

次世代暗号化(NGE)に基づくCUCMとCUC間のセキュアSIP統合の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[ネットワーク図](#)

[証明書の要件](#)

[ネゴシエートされたRSAキーベースの暗号](#)

[ネゴシエートされたECキーベースの暗号](#)

[設定 – Cisco Unity Connection\(CUC\)](#)

[1.新しいポートグループの追加](#)

[2. TFTPサーバ参照の追加](#)

[3.ボイスメールポートの追加](#)

[4.サードパーティCAのCUCMルートおよび中間証明書のアップロード](#)

[設定 – Cisco Unified CM\(CUCM\)](#)

[1. SIPトランクセキュリティプロファイルの作成](#)

[2.セキュアSIPトランクの作成](#)

[3. TLSおよびSRTP暗号の設定](#)

[4. CUC Tomcat証明書のアップロード \(RSAおよびECベース \)](#)

[5.ルートパターンの作成](#)

[6.ボイスメールパイロット、ボイスメールプロファイルを作成し、DNに割り当てます](#)

[設定：サードパーティCAによるECキーベースの証明書の署名 \(オプション \)](#)

[確認](#)

[セキュアSIPトランクの検証](#)

[セキュアRTPコールの検証](#)

[関連情報](#)

概要

このドキュメントでは、次世代暗号化を使用したCisco Unified Communication Manager(CUCM)とCisco Unity Connection(CUC)サーバ間のセキュアSIP接続の設定と検証について説明します。

Next Generation Security over SIPインターフェイスは、TLS 1.2、SHA-2、およびAES256プロトコルに基づくSuite B暗号を使用するようにSIPインターフェイスを制限します。RSA暗号またはECDSA暗号の優先順位に基づいて、さまざまな暗号の組み合わせを可能にする。Unity ConnectionとCisco Unified CM間の通信中に、暗号とサードパーティ証明書の両方が両端で検証されます。次世代暗号化サポートの設定を次に示します。

サードパーティの証明機関によって署名された証明書を使用する場合は、構成セクションの最後で証明書署名から開始します (構成 – サードパーティCAによるECキーベースの証明書への署名

)

前提条件

要件

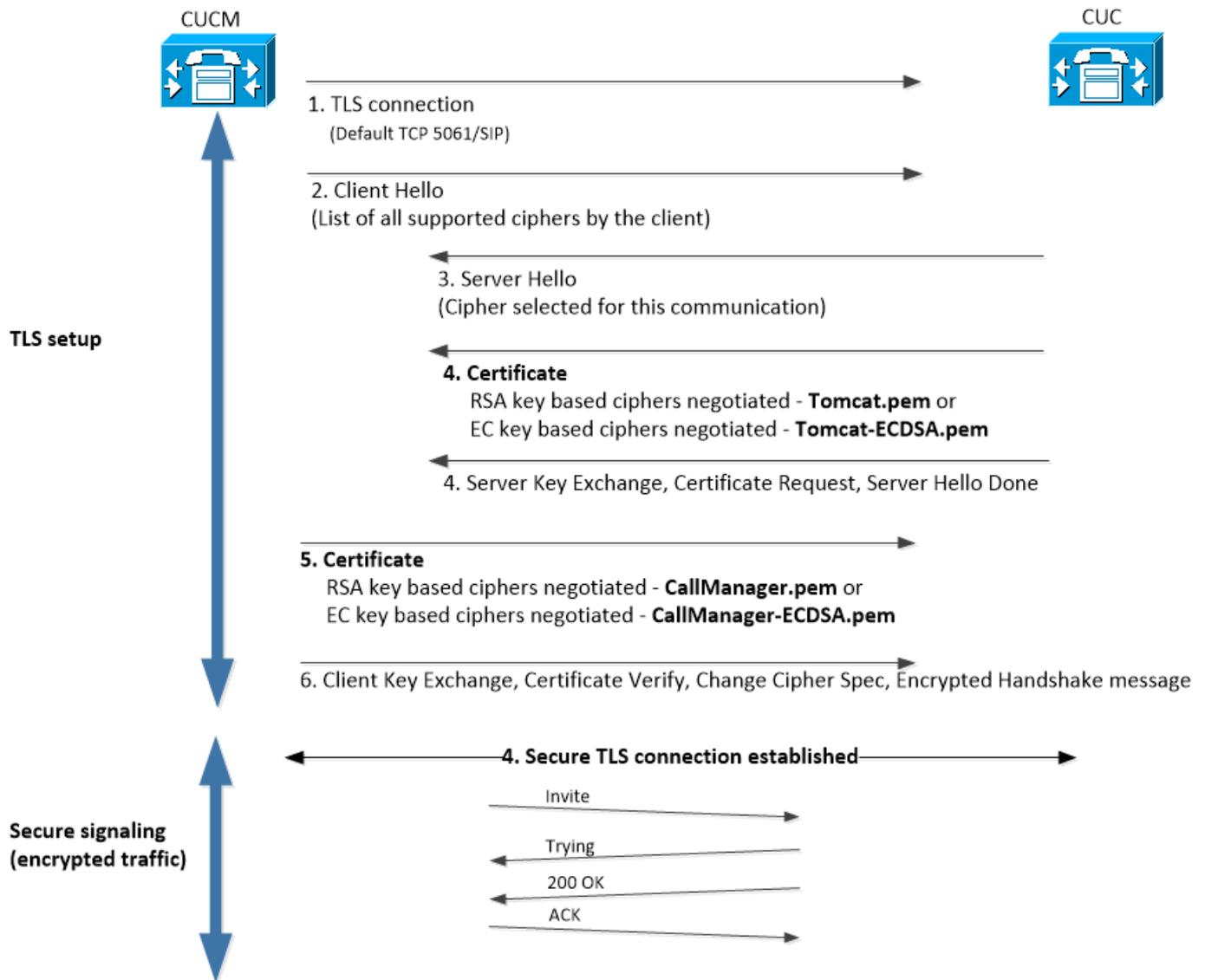
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

混合モードのCUCMバージョン11.0以降
CUCバージョン11.0以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

次の図は、次世代暗号化のサポートが有効になった後にCUCMとCUC間のセキュアな接続を確立するためのプロセスを簡単に説明しています。



証明書の要件

Cisco Unity ConnectionでNext Generation Encryptionサポートを有効にした後の証明書交換要件を次に示します。

・ネゴシエートされたRSAキーベースの暗号

使用されるCUCM証明書	使用されるCUC証明書	CUCMにアップロードする証明書
CallManager.pem (自己署名)	Tomcat.pem (自己署名)	CUCMにアップロードされるTomcat.pem
CallManager.pem (CA署名付き)	Tomcat.pem (CA署名付き)	CUCMにアップロードされるCUCルート証明書 *1 > CallManager-trust
CallManager.pem (CA署名付き)	Tomcat.pem (自己署名)	CUCMにアップロードされるTomcat.pem
CallManager.pem (自己署名)	Tomcat.pem (CA署名付き)	CUCMにアップロードされるCUCルート証明書 CallManager-trust

*1 CUCルートおよび中間CA証明書は、Unity connection Tomcat証明書(Tomcat.pem)に署名したCA証明書を参照します。

*2 CUCMルートおよび中間CA証明書は、CUCM CallManager証明書(Callmanager.pem)に署名したCA証明書を参照します。

・ネゴシエートされたECキーベースの暗号

使用されるCUCM証明書	使用されるCUC証明書	CUCMにアップロードする証明書	CUCにアップロードする証明書
CallManager-ECDSA.pem (自己署名)	Tomcat-ECDSA.pem (自己署名)	[CUCM] > [CallManger-trust] にアップロードされる Tomcat-ECDSA.pem	ありません。
CallManager-ECDSA.pem (CA署名付き)	Tomcat-ECDSA.pem (CA署名付き)	CUCMにアップロードされるCUCルートおよび中間CA証明書*1 > CallManager-trust	CUC > CallManager-trustにアップロードするCUCMルートおよび中間CA証明書*2。
CallManager-ECDSA.pem (CA署名付き)	Tomcat-ECDSA.pem (自己署名)	[CUCM] > [CallManger-trust] にアップロードされる Tomcat-ECDSA.pem。	CUCにアップロードされるCUCMルートおよび中間CA証明書 > CallManager-trust。
CallManager-ECDSA.pem (自己署名)	Tomcat-ECDSA.pem (CA署名付き)	CUCMにアップロードされるCUCルートおよび中間CA証明書 > CallManager-trust	ありません。

*1 CUCルートおよび中間CA証明書は、Unity connection ECベースのTomcat証明書(Tomcat-ECDSA.pem)に署名したCA証明書を指します。

*2 CUCMルートおよび中間CA証明書は、CUCM CallManager証明書(CallManager-ECDSA.pem)に署名したCA証明書を指します。

- 注：Tomcat-ECDSA.pem証明書は、11.0.1バージョンのCUCではCallManager-ECDSA.pemと呼ばれます。CUC 11.5.xから、証明書の名前がTomcat-ECDSA.pemに変更されました。

設定 – Cisco Unity Connection(CUC)

1.新しいポートグループの追加

[Cisco Unity Connection Administration]ページ > [Telephony integration] > [Port group]に移動し、[Add New]をクリックします。必ず[Enable Next Generation Encryption]チェックボックスをオンにします。

New Port Group

Phone System

Create From Port Group Type Port Group

Port Group Description

Display Name*

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile

Enable Next Generation Encryption

Secure RTP

Primary Server Settings

IPv4 Address or Host Name

IPv6 Address or Host Name

Port

1. 注:[Enable Next Generation Encryption]チェックボックスが有効になると、Unity ConnectionのCisco Tomcat証明書はSSLハンドシェイク時に使用されます。
 - ・ ECDSAベースの暗号がネゴシエートされた場合、SSLハンドシェイクでECキーベースのtomcat-ECDSA証明書が使用されます。
 - ・ RSAベースの暗号がネゴシエートされた場合、SSLハンドシェイクでRSAキーベースのtomcat証明書が使用されます。

2. TFTPサーバ参照の追加

[Port Group Basics]ページで、[Edit] > [Servers]に移動し、CUCMクラスタのTFTPサーバのFQDNを追加します。TFTPサーバのFQDN/ホスト名は、CallManager証明書の共通名(CN)と一致している必要があります。サーバのIPアドレスが機能せず、ITLファイルのダウンロードに失敗します。したがって、DNS名は、設定されたDNSサーバを介して解決できる必要があります。

SIP Servers			
Delete Selected Add			
<input type="checkbox"/>	Order	IPv4 Address or Host Name	
<input type="checkbox"/>	0	10.48.47.109	
Delete Selected Add			

TFTP Servers			
Delete Selected Add			
<input type="checkbox"/>	Order	IPv4 Address or Host Name	
<input type="checkbox"/>	0	CUCMv11	
Delete Selected Add			

[Cisco Unity Connection Serviceability] > [Tools] > [Service Management]に移動して、各ノードの Connection Conversation Managerを再起動します。これは、設定を有効にするために必須です。

- 注：Unity Connectionは、セキュアな6972ポート(URL:https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv)でhttpsプロトコルを使用して、CUCMのTFTPからITLファイル(ITLfile.tlv)をダウンロードします。CUCがITLファイルから「CCM+TFTP」機能証明書を検索しているため、CUCMは混合モードである必要があります。

[Telephony integration] > [Port group] > [Port Group Basics]設定ページに戻り、新しく追加したポートグループをリセットします。

Port Group		
Display Name*	PhoneSystem-1	
Integration Method	SIP	
Reset Status	Reset Required	Reset

Session Initiation Protocol (SIP) Settings

Register with SIP Server

Authenticate with SIP Server

- 注：ポートグループがリセットされるたびに、CUCサーバはCUCMサーバに接続して、ローカルに保存されたITLファイルを更新します。

3.ボイスメールポートの追加

[Telephony integration] > [Port]に戻り、[Add new]をクリックして、新しく作成したポートグループにポートを追加します。

New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

Port Behavior

Answer Calls

Perform Message Notification

Send MWI Requests (may also be disabled by the port group)

Allow TRAP Connections

4. サードパーティCAのCUCMルートおよび中間証明書のアップロード

サードパーティ証明書の場合は、Unity ConnectionのCallManager信頼にサードパーティ認証局(CA)のルート証明書と中間証明書をアップロードする必要があります。これは、サードパーティCAがCall Manager証明書に署名した場合にのみ必要です。このアクションを実行するには、[Cisco Unified OS Administration] > [Security] > [Certificate Management]に移動し、[Upload Certificate]をクリックします。

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

設定 – Cisco Unified CM(CUCM)

1. SIPトランクセキュリティプロファイルの作成

[CUCM Administration] > [System] > [Security] > [SIP Trunk Security Profile]に移動し、新しいプロファイルを追加します。[X.509 Subject Name]は、CUCサーバのFQDNと一致している必要があります。

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

- 注:CLIコマンド「show cert own tomcat/tomcat.pem」は、Unity Connection上のRSAキーベースのtomcat証明書を表示できます。CNは、CUCMで設定されているX.509のサブジェクト名と一致する必要があります。CNは、UnityサーバのFQDN/ホスト名と同じです。ECキーベースの証明書の[サブジェクト代替名(SAN)(Subject Alternate Name (SAN))]フィールドにFQDN/ホスト名が含まれています。

2.セキュアSIPトランクの作成

[Device] > [Trunk] > [Click and Add new]に移動し、Unity Connectionとのセキュアな統合に使用される標準SIPトランクを作成します。

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure*

Route Class Signaling Enabled*

Use Trusted Relay Point*

PSTN Access

Run On All Active Unified CM Nodes

Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Inbound	

Outbound Calls

Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS	
Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Calling and Connected Party Info Format*	Deliver DN only in connected party
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Outbound	
Redirecting Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Redirecting Party Transformation CSS	

Destination

<input type="checkbox"/> Destination Address is an SRV			
	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.123		5061
MTP Preferred Originating Codec*	711ulaw		
BLF Presence Group*	Standard Presence group		
SIP Trunk Security Profile*	cuc-secure-profile-EDCS		
Rerouting Calling Search Space	< None >		
Out-Of-Dialog Refer Calling Search Space	< None >		
SUBSCRIBE Calling Search Space	< None >		
SIP Profile*	Standard SIP Profile	View Details	
DTMF Signaling Method*	No Preference		

3. TLSおよびSRTP暗号の設定

1. 注： Unity ConnectionとCisco Unified Communications Manager間のネゴシエーションは、次の条件を満たすTLS暗号化設定によって異なります。 Unity Connectionがサーバとして機能する場合、TLS暗号化ネゴシエーションはCisco Unified CMによって選択されたプリファレンスに基づいて行われます。 ECDSAベースの暗号がネゴシエートされた場合、SSLハンドシェイクでECキーベースのtomcat-ECDSA証明書が使用されます。 RSAベースの暗号がネゴシエートされた場合、SSLハンドシェイクではRSAキーベースのtomcat証明書が使用されます。 Unity Connectionがクライアントとして機能する場合、TLS暗号化ネゴシエーションはUnity Connectionによって選択されたプリファレンスに基づいて行われます。

[Cisco Unified CM] > [システム(Systems)] > [エンタープライズパラメータ(Enterprise Parameters)]に移動し、[TLS and SRTP Ciphers from]ドロップダウンリストから適切な暗号オプションを選択します。

Security Parameters	
Cluster Security Mode *	1
LBM Security Mode *	Insecure ▼
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
TFTP File Signature Algorithm *	SHA-1 ▼
Enable Caching *	True ▼
Authentication Method for API Browser Access *	Basic ▼
TLS Ciphers *	All Ciphers RSA Preferred ▼
SRTP Ciphers *	All Supported Ciphers ▼
HTTPS Ciphers *	RSA Ciphers Only ▼

[Cisco Unified Serviceability]ページの[Tools] > [Control Center-Feature Services]に移動し、[CM Services]で[Cisco Call Manager]を選択して、各ノードのCisco Call Managerサービスを再起動します

[Cisco Unity Connection Administration]ページ > [System Settings] > [General Configurations]に移動し、[TLS and SRTP Ciphers from]ドロップダウンリストから適切な暗号オプションを選択します。

Edit General Configuration	
Time Zone	(GMT+01:00) Europe/Warsaw ▼
System Default Language	English(United States) ▼
System Default TTS Language	English(United States) ▼
Recording Format	G.711 mu-law ▼
Maximum Greeting Length	90
Target Decibel Level for Recordings and Messages	-26
Default Partition	cucv11 Partition ▼
Default Search Scope	cucv11 Search Space ▼
When a recipient cannot be found	Send a non-delivery receipt ▼
IP Addressing Mode	IPv4 ▼
TLS Ciphers	All Ciphers RSA Preferred ▼
SRTP Ciphers	All supported AES-256, AES-128 ciphers ▼
HTTPS Ciphers	RSA Ciphers Only ▼

[Cisco Unity Connection Serviceability] > [Tools] > [Service Management]に移動して、各ノードのConnection Conversation Managerを再起動します。

優先順位の付いたTLS暗号化オプション

TLS暗号化オプション

最強 – AES-256 SHA-384のみ : RSA推奨

最強のAES-256 SHA-384のみ : ECDSA優先

中AES-256 AES-128のみ : RSA推奨

優先順のTLS暗号

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

中AES-256 AES-128のみ : ECDSA優先

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

すべての暗号RSA優先 (デフォルト)

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

すべての暗号ECDSA優先

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

優先順位のSRTP暗号化オプション

SRTP暗号化オプション

優先順位のSRTP

サポートされているすべてのAES-256、AES-128暗号

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_32

AEAD AES-256、AES-128 GCMベースの暗号

- AEAD_AES_256_GCM

AEAD AES256 GCMベースの暗号のみ

- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

4. CUC Tomcat証明書のアップロード (RSAおよびECベース)

[OS Administration] > [Security] > [Certificate Management]に移動し、両方のCUC Tomcat証明書 (RSAおよびECベース) をCallManager信頼ストアにアップロードします。

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File tomcat-ECDSA.pem

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File tomcat.pem

1. 注:ECDSA暗号のみがネゴシエートされる場合は、両方のUnity Tomcat証明書のアップロードは必須ではありません。このような場合、ECベースのTomcat証明書で十分です。サードパーティ証明書の場合は、サードパーティ認証局のルート証明書と中間証明書をアップロードする必要があります。これは、サードパーティCAがUnity Tomcat証明書に署名した場合にのみ必要です。

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

すべてのノードでCisco Call Managerプロセスを再起動し、変更を適用します。

5. ルートパターンの作成

[コールルーティング(Call Routing)] > [ルート/ハント(Route/Hunt)] > [ルートパターン(Route Pattern)]に移動して、設定済みのトランクをポイントするルートパターンを設定します。ルートパターン番号として入力された内線番号は、ボイスメールパイロットとして使用できます。

Pattern Definition

Route Pattern*	2000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	CUCv11
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

6.ボイスメールパイロット、ボイスメールプロフィールを作成し、DNに割り当てます

[拡張機能(Advanced Features)] > [ボイスメール(Voice Mail)] > [ボイスメールパイロット(Voice Mail Pilot)]に移動して、統合用のボイスメールパイロットを作成します。

Voice Mail Pilot Information

Voice Mail Pilot Number	2000
Calling Search Space	< None >
Description	Default

すべての設定を[Advanced Features] > [Voice Mail] > [Voice Mail Profile]にリンクするために、ボイスメールプロフィールを作成します

Voice Mail Profile Information

Voice Mail Profile	VoiceMailProfile-8000 (used by 0 devices)
Voice Mail Profile Name*	VoiceMailProfile-8000
Description	
Voice Mail Pilot**	2000/< None >
Voice Mail Box Mask	

[コールルーティング(Call Routing)] > [電話番号(Directory number)]に移動し、セキュアな統合を使用するために新しく作成したボイスメールプロフィールをDNに割り当てます

Directory Number Settings

Voice Mail Profile	VoiceMailProfile-8000	(Choose <None> to use system default)
Calling Search Space	< None >	
BLF Presence Group*	Standard Presence group	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	

設定：サードパーティCAによるECキーベースの証明書の署名 (オプション)

証明書は、システム間のセキュアな統合を設定する前に、サードパーティCAによって署名される場合があります。次の手順に従って、両方のシステムで証明書に署名します。

Cisco Unity Connection

1. CUC Tomcat-ECDSA用の証明書署名要求(CSR)を生成し、サードパーティCAによって署名された証明書を取得します
2. CAはアイデンティティ証明書 (CA署名付き証明書) とCA証明書 (CALルート証明書) を提供します。これらは次のようにアップロードする必要があります。
tomcat-trustストアにCALルート証明書をアップロードします
tomcat-EDCSストアへのID証明書のアップロード
3. CUCのConversation Managerの再起動

Cisco Unified CM

1. CUCM CallManager-ECDSA用のCSRを生成し、サードパーティCAによって署名された証明書を使用する
2. CAはアイデンティティ証明書 (CA署名付き証明書) とCA証明書 (CALルート証明書) を提供します。これらは次のようにアップロードする必要があります。
callmanager-trustストアへのCALルート証明書のアップロード
callmanager-EDCSストアへのID証明書のアップロード
3. 各ノードでCisco CCMおよびTFTPサービスを再起動します

同じプロセスを使用して、CUC Tomcat証明書とCallManager証明書に対してCSRが生成され、tomcatストアとcallmanagerストアにそれぞれアップロードされるRSAキーベースの証明書に署名します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

セキュア SIP トランクの検証

電話の [Voice Mail] ボタンを押して、ボイス メールを送信します。Unity Connection システムでユーザの内線番号が設定されていない場合、オープニング グリーティングを聞く必要があります。

または、SIP OPTION のキープアライブを有効にして、SIP トランクのステータスをモニタすることができます。このオプションは、SIP トランクに割り当てられた SIP プロファイルで有効にできます。これを有効にすると、次に示すように、[Device] > [Trunk] でSipトランクのステータスをモニタできます。

Name	Description	Calling Search Space	Device Pool	Route Pattern	Trunk Type	SIP Trunk Status	SIP Trunk Duration
CUCv11			Default	2000	SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

セキュア RTP コールの検証

鍵マークのアイコンが Unity Connection へのコールに表示されるかどうか検証します。これは、次の図に示すように、RTPストリームが暗号化されることを意味します (デバイスセキュリティプロファイルが機能するためにはセキュアである必要があります)



関連情報

- [SIP Integration Guide for Cisco Unity Connectionリリース11.x](#)