



# Beveiliging van de Cisco IP-conferentietelefoon

- [Beveiligingsoverzicht Cisco IP-telefoon, op pagina 1](#)
- [Beveiligingsverbeteringen voor uw telefoonnetwerk, op pagina 2](#)
- [Ondersteunde beveiligingsfuncties, op pagina 3](#)

## 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 8832 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 wordt weergegeven in de statusberichten van 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 5

[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:

- *Systemconfiguratiehandleiding voor Cisco Unified Communications Manager*, versie 14.0(1) of hoger <https://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>)

- SIP OAuth: *Functieconfiguratiegids voor Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-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 8832 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**

Funcie	Beschrijving
Verificatie afbeelding	Ondertekende binaire bestanden (met de extensie .sbn) verhindert het kopiëren van de afbeelding. Als de afbeelding wordt gewijzigd, kan het verifiëren mislukken.
Installatie certificaat op klantlocatie	Elke telefoon vereist een uniek certificaat voor apparaatverificatie. Voor extra beveiliging kunt u in Cisco Unified Communications Manager de Certificate Authority Proxy Function (CAPF) configureren. U kunt ook een Beveiligingsconfiguratie op de telefoon.
Apparaatverificatie	Vindt plaats tussen de Cisco Unified Communications Manager en de telefoon. De telefoon accepteert. Bepaalt of een veilige verbinding tussen de telefoon en de server veilig signaleringspad tussen de entiteiten met TLS-protocol. Gebruikt de telefoon om te kunnen worden geverifieerd door Cisco Unified Communications Manager.
Bestandsverificatie	Valideert digitaal ondertekende bestanden die de telefoon downloaden. Als de bestanden niet wordt gewijzigd. Bestanden waarvan de verificatie mislukt, wordt de telefoon weigert zulke bestanden zonder verdere verwerking.
Verificatie signalering	Gebruikt het TLS-protocol om te valideren dat de signaleringspad veilig is.
Manufacturing Installed Certificate	Elke telefoon vereist een uniek tijdens de fabricage geïnstalleerd certificaat. Het MIC is een permanent uniek identiteitsbewijs voor de telefoon.
Veilige SRST-referentie	Nadat u een SRST-referentie voor beveiliging hebt geconfigureerd in Cisco Unified Communications Manager Administration hebt gereset, voegt de TFTP-server het SRST-referentiebestand toe. Een veilige telefoon gebruikt vervolgens een TLS-verbinding om de referentie te downloaden.
Mediacodering	Gebruikt SRTP om te zorgen dat de mediastromen tussen de telefoon en de server veilig wordt ontvangen en gelezen. Dit omvat het maken van een mediahoofdsleutel en het beveiligen van de sleutels tijdens het transport.
CAPF (Certificate Authority Proxy Function)	Implementeert delen van de certificaatgeneratieprocedure met de telefoon om te zorgen voor het genereren van sleutels en het installeren van het certificaat op de telefoon bij door de klant opgegeven certificeringsinstellingen.
Beveiligingsprofielen	Bepaalt of de telefoon onveilig, geverifieerd of gecodeerd is.

Functie	Beschrijving
Gecodeerde configuratiebestanden	Garandeert de privacy van de telefoonconfiguratiebestanden
Optionele uitschakeling van de webserverfunctionaliteit voor een telefoon	U kunt toegang verhinderen tot de telefoonwebpagina wa
Telefoon versterken	Aanvullende beveiligingsopties die u beheert via Cisco Un <ul style="list-style-type: none"> <li>• Toegang tot webpagina's voor een telefoon uitschakel</li> </ul> <p><b>Opmerking</b> U kunt de huidige instellingen weergeven voor Configuratiemenu van de telefoon te gaan.</p>
802.1X-verificatie	De telefoon kan 802.1X-verificatie gebruiken om te verzo
AES 256-codering	Bij verbinding met Cisco Unified Communications Manager en SIP voor signalering en mediacodering. Zo kunnen tele cijfers conform SHA-2-standaarden (Secure Hash Algorithm cijfers zijn): <ul style="list-style-type: none"> <li>• Voor TLS-verbindingen: <ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_S</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_S</li> </ul> </li> <li>• Voor sRTP: <ul style="list-style-type: none"> <li>• AEAD_AES_256_GCM</li> <li>• AEAD_AES_128_GCM</li> </ul> </li> </ul> <p>Voor meer informatie raadpleegt u de documentatie bij Cis</p>
Elliptic Curve Digital Signature Algorithm (ECDSA)-certificaten	Als onderdeel van het CC-certificaat (Common Criteria), z toegevoegd. Dit geldt voor alle VOS-producten (Sprakbes

**Verwante onderwerpen**

[Cisco Unified Communications Manager Documentatie](#)

## 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** Kies op de telefoon **Instellingen**.

**Stap 3** 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 4** Kies **LSC** en druk op **Selecteren** of **Bijwerken**.

De telefoon vraagt om een verificatiereeks.

**Stap 5** 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.

## 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 "beschermd" status krijgen. Nadat een telefoon is beschermd, kan deze worden geconfigureerd om een indicatietoon af te spelen aan het begin van een gesprek:

- Beschermd telefoon: als u de status van een veilige telefoon wilt wijzigen in beschermd, schakelt u het selectievakje Beschermd telefoon in in het telefoonconfiguratievenster in Cisco Unified Communications Manager Administration (**Apparaat > Telefoon**).
- Beveiligde indicatietoon afspelen: als u wilt dat de beschermd 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 <code>Does not meet Security Level, call rejected</code> (beveiligingsniveau onvoldoende en gesprek ge
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.

## Codering voor inbreken bieden

Cisco Unified Communications Manager controleert de telefoonbeveiligingsstatus wanneer conferenties tot stand worden gebracht. De beveiligingsaanduiding voor de conferentie wordt gewijzigd of de voltooiing van het gesprek wordt geblokkeerd om de integriteit en beveiliging in het systeem te handhaven.

Een gebruiker kan niet inbreken in een gecodeerd gesprek als de telefoon die wordt gebruikt voor inbreken, niet is geconfigureerd voor codering. Wanneer het inbreken mislukt, wordt een herkiestoon (snelle bezettoon) afgespeeld op de telefoon waarop het inbreken is gestart.

Als de telefoon van de initiator is geconfigureerd voor versleuteling, kan de initiator inbreken in een onbeveiligd gesprek via de gecodeerde telefoon. Na het inbreken wordt het gesprek in Cisco Unified Communications Manager als niet-beveiligd geclassificeerd.

Als de telefoon van de initiator is geconfigureerd voor versleuteling, kan de initiator inbreken in een gecodeerd gesprek en op de telefoon wordt aangegeven dat het gesprek is gecodeerd.

## WLAN-beveiliging

Omdat alle WLAN-apparaten die binnen het bereik zijn al het andere WLAN-verkeer kunnen ontvangen, is veilige gesproken communicatie van cruciaal belang in WLAN's. Om ervoor te zorgen dat indringers het spraakverkeer niet manipuleren of onderscheppen, ondersteunt de Cisco SAFE Security-architectuur de Cisco IP-telefoon en Cisco Aironet-toegangspunten. Zie voor meer informatie over beveiliging in netwerken [http://www.cisco.com/en/US/netsol/ns744/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html).

De Cisco Wireless IP-telefonie-oplossing biedt draadloze netwerkbeveiliging die ongeautoriseerde aanmeldingen en verstoorde communicatie voorkomt door de volgende verificatiemethoden te gebruiken die worden ondersteund door de draadloze Cisco IP-telefoon:

- Open verificatie: een draadloos apparaat kan verificatie aanvragen in een open systeem. Het toegangspunt dat het verzoek ontvangt, verleent verificatie voor een aanvrager of alleen voor aanvragers in een lijst met gebruikers. De communicatie tussen het draadloze apparaat en het toegangspunt kan niet-gecodeerd zijn of apparaten kunnen WEP-sleutels (Wired Equivalent Privacy) gebruiken om beveiliging te bieden. Apparaten die gebruikmaken van WEP proberen alleen te verifiëren met een toegangspunt dat van WEP gebruikmaakt.
- Verificatie met Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST): deze client-serverbeveiligingsarchitectuur codeert EAP transacties binnen een TLS-tunnel (Transport Level Security) tussen het toegangspunt en de RADIUS-server, zoals de Cisco ACS-server (Access Control Server).

De TLS-tunnel gebruikt PAC (Protected Access Credentials) voor de verificatie tussen de client (telefoon) en de RADIUS-server. De server verstuurt een Authority ID (AID) naar de client (telefoon), die vervolgens de juiste PAC selecteert. De client (telefoon) retourneert een PAC-Opaque naar de RADIUS-server. De server decodeert de PAC met de hoofdsleutel. Beide eindpunten bevatten nu de PAC-sleutel en een TLS-tunnel wordt gemaakt. EAP-FAST ondersteunt automatische PAC-levering, maar u moet dit inschakelen op de RADIUS-server.



#### Opmerking

In de Cisco-ACS verloopt de PAC standaard over één week. Als de telefoon een verlopen PAC heeft, duurt verificatie met de RADIUS-server langer terwijl de telefoon een nieuwe PAC krijgt. Om vertragingen in de PAC-levering te voorkomen stelt u de PAC-vervalperiode in op 90 dagen of meer op de ACS-of RADIUS-server.

- EAP-TLS-verificatie (Extensible Authentication Protocol-Transport Layer Security): EAP-TLS vereist een clientcertificaat voor verificatie en netwerktoegang. Voor vaste EAP-TLS kan het clientcertificaat de MIC van de telefoon of een LSC zijn. LSC is het aanbevolen clientverificatiecertificaat voor vaste EAP-TLS.
- Protected Extensible Authentication Protocol (PEAP): Cisco's eigen op wachtwoorden gebaseerde wederzijdse verificatieschema tussen de client (telefoon) en een RADIUS-server. Cisco IP-telefoon kan PEAP gebruiken voor verificatie met het draadloze netwerk. Alleen PEAP-MSCHAPV2 wordt ondersteund. PEAP-GTC wordt niet ondersteund.

De volgende verificatieschema's gebruiken de RADIUS-server om verificatiesleutels te beheren:

- WPA/WPA2: gebruikt RADIUS-serverinformatie voor het genereren van unieke sleutels voor de verificatie. Omdat deze sleutels zijn gegenereerd op de centrale RADIUS-server, biedt WPA/WPA2 betere beveiliging dan de vooraf gedeelde WPA-sleutels die op de telefoon en het toegangspunt zijn opgeslagen.
- Snelle beveiligde roaming: gebruikt de RADIUS-server en de gegevens van een draadloze domeinserver (WDS) voor het beheren en verifiëren van sleutels. De WDS maakt een cache met veiligheidsgegevens voor clientapparaten met CCKM-ondersteuning voor snelle en beveiligde verificatie. De Cisco IP-telefoon 8800-serie ondersteunt 802.11r (FT). Zowel 11r (FT) als CCKM worden ondersteund voor snelle beveiligde roaming. Maar Cisco raadt aan om de 802.11r (FT)-methode te gebruiken.

Met WPA/WPA2 en CCKM worden coderingssleutels niet ingevoerd op de telefoon, maar automatisch afgeleid tussen het toegangspunt en de telefoon. Maar de EAP-gebruikersnaam en het wachtwoord die worden gebruikt voor de verificatie, moeten worden ingevoerd op elke telefoon.

Om ervoor te zorgen dat spraakverkeer veilig is, ondersteunt de Cisco IP-telefoon de standaarden WEP, TKIP en AES (Advanced Encryption) voor codering. Als deze mechanismen worden gebruikt voor versleuteling, worden zowel de SIP-signaleringspakketten als Real-Time Transport Protocol (RTP) spraakpakketten gecodeerd tussen het toegangspunt en de Cisco IP-telefoon.

### WEP

Als WEP wordt gebruikt in het draadloze netwerk vindt verificatie plaats via open of gedeelde sleutelverificatie op het toegangspunt. De WEP-sleutel die is ingesteld op de telefoon moet overeenkomen met de WEP-sleutel die is geconfigureerd op het toegangspunt voor geslaagde verbindingen. De Cisco IP-telefoon ondersteunt WEP-sleutels die gebruikmaken van 40-bits of 128-bits codering en blijven ongewijzigd op de telefoon en het toegangspunt.

EAP en CCKM-verificatie kunnen WEP-sleutels gebruiken voor codering. De RADIUS-server beheert de WEP-sleutel en geeft na verificatie een unieke sleutel door aan het toegangspunt voor het coderen van alle spraakpakketten. Deze WEP-sleutels kunnen veranderen met elke verificatie.

### TKIP

WPA en CCKM werken met TKIP-codering die verschillende verbeteringen heeft ten opzichte van WEP. TKIP biedt sleutelcodering per pakket en langere initialisatievectoren (IV's) die de codering versterken. Bovendien zorgt een Message Integrity Check (MIC) ervoor dat gecodeerde pakketten niet worden gewijzigd. TKIP voorkomt de voorspelbaarheid van WEP waarmee indringers de WEP-sleutel decoderen.

### AES

Een coderingsmethode die wordt gebruikt voor WPA2-verificatie. Deze nationale standaard voor codering gebruikt een symmetrisch algoritme dat dezelfde sleutel voor codering en decodering heeft. AES werkt met CBC-codering (Cipher Blocking Chain) van 128-bits groot, die minimaal de sleutelgrootten 128, 192 en 256 bits ondersteunt. De Cisco IP-telefoon ondersteunt een sleutelgrootte van 256 bits.



---

**Opmerking** De Cisco IP-telefoon biedt geen ondersteuning voor Cisco Key Integrity Protocol (CKIP) met CMIC.

---

Verificatie en coderingschema's worden ingesteld binnen het draadloze LAN-netwerk. VLAN's zijn geconfigureerd in het netwerk en op de toegangspunten en geven verschillende verificatie- en coderingscombinaties. Een SSID wordt gekoppeld aan een VLAN en het specifieke verificatie- en coderingschema. Voor een geslaagde verificatie van draadloze clientapparaten moet u dezelfde SSID's configureren met de verificatie- en coderingschema's op de toegangspunten en op de Cisco IP-telefoon.

Sommige verificatieschema's vereisen specifieke coderingstypen. Met Open verificatie kunt u statische WEP voor codering gebruiken met extra beveiliging. Maar als u verificatie met gedeelde sleutels gebruikt, moet u statische WEP voor codering instellen een WEP-sleutel configureren op de telefoon.



---

**Opmerking**

- Wanneer u vooraf gedeelde WPA-sleutels of vooraf gedeelde WPA2-sleutels gebruikt, moet de vooraf gedeelde sleutel statisch zijn ingesteld op de telefoon. Deze sleutels moeten overeenkomen met de sleutels op het toegangspunt.
- De Cisco IP-telefoon biedt geen ondersteuning voor automatische EAP-onderhandeling. Als u de EAP-FAST-modus wilt gebruiken, moet u deze opgeven.

---

De volgende tabel bevat een lijst met verificatie- en coderingschema's die zijn geconfigureerd op de Cisco Aironet-toegangspunten die worden ondersteund door de Cisco IP-telefoon. De tabel geeft de netwerkconfiguratie-optie weer voor de telefoon die met de toegangspuntconfiguratie overeenkomt.

Tabel 3: Verificatie- en coderingschema's

Configuratie Cisco IP-telefoon	Configuratie toegangspunt			
	Beveiliging	Toetsbeheer	Versleuteling	Snelle roaming
Geen	Geen	Geen	Geen	N.v.t
WEP	Statisch WEP	Static	WEP	N.v.t
PSK	PSK	WPA	TKIP	Geen
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Zie voor meer informatie over het configureren van verificatie- en coderingschema's op toegangspunten de handleiding *Cisco Aironet Configuration* voor uw model en versie onder de volgende URL:

<http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243>

## Beveiliging draadloos LAN

Cisco-telefoons die Wi-Fi ondersteunen, hebben meer vereisten voor de beveiliging waarvoor extra configuratie nodig is. Deze extra stappen omvatten het installeren van certificaten en het instellen van beveiliging op de telefoons en op de Cisco Unified Communications Manager.

Voor meer informatie raadpleegt u de *beveiligingshandleiding van Cisco Unified Communications Manager*.

## Beheerpagina Cisco IP-telefoon

Cisco-telefoons die Wi-Fi ondersteunen hebben speciale webpagina's die afwijken van de pagina's voor andere telefoons. U gebruikt deze speciale webpagina's voor de configuratie van de telefoonbeveiliging wanneer het

'Simple Certificate Enrollment Protocol (SCEP) niet beschikbaar is. Gebruik deze pagina's om beveiligingscertificaten handmatig te installeren op een telefoon, om een beveiligingscertificaat te downloaden of om de datum en de tijd van de telefoon handmatig te configureren.

Deze webpagina's laten dezelfde informatie zien als andere telefoonwebpagina's, waaronder apparaatinformatie, netwerkinstellingen, logboeken en statistische informatie.

## De beheerpagina voor de telefoon configureren

De beheerwebpagina wordt ingeschakeld wanneer de telefoon van de fabriek wordt verzonden en het wachtwoord is ingesteld op Cisco. Maar als een telefoon wordt geregistreerd met Cisco Unified Communications Manager, moet de beheerwebpagina worden ingeschakeld en een nieuw wachtwoord worden geconfigureerd.

Schakel deze webpagina in en stel aanmeldgegevens in voordat u de webpagina voor het eerst gebruikt nadat de telefoon is geregistreerd.

Na het inschakelen is de beheerwebpagina toegankelijk via HTTPS-poort 8443 (<https://x.x.x.x:8443>, waarbij x.x.x.x is een IP-adres voor de telefoon is).

### Voordat u begint

Kies een wachtwoord voordat u de webpagina voor beheer inschakelt. Het wachtwoord kan een combinatie van letters of cijfers, maar moet tussen 8 en 127 tekens lang zijn.

Uw gebruikersnaam is permanent ingesteld op beheerder.

### Procedure

---

- Stap 1** Selecteer in Cisco Unified Communications Manager Administration **Apparaat > Telefoon**.
  - Stap 2** Ga naar de telefoon.
  - Stap 3** Stel in **Productspecifieke configuratie-indeling** de parameter **Webbeheerder** in op **Ingeschakeld**.
  - Stap 4** Voer in het veld **Beheerderswachtwoord** een wachtwoord in.
  - Stap 5** Selecteer **Opslaan** en klik op **OK**.
  - Stap 6** Selecteer **Config toepassen** en klik op **OK**.
  - Stap 7** Start de telefoon opnieuw.
- 

## Webpagina telefoonbeheer openen

Wanneer u toegang wilt tot de webpagina's voor telefoonbeheer, moet u de beheerderspoort opgeven.

### Procedure

---

- Stap 1** Het IP-adres van de telefoon verkrijgen:
  - Selecteer in Cisco Unified Communications Manager Administration **Apparaat > Telefoon** en zoek de telefoon. Telefoon die zijn aangemeld bij Cisco Unified Communications Manager, geven het IP-adres weer in het venster **Telefoons zoeken en vermelden** en boven aan het **telefoonconfiguratievenster**.
- Stap 2** Open een webbrowser en voer de volgende URL in waarbij *IP-adres* het IP-adres is van de Cisco IP-telefoon.

`https://<IP_address>:8443`

**Stap 3** Voer in het veld Wachtwoord uw wachtwoord in.

**Stap 4** Klik op **Verzenden**.

---

### Een gebruikerscertificaat installeren via de webpagina voor telefoonbeheer

U kunt een gebruikerscertificaat handmatig installeren op de telefoon als Simple Certificate Enrollment Protocol (SCEP) niet beschikbaar is.

Het vooraf geïnstalleerde Manufacturing Installed Certificate (MIC) kan worden gebruikt als het gebruikerscertificaat voor EAP TLS.

Nadat het gebruikerscertificaat wordt geïnstalleerd, moet u aan het toevoegen aan de vertrouwde lijst van de RADIUS-server.

#### Voordat u begint

Voordat u een gebruikerscertificaat voor een telefoon kunt installeren, moet u:

- Een gebruikerscertificaat op uw computer opslaan. Het certificaat moet de PKCS #12-indeling hebben.
- Het wachtwoord van het certificaat ophalen.

#### Procedure

---

**Stap 1** Selecteer **Certificaten** op de webpagina voor telefoonbeheer.

**Stap 2** Blader naar het certificaat op uw computer.

**Stap 3** In het veld **Wachtwoord ophalen** voert u het certificaatwachtwoord in.

**Stap 4** Klik op **Uploaden**.

**Stap 5** Start de telefoon opnieuw nadat het uploaden voltooid is.

---

### Een certificaat voor de verificatieserver installeren via de webpagina voor telefoonbeheer

U kunt een certificaat voor de verificatieserver handmatig installeren op de telefoon als Simple Certificate Enrollment Protocol (SCEP) niet beschikbaar is.

Voor EAP-TLS moet de het CA-basiscertificaat dat het certificaat RADIUS-server heeft afgegeven, zijn geïnstalleerd.

#### Voordat u begint

Voordat u een certificaat op een telefoon kunt installeren, moet u een certificaat voor de verificatieserver op uw computer opgeslagen hebben. Het certificaat moet zijn gecodeerd in PEM (Base-64) of DER.

#### Procedure

---

**Stap 1** Selecteer **Certificaten** op de webpagina voor telefoonbeheer.

**Stap 2** Ga naar het veld **Verificatieserver CA (beheerderswebpagina)** en klik op **Installeren**.

**Stap 3** Blader naar het certificaat op uw computer.

**Stap 4** Klik op **Uploaden**.

**Stap 5** Start de telefoon opnieuw nadat het uploaden voltooid is.

Als u meer dan één certificaat wilt installeren, installeert u alle certificaten voordat u de telefoon opnieuw start.

---

## Een beveiligingscertificaat handmatig verwijderen van de webpagina voor telefoonbeheer

U kunt een beveiligingscertificaat handmatig verwijderen van de telefoon als Simple Certificate Enrollment Protocol (SCEP) niet beschikbaar is.

### Procedure

---

**Stap 1** Selecteer **Certificaten** op de webpagina voor telefoonbeheer.

**Stap 2** Zoek het certificaat op de pagina **Certificaten**.

**Stap 3** Klik op **Verwijderen**.

**Stap 4** Start de telefoon opnieuw nadat de verwijdering is voltooid.

---

## Handmatig instellen van datum en tijd op de telefoon

Met certificaatgebaseerde verificatie moet de telefoon de juiste datum en tijd weergeven. Een verificatieserver controleert de datum en tijd op de telefoon tegen de vervaldatum van het certificaat. Als de datums en tijden van de telefoon en de server niet overeenkomen, werkt de telefoon niet meer.

Gebruik deze procedure om de datum en tijd op de telefoon handmatig in te stellen als de telefoon niet de juiste informatie van uw netwerk ontvangt.

### Procedure

---

**Stap 1** Schuif van de telefoonbeheerpagina naar **Datum en tijd**.

**Stap 2** Voer een van de volgende handelingen uit:

- Klik op **Telefoon instellen op lokale datum en tijd** om de telefoon te synchroniseren met een lokale server.
  - Selecteer in de velden **Datum en tijd opgeven** de maand, de dag, het jaar, het uur, de minuut en de seconde in de menu's en klik op **Telefoon instellen op specifieke datum en tijd**.
- 

## SCEP instellen

Simple Certificate Enrollment Protocol (SCEP) is de norm voor het automatisch afgeven en vernieuwen van certificaten. Hiermee wordt voorkomen dat u certificaten handmatig op uw telefoon moet installeren.

## De SCEP-productspecifieke configuratieparameters configureren

U moet de volgende SCEP-parameters configureren op de webpagina van de telefoon

- RA IP-adres
- SHA-1 of SHA-256 vingerafdruk van het CA-basiscertificaat voor de SCEP-server

De Cisco IOS Registration Authority (RA) dient als proxy voor de SCEP-server. De SCEP-client op de telefoon gebruikt de parameters die worden gedownload van Cisco Unified Communication Manager. Nadat u de parameters hebt geconfigureerd, verzendt de telefoon een SCEP `getcs`-verzoek aan de RA en het CA basiscertificaat wordt gevalideerd met de gedefinieerde vingerafdruk.

### Procedure

- 
- Stap 1** Selecteer in Cisco Unified Communications Manager Administration **Apparaat > Telefoon** .
  - Stap 2** Zoek de telefoon.
  - Stap 3** Navigeer naar het gedeelte **Productspecifieke configuratie-indeling**.
  - Stap 4** Schakel het selectievakje **WLAN SCEP-server** in om de SCEP-parameter te activeren.
  - Stap 5** Schakel het selectievakje **WLAN Root CA Fingerprint (SHA256 of SHA1)** in om de SCEP QED-parameter te activeren.
- 

## Ondersteuning voor Simple Certificate Enrollment Protocol-server (SCEP)

Als u een SCEP-server (Simple Certificate Enrollment Protocol) gebruikt, kan de server automatisch uw gebruikers- en servercertificaten onderhouden. Configureer op de SCEP-server de SCEP Registration Agent (RA) voor:

- Fungeren als een vertrouwd PKI-punt
- Fungeren als een PKI RA
- Apparaatverificatie uitvoeren met een RADIUS-server

Zie de documentatie bij uw SCEP-server voor meer informatie.

## 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-suppliant. Met deze suppliant kunnen netwerkbeheerders de verbinding regelen van IP-telefoons met de LAN-switchpoorten. De huidige versie van de 802.1X-suppliant 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](#)



## Over de vertaling

Cisco biedt voor sommige gebieden lokalisatie aan voor deze content. De vertalingen worden echter alleen aangeboden ter informatie. Als er sprake is van inconsistentie, heeft de Engelse versie van de content de voorkeur.