Inrichting

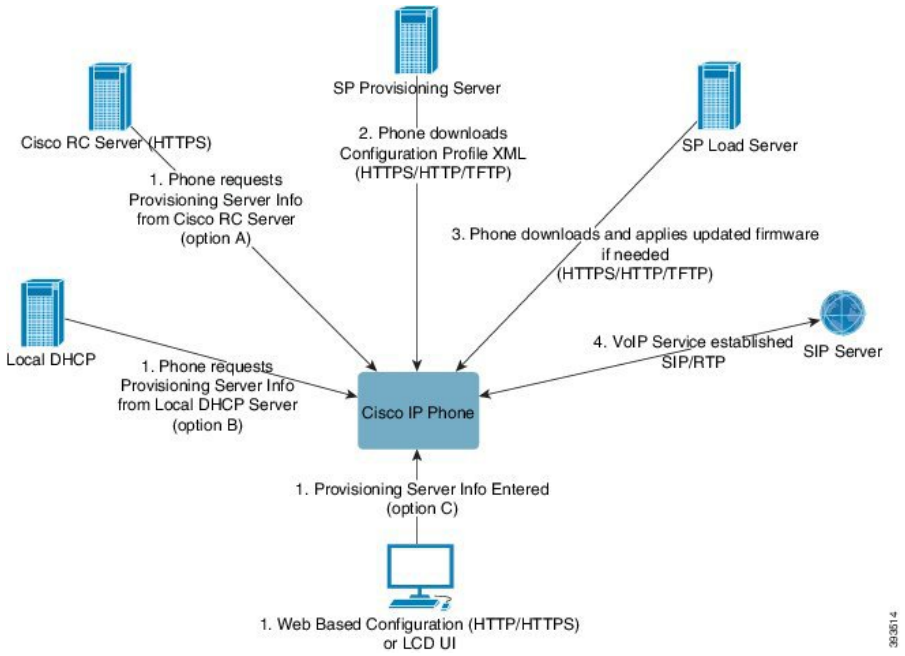
Overzicht inrichting

Cisco IP-telefoons zijn bedoeld voor implementaties met grote volumes door VoIP-serviceproviders (Voice-over-IP) aan klanten thuis, aan bedrijven of aan grote ondernemingen. Daarom verzekert inrichting van de telefoon met behulp van extern beheer en configuratie de correcte werking van de telefoon op de locatie van de klant.

Cisco ondersteunt de aangepaste, voortdurende functieconfiguratie van de telefoon met behulp van:

- Betrouwbaar extern beheer van de telefoon.
- Codering van de communicatie waarmee de telefoon wordt bestuurd.
- Gestroomlijnde binding van het telefoonaccount.

Telefoons kunnen worden ingericht om configuratieprofielen of bijgewerkte firmware van een externe server te downloaden. Downloads kunnen plaatsvinden wanneer de telefoons zijn aangesloten op een netwerk, wanneer ze worden opgestart en op vaste intervallen. Inrichting is over het algemeen onderdeel van VoIP-implementaties met grote volumes die veel door serviceproviders worden aangeboden. Configuratieprofielen of bijgewerkte firmware worden overgebracht naar het apparaat door middel van TFTP, HTTP of HTTPS.



Op een hoog niveau is het inrichtingsproces voor de telefoon als volgt:

1. Als de telefoon niet is geconfigureerd, wordt de informatie van de inrichtingsserver toegepast op de telefoon met behulp van een van de volgende opties:
   - **A**: gedownload van de Cisco Enablement Data Orchestration System (EDOS) Remote Customization (RC) server via HTTPS, DNS SRV, GDS (onboarding via activeringscode), EDOS apparaatactivering.
   - **B**: aangevraagd van een lokale DHCP-server.
   - **C**: handmatig ingevoerd met behulp van het hulpprogramma voor webgebaseerde configuratie van de Cisco-telefoon of de gebruikersinterface van de telefoon.
2. De telefoon downloadt de informatie van de inrichtingsserver en past de configuratie-XML toe met behulp van het HTTPS-, HTTP- of TFTP-protocol.
3. De telefoon downloadt (indien nodig) de bijgewerkte firmware en past deze toe, met behulp van HTTPS, HTTP of TFTP.
4. De VoIP-service wordt tot stand gebracht met de gespecificeerde configuratie en firmware.

VoIP-serviceproviders willen veel telefoons implementeren naar particuliere klanten en kleine bedrijven. In bedrijven en grote ondernemingen kunnen telefoons dienst doen als terminalknooppunten. Providers distribueren deze apparaten breed over het internet en deze zijn verbonden via routers en firewalls op het kantoor van de klant.

De telefoon kan worden gebruikt als een externe uitbreiding van de back-end-apparatuur van de serviceprovider. Extern beheer en configuratie verzekeren de correcte werking van de telefoon op het kantoor van de klant.

Inrichting

Een telefoon kan worden geconfigureerd om periodiek en bij opstarten de interne configuratiestatus te hersynchroniseren om overeen te komen met een extern profiel. De telefoon maakt verbinding met een normale inrichtingsserver (NPS) of een toegangsbeheerserver (ACS).

Standaard wordt een profiel alleen gehersynchroniseerd als de telefoon inactief is. Dit voorkomt dat de software door de upgrade opnieuw wordt opgestart en een gesprek wordt afgebroken. Als tussentijdse upgrades zijn vereist om een actuele upgradestatus vanuit een oudere versie te bereiken, kan de upgradelogica getrapte upgrades automatiseren.

Normale inrichtingsserver

De normale inrichtingsserver (NPS) kan een TFTP-, HTTP- of HTTPS-server zijn. Een externe firmware-upgrade wordt bereikt via TFTP, HTTP of HTTPS, omdat de firmware geen gevoelige informatie bevat.

Hoewel HTTPS wordt aanbevolen, hoeft er bij communicatie met de NPS geen beveiligd protocol te worden gebruikt omdat het bijgewerkte profiel kan worden gecodeerd met een gedeelde geheime sleutel. Zie voor meer informatie over het gebruik van HTTPS Communicatiecodering, op pagina 11. Beveiligde eerste inrichting wordt aangeboden via een mechanisme dat SSL-functionaliteit gebruikt. Een telefoon zonder inrichting kan een profiel dat is gecodeerd met een 256-bits symmetrische sleutel ontvangen dat aan dat apparaat is gericht.

Werkwijzen telefooninrichting

Normaal gesproken is de Cisco IP-telefoon geconfigureerd voor inrichting wanneer het voor het eerst verbinding met het netwerk maakt. De telefoon ook is ingericht op de geplande intervallen die zijn ingesteld wanneer de serviceprovider of de VAR de telefoon voorinricht (configureert). Serviceproviders kunnen VAR's of geavanceerde gebruikers autoriseren om de telefoon handmatig in te richten met behulp van het toetsenblok van de telefoon. U kunt ook de inrichting configureren via de webgebruikersinterface van de telefoon.

Controleer de **Status** > **Telefoonstatus** > **Inrichting** vanuit de LCD-gebruikersinterface van de telefoon, of de inrichtingsstatus in het tabblad **Status** van het webgebaseerde configuratiehulpprogramma.

Uw telefoon in gebruik nemen met de activeringscode

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. U geeft de telefoon de opdracht een upgrade uit te voeren naar de nieuwe firmware en de profielregel `gds://` te gebruiken om het scherm met de activeringscode te openen. Een gebruiker voert in het weergegeven veld een code van 16 cijfers in om de telefoon automatisch in gebruik te nemen.

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.

Procedure

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

Stap 2 Voer het onderstaande voorbeeld in het bestand config.xml in om de profielregel voor onboarding via activeringscode in te stellen.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

Opmerking Voor de firmwareversie na de 11.2 (3) SR1 is de instelling van `Firmware-upgrade` optioneel.

Stap 3 Sla de wijzigingen in het config.xml-bestand op.

Telefoon verbinden met Webex Cloud

Telefoonverbinding biedt een eenvoudige en veilige manier om Webex-telefoons te verbinden met de Webex-cloud. U kunt het verbindingsproces uitvoeren met activeringscode (GDS) of met telefoon MAC-adres (EDOS-apparaat activeren).

Zie *Cisco BroadWorks-partner configuratiehandleiding, Cisco multi-platform telefoons* voor meer informatie over het genereren van de activeringscode.

Zie *Webex voor Cisco BroadWorks oplossingshandleiding* voor meer informatie over het verbinden van de telefoon met Webex.

Een telefoon activeren voor verbinding met Webex Cloud

Na de geslaagde registratie van de telefoon bij Webex Cloud, wordt een wolksymbool weergegeven op het telefoonscherm.

Voordat u begint

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

Procedure

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

Stap 2 Stel in de sectie **Webex** de parameter **Onboard activeren** in op **Ja**.

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

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

Standaardwaarde: Ja

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

Automatische inrichting met een korte activeringscode inschakelen

Voer de volgende stappen uit om automatische inrichting met een korte activeringscode in te schakelen.

Voordat u begint

Zorg ervoor dat uw telefoons zijn bijgewerkt met firmwareversie 11.3(1) of hoger.

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

Bekijk hoe u de CDA-server voor het omleidingsprofiel instelt:

https://community.cisco.com/t5/collaboration-voice-and-video/cisco-multi-platform-phones-cloud-provisioning-process/ta-p/3910244

Procedure

Stap 1 Maak een omleidingsprofielnaam met een willekeurig aantal cijfers van drie tot en met 16. Dit wordt later de activeringscode. Gebruik een van deze notaties:

- **nnn**.
- **nnnnnnnnnnnnnnnn**
- Een willekeurig aantal cijfers van drie tot en met zestien. Voorbeeld: **123456**

Stap 2 Geef de profielnaam die u in stap 1 hebt gemaakt, door aan het CDA-ondersteuningsteam (activering van klantapparaat) op cdap-support@cisco.com.

Stap 3 Vraag het CDA-ondersteuningsteam om uw profiel in te schakelen voor ontdekking.

Stap 4 Wanneer u een bevestiging krijgt van het CDA-ondersteuningsteam, distribueert u de activeringscode naar de gebruikers.

Stap 5 Geef aan of gebruikers op een hekje (#) moeten drukken voordat ze de cijfers in het activeringsscherm invoeren.

Handmatige inrichting van een telefoon vanuit het toetsenblok

Procedure

Stap 1 Druk op **Toepassingen** .

Stap 2 Selecteer **Apparaatbeheer** > **Profielregel**.

Stap 3 Voer de profielregel in met de volgende indeling:

```
protocol://server[:poort]/profile_pathname
```

Bijvoorbeeld:

```
tftp://192.168.1.5/CP_x8xx_MPP.cfg
```

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).

Stap 4 Druk op **Opnieuw synchroniseren**.

DNS SRV voor HTTP-inrichting

De DNS SRV voor HTTP-inrichtingsfunctie zorgt voor automatische inrichting van uw telefoon voor meerdere platforms. Met DNS SRV-records (Domain Name System Service) worden verbindingen tussen een service en een hostnaam tot stand gebracht. Wanneer de telefoon naar de locatie van de inrichtingsservice zoekt, wordt eerst een query uitgevoerd op de opgegeven DNS SRV-domeinnaam en vervolgens op SRV-records. De telefoon valideert de records om na te gaan of de server toegankelijk is. Vervolgens wordt de daadwerkelijke inrichtingsflow voortgezet. Serviceproviders kunnen deze DNS SRV-inrichtingsflow gebruiken om automatische inrichting te bieden.

DNS SRV baseert de hostnaamvalidatie op het certificaat van de door DHCP verstrekte domeinnaam. Het is belangrijk dat alle SRV-records een geldig certificaat gebruiken dat de door DHCP verstrekte domeinnaam bevat.

De DNS SRV-query bevat de DHCP-domeinnaam als volgt: **_<servicename>._<transport>.<domainName>**.

Bijvoorbeeld: **_ciscoprov-https._tls.voorbeeld.com** geeft de telefoon de instructie om naar voorbeeld.com te zoeken. De telefoon gebruikt de hostnaam en het poortnummer die zijn opgehaald door de DNS SRV-query om de URL samen te stellen die wordt gebruikt om de aanvankelijke configuratie te downloaden.

DNS SRV is een van de vele mechanismen voor automatische die door de telefoon worden gebruikt. De telefoon probeert deze volgorde voor de mechanismen aan te houden:

1. DHCP
2. DNS SRV
3. EDOS
4. GDS (onboarding via activeringscode) of EDOS-apparaatactivering

De volgende tabel bevat een beschrijving van de SRV-recordvelden.

Tabel 1: SRV-recordvelden

Veld	Beschrijving	Voorbeeld
<_servicename.>	De naam van de service begint met een onderstrepingsteken. Serverservices maken gebruik van symbolische namen in SRV-records. Een punt (.) achter de service geeft aan dat de service tot stand is gebracht en de volgende sectie begint.	**`_ciscoprov-https.`** Of **`_ciscoprov-http.`** DNS SRV ondersteunt het TFTP-protocol niet. Als u TFTP gebruikt, wordt het volgende foutbericht weergegeven: `Fout - TFTP-schema wordt niet ondersteund in SRV-zoekopdrachten.`
<_proto.>	Het transportprotocol begint met een onderstrepingsteken. De punt achter het protocol geeft aan dat de protocolsectie is beëindigd.	**`_tls.`** U moet HTTPS gebruiken met TLS. Of **`_tcp.`** U moet HTTP gebruiken met TCP.
<domainName>	De naam van het servicedomein volgt het protocol. Hostnaamvalidatie: alle SRV-records worden gevalideerd op basis van de oorspronkelijke door DHCP verstrekte domeinnaam. Het is belangrijk dat alle records een geldig certificaat met de oorspronkelijke domeinnaam gebruiken.	**`voorbeeld.com`**
TTL (Time to Live)	De vervalwaarde van de record in seconden.	86400
Klasse	Internettype: standaard BIND-notatie geeft aan dat het een SRV-record is.	IN
<priority>	Elke lijn bevat een prioriteitsnummer. Hoe lager het nummer, des te eerder de telefoon de hostnaam en poort van het doel in deze DNS SRV-record probeert.	**`10`**
<weight>	Als twee of meer services dezelfde prioriteit hebben, bepaalt het gewichtsgetal welke lijn voorrang krijgt. Hoe lager het nummer, des te eerder de telefoon de hostnaam en poort van het doel in deze DNS SRV-record probeert.	**`20`**
<port>	optioneel poortnummer	**`5060`**
<target>	De A-record van de computer die de service levert. A-records zijn het meest algemene type DNS-record en worden gebruikt om een domein of subdomein naar een IP-adres te verwijzen.	**`pr1.voorbeeld.com`**

Voorbeelden van SRV-configuraties

_service._proto.naam. Doel van de SRV-poort voor prioriteitsgewicht voor TTL.

_ciscoprov-https._tls.voorbeeld.com. 86400 IN SRV 10 60 5060 pr1.voorbeeld.com.

_ciscoprov-https._tls.voorbeeld.com. 86400 IN SRV 10 20 5060 pr2.voorbeeld.com.

_ciscoprov-http._tcp.voorbeeld.com. 86400 IN SRV 10 50 5060 px1.voorbeeld.com.

_ciscoprov-http._tcp.voorbeeld.com. 86400 IN SRV 10 30 5060 px2.voorbeeld.com.

DNS SRV gebruiken voor HTTP-inrichting

Nieuwe telefoons maken gebruik van DNS SRV als methode voor automatische inrichting. Voor bestaande telefoons kunt u deze functie gebruiken om uw telefoon te hersynchroniseren als uw netwerk is ingesteld voor inrichting met DNS SRV voor HTTP. Voorbeeldconfiguratiebestand:

```
<flat-profile>
<!-- System Configuration -->
<Primary_DNS ua="rw">10.89.68.150</Primary_DNS>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Profile_Authentication_Type ua="na">Basic Http Authentication </Profile_Authentication_Type>
<Proxy_1_ ua="na">example.com</Proxy_1_>
<Display_Name_1_ ua="na">4081001141</Display_Name_1_>
<User_ID_1_ ua="na">4081001141</User_ID_1_>
</flat-profile>
```

Voordat u begint

Als u voor de HTTP-inrichting een proxyserver wilt instellen, moet u controleren of de proxyserver correct is geconfigureerd. Zie Een proxyserver instellen.

Procedure

Voer een van de volgende acties uit. Daarna De profielregel instellen met de optie SRV op de webpagina, op pagina 8 of De profielregel instellen met de optie SRV op de telefoon, op pagina 9

- Plaats het XML-configuratiebestand $PSN.xml in de hoofdmap van de `webserver`.
- Plaats het XML-configuratiebestand $MA.cfg in de `hoofdmap/Cisco/` van de webserver.

De profielregel instellen met de optie SRV op de webpagina

U kunt de optie SRV gebruiken om een configuratiebestand naar uw telefoon te downloaden.

Voordat u begint

De webinterface van de telefoon openen

Procedure

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

Stap 2 Voer in het veld **Profile Rule** (Profielregel) de profielregel in met de optie SRV. Alleen HTTP en HTTPS worden ondersteund.

Voorbeeld:

```
[--srv] https://example.com/$PSN.xml
```

De profielregel instellen met de optie SRV op de telefoon

U kunt de optie SRV op uw telefoon gebruiken om een configuratiebestand te downloaden.

Procedure

Stap 1 Druk op **Toepassingen** .

Stap 2 Selecteer **Apparaatbeheer** > **Profielregel**.

Stap 3 Voer de profielregel in met de parameter **`[--srv]`**. Alleen HTTP en HTTPS worden ondersteund.

Voorbeeld:

```
[--srv] https://example.com/$PSN.xml
```

Stap 4 Druk op **Opnieuw synchroniseren**.

TR69-inrichting

De Cisco IP-telefoon helpt de beheerder bij de configuratie van de TR69-parameters met behulp van de webgebruikersinterface. Voor informatie over de parameters, met inbegrip van een vergelijking van de XML- en TR69-parameters, raadpleegt u de beheerdershandleiding voor de bijbehorende telefoonserie.

De telefoons ondersteunen ACS-ontdekking (Auto Configuration Server) vanuit DHCP-optie 43, 60 en 125.

- Optie 43: leverancier-specifieke informatie voor de ACS-URL.
- Optie 60: leverancierklasse-id, zodat de telefoon zichzelf identificeert met `dslforum.org` naar de ACS.
- Optie 125: leverancier-specifieke informatie voor de gateway-koppeling.

TR69 RPC Methods

Ondersteunde RPC-methoden

De telefoons ondersteunen slechts een beperkt aantal RPC-methoden (Remote Procedure Call), zoals hieronder aangegeven:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: de Download RPC-methode, de ondersteunde bestandstypen zijn:
  - Image van de firmware-upgrade
  - Leverancierconfiguratiebestand
  - Aangepast Certificate Authority (CA)-bestand
- Overdracht voltooid

Ondersteunde gebeurtenistypen

De telefoons ondersteunen gebeurtenistypen op basis van de functies en methoden die worden ondersteund. Alleen de volgende gebeurtenistypen worden ondersteund:

- Bootstrap
- Boot
- waardewijziging
- verbindingsverzoek
- Periodiek
- Overdracht voltooid
- M-download
- M-reboot

Communicatiecodering

De configuratieparameters die aan het apparaat worden gecommuniceerd, kunnen autorisatiecodes of andere informatie bevatten waarmee het systeem tegen ongeautoriseerde toegang wordt beschermd. Het is in het belang van de serviceprovider om ongeautoriseerde klantactiviteit te voorkomen. Het is in het belang van de klant om ongeautoriseerd gebruik van het account te voorkomen. De serviceprovider kan de communicatie van het configuratieprofiel tussen de inrichtingsserver en het apparaat coderen, naast het beperken van de toegang tot de beheerwebserver.

Telefoongedrag tijdens netwerkcongestie

Alle factoren die de netwerkprestaties verslechteren, kunnen invloed hebben op de audio- en videokwaliteit van de telefoon. In sommige gevallen kan een gesprek zelfs wegvallen. Bronnen van netwerkverslechtering zijn onder andere de volgende activiteiten:

Alle factoren die de netwerkprestaties verslechteren, kunnen invloed hebben op de audiokwaliteit van de telefoon. In sommige gevallen kan een gesprek zelfs wegvallen. Bronnen van netwerkverslechtering zijn onder andere de volgende activiteiten:

- Beheertaken, zoals een interne poortscan of een beveiligingsscan.
- Aanvallen die zich voordoen op uw netwerk, zoals een Denial of Service-aanval.

Voorinrichting op kantoor locatie en inrichtingsservers

De serviceprovider richt telefoons vooraf in, anders dan RC-toestellen, met een profiel. Het vooringerichte profiel kan bestaan uit een beperkte set parameters waarmee de telefoon wordt gehersynchroniseerd. Het profiel kan ook bestaan uit een volledige set parameters die de externe server levert. De telefoon hersynchroniseert standaard bij opstarten en op intervallen die zijn geconfigureerd in het profiel. Wanneer de gebruiker de telefoon verbindt op het kantoor van de klant, downloadt het apparaat het bijgewerkte profiel en eventuele firmware-updates.

Dit proces van voorinrichting, implementatie en externe inrichting kan worden uitgevoerd op vele manieren.

Servervoorbereiding en hulpprogramma's

Voor de voorbeelden in dit hoofdstuk moeten een of meer servers beschikbaar zijn. Deze servers kunnen worden geïnstalleerd en uitgevoerd op een lokale computer:

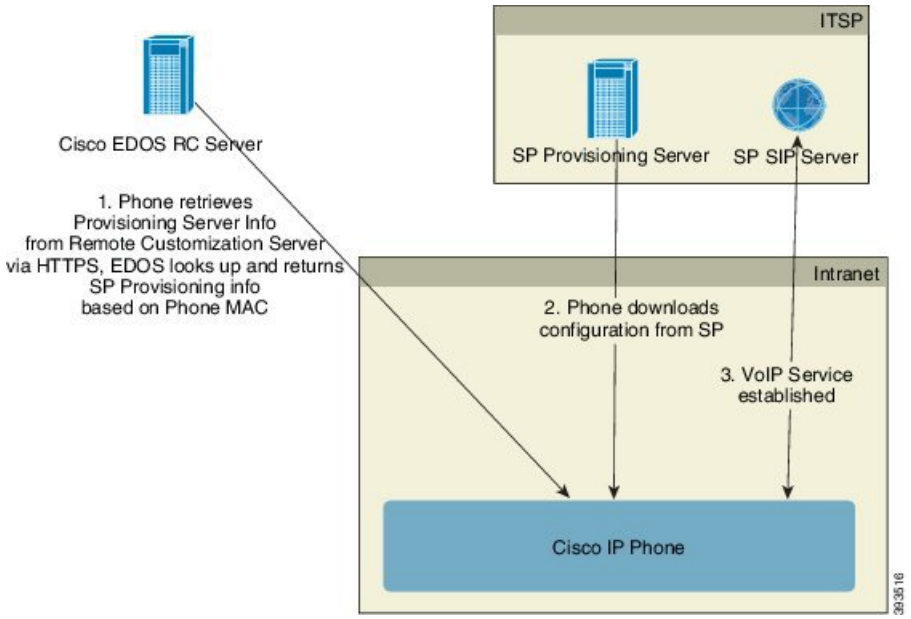
- TFTP (UDP-poort 69)
- syslog (UDP-poort 514)
- HTTP (TCP-poort 80)
- HTTPS (TCP-poort 443).

Als u problemen met de serverconfiguratie wilt oplossen, is het handig om clients voor elk type server te installeren op een afzonderlijke servercomputer. Daarmee maakt u een juiste serverwerking mogelijk, onafhankelijk van de interactie met de telefoons.

We raden u ook aan dat u deze hulpprogramma's installeert:

- Als u configuratieprofielen wilt genereren, kunt u het open-source gzip-compressiehulpprogramma installeren.
- Voor profielcodering en HTTPS-bewerkingen, installeert u het open-source OpenSSL-softwarepakket.
- Als u dynamische profielgeneratie en externe inrichting in één stap via HTTPS wilt testen, raden wij een scripttaal met CGI-scriptondersteuning aan. Open-source Perl-taalhulpprogramma's is een voorbeeld van een dergelijke scripttaal.
- Als u een veilige uitwisseling tussen inrichtingsservers en de telefoons wilt verifiëren, installeert u een Ethernet-pakketsniffer (zoals de vrij downloadbare Ethereal/Wireshark). Leg een Ethernet-pakkettracering van de interactie tussen de telefoon en de inrichtingsserver vast. Als u dit wilt doen, voert u de pakketsniffer uit op een computer die is verbonden met een schakelaar waarop poortspiegeling is ingeschakeld. Voor HTTPS-transacties kunt u het hulpprogramma ssldump gebruiken.

RC-distributie (externe aanpassing)



Alle telefoons nemen contact op met de Cisco EDOS RC-server totdat ze voor het eerst worden ingericht.

Bij een RC-distributiemodel koopt een klant een telefoon die al is gekoppeld aan een specifieke serviceprovider op de Cisco EDOS RC-server. De internettelefonie-serviceprovider (ITSP) installeert een inrichtingsserver en onderhoudt deze, en registreert de informatie van deze inrichtingsserver bij de Cisco EDOS RC-server.

Wanneer de telefoon met een internetverbinding wordt ingeschakeld, is de aanpassingsstatus van de niet-ingerichte telefoon **Open**. De telefoon vraagt eerst bij de lokale DHCP-server voor de informatie van de inrichtingsserver en stelt de aanpassingsstatus van de telefoon in. Als de DHCP-aanvraag is geslaagd, is de

aanpassingsstatus ingesteld op **Afgebroken** en wordt RC niet geprobeerd omdat DHCP de vereiste informatie van de inrichtingsserver aanbiedt.

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. Cisco raadt aan om beide domeinnamen toe te staan via uw firewall.

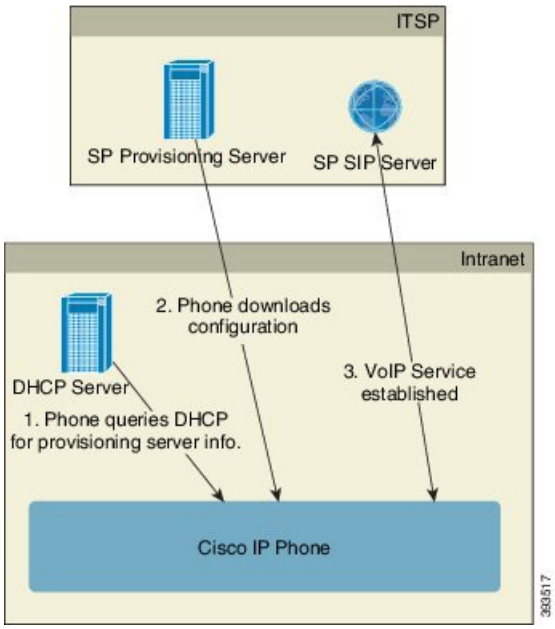
Als de DHCP-server geen informatie van de inrichtingsserver aanbiedt, vraagt de telefoon dit aan bij de Cisco EDOS RC-server en biedt deze het MAC-adres en het model aan. De aanpassingstatus wordt ingesteld op **In behandeling**. De Cisco EDOS-server reageert met de gekoppelde informatie van de inrichtingsserver van de serviceprovider, met inbegrip van de inrichtingsserver-URL. De aanpassingsstatus van de telefoon wordt ingesteld op **Aangepast in behandeling**. De telefoon voert vervolgens een URL-opdracht uit voor hersynchronisatie om de configuratie van de serviceprovider op te halen. Indien dit lukt, wordt de aanpassingsstatus ingesteld op **Verworven**.

Als de Cisco EDOS RC-server geen gekoppelde serviceprovider heeft voor de telefoon, wordt de aanpassingsstatus van de telefoon ingesteld op **Niet beschikbaar**. De telefoon kan handmatig worden geconfigureerd of er kan een koppeling voor de serviceprovider van de telefoon aan de Cisco EDOS-server worden toegevoegd.

Als een telefoon wordt ingericht via LCD of het webconfiguratiehulpprogramma, voorafgaand aan dat de aanpassingsstatus **Verworven** wordt, wordt de aanpassingsstatus ingesteld op **Afgebroken** en wordt er geen aanvraag naar de Cisco EDOS-server gestuurd, tenzij de fabrieksinstellingen van de telefoon worden hersteld.

Zodra de telefoon is ingericht, kan de Cisco EDOS RC-server niet worden gebruikt tenzij de fabrieksinstellingen van de telefoon worden hersteld.

Voorinrichting van apparaten op locatie



Met standaard fabriekskonfiguratie van Cisco probeert de telefoon automatisch te hersynchroniseren naar een profiel op een TFTP-server. Een beheerde DHCP-server op een LAN-netwerk levert de informatie over het profiel en de TFTP-server die is geconfigureerd voor voorinrichting aan het apparaat. De serviceprovider verbindt elke nieuwe telefoon met het LAN-netwerk. De telefoon synchroniseert automatisch opnieuw naar de lokale TFTP-server en initialiseert de interne status ter voorbereiding op implementatie. Dit profiel voor voorinrichting bevat doorgaans de URL van een externe inrichtingsserver. De inrichtingsserver houdt het apparaat bijgewerkt nadat het apparaat is geïmplementeerd en verbonden met het klantnetwerk.

De vooraf ingerichte streepjescode van het apparaat kan worden gescand om het MAC-adres of het serienummer vast te leggen voordat de telefoon naar de klant wordt verzonden. Deze informatie kan worden gebruikt om het profiel te maken waarnaar de telefoon hersynchroniseert.

Bij ontvangst van de telefoon, verbindt de klant deze met de breedbandkoppeling. Bij het opstarten maakt de telefoon contact met de inrichtingsserver via de URL die bij voorinrichting is geconfigureerd. De telefoon kan op deze wijze hersynchroniseren en het profiel en de firmware indien nodig bijwerken.

Instellen van de inrichtingsserver

In deze sectie worden de installatievereisten beschreven voor de inrichting van een telefoon met behulp van verschillende servers en in verschillende scenario's. Ten behoeve van dit document en om te testen, worden de inrichtingsservers geïnstalleerd en uitgevoerd op een lokale computer. Bovendien zijn algemeen beschikbare softwarehulpprogramma's nuttig voor de inrichting van de telefoons.

TFTP-inrichting

De telefoons ondersteunen TFTP voor inrichting van zowel hersynchronisatie als firmware-upgrades. Wanneer apparaten extern worden geïmplementeerd, wordt HTTPS aanbevolen, maar HTTP en TFTP kunnen ook worden gebruikt. Hiervoor is vervolgens nodig dat bestandscodering tijdens de inrichting beveiliging toevoegt, omdat dit grotere betrouwbaarheid biedt, gezien de NAT en routerbeveiligingsmechanismen. TFTP is nuttig voor voorinrichting op locatie van een groot aantal niet-ingerichte apparaten.

Via DHCP-optie 66 kan de telefoon een TFTP-server IP-adres rechtstreeks ophalen via de DHCP-server. Als een Profile_Rule is geconfigureerd met het bestandspad van die TFTP-server, wordt het profiel van de TFTP-server gedownload door het apparaat. Het downloaden vindt plaats wanneer het apparaat is verbonden met een LAN en wanneer het is opgestart.

De Profile_Rule die wordt aangeboden bij de standaardfabriekskonfiguratie is *&PN*.cfg, waarbij *&PN* staat voor de telefoonmodelnaam.

Voor een CP-7841-3PCC is de bestandsnaam bijvoorbeeld CP-7841-3PCC.cfg. Voor een CP-7832-3PCC is de bestandsnaam CP-7832-3PCC.cfg.

Voor een apparaat met het standaardfabrieksprofiel hersynchroniseert het apparaat bij het opstarten naar dit bestand op de lokale TFTP-server die wordt gespecificeerd door DHCP-optie 66. Het bestandspad is relatief aan de virtuele hoofdmap van de TFTP-server.

Extern eindpuntbeheer en NAT

De telefoon is compatibel met netwerkadresomzetting (NAT) om het internet via een router te gebruiken. Voor betere beveiliging kan de router proberen ongeautoriseerde binnenkomende pakketten te blokkeren door symmetrisch NAT te implementeren, een strategie voor het filteren van pakketten waarmee de pakketten die

zijn toegestaan om via het internet het beveiligde netwerk binnen te komen ernstig worden beperkt. Daarom wordt externe inrichting via TFTP niet aanbevolen.

VoIP kan alleen samen met NAT worden gebruikt als er een vorm van NAT-traversal aanwezig is. Simple Traversal van UDP via NAT (STUN) configureren. Voor deze optie moet de gebruiker beschikken over:

- Een dynamisch extern (openbaar) IP-adres van uw service
- Een computer die over STUN-serversoftware beschikt
- Een randapparaat met een mechanisme voor asymmetrische NAT

HTTP-inrichting

De telefoon gedraagt zich als een browser die webpagina's aanvraagt van een externe internetsite. Dit biedt een betrouwbare methode om de inrichtingsserver te bereiken, zelfs wanneer de router van een klant symmetrisch NAT of andere beveiligingsmechanismes implementeert. HTTP en HTTPS werken betrouwbaarder dan TFTP bij externe implementaties, met name wanneer de geïmplementeerde toestellen zijn verbonden achter particuliere firewalls of routers met NAT-ondersteuning. HTTP en HTTPs worden afwisselend gebruikt in de volgende beschrijvingen van verzoektypes.

Standaard HTTP-gebaseerde inrichting is afhankelijk van de HTTP GET-methode voor het ophalen van configuratieprofielen. Over het algemeen wordt er een configuratiebestand gemaakt voor elke geïmplementeerde telefoon en worden deze bestanden opgeslagen in een HTTP-servermap. Wanneer de server het GET-verzoek ontvangt, stuurt het eenvoudig het bestand terug dat is gespecificeerd in de koptekst van het GET-verzoek.

In plaats een statisch profiel, kan het configuratieprofiel dynamisch worden gegenereerd door een klantendatabase te verzoeken en het profiel op het moment zelf te produceren.

Wanneer de telefoon een hersynchronisatie aanvraagt, kan het hiervoor de HTTP POST-gebruiken om de configuratiegegevens voor hersynchronisatie aan te vragen. Het apparaat kan worden geconfigureerd om bepaalde status- en de identificatie-informatie aan de server over te brengen in de hoofdtekst van het HTTP POST-verzoek. De server gebruikt deze informatie om een gewenst configuratieprofiel te genereren, of om de statusinformatie op te slaan voor latere analyse en tracering.

Als onderdeel van zowel GET- als POST-verzoeken bevat de telefoon identificerende basisinformatie in het veld User-Agent (gebruiker-agent) van de koptekst van het verzoek. Deze informatie geeft de fabrikant, de productnaam, de huidige firmwareversie en het productserienummer van het apparaat.

Gebruikersagent is configureerbaar en de telefoon gebruikt deze waarde als deze niet is geconfigureerd (nog steeds op standaard).

Wanneer de telefoon is geconfigureerd om te hersynchroniseren met een configuratieprofiel via HTTP, wordt het aangeraden om HTTPS te gebruiken of om het profiel te coderen om vertrouwelijke informatie te beschermen. Gecodeerde profielen die de telefoon downloadt via HTTP lopen geen gevaar dat vertrouwelijke informatie die is opgenomen in het configuratieprofiel wordt vrijgegeven. Deze hersynchronisatiemodus produceert een lagere rekenkundige belasting van de inrichtingsserver in vergelijking met HTTPS.

De telefoon kan gecodeerde bestanden met een van de volgende coderingsmethoden decoderen:

- AES-256-CBC-codering
- Codering op basis van RFC-8188 met AES-128-GCM ciphering

Opmerking De telefoons ondersteunen HTTP-versie 1.0, HTTP-versie 1.1 en Chunk Encoding wanneer HTTP-versie 1.1 het onderhandelde transportprotocol is.

HTTP-statuscode verwerken bij hersynchronisatie en upgraden

De telefoon ondersteunt HTTP-antwoord voor externe inrichting (hersynchroniseren). Huidig telefoongedrag is ingedeeld op drie manieren:

- A: geslaagd, waarbij de waarden Periodiek hersynchroniseren en Willekeurige vertraging hersynchronisatie de volgende aanvragen bepalen.
- B: fout wanneer het bestand niet is gevonden of het profiel is beschadigd. De waarde Vertraging nieuwe poging na fout bij hersynchroniseren bepaalt de volgende aanvragen.
- C: andere fout wanneer een ongeldig(e) URL of IP-adres een verbindingsfout veroorzaakt. De waarde Vertraging nieuwe poging na fout bij hersynchroniseren bepaalt de volgende aanvragen.

Tabel 2: Telefoongedrag voor HTTP-antwoorden

HTTP-statuscode	Beschrijving	Telefoongedrag
301 permanent verplaatst	Deze en toekomstige aanvragen moeten worden omgeleid naar een nieuwe locatie.	Aanvraag direct opnieuw proberen met de nieuwe locatie.
302 gevonden	Bekend als tijdelijk verplaatst.	Aanvraag direct opnieuw proberen met de nieuwe locatie.
3xx	Andere 3xx antwoorden niet verwerkt.	C
400 onjuiste aanvraag	De aanvraag kan niet worden voldaan vanwege onjuiste syntaxis.	C
401 niet-geautoriseerd	Uitdaging standaard of Digest-toegangsverificatie.	Aanvraag direct opnieuw proberen met de verificatiereferenties. Maximaal 2 keer opnieuw proberen. Bij een fout is het telefoongedrag C.
403 verboden	Server weigert om te antwoorden.	C
404 niet gevonden	Gevraagde bron niet gevonden. Volgende aanvragen door client worden toegestaan.	B
407 proxyverificatie vereist	Uitdaging standaard of Digest-toegangsverificatie.	Aanvraag direct opnieuw proberen met de verificatiereferenties. Maximaal twee keer opnieuw proberen. Bij een fout is het telefoongedrag C.
4xx	Andere statuscodes voor clientfouten worden niet verwerkt.	C

HTTP-statuscode	Beschrijving	Telefoongedrag
500 interne serverfout	Algemene foutmelding.	Het telefoongedrag is C.
501 niet geïmplementeerd	De server herkent de aanvraagmethode niet, of de server kan niet voldoen aan de aanvraag.	Het telefoongedrag is C.
502 ongeldige gateway	De server fungeert als een gateway of proxy en ontvangt een ongeldig antwoord van de volgende server.	Het telefoongedrag is C.
503 service niet beschikbaar	De server is op dit moment niet beschikbaar (overbelast of uitgeschakeld voor onderhoud). Dit is een tijdelijke status.	Het telefoongedrag is C.
504 time-out van gateway	De server gedraagt zich als een gateway of proxy en ontvangt geen tijdig antwoord van de volgende server.	C
5xx	Andere serverfout	C