Inrichtingsmethoden

Inrichting van een telefoon met BroadSoft-server

Alleen voor gebruiker van BroadSoft-server.

U kunt uw Cisco IP-telefoons voor meerdere platforms registreren op een BroadWorks-platform.

Procedure

Stap 1 Download de CPE-kit van BroadSoft Xchange. Ga voor de nieuwste CPE-kits naar deze URL: https://xchange.broadsoft.com.

Stap 2 Upload het recentste DTAF-bestand naar de BroadWorks-server (systeemniveau).

Ga voor meer informatie naar deze URL: (https://xchange.broadsoft.com/node/1031047). Open de *partnerconfiguratiehandleiding van BroadSoft* en bekijk de sectie "*Configure BroadWorks device profile type*" (Profieltype BroadWorks-apparaat configureren).

Stap 3 Configureer het profieltype van het Broadworks-apparaat.

Ga naar deze URL voor meer informatie over het configureren van het apparaatprofieltype:

https://xchange.broadsoft.com/node/1031047. Open de *partnerconfiguratiehandleiding van BroadSoft* en bekijk de sectie "*Configure BroadWorks device profile type*" (Configuratie profieltype BroadWorks-apparaat).

Overzicht voorbeelden van inrichting

Dit hoofdstuk bevat voorbeeldprocedures voor de overdracht van configuratieprofielen tussen de telefoon en de inrichtingsserver.

Voor meer informatie over het maken van configuratieprofielen raadpleegt u Inrichtingsindelingen.

Standaard hersynchroniseren

In deze sectie wordt de standaardfunctionaliteit voor hersynchroniseren van de telefoons besproken.

Syslog gebruiken om berichten op te slaan

Een telefoon kan worden geconfigureerd om logboekberichten te verzenden naar een syslog-server via UDP, inclusief berichten die betrekking hebben op inrichting. Om deze server te identificeren, opent u de webinterface van de telefoon (zie De webinterface van de telefoon openen), selecteert u **Voice (Spraak)** > **System (Systeem)** en identificeert u de server in de parameter **Syslog Server** van de sectie **Optional Network Configuration** (Optionele netwerkconfiguratie). Configureer het IP-adres van de syslog-server in het apparaat en controleer de berichten die tijdens de resterende procedures worden gegenereerd.

Als u de informatie wilt opvragen, opent u de webinterface van de telefoon, selecteert u **Info** > **Debug Info (Foutopsporingsinfo)** > **Control Logs (Controlelogboeken)** en klikt u op **messages** (berichten).

Voordat u begint

Procedure

Stap 1 Installeer en activeer een syslog-server op de lokale computer.

Stap 2 Programmeer het IP-adres van de computer in de parameter Syslog_Server van het profiel en dien de wijziging in:

```
<Syslog_Server>192.168.1.210</Syslog_Server>
```

Stap 3 Klik op het tabblad **Systeem** en voer de waarde van uw lokale syslog-server in de parameter Syslog_Server in.

Stap 4 Herhaal de hersynchronisatiebewerking zoals beschreven in Hersynchroniseren via TFTP, op pagina 3.

Het apparaat genereert twee syslog-berichten tijdens het hersynchroniseren. Het eerste bericht geeft aan dat er een verzoek wordt uitgevoerd. Het tweede bericht markeert of de hersynchronisatie is gelukt of is mislukt.

Stap 5 Verifieer dat uw syslog-server berichten heeft ontvangen die vergelijkbaar zijn met het volgende:

```
CP-68xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txtc.txt
```

Gedetailleerde berichten zijn beschikbaar door een parameter Debug_Server te programmeren (in plaats van de parameter Syslog_Server) met het IP-adres van de syslog-server en door Debug_Level in te stellen op een waarde tussen 0 en 3 (3 is de meest uitgebreide):

```
<Debug_Server>192.168.1.210</Debug_Server>
<Debug_Level>3</Debug_Level>
```

De inhoud van deze berichten kan worden geconfigureerd met behulp van de volgende parameters:

- Log_Request_Msg (Aanvraagbericht registreren)
- Log_Success_Msg (Succesbericht registreren)
- Log_Failure_Msg (Foutbericht registreren)

Als een van deze parameters worden gewist, wordt het bijbehorende syslog-bericht niet gegenereerd.

Hersynchroniseren via TFTP

De telefoon ondersteunt meerdere netwerkprotocollen voor het ophalen van configuratieprofielen. Het meest eenvoudige profieloverdrachtsprotocol is TFTP (RFC1350). TFTP wordt veel gebruikt voor de inrichting van netwerkapparaten binnen privé LAN-netwerken. Hoewel het niet wordt aanbevolen voor de implementatie van externe eindpunten via het internet, kan TFTP nuttig zijn voor implementatie binnen kleine organisaties, voorinrichting op locatie en het ontwikkelen en testen. Zie Voorinrichting van apparaten op locatie voor meer informatie over voorinrichting op locatie. In de volgende procedure wordt een profiel aangepast na het downloaden van een bestand van een TFTP-server.

Procedure

Stap 1 Sluit een computer en een telefoon aan op een hub, switch of kleine router in een LAN-omgeving.

Stap 2 Installeer en activeer een TFTP-server op de computer.

Stap 3 Gebruik een tekstverwerker om een configuratieprofiel te maken waarin de waarde voor GPP_A wordt ingesteld op 12345678 zoals weergegeven in het voorbeeld.

```
<flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile>
```

Stap 4 Sla het profiel op met de naam `basic.txt` in de hoofdmap van de TFTP-server.

U kunt controleren of de TFTP-server juist is geconfigureerd: verzoek het bestand `basic.txt` via een TFTP-client anders dan de telefoon. Bij voorkeur gebruikt u een TFTP-client die wordt uitgevoerd op een andere host dan de inrichtingsserver.

Stap 5 Open de webbrowser van de computer op de beheerpagina/geavanceerde configuratiepagina. Bijvoorbeeld als het IP-adres van de telefoon 192.168.1.100 is:

```
http://192.168.1.100/admin/advanced
```

Stap 6 Selecteer het tabblad **Spraak** > **Inrichting** en controleer de waarden van de parameters voor algemene doeleinden GPP_A tot GPP_P. Deze zouden leeg moeten zijn.

Stap 7 Hersynchroniseer de testtelefoon met het `basic.txt`-configuratieprofiel door de URL voor hersynchronisatie in een browservenster te openen.

Als het IP-adres van de TFTP-server 192.168.1.200 is, zou de opdracht vergelijkbaar moeten zijn met het volgende voorbeeld:

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

Wanneer de telefoon deze opdracht ontvangt, verzoekt het apparaat op adres 192.168.1.100 het bestand `basic.txt` van de TFTP-server op IP-adres 192.168.1.200. De telefoon parseert het gedownloade bestand vervolgens en werkt de parameter GPP_A bij met de waarde 12345678.

Stap 8 Verifieer dat de parameter correct is bijgewerkt: vernieuw de configuratiepagina van de webbrowser op de computer en selecteer het tabblad **Spraak** > **Inrichting**.

De parameter GPP_A moet de waarde 12345678 nu bevatten.

Berichten vastleggen op de Syslog-server

Als een syslog-server is geconfigureerd op de telefoon door het gebruik van de parameters, worden er bij de bewerkingen voor hersynchroniseren en upgraden berichten naar de syslog-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).

U kunt de parameters ook configureren in het configuratiebestand voor de telefoon met XML-code (cfg.xml). Zie de syntaxis van de reeks in Systeemlogparameters, op pagina 5 voor meer informatie over het configureren van de parameters.

Voordat u begint

- Er wordt een syslog-server geïnstalleerd en geconfigureerd.
- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

Stap 1 Klik op **Spraak** > **Systeem**.

Stap 2 Voer in de sectie **Optional Network Configuration** (Optionele netwerkconfiguratie) het IP-adres van de server in bij **Syslog Server** en geef desgewenst een **Syslog Identifier** (Syslog-id) op zoals is gedefinieerd in Systeemlogparameters, op pagina 5.

Stap 3 U kunt optioneel de inhoud van de syslog-berichten definiëren met **Log Request Msg** (Aanvraagbericht registreren), **Log Success Msg** (Succesbericht registreren) en **Log Failure Msg** (Foutbericht registreren), zoals is gedefinieerd in Systeemlogparameters, op pagina 5.

De velden waarmee de inhoud van syslog-berichten wordt gedefinieerd, bevinden zich in de sectie **Configuratieprofiel** van het tabblad **Spraak** > **Inrichting**. Als u de berichtinhoud niet opgeeft, worden de standaardinstellingen in de velden gebruikt. Als een van deze velden wordt gewist, wordt het bijbehorende syslog-bericht niet gegenereerd.

Stap 4 Klik op **Alle wijzigingen indienen** om de configuratie toe te passen.

Stap 5 Controleer de geldigheid van de configuratie.

a) Voer een TFTP-hersynchronisatie uit. Zie Hersynchroniseren via TFTP, op pagina 3.

Het apparaat genereert twee syslog-berichten tijdens het hersynchroniseren. Het eerste bericht geeft aan dat er een verzoek wordt uitgevoerd. Het tweede bericht markeert of de hersynchronisatie is gelukt of is mislukt.

b) Verifieer dat uw syslog-server berichten heeft ontvangen die vergelijkbaar zijn met het volgende:

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef: hersynchronisatie aanvragen tftp://192.168.1.200/basic.txt

CP-88xx-3PCC 00:0e:08:ab:cd:ef: geslaagde hersynchronisatie tftp://192.168.1.200/basic.txt
```

Systeemlogparameters

De volgende tabel definieert de functie en het gebruik van de syslogparameters in de sectie **Optionele netwerkconfiguratie** op het tabblad **Spraak** > **Systeem** op de telefoonwebpagina. 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 1: Parameters voor syslog

Naam van parameter	Beschrijving en standaardwaarde
Syslog-server	Hiermee wordt de server opgegeven voor het registreren van telefoonsysteeminformatie en kritieke gebeurtenissen. Als Debug-server en Syslog-server beide zijn opgegeven, worden Syslog-berichten ook voor de Debug-server geregistreerd. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Syslog_Server ua="na">10.74.30.84</Syslog_Server>` • **Geef op de telefoonwebpagina** de Syslog-server op.

Naam van parameter	Beschrijving en standaardwaarde
Syslog-ID	Selecteer het apparaat-ID dat moet worden opgenomen in de syslogmeldingen die naar de syslog-server worden geüpload. Het apparaat-ID wordt na de tijdstempel in elke melding weergegeven. De opties voor de id's zijn: • Geen: geen apparaat-ID • $MA: het MAC-adres van de telefoon, uitgedrukt als een doorlopende reeks van kleine letters en cijfers. Voorbeeld: `c4b9cd811e29` • $MAU: het MAC-adres van de telefoon, uitgedrukt als een doorlopende reeks van hoofdletters en cijfers. Voorbeeld: `C4B9CD811E29` • $MAC: het MAC-adres van de telefoon in de standaardindeling met scheidende dubbelpunten. Voorbeeld: `c4:b9:cd:81:1e:29` • $SN: het productserienummer van de telefoon. • **Voer in het telefoonconfiguratiebestand met XML(cfg.xml)** een tekenreeks in de volgende notatie in: `<Syslog_Identifier ua="na">$MAC</Syslog_Identifier>` • **Op de telefoonwebpagina** selecteert u een id in de lijst. Standaard: Geen
Aanvraagbericht registreren	Het bericht dat naar de Syslog-server wordt verzonden aan het begin van een hersynchronisatiepoging. Als er geen waarde is opgegeven, wordt het syslogbericht niet gegenereerd. De standaardwaarde is `$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH` • **Voer in het telefoonconfiguratiebestand met XML(cfg.xml)** een tekenreeks in de volgende notatie in: `<Log_Request_Msg ua="na">$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH</Log_Request_Msg>`
Succesbericht registreren	Het Syslog-bericht dat wordt uitgegeven na een succesvolle voltooiing van een hersynchronisatiepoging. Als er geen waarde is opgegeven, wordt het syslogbericht niet gegenereerd. Voer **in het configuratiebestand van de telefoon met XML (cfg.xml)** een tekenreeks in de volgende indeling in: `<Log_Success_Msg ua="na">$PN $MAC -- Successful resync $SCHEME://$SERVIP:$PORT$PATH</Log_Success_Msg>`
Foutbericht registreren	Het Syslog-bericht dat wordt uitgegeven na een mislukte hersynchronisatiepoging. Als er geen waarde is opgegeven, wordt het syslogbericht niet gegenereerd. De standaardwaarde is `$PN $MAC -- Hersynchronisatie mislukt: $ERR` Voer **in het configuratiebestand van de telefoon met XML (cfg.xml)** een tekenreeks in de volgende indeling in: `<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed: $ERR</Log_Failure_Msg>`

Unieke profielen, macro-uitbreiding en HTTP

In een implementatie waarbij elke telefoon moet worden geconfigureerd met verschillende waarden voor sommige parameters, zoals User_ID of Display_Name, kan de serviceprovider een uniek profiel maken voor elk geïmplementeerd apparaat en deze profielen hosten op een inrichtingsserver. Elke telefoon moet afzonderlijk worden geconfigureerd om te hersynchroniseren naar diens eigen profiel, volgens een vooraf bepaalde naamgevingsconventie voor profielen.

De URL-syntaxis voor het profiel kan identificerende informatie bevatten die specifiek is voor elke telefoon, zoals het MAC-adres of het serienummer, door de macro-uitbreiding van ingebouwde variabelen te gebruiken. Met macro-uitbreiding is het niet meer nodig om deze waarden op meerdere locaties binnen elk profiel te specificeren.

Een profielregel ondergaat de macro-uitbreiding voordat de regel wordt toegepast op de telefoon. De macro-uitbreiding bepaalt een aantal waarden, bijvoorbeeld:

- $MA is een uitbreiding op het 12-cijferige MAC-adres van het toestel (met kleine hexadecimale tekens). Bijvoorbeeld 000e08abcdef.
- $SN is een uitbreiding op het serienummer van de eenheid. Bijvoorbeeld 88012BA01234.

Andere waarden kunnen op dezelfde wijze macro-uitbreiding ondergaan, inclusief alle parameters voor algemene doeleinden; GPP _A tot GPP_P. U kunt een voorbeeld van dit proces zien in Hersynchroniseren via TFTP, op pagina 3. Macro-uitbreiding is niet beperkt tot de URL-bestandsnaam, maar kan ook worden toegepast op enig onderdeel van de profielregelparameter. Naar deze parameters wordt verwezen als $P tot en met $A. Zie Variabelen voor macro-uitbreiding voor een volledige lijst met variabelen die beschikbaar zijn voor de macro-uitbreiding.

In deze oefening is een profiel specifiek voor een telefoon ingericht op een TFTP-server.

Inrichting van specifiek IP-telefoonprofiel op een TFTP-server

Procedure

Stap 1 Verkrijg het MAC-adres van de telefoon van het productlabel. (Het MAC-adres is het nummer, met cijfers en kleine hexadecimale tekens, zoals 000e08aabbcc.

Stap 2 Kopieer het configuratiebestand `basic.txt` (zoals beschreven in Hersynchroniseren via TFTP, op pagina 3) naar een nieuw bestand met de naam `CP-xxxx-3PCC mac-adres.cfg` (vervang hierbij `xxxx` met het modelnummer en `mac-adres` met het MAC-adres van de telefoon).

Stap 3 Verplaats het nieuwe bestand in de virtuele hoofdmap van de TFTP-server.

Stap 4 Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Stap 5 Selecteer **Spraak** > **Inrichting**.

Stap 6 Voer `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` in het veld **Profielregel** in.

```
<Profile_Rule>
  tftp://192.168.1.200/CP-6841-3PCC$MA.cfg
</Profile_Rule>
```

Stap 7 Klik op **Submit All Changes**. Hierdoor wordt er direct opnieuw opgestart en gehersynchroniseerd.

Wanneer de volgende hersynchronisatie wordt uitgevoerd, haalt de telefoon het nieuwe bestand op door de macro-expressie $MA uit te breiden tot het MAC-adres.

Hersynchroniseren via HTTP GET

HTTP biedt een meer betrouwbaar mechanisme voor hersynchronisatie dan TFTP omdat HTTP een TCP-verbinding tot stand brengt en TFT het minder betrouwbare UDP gebruikt. Bovendien bieden HTTP-servers verbeterde functies voor filteren en logboeken vergeleken met TFTP-servers.

Aan de kant van de client is er geen speciale configuratie-instelling op de server nodig voor de telefoon om te kunnen hersynchroniseren met HTTP. De syntaxis van de parameter Profile_Rule voor het gebruik van HTTP met de GET-methode is vergelijkbaar met de syntaxis die wordt gebruikt voor TFTP. Als een standaard webbrowser een profiel kan ophalen vanuit uw HTTP-server, zou de telefoon dit ook moeten kunnen doen.

Hersynchroniseren met HTTP GET

Procedure

Stap 1 Installeer een HTTP-server op de lokale computer of een andere toegankelijke host.

De open-source Apache-server kan worden gedownload van internet.

Stap 2 Kopieer het configuratieprofiel `basic.txt` (zoals beschreven in Hersynchroniseren via TFTP, op pagina 3) op de virtuele hoofdmap van de geïnstalleerde server.

Stap 3 Als u de juiste serverinstallatie en toegang tot `basic.txt` wilt verifiëren, opent u het profiel met een webbrowser.

Stap 4 Wijzig de Profile_Rule van de testtelefoon om naar de HTTP-server te verwijzen in plaats van de TFTP-server, zodat het profiel periodiek wordt gedownload.

Bijvoorbeeld, ervan uitgaande dat de HTTP-server zich op 192.168.1.300 bevindt, voert u de volgende waarde in:

```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```

Stap 5 Klik op **Submit All Changes**. Hierdoor wordt er direct opnieuw opgestart en gehersynchroniseerd.

Stap 6 Bekijk de syslog-berichten die de telefoon verzendt. De periodieke hersynchronisaties zouden nu het profiel van de HTTP-server moeten ophalen.

Stap 7 In de HTTP-serverlogboeken ziet u hoe de informatie die de testtelefoon identificeert in het logboek van gebruikersagenten verschijnt.

Deze informatie moet de fabrikant, de productnaam, de huidige firmwareversie en het serienummer bevatten.

Inrichting via Cisco XML

Voor elk van de telefoons, hier aangeduid als xxxx, kunt u de inrichting uitvoeren via Cisco XML-functies.

U kunt een XML-object verzenden naar de telefoon met een SIP Notify-pakket of een HTTP Post naar de CGI-interface van de telefoon: `http://IPAddressPhone/CGI/Execute`.

De CP-xxxx-3PCC breidt de Cisco XML-functie uit om inrichting via een XML-object te ondersteunen:

```
<CP-xxxx-3PCCExecute>
        <ExecuteItem URL=Resync:[profile-rule]/>
</CP-xxxx-3PCCExecute>
```

Nadat de telefoon het XML-object heeft ontvangen, wordt het inrichtingsbestand uit [profiel-regel] gedownload. Deze regel gebruikt macro's om de ontwikkeling van de XML-servicestoepassing te vereenvoudigen.

URL-oplossing met macro-uitbreiding

Submappen met meerdere profielen op de server bieden een handige methode voor het beheren van een groot aantal geïmplementeerde apparaten. De profiel-URL kan het volgende bevatten:

- Een inrichtingsservernaam of een expliciet IP-adres. Als het profiel de inrichtingsserver op naam identificeert, voert de telefoon een DNS-zoekopdracht uit om de naam op te halen.
- Een niet-standaard serverpoort die wordt opgegeven in de URL met behulp van de standaardsyntaxis `:poort` na de servernaam.
- De submap van de virtuele hoofdmap van de server waar het profiel is opgeslagen, opgegeven door de standaard URL-notatie te gebruiken en beheerd door macro-uitbreiding.

Bijvoorbeeld: de volgende Profile_Rule vraagt het profielbestand ($PN.cfg), in de serversubmap `/cisco/config`, op van de TFTP-server die wordt uitgevoerd op de host prov.telco.com die luistert naar een verbinding op poort 6900:

```
<Profile_Rule>
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
</Profile_Rule>
```

Een profiel voor elke telefoon kan worden geïdentificeerd in een parameter voor algemene doeleinden, waarbij binnen een gemeenschappelijke profielregel met behulp van macro-uitbreiding naar de waarde wordt verwezen.

Stel bijvoorbeeld dat GPP_B wordt gedefinieerd als `Dj6Lmp23Q`.

De Profile_Rule heeft de waarde:

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

Wanneer het apparaat hersynchroniseert en de macro's worden uitgebreid, vraagt de telefoon met MAC-adres 000e08012345 het profiel op met de naam die het MAC-adres van het apparaat bevat op de volgende URL:

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

Een apparaat automatisch hersynchroniseren

Een apparaat kan periodiek hersynchroniseren naar de inrichtingsserver om ervoor te zorgen dat eventuele profielwijzigingen op de server worden doorgegeven aan het eindpuntapparaat (in tegenstelling tot het verzenden van een expliciet verzoek tot hersynchronisatie naar het eindpunt).

Zodat de telefoon periodiek hersynchroniseert naar een server, wordt er een configuratieprofiel-URL gedefinieerd met de parameter Profile_Rule en wordt er een hersynchronisatieperiode gedefinieerd met de parameter Resync_Periodic.

Voordat u begint

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

Procedure

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

Stap 2 Definieer de parameter Profile_Rule. In dit voorbeeld wordt verondersteld dat het IP-adres van de TFTP-server 192.168.1.200 is.

Stap 3 Voer in het veld **Resync Periodic** een kleine waarde in om te testen, zoals **30** seconden.

Stap 4 Klik op **Alle wijzigingen verzenden**.

Met de nieuwe parameterinstellingen zal de telefoon twee keer per minuut hersynchroniseren naar het configuratiebestand dat de URL specificeert.

Stap 5 Controleer de resulterende berichten in de syslog-tracering (zoals beschreven in de sectie Syslog gebruiken om berichten op te slaan, op pagina 2).

Stap 6 Zorg ervoor dat het veld **Resync On Request** is ingesteld op **Ja**.

```
<Resync_On_Reset>Yes</Resync_On_Reset>
```

Stap 7 Zet de telefoon uit en weer aan om een hersynchronisatie naar de inrichtingsserver af te dwingen.

Als de hersynchronisatie mislukt om een bepaalde reden, zoals dat de server niet reageert, wacht het toestel (voor het aantal seconden dat is geconfigureerd in **Resync Error Retry Delay**) voordat deze opnieuw probeert te hersynchroniseren. Als de **Resync Error Retry Delay** wordt ingesteld op 0, probeert de telefoon niet nogmaals te hersynchroniseren na een mislukte hersynchronisatiepoging.

Stap 8 (Optioneel) Stel de waarde van het veld **Resync Error Retry Delay** in op een klein nummer, zoals **30**.

```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```

Stap 9 Schakel de TFTP-server uit en observeer de resultaten in de syslog-uitvoer.

Parameters voor het hersynchroniseren van profielen

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

Parameter	Beschrijving
Inrichting inschakelen	Hiermee worden hersynchronisatieacties toegestaan of geweigerd. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Provision_Enable ua="na">Ja</Provision_Enable>` • **Op de webpagina van de telefoon** stelt u dit veld in op **Ja** om hersynchronisatieacties toe te staan of op **Nee** om deze te blokkeren. Standaard: Ja
Hersynchroniseren bij reset	Hiermee geeft u aan of de telefoon de configuraties opnieuw synchroniseert met de inrichtingsserver na het opstarten en na elke upgradepoging. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_On_Reset ua="na">Ja</Resync_On_Reset>` • **Op de webpagina van de telefoon** stelt u dit veld in op **Ja** om hersynchronisatie bij opstarten of resetten toe te staan of op **Nee** om hersynchronisatie bij opstarten of resetten te blokkeren. Standaard: Ja
Resync Random Delay (Willekeurige vertraging hersynchr.)	Hiermee wordt overbelasting van de inrichtingsserver voorkomen wanneer een groot aantal apparaten tegelijk opstart en de eerste configuratiepoging uitvoeren. Deze vertraging heeft alleen effect op de eerste configuratiepoging, na het inschakelen of resetten van een apparaat. De parameter is het maximale tijdsinterval dat het apparaat wacht voordat u contact opneemt met de inrichtingsserver. De werkelijke vertraging is een pseudo-willekeurig getal tussen 0 en deze waarde. Deze parameter is een eenheid van 20 seconden. Geldige waarden zijn van 0 tot 65535. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_Random_Delay ua="na">2</Resync_Random_Delay>` • **Op de webpagina van de telefoon** geeft u het aantal eenheden (20 seconden) op voor de telefoon om de synchronisatie te vertragen na het opstarten of resetten. De standaardwaarde is 2 (40 seconden).

Parameter	Beschrijving
Resync At (HHmm) (Hersynchroniseren om (UUmm))	De uren en minuten (UUmm) waarop het apparaat hersynchroniseert met de inrichtingsserver. De waarde voor dit veld moet een viercijferig nummer zijn van 0000 tot 2400 om de tijd in de indeling UUmm aan te geven. 0959 geeft bijvoorbeeld 09:59 aan. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_At__HHmm_ ua="na">0959</Resync_At__HHmm_>` • **Geef op de webpagina telefoon** de tijd op in de uumm-indeling voor de telefoon om de synchronisatie te starten. De standaardwaarde is leeg. Als de waarde ongeldig is, wordt de parameter genegeerd. Als deze parameter is ingesteld met een geldige waarde, wordt de parameter **Periodiek hersynchroniseren** genegeerd.
Resync At Random Delay (Hersynchr. bij willekeurige vertraging)	Hiermee wordt overbelasting van de inrichtingsserver voorkomen wanneer een groot aantal apparaten tegelijk opstart. Om te voorkomen dat de server overbelast raakt met verzoeken voor hersynchronisatie van meerdere telefoons, wordt de telefoon gehersynchroniseerd binnen het bereik van de uren en minuten, en de uren en minuten plus de willekeurige vertraging (hhmm, hhmm + random_delay). Als de willekeurige vertraging bijvoorbeeld = (Hersynchroniseren bij willekeurige vertraging +30)/60 minuten is, wordt de ingevoerde waarde in seconden geconverteerd naar minuten, met afronding naar boven tot de volgende minuut om het uiteindelijke random_delay-interval te berekenen. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_At_Random_Delay ua="na">600</Resync_At_Random_Delay>` • **Geef op de webpagina van de telefoon** de tijdperiode in seconden op. Geldige waarden zijn van 600 tot 65535. Als de waarde lager is dan 600, wordt de interne willekeurige vertraging tussen 0 en 600. De standaardwaarde is 600 seconden (10 minuten).

Parameter	Beschrijving
Resync Periodic (Periodiek hersynchroniseren)	Het tijdsinterval tussen periodieke hersynchronisatie met de inrichtingsserver. De gekoppelde hersynchronisatietimer is alleen actief na de eerste geslaagde synchronisatie met de server. De geldige indelingen zijn als volgt: • Een geheel getal Voorbeeld: een invoer van **`3000`** geeft aan dat de volgende hersynchronisatie over 3000 seconden optreedt. • Meerdere gehele getallen Voorbeeld: een invoer van **`600,1200,300`** geeft aan dat de eerste hersynchronisatie optreedt over 600 seconden, de tweede hersynchronisatie 1200 seconden na de eerste en de derde hersynchronisatie 300 seconden na de tweede. • Een tijdsbereik Bijvoorbeeld, een invoer van **`2400+30`** geeft aan dat de volgende hersynchronisatie tussen 2400 en 2430 seconden na een geslaagde hersynchronisatie optreedt. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_Periodic ua="na">3600</Resync_Periodic>` • **Geef op de webpagina van de telefoon** de tijdperiode in seconden op. Stel deze parameter in op nul om periodieke hersynchronisatie uit te schakelen. De standaardwaarde is 3600 seconden.

Parameter	Beschrijving
Resync Error Retry Delay (Vertraging nieuwe poging na hersynchronisatiefout)	Als een hersynchronisatiebewerking mislukt omdat het IP-telefonieapparaat geen profiel van de server kan ophalen, omdat het gedownloade bestand beschadigd is of omdat er een interne fout optreedt, probeert het apparaat opnieuw te hersynchroniseren na een in seconden gespecificeerde tijd. De geldige indelingen zijn als volgt: • Een geheel getal Voorbeeld: een invoer van **300** geeft aan dat de volgende poging tot hersynchronisatie over 300 seconden optreedt. • Meerdere gehele getallen Voorbeeld: een invoer van **600,1200,300** geeft aan dat de eerste poging optreedt over 600 seconden na de fout, de tweede poging 1200 seconden nadat de eerste poging is mislukt en de derde poging 300 seconden nadat de tweede poging is mislukt. • Een tijdsbereik Bijvoorbeeld, een invoer van **2400+30** geeft aan dat de volgende poging tussen 2400 en 2430 seconden na een mislukte hersynchronisatie optreedt. Als de vertraging wordt ingesteld op 0, probeert het apparaat niet nogmaals te hersynchroniseren na een mislukte hersynchronisatiepoging. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: <Resync_Error_Retry_Delay ua="na">60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400</Resync_Error_Retry_Delay> • **Geef op de webpagina van de telefoon** de tijdperiode in seconden op. Standaard: 60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400

Parameter	Beschrijving
Forced Resync Delay (Geforceerde vertraging hersynchronisatie)	Maximale vertraging (in seconden) die de telefoon wacht voordat een hersynchronisatie wordt uitgevoerd. Het apparaat voert geen hersynchronisatie uit terwijl een van de telefoonlijnen actief is. Omdat een hersynchronisatie enkele seconden kan duren, is het gewenst om te wachten totdat het apparaat gedurende langere tijd inactief is voordat hersynchronisatie wordt uitgevoerd. Hierdoor kan een gebruiker zonder onderbreking oproepen blijven plaatsen. Het apparaat heeft een timer die begint af te tellen wanneer alle lijnen inactief worden. Deze parameter is de eerste waarde van de teller. Hersynchronisaties worden uitgesteld tot deze teller op nul staat. Geldige waarden zijn van 0 tot 65535. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Forced_Resync_Delay ua="na">14400</Forced_Resync_Delay>` • **Geef op de webpagina van de telefoon** de tijdperiode in seconden op. De standaardwaarde is 14.400 seconden.
Resync From SIP (Hersynchroniseren via SIP)	Hiermee worden aanvragen voor hersynchronisatiebewerkingen geregeld via een SIP NOTIFY-gebeurtenis die vanaf de proxyserver van de serviceprovider naar de telefoon is verzonden. Indien ingeschakeld kan de proxy een hersynchronisatie aanvragen door een SIP NOTIFY-bericht met de koptekst Gebeurtenis: hersynchr. naar het apparaat te verzenden. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_From_SIP ua="na">Ja</Resync_From_SIP>` • **Op de webpagina van de telefoon** selecteert u **Ja** om deze functie in te schakelen of op **Nee** om deze uit te schakelen. Standaard: Ja
Resync After Upgrade Attempt (Hersynchroniseren na upgradepoging)	Hiermee schakelt u of de hersynchronisatiebewerking in of uit nadat een upgrade is uitgevoerd. Als **Ja** is geselecteerd, wordt de synchronisatie na een firmware-upgrade gestart. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_After_Upgrade_Attempt ua="na">Ja</Resync_After_Upgrade_Attempt>` • **Op de webpagina van de telefoon** selecteert u **Ja** om hersynchroniseren na een firmware-upgrade te starten of **Nee** op niet opnieuw synchroniseren. Standaard: Ja

Parameter	Beschrijving

Resync Trigger 1 (Trigger 1 hersynchronisatie)
Resync Trigger 2 (Trigger 2 hersynchronisatie)
	Als het resultaat van de logische vergelijking in de deze parameters FALSE is, wordt hersynchroniseren niet geactiveerd, zelfs niet wanneer **Hersynchroniseren bij reset** is ingesteld op **TRUE**. Deze trigger voor hersynchronisatie wordt alleen genegeerd bij hersynchroniseren via directe actie-URL en SIP-melding.
	De parameters kunnen worden geprogrammeerd met een voorwaardelijke expressie die macro-uitbreiding ondergaat. Zie Variabelen voor macro-uitbreiding voor de geldige macro-uitbreidingen.
	• **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in:
	`<Resync_Trigger_1 ua="na">$UPGTMR gt 300 en $PRVTMR ge 600</Resync_Trigger_1>`
	`<Resync_Trigger_2 ua="na"/>`
	• **Op de webpagina van de telefoon**geeft u de triggers op.
	Standaard: leeg

Door gebruiker configureerbare hersynchronisatie	Hiermee kan een gebruiker de telefoon hersynchroniseren via het menu op het telefoonscherm. Wanneer deze is ingesteld op **Ja**, kan een gebruiker de telefoon configuratie opnieuw synchroniseren door de profielregel van de telefoon in te voeren. Wanneer **Nee**is ingesteld, wordt de parameter **Profielregel** niet weergegeven in het menu op het telefoonscherm. De parameter **Profielregel** bevindt zich onder **Toepassingen** > **Apparaatbeheer**. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<User_Configurable_Resync ua="na">Ja</User_Configurable_Resync>` • Op de **webpagina telefoon** selecteert u **Ja** om de parameter **profielregel** in het telefoonmenu weer te geven of selecteert u **Nee** om deze parameter te verbergen. Standaard: Ja
Resync Fails On FNF (Hersynchronisatie bij FNF)	Een hersynchronisatie wordt meestal als mislukt beschouwd als een aangevraagd profiel niet van de server wordt ontvangen. Deze parameter negeert dit gedrag. Wanneer deze optie is ingesteld op **Nee**, accepteert het apparaat een `file-not-found`-antwoord van de server als een succesvolle hersynchronisatie. • **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in: `<Resync_Fails_On_FNF ua="na">Ja</Resync_Fails_On_FNF>` • **Op de webpagina telefoon** selecteert u **Ja** als u een `niet-gevonden` antwoord wilt ontvangen als een mislukte hersynchronisatie, of selecteert u **Nee** als u een `niet-gevonden` antwoord als een geslaagde hersynchronisatie wilt door voeren. Standaard: Ja

Parameter	Beschrijving

Profielverificatietype	Geeft de aanmeldgegevens aan die moeten worden gebruikt voor de profielaccountverificatie. De beschikbare opties zijn:
	• **Uitgeschakeld**: schakelt de profielaccountfunctie uit. Wanneer deze functie is uitgeschakeld, wordt het menu **Profielaccountinstelling** niet weergegeven op het scherm van de telefoon.
	• **Standaard HTTP-verificatie**: de HTTP-aanmeldgegevens worden gebruikt om de profielaccount te verifiëren.
	• **XSI-verificatie**: XSI- of XSI SIP-aanmeldgegevens worden gebruikt om de profielaccount te verifiëren. De aanmeldgegevens voor de verificatie hangen af van het **XSI-verificatietype** voor de telefoon:
	  • Wanneer het **XSI-verificatietype** voor de telefoon is ingesteld op **Aanmeldgegevens**, worden de XSI-aanmeldgegevens gebruikt.
	  • Wanneer het **XSI-verificatietype** voor de telefoon is ingesteld op **SIP-aanmeldgegevens**, worden de XSI SIP-aanmeldgegevens gebruikt.
	• **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in:
	`<Profile_Authentication_Type ua="na">Basis-HTTP-verificatie</Profile_Authentication_Type>`
	• **Op de webpagina van de telefoon**selecteert u een optie in de lijst voor de telefoon om de synchronisatie van het profiel te verifiëren.
	Standaard: standaard HTTP-verificatie

Profielregel
Profielregel B
Profielregel C
Profielregel D
	Elke profielregel informeert de telefoon over een bron waarvan hij een profiel kan halen (configuratiebestand). Tijdens elke hersynchronisatie past de telefoon alle profielen achtereenvolgens toe.
	Als u AES-256-CBC-codering op de configuratiebestanden toepast, geef de coderingssleutel dan als volgt op met het trefwoord **`--sleutel`**:
	`[--toets <encryption key>]`
	U kunt de coderingssleutel optioneel tussen dubbele aanhalingstekens (") plaatsen.
	• **Voer in het telefoonconfiguratiebestand met XML (cfg.xml)** een tekenreeks in deze notatie in:
	`<Profile_Rule ua="na">/$PSN.xml</Profile_Rule>`
	`<Profile_Rule_B ua="na"/>`
	`<Profile_Rule_C ua="na"/>`
	`<Profile_Rule_D ua="na"/>`
	• **Op de webpagina van de telefoon** geeft u de profielregel op.
	Standaard: **`/$PSN.xml`**

Parameter	Beschrijving
DHCP Option To Use (Te gebruiken DHCP-optie)	DHCP-opties, gescheiden door komma's, gebruikt om firmware en profielen op te halen. Standaard: 66,160,159,150,60,43,125
Te gebruiken DHCPv6-optie	DHCP-opties, gescheiden door komma's, gebruikt om firmware en profielen op te halen. Standaard: 17,160,159

Uw telefoons instellen voor onboarding via activeringscode

Als uw netwerk is geconfigureerd voor onboarding via een activeringscode, kunt u nieuwe telefoons zo instellen dat deze automatisch op een veilige manier worden geregistreerd. U genereert een unieke activeringscode van 16 cijfers en verstrekt deze aan elke gebruiker. De gebruiker voert de activeringscode in en de telefoon wordt automatisch geregistreerd. Met deze functie blijft uw netwerk beveiligd omdat de telefoon pas kan worden geregistreerd als de gebruiker een geldige activeringscode invoert.

Activeringscodes kunnen slechts één keer worden gebruikt en hebben een vervaldatum. Als een gebruiker een verlopen code invoert, wordt op het scherm van de telefoon `Ongeldige activeringscode` weergegeven. In dat geval geeft u de gebruiker een nieuwe code.

Deze functie is beschikbaar in firmwareversie 11-2-3MSR1, BroadWorks Application Server versie 22.0 (patch AP.as.22.0.1123.ap368163 en de bijbehorende afhankelijkheden). U kunt ook telefoons met oudere firmware wijzigen om deze functie te gebruiken. Gebruik hiervoor de volgende procedure.

Voordat u begint

Zorg ervoor dat u de service activation.webex.com via uw firewall toestaat onboarding via activeringscode te ondersteunen.

Als u voor het verbinden een proxyserver wilt instellen, moet u controleren of de proxyserver correct is geconfigureerd. Zie Een proxyserver instellen.

Open de webpagina van de telefoon. De webinterface van de telefoon openen

Procedure

Stap 1 Reset de telefoon op de fabrieksinstellingen.

Stap 2 Selecteer **Spraak** > **Inrichting** > **Configuratieprofiel**.

Stap 3 Voer de profielregel in het veld **Profielregel** in, zoals wordt beschreven in de tabel Parameters voor de inrichting van activeringscodes, op pagina 19.

Stap 4 (Optioneel) Voer in de sectie **Firmware-upgrade** de upgraderegel in het veld **Upgraderegel** in, zoals wordt beschreven in de tabel Parameters voor de inrichting van activeringscodes, op pagina 19.

Stap 5 Verzend alle wijzigingen.

Parameters voor de inrichting van activeringscodes

In de volgende tabel wordt een definitie gegeven van de functie en het gebruik van de parameters voor de activeringscode in de sectie **Configuratieprofiel** op het tabblad **Spraak** > **Inrichting** op de telefoonwebpagina. Hij definieert ook de syntaxis van de tekenreeks die aan het telefoonconfiguratiebestand (cfg.xml) is toegevoegd met XML-code om een parameter te configureren.

Parameter	Beschrijving

Profielregel
Profielregel B
Profielregel C
Profielregel D
	Profielregels voor externe configuratie die achtereenvolgens worden geëvalueerd. Met elke hersynchronisatiebewerking kunnen meerdere bestanden worden opgehaald, mogelijk beheerd door verschillende servers.
	Voer een van de volgende handelingen uit:
	• Voer in het XML-bestand met de telefoonconfiguratie (cfg.xml) een tekenreeks in deze notatie in:
	`<Profile_Rule ua="na">gds://</Profile_Rule>`
	• In de telefoonwebinterface voert u een tekenreeks in deze notatie in:
	`gds://`
	Standaard: /$PSN.xml

Upgraderegel	Geeft het script voor de firmware-upgrade op waarmee de upgradevoorwaarden en de bijbehorende firmware-URL's worden gedefinieerd. Hierbij wordt dezelfde syntaxis als bij profielregel gebruikt.
	Voer een van de volgende handelingen uit:
	• Voer in het XML-bestand met de telefoonconfiguratie (cfg.xml) een tekenreeks in deze notatie in:
	`<Upgrade_Rule ua="na">http://<server ip address>/ sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>`
	• Voer in de telefoonwebinterface de upgraderegel in:
	`protocol://server[:port]/profile_pathname`
	Bijvoorbeeld:
	`tftp://192.168.1.5/image/sip88xx.11-2-3MSR1-1.loads`
	Als er geen protocol wordt opgegeven, wordt TFTP verondersteld. Als er geen servernaam wordt opgegeven, wordt de host die de URL aanvraagt, gebruikt als de servernaam. Als er geen poort wordt opgegeven, wordt de standaardpoort gebruikt (69 voor TFTP, 80 voor HTTP of 443 voor HTTPS).
	Standaard: leeg

Hersynchroniseren via beveiligde HTTPS

Deze mechanismen zijn beschikbaar op de telefoon voor hersynchronisatie met behulp van een beveiligd communicatieproces:

- Standaard hersynchroniseren via HTTPS
- HTTPS met clientcertificaatverificatie
- HTTPS-clientfiltering en dynamische inhoud

Standaard hersynchroniseren via HTTPS

Met HTTPS wordt SSL toegevoegd aan HTTP voor externe inrichting, zodat:

- de telefoon de inrichtingsserver kan verifiëren.
- de inrichtingsserver de telefoon kan verifiëren.
- Vertrouwelijkheid van informatie die wordt uitgewisseld tussen de telefoon en de inrichtingsserver wordt gegarandeerd.

SSL genereert geheime (symmetrische) sleutels en wisselt deze uit voor elke verbinding tussen de telefoon en de server, met openbare/privé sleutelparen die vooraf zijn geïnstalleerd op de telefoon en de inrichtingsserver.

Aan de kant van de client is er geen speciale configuratie-instelling op de server nodig voor de telefoon om te kunnen hersynchroniseren met HTTPS. De syntaxis van de parameter Profile_Rule voor het gebruik van HTTPS met de GET-methode is vergelijkbaar met de syntaxis die wordt gebruikt voor HTTP of TFTP. Als een standaard webbrowser een profiel kan ophalen vanuit uw HTTPS-server, zou de telefoon dit ook moeten kunnen doen.

Naast het installeren van een HTTPS-server, moet een SSL-servercertificaat met ondertekening van Cisco op de inrichtingsserver worden geïnstalleerd. De apparaten kunnen niet hersynchroniseren met een server die HTTPS gebruikt tenzij de server een door Cisco ondertekend servercertificaat levert. Instructies voor het maken van ondertekende SSL-certificaten voor spraakproducten zijn te vinden op https://supportforums.cisco.com/docs/DOC-9852.

Verifiëren met Standaard hersynchroniseren via HTTPS

Procedure

Stap 1 Installeer een HTTPS-server op een host waarvan het IP-adres bekend is voor de DNS-netwerkserver via normale hostnaamvertaling.

De open-source Apache-server kan worden geconfigureerd om te werken als een HTTPS-server wanneer het open-source mod_ssl-pakket is geïnstalleerd.

Stap 2 Genereer een ondertekeningsverzoek voor het servercertificaat voor de server. Voor deze stap moet u mogelijk het open-source OpenSSL-pakket of gelijkwaardige software installeren. Indien u OpenSSL gebruikt, is de opdracht om het standaard CSR-bestand te genereren als volgt:

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

Deze opdracht genereert een gecombineerde openbare/privésleutel, die wordt opgeslagen in het bestand `privkey.pem`.

Stap 3 Stuur het CSR-bestand (provserver.csr) naar Cisco om het te laten ondertekenen.

Een ondertekend servercertificaat wordt teruggezonden (provserver.cert) samen met een Sipura CA Client Root-certificaat, spacroot.cert.

Zie https://supportforums.cisco.com/docs/DOC-9852 voor meer informatie.

Stap 4 Sla het ondertekende servercertificaat, het bestand met de gecombineerde privésleutel en het clientbasiscertificaat op in de juiste locaties op de server.

In het geval van een Apache-installatie op Linux zijn deze locaties meestal als volgt:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

Stap 5 Start de server opnieuw op.

Stap 6 Kopieer het configuratiebestand `basic.txt` (zoals beschreven in Hersynchroniseren via TFTP, op pagina 3) naar de virtuele hoofdmap van de HTTPS-server.

Stap 7 Controleer of de server correct werkt door `basic.txt` te downloaden van de HTTPS-server met een standaardbrowser vanuit de lokale computer.

Stap 8 Controleer het servercertificaat dat de server levert.

De browser herkent het certificaat waarschijnlijk niet als geldig tenzij de browser vooraf is geconfigureerd voor het accepteren van Cisco als een basis-CA. De telefoons verwachten echter dat het certificaat op deze manier is ondertekend.

Pas de Profile_Rule van het testapparaat aan om een verwijzing naar de HTTPS-server te bevatten, bijvoorbeeld:

```
<Profile_Rule>
https://my.server.com/basic.txt
</Profile_Rule>
```

In dit voorbeeld wordt ervan uitgegaan dat de naam van de HTTPS-server **`my.server.com`** is.

Stap 9 Klik op **Submit All Changes**.

Stap 10 Bekijk de syslog-tracering die de telefoon verzendt.

Het syslog-bericht zou moeten aangeven dat de hersynchronisatie het profiel van de HTTPS-server heeft verkregen.

Stap 11 (Optioneel) Gebruik een Ethernet-protocolanalysator op het telefoonsubnet om te verifiëren dat de pakketten zijn gecodeerd.

In deze oefening is clientcertificaatverificatie niet ingeschakeld. De verbinding tussen de telefoon en de server is gecodeerd. De overdracht is echter niet beveiligd omdat elke client verbinding kan maken met de server en het bestand kan aanvragen, indien de bestandsnaam en maplocatie bekend zijn. Voor beveiligd hersynchroniseren moet de server de client ook verifiëren, zoals aangetoond in de oefening beschreven in HTTPS met clientcertificaatverificatie, op pagina 22.

HTTPS met clientcertificaatverificatie

In de standaardfabriekskonfiguratie verzoekt de server geen SSL-clientcertificaat van een client. Overdracht van het profiel is niet veilig omdat alle clients verbinding kunnen maken met de server en het profiel kunnen verzoeken. U kunt de configuratie bewerken om clientverificatie in te schakelen; de server vereist een clientcertificaat om de telefoon te verifiëren voordat een verbindingsverzoek wordt geaccepteerd.

Vanwege deze vereiste, kan de hersynchronisatiebewerking niet onafhankelijk worden getest via een browser die niet over de juiste referenties beschikt. De uitwisseling van SSL-sleutels binnen de HTTPS-verbinding tussen de testtelefoon en de server kan worden waargenomen met het hulpprogramma ssldump. De tracering van het hulpprogramma toont de interactie tussen client en server.

HTTPS verifiëren met clientcertificaten

Procedure

Stap 1 Clientcertificaatverificatie inschakelen op de HTTPS-server.

Stap 2 Stel het volgende in het serverconfiguratiebestand in Apache (v.2) in:

```
SSLVerifyClient  require
```

Zorg er ook voor dat spacroot.cert is opgeslagen zoals u ziet in de oefening Standaard hersynchroniseren via HTTPS, op pagina 20.

Stap 3 Start de HTTPS-server opnieuw op en observeer de syslogtracering vanaf de telefoon.

Elke keer dat er naar de server wordt gehersynchroniseerd wordt er nu een symmetrische verificatie uitgevoerd, zodat zowel het servercertificaat als het clientcertificaat wordt geverifieerd voordat het profiel wordt overgedragen.

Stap 4 Gebruik ssldump om een verbinding voor het hersynchroniseren tussen de telefoon en de HTTPS-server tot stand te brengen.

Als clientcertificaatverificatie correct op de server is ingeschakeld, geeft de ssldump-tracering een symmetrische uitwisseling van certificaten weer (eerst server-naar-client en vervolgens client-naar-server) vóór de gecodeerde pakketten met het profiel.

Met de clientverificatie ingeschakeld, kan alleen een telefoon met een MAC-adres dat overeenkomt met een geldig clientcertificaat het profiel van de inrichtingsserver verzoeken. De server weigert een verzoek van een gewone browser of een ander niet-geautoriseerd apparaat.

Een HTTPS-server configureren voor clientfiltering en dynamische inhoud

Als de HTTPS-server is geconfigureerd om een clientcertificaat te vereisen, identificeert de informatie in het certificaat de telefoon die wordt gehersynchroniseerd en levert het de correcte configuratie-informatie aan de telefoon.

De HTTPS-server stelt de certificaat-informatie beschikbaar aan CGI-scripts (of gecompileerde CGI-programma's) die worden opgeroepen als onderdeel van het verzoek voor hersynchronisatie. Deze

oefening maakt ter illustratie gebruik van de open-source Perl-scripttaal en er wordt aangenomen dat Apache (v.2) wordt gebruikt als de HTTPS-server.

Procedure

Stap 1 Installeer Perl op de host waarop de HTTPS-server wordt uitgevoerd.

Stap 2 Genereer het volgende Perl-reflectorscript:

```
#!/usr/bin/perl -wT
use strict;
print "Content-Type: text/plain\n\n";
print "<flat-profile><GPP_D>";

print "OU=$ENV{'SSL_CLIENT_I_DN_OU'},\n";
print "L=$ENV{'SSL_CLIENT_I_DN_L'},\n";
print "S=$ENV{'SSL_CLIENT_I_DN_S'}\n";
print "</GPP_D></flat-profile>";
```

Stap 3 Sla dit bestand op met de bestandsnaam `reflect.pl`, met uitvoeringstoestemming (chmod 755 op Linux), in de map CGI-scripts van de HTTPS-server.

Stap 4 Verifieer de toegankelijkheid van CGI-scripts op de server (dat wil zeggen `/cgi-bin/...`).

Stap 5 Wijzig de Profile_Rule op het testapparaat zodat deze hersynchroniseert met het reflectorscript, zoals in het volgende voorbeeld:

```
https://prov.server.com/cgi-bin/reflect.pl?
```

Stap 6 Klik op **Submit All Changes**.

Stap 7 Bekijk de syslogtracering om te controleren dat hersynchroniseren lukt.

Stap 8 Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Stap 9 Selecteer **Spraak** > **Inrichting**.

Stap 10 Verifieer dat de parameter GPP_D de informatie bevat die het script heeft vastgelegd.

Deze informatie bevat de productnaam, het MAC-adres en het serienummer als het testapparaat een uniek certificaat van de fabrikant heeft. De informatie bevat algemene tekenreeksen als het toestel is geproduceerd vóór firmwareversie 2.0.

Een soortgelijk script kan informatie over het apparaat dat hersynchroniseert bepalen en het apparaat vervolgens de juiste configuratieparameterwaarden geven.

HTTPS-certificaten

De telefoon biedt een betrouwbare en veilige inrichtingsstrategie die is gebaseerd op de HTTPS-verzoeken van het apparaat naar de inrichtingsserver. Zowel een servercertificaat als een clientcertificaat wordt gebruikt om de telefoon aan de server en de server aan de telefoon te verifiëren.

Naast de door Cisco uitgegeven certificaten accepteert de telefoon ook servercertificaten van veelgebruikte SSL-certificaatproviders.

Als u HTTPS wilt gebruiken met de telefoon, moet u een Certificate Signing Request (CSR) genereren en dit indienen bij Cisco. De telefoon genereert een certificaat voor installatie op de inrichtingsserver. De telefoon accepteert het certificaat wanneer deze een HTTPS-verbinding wil maken met de inrichtingsserver.

HTTPS-methodologie

HTTPS codeert de communicatie tussen een client en een server, waarmee de berichtinhoud wordt beschermd tegen andere netwerkapparaten. De coderingsmethode voor de hoofdtekst van de communicatie tussen een client en een server is gebaseerd op cryptografie met symmetrische sleutels. Met cryptografie met symmetrische sleutels delen een client en een server een enkele geheime sleutel via een beveiligd kanaal dat wordt beschermd met openbare/privésleutelcodering.

Berichten die met de geheime sleutel zijn gecodeerd kunnen alleen worden gedecodeerd met behulp van dezelfde sleutel. HTTPS ondersteunt een breed scala aan symmetrische coderingsalgoritmen. De telefoon implementeert maximaal 256-bits symmetrische codering, met de Amerikaanse Encryption Standard (AES), naast 128-bits RC4.

HTTPS zorgt ook voor de verificatie van een server en een client in een beveiligde transactie. Deze functie zorgt ervoor dat een inrichtingsserver en een afzonderlijke client niet kunnen worden vervalst door andere apparaten op het netwerk. Deze functionaliteit is van essentieel belang in de context van externe eindpuntinrichting.

Server- en clientverificatie wordt uitgevoerd met openbare/privésleutelcodering met een certificaat dat de openbare sleutel bevat. Tekst die is gecodeerd met een openbare sleutel kan alleen worden gedecodeerd door de bijbehorende privésleutel (en vice versa). De telefoon ondersteunt het RSA-algoritme (Rivest-Shamir-Adleman) voor cryptografie met openbare/privésleutel.

SSL-servercertificaat

Elke veilige inrichtingsserver krijgt een SSL-servercertificaat (secure sockets layer) dat rechtstreeks door Cisco wordt ondertekend. De firmware die wordt uitgevoerd op de telefoon herkent alleen een Cisco-certificaat als geldig. Wanneer een client verbinding met een server maakt via HTTPS, weigert het alle servercertificaten die niet zijn ondertekend door Cisco.

Dit mechanisme beschermt de serviceprovider tegen ongeautoriseerde toegang tot de telefoon of valse pogingen om de inrichtingsserver te bereiken. Zonder deze bescherming kan een aanvaller de telefoon mogelijk opnieuw inrichten om configuratie-informatie te verkrijgen, of om een andere VoIP-service te gebruiken. Zonder de privésleutel die overeenkomt met een geldig servercertificaat, kan de aanvaller geen communicatie met een telefoon tot stand brengen.

Een servercertificaat verkrijgen

Procedure

Stap 1 Neem contact op met iemand van Cisco Support die u kan helpen bij het certificaatproces. Als u geen ondersteuning krijgt van een specifiek persoon, kunt u uw verzoek e-mailen naar ciscosb-certadmin@cisco.com.

Stap 2 Genereer een privésleutel die wordt gebruikt in een CSR (certificaatondertekeningsverzoek). Deze sleutel is privé. U hoeft deze sleutel niet aan Cisco Support door te geven. Gebruik open-source "openssl" om de sleutel te genereren. Bijvoorbeeld:

```
openssl genrsa -out <file.key> 1024
```

Stap 3 Genereer een CSR met velden die uw organisatie en locatie identificeren. Bijvoorbeeld:

```
openssl req -new -key <file.key> -out <file.csr>
```

U hebt de volgende informatie nodig:

- Onderwerpveld: voer de algemene naam (CN) in die een FQDN-syntax (Fully Qualified Domain Name) moet zijn. Tijdens de SSL-verificatiehandshake, verifieert de telefoon dat het certificaat dat wordt ontvangen van de computer afkomt dat het heeft gepresenteerd.
- Serverhostnaam: bijvoorbeeld provserv.domain.com.
- E-mailadres: voer een e-mailadres in zodat de klantondersteuning indien nodig contact met u kan opnemen. Dit e-mailadres is zichtbaar in het CSR.

Stap 4 E-mail de CSR (in zip-bestandsindeling) naar uw contactpersoon van Cisco Support of naar ciscosb-certadmin@cisco.com. Het certificaat wordt ondertekend door Cisco. Cisco verzendt het certificaat naar u zodat u dit kunt installeren op uw systeem.

Clientcertificaat

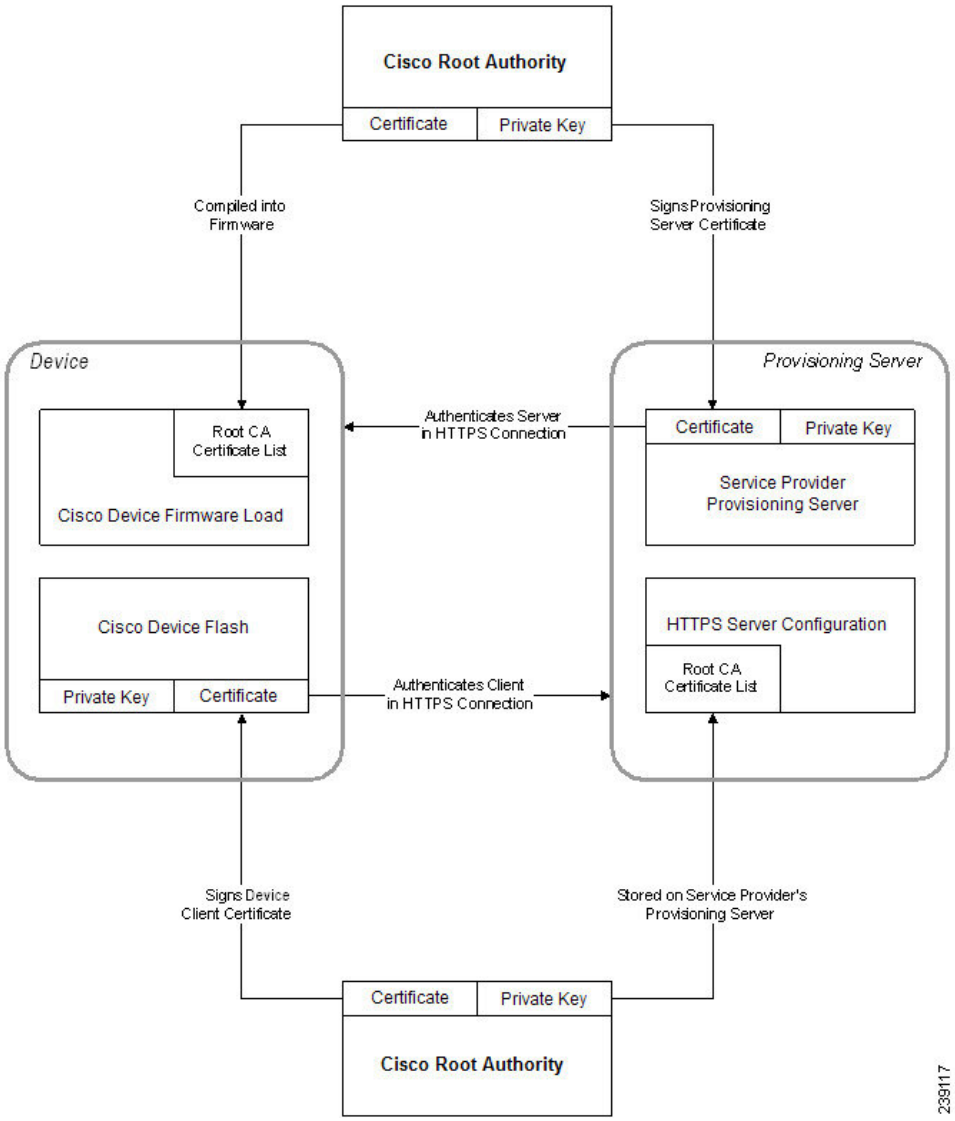
Naast een directe aanval op een telefoon, kan een aanvaller contact maken met een inrichtingsserver via een standaard webbrowser of een andere HTTPS-client om het configuratieprofiel van de inrichtingsserver te proberen te verkrijgen. Om dit soort aanvallen te voorkomen, heeft elke telefoon ook een uniek clientcertificaat dat is ondertekend door Cisco, met identificerende informatie over elk afzonderlijke eindpunt. Een Certificate Authority-basiscertificaat dat het clientcertificaat van het apparaat kan verifiëren wordt aan elke serviceprovider toegekend. Met dit verificatiepad kan de inrichtingsserver ongeautoriseerde verzoeken voor configuratieprofielen weigeren.

Certificaatstructuur

De combinatie van een servercertificaat en een clientcertificaat zorgt voor veilige communicatie tussen een externe telefoon en de inrichtingsserver. In de onderstaande afbeelding ziet u de relatie en de plaatsing van certificaten, paren van openbare/privé sleutels en ondertekenende basiscertificeringsinstanties, tussen de Cisco-client, de inrichtingsserver en de Certificate Authority.

De bovenste helft van het diagram toont de hoofdautoriteit van de inrichtingsserver die wordt gebruikt om het afzonderlijke inrichtingsservercertificaat te ondertekenen. Het overeenkomstige hoofdcertificaat is in de firmware gecompileerd, zodat de telefoon geautoriseerde inrichtingsservers kan verifiëren.

Figuur 1: Certificate Authority-stroom



Een aangepaste Certificate Authority configureren

Digitale certificaten kunnen worden gebruikt om netwerkapparaten en gebruikers op het netwerk te verifiëren. Ze kunnen worden gebruikt om IPSec-sessies te verwerken tussen netwerkknooppunten.

Een externe partij gebruikt een Certificate Authority-certificaat om twee of meer knooppunten die proberen te communiceren te valideren en te verifiëren. Elk knooppunt heeft een openbare en een privésleutel. De openbare sleutel codeert gegevens. De privésleutel decodeert gegevens. Omdat de knooppunten hun certificaten van dezelfde bron hebben verkregen, worden hun respectieve identiteiten zeker gesteld.

Het apparaat kan digitale certificaten die door een externe Certificate Authority (CA) worden aangeboden gebruiken om IPSec-verbindingen te verifiëren.

De telefoons ondersteunen een aantal vooraf geladen Root Certificate Authority die zijn ingesloten in de firmware:

- Cisco Small Business CA-certificaat
- CyberTrust CA-certificaat
- VeriSign CA-certificaat
- Sipura Root CA-certificaat
- Linksys Root CA-certificaat

Voordat u begint

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

Procedure

Stap 1 Selecteer **Info** > **Status**.

Stap 2 Blader naar **Aangepaste CA-status**. Hier ziet u de volgende velden:

- Aangepaste CA-inrichtingsstatus: geeft de inrichtingsstatus aan.
  - Laatste inrichting is gelukt op mm/dd/jjjj UU:MM:SS of
  - Laatste inrichting is mislukt op mm/dd/jjjj UU:MM:SS
- Aangepaste CA-informatie: geeft informatie over de aangepaste CA.
  - Geïnstalleerd: hiermee wordt de “CN-waarde” weergegeven en dit is de waarde van de CN-parameter voor het veld Onderwerp in het eerste certificaat.
  - Niet geïnstalleerd: hiermee wordt aangegeven of er geen aangepast CA-certificaat is geïnstalleerd.

Profielbeheer

In deze sectie wordt de formatie van configuratieprofielen ter voorbereiding op het downloaden gedemonstreerd. Om deze functionaliteit uit te leggen, wordt TFTP vanaf een lokale computer gebruikt als de hersynchronisatiemethode, hoewel HTTP of HTTPS ook kan worden gebruikt.

Een open profiel met Gzip comprimeren

Een configuratieprofiel in XML-indeling kan zeer groot worden als het profiel alle parameters afzonderlijk specificeert. Als u de belasting op de inrichtingsserver wilt verlagen, ondersteunt de telefoon het comprimeren van het XML-bestand, door de verkleinende compressie-indeling te gebruiken die GZIP (RFC 1951) ondersteunt.

Opmerking Compressie moet aan codering voorafgaan, anders herkent de telefoon een gecomprimeerd en versleuteld XML-profiel niet.

Voor de integratie met aangepaste back-end inrichtingsserveroplossingen, kan de open-source zlib-compressiebibliotheek worden gebruikt in plaats van het zelfstandige gzip-hulpprogramma voor het comprimeren van het profiel. De telefoon verwacht echter dat het bestand een geldige gzip-koptekst bevat.

Procedure

Stap 1 Installeer gzip op de lokale computer.

Stap 2 Comprimeer het configuratieprofiel `basic.txt` (beschreven in Hersynchroniseren via TFTP, op pagina 3) door gzip te activeren vanaf de opdrachtregel:

```
gzip basic.txt
```

Dit genereert het bestand `basic.txt.gz`.

Stap 3 Sla het bestand `basic.txt.gz` op in de virtuele hoofdmap van de TFTP-server.

Stap 4 Wijzig de Profile_Rule op het testapparaat om opnieuw te synchroniseren naar dit bestand in plaats van het oorspronkelijke XML-bestand, zoals weergegeven in het volgende voorbeeld:

```
tftp://192.168.1.200/basic.txt.gz
```

Stap 5 Klik op **Alle wijzigingen verzenden**.

Stap 6 Bekijk de syslog-tracering op de telefoon.

Bij hersynchronisatie downloadt de telefoon het nieuwe bestand en gebruikt het dit bestand om de parameters bij te werken.

Een profiel coderen met OpenSSL

Een gecomprimeerd of niet-gecomprimeerd profiel kan worden gecodeerd (een bestand moet echter worden gecomprimeerd voordat dit wordt gecodeerd). Codering is nuttig wanneer de vertrouwelijkheid van de profielinformatie in gevaar is, zoals wanneer TFTP of HTTP wordt gebruikt voor communicatie tussen de telefoon en de inrichtingsserver.

De telefoon ondersteunt codering met een symmetrische sleutel door gebruik van het 256-bits AES-algoritme. Deze codering kan worden uitgevoerd met behulp van het open-source OpenSSL-pakket.

Procedure

Stap 1 Installeer OpenSSL op een lokale computer. Hiervoor moet de OpenSSL-toepassing mogelijk opnieuw worden gecompileerd om AES in te schakelen.

Stap 2 Met het configuratiebestand `basic.txt` (zoals beschreven in Hersynchroniseren via TFTP, op pagina 3) kunt u een gecodeerd bestand met de volgende opdracht genereren:

```
>openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

Het gecomprimeerde `basic.txt.gz` -bestand dat is gemaakt in Een open profiel met Gzip comprimeren, op pagina 27 kan ook worden gebruikt, omdat het XML-profiel zowel gecomprimeerd als gecodeerd kan zijn.

Stap 3 Sla het gecodeerde bestand `basic.cfg` op in de virtuele hoofdmap van de TFTP-server.

Stap 4 Wijzig de Profile_Rule op het testapparaat om te hersynchroniseren naar het gecodeerde bestand in plaats van het oorspronkelijke XML-bestand. De coderingssleutel wordt met de volgende URL aan de telefoon bekendgemaakt:

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

Stap 5 Klik op **Submit All Changes**.

Stap 6 Bekijk de syslog-tracering op de telefoon.

Bij hersynchronisatie downloadt de telefoon het nieuwe bestand en gebruikt het dit bestand om de parameters bij te werken.

Gepartitioneerde profielen maken

Een telefoon downloadt meerdere afzonderlijke profielen tijdens elke keer hersynchroniseren. Hiermee kunnen verschillende soorten profielinformatie worden beheerd op afzonderlijke servers en kunnen algemene configuratieparameterwaarden die losstaan van accountspecifieke waarden worden onderhouden.

Procedure

Stap 1 Maak een nieuw XML-profiel, `basic2.txt`, dat een waarde aangeeft voor een parameter waardoor deze verschilt van de eerdere oefeningen. U kunt bijvoorbeeld het volgende toevoegen aan het `basic.txt`-profiel:

```
<GPP_B>ABCD</GPP_B>
```

Stap 2 Sla het `basic2.txt`-profiel op in de virtuele hoofdmap van de TFTP-server.

Stap 3 Laat de eerste profielregel van de eerdere oefeningen in de map staan, maar configureer de tweede profielregel (Profile_Rule_B) om te verwijzen naar het nieuwe bestand:

```
<Profile_Rule_B>tftp://192.168.1.200/basic2.txt
</Profile_Rule_B>
```

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

De telefoon hersynchroniseert nu met zowel het eerste als het tweede profiel, in die volgorde, wanneer er moet worden gehersynchroniseerd.

Stap 5 Observeer de syslogtracering om het verwachte gedrag te bevestigen.

Privacykoptekst telefoon instellen

Een koptekst voor gebruikersprivacy in het SIP-bericht stelt de wensen voor gebruikersprivacy in via het vertrouwde netwerk.

U kunt de koptekstwaarde voor gebruikersprivacy instellen voor elk toestelnummer met een XML-tag in het `config.xml`-bestand.

De opties voor de privacykoptekst zijn:

- Uitgeschakeld (standaard)
- Geen: de gebruiker eist dat een privacyservice geen privacyfuncties voor dit SIP-bericht toepast.
- Koptekst: de gebruiker gebruikt een privacyservice om kopteksten te verbergen waaruit de persoonsgegevens niet kunnen worden gewist.
- Sessie: de gebruiker eist dat een privacyservice anonimiteit biedt voor de sessies.
- Gebruiker: de gebruiker eist alleen een privacyniveau via tussenpersonen.
- Id: de gebruiker eist dat het systeem een vervangende id toepast die niet het IP-adres of de hostnaam weergeeft.

Procedure

Stap 1 Bewerk het bestand `config.xml` van de telefoon in een tekst- of XML-editor.

Stap 2 Voeg de **<Privacy_Header_N_ ua="na">*waardecode*</Privacy_Header_N_>** in, waarbij N het nummer van het toestelnummer (1–10) is en gebruik een van de volgende waarden.

- Standaardwaarde: **Uitgeschakeld**
- **geen**
- **kopregel**
- **sessie**
- **gebruiker**
- **id**

Stap 3 (Optioneel) Geef eventuele extra toestelnummers op met dezelfde tag voor het toestelnummer van de gewenste lijn.

Stap 4 Sla de wijzigingen in het `config.xml`-bestand op.

Het MIC-certificaat vernieuwen

U kunt het MIC-certificaat vernieuwen door een opgegeven of standaard SUDI-service (Secure Unique Device Identifier). Als het MIC-certificaat verloopt, werken de functies die SSL/TLS gebruiken niet.

Voordat u begint

- Zorg ervoor dat u de service `sudirenewal.cisco.com` (poort 80) via uw firewall toestaat om de vernieuwing van het MIC-certificaat te ondersteunen.
- Open de beheerwebpagina van de telefoon. Zie De webinterface van de telefoon openen.

Procedure

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

Stap 2 Stel onder de sectie **Instellingen MIC-certificaat** de parameters in zoals gedefinieerd in Parameters voor vernieuwen van het MIC-certificaat door de SUDI-service, op pagina 31.

Stap 3 Klik op **Submit All Changes**.
Nadat de certificaatvernieuwing is voltooid, wordt de telefoon opnieuw opgestart.

Stap 4 (Optioneel) Controleer de meest recente status van de vernieuwing van het MIC-certificaat onder de sectie **Vernieuwingsstatus MIC-certificaat** van **Info** > **Downloadstatus**.

Opmerking Als u de telefoon terugzet naar de fabrieksinstellingen, gebruikt de telefoon nog steeds het vernieuwde certificaat.

Parameters voor vernieuwen van het MIC-certificaat door de SUDI-service

In de volgende tabel worden de functie en het gebruik van elke parameter in de sectie **Instellingen MIC-certificaat** van het tabblad **Spraak** > **Inrichting** gedefinieerd.

Tabel 2: Parameters voor vernieuwen van het MIC-certificaat door de SUDI-service

Naam van parameter	Beschrijving en standaardwaarde
Vernieuwen van MIC-certificaat inschakelen	Hiermee bepaalt u of de MIC-vernieuwing (Manufacture Installed Certificate) door de standaard of de opgegeven SUDI-service (Secure Unique Device Identifier) moet worden ingeschakeld. Voer een van de volgende handelingen uit: • Voer in het XML-bestand met de telefoonconfiguratie (cfg.xml) een tekenreeks in deze notatie in: `<MIC_Cert_Refresh_Enable ua="na">Yes</MIC_Cert_Refresh_Enable>` • Selecteer **Ja** of **Nee** in de webinterface van de telefoon om de verlenging van het MIC-certificaat in of uit te schakelen. Geldige waarden: Ja en Nee Standaard: Nee

Regel voor vernieuwen van MIC-certificaat	Voer de HTTP-URL in van de SUDI-service die het vernieuwde MIC-certificaat biedt, bijvoorbeeld:
	`http://sudirenewal.cisco.com/`
	Opmerking Wijzig de URL niet. Alleen de standaard-URL wordt ondersteund voor de verlenging van het MIC-certificaat.
	Voer een van de volgende handelingen uit:
	• Voer in het XML-bestand met de telefoonconfiguratie (cfg.xml) een tekenreeks in deze notatie in:
	`<MIC_Cert_Refresh_Rule ua="na">http://sudirenewal.cisco.com/</MIC_Cert_Refresh_Rule>`
	• Voer in de webinterface van de telefoon de te gebruiken HTTP-URL in.
	Toegestane waarden: een geldige URL die niet langer is dan 1024 tekens
	Standaard: `http://sudirenewal.cisco.com/`

De upgraderegel instellen voor de Cisco-hoofdtelefoon

U kunt de firmware van een Cisco-headset upgraden door deze te verbinden met een Cisco IP-telefoon voor meerdere platforms. Voordat de gebruiker de upgrade uitvoert, moet u de upgraderegel instellen op de webpagina voor telefoonbeheer. Wanneer de headset is aangesloten op de telefoon, detecteert de telefoon automatisch de nieuwe versie van de headsetfirmware en wordt de gebruiker gevraagd de upgrade uit te voeren.

De ondersteunde verbindingen voor de upgrade zijn:

- Cisco-hoofdtelefoonserie 520: USB-kabel

- Cisco-hoofdtelefoonserie 560: USB-kabel en Y-kabel (RJ-9 en AUX-aansluiting)
- Cisco-hoofdtelefoonserie 700: USB-kabel

De instellingen voor de headset worden niet gewist als de telefoon opnieuw wordt ingesteld. De upgraderegel ondersteunt HTTP-, HTTPS- en TFTP-protocollen.

De versie van de Cisco-hoofdtelefoon biedt het headset-XML-bestand dat kan worden gebruikt voor de firmware-upgrade. Als de softwareversie in het bestand later zijn dan de firmware van de headset, wordt op het telefoonscherm gevraagd om de headset te upgraden. De gebruiker kan kiezen om meteen te upgraden, of dit uitstellen tot een later tijdstip.

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 de parameter **Upgraderegel voor de Cisco-hoofdtelefoon** in de sectie **Firmware-upgrade voor de Cisco-hoofdtelefoon**.

Stap 3 Geef het TFTP-, HTTP- of HTTPS-protocol op, een IP-adres van de te upgraden hoofdtelefoon en de naam van het XML-bestand van de hoofdtelefoon. Voer de waarden in als een enkele tekenreeks in de parameter.

Voorzichtig WIjzig niet de inhoud van het XML-bestand van de headset.

Bijvoorbeeld `tftp://10.74.51.81/Prov/headset/1-6-0-162/ciscoheadsetfirmware.XML`

U kunt deze parameter ook configureren in het configuratiebestand (cfg.xml).

```
<Cisco_Headset_Upgrade_Rule
ua="na">tftp://10.74.51.81/prov/headset/1-6-0-162/ciscoheadsetfirmware.xml</Cisco_Headset_Upgrade_Rule>
```

Stap 4 Klik op **Submit All Changes**.
Als een nieuwe versie van de headsetfirmware wordt herkend, geeft de telefoon een upgrade-prompt.