Beveiliging van de Cisco IP-conferentietelefoon

Beveiligingsoverzicht Cisco IP-telefoon

De beveiligingsfuncties beschermen tegen diverse bedreigingen, waaronder bedreigingen van de identiteit van de telefoon en gegevens. Deze functies vormen en onderhouden geverifieerde communicatiestromen tussen de telefoon en de Cisco Unified Communications Manager-server en zorgen dat de telefoon alleen digitaal ondertekende bestanden gebruikt.

Cisco Unified Communications Manager Release 8.5(1) en later omvat standaardbeveiliging met de volgende functies voor Cisco IP-telefoons waarop geen CTL-client wordt uitgevoerd:

- Ondertekenen van telefoonconfiguratiebestanden
- Codering telefoonconfiguratiebestand
- HTTPS met Tomcat en andere Webservices

Opmerking Veilige signalering en mediafuncties vereisen nog steeds dat u de CTL-client uitvoert en hardware-eTokens gebruikt.

Voor meer informatie over beveiligingsfuncties raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Er wordt een LSC-certificaat (Locally Significant Certificate) op de telefoons geïnstalleerd nadat u de vereiste taken hebt uitgevoerd die samenhangen met de Certificate Authority Proxy Function (CAPF). U kunt Cisco Unified Communications Manager Administration gebruiken om een LSC te configureren. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Een LSC kan niet worden gebruikt als gebruikerscertificaat voor EAP-TLS met WLAN-verificatie.

U kunt de installatie van een LSC ook starten via het menu Beveiligingsconfiguratie op de telefoon. Met dit menu kunt u een LSC bijwerken en verwijderen.

De Cisco IP-conferentietelefoon 7832 is compatibel met Federal Information Processing Standard (FIPS). Om correct te kunnen werken vereist de FIPS-modus een RSA-sleutelomvang van 2048 bits of meer. Als het RSA-servercertificaat niet 2048 bits of groter is, wordt de telefoon niet geregistreerd met Cisco Unified Communications Manager en ziet u `Telefoon wordt niet geregistreerd. Certificaatsleutelgrootte is niet compatibel met FIPS` op de telefoon.

U kunt geen privésleutels (LSC of MIC) gebruiken in FIPS-modus.

Als de telefoon een bestaande LSC heeft die kleiner is dan 2048 bits, moet u de lengte van de LSC-sleutel bijwerken naar 2048 bits of hoger voordat u FIPS inschakelt.

Verwante onderwerpen

Een lokaal significant certificaat instellen, op pagina 12
Cisco Unified Communications Manager Documentatie

Beveiligingsverbeteringen voor uw telefoonnetwerk

U kunt Cisco Unified Communications Manager 11.5(1) en 12.0(1) inschakelen om te werken in een verbeterde beveiligingsomgeving. Met deze verbeteringen kan uw telefoonnetwerk werken met een set strikte beveiligings- en risicobeheerinstellingen om u en uw gebruikers te beschermen.

Cisco Unified Communications Manager 12.5(1) biedt geen ondersteuning voor een verbeterde beveiligingsomgeving. Schakel FIPS uit voordat u de upgrade naar Cisco Unified Communications Manager 12.5(1) uitvoert, anders werken uw TFTP- en andere services niet naar behoren.

De verbeterde beveiligingsomgeving bevat de volgende functies:

- Verificatie voor contactpersonen zoeken.
- TCP als standaardprotocol voor externe logboekregistratie controlespoor.
- FIPS-modus.
- Een verbeterd referentiebeleid.
- Ondersteuning voor de SHA-2-hashreeks voor digitale handtekeningen.
- Ondersteuning voor een RSA-sleutelomvang van 512 en 4096 bits.

Met Cisco Unified Communications Manager versie 14.0 en Cisco IP-telefoonfirmware versie 14.0 en hoger ondersteunen de telefoons SIP OAuth-verificatie.

OAuth wordt ondersteund voor proxy Trivial File Transfer Protocol (TFTP) met Cisco Unified Communications Manager versie 14.0(1)SU1 of hoger en de firmwarerelease 14.1(1) voor Cisco IP-telefoons. Proxy TFTP en OAuth voor proxy TFTP wordt niet ondersteund op Mobile Remote Access (MRA).

Raadpleeg voor meer informatie over beveiliging, het volgende:

- *Systeemconfiguratiehandleiding voor Cisco Unified Communications Manager*, versie 14.0(1) of hogerhttps://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

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

Opmerking Uw Cisco IP-telefoon kan slechts een beperkt aantal ITL-bestanden (Identity Trust List) opslaan. ITL-bestanden mogen de beperking van 64K niet overschrijden, dus beperk het aantal bestanden dat de Cisco Unified Communications Manager naar de telefoon kan doorsturen.

Ondersteunde beveiligingsfuncties

Beveiligingsfuncties beschermen tegen diverse bedreigingen, waaronder bedreigingen van de identiteit van de telefoon en gegevens. Deze functies vormen en onderhouden geverifieerde communicatiestromen tussen de telefoon en de Cisco Unified Communications Manager-server en zorgen dat de telefoon alleen digitaal ondertekende bestanden gebruikt.

Cisco Unified Communications Manager Release 8.5(1) en later omvat standaardbeveiliging met de volgende functies voor Cisco IP-telefoons waarop geen CTL-client wordt uitgevoerd:

- Ondertekenen van telefoonconfiguratiebestanden
- Codering telefoonconfiguratiebestand
- HTTPS met Tomcat en andere Webservices

Opmerking Veilige signalering en mediafuncties vereisen nog steeds dat u de CTL-client uitvoert en hardware-eTokens gebruikt.

Door beveiliging te implementeren in het Cisco Unified Communications Manager-systeem voorkomt u identiteitsdiefstal van de telefoon en de Cisco Unified Communications Manager-server, en ongewenste bewerking van gegevens, gespreksignalen en mediastreams.

Als bescherming tegen deze bedreigingen brengt het Cisco IP-telefonienetwerk beveiligde (gecodeerde) communicatiestromen tot stand tussen een telefoon en de server, worden bestanden digitaal ondertekend voordat ze worden overgebracht naar een telefoon en worden mediastromen en gespreksignalen tussen Cisco IP-telefoons gecodeerd.

Er wordt een LSC-certificaat (Locally Significant Certificate) op de telefoons geïnstalleerd nadat u de vereiste taken hebt uitgevoerd die samenhangen met de Certificate Authority Proxy Function (CAPF). U kunt Cisco Unified Communications Manager Administration gebruiken voor het configureren van een LSC, zoals wordt beschreven in de Cisco Unified Communications Manager beveiligingshandleiding. U kunt de installatie van een LSC ook starten via het menu Beveiligingsconfiguratie op de telefoon. Met dit menu kunt u een LSC bijwerken en verwijderen.

Een LSC kan niet worden gebruikt als gebruikerscertificaat voor EAP-TLS met WLAN-verificatie.

De telefoons gebruiken het beveiligingsprofiel van de telefoon, dat aangeeft of het apparaat niet-veilig of veilig is. Voor meer informatie over het toepassen van het beveiligingsprofiel op de telefoon, raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Als u de beveiligingsinstellingen in Cisco Unified Communications Manager Administration configureert, bevat het telefoon-configuratiebestand vertrouwelijke informatie. Om te zorgen voor de privacy van een configuratiebestand moet u dit configureren voor codering. Voor gedetailleerde informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Door beveiliging te implementeren in het Cisco Unified Communications Manager-systeem voorkomt u identiteitsdiefstal van de telefoon en de Cisco Unified Communications Manager-server, en ongewenste bewerking van gegevens, gespreksignalen en mediastreams.

In de volgende tabel ziet u een overzicht van de beveiligingsfuncties die door Cisco IP-conferentietelefoon 7832 worden ondersteund. Voor meer informatie over deze voorzieningen, Cisco Unified Communications Manager en Cisco IP-telefoon-beveiliging raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Tabel 1: Overzicht van beveiligingsfuncties

Functie	Beschrijving
Verificatie afbeelding	Ondertekende binaire bestanden (met de extensie .sbn) verhinderen dat de firmware-afbeelding wordt gewijzigd voordat deze op een telefoon wordt geladen. Als de afbeelding wordt gewijzigd, kan het verificatieproces op de telefoon mislukken en de nieuwe afbeelding worden geweigerd.
Installatie certificaat op klantlocatie	Elke telefoon vereist een uniek certificaat voor apparaatverificatie. Telefoons bevatten een in de fabriek geïnstalleerd certificaat (MIC), maar voor extra beveiliging kunt u in Cisco Unified Communications Manager Administration opgeven dat een certificaat wordt geïnstalleerd met Certificate Authority Proxy Function (CAPF). U kunt ook een Locally Significant Certificate (LSC) installeren via het menu Beveiligingsconfiguratie op de telefoon.
Apparaatverificatie	Vindt plaats tussen de Cisco Unified Communications Manager-server en de telefoon wanneer elke entiteit het certificaat van de andere entiteit accepteert. Bepaalt of een veilige verbinding tussen de telefoon en Cisco Unified Communications Manager nodig is en maakt zo nodig een veilig signaleringspad tussen de entiteiten met TLS-protocol. Cisco Unified Communications Manager registreert geen telefoons tenzij ze kunnen worden geverifieerd door Cisco Unified Communications Manager.

Functie	Beschrijving
Bestandsverificatie	Valideert digitaal ondertekende bestanden die de telefoon downloadt. De telefoon valideert de handtekening zodat het bestand na het maken niet wordt gewijzigd. Bestanden waarvan de verificatie mislukt, worden niet weggeschreven naar het Flash-geheugen op de telefoon. De telefoon weigert zulke bestanden zonder verdere verwerking.
Verificatie signalering	Gebruikt het TLS-protocol om te valideren dat de signaleringspakketten niet zijn gewijzigd tijdens de verzending.
Manufacturing Installed Certificate	Elke telefoon vereist een uniek tijdens de fabricage geïnstalleerd certificaat (Manufacturing Installed Certificate, MIC) voor apparaatverificatie. MIC is een permanent uniek identiteitsbewijs voor de telefoon waarmee Cisco Unified Communications Manager de telefoon kan verifiëren.
Veilige SRST-referentie	Nadat u een SRST-referentie voor beveiliging hebt geconfigureerd en de afhankelijke apparaten in Cisco Unified Communications Manager Administration hebt gereset, voegt de TFTP-server het SRST-certificaat toe aan het cnf.xml-bestand en stuurt het bestand naar de telefoon. Een veilige telefoon gebruikt vervolgens een TLS-verbinding voor interactie met de SRST-router.
Mediacodering	Gebruikt SRTP om te zorgen dat de mediastromen tussen ondersteunde apparaat veilig zijn dat alleen het bedoelde apparaat de gegevens ontvangt en leest. Dit omvat het maken van een mediahoofdsleutelpaar voor de apparaten, het leveren van de sleutels aan de apparaten en het beveiligen van de sleutels tijdens het transport.
CAPF (Certificate Authority Proxy Function)	Implementeert delen van de certificaatgeneratieprocedure met een te intensieve verwerking voor de telefoon en communiceert met de telefoon voor het genereren van sleutels en het installeren van het certificaat. De CAPF kan worden geconfigureerd voor het aanvragen van certificaten voor de telefoon bij door de klant opgegeven certificeringsinstanties of voor het lokaal genereren van certificaten.
Beveiligingsprofielen	Bepaalt of de telefoon onveilig, geverifieerd of gecodeerd is.
Gecodeerde configuratiebestanden	Garandeert de privacy van de telefoonconfiguratiebestanden.

Functie	Beschrijving
Optionele uitschakeling van de webserverfunctionaliteit voor een telefoon	U kunt toegang verhinderen tot de telefoonwebpagina waarop allerlei operationele statistieken worden weergegeven.
Telefoon versterken	Aanvullende beveiligingsopties die u beheert via Cisco Unified Communications Manager Administration: • Toegang tot webpagina's voor een telefoon uitschakelen **Opmerking** U kunt de huidige instellingen weergeven voor de opties GARP ingeschakeld en Spraak-VLAN ingeschakeld door naar het Configuratiemenu van de telefoon te gaan.
802.1X Verificatie	De telefoon kan 802.1X-verificatie gebruiken om te verzoeken om toegang tot het netwerk.
AES 256-codering	Bij verbinding met Cisco Unified Communications Manager Release 10.5(2) en hoger ondersteunen de telefoons AES 256-codering voor TLS en SIP voor signalering en mediacodering. Zo kunnen telefoons TLS 1.2-verbinding initiëren en ondersteunen met op AES-256 gebaseerde cijfers conform SHA-2-standaarden (Secure Hash Algorithm) en compatibel met Federal Information Processing Standards (FIPS). De nieuwe cijfers zijn|: • Voor TLS-verbindingen: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Voor sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Voor meer informatie raadpleegt u de documentatie bij Cisco Unified Communications Manager.
Elliptic Curve Digital Signature Algorithm (ECDSA)-certificaten	Als onderdeel van het CC-certificaat (Common Criteria), zijn er in Cisco Unified Communications Manager-versie 11.0 ECDSA-certificaten toegevoegd. Dit geldt voor alle VOS-producten (Spraakbesturingssysteem) van versie Cisco Unified Communications Manager 11.5 en hoger.

Verwante onderwerpen

Cisco Unified Communications Manager Documentatie

Beveiliging telefoongesprek

Wanneer beveiliging is geïmplementeerd voor een telefoon, kunt u veilige telefoongesprekken herkennen aan de pictogrammen op het telefoonscherm. U kunt ook bepalen of de verbonden telefoon veilig is en beschermd als een beveiligingstoon weerklinkt aan het begin van het gesprek.

In een beveiligd gesprek worden alle gespreksignalen en mediastreams gecodeerd. Een beveiligd gesprek biedt een hoog beveiligingsniveau, met integriteit en privacy voor het gesprek. Wanneer een actief gesprek wordt gecodeerd, verandert het pictogram voor actief gesprek rechts van de gespreksduurtimer op het telefoonscherm in het volgende pictogram:  .

Opmerking Als het gesprek wordt gerouteerd via niet-IP-gesprekspaden, zoals bijvoorbeeld PSTN, kan het gesprek onveilig worden ook al is het gecodeerd binnen het IP-netwerk en is er een vergrendelingspictogram aan gekoppeld.

In een beveiligd gesprek weerklinkt een beveiligingstoon aan het begin van het gesprek om aan te geven dat de andere verbonden telefoon veilige audio ontvangt en verzendt. Als uw gesprek tot stand komt met een onbeveiligde telefoon, hoort de gebruiker geen beveiligingstoon.

Opmerking Beveiligd bellen wordt ondersteund tussen twee telefoons. Beveiligde conferentie, Cisco Extension Mobility en gedeelde lijnen kunnen worden geconfigureerd via een veilige conferentiebrug.

Als een telefoon is geconfigureerd als 'beveiligd' (gecodeerd en vertrouwd) in Cisco Unified Communications Manager, kan deze een “beschermde” status krijgen. Nadat een telefoon is beschermd, kan deze worden geconfigureerd om een indicatietoon af te spelen aan het begin van een gesprek:

- Beschermde telefoon: als u de status van een veilige telefoon wilt wijzigen in beschermd, schakelt u het selectievakje Beschermde telefoon in in het telefoonconfiguratievenster in Cisco Unified Communications Manager Administration (**Apparaat** > **Telefoon**).
- Beveiligde indicatietoon afspelen: als u wilt dat de beschermde telefoon een veilige of onveilige indicatietoon afspeelt, stelt u de instelling Beveiligde indicatietoon afspelen in op Waar. Standaard is Beveiligde indicatietoon afspelen ingesteld op Onwaar. Stel deze optie in in Cisco Unified Communications Manager Administration (**Systeem** > **Serviceparameters**). Selecteer de server en vervolgens de Cisco Unified Communications Manager-service. Selecteer in het venster Serviceparameterconfiguratie de optie in het gedeelte Functie - Veilige toon. De standaardinstelling is onwaar.

Identificatie veilig conferentiegesprek

U kunt een veilig conferentiegesprek starten en het beveiligingsniveau van de deelnemers controleren. Een veilig conferentiegesprek wordt met dit proces tot stand gebracht:

1. Een gebruiker start het conferentiegesprek vanaf een veilige telefoon.
2. Cisco Unified Communications Manager wijst een veilige conferentiebrug toe aan het gesprek.
3. Als deelnemers worden toegevoegd, controleert Cisco Unified Communications Manager de beveiligde modus van elke telefoon en wordt het beveiligingsniveau voor de conferentie gehandhaafd.

4. Op het telefoonscherm wordt het beveiligingsniveau van het conferentiegesprek weergegeven. In een veilige conferentie wordt het veilige pictogram  rechts van **Conferentie** weergegeven op het telefoonscherm.

Opmerking Beveiligd bellen wordt ondersteund tussen twee telefoons. Voor beveiligde telefoons zijn bepaalde functies zoals conferentiegesprekken, gedeelde lijnen en Extension Mobility, niet beschikbaar wanneer beveiligd bellen is geconfigureerd.

De volgende tabel bevat informatie over wijzigingen in conferentiebeveiligingsniveaus afhankelijk van het beveiligingsniveau van de telefoon van de initiator, de beveiligingsniveaus van de deelnemers en de beschikbaarheid van veilige conferentiebruggen.

Tabel 2: Beveiligingsrestricties met conferentiegesprekken

Initiator beveiligingsniveau telefoon	Gebruikte functie	Beveiligingsniveau van deelnemers	Resultaten van actie
Onveilig	Conferentie	Beveiligd	Onveilige conferentiebrug Onveilige conferentie
Beveiligd	Conferentie	Er is ten minste één lid niet veilig.	Veilige conferentiebrug Onveilige conferentie
Beveiligd	Conferentie	Beveiligd	Veilige conferentiebrug Veilig gecodeerd niveau conferentie
Onveilig	Meet Me	Minimum beveiligingsniveau is gecodeerd.	Initiator ontvangt bericht `Does not meet Security Level, call rejected` (beveiligingsniveau onvoldoende en gesprek geweigerd).
Beveiligd	Meet Me	Minimum beveiligingsniveau is onveilig.	Veilige conferentiebrug Conferentie accepteert alle gesprekken.

Identificatie veilig telefoongesprek

Een veilig gesprek wordt tot stand gebracht als uw telefoon en de telefoon aan de andere kant zijn geconfigureerd voor veilig bellen. De andere telefoon kan zich in hetzelfde Cisco IP-netwerk bevinden of in een netwerk buiten het IP-netwerk. Beveiligde oproepen kunnen alleen plaatsvinden tussen twee telefoons. Conferentiegesprekken ondersteunen veilige gesprekken nadat een veilige conferentiebrug is ingesteld.

Een veilig gesprek wordt als volgt tot stand gebracht:

1. Een gebruiker start het gesprek vanaf een veilige telefoon (beveiligde modus).
2. Op het telefoonscherm wordt het veilige pictogram  weergegeven. Dit pictogram geeft aan dat de telefoon is geconfigureerd voor veilige gesprekken, maar niet dat de andere verbonden telefoon ook beveiligd is.
3. De gebruiker hoort een beveiligingstoon als het gesprek wordt verbonden met de andere beveiligde telefoon, wat aangeeft dat het gesprek aan beide einden wordt gecodeerd en beveiligd. Als het gesprek tot stand komt met een onbeveiligde telefoon, hoort de gebruiker geen beveiligingstoon.

Opmerking Beveiligd bellen wordt ondersteund tussen twee telefoons. Voor beveiligde telefoons zijn bepaalde functies zoals conferentiegesprekken, gedeelde lijnen en Extension Mobility, niet beschikbaar wanneer beveiligd bellen is geconfigureerd.

Deze indicatietonen voor beveiligd of niet beveiligd bellen worden alleen afgespeeld op beveiligde telefoons. Onbeveiligde telefoons spelen nooit tonen af. Als de algemene gespreksstatus wijzigt tijdens een gesprek, verandert de indicatietoon en speelt de beveiligde telefoon de bijbehorende toon af.

Een beveiligde telefoon speelt al dan niet een toon af onder de volgende omstandigheden:

- Wanneer de optie Beveiligde indicatietoon afspelen is ingeschakeld:
  - Als end-to-end beveiligde media wordt opgezet en de gespreksstatus beveiligd is, speelt de telefoon de beveiligde indicatietoon af (drie lange piepjes met pauzes).
  - Als end-to-end niet-beveiligde media wordt opgezet en de gespreksstatus niet-beveiligd is, speelt de telefoon de niet-beveiligde indicatietoon af (zes korte piepjes met korte pauzes).

Als de optie Beveiligde indicatietoon afspelen is uitgeschakeld, wordt er geen toon afgespeeld.

802.1X Verificatie

Cisco IP-telefoon ondersteunt 802.1X-verificatie.

Cisco IP-telefoons en Cisco Catalyst-switches gebruiken traditioneel Cisco Discovery Protocol (CDP) om elkaar te herkennen en om parameters te bepalen zoals VLAN-toewijzing en inline voedingsvereisten.

Voor ondersteuning van de 802.1X-verificatie zijn diverse onderdelen vereist:

- Cisco IP-telefoon: de telefoon initieert het verzoek voor toegang tot het netwerk. Telefoons bevatten een 802.1X-supplicant. Met deze supplicant kunnen netwerkbeheerders de verbinding regelen van IP-telefoons met de LAN-switchpoorten. De huidige versie van de 802.1X-supplicant voor de telefoon gebruikt de opties EAP-FAST en EAP-TLS voor netwerkverificatie.
- Cisco Catalyst Switch (of andere switch van derden): de switch moet 802.1X ondersteunen, zodat deze kan optreden als authenticator en de berichten tussen de telefoon en de verificatieserver kan doorgeven. Nadat de uitwisseling is afgerond, kan de switch toegang tot het netwerk toestaan of weigeren.

U moet de volgende acties uitvoeren om 802.1X te configureren.

- Configureer de overige componenten voordat u 802.1X-verificatie op de telefoon inschakelt.

- Spraak-VLAN configureren: omdat de 802.1X-standaard geen rekening houdt met VLAN's, moet u deze instelling configureren op basis van de switchondersteuning.
  - Ingeschakeld: als u een switch gebruikt die multidomeinverificatie ondersteunt, kunt u hetzelfde spraak-VLAN blijven gebruiken.
  - Uitgeschakeld: als de switch niet multidomeinverificatie ondersteunt, schakelt u het spraak-VLAN uit en probeert u de poort toe te wijzen aan het native VLAN.

Verwante onderwerpen

Cisco Unified Communications Manager Documentatie

Huidige beveiligingsfuncties weergeven op de telefoon

Voor meer informatie over deze beveiligingsfuncties en over Cisco Unified Communications Manager en Cisco IP-telefoon-beveiliging raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Procedure

Stap 1 Selecteer **Instellingen**.

Stap 2 Selecteer **Beheerdersinstellingen** > **Beveiligingsinstellingen**.

De meeste beveiligingsfuncties zijn alleen beschikbaar als een vertrouwde certificaatlijst (CTL) op de telefoon is geïnstalleerd.

Verwante onderwerpen

Cisco Unified Communications Manager Documentatie

Beveiligingsprofielen weergeven

Alle Cisco IP-telefoons die Cisco Unified Communications Manager ondersteunen, werken met een beveiligingsprofiel, wat bepaalt of de telefoon niet-beveiligd, geverifieerd of gecodeerd is. Voor meer informatie over het configureren van het beveiligingsprofiel en het toepassen ervan op de telefoon, raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Procedure

Stap 1 Selecteer in Cisco Unified Communications Manager Administration **Systeem** > **Beveiliging** > **Beveiligingsprofiel telefoon**.

Stap 2 Kijk naar de instelling voor Beveiligde modus.

Verwante onderwerpen

Cisco Unified Communications Manager Documentatie

Beveiligingsinstellingen configureren

Procedure

Stap 1 Druk op **Instellingen**.

Stap 2 Selecteer **Beheerdersinstellingen** > **Beveiligingsinstellingen**.

Stap 3 Stel de velden in.
Nadat u de velden hebt ingesteld, moet u mogelijk de telefoon opnieuw opstarten.

Velden met beveiligingsinstellingen

Het menu Beveiligingsinstellingen bevat velden en submenu's voor vertrouwde lijsten en 802.1x-verificatie.

Tabel 3: Menu Beveiligingsinstellingen

Invoer	Type	Standaard	Beschrijving
Beveiligde modus			Alleen lezen
LSC			Zie Een lokaal significant certificaat instellen, op pagina 12.
Vertrouwde lijst	Menu		Zie de tabel “Submenu Vertrouwde lijst”.
802.1X Verificatie	Menu		Zie de tabel “Submenu 802.1x-verificatie”.

Tabel 4: Submenu Vertrouwde Lijst

Invoer	Type	Standaard	Beschrijving
CTL-bestand	Menu		Geeft een lijst met CTL-bestanden weer
ITL-bestand	Menu		Geeft een lijst met ITL-bestanden weer
Configuratie (ondertekend)	Menu		Zie de tabel “Submenu Configuratie”.

Tabel 5: Submenu Configuratie

Invoer	Type	Standaard	Beschrijving
SRST-router			Geeft het IP-adres van SRST weer.

Tabel 6: Submenu 802.1x-verificatie

Invoer	Type	Standaard	Beschrijving
Apparaatverificatie	Uitgeschakeld Ingeschakeld	Uitgeschakeld	
Transactiestatus	Submenu		Zie de tabel “Submenu Transactiestatus”.

Tabel 7: Submenu Transactiestatus

Invoer	Type	Standaard	Beschrijving
Transactiestatus	Verb.verbroken Verbonden		
Protocollen			Lijst met protocollen.

Een lokaal significant certificaat instellen

Deze taak is van toepassing op het instellen van een LSC met de methode verificatiereeks.

Voordat u begint

Zorg dat de juiste configuraties voor Cisco Unified Communications Manager en de CAPF-beveiliging (Certificate Authority Proxy Function) zijn voltooid

- Het CTL- of ITL-bestand heeft een CAPF-certificaat.
- Controleer in Besturingssysteem van Cisco Unified Communications Administration of het CAPF-certificaat is geïnstalleerd.
- CAPF wordt uitgevoerd en is geconfigureerd.

Voor meer informatie over deze instellingen raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Procedure

Stap 1 Haal de CAPF-verificatiecode op die werd ingesteld toen CAPF werd geconfigureerd.

Stap 2 Druk op de telefoon op **Toepassingen** .

Stap 3 Kies op de telefoon **Instellingen**.

Stap 4 Kies **Beheerdersinstellingen** > **Beveiligingsinstellingen**.

Opmerking U kunt de toegang bepalen tot het menu Instellingen met behulp van het veld Toegang tot instellingen in het venster Telefoonconfiguratie van Cisco Unified Communications Manager Administration.

Stap 5 Kies **LSC** en druk op **Selecteren** of **Bijwerken**.

De telefoon vraagt om een verificatiereeks.

Stap 6 Voer de verificatiecode in en druk op **Verzenden**.

De telefoon begint met het installeren, bijwerken of verwijderen van de LSC, afhankelijk van hoe CAPF is geconfigureerd. Tijdens de procedure verschijnt een reeks berichten in het LSC-optieveld in het menu Beveiligingsconfiguratie, zodat u de voortgang kunt bewaken. Wanneer de procedure is voltooid, verschijnt Geïnstalleerd of Niet geïnstalleerd op de telefoon.

Het proces voor het installeren, bijwerken of verwijderen van LSC kan geruime tijd in beslag nemen.

Wanneer de installatieprocedure voor de telefoon is voltooid, verschijnt het bericht `Geïnstalleerd`. Als de telefoon `Niet geïnstalleerd` aangeeft, is mogelijk de autorisatietekenreeks onjuist of is de telefoonupgrade niet ingeschakeld. Als bij de CAPF-bewerking de LSC wordt verwijderd, geeft de telefoon mogelijk `Niet geïnstalleerd` aan om aan te geven of de bewerking is geslaagd. De CAPF-server logt de foutmeldingen. Raadpleeg de CAPF-serverdocumentatie om de logbestanden te vinden en de betekenis van de foutmeldingen te achterhalen.

Verwante onderwerpen

Cisco Unified Communications Manager Documentatie

FIPS-modus inschakelen

Procedure

Stap 1 Selecteer in Cisco Unified Communications Manager Administration **Apparaat** > **Telefoon** en zoek de telefoon.

Stap 2 Navigeer naar het gedeelte Productspecifieke configuratie.

Stap 3 Stel het veld **FIPS-modus** in op Ingeschakeld.

Stap 4 Selecteer **Config toepassen**.

Stap 5 Selecteer **Opslaan**.

Stap 6 Start de telefoon opnieuw.