



## Beveiliging Cisco IP-telefoon

- [Beveiligingsverbeteringen voor uw telefoonnetwerk, op pagina 1](#)
- [Ondersteunde beveiligingsfuncties, op pagina 2](#)

### 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 hoger <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>.

- *Beveiligingsoverzicht van Cisco IP-telefoon 7800- en 8800-serie* (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.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.

De Cisco IP-telefoon 8800-serie is compatibel met Federal Information Processing Standard (FIPS). Om correct te kunnen werken vereist de FIPS-modus een steutelomvang van 2048 bits of meer. Als het certificaat 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.

Als de telefoon een LSC heeft, moet u de LSC-sleutelgrootte bijwerken tot 2048 bits of meer voordat u FIPS inschakelt.

In de volgende tabel ziet u een overzicht van de beveiligingsfuncties die door de telefoons worden ondersteund. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Als u de huidige beveiligingsinstellingen op een telefoon wilt zien, inclusief de beveiligde modus, de vertrouwde lijst en 802.1X-verificatie, drukt u op **Toepassingen**  en kiest u **Beheerdersinstellingen** > **Beveiligingsinstellingen**.

**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.
Codering afbeelding	Gecodeerde binaire bestanden (met de extensie .sebn) 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 Cisco IP-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. In Cisco Unified Communications Manager worden telefoons pas geregistreerd, als ze kunnen worden geverifieerd.

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.
Bestandscodering	Codering voorkomt dat vertrouwelijke informatie wordt weergegeven, terwijl het bestand op weg naar de telefoon is. Bovendien valideert de telefoon 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 Cisco IP-telefoon vereist een uniek tijdens de fabricage geïnstalleerd certificaat (Manufacturing Installed Certificate, MIC) voor apparaatverificatie. MIC levert een permanent uniek identiteitsbewijs voor de telefoon waarmee Cisco Unified Communications Manager de telefoon kan verifiëren.
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 mediahoofdsleutelbaar 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.
Beveiligingsprofiel	Bepaalt of de telefoon onveilig, geverifieerd, gecodeerd of beveiligd is. Andere vermeldingen in deze tabel beschrijven beveiligingsfuncties.
Gecodeerde configuratiebestanden	Garandeert de privacy van de telefoonconfiguratiebestanden.
Optionele webserver uitschakelen voor een telefoon	Omwille van de beveiliging kunt u toegang tot de webpagina's voor een telefoon (met verschillende operationele statistische gegevens voor de telefoon) en de Self Care Portal verhinderen.

Functie	Beschrijving
Telefoon versterken	<p>Aanvullende beveiligingsopties die u beheert via Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> <li>• PC-poort uitschakelen</li> <li>• Gratuitous ARP (GARP) uitschakelen</li> <li>• PC Voice VLAN-toegang uitschakelen</li> <li>• Toegang tot de menu's met instellingen uitschakelen of beperkte toegang bieden die toegang tot het menu Voorkeuren toestaat en het opslaan van alleen volumewijzigingen</li> <li>• Toegang tot webpagina's voor een telefoon uitschakelen</li> <li>• Bluetooth-accessoirepoort uitschakelen</li> <li>• TLS-cijfers beperken</li> </ul>
802.1X-verificatie	De Cisco IP-telefoon kan 802.1X-verificatie gebruiken om te verzoeken om toegang tot het netwerk. Zie <a href="#">802.1X-verificatie, op pagina 27</a> voor meer informatie.
SIP-Failover voor SRST beveiligen	Nadat u een SRST-referentie (Survivable Remote Site Telephony) 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.
Codering signalering	Zorgt ervoor dat alle SIP-signaleringsberichten die worden verzonden tussen het apparaat en de Cisco Unified Communications Manager-server worden gecodeerd.
Waarschuwing bijwerken vertrouwde lijst	Wanneer de vertrouwde lijst op de telefoon wordt gewijzigd, ontvangt de Cisco Unified Communications Manager een waarschuwing om aan te geven of het bijwerken al dan niet is gelukt. Raadpleeg de volgende tabel voor meer informatie.
AES 256-codering	<p>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 cijfers omvatten:</p> <ul style="list-style-type: none"> <li>• Voor TLS-verbindingen: <ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</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 Cisco Unified Communications Manager.</p>
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 (Sprakbesturingssysteem) van versie CUCM 11.5 en hoger.

De volgende tabel bevat de waarschuwingsberichten voor het bijwerken van de vertrouwde lijst en de betekenis daarvan. Voor meer informatie raadpleegt u de documentatie bij Cisco Unified Communications Manager.

**Tabel 2: Waarschuwingsberichten bijwerken vertrouwde lijst**

Code en bericht	Beschrijving
1 - TL_SUCCESS	Nieuwe CTL en/of ITL ontvangen
2 - CTL_INITIAL_SUCCESS	Nieuwe CTL ontvangen, geen bestaande TL
3 - ITL_INITIAL_SUCCESS	Nieuwe ITL ontvangen, geen bestaande TL
4 - TL_INITIAL_SUCCESS	Nieuwe CTL en ITL ontvangen, geen bestaande TL
5 - TL_FAILED_OLD_CTL	Bijwerken nieuwe CTL mislukt, maar vorige TL bestaat
6 - TL_FAILED_NO_TL	Bijwerken nieuwe TL mislukt en oude TL bestaat niet
7 - TL_FAILED	Algemene fout
8 - TL_FAILED_OLD_ITL	Bijwerken nieuwe ITL mislukt, maar vorige TL bestaat
9 - TL_FAILED_OLD_TL	Bijwerken nieuwe TL mislukt, maar vorige TL bestaat

Het menu Beveiligingsinstellingen biedt informatie over de verschillende instellingen. Het menu biedt ook toegang tot het menu Vertrouwde lijst en geeft aan of het CTL- of ITL-bestand is geïnstalleerd op de telefoon.

In de volgende tabel worden de opties in het menu Beveiligingsinstellingen beschreven.

**Tabel 3: Menu Beveiligingsinstellingen**

Optie	Beschrijving	Wijzigen
Beveiligingsmodus	Geeft de beveiligde modus weer die voor de telefoon is ingesteld.	Selecteer in Cisco Unified Communications Manager Administration <b>Apparaat &gt; Telefoon</b> . De instelling wordt weergegeven in het gedeelte Protocolspecifieke informatie van het venster Telefoonconfiguratie.
LSC	Geeft aan of een lokaal significant certificaat dat wordt gebruikt voor beveiligingsfuncties, al dan niet op de telefoon is geïnstalleerd (Ja/Nee).	Voor meer informatie over het beheren van de LSC voor uw telefoon, raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

Optie	Beschrijving	Wijzigen
Vertrouwde lijst	<p>De vertrouwde lijst biedt submenu's voor de CTL-, ITL- en ondertekende configuratiebestanden.</p> <p>Het submenu CTL-bestand geeft de inhoud van het CTL-bestand weer. Het submenu ITL-bestand geeft de inhoud van het ITL-bestand weer.</p> <p>Het menu Vertrouwde lijst geeft ook de volgende informatie:</p> <ul style="list-style-type: none"> <li>• CTL-handtekening: de SHA1-hash van het CTL-bestand</li> <li>• Unified CM/TFTP-Server: de naam van de Cisco Unified Communications Manager en de TFTP-Server die gebruikmaakt van de telefoon. Een certificaatpictogram wordt weergegeven als een certificaat voor deze server is geïnstalleerd.</li> <li>• CAPF-server: de naam van de CAPF-server die gebruikmaakt van de telefoon. Een certificaatpictogram wordt weergegeven als een certificaat voor deze server is geïnstalleerd.</li> <li>• SRST-router: het IP-adres van de vertrouwde SRST-router die de telefoon kan gebruiken. Een certificaatpictogram wordt weergegeven als een certificaat voor deze server is geïnstalleerd.</li> </ul>	Zie <a href="#">Een lokaal significant certificaat instellen, op pagina 7</a> voor meer informatie.
802.1X-verificatie	Hiermee kunt u 802.1X-verificatie voor deze telefoon inschakelen.	Zie <a href="#">802.1X-verificatie, op pagina 27</a> .

**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** Druk op de telefoon op **Toepassingen** .

**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.

---

## 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 alleen ondersteund voor verbindingen tussen twee telefoons. Bepaalde functies zoals conferentiegesprekken en gedeelde lijnen, zijn niet beschikbaar wanneer beveiligd bellen is geconfigureerd.

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 4: Beveiligingsrestricties met conferentiegesprekken**

Initiator beveiligingsniveau telefoon	Gebroekte 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 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. Zowel de PEAP-MSCHAPV2 als PEAP-GTC verificatiemethoden worden 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 5: 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
PEAP-GTC	PEAP-GTC	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>

## Verificatiemodus instellen

Als u de verificatiemodus voor dit profiel wilt selecteren, voert u de volgende stappen uit:

## Procedure

---

**Stap 1** Kies het netwerkprofiel die u wilt configureren.

**Stap 2** Kies de verificatiemodus.

**Opmerking** Afhankelijk van wat u hebt geselecteerd, moet u aanvullende opties configureren voor draadloze beveiliging of draadloze codering. Zie [WLAN-beveiliging, op pagina 11](#) voor meer informatie.

**Stap 3** Klik op **Opslaan** om de wijziging aan te brengen.

---

## Aanmeldingsgegevens draadloze beveiliging

Wanneer uw netwerk EAP-FAST en PEAP voor gebruikersverificatie gebruikt, moet u de gebruikersnaam en het wachtwoord configureren als dit verplicht is voor de RADIUS (Remote Authentication Dial-In User Service) en de telefoon.



**Opmerking** Als u domeinen binnen het netwerk gebruikt, moet u de gebruikersnaam en de domeinnaam invoeren in de indeling: *domein\gebruikersnaam*.

---

De volgende acties kunnen tot gevolg hebben dat het bestaande Wi-Fi-wachtwoord wordt gewist:

- Een ongeldige gebruikers-id of een ongeldig wachtwoord invoeren
- Een ongeldige of verlopen Root CA installeren als het EAP-type is ingesteld op PEAP-MSCHAPV2 of PEAP-GTC
- Het EAP-type uitschakelen op de RADIUS-server die door de telefoon wordt gebruikt voor het wijzigen van een telefoon in het nieuwe EAP-type

Als u EAP-typen wilt wijzigen, doet u het volgende in de vermelde volgorde:

- Schakel de nieuwe EAP-typen in op de RADIUS.
- Wijzig het EAP-type op een telefoon in het nieuwe EAP-type.

Laat het huidige EAP-type geconfigureerd op de telefoon totdat het nieuwe EAP-type is ingeschakeld op de RADIUS-server. Wanneer het nieuwe EAP-type is ingeschakeld op de RADIUS-server, kunt u EAP-type van de telefoon wijzigen. Zodra alle telefoons zijn gewijzigd in het nieuwe EAP-type, kunt u het vorige EAP-type uitschakelen.

## Gebruikersnaam en wachtwoord instellen

Als u de gebruikersnaam of het wachtwoord wilt opgeven of wijzigen voor de netwerkprofiel, moet u dezelfde gebruikersnaam en dezelfde tekenreeks van het wachtwoord gebruiken die zijn geconfigureerd in de RADIUS-server. De maximale lengte van de gebruikersnaam of het wachtwoord is 64 tekens.

Als u de gebruikersnaam en het wachtwoord wilt instellen in draadloze veiligheidsgegevens, voert u de volgende stappen uit:

### Procedure

---

- Stap 1** Kies het netwerkprofiel.
  - Stap 2** Voer de netwerkgebruikersnaam voor dit profiel in in het veld Gebruikersnaam.
  - Stap 3** Voer het netwerk wachtwoord voor dit profiel in in het veld Wachtwoord.
  - Stap 4** Klik op **Opslaan** om de wijziging aan te brengen.
- 

## Instellingen vooraf gedeelde sleutel

Gebruik de volgende secties om u te helpen bij het instellen van vooraf gedeelde sleutels.

### Vooraf gedeelde sleutelindelingen

De Cisco IP-telefoon ondersteunt ASCII- en hexadecimale indelingen. Wanneer u een vooraf gedeelde WPA-sleutel instelt, moet u een van deze indelingen gebruiken:

#### Hexadecimaal

Voor hexadecimale toetsen voert u 64 hexadecimale cijfers (0-9 en A-F) in; bijvoorbeeld, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

#### ASCII

Voor ASCII-sleutels voert u een tekenreeks in die gebruikmaakt van 0-9, A-Z (hoofdletters en kleine letters), met inbegrip van symbolen, en die 8 tot 63 tekens lang is; bijvoorbeeld, GREG12356789ZXYW

### PSK instellen

Als u een PSK wilt instellen in het gedeelte voor draadloze aanmeldingsgegevens, voert u de volgende stappen uit:

### Procedure

---

- Stap 1** Kies het netwerkprofiel dat de vooraf gedeelde WPA-sleutel of een vooraf gedeelde WPA2-sleutel inschakelt.
  - Stap 2** Voer de juiste sleutel in het gebied Sleuteltype in.
  - Stap 3** Voer een ASCII-tekenreeks of hexadecimale cijfers in in het veld Wachtwoordzin/Vooraf gedeelde sleutel.
  - Stap 4** Klik op **Opslaan** om de wijziging aan te brengen.
- 

## Draadloze codering

Als u uw draadloze netwerk WEP-codering gebruikt en u de verificatiemodus Open + WEP instelt, moet u een ASCII- of hexadecimale WEP-sleutel invoeren.

De WEP-sleutels voor de telefoon moeten overeenkomen met de WEP-sleutels die zijn toegewezen aan het toegangspunt. Cisco IP-telefoon en Cisco Aironet-toegangspunten ondersteunen beide 40-bits en 128-bits coderingssleutels.



## Indelingen WEP-sleutel

Wanneer u een WEP-sleutel instelt, moet u een van deze indelingen gebruiken:

### Hexadecimaal

Voor hexadecimale sleutels gebruikt u een van de sleutelgroottes:

#### 40-bits

U voert een 10-cijferige tekenreeks in voor een coderingssleutel die gebruikmaakt van de hexadecimale tekens (0-9 en A-F); bijvoorbeeld, ABCD123456.

#### 128-bits

U voert een 26-cijferige tekenreeks in voor een coderingssleutel die gebruikmaakt van de hexadecimale tekens (0-9 en A-F); bijvoorbeeld, AB123456789CD01234567890EF.

### ASCII

Voor ASCII-sleutels voert u een tekenreeks in die gebruikmaakt van 0-9, A-Z (hoofdletters en kleine letters), en alle symbolen, met een van de volgende sleutelgroottes:

#### 40-bits

U voert u een tekenreeks van 5 tekens in; bijvoorbeeld GREG5.

#### 128-bits

U voert u een tekenreeks van 13 tekens in; bijvoorbeeld GREGSSECRET13.

## WEP-sleutels instellen

Ga als volgt te werk om WEP-sleutels in te stellen.

### Procedure

- 
- |               |  |
|---------------|--|
| <b>Stap 1</b> | Kies het netwerkprofiel dat Open+WEP of Shared+WEP gebruikt.   |
| <b>Stap 2</b> | Voer de juiste sleutel in het gebied Sleuteltype in.   |
| <b>Stap 3</b> | Kies een van deze tekenlengtes in het gedeelte Sleutelgrootte: <ul style="list-style-type: none"><li>• 40</li><li>• 128</li></ul>  |
| <b>Stap 4</b> | Voer de juiste sleuteltekenreeks in op basis van het geselecteerde Type sleutel en Sleutelgrootte in het veld Coderingssleutel. Zie <a href="#">Indelingen WEP-sleutel, op pagina 17</a> . |
| <b>Stap 5</b> | Klik op <b>Opslaan</b> om de wijziging aan te brengen.   |
- 

## CA-certificaat exporteren van ACS met Microsoft Certificate Services

Exporteer het CA-basiscertificaat van de ACS-server. Zie voor meer informatie de documentatie van CA of RADIUS.

## Manufacturing Installed Certificate

Cisco heeft in de fabriek een Manufacturing Installed Certificate (MIC) in de telefoon opgenomen.

Tijdens EAP-TLS-verificatie moet de ACS-server het vertrouwen van de telefoon controleren en verifieert de telefoon het vertrouwen van de ACS-server.

Voor het controleren van de MIC moeten het basiscertificaat van fabrikant en het Manufacturing Certificate Authority-certificaat (CA) worden geëxporteerd van een Cisco IP-telefoon en op de Cisco ACS-server worden geïnstalleerd. Deze twee certificaten zijn onderdeel van de vertrouwde certificaatketen om de MIC te controleren die wordt gebruikt door de Cisco ACS-server.

Om het Cisco ACS-certificaat te controleren moeten een vertrouwd onderliggend certificaat (indien van toepassing) en het basiscertificaat (gemaakt op basis van een CA) op de Cisco ACS-server worden geëxporteerd en worden geïnstalleerd op de telefoon. Deze certificaten zijn onderdeel van de vertrouwde certificaatketen die wordt gebruikt om het vertrouwen van het certificaat van de ACS-server te controleren.

## Door gebruiker geïnstalleerd certificaat

Als u een door een gebruiker geïnstalleerd certificaat wilt gebruiken, wordt een Certificate Signing Request (CSR) gegenereerd en naar de CA verzonden voor goedkeuring. Het gebruikerscertificaat kan ook worden gegenereerd door de CA zonder een CSR.

Tijdens EAP-TLS-verificatie wordt door de ACS-server het vertrouwen van de telefoon gecontroleerd en verifieert de telefoon het vertrouwen van de ACS-server.

Om de authenticiteit te controleren van het door de gebruiker geïnstalleerde certificaat, moet u een vertrouwd onderliggend certificaat installeren (indien van toepassing) en het basiscertificaat van de CA die het certificaat van de gebruiker op de Cisco ACS-server heeft goedgekeurd. Deze certificaten zijn onderdeel van de vertrouwde certificaatketen die is gebruikt om het vertrouwen van het door de gebruiker geïnstalleerde certificaat te controleren.

Om het Cisco ACS-certificaat te controleren exporteert u een vertrouwd onderliggend certificaat (indien van toepassing) en het basiscertificaat (gemaakt op basis van een CA) op de Cisco ACS-server en de geëxporteerde certificaten worden geïnstalleerd op de telefoon. Deze certificaten zijn onderdeel van de vertrouwde certificaatketen die wordt gebruikt om het vertrouwen van het certificaat van de ACS-server te controleren.

## Certificaten EAP-TLS-verificatie installeren

Voer de volgende stappen uit om verificatiecertificaten voor EAP-TLS te installeren.

### Procedure

- 
- Stap 1** Stel op de webpagina van de telefoon de Cisco Unified Communications Manager-datum en tijd in op de telefoon.
- Stap 2** Als u Manufacturing Installed Certificate (MIC) gebruikt:
- Exporteer via de webpagina van de telefoon het CA-basiscertificaat en het CA-certificaat van de fabrikant.
  - Installeer in Internet Explorer certificaten op de Cisco ACS-server en bewerkt de vertrouwde lijst.
  - Importeer de basis-CA naar de telefoon.

Zie voor meer informatie:

- [Exporteren en certificaten installeren op ACS, op pagina 19](#)
- [CA-certificaat exporteren van ISE met Microsoft Certificate Services, op pagina 20](#)

**Stap 3** Stel met het hulpprogramma ACS-configuratie het gebruikersaccount in.

Zie voor meer informatie:

- [ACS-gebruikersaccount instellen en certificaat installeren, op pagina 21](#)
- *Gebruikershandleiding voor Cisco Secure ACS voor Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

---

## Datum en tijd instellen

EAP-TLS gebruikt op een certificaat gebaseerde verificatie waarvoor de interne klok op de Cisco IP-telefoon goed moet worden ingesteld. De datum en tijd op de telefoon kan veranderen wanneer deze is geregistreerd bij Cisco Unified Communications Manager.



---

**Opmerking** Als een nieuw verificatiecertificaat voor de server wordt aangevraagd en de lokale tijd achterloopt op de Greenwich Mean Time (GMT), kan de validering van het verificatiecertificaat mislukken. Cisco raadt aan dat u de lokale datum en tijd vóór de GMT instelt.

---

Ga als volgt te werk om de telefoon op de juiste lokale datum en tijd in te stellen.

### Procedure

---

**Stap 1** Selecteer **Datum en tijd** in het linkerdeelvenster.

**Stap 2** Als u de instelling in het veld **Huidige datum en tijd** op telefoon afwijkt van het veld **Lokale datum en tijd**, klikt u op **Telefoon instellen op plaatselijke datum en tijd**.

**Stap 3** Klik op **Telefoon herstarten** en vervolgens op **OK**.

---

## Exporteren en certificaten installeren op ACS

Als u MIC wilt gebruiken, exporteert u het basiscertificaat van de fabrikant en het CA-certificaat van de fabrikant en installeert u deze op de Cisco ACS-server.

Ga als volgt te werk om het basiscertificaat van de fabrikant en het CA-certificaat van de fabrikant te exporteren naar de ACS-server.

### Procedure

---

**Stap 1** Kies **Certificaten** op de telefoonwebpagina.

**Stap 2** Klik op **Exporteren** naast het basiscertificaat van fabrikant.

**Stap 3** Sla het certificaat op en kopieer het naar de ACS-server.

**Stap 4** Herhaal stap 1 en 2 voor de CA-certificaat fabrikant.

**Stap 5** Voer het bestandspad voor elk certificaat in en installeer de certificaten van de pagina **Systeemconfiguratie ACS Server**.

**Opmerking** Zie voor meer informatie over het gebruik van het hulpprogramma ACS-configuratie, de ACS online help of de *Gebruikershandleiding voor Cisco Secure ACS voor Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>).

**Stap 6** Gebruik de pagina Certificate Trust List (CTL) bewerken om certificaten toe te voegen die moeten worden vertrouwd door ACS.

---

## Exportmethoden ACS-certificaat

Afhankelijk van het type certificaat dat u uit ACS exporteert, gebruikt u een van de volgende methoden:

- Als u het CA-certificaat wilt exporteren van de ACS-server die het door de gebruiker geïnstalleerde certificaat of ACS-certificaat heeft ondertekend, zie [CA-certificaat exporteren van ISE met Microsoft Certificate Services](#), op pagina 20.
- Zie [CA-certificaat van ACS exporteren met Internet Explorer](#), op pagina 20 om het CA-certificaat te exporteren van de ACS-server die een zelf-ondertekend certificaat gebruikt.

## CA-certificaat exporteren van ISE met Microsoft Certificate Services

Gebruik deze methoden als u het CA-certificaat wilt exporteren van de ISE-server die het door de gebruiker geïnstalleerde certificaat of ISE-certificaat heeft ondertekend.

Voer de volgende stappen uit als u het CA-certificaat wilt exporteren via de webpagina van Microsoft Certificate Services.

### Procedure

---

- Stap 1** Selecteer in de webpagina van Microsoft Certificate Services **Een CA-certificaat, certificaatketen of certificaatintrekkingslijst downloaden**.
- Stap 2** Markeer op de volgende pagina het huidige CA-certificaat in het tekstvak, kies DER onder coderingsmethode en klik op **CA-certificaat downloaden**.
- Stap 3** Sla het CA-certificaat op.
- 

## CA-certificaat van ACS exporteren met Internet Explorer

Gebruik deze methode om het CA-certificaat te exporteren van de ACS-server die een zelf-ondertekend certificaat gebruikt.

Voer de volgende stappen uit als u certificaten wilt exporteren van de ACS-server met Internet Explorer.

### Procedure

---

- Stap 1** Kies in Internet Explorer, **Hulpprogramma's > Internet-opties**, en klik op het tabblad Inhoud.
- Stap 2** Klik onder Certificaten op **Certificaten** en vervolgens op het tabblad Vertrouwde basiscertificeringsinstanties.
- Stap 3** Markeer het basiscertificaat en klik op **Exporteren**. De wizard Certificaat exporteren wordt geopend.

- Stap 4** Klik op **Volgende**.
  - Stap 5** Selecteer in het volgende venster **DER encoded binary X.509 (. CER)** en klik op **Volgende**.
  - Stap 6** Geef een naam op voor het certificaat en klik op **Volgende**.
  - Stap 7** Sla het CA-certificaat dat wilt installeren op de telefoon op.
- 

### Door gebruiker geïnstalleerd certificaat aanvragen en importeren

Voer de volgende stappen uit om het certificaat aan te vragen en op de telefoon te installeren.

#### Procedure

---

- Stap 1** Kies via de webpagina van de telefoon het netwerkprofiel dat werkt met EAP-TLS en selecteer Gebruiker geïnstalleerd in het veld EAP-TLS-certificaat.
  - Stap 2** Klik op **Certificaten**.  
Het veld Algemene naam op de pagina Gebruikercertificaat moet overeenkomen met de naam van de gebruiker in de ACS-server.  
**Opmerking** U kunt het veld Algemene naam bewerken. Zorg dat het overeenkomt met de gebruikersnaam in de ACS-server. Zie [ACS-gebruikersaccount instellen en certificaat installeren, op pagina 21](#).
  - Stap 3** Voer de gegevens in die worden weergegeven op het certificaat en klik op **Indienen** voor het genereren van het Certificate Signing Request (CSR).
- 

### Basiscertificaat verificatieserver installeren

Voer de volgende stappen uit om het basiscertificaat voor de verificatieserver te installeren op de telefoon.

#### Procedure

---

- Stap 1** Exporteer het basiscertificaat van de verificatieserver van de ACS. Zie [Exportmethoden ACS-certificaat, op pagina 20](#).
  - Stap 2** Ga naar de webpagina van de telefoon en kies **Certificaten**.
  - Stap 3** Klik op **Importeren** naast het basiscertificaat van de verificatieserver.
  - Stap 4** Start de telefoon opnieuw.
- 

### ACS-gebruikersaccount instellen en certificaat installeren

Voer de volgende stappen uit om de naam van het gebruikersaccount in te stellen en het MIC-basiscertificaat voor de telefoon op de ACS te installeren.



#### Opmerking

Zie voor meer informatie over het gebruik van het hulpprogramma ACS-configuratie, de ACS online help of de *Gebruikershandleiding voor Cisco Secure ACS voor Windows*.

---

## Procedure

---

- Stap 1** Maak in het ACS-configuratiehulpprogramma op de pagina met gebruikersinstellingen een naam voor een gebruikersaccount als deze nog niet is ingesteld.
- Doorgaans bevat de gebruikersnaam aan het einde het MAC-adres voor de telefoon. Een wachtwoord is niet nodig voor EAP-TLS.
- Opmerking** Zorg dat de gebruikersnaam overeenkomt met het veld Algemene naam op de installatiepagina voor het gebruikerscertificaat. Zie [Door gebruiker geïnstalleerd certificaat aanvragen en importeren, op pagina 21](#).
- Stap 2** Schakel op de pagina Systeemconfiguratie in het gedeelte EAP-TLS deze velden in:
- **EAP-TLS toestaan**
  - **Vergelijking Certificaat CN**
- Stap 3** Voeg op de pagina ACS Certificate Authority-instellingen het Manufacturing basiscertificaat en het Manufacturing CA-certificaat toe aan de ACS-server.
- Stap 4** Schakel het Manufacturing Root-certificaat en het Manufacturing CA-certificaat in in de lijst met vertrouwde ACS-certificaten.
- 

## PEAP-instellingen

Het PEAP-protocol (Protected Extensible Authentication Protocol) gebruikt openbare sleutelcertificaten aan de serverzijde om clients te verifiëren door het maken van een gecodeerde SSL-/TLS-tunnel tussen de client en de verificatieserver.

Cisco IP-telefoon 8865 ondersteunt slechts één servercertificaat dat kan worden geïnstalleerd met SCEP of de methode voor handmatige installatie, maar niet beide methoden. De telefoon biedt geen ondersteuning voor de TFTP-methode voor het installeren van het certificaat.



- 
- Opmerking** De validatie van de serververificatie kan worden gebruikt door het importeren van het certificaat van de verificatieserver.
- 

### Voordat u begint

Voordat u PEAP-verificatie voor de telefoon configureert, moet u controleren of aan deze Cisco Secure ACS-vereisten is voldaan:

- Het ACS-basiscertificaat moet zijn geïnstalleerd.
- Een certificaat kan ook worden geïnstalleerd om servervalidatie voor PEAP in te schakelen. Maar, als een servercertificaat is geïnstalleerd dan is servervalidatie ingeschakeld.
- De instelling EAP-MSCHAPv2 toestaan moet zijn ingeschakeld.
- Gebruikersaccount en wachtwoord moeten zijn geconfigureerd.

- Voor wachtwoordverificatie kunt u de lokale ACS-database of een externe database (zoals Windows of LDAP) gebruiken.

## PEAP-verificatie inschakelen

### Procedure

- 
- Stap 1** Kies in de configuratiewebpagina van de telefoon PEAP als de verificatiemodus.
- Stap 2** Geef een gebruikersnaam en wachtwoord op.
- 

## 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.

### Verwante onderwerpen

[Webpagina Cisco IP-telefoon](#)

## 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**.
    - Druk op de telefoon op **Toepassingen** , kies **Telefoongegevens** en schuif vervolgens naar het veld IPv4-adres.
  - 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\_adres>: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** Ga naar het veld Gebruiker installeren en klik op **Installeren**.
- Stap 3** Blader naar het certificaat op uw computer.
- Stap 4** In het veld **Wachtwoord ophalen** voert u het certificaatwachtwoord in.
- Stap 5** Klik op **Uploaden**.
- Stap 6** 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. CDP herkent geen lokaal aangesloten werkstations. Cisco IP-telefoons beschikken over een EAPOL-doorgeefmechanisme. Hiermee kan een werkstation dat is verbonden met de Cisco IP-telefoon EAPOL-berichten doorgeven voor 802.1X-verificatie op de LAN-switch. Het doorgeefmechanisme zorgt dat de IP-telefoon niet fungeert als LAN-switch voor het verifiëren van een gegevenseindpunt voor toegang tot het netwerk.

Cisco IP-telefoons beschikken ook over een proxy EAPOL-uitlogmechanisme. Als de lokaal verbonden pc de verbinding met een IP-telefoon verbreekt, ziet de LAN-switch niet dat de fysieke koppeling niet meer werkt, omdat de koppeling tussen de LAN-switch en de IP-telefoon in stand blijft. Om te voorkomen dat de netwerkintegriteit in gevaar komt, stuurt de IP-telefoon een EAPOL-afmeldbericht naar de switch uit naam van de downstream-pc, waardoor de LAN-switch wordt getriggerd om de verificatievermelding voor de downstream-pc te wissen.

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

- Cisco IP-telefoon: de telefoon initieert het verzoek voor toegang tot het netwerk. Cisco IP-telefoon bevat 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 Secure Access Control Server (ACS) (of een andere verificatieserver van derden): de verificatieserver en de telefoon moeten beide worden geconfigureerd met een gedeeld geheim waarmee de telefoon wordt geverifieerd.
- 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.

- Configureer pc-poort: de 802.1X-standaard houdt geen rekening met VLAN's en beveelt aan om slechts één apparaat te verifiëren voor een specifieke switchpoort. Sommige switches (waaronder Cisco Catalyst-switches) ondersteunen echter multidomeinverificatie. De switchconfiguratie bepaalt of u een pc kunt aansluiten op de pc-poort van de telefoon.
  - Ingeschakeld: als u een switch gebruikt die multidomeinverificatie ondersteunt, kunt u de pc-poort inschakelen en een pc aansluiten. In dat geval ondersteunt de Cisco IP-telefoon de proxy-EAPOL-uitlogfunctie om de verificatie-uitwisseling tussen de switch en de aangesloten pc te controleren. Meer informatie over IEEE 802.1X-ondersteuning op Cisco Catalyst-switches vindt u in de handleidingen voor Cisco Catalyst-switchconfiguratie op: [http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)
  - Uitgeschakeld: als de switch niet meerdere met 802.1X compatibele apparaten ondersteunt op dezelfde poort, moet u de pc-poort uitschakelen als 802.1X-verificatie wordt ingeschakeld. Als u deze poort niet uitschakelt en er vervolgens een pc op aansluit, weigert de switch netwerktoegang voor de telefoon en de pc.
- 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.

## Toegang tot 802.1X-verificatie

U kunt de instellingen voor 802.1X-verificatie openen via de volgende stappen:

### Procedure

- 
- Stap 1** Druk op **Toepassingen** .
  - Stap 2** Kies **Beheerdersinstellingen** > **Beveiligingsinstellingen** > **802.1X-verificatie**.
  - Stap 3** Configureer de opties, zoals wordt beschreven in [802.1X-verificatieopties](#), op pagina 28.
  - Stap 4** Druk op **Afsluiten** om dit menu af te sluiten.
- 

### 802.1X-verificatieopties

In de volgende tabel worden de opties voor 802.1X-verificatie beschreven.

Tabel 6: Instellingen 802.1X-verificatie

Optie	Beschrijving	Wijzigen
Apparaatverificatie	<p>Hiermee wordt bepaald of 802.1X-verificatie is ingeschakeld:</p> <ul style="list-style-type: none"> <li>• Ingeschakeld: telefoon gebruikt 802.1X-verificatie om toegang tot het netwerk aan te vragen.</li> <li>• Uitgeschakeld: standaardinstelling. De telefoon gebruikt CDP voor VLAN- en netwerktoegang.</li> </ul>	Zie <a href="#">Veld Apparaatverificatie instellen</a> pagina 29.
Transactiestatus	<p>Status: hiermee wordt de status van 802.1X-verificatie weergegeven:</p> <ul style="list-style-type: none"> <li>• Verbroken: geeft aan dat 802.1X-verificatie niet is geconfigureerd op de telefoon.</li> <li>• Geverifieerd: geeft aan dat de telefoon wordt geverifieerd.</li> <li>• In de wacht: geeft aan dat het verificatieproces in behandeling is.</li> </ul> <p>Protocol: geeft de EAP-methode weer die wordt gebruikt voor 802.1X-verificatie (EAP-FAST of EAP-TLS).</p>	Alleen op het scherm. Kan niet worden geconfigureerd.

## Veld Apparaatverificatie instellen

### Procedure

- 
- Stap 1** Druk op **Toepassingen** .
- Stap 2** Kies **Beheerdersinstellingen > Beveiligingsinstellingen > 802.1X-verificatie**
- Stap 3** De optie Apparaatverificatie instellen:
- Ja
  - Nee
- Stap 4** Druk op **Toepassen**.
-



## 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.