

次世代 暗号化 (NGE) に基づいて CUCM と CUC 間のセキュア SIP 統合のための設定例

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[ネットワーク図](#)

[証明書の要件](#)

[ネゴシエートされる RSA キーによって基づく暗号](#)

[ネゴシエートされる EC キーによって基づく暗号](#)

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

- [1. 新しいポート グループの追加](#)
- [2. TFTPサーバ参照を追加して下さい](#)
- [3. ボイス メール ポートの追加](#)
- [4. サードパーティ CA の CUCM ルートおよび中間物証明書をアップロードして下さい](#)

[設定- Cisco Unified CM \(CUCM \)](#)

- [1. SIP トランク セキュリティプロファイルを作成して下さい](#)
 - [2. セキュア SIP トランクを作成して下さい](#)
 - [3. TLS および SRTP 暗号を設定して下さい](#)
 - [4. CUC Tomcat 証明書をアップロードして下さい \(基づいて RSA 及び EC \)](#)
 - [5. ルートパターンを作成して下さい](#)
 - [6. 音声メールパイロットを、音声メールプロファイル作成し、DN にそれを割り当てて下さい](#)
- [設定- EC キーに署名することはサードパーティ CA \(オプションの \) によって証明書を基づかせていました](#)

[確認](#)

[SIP トランク 確認を保護して下さい](#)

[セキュア RTP コールの検証](#)

[関連情報](#)

概要

この資料は次世代 暗号化を使用して Cisco Unified 通信マネージャ (CUCM) および Cisco Unity Connection (CUC) サーバ間のセキュア SIP 接続の設定および確認を記述したものです。

SIP インターフェイス上の次世代のセキュリティは TLS 1.2、SHA-2 および AES256 基づいてスイート B 暗号を使用するために SIP インターフェイスをプロトコルに制限します。それは RSA または ECDSA 暗号の優先順位に基づいて暗号のさまざまな組み合わせを割り当てます。Unity Connection と Cisco Unified CM 間のコミュニケーションの間に、暗号およびサードパーティ証明書は両方両端に確認されます。次世代 暗号化サポートのための設定は下記にあります。

使用するために計画すればサードパーティ認証局 (CA) が署名する証明書はにコンフィギュレーションセクション (設定署名する証明書から-開始しま EC キーによって基づく証明書にサード

パーティ CA によって署名します) の終わり

前提条件

要件

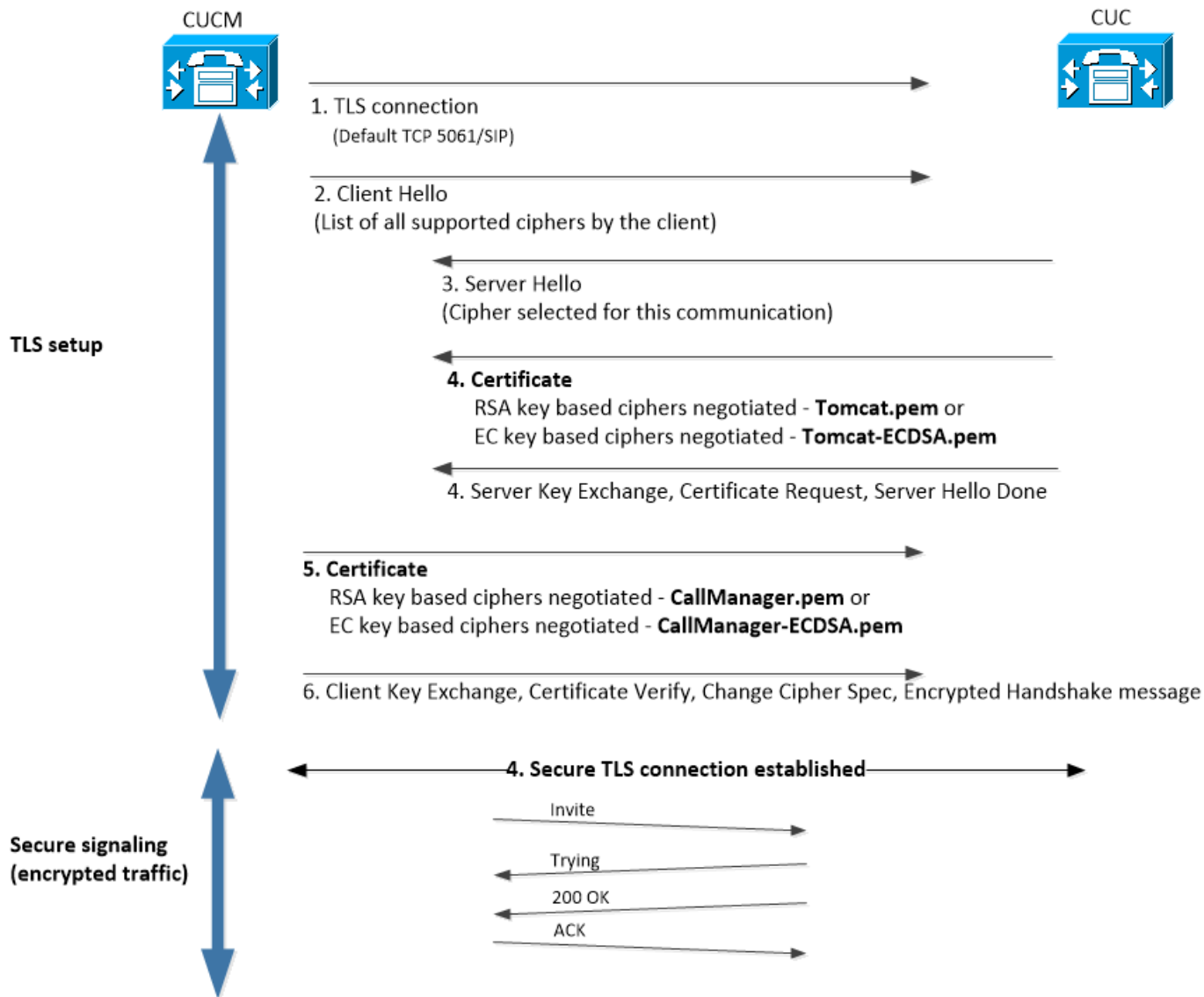
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

ミックス モードの CUCM バージョン 11.0 および それ 以降
CUC バージョン 11.0 および それ 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

ネットワーク図

このダイアグラムは簡潔に一度次世代 暗号化サポートが有効になることをヘルプが CUCM と CUC 間の信頼できる接続を確立することプロセスを説明します:



証明書の要件

これらは次世代 暗号化サポートが有効にされた on Cisco Unity Connection なら証明書交換要件です。

・ネゴシエートされる RSA キーによって基づく暗号

使用される CUCM 証明書	使用される CUC 証明書	CUCM にアップロードすべき証明書	CUC にアップロードすべき証明書
CallManager.pem (自己署名)	Tomcat.pem (自己署名)	にアップロードされるべき Tomcat.pem CUCM > CallManger 信頼	ありません。
CallManager.pem (署名する CA)	Tomcat.pem (署名する CA)	にアップロードされるべき CUC ルート及び中間物 CA 認証 *1 CUCM > CallManager 信頼	にアップロードされるべき CUCM ルート及び中間物 CA 認証 *2 CUC > CallManager 信頼
CallManager.pem (署名する CA)	Tomcat.pem (自己署名)	にアップロードされるべき Tomcat.pem CUCM > CallManger 信頼	にアップロードされるべき CUCM ルート及び中間物 CA 認証 CUC > CallManager 信頼
CallManager.pem (自己署名)	Tomcat.pem (署名する CA)	にアップロードされるべき CUC ルート及び中間物 CA 認証	ありません。

*1CUC ルート及び中間物 CA 認証は Unity 接続 Tomcat 証明書 (Tomcat.pem) に署名した CA 認証を示します。

*2CUCM ルート及び中間物 CA 認証は CUCM CallManager 証明書 (Callmanager.pem) に署名した CA 認証を示します。

・ネゴシエートされる EC キーによって基づく暗号

使用される CUCM 証明書	使用される CUC 証明書	CUCM にアップロードすべき証明書にアップロードされるべき	CUC にアップロードすべき証明書
CallManagerECDSA.pem (自己署名)	TomcatECDSA.pem (自己署名)	TomcatECDSA.pem CUCM > CallManger 信頼	ありません。
CallManagerECDSA.pem (署名する CA)	TomcatECDSA.pem (署名する CA)	にアップロードされるべき CUC ルート及び中間物 CA 認証 *1 CUCM > CallManager 信頼	にアップロードされるべき CUCM ルート及び中間物 CA 認証 *2 CUC > CallManager 信頼。
CallManagerECDSA.pem (署名する CA)	TomcatECDSA.pem (自己署名)	にアップロードされるべき TomcatECDSA.pem CUCM > CallManger 信頼。	にアップロードされるべき CUCM ルート及び中間物 CA 認証 CUC > CallManager 信頼。
CallManagerECDSA.pem (自己署名)	TomcatECDSA.pem (署名する CA)	にアップロードされるべき CUC ルート及び中間物 CA 認証 CUCM > CallManager 信頼	ありません。

*1 CUC ルート及び中間物 CA 認証は Unity 接続 EC によって基づいた Tomcat 証明書 (TomcatECDSA.pem) に署名した CA 認証を示します。

*2 CUCM ルート及び中間物 CA 認証は CUCM CallManager 証明書 (CallManagerECDSA.pem) に署名した CA 認証を示します。

1. 注: TomcatECDSA.pem 証明書は CUC の 11.0.1 バージョンの CallManagerECDSA.pem と呼ばれます。 CUC 11.5.x から証明書は TomcatECDSA.pem に名前を変更されました。

設定- Cisco Unity Connection (CUC)

1. [新しいポートグループの追加](#)

Cisco Unity Connection 管理 ページ > テレフォニー 統合 > ポートグループへのナビゲートはおよび『Add New』をクリックします。 イネーブル 次世代 暗号化チェックボックスをチェックすることを確かめて下さい。

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: Unity Connection の Cisco Tomcat 証明書は SSL ハンドシェイクの間にイネーブル 次世代 暗号化チェックボックスが有効に なれば使用されます。
 - ECDSA によって基づく暗号がそれからネゴシエートされれば EC キー基づいた TomcatECDSA 証明書は SSL ハンドシェイクで使用されます。
 - RSA によって基づく暗号がそれからネゴシエートされれば RSA キー基づいた Tomcat 証明書は SSL ハンドシェイクで使用されます。

2. TFTPサーバ参照を追加して下さい

ポートグループ 基本 ページで、> サーバは編集し、CUCM クラスタの TFTPサーバの FQDN を追加するためにナビゲートします。TFTPサーバの FQDN/ホスト名は CallManager 証明書の Common Name (CN) を一致する必要があります。サーバの IP アドレスははたらかないし、ITL ファイルをダウンロードするために失敗に終わります。DNS名は設定された DNSサーバによって解決可能である必要があります従って。

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

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

Cisco Unity Connection サービスビリティ > Tools > Service 管理へのナビゲートによって各ノードの接続メッセージ交換マネージャを再起動して下さい。これは設定が実施されることができるよう必須です。

- 注: Unity 接続はセキュア 6972 ポートの 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 (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv)。CUCM はミックス モードに CUC が ITL ファイルからの「CCM+TFTP」機能 証明書を探している必要があるためです。

テレフォニー 統合 > ポートグループ > ポートグループ 基本 設定 ページに戻ってナビゲートし、新たに追加されたポートグループをリセットして下さい。

Port Group	
Display Name*	PhoneSystem-1
Integration Method	SIP
Reset Status	Reset Required
	<input type="button" value="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度に、CUC サーバは CUCM サーバに接続によってローカルで保存された ITL ファイルをアップデートします。

3. [ボイス メール ポートの追加](#)

テレフォニー 統合 > ポートに戻ってナビゲートし、新しく作成されたポートグループにポートを追加するために『Add New』をクリックして下さい。

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 ルートおよび中間物証明書をアップロードして下さい

サードパーティ証明書の場合には、Unity Connection の CallManager 信頼のサードパーティ認証局（CA）のルートおよび中間物証明書をアップロードして下さい。これはサードパーティ CA が Call Manager 証明書に署名したときだけ必要とされます。このアクションを Cisco Unified OS 管理 > Security > Certificate Management へのナビゲートによって行い、証明書を『Upload』をクリックして下さい。

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を作成して下さい

CUCM Administration > システム > Security > SIP トランク セキュリティプロファイルにナビゲートし、新しいプロファイルを追加して下さい。X.509 サブジェクト名は CUC サーバの FQDN を一致する必要があります。

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 コマンドは「CERT が Tomcat/tomcat.pem」を所有するために Unity Connection の RSA キーによって基づく Tomcat 証明書を表示することができることを示します。それは CN CUCM で設定される X.509 サブジェクト名を一致する必要があります。CN はユニティサーバの FQDN/ホスト名と等しいです。EC キーによって基づく証明書は-認証対象代替名 (SAN) フィールドの... FQDN/hostname が含まれています。

2. セキュア SIP トランクを作成して下さい

デバイス > トランクに > クリックし、追加し、新しい作成します Unity Connection とセキュア統合のために使用される標準 SIP トランクをナビゲートして下さい。

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 暗号を設定して下さい

- 注: Unity Connection と Cisco Unified Communications Manager 間のネゴシエーションは次の状態の TLS 暗号設定によって決まります: Unity Connection がサーバとして機能するとき、TLS 暗号ネゴシエーションは Cisco Unified CM によって選択されるプリファレンスに基づいています。ECDSA によって基づく暗号がそれからネゴシエートされれば EC キーに基づいた TomcatECDSA 証明書は SSL ハンドシェイクで使用されます。RSA によって基づく暗号がそれからネゴシエートされれば RSA キーに基づいた Tomcat 証明書は SSL ハンドシェイクで使用されます。Unity Connection がクライアントとして機能するとき、TLS 暗号ネゴシエーションは Unity Connection によって選択されるプリファレンスに基づいています。

CM > システム > エンタープライズ パラメータは Cisco Unified にナビゲートし、ドロップダウン リストからの TLS および SRTP 暗号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

各ノードの Cisco Call Manager サービスを Cisco Unified サービスビリティ ページ、ツール > コントロール センター機能 サービスへのナビゲートによって再開し、CM サービスの下で『Cisco Call Manager』を選択して下さい

Cisco Unity Connection 管理 ページ > システム設定 > 一般的な設定にナビゲートし、ドロップダウン リストからの TLS および SRTP 暗号から適切な暗号オプションを選択して下さい。

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 サービスビリティ > Tools > Service 管理へのナビゲートによって各ノードの接続メッセージ交換マネージャを再起動して下さい。

TLS は優先順位のオプションを暗号化します

TLS 暗号オプション

最も強い AES-256 SHA-384 だけ: 好まれる RSA

Strongest-AES-256 SHA-384 だけ: 好まれる ECDSA

Medium-AES-256 AES-128 だけ: 好まれる RSA

優先順位の 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
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Medium-AES-256 AES-128 だけ: 好まれる ECDSA

好まれるすべての暗号 RSA (デフォルト)

好まれるすべての暗号 ECDSA

- 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
- 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_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 暗号オプション

SRTP 暗号オプション

すべては AES-256 を、AES-128 暗号サポートしました

AEAD AES-256、AES-128 GCM ベースの暗号

AEAD AES256 GCM ベースの暗号だけ

優先順位の SRTP

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_32
- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

4. アップロード CUC Tomcat 証明書 (基づいて RSA 及び EC)

OS 管理 > Security > Certificate Management にナビゲートし、CallManager 信頼ストアに両方の CUC Tomcat 証明書を (基づく RSA 及び EC) アップロードして下さい。

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: 両方の Unity Tomcat 証明書をアップロードすることは ECDSA 暗号がただネゴシエートされる場合必須ではありません。そのようなケース EC によって基づく Tomcat 証明書で十分はあります。

サードパーティ 証明書の場合には、サードパーティ 認証局 (CA) のルートおよび中間物証明書をアップロードして下さい。これはサードパーティ CA が Unity Tomcat 証明書に署名したときだけ必要とされます。

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

変更を加えるためにすべてのノードの Cisco Call Manager プロセスを再起動して下さい。

5. ルートパターンを作成して下さい

呼ルーティング > ルート/ハントする > ルートパターンへのナビゲートによる設定されたトランクへのポイント ルートパターンを設定して下さい。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*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence*

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain

Route Class*

Gateway/Route List*

Route Option

Route this pattern

Block this pattern

6. 音声メールパイロットを、音声メールプロファイル作成し、DN にそれを割り

当てて下さい

進んだ機能 > 音声メール > 音声メールパイロットへ行くことによって統合のための音声メールパイロットを作成して下さい。

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

すべての設定進んだ機能 > 音声メール > 音声メール プロファイルをリンクするために音声メールプロファイルを作成して下さい

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	

セキュア統合を使用するように呼ルーティング > ディレクトリ番号へ行くことによって意図されている DN に新しく作成された音声メール プロファイルを割り当てて下さい

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- EC キーに署名することはサードパーティ CA (オプションの) によって証明書を基づかせていました

証明書はシステム間のセキュア統合を設定する前のサードパーティ CA によって署名されるかもしれません。両方のシステムの証明書を署名するために次のステップに従って下さい。

Cisco Unity Connection

1. CUC TomcatECDSA のための証明書署名要求 (CSR) を生成し、証明書をサードパーティ CA によって署名してもらって下さい
2. CA はように続くアップロードする必要がある CA 認証 (CA ルート証明) をおよび ID証明 (CA 署名入り認証) 提供します:
Tomcat 信頼ストアに CA ルート証明をアップロードして下さい
Tomcat EDCA ストアに ID証明をアップロードして下さい
3. CUC のメッセージ交換マネージャを再起動して下さい

Cisco Unified CM

1. CUCM CallManagerECDSA のための CSR を生成し、証明書をサードパーティ CA によって署名してもらって下さい
2. CA はように続くアップロードする必要がある CA 認証 (CA ルート証明) をおよび ID証明 (CA 署名入り認証) 提供します:
CallManager 信頼ストアに CA ルート証明をアップロードして下さい
CallManager EDCS ストアに ID証明をアップロードして下さい
3. Cisco CCM を再起動し、各ノードのサービスを TFTP して下さい

同じプロセスが CSR が CUC Tomcat 証明書および CallManager 証明書のために生成され、Tomcat ストアおよびそれぞれ CallManager ストアにアップロードされる RSA キーによって基づいた証明書に署名するのに使用されます。

確認

ここでは、設定が正常に動作していることを確認します。

SIP トランク 確認を保護して下さい

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。これが有効になれば下記に示されているようにデバイス > トランクによって一ポートリンクステータスを監視できます:

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。それは RTP がこのイメージに示すようにストリーム (デバイスセキュリティ プロファイルははたらくためにそのためにセキュアである必要があります) 暗号化されることを意味します



関連情報

- [Cisco Unity Connection リリース 11.x のための SIP 統合ガイド](#)