Beveiliging Cisco IP-telefoon

- Domein- en internetinstelling, op pagina 1
- De identiteitsvraag voor SIP INVITE-berichten configureren, op pagina 4
- Ondersteuning voor RFC-8760, op pagina 5
- Auth INVITE en Auth Resync Reboot inschakelen, op pagina 5
- Ondersteuning voor aanvullende digestalgoritmen voor hotelingverificatie, op pagina 6
- De TLS-minimumwaarde beheren, op pagina 6
- De besturing van de service Webex-meetwaarden inschakelen, op pagina 7
- De besturing voor PRT uploaden bij crashservices inschakelen, op pagina 8
- Transport Layer Security (TLS), op pagina 8
- HTTPS-inrichting, op pagina 11
- De firewall inschakelen, op pagina 14
- Uw firewall configureren met extra opties, op pagina 15
- De coderingslijst configureren, op pagina 17
- Hostnaamverificatie inschakelen voor SIP via TLS, op pagina 20
- Door de client geïnitieerde modus voor beveiligingsonderhandelingen over mediaplane inschakelen, op pagina 21
- 802.1X-verificatie, op pagina 23
- Een proxyserver instellen, op pagina 25
- FIPS-modus inschakelen, op pagina 31
- Overzicht beveiliging Cisco-producten, op pagina 32

Domein- en internetinstelling

Domeinen met beperkte toegang configureren

U kunt de telefoon configureren voor het registreren, inrichting, bijwerken van de firmware en het verzenden van rapporten met alleen de opgegeven servers. Alle registraties, inrichting, upgrades en rapporten die niet de opgegeven servers gebruiken, kunnen niet op de telefoon worden uitgevoerd. Als u de te gebruiken servers opgeeft, moet u ervoor zorgen dat de servers die u in de volgende velden invoert, worden opgenomen in de lijst:

- **Profielregel**, **Profielregel B**, **Profielregel C** en **Profielregel D** op het tabblad **Inrichting**
- **Upgraderegel** en **Upgraderegel Cisco-hoofdtelefoon** op het tabblad **Inrichting**

- **Rapportregel** op het tabblad **Inrichting**
- **Aangepaste CA-regel** op het tabblad **Inrichting**
- **Proxy** en **Outbound Proxy** (Uitgaande proxy) op het tabblad **Ext (n)** (Toestel (n))

Voordat u begint

De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Systeem**.

Stap 2 Zoek in de sectie **System Configuration** (Systeemconfiguratie) naar het veld **Restricted Access Domains** (Domeinen met beperkte toegang) en voer de volledig gekwalificeerde domeinnamen (FQDN's) in voor elke server. Scheid FQDN's met komma's.

Voorbeeld:

```
voiceip.com, voiceip1.com
```

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<Restricted_Access_Domains ua="na">voiceip.com, voiceip1.com</Restricted_Access_Domains>
```

Stap 3 Klik op **Submit All Changes**.

De DHCP-opties configureren

U kunt de volgorde instellen waarin de telefoon de DHCP-opties gebruikt. Zie Ondersteuning van DHCP-optie, op pagina 3 voor meer informatie over DHCP-opties.

Voordat u begint

De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Inrichting**.

Stap 2 Stel in de sectie **Configuration Profile** (Configuratieprofiel) de parameters **DHCP Option To Use** (Te gebruiken DHCP-optie) en **DHCPv6 Option To Use** (Te gebruiken DHCPv6-optie) in zoals wordt beschreven in de tabel Parameters voor de configuratie van DHCP-opties, op pagina 3.

Stap 3 Klik op **Submit All Changes**.

Parameters voor de configuratie van DHCP-opties

In de volgende tabel worden de functie en het gebruik van parameters voor de configuratie van DHCP-opties gedefinieerd in de sectie Configuratieprofiel op het tabblad Spraak>Inrichting in de webinterface van de telefoon. Hij definieert ook de syntaxis van de string die aan het telefoonconfiguratiebestand is toegevoegd met XML-code (cfg.xml) om een parameter te configureren.

Tabel 1: Parameters voor de configuratie van DHCP-opties

Parameter	Beschrijving
DHCP Option To Use (Te gebruiken DHCP-optie)	DHCP-opties, gescheiden door komma's, gebruikt om firmware en profielen op te halen. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • Op de telefoonwebpagina voert u de DHCP-opties in, gescheiden door komma's. **Voorbeeld**: 66,160,159,150,60,43,125 Standaard: 66,160,159,150,60,43,125
Te gebruiken DHCPv6-optie	DHCPv6-opties, gescheiden door komma's, gebruikt om firmware en profielen op te halen. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • Op de telefoonwebpagina voert u de DHCP-opties in, gescheiden door komma's. **Voorbeeld**: 17,160,159 Standaard: 17,160,159

Ondersteuning van DHCP-optie

De volgende tabel bevat de DDHCP-opties die worden ondersteund op telefoons voor meerdere platforms.

Netwerkstandaard	Beschrijving
DHCP-optie 1	Subnetmasker
DHCP-optie 2	Tijdverschil (UU/mm)
DHCP-optie 3	Router
DHCP-optie 6	Domeinnaamserver

Netwerkstandaard	Beschrijving
DHCP-optie 15	Domeinnaam
DHCP-optie 41	Leasetijd IP-adres
DHCP-optie 42	NTP-server
DHCP-optie 43	Leverancierssspecifieke informatie Kan worden gebruikt voor detectie van TR.69 Auto Configurations Server (ACS).
DHCP-optie 56	NTP-server Configuratie van de NTP-server met IPv6
DHCP-optie 60	Klasse-id leverancier
DHCP-optie 66	TFTP-servernaam
DHCP-optie 125	Leverancierssspecifieke informatie waarmee leveranciers worden geïdentificeerd Kan worden gebruikt voor detectie van TR.69 Auto Configurations Server (ACS).
DHCP-optie 150	TFTP-server
DHCP-optie 159	IP inrichtingsserver
DHCP-optie 160	URL-inrichting

De identiteitsvraag voor SIP INVITE-berichten configureren

U kunt op de telefoon een identiteitsvraag stellen bij elk (initieel) SIP INVITE-bericht in een sessie. Met de vraag worden de SIP-servers beperkt die mogen communiceren met apparaten in een serviceprovidernetwerk. Op deze manier voorkomt u kwaadaardige aanvallen op de telefoon. Wanneer u deze parameter inschakelt, is autorisatie vereist voor eerste inkomende INVITE-aanvragen van de SIP-proxy.

U kunt de parameters ook configureren in het configuratiebestand voor de telefoon met XML-code (cfg.xml).

Voordat u begint

De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Toest.(n)**, waarbij n een toestelnummer is.

Stap 2 Selecteer in de sectie **SIP Settings** (SIP-instellingen) de optie **Yes** (Ja) in de lijst **Auth INVITE** (INVITE autoriseren) om deze functie in te schakelen of selecteer **No** (Nee) om deze uit te schakelen.

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```

Standaardwaarde: **No** (Nee).

Stap 3 Klik op **Submit All Changes**.

Ondersteuning voor RFC-8760

U kunt RFC-3261 vervangen en ondersteuning toevoegen voor extra digestalgoritmen voor verificatie die zijn opgegeven in RFC-8760. RFC-8760 geeft digestalgoritmen op, zoals SHA256, SHA-512/256 en MD5. Met RFC-8760 verzendt de telefoon SIP REGISTER-, INVITE- of SUBSCRIBE-verzoeken zonder autorisatieheader. De SIP-server reageert met de statuscode 401/407 met het headerveld www-authenticate of proxy-authenticate. Een SIP-server reageert met meerdere www-authenticate-headers. Als er meerdere headers worden verzonden, moet elk een ander algoritme hebben, waarbij de header met de grootste voorkeur eerst komt. Ondersteuning voor RFC-8760 biedt voordelen ten opzichte van RFC-3261 en deze worden beschreven in de volgende tabel voor verschillende scenario's.

Stappen	Richting SIP-verzoek	RFC-3261	RFC-8760
Stap 1	Telefoon naar SIP-server	Telefoon verzendt SIP-verzoeken zonder autorisatie.	Telefoon verzendt SIP-verzoeken zonder autorisatie.
Stap 2	SIP-server naar telefoon	SIP-server reageert met status 401 met één www-authenticate met het MD5-algoritme.	SIP-server reageert met status 401 met een of meer www-authenticates met verschillende algoritmen, zoals SHA-256, SHA-512-256 en MD5.
Stap 3	Telefoon naar SIP-server	Telefoon probeert verzoek opnieuw te verzenden en voegt een autorisatieheader toe met het MD5-algoritme.	Telefoon probeert verzoek opnieuw te verzenden en voegt een autorisatie toe met het bovenste headerveld (SHA-256).
Stap 4	SIP-server naar telefoon	SIP-server valideert de autorisatie.	SIP-server valideert de autorisatie.

Auth INVITE en Auth Resync Reboot inschakelen

U kunt de telefoonautorisatie inschakelen met RFC 8760.

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.
- In de sectie **SIP-instellingen** is **Auth Invite** ingesteld op **Ja**.

Procedure

Stap 1 Selecteer **Spraak** > **Toestel (n)**, waarbij n een toestelnummer is.

Stap 2 Selecteer in de sectie **SIP-instellingen** de optie **Ja** in de lijst **Auth Support RFC8760**.

Als u **Ja** selecteert, ondersteunt de telefoonautorisatie RFC 8760. U kunt het uitschakelen als u **Nee** selecteert.

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<Auth_Support_RFC8760>Yes</Auth_Support_RFC8760/>
```

Standaard: **Nee**

Stap 3 Klik op **Submit All Changes**.

Ondersteuning voor aanvullende digestalgoritmen voor hotelingverificatie

Telefoon ondersteunt nu RFC 8760 voor hotelingverificatie. Om deze functie te ondersteunen, worden de digestalgoritmen SHA-256, SHA-512 en SHA-256 aan de telefoon toegevoegd. Voorheen ondersteunde de telefoon alleen het MD5-algoritme.

De TLS-minimumwaarde beheren

U kunt de TLS-minimumwaarde van de telefoon bepalen met de nieuwe TLS-parameter. In de volgende tabel ziet u de korte weergave van het resultaat van de TLS-minimumwaarde.

Minimale versie client-TLS	Hoogste versie server-TLS	Resultaten
TLS 1.0	TLS 1.0	TLS 1.0
	TLS 1.1	TLS 1.1
	TLS 1.2	TLS 1.2
TLS 1.1	TLS 1.0	Protocolwaarschuwing
	TLS 1.1	TLS 1.1
	TLS 1.2	TLS 1.2
TLS 1.2	TLS 1.0	Protocolwaarschuwing
	TLS 1.1	Protocolwaarschuwing
	TLS 1.2	TLS 1.2

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Systeem**

Stap 2 Selecteer in de sectie **Beveiligingsinstellingen** de optie **TLS 1.1** uit de lijst **Min. TLS-versie**.

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<TLS_Min_Version ua="na">TLS 1.1</TLS_Min_Version>
```

Standaardwaarde: **TLS 1.1**

Stap 3 Klik op **Submit All Changes**.

Opmerking Deze functie is toegepast op de meeste TLS-clients die telefonisch zijn gestart. Bijvoorbeeld SIP over TLS, XMPP, E911 Geolocatie, Wi-Fi.

De besturing van de service Webex-meetwaarden inschakelen

Met Meetwaarden inschakelen schakelt u de telefoonbediening van alle statistische services in.

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Telefoon**

Stap 2 Selecteer in de sectie **Webex** de optie **Ja** uit de lijst **Meetwaarden inschakelen**.

Wanneer u **Ja** selecteert, bepaalt de telefoon het verzenden van alle berichten met meetwaarden. U kunt dit uitschakelen als u **Nee** selecteert.

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<Webex_Metrics_Enable ua="na">Yes</Webex_Metrics_Enable>
```

Standaard: **Nee**

Stap 3 Klik op **Submit All Changes**.

De besturing voor PRT uploaden bij crashservices inschakelen

U kunt aangeven of u het PRT-pakket automatisch naar de server wilt uploaden wanneer de telefoon crasht.

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Inrichting**

Stap 2 Selecteer in de sectie **Hulpprogramma probleemrapportage** de optie **Ja** in de lijst **PRT uploaden bij crash**.

Wanneer u **Ja** selecteert, beheert de telefoon het automatisch uploaden van de crash van het proces. U kunt dit uitschakelen als u **Nee** selecteert.

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<PRT_Upload_at_Crash ua="na">Yes</PRT_Upload_at_Crash>
```

Standaard: **Nee**

Stap 3 Klik op **Submit All Changes**.

Transport Layer Security (TLS)

TLS (Transport Layer Security) is een standaardprotocol voor het beveiligen en verifiëren van communicatie via internet. Met SIP via TLS worden de SIP-berichten tussen de SIP-proxy van de serviceprovider en de eindgebruiker gecodeerd.

Cisco IP-telefoon gebruikt UDP als de standaard voor SIP-transport, maar de telefoon ondersteunt ook SIP via TLS voor extra beveiliging.

In de volgende tabel worden de twee TLS-lagen beschreven.

Tabel 2: TLS-lagen

Naam protocol	Beschrijving
TLS-opnameprotocol	Gebaseerd op een betrouwbaar transportprotocol, zoals SIP of TCH, zorgt deze laag ervoor dat de verbinding privé is door middel van het gebruik van symmetrische gegevenscodering en wordt gegarandeerd dat de verbinding betrouwbaar is.
TLS Handshake-protocol	Hiermee worden de server en client geverifieerd en worden het coderingsalgoritme en cryptografische toetsen onderhandeld voordat gegevens worden ontvangen of verzonden met het toepassingsprotocol.

Signalering versleutelen met SIP via TLS

U kunt extra beveiliging configureren wanneer u signaleringsberichten met SIP via TLS versleutelt.

Voordat u begint

De webinterface van de telefoon openen. Zie Transport Layer Security (TLS), op pagina 8.

Procedure

Stap 1 Selecteer **Spraak** > **Toest.(n)**, waarbij n een toestelnummer is.

Stap 2 Selecteer in de sectie **SIP Settings** (SIP-instellingen) de optie **TLS** in de lijst **SIP Transport** (SIP-transport).

U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<SIP_Transport_1_ ua="na">TLS</SIP_Transport_1_>
```

.

Beschikbare opties:

- UDP
- TCP
- TLS
- Auto

Standaardwaarde: **UDP**.

Stap 3 Klik op **Submit All Changes**.

LDAP configureren via TLS

U kunt LDAP via TLS (LDAPS) configureren om veilige gegevensoverdracht in te schakelen tussen de server en een bepaalde telefoon.

Let op Cisco raadt aan om de verificatiemethode op de standaardwaarde van **Geen** te laten staan. Naast het serververveld ziet u een verificatieveld met de waarden **Geen**, **Eenvoudig** of **DIGEST-MD5**. Er is geen **TLS**-waarde voor de verificatie. In de software wordt de verificatiemethode van het LDAPS-protocol bepaald in de servertekenreeks.

U kunt de parameters ook configureren in het configuratiebestand voor de telefoon met XML-code (cfg.xml).

Voordat u begint

Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Telefoon**.

Stap 2 Voer in de sectie **LDAP** een serveradres in in het veld **Server**.

U kunt deze parameter ook configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

Voer bijvoorbeeld `ldaps://<ldaps_server>[:port]` in.

Waarbij:

- **`ldaps://`**= het begin van de tekenreeks voor het serveradres.
- **`ldaps_server`** = IP-adres of domeinnaam
- **`port`** = poortnummer. Standaard: 636

Stap 3 Klik op **Submit All Changes**.

Start TLS configureren

U kunt Start Transport Layer Security (StartTLS) inschakelen voor de communicatie tussen de telefoon en de LDAP-server. Het maakt gebruik dezelfde netwerkpoort (standaard 389) voor zowel veilige als onveilige communicatie. Als de LDAP-server StartTLS ondersteunt, versleutelt TLS de communicatie. Anders is de communicatie in platte tekst.

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Telefoon**.

Stap 2 Voer in de sectie **LDAP** een serveradres in in het veld **Server**.

Voer bijvoorbeeld `ldap://<ldap_server>[:port]` in.

Hierbij is:

- **`ldap://`**= het begin van de tekenreeks voor het serveradres.
- **`ldap_server`** = IP-adres of domeinnaam
- **`port`** = poortnummer.

U kunt deze parameter ook configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

Stap 3 Stel het veld **StartTLS ingeschakeld** in op **Ja**.

U kunt deze parameter ook configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:

```
<LDAP_StartTLS_Enable ua="na">Ja</LDAP_StartTLS_Enable>
```

Stap 4 Klik op **Submit All Changes**.

Verwante onderwerpen

Parameters voor LDAP-telefoonlijst

HTTPS-inrichting

De telefoon ondersteunt HTTPS voor inrichting voor betere beveiliging bij het extern beheer van geïmplementeerde toestellen. Elke telefoon heeft een uniek SSL-clientcertificaat (en de bijbehorende privésleutel), naast een Sipura CA-basisservercertificaat. Het laatste zorgt ervoor dat de telefoon geverifieerde inrichtingsservers kan herkennen en niet-geverifieerde servers kan afwijzen. Aan de andere kant zorgt het clientcertificaat ervoor dat de inrichtingsserver het individuele toestel kan herkennen dat het verzoek verzendt.

Als een serviceprovider de implementatie wil beheren via HTTPS, moet een servercertificaat worden gegenereerd voor elke inrichtingsserver waarnaar een telefoon hersynchroniseert met behulp van HTTPS. Het servercertificaat moet zijn ondertekend door de Cisco Server CA-basissleutel. Alle geïmplementeerde toestellen hebben dit certificaat. Als u een ondertekend servercertificaat wilt verkrijgen, moet de serviceprovider een aanvraag voor certificaatondertekening indienen bij Cisco. Cisco ondertekent het servercertificaat en stuurt het terug voor installatie op de inrichtingsserver.

Het certificaat van de inrichtingsserver moet het veld Algemene naam (CN) en de FQDN van de host waarop de server wordt uitgevoerd in het onderwerp bevatten. Het kan optioneel ook informatie bevatten na de host-FQDN, gescheiden door een slash (/). De volgende voorbeelden zijn van CN-vermeldingen die door de telefoon als geldig worden geaccepteerd:

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

Naast het verifiëren van het servercertificaat, controleert de telefoon het IP-adres van de server tegen een DNS-zoekopdracht van de servernaam die is gespecificeerd in het servercertificaat.

Een ondertekend servercertificaat verkrijgen

Het hulpprogramma OpenSSL kan een verzoek voor certificaatondertekening genereren. Het volgende voorbeeld toont de **openssl**-opdracht waarmee een RSA openbare/privésleutelpaar van 1024-bits en een verzoek tot certificaatondertekening wordt geproduceerd:

```
openssl req -new -out provserver.csr
```

Deze opdracht genereert de privé serversleutel in **privkey.pem** en een bijbehorend verzoek tot certificaatondertekening in **provserver.csr** . De serviceprovider houdt de **privkey.pem** geheim en

dient **provserver.csr** in bij Cisco voor ondertekening. Na ontvangst van het bestand **provserver.csr**, genereert Cisco **provserver.crt**, het ondertekende servercertificaat.

Procedure

Stap 1 Ga naar https://software.cisco.com/software/cda/home en meld u aan met uw CCO-referenties.

Opmerking Wanneer een telefoon voor de eerste keer verbinding maakt met een netwerk of nadat de fabrieksinstellingen zijn teruggezet en er geen DHCP-opties zijn ingesteld, maakt de telefoon contact met een apparaatactiveringsserver voor automatische inrichting. Nieuwe telefoons gebruiken “activate.cisco.com” in plaats van “webapps.cisco.com” voor inrichting. Telefoons met een firmwareversie van vóór 11.2(1) blijven “webapps.cisco.com” gebruiken. We raden aan om beide domeinnamen toe te staan door uw firewall.

Stap 2 Selecteer **Certificate Management**.

Op het tabblad **CSR ondertekenen** kunt u de CRS uit de vorige stap uploaden voor ondertekening.

Stap 3 In de vervolgkeuzelijst **Product selecteren** selecteert u **SPA1xx-firmware 1.3.3 en hoger/SPA232D-firmware 1.3.3 en hoger/SPA5xx-firmware 7.5.6 en hoger/CP-78xx-3PCC/CP-88xx-3PCC**.

Stap 4 In het veld **CSR-bestand** klikt u op **Bladeren** en selecteert u de CSR voor ondertekening.

Stap 5 De coderingsmethode selecteren:

- MD5
- SHA1
- SHA256

Cisco beveelt aan om SHA256-codering te selecteren.

Stap 6 In de vervolgkeuzelijst **Duur aanmelden** selecteert u de duur van toepassing (bijvoorbeeld 1 jaar).

Stap 7 Klik op **Verzoek tot certificaatondertekening**.

Stap 8 Selecteer een van de volgende opties om het ondertekende certificaat te ontvangen:

- **Voer e-mailadres van de ontvanger in**: als u het certificaat via e-mail wilt ontvangen, voert u uw e-mailadres in dit veld in.
- **Downloaden**: selecteer deze optie als u het ondertekende certificaat wilt downloaden.

Stap 9 Klik op **Verzenden**.

Het ondertekende servercertificaat wordt per e-mail verzonden naar het eerder opgegeven e-mailadres of gedownload.

CA-clientbasiscertificaat voor telefoons voor meerdere platforms

Cisco biedt ook een clientbasiscertificaat voor telefoons voor meerdere platforms aan de serviceprovider. Dit basiscertificaat verklaart de betrouwbaarheid van het clientcertificaat dat elke telefoon heeft. De telefoons voor meerdere platforms ondersteunen ook certificaten die door externe partijen zijn ondertekend, zoals die van Verisign, Cybertrust, etc.

Om te bepalen of een telefoon een individueel certificaat draagt, gebruikt u de macrovariabele $CCERT voor inrichting. De waarde van de variabele wordt uitgebreid tot geïnstalleerd of niet geïnstalleerd, afhankelijk van de aanwezigheid of afwezigheid van een uniek clientcertificaat. In het geval van een algemeen certificaat, is het mogelijk om het serienummer van het toestel te verkrijgen van de HTTP-aanvraagkoptekst in het veld User-Agent.

HTTPS-servers kunnen worden geconfigureerd om SSL-certificaten aan te vragen van clients die verbinding maken. Indien dit is ingeschakeld, kan de server het clienthoofdcertificaat voor telefoons voor meerdere platforms gebruiken dat door Cisco wordt geleverd om het clientcertificaat te verifiëren. De server kan de certificaatinformatie vervolgens aan een CGI aanbieden voor verdere verwerking.

De locatie voor opslag van certificaten kan variëren. Bij een Apache-installatie bijvoorbeeld, is het bestandspad voor de opslag van het door de inrichtingsserver ondertekende certificaat, de bijbehorende privé sleutel en het CA-clientbasiscertificaat voor telefoons voor meerdere platforms als volgt:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

Raadpleeg de documentatie voor een HTTPS-server voor specifieke informatie.

De Cisco Client Certificate Root Authority ondertekent elk unieke certificaat. Het overeenkomstige hoofdcertificaat wordt beschikbaar gesteld aan serviceproviders ten behoeve van clientverificatie.

Redundante inrichtingsservers

De inrichtingsserver kan worden gespecificeerd als een IP-adres of als een volledig gekwalificeerde domeinnaam (FQDN). Het gebruik van een FQDN faciliteert de implementatie van redundante inrichtingsservers. Wanneer de inrichtingsserver wordt geïdentificeerd via een FQDN, probeert de telefoon de FQDN om te zetten naar een IP-adres via DNS. Alleen DNS A-records worden ondersteund voor inrichting; DNS SRV-adresresolutie is niet beschikbaar voor inrichting. Totdat een server reageert, blijft de telefoon A-records verwerken. Als er geen server reageert die is gekoppeld aan de A-records, meldt de telefoon een fout bij de syslog-server.

Syslog-server

Als er via het gebruik van de <Syslog Server>-parameters een Syslog-server is geconfigureerd op de telefoon, worden er bij de bewerkingen voor opnieuw synchroniseren en upgraden berichten naar de slogan-server verzonden. Een bericht kan worden gegenereerd aan het begin van een verzoek voor een extern bestand (configuratieprofiel of firmwareversie) en aan het eind van de bewerking (om succes of mislukking aan te geven).

Berichten in het logboek worden geconfigureerd in de volgende parameters en worden macro-uitgebreid tot de werkelijke syslog-berichten:

De firewall inschakelen

Wij hebben de telefoonbeveiliging verbetert door het besturingssysteem te versterken. Dit betekent dat de telefoon nu een firewall heeft om deze te beschermen tegen schadelijk inkomend verkeer. De firewall houdt de poorten voor inkomende en uitgaande gegevens bij. Inkomend verkeer van onverwachte bronnen wordt gedetecteerd, waarna de toegang wordt geblokkeerd. Uw firewall staat al het uitgaande verkeer toe.

De firewall kan de blokkering van poorten die normaal zijn geblokkeerd, opheffen. Met de uitgaande TCP-verbinding of UDP-stroom wordt de blokkering van de poort voor teruggaand en doorgaand verkeer opgeheven. De poort wordt onblok kering behouden terwijl de stroom is Alive. De poort wordt weer in de status Geblokkeerd gezet wanneer de stroom wordt beëindigd of is verlopen.

De oude instelling, IPv6 Multicast Ping **Voice (Spraak)** > **System (Systeem)** > **IPv6 Settings (IPv6-instellingen)** > **Broadcast Echo** blijft onafhankelijk van de nieuwe firewallinstellingen werken.

Wanneer de firewallconfiguratie wordt gewijzigd, hoeft de telefoon meestal niet opnieuw te worden opgestart. Het opnieuw starten van telefoonsoftware heeft meestal geen invloed op de werking van de firewall.

De firewall is standaard ingeschakeld. Als de firewall is uitgeschakeld, kunt u deze inschakelen vanaf de webpagina van de telefoon.

Voordat u begint

De webinterface van de telefoon openen

Procedure

Stap 1 Selecteer **Voice (Spraak)** > **System (Systeem)** > **Security Settings (Beveiligingsinstellingen)**.

Stap 2 Selecteer in de vervolgkeuzelijst **Firewall** de optie **Enabled** (Ingeschakeld).

U kunt deze parameter ook configureren in het configuratiebestand (cfg.xml) door een reeks in deze indeling in te voeren:

```
<Firewall ua="na">Enabled</Firewall>
```

De toegestane waarden zijn Uitgeschakeld|Ingeschakeld. De standaardwaarde is Ingeschakeld.

Stap 3 Klik op **Submit All Changes**.
Hierdoor wordt de firewall ingeschakeld met de standaard geopende UDP- en TCP-poorten.

Stap 4 Selecteer **Uitgeschakeld** om de firewall uit te schakelen als u wilt dat uw netwerk weer terugkeert naar de eerdere werking.

In de volgende tabel worden de standaard geopende UDP-poorten beschreven.

Tabel 3: Standaard geopende UDP-poorten voor firewall

Standaard geopende UDP-poort	Beschrijving
DHCP/DHCPv6	Poort 68 voor DHCP-clients Poort 546 voor DHCPv6-clients

Standaard geopende UDP-poort	Beschrijving
SIP/UDP	Configureer de poort in **Spraak** > **Toestel<n>** > **SIP-instellingen** > **SIP-poort** (voorbeeld: 5060), wanneer **Lijn inschakelen** is ingesteld op **Ja** en **SIP-transport** is ingesteld op **UDP** of **Auto**.
RTP/RTCP	UDP-poortbereik van **RTP Port Min** (Min. RTP-poort) tot **RTP Port Max+1** (Max. RTP-poort+1)
PFS (Peer Firmware delen)	Poort 4051, wanneer **Upgrade Enable** (Upgrade inschakelen) en **Peer Firmware Sharing** (Peer Firmware delen) zijn ingesteld op **Yes** (Ja).
TFTP-clients	Poorten 53240-53245. U hebt dit poortbereik nodig als de externe server een andere poort gebruikt dan de standaard TFTP-poort 69. U kunt deze functie uitschakelen als de server standaard poort 69 gebruikt. Zie Uw firewall configureren met extra opties, op pagina 15.
TR-069	UDP/STUN-poort 7999, wanneer **Enable TR-069** (TR-069 inschakelen) is ingesteld op **Yes** (Ja).

In de volgende tabel worden de standaard geopende TCP-poorten beschreven.

Tabel 4: Standaard geopende TCP-poorten voor firewall

Standaard geopende TCP-poort	Beschrijving
Webserver	Poort geconfigureerd via webserverpoort (standaard 80) wanneer **Enable Web Server** (Webserver inschakelen) is ingesteld op **Yes** (Ja).
PFS (Peer Firmware delen)	De poorten 4051 en 6970, wanneer **Upgrade Enable** (Upgrade inschakelen) en **Peer Firmware Sharing** (Peer Firmware delen) zijn ingesteld op **Yes** (Ja).
TR-069	HTTP/SOAP-poort in TR-069 Connection Request URL (URL van verbindingsverzoek TR-069), wanneer **Enable TR-069** (TR-069 inschakelen) is ingesteld op **Yes** (Ja). De poort wordt willekeurig gekozen uit het bereik 8000-9999.

Uw firewall configureren met extra opties

U kunt extra opties configureren in het veld **Firewall Options** (Firewallopties). Typ het trefwoord voor elke optie in het veld en scheid de trefwoorden met komma's (,). Sommige trefwoorden hebben waarden. Scheid de waarden met dubbele punten (:).

Voordat u begint

De webinterface van de telefoon openen

Procedure

Stap 1 Ga naar **Voice (Spraak)** > **System (Systeem)** > **Security Settings (Beveiligingsinstellingen)**.

Stap 2 Selecteer **Enabled** (Ingeschakeld) bij het veld **Firewall**.

Stap 3 Voer in het veld **Firewall Options** (Firewallopties) de trefwoorden in. De lijst met poorten is van toepassing op zowel IPv4- als IPv6-protocollen.

Wanneer u de trefwoorden invoert,

- Scheidt u de trefwoorden met komma's (,).
- Scheidt u de waarden van trefwoorden met een dubbele punt (:).

Tabel 5: Optionele instellingen voor de firewall

Trefwoorden firewallopties	Beschrijving
Het veld is leeg.	De firewall wordt uitgevoerd met standaard open poorten.
NO_ICMP_PING	De firewall blokkeert inkomende ICMP/ICMPv6 **`ECHO`**-verzoeken (ping). Met deze optie kunnen bepaalde typen traceroute-verzoeken naar de telefoon worden verzonden. Windows **`tracert`** is hier een voorbeeld van. Voorbeeld van invoer van **Firewall Options** (Firewallopties) met een combinatie van opties: NO_ICMP_PING,TCP:12000,UDP:8000:8010 De firewall wordt uitgevoerd met de standaardinstellingen en de volgende aanvullende opties: • Negeert inkomende ICMP/ICMPv6 **`Echo`** (Ping)-verzoeken. • Hiermee opent u TCP-poort 12000 (IPv4 en IPv6) voor inkomende verbindingen. • Hiermee opent u het UDP-poortbereik 8000-8010 (IPv4 en IPv6) voor inkomende verzoeken.
NO_ICMP_UNREACHABLE	De telefoon verzendt geen ICMP/ICMPv6 `Destination Unreachable` (Doel onbereikbaar) voor UDP-poorten. **Opmerking** De uitzondering is het altijd verzenden van `Destination Unreachable` voor poorten in het RTP-poortbereik. Met deze optie kunnen bepaalde typen **`traceroute`**-verzoeken naar het apparaat worden verzonden. **`traceroute`** van Linux kan bijvoorbeeld worden verzonden.
NO_CISCO_TFTP	• De telefoon opent geen poortbereik voor TFTP-clients (UDP 53240:53245). • Verzoeken aan niet-standaard TFTP-serverpoorten (niet 69) mislukken. • Verzoeken aan de standaard-TFTP-serverpoort 69 werken.

Trefwoorden firewallopties	Beschrijving
De volgende trefwoorden en opties zijn van toepassing wanneer op de telefoon aangepaste toepassingen worden uitgevoerd waarmee inkomende verzoeken worden verwerkt.	
UDP:<xxx>	Hiermee wordt UDP-poort <xxx> geopend.
UDP:<xxx:yyy>	Hiermee wordt het UDP-poortbereik <xxx to yyy> geopend. U kunt maximaal vijf opties voor UDP-poorten (enkele poorten en poortbereiken) hebben. U kunt bijvoorbeeld 3 UDP:<xxx> en 2 UDP:<xxx:yyy> hebben.
TCP:<xxx>	Hiermee wordt TCP-poort <xxx> geopend.
TCP:<xxx:yyy>	Hiermee wordt het TCP-poortbereik <xxx to yyy> geopend. U kunt maximaal vijf opties voor TCP-poorten (enkele poorten en poortbereiken) hebben. U kunt bijvoorbeeld 4 TCP:<xxx> en één TCP:<xxx:yyy> hebben.

U kunt deze parameter ook configureren in het configuratiebestand (cfg.xml) door een reeks in deze indeling in te voeren:

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

Stap 4 Klik op **Submit All Changes**.

De coderingslijst configureren

U kunt de coderingssuites opgeven die door de TLS-toepassingen van de telefoon worden gebruikt. De opgegeven coderingslijst is van toepassing op alle toepassingen die het TLS-protocol gebruiken. De TLS-toepassingen op uw telefoon zijn:

- Aangepaste CA-inrichting
- E911-geolocatie
- Upgrade van firmware/Cisco-hoofdtelefoon
- LDAPS
- LDAP (Start TLS)
- Afbeelding downloaden
- Logo downloaden
- Woordenlijst downloaden

- Inrichting
- Rapport uploaden
- PRT uploaden
- SIP over TLS
- TR-069
- WebSocket-API
- XML-services
- XSI-services

U kunt de coderingssuites ook opgeven met de TR-069-parameter (`Device.X_CISCO_SecuritySettings.TLSCipherList`) of met het configuratiebestand (cfg.xml). Voer in het configuratiebestand een tekenreeks met deze notatie in:

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

Voordat u begint

Open de webpagina voor telefoonbeheer. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Systeem**.

Stap 2 Voer in de sectie **Security Settings** (Beveiligingsinstellingen) de coderingssuite of de combinatie van coderingssuites in het veld **TLS Cipher List** (TLS-coderingssuite) in.

Voorbeeld:

```
RSA:!aNULL:!eNULL
```

Ondersteunt coderingssuites die RSA-verificatie gebruiken, maar sluit coderingssuites uit die geen versleuteling en verificatie bevatten.

Opmerking Een geldige coderingslijst moet de notatie hebben die is gedefinieerd op https://www.openssl.org/docs/man1.1.1/man1/ciphers.html. Uw telefoon ondersteunt niet alle coderingsreeksen die worden vermeld op de webpagina OpenSSL. Zie Ondersteunde versleutelingsreeksen, op pagina 19 voor de ondersteunde reeksen.

Als het veld **TLS-coderingslijst** een lege of ongeldige waarde bevat, verschillen de gebruikte coderingssuites per toepassing. Zie de volgende lijst voor de suites die door de toepassingen worden gebruikt wanneer dit veld leeg is of een ongeldige waarde bevat.

- Webservertoepassingen (HTTPS) gebruiken de volgende coderingssuites:
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**

- **DES-CBC3-SHA**

- XMPP gebruikt de coderingslijst **HIGH:MEDIUM:AES:@STRENGTH**.
- SIP, TR-069 en andere toepassingen die de cURL-bibliotheek gebruiken, gebruiken de coderingsreeks **STANDAARD**. De coderingsreeks **STANDAARD** bevat de volgende coderingssuites die de telefoon ondersteunt:

```
DEFAULT Cipher Suites (28 suites):
        ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ECDHE_RSA_WITH_AES_256_GCM_SHA384
        DHE_RSA_WITH_AES_256_GCM_SHA384
        ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        ECDHE_RSA_WITH_AES_128_GCM_SHA256
        DHE_RSA_WITH_AES_128_GCM_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        ECDHE_RSA_WITH_AES_256_CBC_SHA384
        DHE_RSA_WITH_AES_256_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        ECDHE_RSA_WITH_AES_128_CBC_SHA256
        DHE_RSA_WITH_AES_128_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        ECDHE_RSA_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        ECDHE_RSA_WITH_AES_128_CBC_SHA
        DHE_RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_GCM_SHA384
        RSA_WITH_AES_128_GCM_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        RSA_WITH_AES_128_CBC_SHA256
        RSA_WITH_AES_256_CBC_SHA
        RSA_WITH_AES_128_CBC_SHA
        EMPTY_RENEGOTIATION_INFO_SCSV
```

Stap 3 Klik op **Submit All Changes**.

Ondersteunde versleutelingsreeksen

De ondersteunde versleutelingsreeksen die hieronder worden beschreven, zijn gebaseerd op de OpenSSL 1.1.1d-standaarden.

Tabel 6: Ondersteunde versleutelingsreeksen (OpenSSL 1.1.1 d)

Tekenreeksen	Tekenreeksen	Tekenreeksen
STANDAARD	kECDHE, kEECDH	CAMELLIA128, CAMELLIA256, CAMELLIA
COMPLEMENTOFDEFAULT	ECDHE, EECDH	CHACHA20
ALLES	ECDH	SEED

Tekenreeksen	Tekenreeksen	Tekenreeksen
COMPLEMENTOFALL	AECDH	MD5
HOOG	aRSA	SHA1, SHA
GEMIDDELD	aDSS, DSS	SHA256, SHA384
eNULL, NULL	aECDSA, ECDSA	SUITEB128, SUITEB128ONLY, SUITEB192
aNULL	TLSv1.2, TLSv1, SSLv3	
kRSA, RSA	AES128, AES256, AES	
kDHE, kEDH, DH	AESGCM	
DHE, EDH	AESCCM, AESCCM8	
ADH	ARIA128, ARIA256, ARIA	

Hostnaamverificatie inschakelen voor SIP via TLS

U kunt verhoogde telefoonbeveiliging op een telefoonlijn inschakelen als u TLS gebruikt. De telefoonlijn kan de hostnaam controleren om te bepalen of de verbinding veilig is.

Via een TLS-verbinding kan de telefoon de hostnaam verifiëren om de identiteit van de server te controleren. De telefoon kan de SAN (alternatieve naam voor onderwerp) en de CN (algemene naam) van het onderwerp controleren. Als de hostnaam op het geldige certificaat overeenkomt met de hostnaam die wordt gebruikt om te communiceren met de server, wordt de TLS-verbinding tot stand gebracht. Anders mislukt de TLS-verbinding.

De telefoon controleert altijd de hostnaam voor de volgende toepassingen:

- LDAPS
- LDAP (Start TLS)
- XMPP
- Upgrade van afbeelding via HTTPS
- XSI via HTTPS
- Bestand downloaden via HTTPS
- TR-069

Wanneer op een telefoonlijn SIP-berichten worden getransporteerd via TLS, kunt u de lijn zo configureren dat hostnaamverificatie wordt ingeschakeld of genegeerd via het veld **TLS Name Validate** (TLS-naam valideren) op het tabblad **Ext(n)** Toestel(n).

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

- Stel op het tabblad **Ext(n)** (Toestel(n)) de optie **SIP Transport** (SIP-transport) in op **TLS**.

Procedure

Stap 1 Ga naar **Voice (Spraak)** > **Ext(n) (Toestel(n))**.

Stap 2 Stel in de sectie **Proxy and Registration** (Proxy en registratie) het veld **TLS Name Validate** (TLS-naam valideren) in op **Yes** (Ja) om hostnaamverificatie in te schakelen of op **No** (Nee) om hostnaamverificatie te negeren.

U kunt deze parameter ook configureren in het configuratiebestand (cfg.xml) door een reeks in deze indeling in te voeren:

```
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
```

De toegestane waarden zijn Ja of Nee. De standaardinstelling is Ja.

Stap 3 Klik op **Submit All Changes**.

Door de client geïnitieerde modus voor beveiligingsonderhandelingen over mediaplane inschakelen

Als u mediasessies wilt beveiligen, kunt u de telefoon zo configureren dat de beveiligingsonderhandelingen voor het mediaplane op de server worden geïnitieerd. Het beveiligingsmechanisme voldoet aan de standaarden die zijn opgegeven in RFC 3329 en het bijbehorende uitbreidingsconcept *Security Mechanism Names for Media* (Namen van beveiligingsmechanisme voor media) (Zie https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2). Voor het transport van onderhandelingen tussen de telefoon en de server kan het SIP-protocol via UDP, TCP en TLS worden gebruikt. U kunt instellen dat de beveiligingsonderhandeling van het mediaplane alleen wordt toegepast wanneer het signaleringstransportprotocol TLS is.

U kunt de parameters ook configureren in het configuratiebestand (cfg.xml). Zie de syntaxis van de reeks in Parameters voor beveiligingsonderhandeling in mediaplane, op pagina 22 voor meer informatie over het configureren van de parameters.

Voordat u begint

Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Voice (Spraak)** > **Ext (n) (Toestel (n))**.

Stap 2 Stel in de sectie **SIP Settings** (SIP-instellingen) de velden **MediaSec Request** (MediaSec-verzoek) en **MediaSec Over TLS Only** (Alleen MediaSec via TLS) in zoals is gedefinieerd in Parameters voor beveiligingsonderhandeling in mediaplane, op pagina 22

Stap 3 Klik op **Submit All Changes**.

Parameters voor beveiligingsonderhandeling in mediaplane

De volgende tabel definieert de functie en het gebruik van elke de parameters voor beveiligingsonderhandeling in mediaplane in de sectie **SIP-instellingen** op het tabblad **Spraak**> **Ext (n)** in de webinterface van de telefoon. Hij definieert ook de syntaxis van de tekenreeks die aan het telefoonconfiguratiebestand (cfg.xml) is toegevoegd met XML-code om een parameter te configureren.

Tabel 7: Parameters voor beveiligingsonderhandeling in mediaplane

Parameter	Beschrijving
MediaSec-aanvraag	Geeft aan of de telefoon beveiligingsonderhandelingen in de mediaplane initieert met de server. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • Stel dit veld in de telefoonwebinterface in op **Ja** of **Nee**. Toegestane waarden: Ja|Nee • **Ja**— modus door client gestart. De telefoon initieert beveiligings onderhandelingen voor media vlieg tuigen. • **Nee**— modus door server gestart. De server initieert beveiligings onderhandelingen voor media vlieg tuigen. De telefoon start geen onderhandelingen, maar kan onderhandelings verzoeken van de server afhandelen om veilige gesp rekken tot stand te brengen. Standaard: Nee

Parameter	Beschrijving
Alleen MediaSec via TLS	Geeft het signalerings transport protocol aan waarop de beveiligings onderhandeling voor media vlak wordt toegepast. Voordat u dit veld instelt op **Ja**, moet u controleren of het signaleringstransportprotocol TLS is. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • Stel dit veld in de telefoonwebinterface in op **Ja** of **Nee**. Toegestane waarden: Ja|Nee • **Ja**— de telefoon initieert of afhandelt alleen beveiligings onderhandelingen als het signalerings transport protocol TLS is. • **Nee**— de telefoon initieert de beveiligings onderhandelingen voor media vlieg tuigen, ongeacht het protocol voor het signalerings transport protocol. Standaard: Nee

802.1X-verificatie

Cisco IP-telefoons gebruiken Cisco Discovery Protocol (CDP) om de LAN-switch te detecteren en parameters vast te stellen, 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-supplicant. Met deze supplicant kunnen netwerkbeheerders de verbinding regelen van IP-telefoons met de LAN-switchpoorten. De huidige versie van de 802.1X-supplicant voor de telefoon gebruikt de opties EAP-FAST en EAP-TLS voor netwerkverificatie.
- Cisco 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.

- Een LAN-switch die 802.1X ondersteunt: de switch werkt als de verificatie en geeft de berichten tussen de telefoon en de verificatieserver door. 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 ondersteunen echter verificatie voor meerdere domeinen. De switchconfiguratie bepaalt of u een pc kunt aansluiten op de pc-poort van de telefoon.
  - Ja: als u een switch gebruikt die verificatie voor meerdere domeinen ondersteunt, kunt u de pc-poort inschakelen en er een pc op 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.
  - Nee: als de switch niet meerdere 802.1X-conforme apparaten op dezelfde poort ondersteunt, moet u de pc-poort uitschakelen wanneer 802.1X-verificatie is 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.

802.1X-verificatie inschakelen

U kunt 802.1X-verificatie voor de telefoon inschakelen. Wanneer 802.1 X-verificatie is ingeschakeld, gebruikt de telefoon 802.1x-verificatie om netwerktoegang aan te vragen. Wanneer 802.1 X-verificatie is uitgeschakeld, gebruikt de telefoon CDP om VLAN- en netwerktoegang te verkrijgen. U kunt ook de transactiestatus bekijken in het menu van het telefoonscherm.

Procedure

Stap 1 Voer een van de volgende handelingen uit om 802.1x-verificatie in te schakelen:

- Selecteer in de webinterface van de telefoon de optie **Voice (Spraak)** > **System (Systeem)** en stel het veld **Enable 802.1X Authentication** (802.1X-verificatie inschakelen) in op **Yes** (Ja). Klik vervolgens op **Alle wijzigingen indienen**.
- Voer in het configuratiebestand (cfg.xml) een tekenreeks met deze notatie in:

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```

- Druk op de telefoon op **Applications (Toepassingen)** > **Network configuration (Netwerkconfiguratie)** > **Ethernet configuration (Ethernet-configuratie)** > **802.1X authentication**

(802.1X-verificatie). Schakel vervolgens het veld **Device authentication** (Apparaatverificatie) **in** met de knop **Select** (Selecteren) en druk op **Submit** (Verzenden).

Stap 2 (Optioneel) Selecteer **Transaction status** (Transactiestatus) om het volgende weer te geven:

- **Transaction status** (Transactiestatus): hiermee wordt de status van 802.1x-verificatie weergegeven. De status kan het volgende zijn
  - *Authenticating* (Verifiëren): hiermee wordt aangegeven dat het verificatieproces wordt uitgevoerd.
  - *Authenticated* (Geverifieerd): hiermee wordt aangegeven dat de telefoon is geverifieerd.
  - *Uitgeschakeld*: hiermee wordt aangegeven dat 802.1X-verificatie niet is geconfigureerd op de telefoon.
- **Protocol**: hiermee wordt de EAP-methode weergegeven die wordt gebruikt voor 802.1X verificatie. Het protocol kan EAP-FAST of EAP-TLS zijn.

Stap 3 Druk op **Terug** om het menu te sluiten.

Een proxyserver instellen

U kunt de telefoon zo configureren dat de beveiliging met een proxyserver wordt verbeterd. Een proxyserver fungeert als een firewall tussen de telefoon en internet. Wanneer de configuratie goed is ingesteld, maakt de telefoon via de proxyserver die de telefoon beschermt tegen cyberaanvallen, verbinding met internet.

U kunt een proxyserver instellen door een automatisch configuratiescript te gebruiken of door de hostserver (hostnaam of IP-adres) en de poort van de proxyserver handmatig te configureren.

Wanneer de proxyserver is geconfigureerd, is de HTTP-proxyfunctie van toepassing op alle toepassingen die gebruik maken van het HTTP-protocol. De toepassingen bevatten het volgende:

- GDS (verbinding tot stand brengen met de activeringscode)
- EDOS-apparaatactivering
- Verbinding maken met de Webex-cloud (via EDOS en GDS)
- Certificaatverificatie
- Inrichting
- Firmware-upgrade
- Telefoonstatusrapport
- PRT uploaden
- XSI-services
- Webex-services

Voordat u begint

Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Systeem**.

Stap 2 Configureer in de sectie **HTTP-proxyinstellingen** de parameter **Proxymodus** en andere parameters op basis van uw vereisten. In de volgende stappen vindt u de gedetailleerde procedures.

Stap 3 Voer een van de volgende handelingen uit:

- De **Proxymodus** is **automatisch**:
  - Als **Automatische detectie gebruiken (WPAD)** staat ingesteld op **Ja**, hoeft u verder niets te doen. De telefoon haalt automatisch met het WPAD-protocol (Web Proxy Auto-Discovery) een PAC-bestand (Proxy Auto-Configuration) op.
  - Als **Automatische detectie gebruiken (WPAD)** staat ingesteld op **Nee**, voert u een geldige URL in **PAC-URL** in.
- **Proxymodus** is **Handmatig**:
  - Als **Proxyserver moet worden geverifieerd** staat ingesteld op **Nee**, voert u een proxyserver in **Proxyhost** en een proxypoort in **Proxypoort** in.
  - Als **Proxyserver moet worden geverifieerd** staat ingesteld op **Ja**, voert u een proxyserver in **Proxyhost** en een proxypoort in **Proxypoort** in. En voert u een gebruikersnaam in **Gebruikersnaam** en een wachtwoord in **Wachtwoord** in.
- Als de **proxymodus** is **uitgeschakeld**, is de functie HTTP-proxy uitgeschakeld op de telefoon.

U kunt de parameters ook configureren in het configuratiebestand van de telefoon (cfg.xml). Zie de syntaxis van de reeks in de Parameters voor HTTP-proxyinstellingen, op pagina 26 voor het configureren van elke parameter.

Stap 4 Klik op **Submit All Changes**.

Parameters voor HTTP-proxyinstellingen

De volgende tabel definieert de functie en het gebruik van de parameters voor de HTTP-proxy in de sectie **HTTP-proxyinstellingen** onder het tabblad **Spraak** > **Systeem** in de webinterface van de telefoon. Hij definieert ook de syntaxis van de tekenreeks die aan het telefoonconfiguratiebestand (cfg.xml) is toegevoegd met XML-code om een parameter te configureren.

Tabel 8: Parameters voor HTTP-proxyinstellingen

Parameter	Beschrijving en standaardwaarde
Proxymodus	Hiermee geeft u de HTTP-proxymodus op die op de telefoon wordt gebruikt, of schakelt u de functie HTTP-proxy uit. • Auto Op de telefoon wordt automatisch een bestand voor de automatische configuratie van een proxy (PAC) opgehaald om een proxyserver te selecteren. In deze modus kunt u bepalen of u met het WPAD-protocol (Web Proxy Auto-Discovery) een PAC-bestand wilt ophalen of handmatig een geldige URL van het PAC-bestand wilt opgeven. Zie Automatische detectie gebruiken (WPAD) en PAC-URL voor meer informatie over de parameters. • Handmatig U moet handmatig een server (hostnaam of IP-adres) en een poort van een proxyserver opgeven. Zie Proxyhost en Proxypoort voor meer informatie over de parameters. • Uit U kunt de functie HTTP-proxy op de telefoon uitschakelen. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<Proxy_Mode ua="rw">Off</Proxy_Mode>` • Selecteer in de webinterface van de telefoon een proxymodus of schakel de functie uit. Toegestane waarden: Automatisch, Handmatig en Uit Standaard: Uit

Parameter	Beschrijving en standaardwaarde
Automatische detectie gebruiken (WPAD)	Hiermee wordt bepaald of op de telefoon het WPAD-protocol (Web Proxy Auto-Discovery) wordt gebruikt om een PAC-bestand op te halen. Het WPAD-protocol gebruikt DHCP of DNS, of beide netwerkprotocollen voor het automatisch opzoeken van een PAC-bestand (Proxy Auto-Configuration). Met het PAC-bestand wordt een proxyserver voor een bepaalde URL geselecteerd. Dit bestand kan lokaal of op een netwerk worden gehost. • De parameterconfiguratie wordt pas toegepast wanneer **Proxymodus** is ingesteld op **Automatisch**. • Als u de parameter instelt op **Nee**, moet u een PAC-URL opgeven. Zie PAC-URL voor meer informatie over de parameter. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_>` • Selecteer zo nodig Ja of Nee in de webinterface van de telefoon. Toegestane waarden: Ja en Nee Standaard: Ja
PAC-URL	URL van een PAC-bestand. Bijvoorbeeld `http://proxy.department.branch.example.com` TFTP, HTTP en HTTPS worden ondersteund. Als u **Proxymodus** instelt op **Automatisch** en **Automatische detectie gebruiken (WPAD)** op **Nee**, moet u deze parameter configureren. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL>` • Voer in de webinterface van de telefoon een geldige URL in waarmee een PAC-bestand kan worden opgezocht. Standaard: leeg

Parameter	Beschrijving en standaardwaarde

Proxyhost	IP-adres of hostnaam van de proxyserver voor de telefoon waartoe de telefoon toegang moet krijgen. Bijvoorbeeld:
	`proxy.example.com`
	Het schema (`http://` of `https://`) is niet vereist.
	Als u de **Proxymodus** instelt op **Handmatig**, moet u deze parameter configureren.
	Voer een van de volgende handelingen uit:
	• Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in:
	`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`
	• Voer in de webinterface van de telefoon het IP-adres of de hostnaam van de proxyserver in.
	Standaard: leeg

Proxypoort	Poortnummer van de proxyhostserver. Als u de **Proxymodus** instelt op **Handmatig**, moet u deze parameter configureren. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<Proxy_Port ua="rw">3128</Proxy_Port>` • Voer in de webinterface van de telefoon een serverpoort in. Standaard: 3128

Parameter	Beschrijving en standaardwaarde
De proxyserver moet worden geverifieerd	Hiermee wordt bepaald of de gebruiker de aanmeldgegevens voor de verificatie (gebruikersnaam en wachtwoord) moet opgeven die nodig zijn voor de proxyserver. Deze parameter wordt geconfigureerd op basis van de werkelijke werking van de proxyserver. Als u de parameter instelt op **Ja**, moet u **Gebruikersnaam** en **Wachtwoord** configureren. Zie Gebruikersnaam en Wachtwoord voor meer informatie over de parameters. De parameterconfiguratie wordt pas toegepast wanneer **Proxymodus** wordt ingesteld op **Handmatig**. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>` • Stel in de webinterface van de telefoon dit veld in op Ja of Nee. Toegestane waarden: Ja en Nee Standaard: Nee
Gebruikersnaam	Gebruikersnaam voor een bekende gebruiker op de proxyserver. Als **Proxymodus** is ingesteld op **Handmatig** en **Proxyserver moet worden geverifieerd** is ingesteld op **Ja**, moet u de parameter configureren. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<Proxy_Username ua="rw">Example</Proxy_Username>` • Voer in de webinterface van de telefoon de gebruikersnaam in. Standaard: leeg
Wachtwoord	Wachtwoord voor de opgegeven gebruikersnaam voor het verifiëren van de proxy. Als **Proxymodus** is ingesteld op **Handmatig** en **Proxyserver moet worden geverifieerd** is ingesteld op **Ja**, moet u de parameter configureren. Voer een van de volgende handelingen uit: • Voer in het telefoonconfiguratiebestand met XML(cfg.xml) een tekenreeks in de volgende notatie in: `<Proxy_Password ua="rw">Example</Proxy_Password>` • Voer in de webinterface van de telefoon een geldig wachtwoord in voor de proxyverificatie van de gebruiker. Standaard: leeg

FIPS-modus inschakelen

U kunt een telefoon compatibel maken met FIPS (Federal Information Processing Standards).

FIPS zijn een reeks standaarden die de documentverwerking, coderingsalgoritmen en andere normen voor informatietechnologie beschrijven voor gebruik binnen niet-militaire overheidsinstanties en door overheidsaannemers en -leveranciers die met deze instanties samenwerken. OpenSSL FOM (FIPS-Object Module) is een zorgvuldig gedefinieerde softwarecomponent die is ontworpen voor compatibiliteit met de OpenSSL-bibliotheek. Producten die de OpenSSL-bibliotheek en -API gebruiken, kunnen daardoor vrij eenvoudig worden omgezet om door FIPS 140-2 gevalideerde cryptografie te gebruiken.

De FIPS-modus heeft de volgende beperkingen:

- TR069 is uitgeschakeld
- HTTP-digestverificatie is uitgeschakeld

Voordat u begint

- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Selecteer **Spraak** > **Systeem**.

Stap 2 Kies **Ja** of **Nee** voor de parameter **FIPS-modus** in de sectie **Security Settings** (Beveiligingsinstellingen).

Wanneer u de FIPS-modus niet inschakelt, wordt een foutmelding over beveiliging op de telefoon weergegeven en moet de telefoon opnieuw worden opgestart.

Ook wordt in het scherm **Statusberichten** een foutmelding over FIPS weergegeven wanneer de FIPS-modus mislukt.

Stap 3 Klik op **Submit All Changes**.
Wanneer u FIPS inschakelt, werken de volgende functies probleemloos op de telefoon:

Verificatie afbeelding	PRT uploaden	Deelnemen met één knop (OBTJ)
Veilige opslag	Firmware-upgrade	SIP over TLS
Codering van configuratiebestand	Profiel opnieuw synchroniseren	SRTP
802.1x	Onboardingservice	SIP-digest (RFC 8760)
HTTPs-server	Webex-onboarding, Webex-gesprekslogs, Webex-telefoonlijst	HTTP-proxy

Overzicht beveiliging Cisco-producten

Dit product bevat cryptografische functies en is onderhevig aan de wetgeving in de Verenigde Staten en andere landen met betrekking tot import, export, overdracht en gebruik. Levering van cryptografische producten van Cisco betekent niet dat derden bevoegd zijn codering te importeren, te exporteren of te gebruiken. Importeurs, exporteurs, distributeurs en gebruikers zijn verantwoordelijk voor naleving van eerder genoemde wetgeving. Door dit product te gebruiken, gaat u akkoord met de wetten en bepalingen die hierop van toepassing zijn. Als u hieraan niet kunt voldoen, dient u dit product onmiddellijk te retourneren.

Meer informatie over exportvoorschriften van de Verenigde Staten vindt u op https://www.bis.doc.gov/policiesandregulations/ear/index.htm.

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.