Cisco IP-Konferenztelefon – Sicherheit

Übersicht der Sicherheit des Cisco IP Phone

Die Sicherheitsfunktionen schützen vor mehreren Gefahren, beispielsweise der Gefährdung der Identität des Telefons und der Daten. Diese Funktionen erstellen und halten authentifizierte Kommunikationsstreams zwischen dem Telefon und dem Cisco Unified Communications Manager-Server aufrecht, und stellen sicher, dass das Telefon nur digital signierte Dateien verwendet.

In Cisco Unified Communications Manager Version 8.5(1) und höheren Versionen ist Security by Default implementiert. Diese Komponente stellt die folgenden Sicherheitsfunktionen für Cisco IP-Telefons ohne CTL-Client bereit:

- Signierung der Konfigurationsdateien für das Telefon
- Verschlüsselung der Telefonkonfigurationsdatei
- HTTPS mit Tomcat und andere Webservices

Hinweis Für sichere Signalübertragungs- und Medienfunktionen muss der CTL-Client jedoch weiterhin ausgeführt werden, und es ist weiterhin die Verwendung von Hardware-eToken erforderlich.

Weitere Informationen zu den Sicherheitsfunktionen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachdem Sie die für die CAPF (Certificate Authority Proxy Function) erforderlichen Aufgaben ausgeführt haben, wird auf den Telefonen ein LSC (Locally Significant Certificate) installiert. Sie können ein LSC in der Cisco Unified Communications Manager Administration-Verwaltung konfigurieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Ein LSC kann für EAP-TLS mit WLAN-Authentifizierung nicht als Benutzerzertifikat verwendet werden.

Alternativ dazu können Sie die Installation eines LSC auch im Menü „Sicherheits-Setup“ des Telefons veranlassen. In diesem Menü können Sie ein LSC auch aktualisieren und entfernen.

Das Cisco IP-Konferenztelefon 7832 entspricht dem FIPS (Federal Information Processing Standard). Um ordnungsgemäß zu funktionieren, ist für den FIPS-Modus eine RSA-Schlüssellänge von mindestens 2048 Bit erforderlich. Wenn das RSA-Serverzertifikat nicht 2048 Bit oder mehr umfasst, wird das Telefon nicht beim Cisco Unified Communications Manager registriert und die Meldung `Telefon konnte nicht registriert werden erscheint. Die Größe des Zertifikatsschlüssels ist nicht FIPS-konform.` wird auf dem Telefon angezeigt.

Sie können im FIPS-Modus keine privaten Schlüssel (LSC oder MIC) verwenden.

Wenn das Telefon über ein vorhandenen LSC mit weniger als 2.048 Bits verfügt, müssen Sie die LSC-Schlüssellänge auf 2048 Bit oder mehr aktualisieren, bevor Sie FIPS aktivieren.

Verwandte Themen

Einrichten eines LSC (Locally Significant Certificate), auf Seite 11
Dokumentation Cisco Unified Communications Manager

Sicherheitsverbesserungen für Ihr Telefonnetzwerk

Sie können Cisco Unified Communications Manager 11.5(1) und 12.0(1) ermöglichen, in einer Umgebung mit verbesserter Sicherheit zu arbeiten. Mit diesen Verbesserungen wird Ihr Telefonnetzwerk unter Anwendung einer Reihe von strengen Sicherheits- und Risikomanagementkontrollen betrieben, um Sie und die Benutzer zu schützen.

Cisco Unified Communications Manager 12.5 (1) unterstützt keine Umgebung mit verbesserter Sicherheit. Deaktivieren Sie FIPS, bevor Sie ein Upgrade auf Cisco Unified Communications Manager 12.5(1) vornehmen oder Ihr TFTP-Dienst wird nicht ordnungsgemäß funktionieren.

Die Umgebung mit verbesserter Sicherheit bietet die folgenden Funktionen:

- Kontaktsuchen-Authentifizierung
- TCP als Standardprotokoll für Remote-Audit-Protokolle
- FIPS-Modus
- Verbesserte Richtlinie für Anmeldeinformationen
- Unterstützung für die SHA-2-Hash-Familie für digitale Signaturen
- Unterstützung für eine RSA-Schlüsselgröße von 512 und 4096 Bits.

Mit Cisco Unified Communications Manager Version 14.0 und Cisco IP-Telefon-Firmware Version 14.0 und höher unterstützen die Telefone die SIP-OAuth-Authentifizierung.

OAuth wird für Proxy Trivial File Transfer Protocol (TFTP) mit Cisco Unified Communications ManagerVersion 14.0 (1) SU1 oder höher und Cisco IP-Telefon-Firmware Version 14.1 (1) unterstützt. Proxy-TFTP und OAuth für Proxy-TFTP werden für Mobile Remote Access (MRA) nicht unterstützt.

Weitere Informationen zur Sicherheit finden Sie unter:

- *Systemkonfigurationshandbuch für Cisco Unified Communications Manager*, Version 14.0(1) oder höher (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

- *Sicherheitshandbuch für Cisco Unified Communications Manager*(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)

Hinweis Ihr Cisco IP-Telefon kann nur eine begrenzte Anzahl an Identity Trust List(ITL-)Dateien speichern. ITL-Dateien dürfen die Begrenzung von 64000 nicht überschreiten. Begrenzen Sie daher die Anzahl an Dateien, die Cisco Unified Communications Manager an das Telefon senden kann.

Unterstützte Sicherheitsfunktionen

Die Sicherheitsfunktionen schützen vor mehreren Gefahren, beispielsweise der Gefährdung der Identität des Telefons und der Daten. Diese Funktionen erstellen und halten authentifizierte Kommunikationsstreams zwischen dem Telefon und dem Cisco Unified Communications Manager-Server aufrecht, und stellen sicher, dass das Telefon nur digital signierte Dateien verwendet.

In Cisco Unified Communications Manager Version 8.5(1) und höheren Versionen ist Security by Default implementiert. Diese Komponente stellt die folgenden Sicherheitsfunktionen für Cisco IP-Telefons ohne CTL-Client bereit:

- Signierung der Konfigurationsdateien für das Telefon
- Verschlüsselung der Telefonkonfigurationsdatei
- HTTPS mit Tomcat und andere Webservices

Hinweis Für sichere Signalübertragungs- und Medienfunktionen muss der CTL-Client jedoch weiterhin ausgeführt werden, und es ist weiterhin die Verwendung von Hardware-eToken erforderlich.

Die Implementierung von Sicherheitsfunktionen in das Cisco Unified Communications Manager-System verhindert den Identitätsdiebstahl hinsichtlich Telefon und Cisco Unified Communications Manager-Server und schützt vor unbefugtem Zugriff auf Daten, Anrufsignale und Medien-Datenströme.

Zur Abwehr von Bedrohungen dieser Art erstellt das Cisco IP-Telefonienetzwerk zwischen Telefon und Server sichere (verschlüsselte) Kommunikationsdatenströme und erhält diese aufrecht, signiert Dateien digital, bevor diese auf ein Telefon übertragen werden, und verschlüsselt alle Mediendatenströme und Signale, die zwischen Cisco IP-Telefons übertragen werden.

Nachdem Sie die für die CAPF (Certificate Authority Proxy Function) erforderlichen Aufgaben ausgeführt haben, wird auf den Telefonen ein LSC (Locally Significant Certificate) installiert. Zum Konfigurieren eines LSC können Sie die Cisco Unified Communications Manager-Verwaltung verwenden. Die Vorgehensweise hierfür ist im Sicherheitshandbuch für Cisco Unified Communications Manager beschrieben. Alternativ dazu können Sie die Installation eines LSC auch im Menü „Sicherheits-Setup“ des Telefons veranlassen. In diesem Menü können Sie ein LSC auch aktualisieren und entfernen.

Ein LSC kann für EAP-TLS mit WLAN-Authentifizierung nicht als Benutzerzertifikat verwendet werden.

Im Telefonsicherheitsprofil ist definiert, ob das Gerät sicher oder nicht sicher ist. Weitere Informationen zum Anwenden des Sicherheitsprofils auf das Telefon finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Wenn Sie in der Cisco Unified Communications Manager-Verwaltung sicherheitsrelevante Einstellungen konfigurieren, sind in der Telefonkonfigurationsdatei auch vertrauliche Informationen enthalten. Damit die Konfigurationsdatei entsprechend ihrer Vertraulichkeit geschützt ist, müssen Sie die Datei so konfigurieren, dass eine Verschlüsselung erfolgt. Ausführliche Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Die Implementierung von Sicherheitsfunktionen in das Cisco Unified Communications Manager-System verhindert den Identitätsdiebstahl hinsichtlich Telefon und Cisco Unified Communications Manager-Server und schützt vor unbefugtem Zugriff auf Daten, Anrufsignale und Medien-Datenströme.

Die folgende Tabelle enthält eine Übersicht der Sicherheitsfunktionen, die von Cisco IP-Konferenztelefon 7832 unterstützt werden. Weitere Informationen zu diesen Funktionen und zur Sicherheit von Cisco Unified Communications Manager und Cisco IP-Telefon finden Sie in der Dokumentation zu Ihrer Version von Cisco Unified Communications Manager.

Tabelle 1: Überblick der Sicherheitsfunktionen

Funktion	Beschreibung
Imageauthentifizierung	Signierte Binärdateien (mit der Erweiterung SBN) verhindern Wenn das Image manipuliert wurde, kann das Telefon nicht au
Installation des Zertifikats am Kundenstandort	Für jedes Telefon ist zur Geräteauthentifizierung ein eindeutig Installed Certificate), aber für zusätzliche Sicherheit können S ein Zertifikat über die CAPF (Certificate Authority Proxy Functi auch über das Menü Sicherheitskonfiguration auf dem Telefon
Geräteauthentifizierung	Die Geräteauthentifizierung erfolgt zwischen dem Cisco Unifi Zertifikat der anderen Entität akzeptiert. Bestimmt, ob eine sic Manager hergestellt wird, und erstellt, falls erforderlich, mit d Unified Communications Manager registriert Telefone nur, we können.
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon herunterlä nachdem sie erstellt wurde, nicht manipuliert wurde. Dateien, d dem Telefon geschrieben. Das Telefon weist diese Dateien ohn
Signalisierungsauthentifizierung	Verwendet das TLS-Protokoll, um sicherzustellen, dass die Sig
MIC (Manufacturing Installed Certificate)	Auf jedem Telefon ist ein eindeutiges, vom Hersteller installie die Geräteauthentifizierung verwendet wird. Das MIC ist ein p Communications Manager, das Telefon zu authentifizieren.
Sichere SRST-Referenz	Nachdem Sie eine SRST-Referenz für die Sicherheit konfiguri Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Serv Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung
Medienverschlüsselung	Verwendet SRTP, um sicherzustellen, dass die Medienstreams vorgesehenen Geräten empfangen und gelesen werden können. an die Geräte und schützt die Schlüssel, während diese übertra

Funktion	Beschreibung
CAPF (Certificate Authority Proxy Function)	Implementiert Teile des Prozesses für die Zertifikatsgeneri Telefon bei der Schlüsselgenerierung und Zertifikatsinstalla kundenspezifischen Zertifizierungsstellen anzufordern ode
Sicherheitsprofile	Definiert, ob das Telefon nicht sicher, authentifiziert oder v
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfiguratio
Die Webserverfunktionalität für ein Telefon deaktivieren	Sie können den Zugriff auf eine Telefon-Webseite verhinde
Telefonhärtung	Weitere Sicherheitsoptionen, die in der Cisco Unified Com • Zugriff auf die Webseiten für ein Telefon deaktivieren **Hinweis** Sie können die aktuellen Einstellungen für die Telefonkonfigurationsmenü anzeigen.
802.1X-Authentifizierung	Das Telefon kann die 802.1X-Authentifizierung verwende
AES 256-Verschlüsselung	Telefone, die mit Cisco Unified Communications Manager V für TLS und SIP für die Signalisierung und Medienverschl Schlüsseln, die mit SHA-2 (Secure Hash Algorithm) und F unterstützen. Die neuen Schlüssel: • Für TLS-Verbindungen: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • Für sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Weitere Informationen finden Sie in der Dokumentation zu
Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate	Als Teil der Common Criteria(CC-)Zertifizierung hat Cisco Dies betrifft alle VOS-Produkte (Voice Operating System)

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Anrufsicherheit

Wenn die Sicherheit für ein Telefon implementiert wird, können sichere Anrufe auf dem Telefondisplay mit Symbolen gekennzeichnet werden. Sie können auch bestimmen, ob das verbundene Telefon sicher und geschützt ist, wenn zu Beginn des Anrufs ein Sicherheitssignal ausgegeben wird.

In einem sicheren Anruf sind alle Anrufsignale und Medienstreams verschlüsselt. Ein sicherer Anruf bietet eine hohe Sicherheitsstufe und stellt die Integrität und den Datenschutz des Anrufs sicher. Wenn ein aktiver

Anruf verschlüsselt wird, ändert sich das Anrufstatus-Symbol rechts neben der Anrufdauer in das folgende Symbol: .

Hinweis Wenn der Anruf über nicht-IP-Anrufabschnitte, beispielsweise ein Festnetz, geleitet wird, ist der Anruf möglicherweise nicht sicher, auch wenn er im IP-Netzwerk verschlüsselt wurde und ein Schloss-Symbol angezeigt wird.

Zu Beginn eines sicheren Anrufs wird ein Sicherheitssignal ausgegeben, das angibt, dass das andere verbundene Telefon ebenfalls sicheres Audio empfangen und senden kann. Wenn Sie mit einem nicht sicheren Telefon verbunden sind, wird kein Sicherheitssignal ausgegeben.

Hinweis Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Sichere Konferenzen, Cisco Extension Mobility und gemeinsam genutzte Leitungen können über eine sichere Konferenzbrücke konfiguriert werden.

Wenn ein Telefon in Cisco Unified Communications Manager als sicher (verschlüsselt und vertrauenswürdig) konfiguriert wird, kann es den Status „Geschützt“ erhalten. Anschließend kann das geschützte Telefon so konfiguriert werden, dass es zu Beginn eines Anrufs einen Signalton ausgibt.

- Geschütztes Gerät: Um den Status eines sicheren Telefons in „Geschützt“ zu ändern, aktivieren Sie das Kontrollkästchen „Geschütztes Gerät“ im Fenster „Telefonkonfiguration“ in Cisco Unified Communications Manager Administration (**Gerät** > **Telefon**).
- Sicherheitssignal ausgeben: Damit das geschützte Telefon ein Signal ausgibt, das angibt, ob der Anruf sicher oder nicht sicher ist, legen Sie die Einstellung Sicherheitssignal ausgeben auf True fest. Die Einstellung Sicherheitssignal ausgeben ist standardmäßig auf False festgelegt. Sie legen diese Option in der Cisco Unified Communications Manager-Verwaltung fest (**System** > **Serviceparameter**). Wählen Sie den Server und anschließend den Unified Communications Manager-Service aus. Wählen Sie im Fenster Serviceparameterkonfiguration die Option unter Funktion - Sicherheitssignal aus. Der Standardwert ist False.

Sichere Konferenzanruf-ID

Sie können einen sicheren Konferenzanruf initiieren und die Sicherheitsstufe der Teilnehmer überwachen. Ein sicherer Konferenzanruf wird mit diesem Prozess initiiert:

1. Ein Benutzer startet die Konferenz auf einem sicheren Telefon.
2. Cisco Unified Communications Manager weist dem Anruf eine sichere Konferenzbrücke zu.
3. Während Teilnehmer hinzugefügt werden, überprüft Cisco Unified Communications Manager den Sicherheitsmodus aller Telefone und hält die Sicherheitsstufe für die Konferenz aufrecht.
4. Das Telefon zeigt die Sicherheitsstufe des Konferenzanrufs an. Eine sichere Konferenz zeigt das Sicherheitssymbol rechts neben **Konferenz** auf dem Telefon an.

Hinweis Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Für geschützte Telefone sind einige Funktionen, beispielsweise Konferenzanrufe, gemeinsam genutzte Leitungen und die Anschlussmobilität, nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

Die folgende Tabelle enthält Informationen zu den Änderungen der Konferenzsicherheitsstufe, abhängig von der Sicherheitsstufe des Telefons des Initiators und der Verfügbarkeit von sicheren Konferenzbrücken.

Tabelle 2: Sicherheitseinschränkungen für Konferenzanrufe

Sicherheitsstufe des Telefons des Initiators	Verwendete Funktion	Sicherheitsstufe der Teilnehmer	Ergebnisse der Aktion
Nicht sicher	Konferenz	Sicher	Nicht sichere Konferenzbrücke Nicht sichere Konferenz
Sicher	Konferenz	Mindestens ein Mitglied ist nicht sicher.	Sichere Konferenzbrücke Nicht sichere Konferenz
Sicher	Konferenz	Sicher	Sichere Konferenzbrücke Verschlüsselungsstufe der sicheren Konfer
Nicht sicher	MeetMe	Die minimale Sicherheitsstufe ist verschlüsselt.	Der Initiator erhält die Meldung `Sicherh nicht erfüllt, Anruf abgeleh`
Sicher	MeetMe	Die minimale Sicherheitsstufe ist nicht sicher.	Sichere Konferenzbrücke Die Konferenz nimmt alle Anrufe an.

Sichere Anruf-ID

Ein sicherer Anruf wird initiiert, wenn Ihr Telefon und das Telefon des anderen Teilnehmers für sichere Anrufe konfiguriert ist. Das andere Telefon kann sich im gleichen Cisco IP-Netzwerk oder in einem Netzwerk außerhalb des IP-Netzwerks befinden. Sichere Anrufe sind nur zwischen zwei Telefonen möglich. Konferenzanrufe sollten sichere Anrufe unterstützen, nachdem eine sichere Konferenzbrücke konfiguriert wurde.

Ein sicherer Anruf wird mit diesem Prozess initiiert:

1. Der Benutzer initiiert einen Anruf auf einem geschützten Telefon (Sicherheitsmodus).
2. Das Telefon zeigt das Sicherheitssymbol auf dem Telefondisplay an. Dieses Symbol zeigt an, dass das Telefon für sichere Anrufe konfiguriert ist. Dies bedeutet jedoch nicht, dass das andere verbundene Telefon ebenfalls geschützt ist.
3. Der Benutzer hört einen Signalton, wenn der Anruf mit einem anderen sicheren Telefon verbunden wird, der angibt, dass beide Enden der Konversation verschlüsselt und geschützt sind. Wenn der Anruf mit einem nicht sicheren Telefon verbunden wird, hört der Benutzer keinen Signalton.

Hinweis Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Für geschützte Telefone sind einige Funktionen, beispielsweise Konferenzanrufe, gemeinsam genutzte Leitungen und die Anschlussmobilität, nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

Ein Sicherheitssignal wird nur auf einem geschützten Telefon ausgegeben. Auf einem nicht geschützten Telefon wird kein Signalton ausgegeben. Wenn sich der Gesamtstatus des Anrufs während des Anrufs ändert, gibt das geschützte Telefon den geänderten Signalton wieder.

Geschützte Telefone spielen unter folgenden Umständen einen Signalton ab:

- Wenn die Option Sicherheitssignalton aktiviert ist:
  - Wenn auf beiden Seiten sichere Medien eingerichtet sind und der Anrufstatus „Sicher“ lautet, gibt das Telefon das Signal für eine sichere Verbindung wieder (drei lange Signaltöne mit Pausen).
  - Wenn auf beiden Seiten nicht sichere Medien eingerichtet sind und der Anrufstatus „Nicht sicher“ lautet, wird das Signal für eine nicht sichere Verbindung abgespielt (sechs kurze Signaltöne mit kurzen Pausen).

Wenn die Option Sicherheitssignalton wiedergeben deaktiviert ist, erklingt kein Signalton.

802.1x-Authentifizierung

Cisco IP-Telefons unterstützen die 802.1X-Authentifizierung.

Cisco IP-Telefons und Cisco Catalyst-Switches verwenden normalerweise CDP (Cisco Discovery Protocol), um sich gegenseitig zu identifizieren und Paramater zu bestimmen, beispielsweise die VLAN-Zuweisung und Inline-Energieanforderungen.

Für die Unterstützung der 802.1X-Authentifizierung sind mehrere Komponenten erforderlich:

- Cisco IP-Telefon: Das Telefon initiiert die Anforderung, um auf das Netzwerk zuzugreifen. Die Telefone enthalten einen 802.1X-Supplicant. Dieses Supplicant ermöglicht Netzwerkadministratoren die Verbindung von IP-Telefonen mit den LAN-Switch-Ports zu steuern. Die aktuelle Version des 802.1X Supplicant verwendet EAP-FAST und EAP-TLS für die Netzwerkauthentifizierung.
- Cisco Catalyst-Switch (oder Switch eines Drittanbieters): Der Switch muss 802.1X unterstützen, damit er als Authentifikator agieren und Meldungen zwischen dem Telefon und dem Authentifizierungsserver übermitteln kann. Nach dem Meldungsaustausch gewährt oder verweigert der Switch dem Telefon den Zugriff auf das Netzwerk.

Um 802.1X zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

- Konfigurieren Sie die anderen Komponenten, bevor Sie die 802.1X-Authentifizierung auf dem Telefon aktivieren.
- Sprach-VLAN konfigurieren: Da in der 802.1X-Standardkonfiguration keine VLANs vorgesehen sind, sollten Sie diese Einstellung je nach Switch-Unterstützung konfigurieren.
  - Aktiviert: Wenn Sie einen Switch verwenden, der die Authentifizierung in mehreren Domänen unterstützt, können Sie das Sprach-VLAN weiterhin verwenden.

- Deaktiviert: Wenn der Switch die Authentifizierung in mehreren Domänen nicht unterstützt, deaktivieren Sie das Sprach-VLAN und weisen den Port dem systemeigenen VLAN zu.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Die aktuellen Sicherheitsfunktionen auf dem Telefon anzeigen

Weitere Informationen zu den Sicherheitsfunktionen und zur Sicherheit von Cisco Unified Communications Manager und des Cisco IP-Telefon, finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Wählen Sie **Einstellungen** aus.

Schritt 2 Wählen Sie **Administratoreinstellungen** > **Sicherheitskonfiguration** aus.

Die meisten Sicherheitsfunktionen sind nur verfügbar, wenn eine Zertifikatvertrauensliste (CTL) auf dem Telefon installiert ist.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Sicherheitsprofile anzeigen

Alle Cisco IP-Telefons, die Cisco Unified Communications Manager unterstützen, verwenden ein Sicherheitsprofil, das definiert, ob das Telefon nicht geschützt, authentifiziert oder verschlüsselt ist. Weitere Informationen zum Konfigurieren des Sicherheitsprofils und das Übernehmen des Profils auf dem Telefon finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **System** > **Sicherheit** > **Telefonsicherheitsprofil** aus.

Schritt 2 Überprüfen Sie die Einstellung „Sicherheitsmodus“.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Konfigurieren der Sicherheitseinstellungen

Prozedur

Schritt 1 Drücken Sie **Einstellungen**.

Schritt 2 Wählen Sie **Administratoreinstellungen** > **Sicherheitskonfiguration** aus.

Schritt 3 Legen Sie die Felder fest.
Nachdem Sie die Felder festgelegt haben, müssen Sie das Telefon möglicherweise neu starten.

Sicherheitskonfigurationsfelder

Das Menü „Sicherheits-Setup“ enthält Felder und Untermenüs für Vertrauenslisten und 802.1X-Authentifizierung.

Tabelle 3: Menü „Sicherheits-Setup“

Eintrag	Typ	Standard	Beschreibung
Security mode (Sicherheitsmodus)			Nur lesen
LSC			Siehe Einrichten eines LSC (Locally Significant Certificate), auf Seite 11.
Vertrauensliste	Menü		Siehe die Tabelle „Untermenü Vertrauensliste“.
802.1x-Authentifizierung	Menü		Siehe die Tabelle „Untermenü 802.1X-Authentifizierung“.

Tabelle 4: Untermenü Vertrauensliste

Eintrag	Typ	Standard	Beschreibung
CTL-Datei	Menü		Zeigt eine Liste von CTL-Dateien an
ITL-Datei	Menü		Zeigt eine Liste von ITL-Dateien an
Konfiguration (signiert)	Menü		Siehe die Tabelle „Untermenü Konfiguration.“

Tabelle 5: Untermenü Konfiguration

Eintrag	Typ	Standard	Beschreibung
SRST-Router			Zeigt die IP-Adresse von SRST an.

Tabelle 6: Untermenü 802.1X-Authentifizierung

Eintrag	Typ	Standard	Beschreibung
Geräteauthentifizierung	Deaktiviert Aktiviert	Deaktiviert	
Transaktionsstatus	Untermenü		Siehe die Tabelle „Untermenü Transaktionsstatus“.

Tabelle 7: Untermenü Transaktionsstatus

Eintrag	Typ	Standard	Beschreibung
Transaktionsstatus	Getrennt Verbunden		
Protokolle			Liste von Protokollen.

Einrichten eines LSC (Locally Significant Certificate)

Diese Aufgabe bezieht sich auf das Einrichten eines LSC mit der Methode der Authentifizierungszeichenfolge.

Vorbereitungen

Stellen Sie sicher, dass die Sicherheitskonfiguration von Cisco Unified Communications Manager und CAPF (Certificate Authority Proxy Function) vollständig ist:

- Die CTL- oder ITL-Datei hat ein CAPF-Zertifikat.
- Überprüfen Sie in der Cisco Unified Communications Operating System-Verwaltung, ob das CAPF-Zertifikat installiert ist.
- CAPF wird ausgeführt und ist konfiguriert.

Weitere Informationen zu diesen Einstellungen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Sie benötigen den CAPF-Authentifizierungscode, der während der Konfiguration von CAPF festgelegt wurde.

Schritt 2 Drücken Sie auf dem Telefon auf **Anwendungen** .

Schritt 3 Wählen Sie auf dem Telefon **Einstellungen** aus.

Schritt 4 Wählen Sie **Administratoreinstellungen** > **Sicherheits-Setup** aus.

Hinweis Sie können den Zugriff auf das Menü „Einstellungen“ mit dem Feld „Zugriff auf Einstellungen“ im Fenster „Telefonkonfiguration“ in der Cisco Unified Communications Manager-Verwaltung steuern.

Schritt 5 Wählen Sie **LSC** aus und drücken Sie **Auswählen** oder **Aktualisieren**.

Das Telefon fordert eine Authentifizierungszeichenfolge an.

Schritt 6 Geben Sie die Authentifizierungscode ein und drücken Sie **Senden**.

Das Telefon installiert, aktualisiert oder entfernt das LSC, abhängig davon, wie CAPF konfiguriert ist. Während des Verfahrens werden mehrere Meldungen im LSC-Optionsfeld im Menü Sicherheitskonfiguration angezeigt, damit Sie den Status überwachen können. Wenn das Verfahren abgeschlossen ist, wird Installiert oder Nicht installiert auf dem Telefon angezeigt.

Der Prozess zum Installieren, Aktualisieren oder Entfernen des LSC kann längere Zeit dauern.

Wenn das Telefon erfolgreich installiert wurde, wird die Meldung `Installiert` angezeigt. Wenn das Telefon `Nicht installiert` anzeigt, ist möglicherweise die Autorisierungszeichenfolge ungültig oder das Telefon ist nicht für Updates aktiviert. Wenn der CAPF-Vorgang die LSC löscht, zeigt das Telefon `Nicht installiert` an. Der CAPF-Server protokolliert die Fehlermeldungen. Der Pfad zu den Protokollen und die Bedeutung der Fehlermeldungen werden in der CAPF-Serverdokumentation beschrieben.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Aktivieren des FIPS-Modus

Prozedur

Schritt 1 Wählen Sie in Cisco Unified Communications Manager Administration **Gerät** > **Telefon** aus, und navigieren Sie zum Telefon.

Schritt 2 Navigieren Sie zum produktspezifischen Konfigurationsbereich.

Schritt 3 Legen Sie das Feld **FIPS-Modus** auf „Aktiviert“ fest.

Schritt 4 Wählen Sie **Konfiguration übernehmen**.

Schritt 5 Wählen Sie **Speichern** aus.

Schritt 6 Starten Sie das Telefon neu.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.