

Konfigurationsbeispiel für die sichere SIP-Integration zwischen CUCM und CUC basierend auf NGE (Next Generation Encryption)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Netzwerkdiagramm](#)

[Zertifikatsanforderungen](#)

[Aushandlung von schlüsselbasierten RSA-Chiffren](#)

[Aushandlung von Schlüsselziffern mit EC](#)

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

[1. Neue Portgruppe hinzufügen](#)

[2. TFTP-Serverreferenz hinzufügen](#)

[3. Voicemail-Ports hinzufügen](#)

[4. CUCM-Root- und Zwischenzertifikat der Drittanbieter-CA hochladen](#)

[Konfiguration - Cisco Unified CM \(CUCM\)](#)

[1. Erstellen eines SIP-Trunk-Sicherheitsprofils](#)

[2. Erstellen eines sicheren SIP-Trunks](#)

[3. TLS- und SRTP-Chiffren konfigurieren](#)

[4. CUC Tomcat-Zertifikate hochladen \(RSA- und EC-basiert\)](#)

[5. Routenmuster erstellen](#)

[6. Voicemail-Pilot und Voicemail-Profil erstellen und den DNs zuweisen](#)

[Konfiguration - Signierung der auf EG-Schlüsseln basierenden Zertifikate durch Zertifizierungsstelle eines Drittanbieters \(optional\)](#)

[Überprüfen](#)

[Überprüfung sicherer SIP-Trunks](#)

[Überprüfung sicherer RTP-Anrufe](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration und Verifizierung der sicheren SIP-Verbindung zwischen dem Cisco Unified Communication Manager (CUCM)- und dem Cisco Unity Connection (CUC)-Server mithilfe von Verschlüsselungstechnologie der nächsten Generation.

Die Security over SIP-Schnittstelle der nächsten Generation schränkt die SIP-Schnittstelle auf die Verwendung von Suite-B-Chiffren ein, die auf den Protokollen TLS 1.2, SHA-2 und AES256 basieren. Es ermöglicht die verschiedenen Kombinationen von Chiffren, basierend auf der Prioritätsreihenfolge von RSA- oder ECDSA-Chiffren. Während der Kommunikation zwischen Unity Connection und Cisco Unified CM werden sowohl Verschlüsselungszertifikate als auch

Zertifikate von Drittanbietern an beiden Enden überprüft. Nachfolgend finden Sie die Konfiguration für die Unterstützung von Verschlüsselung der nächsten Generation.

Wenn Sie die von einer Zertifizierungsstelle signierten Zertifikate verwenden möchten, beginnen Sie mit der Signierung des Zertifikats am Ende des Konfigurationsabschnitts (Konfigurieren - Signieren der auf EG-Schlüsseln basierenden Zertifikate durch die Zertifizierungsstelle eines Drittanbieters).

Voraussetzungen

Anforderungen

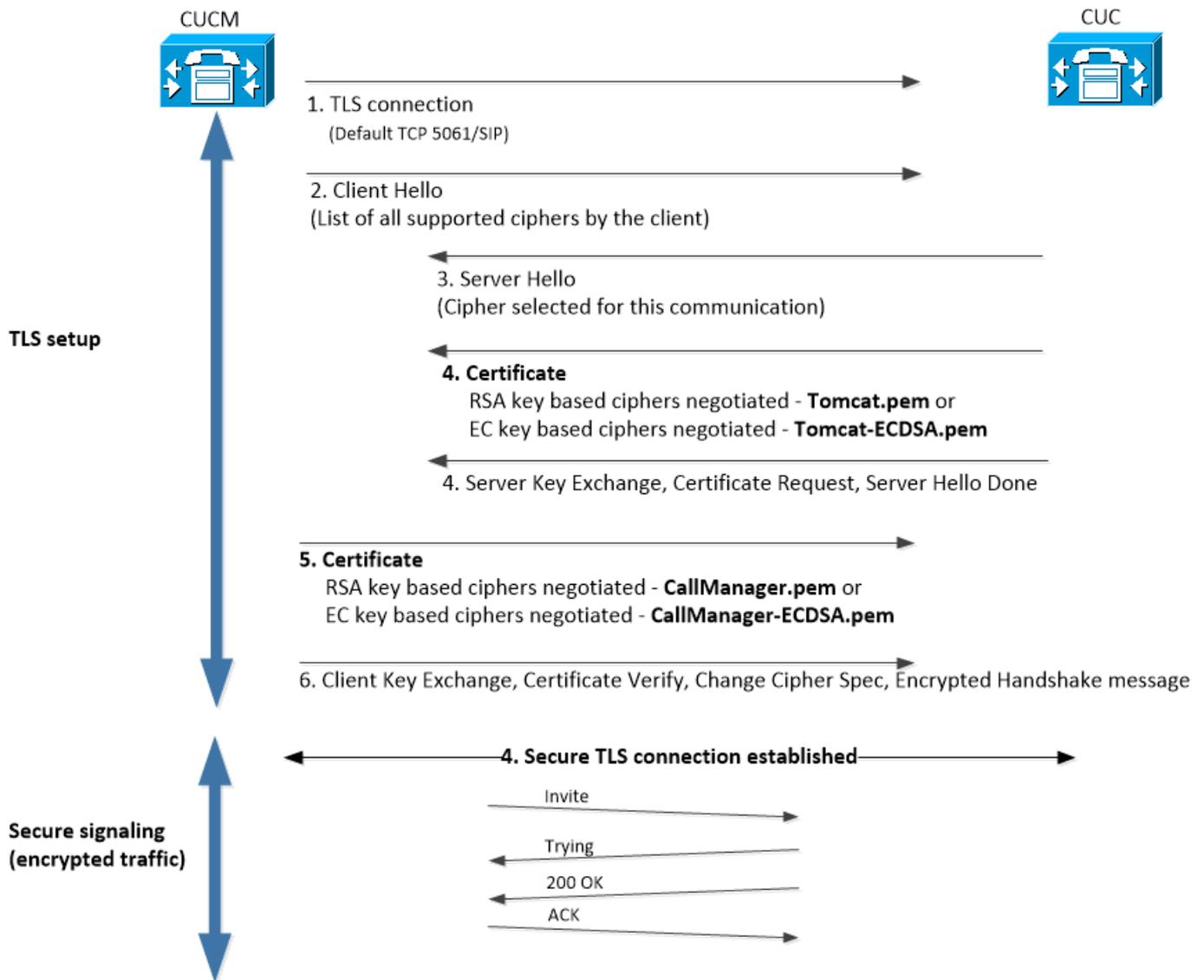
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

CUCM Version 11.0 und höher im gemischten Modus
CUC Version 11.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Diagramm wird kurz erläutert, wie eine sichere Verbindung zwischen CUCM und CUC hergestellt werden kann, wenn die Verschlüsselungsunterstützung der nächsten Generation aktiviert ist:



Zertifikatsanforderungen

Dies sind die Anforderungen für den Zertifikataustausch, sobald die Verschlüsselungsunterstützung der nächsten Generation für Cisco Unity Connection aktiviert ist.

• Aushandlung von schlüsselbasierten RSA-Chiffren

Verwendetes CUCM-Zertifikat	Verwendetes CUC-Zertifikat	Zertifikate für den Upload auf CUCM	Zertifizierungen für den Upload CUC
CallManager.pem (selbstsigniert)	Tomcat.pem (selbstsigniert)	Tomcat.pem zum Hochladen in CUCM > CallManager-trust	Keine.
CallManager.pem (CA-signiert)	Tomcat.pem (CA signiert)	CUC-Root- und Zwischenzertifikat *1 wird in CUCM hochgeladen > CallManager-Trust	CUCM-Root- und Zwischenzertifikat *2 werden in > CallManager-trust hochgeladen
CallManager.pem (CA-signiert)	Tomcat.pem (selbstsigniert)	Tomcat.pem zum Hochladen in CUCM > CallManager-trust	CUCM-Root- und Zwischenzertifikat, das in CUCM hochgeladen wird.
CallManager.pem	Tomcat.pem (CA signiert)	CUC-Root- und	Keine.

(selbstsigniert) signiert) Zwischenzertifikat, das in CUCM > CallManager-Trust hochgeladen wird

*1 CUC Root & Intermediate CA Zertifikat bezieht sich auf CA Zertifikat, das das Unity Connection Tomcat Zertifikat (Tomcat.pem) signiert hat.

*2 CUCM-Root- und Zwischenzertifikat bezieht sich auf Zertifizierungsstellenzertifikat, das das CUCM CallManager-Zertifikat signiert hat (Callmanager.pem).

• Aushandlung von Schlüsselziffern mit EC

Verwendetes CUCM-Zertifikat	Verwendetes CUC-Zertifikat	Zertifikate für den Upload auf CUCM	Zertifizierungen für den Upload in CUC
CallManager-ECDSA.pem (selbstsigniert)	Tomcat-ECDSA.pem (selbstsigniert)	Tomcat-ECDSA.pem wird in CUCM hochgeladen > CallManager-trust	Keine.
CallManager-ECDSA.pem (CA-signiert)	Tomcat-ECDSA.pem (CA-signiert)	CUC-Root- und Zwischenzertifikat *1 wird in CUCM hochgeladen > CallManager-Trust	CUCM-Root- und Zwischenzertifikat *2 werden in CUC > CallManager-trust hochgeladen.
CallManager-ECDSA.pem (CA-signiert)	Tomcat-ECDSA.pem (selbstsigniert)	Tomcat-ECDSA.pem wird in CUCM > CallManager-trust hochgeladen.	CUCM-Root- und Zwischenzertifikat, das in CUC > CallManager-Vertrauenswürdigkeit hochgeladen wird.
CallManager-ECDSA.pem (selbstsigniert)	Tomcat-ECDSA.pem (CA-signiert)	CUC-Root- und Zwischenzertifikat, das in CUCM > CallManager-Trust hochgeladen wird	Keine.

*1 CUC Root & Intermediate CA Zertifikat bezieht sich auf CA Zertifikat, das das Unity Connection EC-basierte Tomcat Zertifikat (Tomcat-ECDSA.pem) signiert hat.

*2 CUCM-Root- und Zwischenzertifikat bezieht sich auf Zertifizierungsstellenzertifikat, das das CUCM CallManager-Zertifikat signiert hat (CallManager-ECDSA.pem).

1. **Hinweis:** Das Zertifikat Tomcat-ECDSA.pem wird in CUC-Versionen 11.0.1 als CallManager-ECDSA.pem bezeichnet. Ab CUC 11.5.x wurde das Zertifikat in Tomcat-ECDSA.pem umbenannt.

Konfigurieren - Cisco Unity Connection (CUC)

1. Neue Portgruppe hinzufügen

Navigieren Sie zu Cisco Unity Connection Administration page > Telephony integration > Port group, und klicken Sie auf Add New (Neu hinzufügen). Aktivieren Sie das Kontrollkästchen

Verschlüsselung der nächsten Generation aktivieren.

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. **Hinweis:** Das Cisco Tomcat-Zertifikat von Unity Connection wird beim SSL-Handshake verwendet, sobald das Kontrollkästchen Verschlüsselung der nächsten Generation aktivieren aktiviert ist.
 - Falls ECDSA-basierte Verschlüsselung ausgehandelt wird, wird das auf dem EG-Schlüssel basierende tomcat-ECDSA-Zertifikat in SSL-Handshake verwendet.
 - Falls eine RSA-basierte Verschlüsselung ausgehandelt wird, wird ein auf RSA-Schlüsseln basierendes Tomcat-Zertifikat im SSL-Handshake verwendet.

2. TFTP-Serverreferenz hinzufügen

Navigieren Sie auf der Seite "Port Group Basics" (Grundlagen der Portgruppe) zu Bearbeiten > Server, und fügen Sie den FQDN des TFTP-Servers des CUCM-Clusters hinzu. FQDN/Hostname des TFTP-Servers muss mit dem Common Name (CN) des CallManager-Zertifikats übereinstimmen. Die IP-Adresse des Servers funktioniert nicht und führt dazu, dass die ITL-Datei nicht heruntergeladen wird. Der DNS-Name muss daher über einen konfigurierten DNS-Server auflösbar sein.

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

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

Starten Sie Connection Conversation Manager für jeden Knoten neu, indem Sie zu Cisco Unity Connection Serviceability > Tools > Service Management navigieren. Dies ist obligatorisch, damit die Konfiguration wirksam wird.

1. **Hinweis:** Unity Connection lädt die ITL-Datei (ITLfile.tlv) mithilfe des HTTPS-Protokolls vom CUCM auf einem sicheren 6972-Port herunter (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM muss sich im gemischten Modus befinden, da CUC das Funktionszertifikat "CCM+TFTP" aus der ITL-Datei benötigt.

Navigieren Sie zurück zur Konfigurationsseite Telefonieintegration > Portgruppe > Portgruppen-Grundlagen, und setzen Sie die neu hinzugefügte Portgruppe zurück.

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

1. **Hinweis:** Bei jedem Zurücksetzen der Portgruppe aktualisiert der CUC-Server seine lokal gespeicherte ITL-Datei, indem er eine Verbindung zum CUCM-Server herstellt.

3. Voicemail-Ports hinzufügen

Navigieren Sie zurück zu Telefonieintegration > Port, und klicken Sie auf Add new, um der neu erstellten Portgruppe Port hinzuzufügen.

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. CUCM-Root- und Zwischenzertifikat der Drittanbieter-CA hochladen

Im Fall von Zertifikaten von Drittanbietern müssen Sie das Root- und Zwischenzertifikat der Drittanbieter-Zertifizierungsstelle in CallManager-Vertrauenswürdigkeit von Unity Connection hochladen. Dies ist nur erforderlich, wenn eine Zertifizierungsstelle eines Drittanbieters Ihr Call Manager-Zertifikat signiert. Navigieren Sie dazu zu Cisco Unified OS Administration > Security > Certificate Management, und klicken Sie auf Upload Certificate.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

Konfiguration - Cisco Unified CM (CUCM)

1. Erstellen eines SIP-Trunk-Sicherheitsprofils

Navigieren Sie zu CUCM Administration > System > Security > SIP Trunk Security Profile, und fügen Sie ein neues Profil hinzu. Der X.509-Betreffname muss mit dem FQDN des CUC-Servers übereinstimmen.

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

- Hinweis:** Der CLI-Befehl "show cert own tomcat/tomcat.pem" kann das auf dem RSA-Schlüssel basierende Tomcat-Zertifikat für Unity Connection anzeigen. Die CN muss mit dem für CUCM konfigurierten X.509-Betreffnamen übereinstimmen. Der CN entspricht dem FQDN/Hostnamen des Unity-Servers. Das auf EG-Schlüsseln basierende Zertifikat enthält den FQDN/Hostnamen in seinem Feld "Subject Alternate Name (SAN)".

2. Erstellen eines sicheren SIP-Trunks

Navigieren Sie zu Gerät > Trunk > Klicken Sie auf "Neu hinzufügen", und erstellen Sie einen standardmäßigen SIP-Trunk, der für die sichere Integration in Unity Connection verwendet wird.

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- und SRTP-Chiffren konfigurieren

1. **Hinweis:** Die Aushandlung zwischen Unity Connection und Cisco Unified Communications Manager hängt von der TLS-Verschlüsselungskonfiguration mit den folgenden Bedingungen ab: Wenn Unity Connection als Server fungiert, basiert die Verhandlung der TLS-Verschlüsselung auf den von Cisco Unified CM ausgewählten Präferenzen. Falls ECDSA-basierte Verschlüsselung ausgehandelt wird, werden auf dem EG-Schlüssel basierende ECDSA-Zertifikate in SSL-Handshake verwendet. Wenn RSA-basierte Verschlüsselung ausgehandelt wird, werden RSA-Schlüssel-basierte Tomcat-Zertifikate im SSL-Handshake verwendet. Wenn Unity Connection als Client fungiert, basiert die TLS-Verschlüsselung auf

der von Unity Connection ausgewählten Präferenz.

Navigieren Sie zu Cisco Unified CM > Systems > Enterprise Parameters, und wählen Sie die entsprechende Verschlüsselungsoption aus der Dropdown-Liste TLS und SRTP Ciphers aus.

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

Starten Sie den Cisco Call Manager-Service für jeden Knoten neu. Rufen Sie dazu die Seite Cisco Unified Services, Extras > Control Center-Feature-Services auf, und wählen Sie Cisco Call Manager unter CM Services aus.

Navigieren Sie zu Cisco Unity Connection Administration page > System Settings > General Configurations, und wählen Sie in der Dropdown-Liste TLS und SRTP Ciphers die entsprechende Verschlüsselungsoption aus.

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

Starten Sie Connection Conversation Manager für jeden Knoten neu, indem Sie zu Cisco Unity Connection Serviceability > Tools > Service Management navigieren.

TLS-Cipher-Optionen mit Prioritätsreihenfolge

TLS-Cipher-Optionen

Strongest- Nur AES-256 SHA-384: RSA Preferred

Nur am stärksten AES-256 SHA-384: ECDSA
Bevorzugt

TLS-Ciphers in Prioritätsreihenfolge

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_S

Nur Medium-AES-256 AES-128: RSA Preferred

- 4
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 6
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Nur Medium-AES-256 AES-128: ECDSA Bevorzugt

- 4
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 6
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Alle Ciphers RSA Preferred (Standard)

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 6
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Alle Ciphers ECDSA Preferred

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 6
- TLS_RSA_WITH_AES_128_CBC_SHA

SRTP Cipher-Optionen in Prioritätsreihenfolge

SRTP Cipher-Option

SRTP in Prioritätsreihenfolge

Alle unterstützten AES-256-, AES-128-Chiffren

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_32

AEAD AES-256, AES-28 GCM-basierte Chiffren

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Nur auf AEAD AES256 GCM basierende Chiffren

4. CUC Tomcat-Zertifikate hochladen (RSA- und EC-basiert)

Navigieren Sie zu OS Administration > Security > Certificate Management, und laden Sie beide CUC Tomcat-Zertifikate (RSA- und EC-basiert) in den CallManager-Trust-Store hoch.

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. **Hinweis:** Das Hochladen beider Unity Tomcat-Zertifikate ist nicht obligatorisch, wenn nur ECDSA-Verschlüsselungen ausgehandelt werden. In diesem Fall genügt ein EG-basiertes Tomcat-Zertifikat.

Im Falle von Zertifikaten von Drittanbietern müssen Sie das Root- und Zwischenzertifikat der Zertifizierungsstelle eines Drittanbieters hochladen. Dies ist nur erforderlich, wenn eine Zertifizierungsstelle eines Drittanbieters Ihr Unity Tomcat-Zertifikat signiert.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

Starten Sie den Cisco Call Manager-Prozess für alle Knoten neu, um die Änderungen anzuwenden.

5. Routenmuster erstellen

Konfigurieren Sie ein Routenmuster, das auf den konfigurierten Trunk zeigt, indem Sie zu Call Routing > Route/Hunt > Route Pattern navigieren. Die als Weiterleitungsmuster-Nummer eingegebene Durchwahl kann als Voicemail-Pilot verwendet werden.

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. Voicemail-Pilot und Voicemail-Profil erstellen und den DNs zuweisen

Erstellen Sie ein Voicemail-Pilotprogramm für die Integration, indem Sie zu Erweiterte Funktionen > Voicemail > Voicemail Pilot wechseln.

Voice Mail Pilot Information

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

Erstellen Sie ein Voicemail-Profil, um alle Einstellungen mit Advanced Features (Erweiterte Funktionen) > Voicemail (Voicemail) > Voicemail Profile (Voicemail-Profil) zu verknüpfen.

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	

Weisen Sie das neu erstellte Voicemail-Profil den DNs zu, die die sichere Integration verwenden möchten. Gehen Sie dazu zu Call Routing > Directory number (Anrufweiterleitung > Verzeichnisnummer).

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 >	

Konfiguration - Signierung der auf EG-Schlüsseln basierenden Zertifikate durch Zertifizierungsstelle eines Drittanbieters (optional)

Die Zertifikate können von einer Zertifizierungsstelle eines Drittanbieters signiert werden, bevor die sichere Integration zwischen den Systemen eingerichtet wird. Führen Sie die folgenden Schritte aus, um die Zertifikate auf beiden Systemen zu signieren.

Cisco Unity Connection

1. Erstellen Sie eine CSR-Anfrage (Certificate Signing Request) für CUC Tomcat-ECDSA, und lassen Sie das Zertifikat von einer Zertifizierungsstelle eines Drittanbieters unterzeichnen.
2. CA stellt Identitätszertifikat (CA-signiertes Zertifikat) und Zertifizierungsstellenzertifikat (CA-Root-Zertifikat) bereit, die wie folgt hochgeladen werden müssen:
Hochladen des CA-Stammzertifikats in den tomcat-trust-Speicher
Identitätszertifikat in den tomcat-EDCS Store hochladen
3. Call Conversation Manager auf CUC neu starten

Cisco Unified CM

1. Erstellen Sie CSR für CUCM CallManager-ECDSA, und lassen Sie das Zertifikat von einer Zertifizierungsstelle eines Drittanbieters unterzeichnen.
2. CA stellt Identitätszertifikat (CA-signiertes Zertifikat) und Zertifizierungsstellenzertifikat (CA-Root-Zertifikat) bereit, die wie folgt hochgeladen werden müssen:
Hochladen des CA-Stammzertifikats in den CallManager-Trust-Store
Identitätszertifikat in den Call Manager-EDCS Store hochladen
3. Neustarten der Cisco CCM- und TFTP-Services auf jedem Knoten

Derselbe Prozess wird zum Signieren von RSA-Schlüssellängen verwendet, bei denen CSR für das CUC Tomcat-Zertifikat und das CallManager-Zertifikat generiert und in den Tomcat-Speicher bzw. Callmanager-Speicher hochgeladen wird.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfung sicherer SIP-Trunks

Drücken Sie die Voicemail-Taste am Telefon, um die Voicemail-Nachricht anzurufen. Sie sollten die Begrüßung hören, wenn die Durchwahl des Benutzers nicht auf dem Unity Connection-System konfiguriert ist.

Alternativ können Sie die Keepalive-Funktion von SIP OPTIONS aktivieren, um den SIP-Trunk-Status zu überwachen. Diese Option kann im SIP-Profil aktiviert werden, das dem SIP-Trunk zugewiesen ist. Wenn diese Funktion aktiviert ist, können Sie den SIP-Trunk-Status über Gerät > Trunk überwachen, wie unten gezeigt:

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

Überprüfung sicherer RTP-Anrufe

Überprüfen Sie, ob das Schlosssymbol bei Anrufen von Unity Connection vorhanden ist. Dies bedeutet, dass der RTP-Stream verschlüsselt ist (das Gerätesicherheitsprofil muss sicher sein, damit es funktioniert), wie in diesem Bild gezeigt.



Zugehörige Informationen

- [SIP-Integrationsanleitung für Cisco Unity Connection Version 11.x](#)