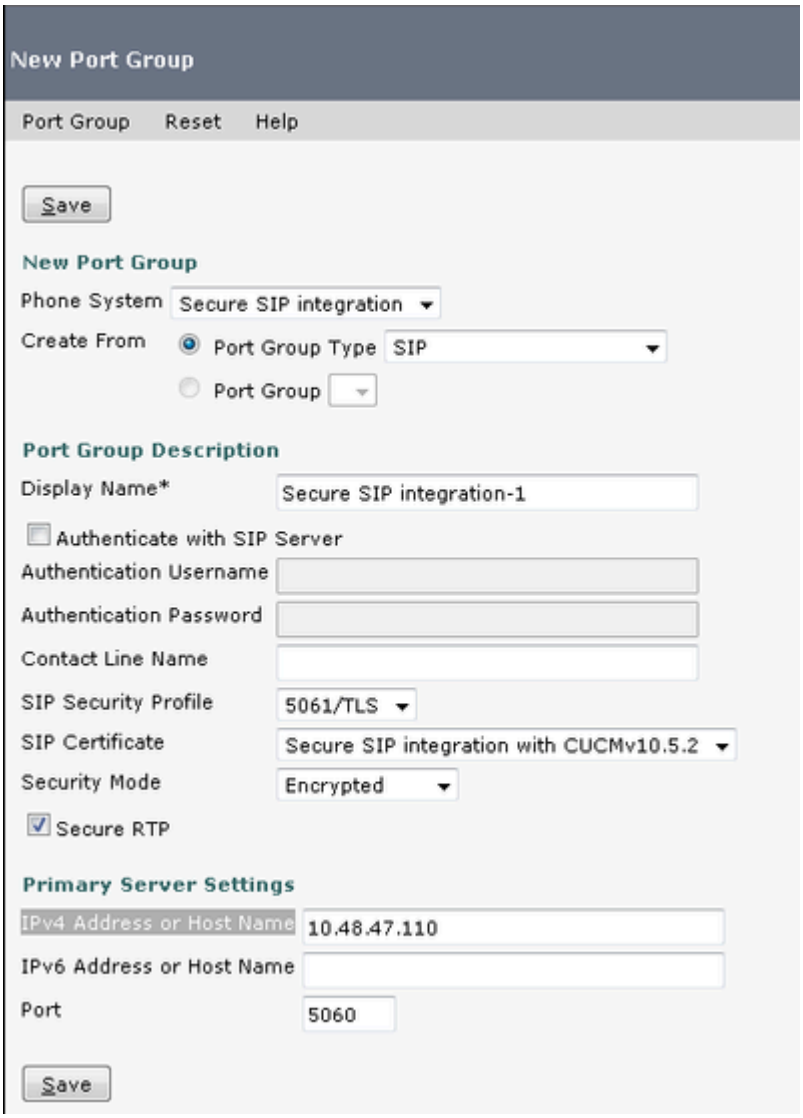


3. Aggiungere un nuovo gruppo di porte

Nella pagina Nozioni fondamentali sul sistema telefonico, nella casella a discesa Collegamenti correlati, selezionare Aggiungi gruppo porte e fare clic su Vai. Nella finestra di configurazione, immettere le seguenti informazioni:

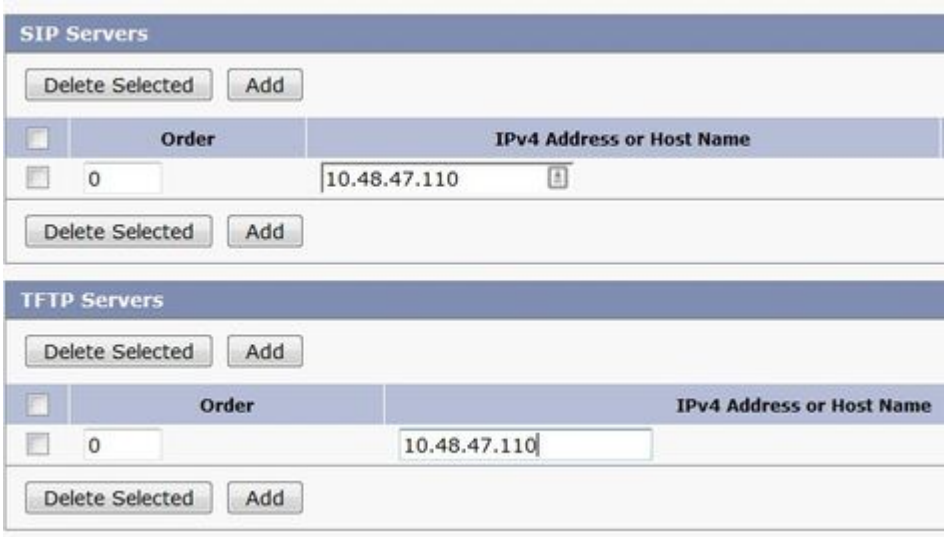
- Sistema telefonico:
- Crea da: Tipo di gruppo porte SIP
- Profilo di sicurezza SIP: 5061/TLS
- Certificato SIP:
- Modalità di protezione: Crittografia
- RTP protetto: Controllato
- Indirizzo IPv4 o nome host:

Scegliere Salva.



4. Modifica server

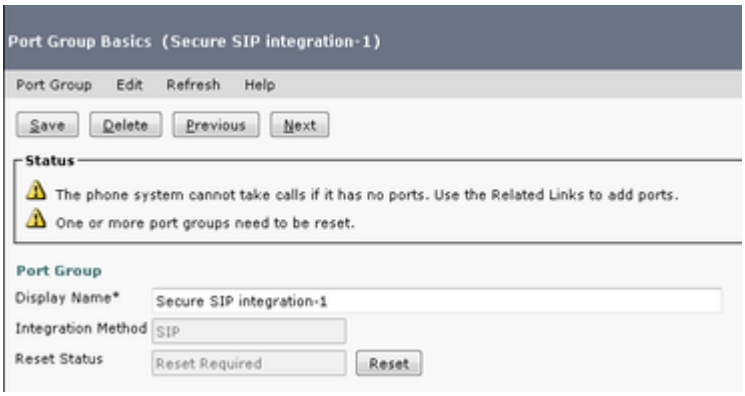
Passare a Modifica > Server e aggiungere il server TFTP dal cluster CUCM, come mostrato in questa immagine.



Nota: È importante fornire un indirizzo TFTP corretto. Il server CUC scarica il file CTL da questo TFTP come spiegato.

5. Ripristino del gruppo di porte

Tornare alle nozioni di base sui gruppi di porte e ripristinare il gruppo di porte come richiesto dal sistema, come mostrato in questa immagine.

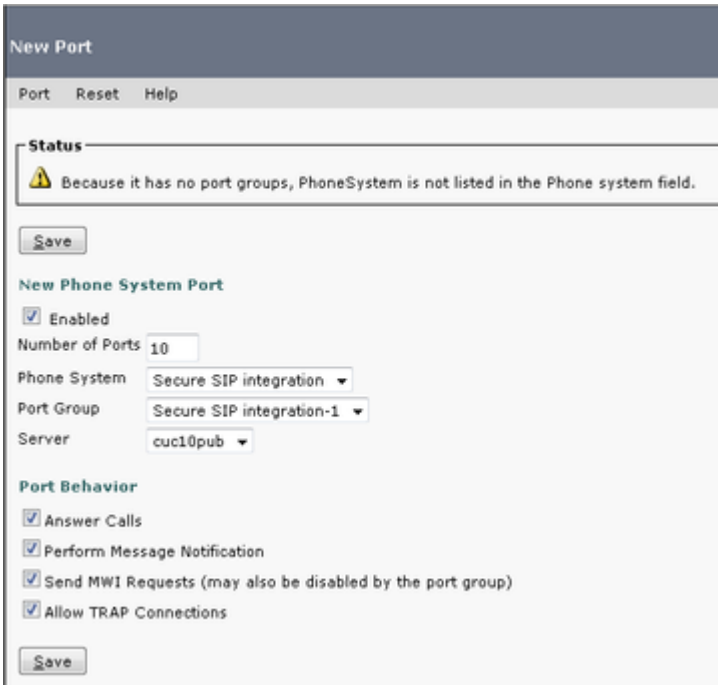


6. Aggiunta delle porte della casella vocale

Nella pagina Nozioni fondamentali sul gruppo di porte, nella casella a discesa Collegamenti correlati, selezionare Aggiungi porte e Vai. Nella finestra di configurazione, immettere le informazioni riportate di seguito.

- Abilitato: Controllato
- Numero di porte:
- Sistema telefonico:

- Gruppo porte:
- Server:
- Comportamento porta:



7. Scarica certificato radice CUC

Passare a Telefonia > Integrazioni > Protezione > Certificato radice, fare clic con il pulsante destro del mouse sull'URL per salvare il certificato come file denominato <nomefile>.0 (l'estensione del file deve essere .0 anziché .htm)' e premere Salva come mostrato nell'immagine.

Configurazione di CUCM

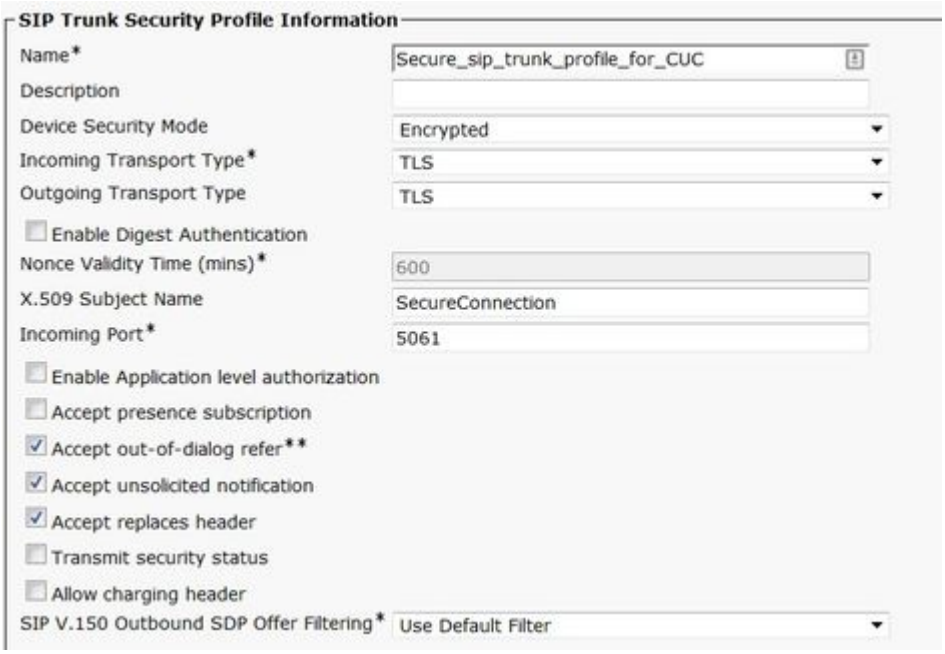
1. Configurare il profilo di sicurezza trunk SIP per il trunk verso CUC

Selezionare CUCM Administration > System > Security > SIP Trunk Security Profile > Add new

Assicurarsi che i campi siano compilati correttamente:

- Modalità di protezione del dispositivo: Crittografia
- Nome soggetto X.509: Connessione sicura>
- Riferimenti esterni all'accettazione: controllato
- Accetta notifica non richiesta: controllato
- Accetta sostituisce l'intestazione: controllato

Nota: Il nome soggetto X.509 deve corrispondere al campo Nome soggetto nel certificato SIP sul server Cisco Unity Connection (configurato nel passaggio 1 della configurazione CUC).



2. Configurare il profilo SIP

Selezionare Periferica > Impostazioni dispositivo > Profilo SIP se è necessario applicare impostazioni specifiche. In caso contrario, è possibile utilizzare il profilo SIP standard.

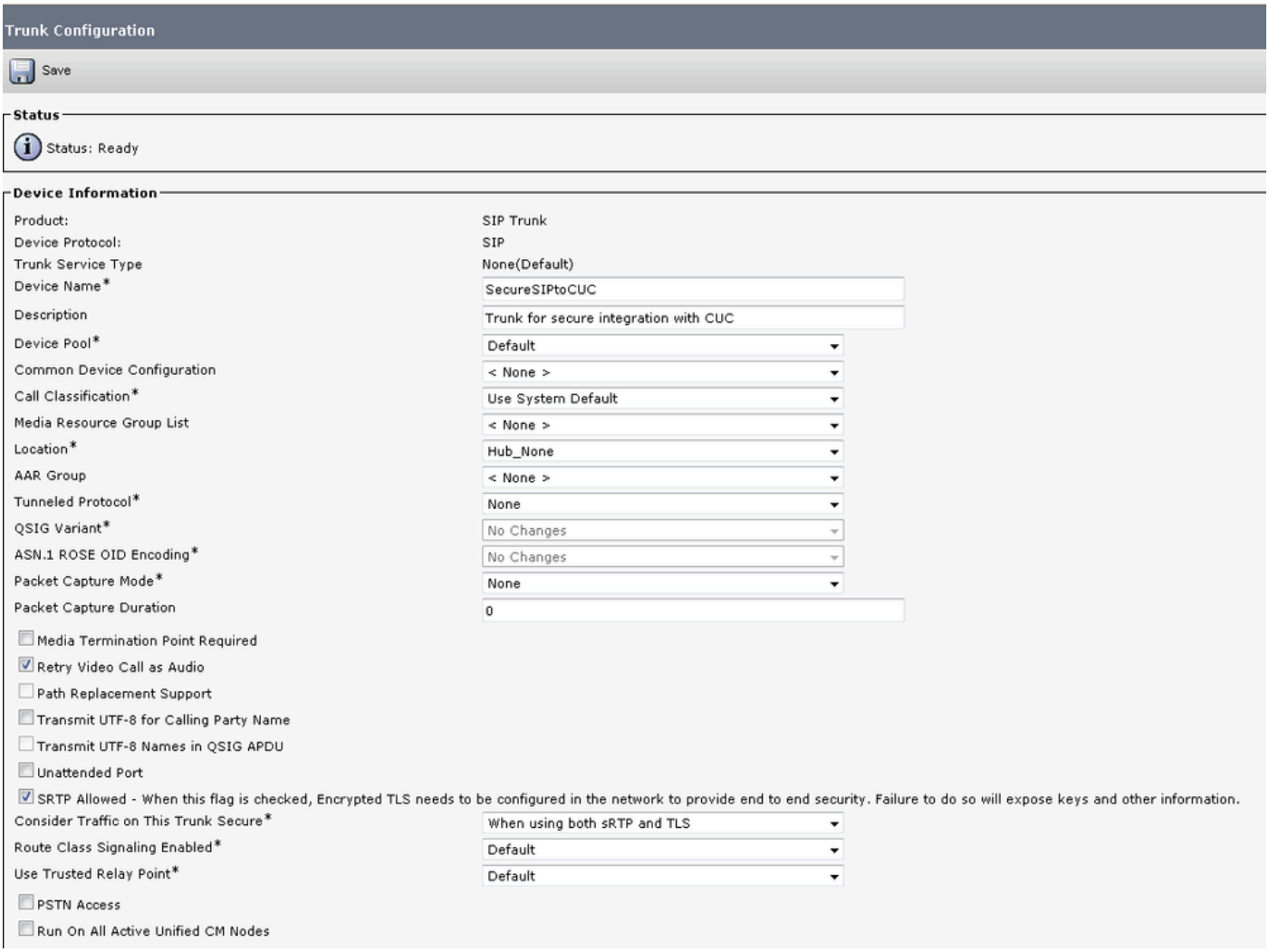
3. Creazione del trunk SIP

Selezionare Device > Trunk > Add new.Create un trunk SIP da utilizzare per l'integrazione sicura con Unity Connection, come mostrato nell'immagine.

Nella sezione Device Information della configurazione del trunk, immettere le seguenti informazioni:

- Nome dispositivo:
- Pool di dispositivi:
- SRTP consentito: Controllato

Nota: Verificare che il gruppo CallManager (nella configurazione del pool di dispositivi) contenga tutti i server configurati in CUC (Gruppo porte > Modifica > Server).

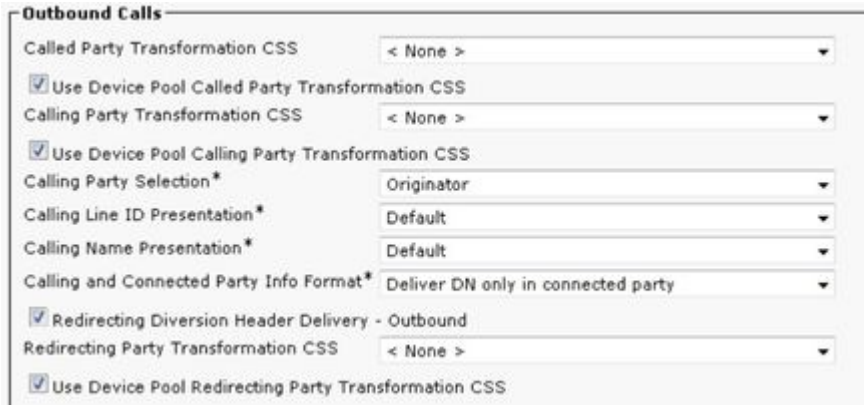


Nella sezione Chiamate in entrata della configurazione trunk, immettere le seguenti informazioni:

- Spazio di ricerca chiamate:
- Reindirizzamento recapito intestazione deviazione - In ingresso: Controllato

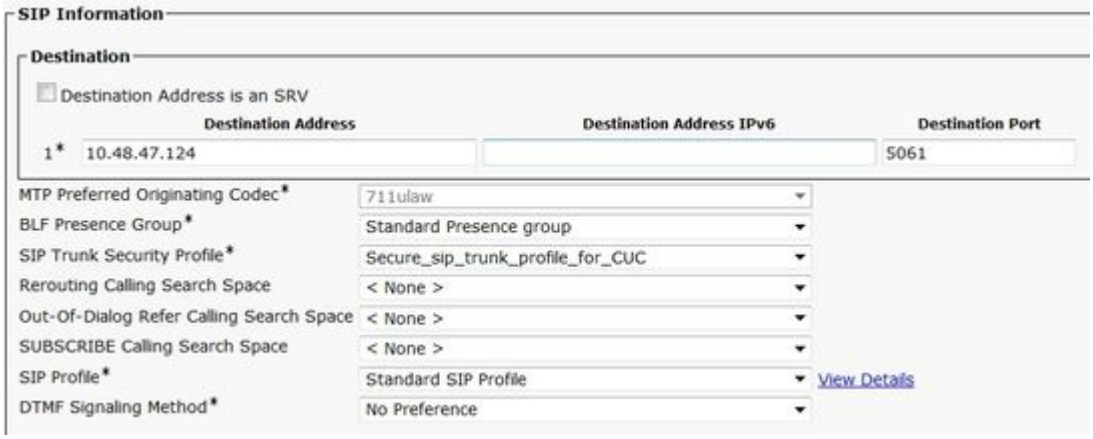
Nella sezione Chiamate in uscita della configurazione trunk, immettere le seguenti informazioni:

- Reindirizzamento consegna intestazione deviazione - In uscita: controllato



Nella sezione Informazioni SIP della configurazione trunk, immettere le seguenti informazioni:

- Indirizzo di destinazione:
- Profilo di sicurezza trunk SIP:
- Reindirizzamento dello spazio di ricerca delle chiamate:
- Riferimento esterno alla chiamata dello spazio di ricerca:
- Profilo SIP:

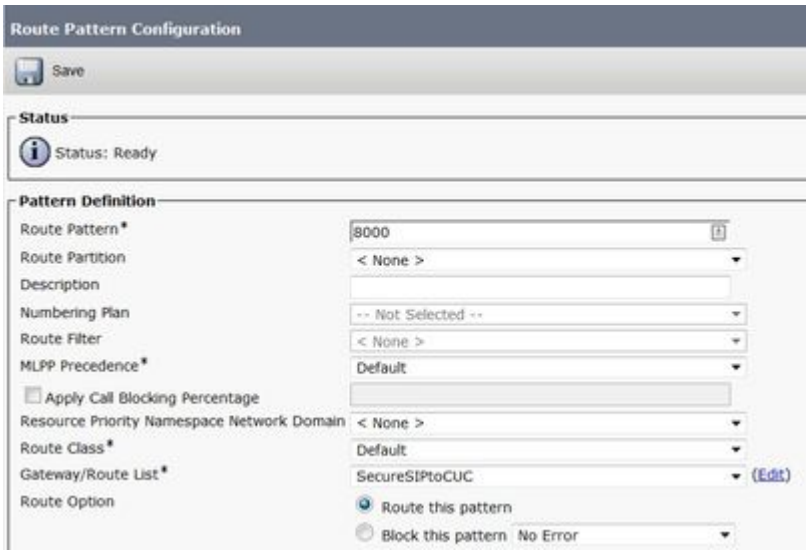


Regolare altre impostazioni in base alle proprie esigenze.

4. Creare una serie di stesura

Creare un modello di route che punti al trunk configurato (Routing chiamate > Route/Hunt > Modello di route). L'estensione immessa come numero di serie del percorso può essere utilizzata come pilota della segreteria telefonica. Immettere le informazioni seguenti:

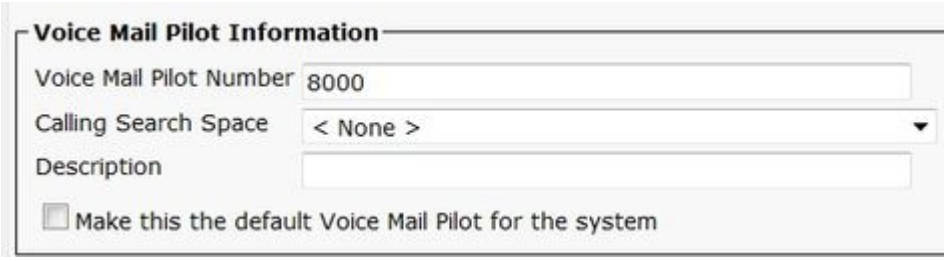
- Motivo route:
- Elenco gateway/route:



5. Creare un programma pilota per la casella vocale

Creare un programma pilota per la casella vocale per l'integrazione (Funzioni avanzate > Casella vocale > Programma pilota casella vocale). Immettere i seguenti valori:

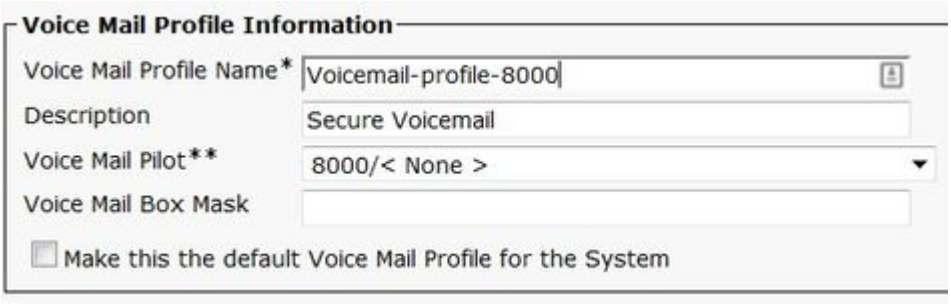
- Numero pilota casella vocale:
- Spazio di ricerca chiamate: che include partizioni contenenti il percorso utilizzato come pilota>



6. Crea profilo casella vocale

Crea un profilo di segreteria telefonica per collegare tutte le impostazioni (Funzioni avanzate > Segreteria telefonica > Profilo segreteria telefonica). Immettere le informazioni seguenti:

- Programma pilota casella vocale:
- Maschera casella vocale:

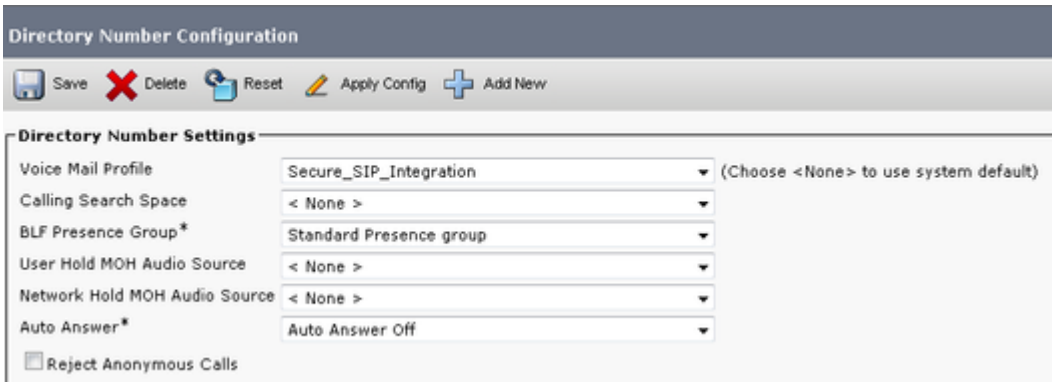


7. Assegnare il profilo della casella vocale ai DN

Assegnare il profilo della segreteria telefonica ai DN destinati a utilizzare un'integrazione protetta. Non dimenticare di fare clic sul pulsante 'Applica configurazione' dopo aver modificato le impostazioni DN:

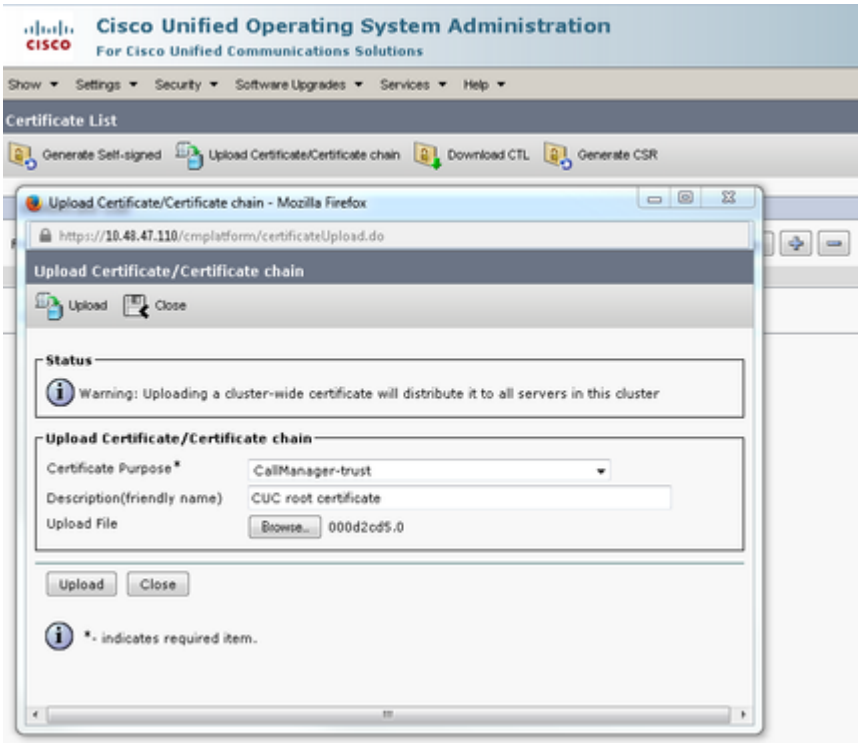
Accedere a: Instradamento delle chiamate > Numero directory e modifica:

- Profilo casella vocale: Integrazione Secure_SIP



8. Carica certificato radice CUC come CallManager-trust

Passare a Amministrazione sistema operativo > Protezione > Gestione certificati > Carica catena certificati/certificati e caricare il certificato radice CUC come CallManager-trust su tutti i nodi configurati per comunicare con il server CUC.



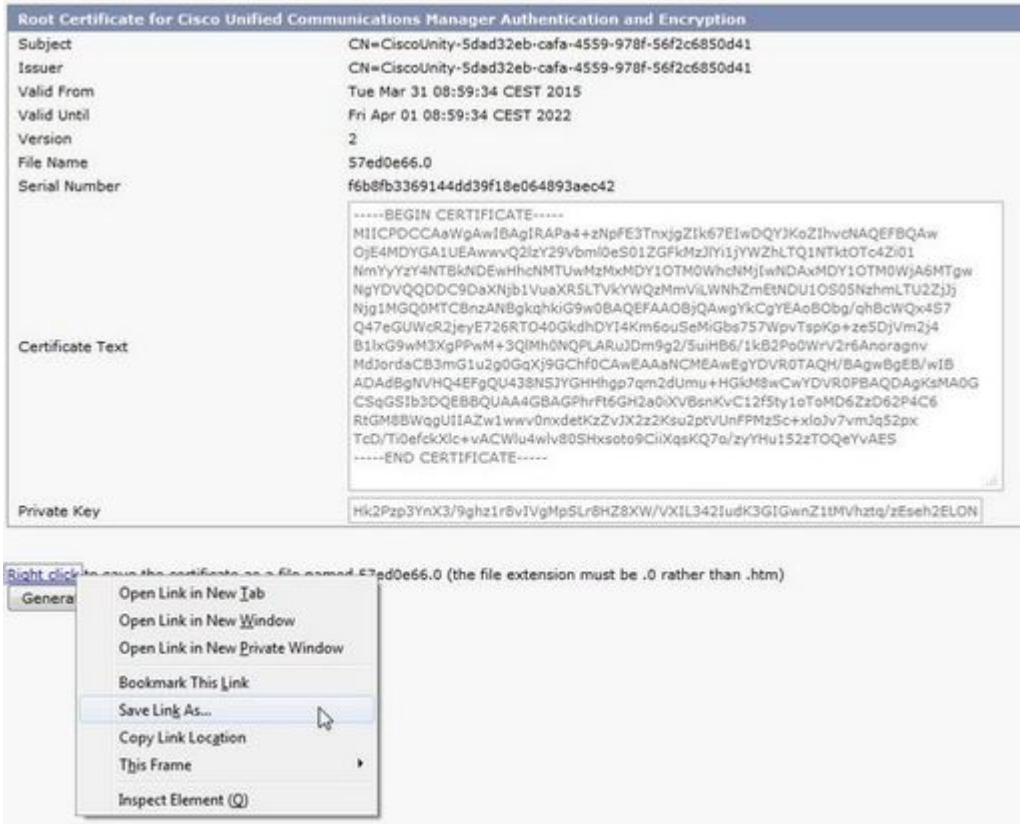
Nota: per rendere effettivo il certificato, è necessario riavviare il servizio Cisco CallManager dopo il caricamento del certificato.

Configurazione delle porte Secure SCCP

Configura CUC

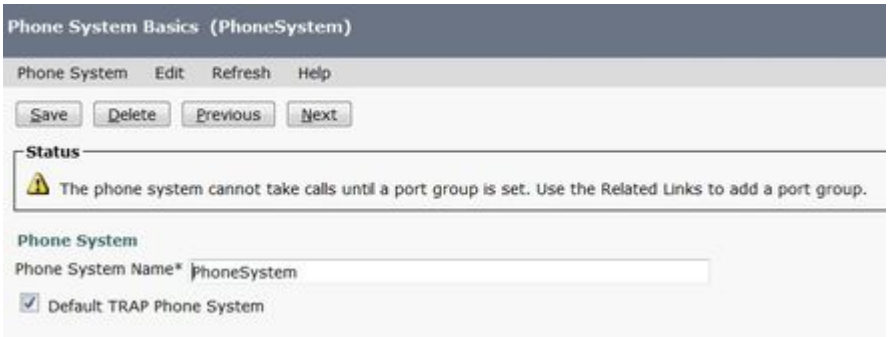
1. Scaricare il certificato radice CUC

Selezionare Amministrazione CUC > Integrazione telefonia > Protezione > Certificato radice. Fare clic con il pulsante destro del mouse sull'URL per salvare il certificato come file denominato <nomefile>.0 (l'estensione del file deve essere .0 anziché .htm)' e scegliere Salva:



2. Creare il sistema telefonico / modificare quello esistente.

Passare a Integrazione telefonia > Sistema telefonico. È possibile utilizzare il sistema telefonico esistente o crearne uno nuovo.

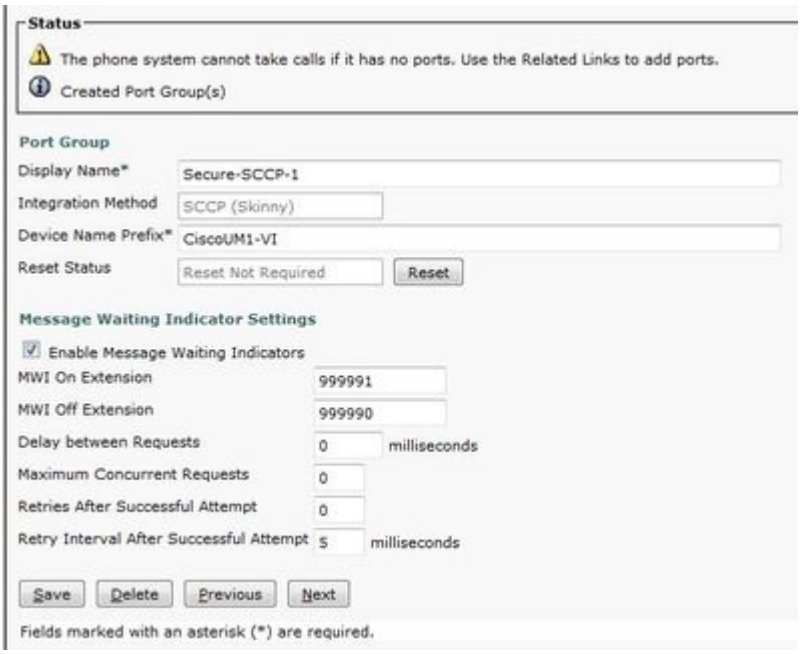


3. Aggiungere un nuovo gruppo di porte SCCP

Nella pagina Informazioni di base sistema telefonico, nella casella a discesa Collegamenti correlati, selezionare Aggiungi gruppo porte e Vai. Nella finestra di configurazione, immettere le seguenti informazioni:

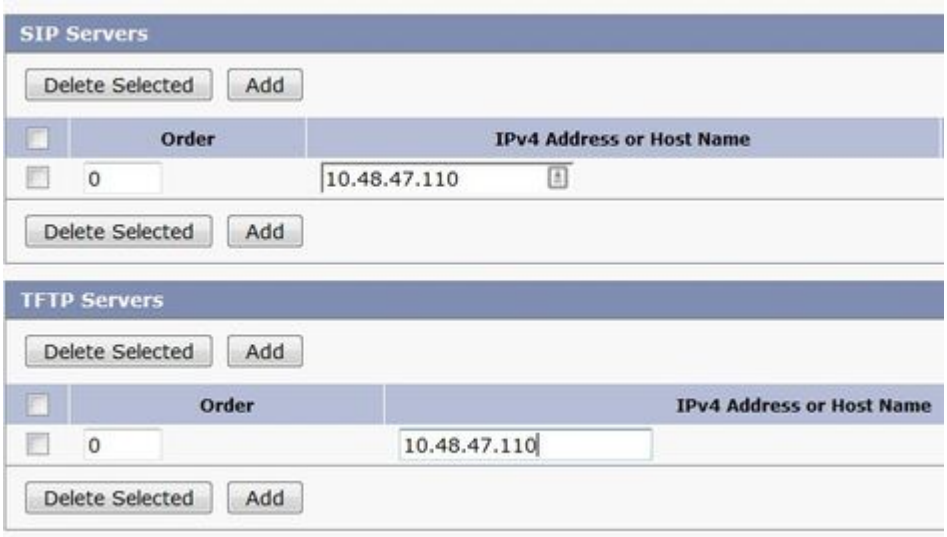
- Sistema telefonico:
- Tipo gruppo porte: SCCP
- Prefisso nome dispositivo*: Cisco UM1-VI
- Estensione MWI On:
- Estensione MWI Off:

Nota: Questa configurazione deve corrispondere alla configurazione di CUCM.



4. Modifica server

Passare a Modifica > Server e aggiungere il server TFTP dal cluster CUCM.

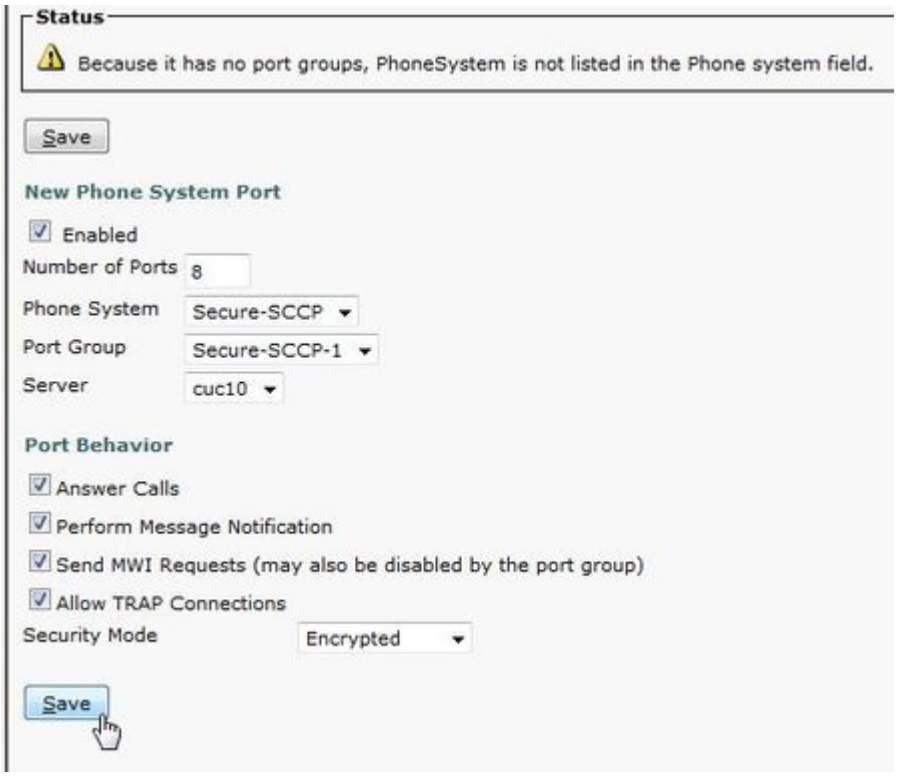


Nota: È importante fornire un indirizzo TFTP corretto. Il server CUC scarica il file CTL da questo TFTP come spiegato.

5. Aggiunta di porte SCCP sicure

Nella pagina Gruppo porte: Nozioni fondamentali selezionare Aggiungi porte nella casella a discesa Collegamenti correlati, quindi Vai. Nella finestra di configurazione immettere le informazioni seguenti:

- Abilitato: controllato
- Numero di porte:
- Sistema telefonico:
- Gruppo porte:
- Server:
- Comportamento porta:
- Modalità di protezione: Crittografia

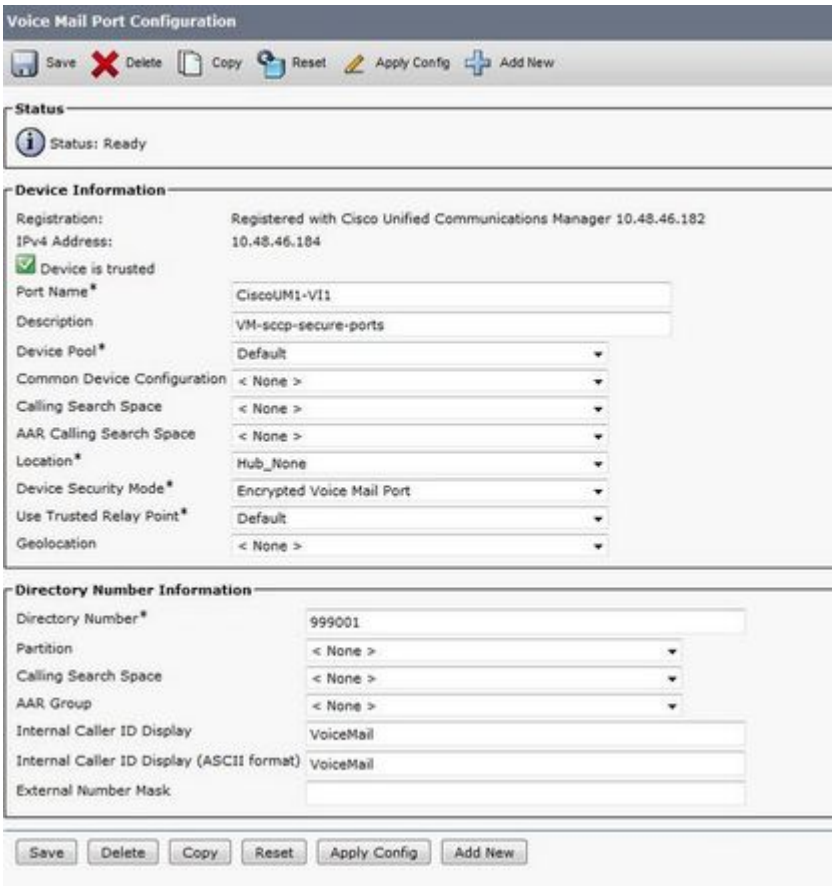


Configurazione di CUCM

1. Aggiunta di porte

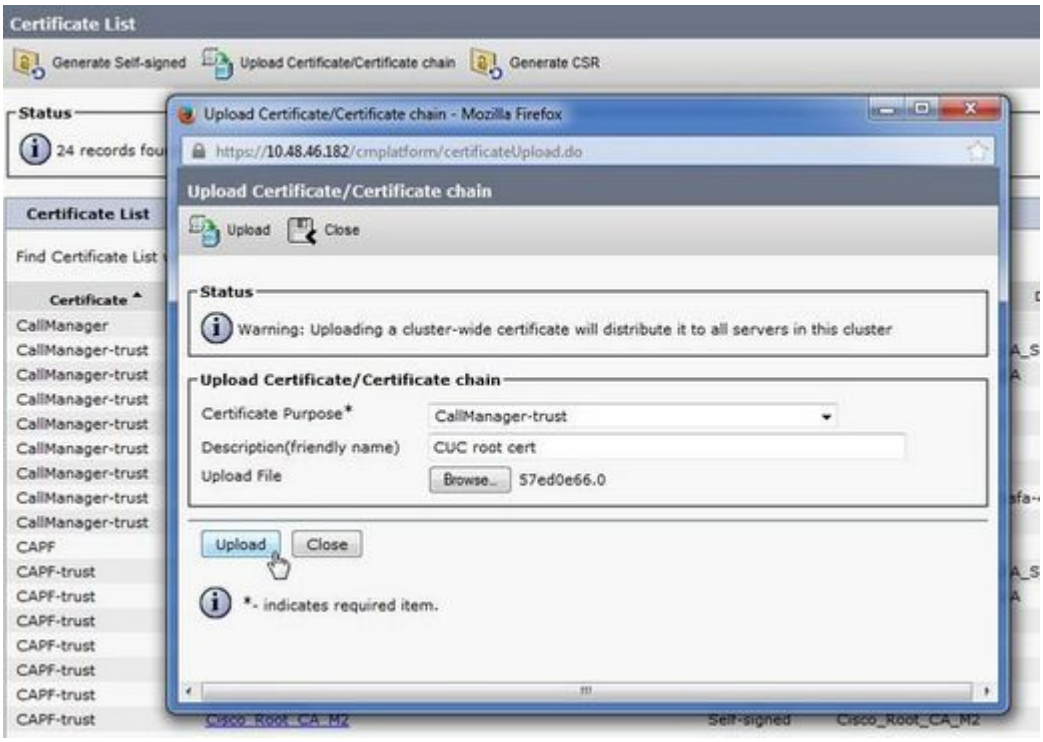
Passa a CUCM Administration > Advanced features > Voice Mail Port Configuration > Add New (Amministrazione CUCM > Funzioni avanzate > Configurazione porta casella vocale > Aggiungi nuovo).

Configurare le porte della casella vocale SCCP come di consueto. L'unica differenza consiste nella modalità di sicurezza del dispositivo nella configurazione della porta, in cui è necessario selezionare l'opzione Encrypted Voice Mail Port (Porta segreteria telefonica crittografata).



2. Carica certificato radice CUC come CallManager-trust

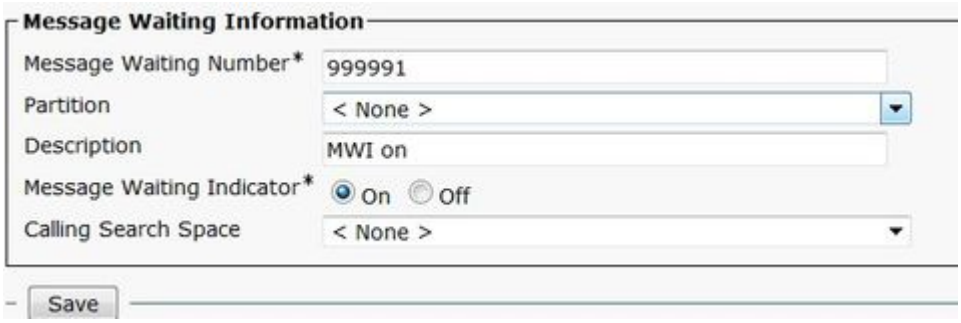
Passare a Amministrazione sistema operativo > Protezione > Gestione certificati > Carica catena certificati/certificati e caricare il certificato radice CUC come CallManager-trust su tutti i nodi configurati per comunicare con il server CUC.

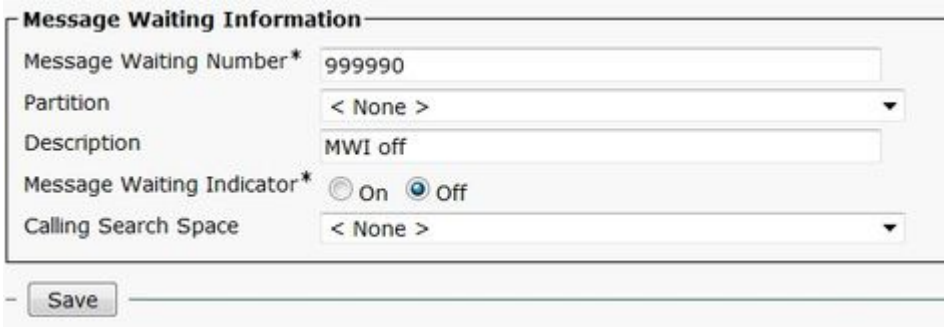


Nota: per rendere effettivo il certificato, è necessario riavviare il servizio Cisco CallManager dopo il caricamento del certificato.

3. Configura estensioni MWI (Message Waiting Information) On/Off

Selezionare Amministrazione CUCM > Funzioni avanzate > Configurazione porta casella vocale e configurare le estensioni MWI On/Off. I numeri MWI devono corrispondere alla configurazione CUC.

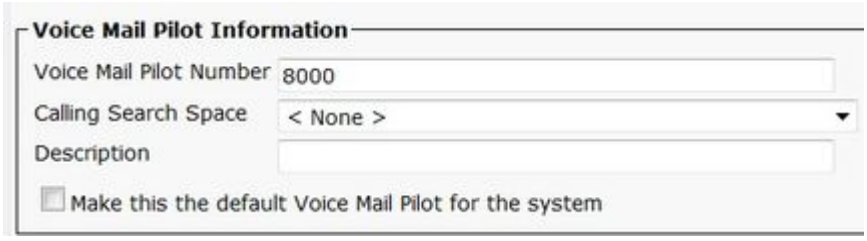




4. Creazione del programma pilota per la casella vocale

Creare un programma pilota per la casella vocale per l'integrazione (Funzioni avanzate > Casella vocale > Programma pilota casella vocale). Immettere i seguenti valori:

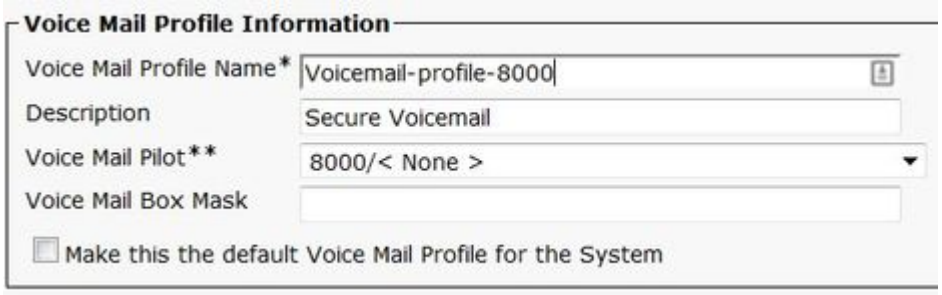
- Numero pilota casella vocale:
- Spazio di ricerca chiamate: che include partizioni contenenti il percorso utilizzato come pilota>



5. Crea profilo casella vocale

Crea un profilo di segreteria telefonica per collegare tutte le impostazioni (Funzioni avanzate > Segreteria telefonica > Profilo segreteria telefonica). Immettere le informazioni seguenti:

- Programma pilota casella vocale:
- Maschera casella vocale:

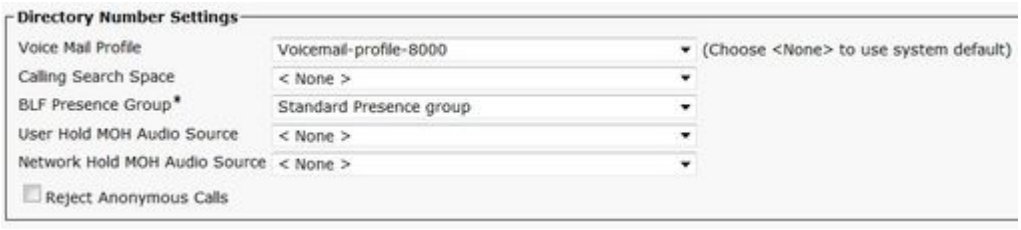


6. Assegnare il profilo della casella vocale ai DN

Assegnare il profilo della casella vocale ai DN che intendono utilizzare un'integrazione protetta. Fare clic sul pulsante Applica configurazione dopo aver modificato le impostazioni del DN:

Passare a Instradamento chiamate > Numero directory e modificare in:

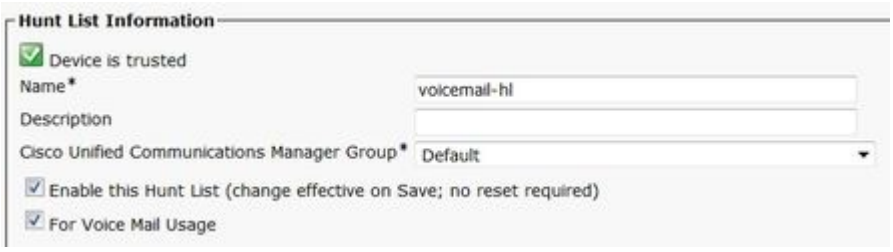
- Profilo casella vocale: Voicemail-profile-8000



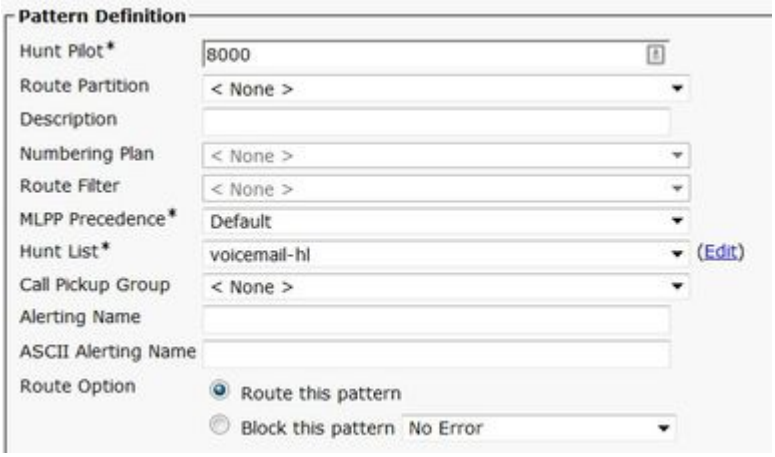
7. Crea un gruppo di ricerca della casella vocale

a) Aggiungere un nuovo gruppo Linea (Instradamento chiamata > Instradamento/Caccia > Gruppo Linea)

b) Aggiungere un nuovo elenco di ricerca della segreteria telefonica (Instradamento delle chiamate > Instradamento/ricerca > Elenco di ricerca)



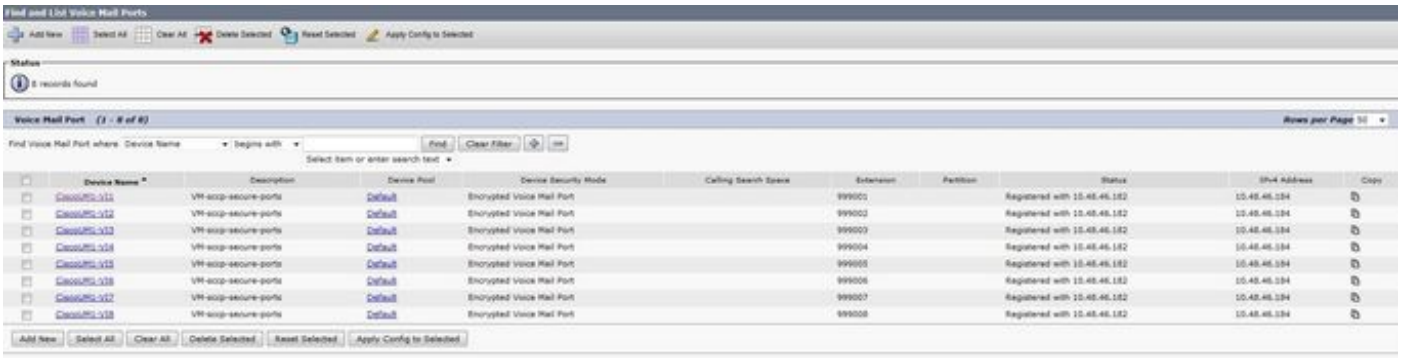
c) Aggiungere un nuovo pilota di ricerca (Instradamento delle chiamate > Instradamento/ricerca > Pilota di ricerca)



Verifica

Verifica porte SCCP

Passare a Amministrazione CUCM > Funzionalità avanzate > Segreteria telefonica > Porte della casella vocale e verificare la registrazione della porta.



Premere il pulsante Voice Mail sul telefono per chiamare la segreteria telefonica. Se l'estensione dell'utente non è configurata nel sistema Unity Connection, verrà visualizzato il messaggio di saluto iniziale.

Verifica Secure SIP Trunk

Premere il pulsante Voice Mail sul telefono per chiamare la segreteria telefonica. Se l'estensione dell'utente non è configurata nel sistema Unity Connection, verrà visualizzato 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 Device > Trunk, come mostrato nell'immagine.

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.

Risoluzione dei problemi

1. Suggerimenti generali per la risoluzione dei problemi

Per risolvere i problemi relativi all'integrazione protetta, attenersi alla procedura seguente:

- Verifica della configurazione.
- Verificare che tutti i servizi correlati siano in esecuzione. (CUCM - CallManager, TFTP, CUC - Gestione conversazioni)
- Verificare che le porte necessarie per una comunicazione sicura tra i server siano aperte nella rete (porta TCP 2443 per l'integrazione SCCP e TCP 5061 per l'integrazione SIP).
- Se tutto questo è corretto, procedere con la raccolta di tracce.

2. Tracce da raccogliere

Raccogli queste tracce per risolvere i problemi relativi all'integrazione protetta.

- Acquisizione di pacchetti da CUCM e CUC
- Tracce di CallManager
- Tracce di Cisco Conversation Manager

Fare riferimento a queste risorse per ulteriori informazioni su:

Come eseguire l'acquisizione di un pacchetto su CUCM:

http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html

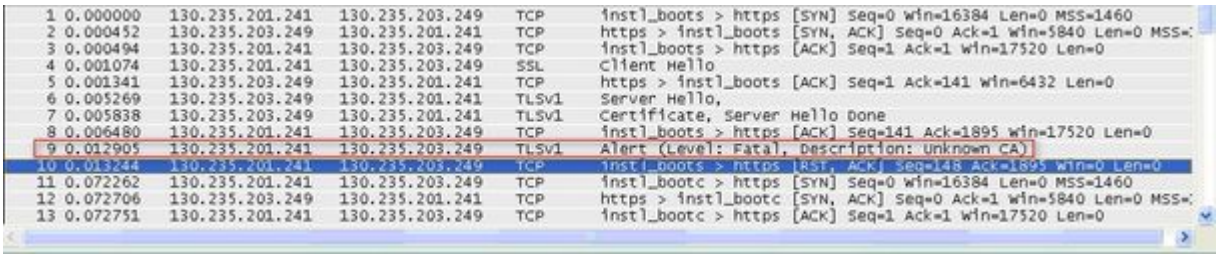
Come abilitare le tracce sul server CUC:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/1

Problemi comuni

Caso 1: Impossibile stabilire una connessione sicura (avviso CA sconosciuto)

Una volta raccolta l'acquisizione del pacchetto da uno dei server, viene stabilita la sessione TLS.



Il client ha inviato al server un avviso con un errore irreversibile di CA sconosciuta, semplicemente perché non è stato in grado di verificare il certificato inviato dal server.

Esistono due possibilità:

1) CUCM invia l'avviso CA sconosciuta

- Verificare che il certificato radice CUC corrente sia caricato sul server che comunica con il server CUC.
- Verificare che il servizio CallManager sia riavviato nel server corrispondente.

2) CUC invia l'avviso CA sconosciuta

- Verificare che l'indirizzo IP TFTP sia stato immesso correttamente nella configurazione Gruppo porte > Modifica > Server sul server CUC.
- Verificare che il server TFTP CUCM sia raggiungibile dal server di connessione.
- Verificare che il file CTL sul CUCM TFTP sia aggiornato (confrontare l'output di "show ctl" con i certificati visualizzati nella pagina Amministratore del sistema operativo). In caso contrario, eseguire nuovamente il client CTLC.
- Riavviare il server CUC OPPURE eliminare e ricreare il gruppo di porte per scaricare nuovamente il file CTL dal server CUCM TFTP.

Caso 2: Impossibile scaricare il file CTL da CUCM TFTP

Questo errore viene visualizzato nelle tracce di Gestione conversazioni:

<#root>

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server ce
MiuGeneral,25,Error executing tftp command
```

'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not found on server)

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true),
```

error retrieving server certificates.

```
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as ID=1
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

Soluzione:

1. Verificare che il server TFTP sia corretto nella configurazione Gruppo porte > Modifica > Server.

2. Verificare che il cluster CUCM sia in modalità protetta.

3. Verificare che il file CTL esista sul TFTP CUCM.

Caso 3: Porte non registrate

Questo errore viene visualizzato nelle tracce di Gestione conversazioni:

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting retry timer
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM IP Add
```

Soluzione:

1. Questo problema è probabilmente dovuto alla mancata corrispondenza nel checksum md5 del file CTL su CUCM e CUC in seguito alla rigenerazione di

certificati. Riavviare il server CUC per aggiornare il file CTL.

Difetti

CSCum48958 - CUCM 10.0 (lunghezza indirizzo IP non corretta)

CSCtn87264 - Connessione TLS non riuscita per porte SIP protette

CSCur10758 - Impossibile eliminare i certificati revocati Unity Connection

CSCur10534 - Unity Connection 10.5 TLS/PKI inter-op redundant CUCM

CSCve47775 - Richiesta di funzionalità per un metodo per aggiornare e rivedere il CTLFile di CUCM sul CUC

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).