Klargjøringsveiledning for Cisco IP Phone 6800-serien av telefoner for flere plattformer

Utgitt første gang: 2017-11-22

Sist endret: 2019-01-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

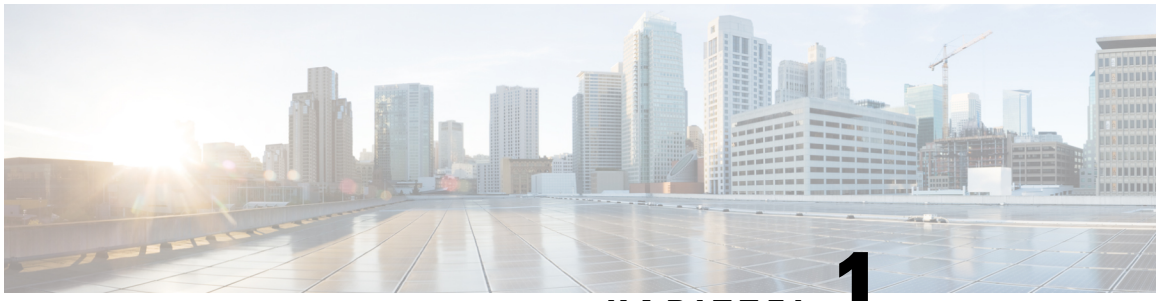
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

INNHOLD



KAPITTEL 1

Distribusjon og klargjøring

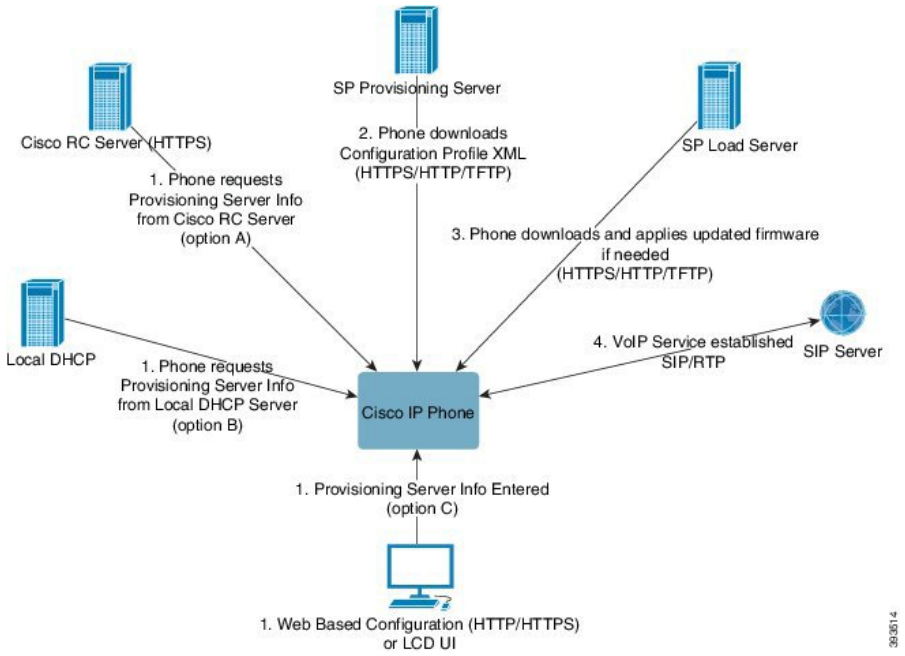
Oversikt over klargjøring

Cisco IP-telefoner er ment for distribusjon i store volum av VoIP-tjenesteleverandører til kunder i hjem, små bedrifter eller større organisasjoner. Klargjøring av telefonen ved hjelp av ekstern administrasjon og konfigurasjon sørger derfor for at telefonen fungerer som den skal hos kunden.

Cisco støtter tilpasset, kontinuerlig konfigurasjon av telefonen gjennom:

- pålitelig fjernkontroll av telefonen
- kryptering av kommunikasjonen som styrer telefonen
- effektiv telefonkontobinding

Telefoner kan klargjøres til å laste ned konfigurasjonsprofiler eller oppdatert fastvare fra en ekstern server. Nedlastinger kan skje når telefoner kobles til et nettverk, når de slås på, og ved bestemte intervaller. Klargjøring utføres ofte i forbindelse med VoIP-distribusjoner med høyt volum, som er vanlige for tjenesteleverandører. Konfigurasjonsprofiler eller oppdatert fastvare overføres til enheten ved hjelp av TFTP, HTTP eller HTTPS.



Klargjøringsprosessen for telefoner er grovt sett som følger:

1. Hvis telefonen ikke konfigureres, tas informasjon fra klargjøringsserveren i bruk på telefonen gjennom ett av følgende alternativer:
   - **A** – lastes ned fra Cisco Enablement Data Orchestration System (EDOS) Remote Customization (RC) server gjennom HTTPS.
   - **B** – etterspørres fra en lokal DHCP-server.
   - **C** – angis manuelt ved hjelp av det nettbaserte konfigurasjonsverktøyet for Cisco-telefoner eller grensesnittet i telefonen.
2. Telefonen laster ned informasjonen fra klargjøringsserveren og tar i bruk konfigurasjons-XML ved hjelp av HTTPS-, HTTP- eller TFTP-protokollen.
3. Ved behov laster telefonen ned og tar i bruk den oppdaterte fastvaren, ved hjelp av HTTPS, HTTP eller TFTP.
4. VoIP-tjenesten etableres ved hjelp av den angitte konfigurasjonen og fastvaren.

VoIP-tjenesteleverandører planlegger å distribuere mange telefoner til private kunder og småbedrifter. I bedrifter eller organisasjoner kan telefoner fungere som bladnoder. Leverandører distribuerer slike enheter i stor grad over Internett, og de kobles til via rutere og brannmurer i kundens lokaler.

Telefonen kan brukes som en ekstern utvidelse av tjenesteleverandørens bakgrunnsutstyr. Ekstern administrasjon og konfigurasjon sikrer at telefonen fungerer som den skal hos kunden.

Klargjøring via TR69

Cisco IP Phone hjelper administratoren å konfigurere TR69-parametrene ved hjelp av nettbrukergrensesnittet. Du finner informasjon om parametrene, inkludert en sammenligning av XML- og TR69-parametre, i administrasjonsveiledningen for den aktuelle telefonserien.

Telefonen støtter ACS-registrering (automatisk konfigurasjonsserver) fra DHCP-alternativ 43, 60 og 125.

- Alternativ 43 – leverandørspesifikk informasjon for URL-adressen til ACS.
- Alternativ 60 – leverandørklasseidentifikator, slik at telefonen kan identifisere seg selv med `dslforum.org` overfor ACS.
- Alternativ 125 – leverandørspesifikk informasjon for gatewaytilknytningen.

RPC-metoder

RPC-metoder som støttes

Telefonen støtter bare følgende begrensede sett med RPC-metoder (eksterne prosedyrekall):

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: RPC-metoden Download, støttede filtyper er:
    - fastvareoppgraderingsbilde
    - leverandørkonfigurasjonsfil
    - egendefinert sertifiseringsutstederfil (CA-fil)
- Transfer Complete

Hendelsestyper som støttes

Telefonen støtter hendelsestyper basert på støttede funksjoner og metoder. Bare følgende hendelsestyper støttes:

- oppstart (bootstrap)
- oppstart (boot)
- verdiendring
- tilkoblingsforespørsel
- regelmessig
- overføring fullført
- M-nedlasting
- M-omstart

Telefonens oppførsel under stor trafikk på nettverket

- Administrative oppgaver, som en intern portskanning eller en sikkerhetsskanning
- Angrep på nettverket, som et tjenestenektangrep

Distribusjon

Cisco IP-telefoner har praktiske klargjøringsmekanismer, basert på disse distribusjonsmodellene:

- Volumdistribusjon – tjenesteleverandøren får Cisco IP-telefoner i bulk og forhåndsklargjør dem internt, eller eksterntilpasningsenheter (RC) fra Cisco. Enhetene leveres deretter til kundene som del av en VoIP-tjenesteavtale.
- Distribusjon via forhandler – kunden kjøper Cisco IP-telefonen fra en butikk og ber om VoIP-tjeneste fra tjenesteleverandøren. Tjenesteleverandøren må støtte sikker ekstern konfigurasjonen av enheten.

Volumdistribusjon

I denne modellen leverer tjenesteleverandøren telefoner til kundene sine som del av en VoIP-tjenesteavtale. Enhetene er enten RC-enheter (ekstern tilpasning) eller forhåndsklargjort internt.

Cisco forhåndsklargjør RC-enheter til å resynkronisere med en Cisco-server som laster ned enhetsprofilen og fastvareoppdateringer.

En tjenesteleverandør kan forhåndsklargjøre telefoner med de ønskede parametrene, inkludert parametrene som styrer resynkroniseringen, på forskjellige måter:

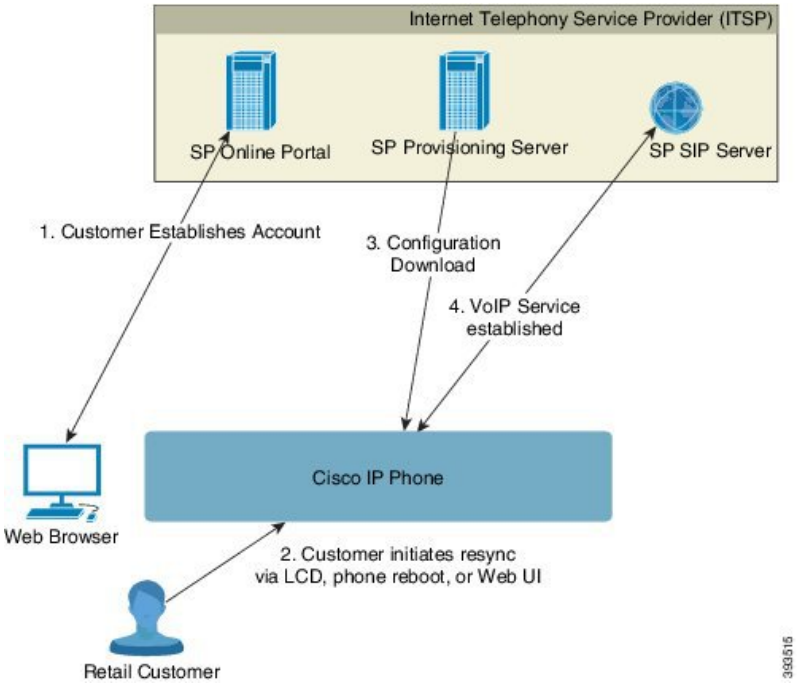
- Internt ved hjelp av DHCP og TFTP
- Eksternt ved hjelp av TFTP, HTTP eller HTTPS

- En kombinasjon av intern og ekstern klargjøring

Distribusjon via forhandler

I en forhandlerdistribusjonsmodell kjøper en kunde en telefon og abonnerer på en bestemt tjeneste. Leverandøren av Internett-telefoni (ITSP) konfigurerer og vedlikeholder en klargjøringsserver, og forhåndsklargjør telefonen til å resynkronisere med leverandørens server.

Figur 1: Distribusjon via forhandler



Telefonen har et nettbasert konfigurasjonsverktøy som viser intern konfigurasjon og godtar nye konfigurasjonsparameterverdier. Serveren godtar dessuten en spesiell URL-kommandosyntaks for ekstern resynkronisering av profiler og oppgradering av fastvare.

Kunden logger på tjenesten, oppretter en VoIP-konto, muligens via en nettportal, og binder enheten til den tilordnede tjenestekontoen. Den uklargjorte telefonen instrueres om å resynkronisere med en bestemt klargjøringsserveren gjennom en resynkroniserings-URL-kommando. URL-kommandoen inneholder ofte kunde-ID-numre for kontoer eller alfanumerisk kode som knytter enheten til den nye kontoen.

I eksemplet nedenfor blir en enhet på den DHCP-tilordnede IP-adressen 192.168.1.102 instruert om å klargjøre seg selv til SuperVoIP-tjenesten:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

I dette eksemplet er 1234abcd kunde-ID-nummeret til den nye kontoen. Den eksterne klargjøringsserveren knytter telefonen som utfører resynkroniseringsforespørselen, til den nye kontoen, basert på URL-adressen og den gitte kunde-ID-en. Gjennom denne første resynkroniseringsoperasjonen konfigureres telefon i ett trinn. Telefonen blir automatisk instruert om senere å resynkronisere seg til en permanent URL-adresse på serveren. Eksempel:

```
https://prov.supervoip.com/cisco-init
```

Ved både den første og den permanente tilgangen er klargjøringsserveren avhengig av telefonens klientsertifikat for godkjenning. Klargjøringsserveren gir korrekte konfigurasjonsparameterverdier basert på den tilknyttede tjenestekontoen.

Når enheten slås på, eller etter et visst tidsrom, resynkroniserer telefonen og laster ned de nyeste parametrene. Disse parametrene kan for eksempel ha som formål å konfigurere en søkegruppe, angi kortnumre og sette grenser for hvilke funksjoner en bruker kan endre.

Beslektede emner

Intern forhåndsklargjøring av enheter, på side 39

Resynkroniseringsprosess

Fastvaren på hver telefon inkluderer en administrasjonsnettserver som godtar nye konfigurasjonsparameterverdier. Telefonen kan instrueres til å resynkronisere konfigurasjonen etter en omstart eller ved planlagte intervaller med en angitt klargjøringsserver via en resynkroniserings-URL-kommando i enhetsprofilen.

Nettserveren er aktivert som standard. Du kan deaktivere eller aktivere nettserveren ved hjelp av resynkroniserings-URL-kommandoen.

Om nødvendig kan du be om umiddelbar resynkronisering via en resynkroniseringshandlings-URL. Resynkroniserings-URL-kommandoen kan inkludere kunde-ID-numre for kontoer eller alfanumerisk kode som knytter enheten unikt til brukerens konto.

Eksempel

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

I dette eksemplet blir en enhet på den DHCP-tilordnede IP-adressen 192.168.1.102 instruert om å klargjøre seg selv til SuperVoIP-tjenesten på prov.supervoip.com. Kunde-ID-nummeret for den nye kontoen er 1234abcd. Den eksterne klargjøringsserveren knytter telefonen som utfører resynkroniseringsforespørselen, til kontoen, basert på URL-adressen og kunde-ID-en.

Gjennom denne første resynkroniseringsoperasjonen konfigureres telefon i ett trinn. Telefonen blir automatisk instruert om senere å resynkronisere seg til en permanent URL-adresse på serveren.

Ved både den første og den permanente tilgangen er avhengig av klargjøringsserveren på klientsertifikatet for godkjenning. Serveren gir konfigurasjonsparameterverdier basert på den tilknyttede tjenestekontoen.

Klargjøring

En telefon kan konfigureres til å resynkronisere sin interne konfigurasjonstilstand til å være i samsvar med en ekstern profil, regelmessig og ved oppstart. Telefonen kontakter en normal klargjøringsserver (NPS) eller en tilgangskontrollserver (ACS).

Som standard gjøres det bare forsøk på resynkronisering når telefonen er ledig. Denne fremgangsmåten hindrer at oppgraderinger fører til omstart av programvare og avbrudd av samtaler. Hvis det er nødvendig med mellomliggende oppgraderinger for å nå en gjeldende oppgraderingstilstand fra en eldre versjon, kan oppgraderingslogikken automatisere flertrinnsoppgraderinger.

Normal klargjøringsserver

Normal klargjøringsserver (NPS) kan være en TFTP-, HTTP- eller HTTPS-server. Eksterne fastvareoppgraderinger gjøres ved hjelp av TFTP eller HTTP eller HTTPS fordi fastvaren ikke inneholder sensitive opplysninger.

Selv om HTTPS anbefales, krever ikke kommunikasjon med NPS bruk av sikre protokoller fordi den oppdaterte profilen kan krypteres med en delt hemmelig nøkkel. Du finner mer informasjon om bruk av HTTPS under Kommunikasjonskryptering, på side 8. Sikker førstegangsklargjøring gjøres med en metode som bruker SSL-funksjonalitet. En telefon som ikke er klargjort, kan motta en 256-biters symmetrisk nøkkelkryptert profil som er målrettet til enheten.

Tilgangskontroll for konfigurasjon

Telefonens fastvare har mekanismer for å begrense sluttbrukertilgang til enkelte parametre. Fastvaren gir bestemte påloggingsrettigheter til en **Admin**-konto (Administrator) eller en **User**-konto (User). Hver av disse kan beskyttes med passord uavhengig av hverandre.

- Administratorkonto – gir tjenesteleverandøren full tilgang til alle parametre på administrasjonsnettserveren.
- Brukerkonto – tillater at brukeren konfigurerer et delsett av parametrene på administrasjonsnettserveren.

Tjenesteleverandøren kan begrense brukerkontoen i klargjøringsprofilen på følgende måter:

- Angi hvilke konfigurasjonsparametre som skal være tilgjengelige for brukerkontoen, når de oppretter konfigurasjonen.
- Deaktivere brukertilgang til administrasjonsnettserveren.
- Deaktiver brukertilgang for LCD-brukergrensesnittet.
- Omgå **Angi passord**-skjermen for brukeren.
- Begrense hvilke Internett-domener enheten kan få tilgang til ved resynkronisering, oppgradering eller SIP-registrering for linje 1.

Beslektede emner

Egenskaper til elementkoder, på side 14
Tilgangskontroll, på side 16

Få tilgang til telefonens nettside

Åpne telefonnettsiden fra en nettleser på en datamaskin som kan nå telefonen i subnettet.

Hvis tjenesteleverandøren har deaktivert tilgang til konfigurasjonsverktøyet, kontakter du tjenesteleverandøren før du fortsetter.

Prosedyre

Trinn 1 Kontroller at datamaskinen kan kommunisere med telefonen. Ingen VPN i bruk.

Trinn 2 Start en nettleser.

Trinn 3 Skriv inn IP-adressen til telefonen i nettleserens adresselinje.

- Brukertilgang: **http://<ip-adressr>/user**
- Administratortilgang: **http://<ip address>/admin/advanced**
- Administratortilgang: **http://<ip address>**, klikk **Admin Login** (Administratorpålogging), og klikk **advanced** (avansert)

For eksempel `http://10.64.84.147/admin`

Tillate nettilgang til Cisco IP Phone

Aktiver konfigurasjonsprofilen hvis du vil vise telefonparametrene. Hvis du vil gjøre endringer i noen av parametrene, må du ha mulighet til å endre konfigurasjonsprofilen. Systemansvarlig kan ha deaktivert telefonalternativet for å gjøre telefonens nettbrukergrensesnitt visbart eller skrivbart.

Du finner mer informasjon under *Klargjøringsveiledning for Cisco IP Phone 6800-serien av telefoner for flere plattformer*.

Før du begynner

Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Prosedyre

Trinn 1 Klikk **Voice (Tale)** > **System**.

Trinn 2 I delen **System Configuration** (Systemkonfigurasjon) angir du **Enable Web Server** (Aktiver nettserver) til **Yes** (Ja).

Trinn 3 Hvis du vil oppdatere konfigurasjonsprofilen, klikker du **Submit All Changes** (Godta alle endringer) etter at du har endret feltene i telefonens nettbrukergrensesnitt.

Telefonen starter på nytt, og endringene tas i bruk.

Trinn 4 Du kan fjerne alle endringer du har gjort i den gjeldende økten (eller etter at du sist klikket **Submit All Changes** (Godta alle endringer)), ved å klikke **Undo All Changes** (Gjør om alle endringer). Verdiene går tilbake til den tidligere innstillingen.

Kommunikasjonskryptering

Konfigurasjonsparametrene som kommuniseres til enheten, kan inneholde godkjenningskoder eller annen informasjon som beskytter systemet mot uautorisert tilgang. Det er i tjenesteleverandørens interesse å hindre uautoriserte handlinger fra kundens side. Det er i kundens interesse å hindre uautorisert bruk av kontoen. Tjenesteleverandøren kan kryptere konfigurasjonsprofilkommunikasjonen mellom klargjøringsserveren og enheten og i tillegg begrense tilgangen til administrasjonsnettserveren.

Når klargjøres telefoner

Vanligvis konfigureres Cisco IP Phone til å klargjøres første gangen den kobles til nettverket. Telefonen klargjøres dessuten ved planlagte intervaller som tjenesteleverandøren eller VAR-forhandleren (value-added retailer) angir når de forhåndsklargjør (konfigurerer) telefonen. Tjenesteleverandører kan gi VAR-forhandlere

eller avanserte brukere tillatelse til klargjøre telefoner manuelt ved hjelp av telefontastaturet. Du kan også konfigurere klargjøring ved hjelp av telefonens nettbrukergrensesnitt.

Sjekk **Status** > **Phone Status (Telefonstatus)** > **Provisioning (Klargjøring)** i telefonens LCD-grensesnitt eller Provisioning Status (Klargjøringsstatus) i **Status**-fanen i det nettbaserte konfigurasjonsverktøyet.

Beslektede emner

Klargjøre telefoner manuelt fra tastaturet, på side 9

Klargjøre telefoner manuelt fra tastaturet

Prosedyre

Trinn 1 Trykk på **Programmer**  .

Trinn 2 Velg **Device administration (Enhetsstyring)** > **Profile Rule(Profilregel)**.

Trinn 3 Skriv inn profilregelen i følgende format:

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

Eksempel:

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

Hvis ingen protokoll angis, antas TFTP. Hvis ingen servernavn angis, brukes verten som ber om URL-adressen, som servernavn. Hvis ingen port angis, brukes standardporten (69 for TFTP, 80 for HTTP eller 443 for HTTPS).

Trinn 4 Trykk på **Resync** (Resynkroniser).

Beslektede emner

Når klargjøres telefoner, på side 8

Peer-fastvaredeling

Peer-fastvaredeling (PFS) er en fastvarefordelingsmodell som gjør det mulig for en Cisco IP Phone å finne andre telefoner av samme modell eller serie på subnettet og dele oppdaterte fastvarefiler når du må oppgradere flere telefoner samtidig. PFS bruker CPPDP (Cisco Peer-to-Peer-Distribution Protocol), som er Ciscos egenutviklede protokoll. Med CPPDP danner alle enhetene i delnettet et node-til-node-hierarki og kopierer deretter fastvaren eller de andre filene fra peer-enhetene til enhetene i nærheten. For å optimalisere fastvareoppgraderinger laster en rottelefon ned et fastvarebilde fra opplastingsserveren og overfører deretter fastvaren til andre telefoner på subnettet ved hjelp av TCP-tilkoblinger.

Peer-fastvaredeling:

- Begrenser opphoping av TFTP-overføringer til sentraliserte eksterne opplastingsservere.
- Fjerner behovet for å kontrollere fastvareoppgraderinger manuelt.
- Reduserer telefonens nedetid under oppgraderinger når et stort antall telefoner tilbakestilles samtidig.

Merk

- Peer-fastvaredeling fungerer ikke hvis ikke flere telefoner er angitt til å oppgradere samtidig. Når VARSLE (NOTIFY) sendes med Event:resync, starter den en ny synkronisering på telefonen. Eksempel på en xml som kan inneholde konfigurasjonene for å starte oppgraderingen:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Når du angir en IP-adresse og port for loggserveren for peer-fastvaredeling, sendes de PFS-spesifikke loggene til serveren som UDP-meldinger. Denne innstillingen må gjøres på hver telefon. Deretter kan du bruke loggmeldingene ved feilsøking av problemer som er knyttet til PFS.

Peer_Firmware_Sharing_Log_Server angir vertsnavn og port for den eksterne UDP-syslogserveren. Porten får automatisk standarden syslog 514.

Eksempel:

```
<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>
```

Hvis du vil bruke denne funksjonen, må du aktivere PFS på telefonene.

Omgå Angi passord-skjermen

Du kan omgå telefonens **Angi passord**-skjerm ved første oppstart eller etter en tilbakestilling til fabrikkinnstillinger, basert på disse klargjøringshandlingene:

- Konfigurasjon av DHCP
- Konfigurasjon av EDOS
- Konfigurasjon av brukerpassord i telefonens XML-konfigurasjonsfil.

Tabell 1: Klargjøringshandlinger som bestemmer om Angi passord-skjermen skal vises

DHCP konfigurert	EDOS konfigurert	Brukerpassord konfigurert	Omgå Angi passord-skjermen
Ja	–	Ja	Ja
Ja	–	Nei	**Nei**
Nei	Ja	Ja	Ja
Nei	Ja	Nei	**Nei**
Nei	Nei	–	**Nei**

Prosedyre

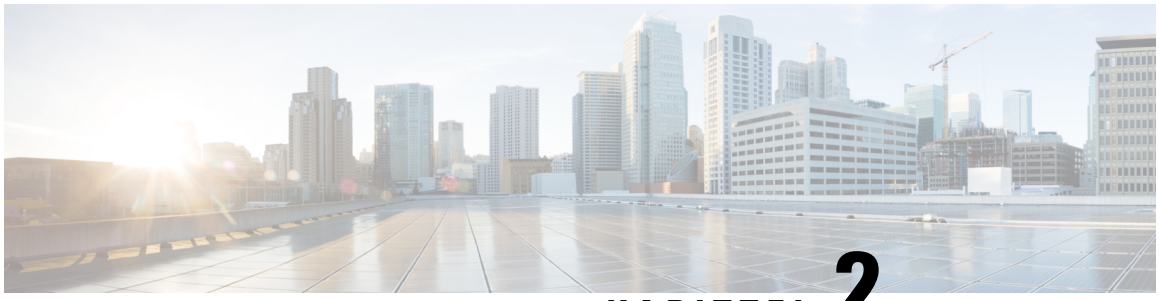
Trinn 1 Rediger `config.xml`-filen til telefonen i et tekst- eller XML-redigeringsprogram.

Trinn 2 Sett inn koden **< User_Password >** på én av følgende måter:

- **Ingen passord (start- og sluttkode)** – **<User_Password></User_Password>**
- **Passordverdi (4 til 127 tegn)** – **<User_Password ua="rw">abc123</User_Password>**

- **Ingen passord (bare startkode)** – **`<User_Password />`**

Trinn 3 Lagre endringene i `config.xml`-filen.



KAPITTEL 2

Klargjøringsskript

Klargjøringsskript

Telefonen godtar konfigurasjon i XML-format.

Du finner detaljert informasjon om telefonen i administrasjonsveiledningen for den aktuelle enheten. Hver veiledning beskriver parametrene som kan konfigureres gjennom administrasjonsnettserveren.

Formater for konfigurasjonsprofiler

Konfigurasjonsprofilen definerer parameterverdiene for telefonen.

XML-formatet for konfigurasjonsprofiler bruker standard XML-redigeringsverktøy til å kompilere parametre og verdier.

Merk Det er bare UTF-8-tegnsettet som støttes. Hvis du endrer profilen i et redigeringsprogram, må du ikke endre kodingsformatet; hvis ikke, gjenkjenner ikke telefonen filen.

Hver telefon har et annet funksjonssett og derfor et annet sett med parametre.

Profil i XML-format (XML)

Profilen i åpent format er en tekstfil med XML-lignende syntaks i et hierarki av elementer, med elementattributter og -verdier. Med dette formatet kan du opprette konfigurasjonsfiler ved hjelp av standardverktøy. En konfigurasjonsfil i dette formatet kan sendes fra klareringsserveren til telefonen under en resynkroniseringsoperasjon. Filen kan sendes uten kompilering som et binært objekt.

Telefonen kan godta konfigurasjonsformater generert av standardverktøy. Denne funksjonen gjør det enklere å utvikle bakgrunnsprogramvare – for klargjøringsservere – som generer konfigurasjonsprofiler fra eksisterende databaser.

Klargjøringsserveren leverer denne typen filer til telefonen via en TLS-sikret kanal for å beskytte konfidensiell informasjon i konfigurasjonsprofilen. Filen kan eventuelt komprimeres ved hjelp av deflate-algoritmen i gzip (RFC1951).

Filen kan krypteres med en av følgende krypteringsmetoder:

- AES-256-CBC-kryptering
- RFC-8188-basert kryptering av HTTP-innhold med AES-128-GCM-kryptering

Eksempel: åpent profilformat

```
<flat-profile>
<Resync_On_Reset> Yes </Resync_On_Reset>
<Resync_Periodic> 7200 </Resync_Periodic>
<Profile_Rule> tftp://prov.telco.com:6900/cisco/config/CP_xxxx_MPP.cfg</Profile_Rule>
</flat-profile>
```

Elementkoden <flat-profile> omslutter alle parameterelementer som telefonen gjenkjenner.

Beslektede emner

Komprimering og kryptering av åpen profil (XML), på side 17

Komponenter i konfigurasjonsfiler

En konfigurasjonsfil kan ha disse komponentene:

- Elementkoder
- Attributter
- Parametre
- Formateringsfunksjoner
- XML-kommentarer

Egenskaper til elementkoder

- XML-klargjøringsformatet og nettgrensesnittet tillater konfigurering av de samme innstillingene. XML-kodenavnet og feltnavnene i nettgrensesnittet er like, men varierer på grunn av navnebegrensninger for XML-elementet. For eksempel understrekingstegn (_) i stedet for " ".
- Telefonen gjenkjenner elementer med gyldige parameternavn som er innkapslet i det spesielle <flat-profile>-elementet.
- Elementnavn står i vinkelparenteser.
- De fleste elementnavn ligner på feltnavnene i administrasjonsnettsidene til enheten, med følgende endringer:

- Elementnavn kan ikke inneholde mellomrom eller spesialtegn. Hvis du vil utlede elementnavnet fra navnet i feltet på administrasjonsnettsiden, setter du inn et understrekingstegn for hvert mellomrom eller spesialtegn `[`, `]`, `(`, `)` eller `/`.

  Eksempel: Elementet <Resync_On_Reset> representerer feltet **Resync On Reset** (Resynkroniser ved tilbakestilling).

- Hvert elementnavn må være unikt. På administrasjonsnettsidene kan de samme feltene vises på flere nettsider, som for eksempel sidene Line (Linje), User (Bruker) og Extension (Internnummer). Føy `[n]` til elementnavnet for å angi nummeret som vises i sidefanen.

  Eksempel: Elementet <Dial_Plan_1_> representerer **Dial Plan** (Oppringingsplan) for linje 1.

- Hver startelementkode må ha en tilsvarende sluttelementkode. Eksempel:

```
<flat-profile>
<Resync_On_Reset> Yes
  </Resync_On_Reset>
<Resync_Periodic> 7200
  </Resync_Periodic>
<Profile_Rule>tftp://prov.telco.com: 6900/cisco/config/CP_xxxx_MPP.cfg
  </Profile_Rule>
</flat-profile>
```

- Elementkoder skiller mellom store og små bokstaver.
- Tomme elementkoder er tillatt og blir tolket som å konfigurere at verdien skal være tom. Skriv inn startelementkoden uten en tilsvarende elementkode, og sett inn et mellomrom og en skråstrek før den avsluttende vinkelhakeparentesen (>). I dette eksemplet er profilregel B tom:

```
<Profile_Rule_B />
```

- Tomme elementkoder kan brukes til å hindre overskriving av brukerdefinerte verdier under en resynkroniseringsoperasjon. I eksemplet nedenfor forblir brukerens kortnummerinnstillinger uendret:

```
<flat-profile>
<Speed_Dial_2_2_ ua=”rw”/>
<Speed_Dial_3_2_ ua=”rw”/>
<Speed_Dial_4_2_ ua=”rw”/>
<Speed_Dial_5_2_ ua=”rw”/>
<Speed_Dial_6_2_ ua=”rw”/>
<Speed_Dial_7_2_ ua=”rw”/>
<Speed_Dial_8_2_ ua=”rw”/>
<Speed_Dial_9_2_ ua=”rw”/>
</flat-profile>
```

- Bruk en tom verdi til å angi en tom streng for den tilsvarende parameteren. Skriv inn et start- og sluttelement uten at det er noen verdier mellom dem. I eksemplet nedenfor er parameteren GPP_A satt til en tom streng.

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

- Elementnavn som ikke gjenkjennes, ignoreres.

Beslektede emner

Tilgangskontroll for konfigurasjon, på side 7

Attributtet brukertilgang

Kontrollene i attributtet brukertilgang (**ua**) kan brukes til å endre tilgang gjennom brukerkontoen. Hvis attributtet **ua** ikke er angitt, beholdes den eksisterende innstillingen for brukertilgang. Attributtet påvirker ikke tilgang gjennom administratorkontoen.

Attributtet **ua** må – hvis det brukes – ha én av følgende verdier:

- na – ingen tilgang
- ro – skrivebeskyttet
- rw – lese og skrive

Følgende eksempel viser attributtet **ua**:

```
<flat-profile>
   <SIP_TOS_DiffServ_Value_1_ ua=”na”/>
   <Dial_Plan_1_ ua=”ro”/>
   <Dial_Plan_2_ ua=”rw”/>
</flat-profile>
```

Verdien til **ua**-alternativet må omsluttes av doble anførselstegn.

Tilgangskontroll

Hvis parameteren <Phone-UI-User-Mode> aktiveres, oppfyller telefonens grafiske brukergrensesnitt (GUI) brukertilgangsattributtet i de aktuelle parametrene når GUI viser et menyelement.

For menyoppføringer knyttet til en enkelt konfigurasjonsparameter:

- Klargjøres parameteren med attributtet "ua=na" ("ua" betyr "brukertilgang»), forsvinner oppføringen.
- Klargjøres parameteren med attributtet "ua=ro", blir oppføringen skrivebeskyttet og kan ikke redigeres.

For menyoppføringer knyttet til flere konfigurasjonsparametre:

- Klargjøres alle aktuelle parametre med attributtet "ua=na", forsvinner oppføringene.

Beslektede emner

Tilgangskontroll for konfigurasjon, på side 7

Parameteregenskaper

Disse egenskapene gjelder for parametre:

- Alle parametre som ikke angis av en profil, forblir uendret i telefonen.
- Parametre som ikke gjenkjennes, ignoreres.
- Hvis en profil med åpent format inneholder flere forekomster av den samme parameterkoden, overstyrer den siste forekomsten alle de tidligere. For å unngå utilsiktet overstyring av konfigurasjonsverdier for en parameter, anbefaler vi at hver profil ikke angir mer enn én forekomst av en parameter.

- Den sist behandlede profilen får prioritet. Hvis flere profiler angir den samme konfigurasjonsparameteren, får verdien til den siste profilen prioritet.

Strengformater

Disse egenskapene gjelder formateringen av strenger:

- Kommentarer er tillatt via standard XML-syntaks.

```
<!-- My comment is typed here -->
```

- Innledende og etterfølgende mellomrom er tillatt for lesing, men fjernes fra parameterverdien.
- Nye linjer innenfor en verdi konverteres til mellomrom.
- Et XML-hode med formen `<? ?>` er tillatt, men telefonen ignorerer det.
- Hvis du vil angi spesialtegn, kan du bruke grunnleggende XML-escapetegn, som vist i tabellen nedenfor.

Spesialtegn	XML-escapesekvens
& (ampersand)	&
< (mindre enn)	<
> (større enn)	>
' (apostrof)	'
" (dobbelt anførselstegn)	"

I eksemplet nedenfor skrives escapetegn inn for å angi større enn- og mindre enn-symboler som er nødvendige i en oppringingsplanregel. Dette eksemplet definerer en oppringingsplan for en informasjonstjeneste som angir parameteren <Dial_Plan_1_> (**Admin Login (Administratorpålogging)** > **advanced (avansert)** > **Voice (Tale)** > **Ext (n) (Int (n))** lik (S0 <:18005551212>).

```
<flat-profile>
 <Dial_Plan_1_>
  (S0 <:18005551212>)
 </Dial_Plan_1_>
</flat-profile>
```

- Numeriske escapetegn, som benytter desimale og heksadesimale verdier (s.a. `&#40;` og `&#46;`), oversettes.
- Telefonens fastvare støtter bare ASCII-tegn.

Komprimering og kryptering av åpen profil (XML)

Åpne konfigurasjonsprofiler kan komprimeres for å redusere nettverksbelastningen på klargjøringsserveren. Profilen kan dessuten krypteres for å beskytte konfidensiell informasjon. Komprimering er ikke nødvendig, men må gjøres før en kryptering.

Beslektede emner

Formater for konfigurasjonsprofiler, på side 13

Komprimering av åpne profiler

Den støttede komprimeringsmetoden er deflate-algoritmen i gzip (RFC1951). Gzip-verktøyet og komprimeringsbiblioteket som implementerer den samme algoritmen (zlib), er tilgjengelige fra Internett-nettsteder.

Telefonen identifiserer komprimering ved at den komprimerte filen inneholder et gzip-kompatibelt filhode. Filhodet genereres når gzip-verktøyet aktiveres på den opprinnelige åpne profilen. Telefonen inspiserer det nedlastede filhodet for å bestemme filformatet.

Hvis for eksempel `profile.xml` er en gyldig profil, godtas også filen `profile.xml.gz`. Én av følgende kommandoer kan generere denne profiltypen:

- `>gzip profile.xml`

  Erstatter den opprinnelige filen med en komprimert fil.

- `>cat profile.xml | gzip > profile.xml.gz`

  Bevarer den opprinnelige filen, lager en ny komprimert fil.

Det gis en innføring i komprimering er i delen Komprimere en åpen profil med Gzip, på side 60.

Beslektede emner

Komprimere en åpen profil med Gzip, på side 60

Kryptering av åpne profiler

Symmetrisk nøkkelkryptering kan brukes til å kryptere åpne konfigurasjonsprofiler, enten filen er komprimert eller ikke. Eventuell komprimering må utføres før kryptering.

Klargjøringsserveren bruker HTTPS til å håndtere den første klargjøringen av telefoner etter distribusjon. Frakoblet forhåndskryptering av konfigurasjonsprofiler gjør det mulig å bruke HTTP til resynkronisering av profiler. Dette reduserer belastningen på HTTPS-serveren ved omfattende distribusjoner.

Telefonen støtter to krypteringsmetoder for konfigurasjonsfiler:

- AES-256-CBC-kryptering
- RFC 8188-basert kryptering av HTTP-innhold med AES-128-GCM-kryptering

Nøkkelen eller nøkkelmaterialet (IKM) må være forhåndsklargjort på enheten. Oppstart av den hemmelige nøkkelen kan gjøres sikkert ved hjelp av HTTPS.

Navnet på konfigurasjonsfilen må ikke ha et bestemt format, men et filnavn som slutter med suffikset `.cfg`, angir normalt en konfigurasjonsprofil.

AES-256-CBC-kryptering

Telefonen støtter AES-256-CBC-kryptering for konfigurasjonsfiler.

OpenSSL-krypteringsverktøyet, som er tilgjengelig for nedlasting fra forskjellige Internett-nettsteder, kan utføre krypteringen. Støtte for 256-biters AES-kryptering kan kreve at verktøyet rekompileres for å aktivere AES-kode. Fastvaren er testet mot versjon openssl-0.9.7c.

Kryptere en profil med OpenSSL, på side 61 gir en innføring i kryptering.

Telefonen identifiserer kryptering ved at filen har formatet som genereres av følgende kommando:

```
# example encryption key = SecretPhrase1234

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml -out profile.cfg

# analogous invocation for a compressed xml file

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml.gz -out profile.cfg
```

En liten -k kommer før den hemmelige nøkkelen, som kan være en hvilken som helst frase med ren tekst, og som brukes til å generere et tilfeldig 64-biters salt. Med hemmeligheten angitt av argumentet -k utleder krypteringsverktøyet en tilfeldig 128-biters initialvektor og den faktiske 256-biters krypteringsnøkkelen.

Når denne formen for kryptering brukes på en konfigurasjonsprofil, må telefonen informeres om den hemmelige nøkkelverdien for å kunne dekryptere filen. Verdien angis som en kvalifikator i profil-URL-adressen. Syntaksen er som følger, ved bruk av eksplisitt URL-adresse:

```
[--key "SecretPhrase1234"] http://prov.telco.com/path/profile.cfg
```

Verdien programmeres ved å bruke én av Profile_Rule-parametrene.

Beslektede emner

Kryptere en profil med OpenSSL, på side 61

Makroutvidelse

Flere klargjøringsparametre gjennomgår makroutvidelse internt før de blir evaluert. Dette preevalueringstrinnet gir større fleksibilitet ved styring av resynkroniserings- og oppgraderingsprosessene.

Disse parametergruppene gjennomgår makroutvidelse før evaluering:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

I enkelte tilfeller kan gjennomgå noen generelle parametre (GPP_ *) også gjennomgå makroutvidelse, som nærmere beskrevet i Valgfrie resynkroniseringsargumenter, på side 22.

Under makroutvidelse erstatter innholdet i de navngitte variablene uttrykk i skjemaet $NAME og $(NAME). Variablene omfatter generelle parametre, flere produktidentifikatorer, visse hendelsestidtakere og klargjøringstilstandsverdier. Du finner en fullstendig liste under Makroutvidelsesvariabler, på side 72.

I eksemplet nedenfor brukes uttrykket $(MAU) til å sette inn MAC-adressen 000E08012345.

Administratoren skriver: **`$(MAU)config.cfg`**

Den påfølgende makroutvidelsen for en enhet med MAC-adresse 000E08012345 er:
`000E08012345config.cfg`

Hvis et makronavn ikke gjenkjennes, utvides det ikke. Navnet STRANGE gjenkjennes for eksempel ikke som et gyldig makronavn, mens MAU gjenkjennes som et gyldig makronavn.

Administratoren skriver: **`$STRANGE$MAU.cfg`**

Den påfølgende makroutvidelsen for en enhet med MAC-adresse 000E08012345 er:
`$STRANGE000E08012345.cfg`

Makroutvidelse brukes ikke rekursivt. $$MAU" utvides for eksempel til $MAU" ($$ utvides) og gir ikke MAC-adressen.

Innholdet i spesialparametrene, fra GPP_SA til GPP_SD, tilordnes til makrouttrykkene fra $SA til $SD. Disse parameterne makroutvides bare som argument i alternativene **--key**, **--uid** og **--pwd** i en resynkroniserings-URL-adresse.

Betingelsesuttrykk

Betingelsesuttrykk kan utløse resynkroniseringshendelser og velge blant alternative URL-adresser for resynkroniserings- og oppgraderingsoperasjoner.

Betingelsesuttrykk består av en liste med sammenligninger, atskilt med operatoren **og**. Alle sammenligninger må oppfylles for at betingelsen skal bli sann.

Hver sammenligning kan være knyttet til én av følgende tre typer litteraler:

- heltall
- versjonsnumre for programvare eller maskinvare
- strenger med doble anførselstegn

Versjonsnumre

Telefoner for flere plattformer (MPP) angir programvareversjon i dette formatet, hvor BN = buildnummer:

- Cisco IP Phone 6800-serien – `sip68xx.v1-v2-v3MPP-BN`

Sammenligningsstrengen må bruke det samme formatet. Det vil ellers oppstå formatanalysefeil.

I programvareversjon kan v1-v2-v3-v4 angi ulike sifre og tegn, men må begynne med et siffer. Ved sammenligning av programvareversjoner sammenlignes v1-v2-v3-v4 i rekkefølge, og sifrene lengst til venstre har prioritet fremfor de siste.

Hvis v[x] bare inneholder sifre, sammenlignes sifrene; hvis v[x] inneholder sifre + bokstaver, sammenlignes sifrene først og deretter sammenlignes bokstavene i alfabetisk rekkefølge.

Eksempel på gyldig versjonsnummer

sipyyyy.11-0-0MPP-BN

Derimot: 11.0.0 er et ugyldig format.

Sammenligning

sip68xx.11-0-0MPP-BN < sip68xx.11-0-1MPP-BN

Strenger med anførselstegn kan sammenlignes for likhet eller ulikhet. Heltall og versjonsnumre kan dessuten sammenlignes aritmetisk. Sammenligningsoperatorene kan uttrykkes som symboler eller akronymer. Akronymer er praktiske å bruke til å uttrykke betingelser i profiler i åpent format.

Operator	Alternativ syntaks	Beskrivelse	Gjelder for heltall og versjonsoperander	Gjelder for strengoperander med anførselstegn
=	eq	er lik	Ja	Ja
!=	ne	er ulik	Ja	Ja
<	lt	mindre enn	Ja	Nei
<=	le	mindre enn eller lik	Ja	Nei
>	gt	større enn	Ja	Nei
>=	ge	større enn eller lik	Ja	Nei
AND		og	Ja	Ja

Det er viktig å sette makrovariabler i doble anførselstegn der det forventes en strenglitteral. Ikke gjør dette når det forventes et tall eller et versjonsnummer.

Når de brukes i forbindelse med parametrene Profile_Rule* og Upgrade_Rule, må betingelsesuttrykk stå i syntaksen "(uttr)?", som i dette eksemplet på en oppgraderingsregel. Husk at BN betyr buildnummer.

```
($SWVER ne sip68xx.11-0-0MPP)? http://ps.tell.com/sw/sip68xx.11-0-0MPP-BN.loads
```

Ikke bruk den foregående syntaksen med parenteser til å konfigurere Resync_Trigger_*-parametre.

URL-syntaks

Bruk standard URL-syntaks til å angi hvordan konfigurasjonsfiler og fastvarelaster skal hentes i parametrene Profile_Rule* og Upgrade_Rule henholdsvis. Syntaksen er som følger:

[skjema://] [server [:port]] filbane

Hvor **skjema** er én av disse verdiene:

- tftp
- http
- https

Hvis **skjema** utelates, antas tftp. Serveren kan være et DNS-gjenkjennelig vertsnavn eller en numerisk IP-adresse. Porten er destinasjonen for UDP- eller TCP-portnummeret. Filbanen må begynne med rotkatalogen (/); det må være en absolutt bane.

Hvis **server** mangler, brukes tftp-server angitt gjennom DHCP (alternativ 66).

Merk Ved oppgraderingsregler må server angis.

Hvis **port** mangler, brukes standardporten for det angitte skjemaet. Tftp bruker UDP-port 69, http bruker TCP-port 80, https bruker TCP-port 443.

Det må angis filbane. Den trenger ikke nødvendigvis vise til en statisk fil, men kan angi dynamisk innhold skaffet gjennom CGI.

Makroutvidelse gjelder i URL-adresser. Følgende er eksempler på gyldige URL-adresser:

```
/$MA.cfg
/cisco/cfg.xml
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/cisco$MA.cfg
http://neptune.speak.net:8080/prov/$D/$E.cfg
https://secure.me.com/profile?Linksys
```

Når du bruker DHCP-alternativ 66, støttes ikke tom syntaks av oppgraderingsregler. Det er bare aktuelt for Profile Rule*.

RFC 8188-basert kryptering av HTTP-innhold

Telefonen støtter RFC 8188-basert kryptering av HTTP-innhold med AES-128-GCM-kryptering for konfigurasjonsfiler. Med denne krypteringsmetoden kan alle enheter lese HTTP-meldingshoder. Imidlertid kan bare enhetene som kjenner til nøkkelmaterialet (IKM), lese pakkeinnholdet. Når telefoner klargjøres ved hjelp av nøkkelmateriale, kan telefonene og klargjøringsserveren utveksle konfigurasjonsfiler på en sikker måte, samtidig som tredjeparts nettverkselementer kan bruke meldingshodene til analyse og overvåking.

XML-konfigurasjonsparameteren **IKM_HTTP_Encrypt_Content** inneholder nøkkelmaterialet på telefonen. Av sikkerhetsmessige årsaker er ikke denne parameteren tilgjengelig på telefonens administrasjonsnettside. Det vises heller ikke i telefonens konfigurasjonsfil, som du får tilgang til via telefonens IP-adresse eller via telefonens konfigurasjonsrapporter, som sendes til klargjøringsserveren.

Hvis du vil bruke RFC 8188-basert kryptering, må du kontrollere at følgende er på plass:

- Klargjør telefonen med nøkkelmateriale ved å angi nøkkelmaterialet med XML-parameteren **IKM_HTTP_Encrypt_Content** i konfigurasjonsfilen som sendes fra klargjøringsserveren til telefonen.
- Hvis denne krypteringen brukes på konfigurasjonsfilene som sendes fra klargjøringsserveren til telefonen, må du sørge for at HTTP-hodet *Content-Encoding* i konfigurasjonsfilen er "aes128gcm".

  Hvis dette hodet mangler, får AES-256-CBC-metoden forrang. Telefonen bruker AES-256-CBC-dekryptering hvis det er en AES-256-CBC-nøkkel i en profilregel, uavhengig av nøkkelmateriale.
- Hvis du vil at telefonen skal bruke denne krypteringen på konfigurasjonsrapporter som sendes til klargjøringsserveren, må du sjekke at det ikke er angitt en AES-256-CBC-nøkkel i rapportregelen.

Valgfrie resynkroniseringsargumenter

Valgfrie argumenter, **key**, **uid** og **pwd** kan stå foran URL-adressene som angis i Profile_Rule*-parametrene, og alt sammen omsluttes av hakeparentes.

Key

Alternativet **--key** forteller telefonen at konfigurasjonsfilen som den mottar fra klargjøringsserveren, er kryptert med AES-256-CBC-kryptering, med mindre hodet *Content-Encoding* i filen angir

"aes128gcm"-kryptering. Selve nøkkelen angis som en streng etter ordet **--key**. Nøkkelen kan eventuelt settes i doble anførselstegn ("). Telefonen bruker nøkkelen til å dekryptere konfigurasjonsfilen.

Brukseksempler

```
[--key VerySecretValue]
[--key "my secret phrase"]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

Valgfrie argumenter i hakeparentes makroutvides. Spesialparametre – GPP_SA til GPP_SD – makroutvides til makrovariabler – fra $SA til $SD – bare når de brukes som nøkkelalternativargumenter. Se disse eksemplene:

```
[--key $SC]
[--key "$SD"]
```

I profiler med åpent format må argumentet til **--key** være det samme som argumentet til alternativet **-k** som gis til **openssl**.

Uid og pwd

Alternativene **uid** og **pwd** kan brukes til å angi godkjenning med bruker-ID og passord for den angitte URL-adressen. Valgfrie argumenter i hakeparentes makroutvides. Spesialparametre – GPP_SA til GPP_SD – makroutvides til makrovariabler – fra $SA til $SD – bare når de brukes som nøkkelalternativargumenter. Se disse eksemplene:

```
GPP_SA = MyUserID
GPP_SB = MySecretPassword
```

[--uid $SA -pwd $SB] https://provisioning_server_url/path_to_your_config/your_config.xml

utvides til:

[--uid MyUserID -pwdMySecretPassword]
https://provisioning_server_url/path_to_your_config/your_config.xml

Ta i bruk en profil på IP-telefonienheten

Når du opprettet et XML-konfigurasjonsskript, må det sendes til telefonen for å bli tatt i bruk. Du kan ta i bruk konfigurasjonen ved å laste ned konfigurasjonsfilen til telefonen fra en TFTP-, HTTP- eller HTTPS-server via en nettleser, eller ved å bruke kommandolinjeverktøyet cURL.

Laste ned konfigurasjonsfilen til telefonen fra en TFTP-server

Følg denne fremgangsmåten for å laste ned konfigurasjonsfilen til et TFTP-serverprogram på datamaskinen.

Prosedyre

Trinn 1 Koble datamaskinen til telefonens lokalnett.

Trinn 2 Kjør et TFTP-serverprogram på datamaskinen, og sjekk at konfigurasjonsfilen er tilgjengelig i TFTP-rotkatalogen.

Trinn 3 Angi IP-adressen til telefonens lokalnett, IP-adressen til datamaskinen, filnavnet og påloggingsinformasjonen i en nettleser. Bruk dette formatet:

http://<WAN_IP_Address>/admin/resync?tftp://<PC_IP_Address>/<file_name>&xuser=admin&xpassword=<password>

Eksempel:

```
http://192.168.15.1/admin/resync?tftp://192.168.15.100/my_config.xml&xuser=admin&xpassword=admin
```

Laste ned konfigurasjonsfilen til telefonen med cURL

Følg denne fremgangsmåten for å laste ned konfigurasjonen til telefonen ved hjelp av cURL. Dette kommandolinjeverktøyet brukes til å overføre data med en URL-syntaks. Du kan laste ned cURL fra:

https://curl.haxx.se/download.html

Merk Vi anbefaler at du ikke bruker cURL til å legge ut konfigurasjonen til telefonen, fordi brukernavn og passord kan bli registrert under bruk av cURL.

Prosedyre

Trinn 1 Koble datamaskinen til lokalnettporten på telefonen.

Trinn 2 Last ned konfigurasjonsfilen til telefonen ved å skrive inn følgende cURL-kommando:

```
curl –d @my_config.xml
“http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin”
```

Klargjøringsparametre

Denne delen beskriver klargjøringsparametrene, grovt gruppert etter funksjon:

Disse klargjøringsparametertypene finnes:

- generelle
- aktiveringsparametre
- utløserparametre
- konfigurerbare tidsplaner
- profilregler
- oppgraderingsregel

Generelle parametre

De generelle parametrene GPP_* (**Admin Login (Administratorpålogging)** > **advanced (avansert)** > **Voice (Tale)** > **Provisioning (Klargjøring)**) brukes som frie strengregistre når telefonen konfigureres til å samhandle med en bestemt klargjøringsserverløsning. GPP_*-parametrene er som standard tomme. De kan konfigureres til å inneholde forskjellige verdier, inkludert følgende:

- krypteringsnøkler
- URL-er
- statusinformasjon om flertrinnsklargjøring
- POST-forespørselsmaler
- aliasmatriser for parameternavn
- delvise strengverdier, eventuelt satt sammen til fullstendige parameterverdier

GPP_*-parametrene er tilgjengelige for makroutvidelse i andre klargjøringsparametre. Til dette er makronavn med én stor bokstav (A til P) tilstrekkelig til å identifisere innholdet i GPP_A til GPP_P. Makronavnene med to store bokstaver fra SA til SD identifiserer dessuten GPP_SA til GPP_SD som et spesielt tilfelle når de brukes som argumenter i følgende URL-alternativ:

key, **uid** og **pwd**

Disse parametrene kan brukes som variabler i klargjørings- og oppgraderingsregler. De kan refereres til ved at man setter et '$'-tegn, som for eksempel $GPP_A, foran variabelnavnet.

Bruke generelle parametre

Hvis for eksempel GPP_A inneholder strengen ABC, og GPP_B inneholder 123, utvides uttrykket AB til ABC123.

Før du begynner

Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Prosedyre

Trinn 1 Velg **Tale** > **Klargjøring**.

Trinn 2 Bla til delen **General Purpose Parameters** (Generelle parametre).

Trinn 3 Angi gyldige verdier i feltene, fra GPP A til GPP P.

Trinn 4 Klikk på **Godta alle endringer**.

Aktiveringsparametre (Enable)

Parametrene Provision_Enable og Upgrade_Enable styrer all resynkronisering av profiler og oppgradering av fastvare. Disse parameterne styrer resynkronisering og oppgraderinger uavhengig av hverandre. Disse parametrene styrer også URL-kommandoer for resynkronisering og oppgradering som utstedes gjennom administrasjonsnettserveren. Begge disse parametrene angis til **Yes** (Ja) som standard.

Parameteren Resync_From_SIP styrer resynkroniseringsforespørsler. Det sendes en SIP-varslingshendelse fra tjenesteleverandørens proxyserver til telefonen. Hvis dette er aktivert, kan proxyserveren be om resynkronisering. Proxyserveren gjør dette ved å sende en SIP-varslingsmelding som inneholder hodet Event: resync, til enheten.

Enheten utfordrer forespørselen med et 401-svar (godkjenning avvist for benyttet påloggingsinformasjon). Enheten forventer en godkjent påfølgende forespørsel før den oppfyller resynkroniseringsforespørselen fra proxyserveren. Hodene Event: reboot_now og Event: restart_now utfører henholdsvis kalde og varme omstarter, som også blir utfordret.

De to gjenstående aktiveringsparametrene er Resync_On_Reset og Resync_After_Upgrade_Attempt. Disse parametrene bestemmer om enheten skal utføre resynkronisering etter at oppstartsprogramvaren har startet på nytt, og etter hvert oppgraderingsforsøk.

Når Resync_On_Reset aktiveres, introduserer enheten en tilfeldig forsinkelse som kommer etter oppstartssekvensen, før tilbakestillingen utføres. Forsinkelsen er en tilfeldig tidsverdi opptil verdien som Resync_Random_Delay (i sekunder) angir. I en gruppe telefoner som slås på samtidig, sprer denne forsinkelsen starttidspunktene for de enkelte enhetenes resynkroniseringsforespørsler. Funksjonen kan være nyttig ved store distribusjoner i boligområder hvis det oppstår strømbrudd.

Utløserparametre

Telefonen kan resynkronisere med bestemte mellomrom eller på et bestemt tidspunkt.

Resynkronisere ved bestemte intervaller

Telefonen er laget for å resynkronisere regelmessig med klargjøringsserveren. Resynkroniseringsintervallet konfigureres i Resync_Periodic (sekunder). Hvis verdien blir stående tom, resynkroniserer ikke enheten regelmessig.

Resynkroniseringen foregår vanligvis mens talelinjene er ledige. Hvis en talelinje er aktiv når det er tid for en resynkronisering, utsetter telefonen resynkroniseringen til linjen blir ledig igjen. En resynkronisering kan føre til at konfigurasjonsparameterverdiene endres.

En resynkroniseringsoperasjonen kan mislykkes fordi telefonen ikke kan hente en profil fra serveren, fordi den nedlastede filen er skadet, eller fordi det har oppstått en intern feil. Enheten prøver å resynkronisere på nytt etter et intervall som angis i Resync_Error_Retry_Delay (sekunder). Hvis Resync_Error_Retry_Delay angis til 0, prøver ikke enheten å resynkronisere på nytt etter et mislykket resynkroniseringsforsøk.

Hvis en oppgradering mislykkes, utføres et nytt forsøk etter Upgrade_Error_Retry_Delay sekunder.

To konfigurerbare parametere er tilgjengelige for betinget utløsing av resynkroniseringer: Resync_Trigger_1 og Resync_Trigger_2. Hver parameter kan programmeres med et betingelsesuttrykk som gjennomgår makroutvidelse. Når resynkroniseringsintervallet utløper (tid for neste resynkronisering), hindrer eventuelle utløsere resynkroniseringen med mindre én eller flere utløsere vurderes som sanne.

Følgende eksempelbetingelse utløser en resynkronisering. I eksemplet har det gått mer enn 5 minutter (300 sekunder) siden det forrige forsøket på oppgradering av telefonen, og minst 10 minutter (600 sekunder) siden det forrige forsøket på resynkronisering.

```
$UPGTMR gt 300 and $PRVTMR ge 600
```

Resynkronisere på et bestemt tidspunkt

Parameteren Resync_At gjør det mulig for telefonen å resynkronisere på et angitt tidspunkt. Denne parameteren bruker 24-timersformat (ttmm) til å angi tidspunktet.

Parameteren Resync_At_Random_Delay gjør det mulig for telefonen å resynkronisere etter en ikke nærmere angitt forsinkelse. Parameteren bruker et positivt heltall til å angi tidspunktet.

Man bør unngå å oversvømme serveren med resynkroniseringsforespørsler fra mange telefoner som er satt til å resynkronisere på det samme tidspunktet. Telefonen unngår dette ved å utløse resynkronisering opptil 10 minutter etter det angitte tidspunktet.

Hvis du for eksempel angir synkroniseringstidspunktet til 1000 (10.00), utløser telefonen resynkronisering når som helst mellom klokken 10.00 og 10.10.

Funksjonen er som standard deaktivert. Hvis parameteren Resync_At blir klargjort, ignoreres parameteren Resync_Periodic.

Konfigurerbare tidsplaner

Du kan konfigurere tidsplaner for regelmessig resynkronisering, og du kan angi omprøvingsintervaller for resynkroniserings- og oppgradingsfeil ved hjelp av disse klargjøringsparametrene:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Hver parameter godtar en enkelt forsinkelsesverdi (sekunder). Den nye utvidede syntaksen tillater en kommadelt liste over påfølgende forsinkelseselementer. Det siste elementet i sekvensen gjentas implisitt i det uendelige.

Du kan dessuten bruke et plusstegn til å angi en annen tallverdi som legger til en tilfeldig ekstra forsinkelse.

Eksempel 1

I dette eksemplet resynkroniserer telefonen regelmessig annenhver time. Hvis det oppstår en resynkroniseringsfeil, prøver enheten på nytt med disse intervallene: 30 minutter, 1 time, 2 timer, 4 timer. Enheten fortsetter å prøve med 4-timers intervaller til resynkroniseringen fullføres.

```
Resync_Periodic=7200
Resync_Error_Retry_Delay=1800,3600,7200,14400
```

Eksempel 2

I dette eksemplet resynkroniserer enheten regelmessig hver time (pluss en ekstra tilfeldig forsinkelse på opptil 10 minutter). Hvis det oppstår en resynkroniseringsfeil, prøver enheten på nytt med disse intervallene: 30 minutter (pluss opptil 5 minutter). 1 time (pluss opptil 10 minutter), 2 timer (pluss opptil 15 minutter). Enheten fortsetter å prøve med 2-timers intervaller (pluss opptil 15 minutter) til resynkroniseringen fullføres.

```
Resync_Periodic=3600+600
Resync_Error_Retry_Delay=1800+300,3600+600,7200+900
```

Eksempel 3

Hvis et forsøk på ekstern oppgradering mislykkes, prøver enheten å oppgradere på nytt etter 30 minutter, deretter på nytt etter nok en time og deretter etter to timer. Hvis oppgraderingen fremdeles mislykkes, forsøker enheten på nytt hver fjerde til femte time helt til oppgraderingen fullføres.

```
Upgrade_Error_Retry_Delay  =  1800,3600,7200,14400+3600
```

Profilregler

Telefonen har flere profilparametre for ekstern konfigurasjon (Profile_Rule*). På denne måten kan hver resynkroniseringsoperasjon hente flere filer administrert av ulike servere.

I det enkleste scenarioet resynkroniserer enheten regelmessig til en enkelt profil på en sentral server som oppdaterer alle relevante interne parametre. Profilen kan eventuelt deles mellom forskjellige filer. Én fil er felles for alle telefonene i en distribusjon. En egen, unik fil gis til hver konto. Krypteringsnøkler og sertifikatinformasjon kan leveres av en annen profil, lagret på en separat server.

Når det er tid for en resynkroniseringsoperasjon, evaluerer telefonen de fire Profile_Rule*-parametrene i rekkefølge:

1. Profile_Rule
2. Profile_Rule_B
3. Profile_Rule_C
4. Profile_Rule_D

Hver evaluering kan føre til at det hentes en profil fra en ekstern klargjøringsserver, med en eventuell oppdatering av noen interne parametre. Hvis en evaluering mislykkes, avbrytes resynkroniseringssekvensen, og den prøves på nytt fra begynnelsen som angitt av parameteren Resync_Error_Retry_Delay (sekunder). Hvis alle evalueringer lykkes, venter enheten på den neste som angitt av parameteren Resync_Periodic og utfører deretter en ny resynkronisering.

Innholdet i hver Profile_Rule*-parameter består av et sett med alternativer. Alternativene er atskilt med tegnet | . Hvert alternativ består av et betingelsesuttrykk, et tilordningsuttrykk, en profil-URL-adresse og eventuelle tilknyttede URL-alternativer. Alle disse komponentene er valgfrie innenfor hvert alternativ. Nedenfor finner du gyldige kombinasjoner og rekkefølgen som de må vises i, hvis de er til stede:

```
[ conditional-expr ] [ assignment-expr ] [[ options ] URL ]
```

Innenfor hver Profile_Rule*-parameter må alle alternativer bortsett fra det siste angi et betingelsesuttrykk. Dette uttrykket evalueres og behandles som følger:

1. Betingelser evalueres fra venstre mot høyre helt til det blir funnet én som vurderes som sann (eller til det blir funnet ett alternativ uten betingelsesuttrykk).
2. Eventuelle medfølgende tilordningsuttrykk evalueres.
3. Hvis en URL-adresse er angitt som en del av dette alternativet, blir det gjort forsøk på å laste ned profilen som ligger på den angitte URL-adressen. Systemet forsøker å oppdatere interne parametrene i samsvar med dette.

Hvis alle alternativer har betingelsesuttrykk og ingen vurderes som sanne (eller hvis hele profilregelen er tom), blir hele Profile_Rule*-parameteren hoppet over. Den neste profilregelparameteren i sekvensen evalueres.

Eksempel 1

Dette eksemplet resynkroniserer uten betingelser til profilen på den angitte URL-adressen og utfører en HTTP GET-forespørsel til den eksterne klargjøringsserveren:

```
http://remote.server.com/cisco/$MA.cfg
```

Eksempel 2

I dette eksemplet resynkroniserer enheten til to ulike URL-adresser, avhengig av registreringstilstanden til linje 1. Ved en mistet registrering utfører enheten en HTTP POST til et CGI-skript. Enheten sender innholdet i den makroutvidede GPP_A, som kan gi ytterligere informasjon om enhetstilstanden:

```
($PRVTMR ge 600)? http://p.tel.com/has-reg.cfg
| [--post a] http://p.tel.com/lost-reg?
```

Eksempel 3

I dette eksemplet resynkroniserer enheten til den samme serveren. Enheten gir mer informasjon hvis det ikke er installert et sertifikat i enheten (for eldre enheter før 2.0):

```
("$CCERT" eq "Installed")? https://p.tel.com/config?
| https://p.tel.com/config?cisco$MAU
```

Eksempel 4

I dette eksemplet deaktiveres linje 1 inntil GPP_A angis lik Provisioned (Klargjort) i den første URL-adressen. Etterpå resynkroniserer den til den andre URL-adressen:

```
("$A" ne "Provisioned")? (Line_Enable_1_ = "No";)! https://p.tel.com/init-prov
| https://p.tel.com/configs
```

Eksempel 5

Dette eksemplet forutsetter at profilen som serveren returnerer, inneholder XML-elementkoder. Disse kodene må tilordnes gyldige parameternavn ved hjelp av aliasmatrisen lagret i GPP_B:

```
[--alias b] https://p.tel.com/account/$PN$MA.xml
```

En resynkronisering regnes vanligvis som mislykket hvis det ikke mottas en forespurt profil fra serveren. Parameteren Resync_Fails_On_FNF kan overstyre denne standardvirkemåten. Hvis Resync_Fails_On_FNF settes til No (Nei), godtar enheten et finner ikke filen-svar fra serveren som en vellykket resynkronisering. Standardverdien for Resync_Fails_On_FNF er Yes (Ja).

Oppgraderingsregel

En oppgraderingsregel gir enheten beskjed om å aktivere en nedlasting og eventuelt hvor lasten skal hentes. Hvis lasten allerede er på enheten, vil den ikke prøve å hente lasten. Lastplasseringens gyldighet spiller derfor ingen rolle når den ønskede lasten befinner seg i den inaktive partisjonen.

Upgrade_Rule angir en fastvarenedlasting som, hvis den er ulik den eksisterende lasten, blir lastet ned og tatt i bruk, med mindre handlingen hindres av et betingelsesuttrykk, eller Upgrade_Enable er satt til **No** (Nei).

Telefonen har én konfigurerbar parameter for ekstern oppgradering, Upgrade_Rule. Parameteren godtar syntaks som er lik syntaksen til profilregelparametrene. URL-alternativer støttes ikke ved oppgraderinger, men betingelsesuttrykk og tilordningsuttrykk kan brukes. Hvis det brukes betingelsesuttrykk, kan parameteren fylles med flere alternativer, atskilt med tegnet |. Syntaksen for hver alternativ er som følger:

```
[ conditional-expr ] [ assignment-expr ] URL
```

Som ved Profile_Rule*-parametre evaluerer Upgrade_Rule-parameteren hvert alternativ inntil et betingelsesuttrykk er oppfylt eller et alternativ ikke har noe betingelsesuttrykk. Eventuelle medfølgende tilordningsuttrykk evalueres. Deretter gjøres det forsøk på å oppgradere med den angitte URL-adressen.

Hvis Upgrade_Rule inneholder en URL-adresse uten et betingelsesuttrykk, oppgraderer enheten til fastvarebildet som URL-adressen angir. Etter makroutvidelse og evaluering av regelen forsøker ikke enheten å oppgradere på nytt før regelen endres eller den effektive kombinasjonen av skjema + server + port + filbane endres.

Ved forsøk på oppgradering av fastvaren deaktiverer enheten lyd ved starten av prosedyren og starter opp på nytt ved slutten av prosedyren. Enheten starter automatisk en oppgradering som drives av innholdet i Upgrade_Rule bare dersom alle talelinjer er inaktive for øyeblikket.

For eksempel:

- For Cisco IP 6800-serien:

  ```
  http://p.tel.com/firmware/sip68xx.11-1-0MPP-BN.loads

  where BN==Build Number
  ```

I dette eksemplet oppgraderer Upgrade_Rule fastvaren til bildet som er lagret på den angitte URL-adressen.

Her er et annet eksempel for Cisco IP Phone 6800-serien:

```
("$F" ne "beta-customer")? http://p.tel.com/firmware/sip68xx.11-0-1MPP-BN.loads
| http://p.tel.com/firmware/sip68xx.11-0-1MPP-BN.loads

where BN==Build Number
```

Dette eksemplet gir enheten beskjed om å laste ned ett av to bilder, basert på innholdet i en generell parameter, GPP_F.

Enheten kan håndheve en nedgraderingsgrense for fastvareversjonsnummer, noe som kan være et nyttig tilpasningsalternativ. Hvis det konfigureres et gyldig fastvareversjonsnummer i parameteren Downgrade_Rev_Limit, forkaster enheten forsøk på oppgraderinger til fastvareversjoner som er eldre enn den angitte grensen.

Datatyper

Disse datatypene brukes med konfigurasjonsprofilparametre:

- {a,b,c,…} – et valg mellom a, b, c, …
- bool – boolsk verdi som enten "ja" eller "nei".
- CadScript – et miniskript som angir kadensparametrene for et signal. Opptil 127 tegn.

  Syntaks: $S_1[;S_2]$, hvor:

  - $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ og er kjent som en seksjon.
  - $on_{i,j}$ og $off_{i,j}$ er på/av-varigheten i sekunder av et *segment*. i = 1 eller 2, og j = 1 til 6.
  - D_i er seksjonens totale varighet i sekunder.

  Alle varigheter kan ha opptil tre desimalplasser for å kunne gi en oppløsning på 1 ms. Jokertegnet "*" betyr ubegrenset varighet. Segmentene i en seksjon spilles av i rekkefølge og gjentas helt til den totale varigheten er avspilt.

  Eksempel 1:

  ```
  60(2/4)

  Number of Cadence Sections = 1
  Cadence Section 1: Section Length = 60 s
  Number of Segments = 1
  Segment 1: On=2s, Off=4s

  Total Ring Length = 60s
  ```

  Eksempel 2 – tydelig ringetone (kort,kort,kort,lang):

  ```
  60(.2/.2,.2/.2,.2/.2,1/4)

  Number of Cadence Sections = 1
  Cadence Section 1: Section Length = 60s
  Number of Segments = 4
  Segment 1: On=0.2s, Off=0.2s
  Segment 2: On=0.2s, Off=0.2s
  Segment 3: On=0.2s, Off=0.2s
  Segment 4: On=1.0s, Off=4.0s

  Total Ring Length = 60s
  ```

- DialPlanScript – skriptsyntaks som brukes til å angi oppringingsplaner for linje 1 og linje 2.
- Float<n> – en flyttallsverdi med opptil n desimalplasser.
- FQDN – fullstendig kvalifisert domenenavn. Kan inneholde opptil 63 tegn. Eksempler:
  - sip.Cisco.com:5060 eller 109.12.14.12:12345
  - sip.Cisco.com eller 109.12.14.12

- FreqScript – et miniscript som spesifiserer frekvens- og nivåparametrene for en tone. Inneholder opptil 127 tegn.

  Syntaks: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, hvor:

  - F_1–F_6 er frekvens i Hz (bare usignerte heltall).
  - L_1–L_6 er tilsvarende nivåer i dBm (med opptil én desimalplass).

  Mellomrom før og etter komma er tillatt, men anbefales ikke.

  Eksempel 1 – samtale venter-tone:

  ```
  440@-10

  Number of Frequencies = 1
  Frequency 1 = 440 Hz at -10 dBm
  ```

  Eksempel 2 – summetone:

  ```
  350@-19,440@-19

  Number of Frequencies = 2
  Frequency 1 = 350 Hz at -19 dBm
  Frequency 2 = 440 Hz at -19 dBm
  ```

- IP – gyldig IPv4-adresse i skjemaet x.x.x.x, hvor x er mellom 0 og 255. Eksempel: 10.1.2.100.
- UserID – bruker-ID slik den vises i en URL-adresse; opptil 63 tegn.
- Phone – en telefonnummerstreng, for eksempel 14081234567, *69, *72, 345678; eller en generell URL-adresse, for eksempel 1234@10.10.10.100:5068 eller jsmith@Cisco.com. Strengen kan inneholde opptil 39 tegn.
- PhTmplt – en telefonnummermal. Hver mal kan inneholde ett eller flere mønstre som er atskilt med komma (,). Mellomrom ved begynnelsen av hvert mønster ignoreres. "?" og "*" representerer jokertegn. Bruk %xx til å representere litterale tegn. %2a representerer for eksempel *. Malen kan inneholde opptil 39 tegn. Eksempler: "1408*, 1510*", "1408123????, 555?1.".
- Port – TCP/UDP-portnummeret (0-65535). Kan angis i desimalt eller heksadesimalt format.
- ProvisioningRuleSyntax – skriptsyntaks som brukes til å definere regler for resynkronisering av konfigurasjoner og oppgradering av fastvare.
- PwrLevel – effekt uttrykt i dBm med én desimalplass, for eksempel –13,5 eller 1,5 (dBm).
- RscTmplt – en mal for SIP-svarstatuskode, som "404, 5*", "61?", "407, 408, 487, 481". Kan inneholde opptil 39 tegn.
- Sig<n> – n-biters verdi med fortegn. Kan angis i desimalt eller heksadesimalt format. Et "-"-tegn må stå foran negative verdier. Et + foran positive verdier er valgfritt.
- Stjernekoder – aktiveringskode for en tilleggstjeneste, som for eksempel *69. Koden kan inneholde opptil 7 tegn.
- Str<n> – en generell streng med opptil n ureserverte tegn.
- Time<n> – varighet i sekunder, med opptil n desimalplasser. Ekstra desimaler som angis, ignoreres.

- ToneScript – et miniscript som angir frekvens-, nivå- og kadensparametre for samtale pågår-tone. Skript kan inneholde opptil 127 tegn.

  Syntaks: FreqScript;Z_1[;Z_2].

  Seksjonen Z_1 ligner seksjonen S_1 i et CadScript, bortsett fra at hvert på/av-segment etterfølges av en frekvenskomponentparameter: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$ hvor:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ angir frekvenskomponentene i FreqScript som brukes i det segmentet.

  Hvis det brukes mer enn én frekvenskomponent i et segment, summeres komponentene.

  Eksempel 1 – summetone:

  ```
  350@-19,440@-19;10(*/0/1+2)

  Number of Frequencies = 2
  Frequency 1 = 350 Hz at -19 dBm
  Frequency 2 = 440 Hz at -19 dBm
  Number of Cadence Sections = 1
  Cadence Section 1: Section Length = 10 s
  Number of Segments = 1
  Segment 1: On=forever, with Frequencies 1 and 2

  Total Tone Length = 10s
  ```

  Eksempel 2 – opptattone:

  ```
  350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)

  Number of Frequencies = 2
  Frequency 1 = 350 Hz at -19 dBm
  Frequency 2 = 440 Hz at -19 dBm
  Number of Cadence Sections = 2
  Cadence Section 1: Section Length = 2s
  Number of Segments = 1
  Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
  Cadence Section 2: Section Length = 10s
  Number of Segments = 1
  Segment 1: On=forever, with Frequencies 1 and 2

  Total Tone Length = 12s
  ```

- Uns<n> – n-biters verdi med fortegn, hvor n = 8, 16 eller 32. Kan angis i desimalt eller heksadesimalt format, for eksempel 12 eller 0x18, så lenge verdien ligger innenfor n biter.

Merk Husk dette:

- <Par Name> representerer et navn på en konfigurasjonsparameter. I en profil dannes den tilsvarende koden ved at mellomrommet erstattes med et understrekingstegn "_", som for eksempel **Par_Name**.
- Et tomt standardverdifelt innebærer at strengen er tom < "" >.
- Telefonen fortsetter å bruke de sist konfigurerte verdiene for koder som mangler i en gitt profil.
- Maler sammenlignes i angitt rekkefølge. Det første, *ikke det nærmeste*, treffet velges. Parameternavnet må samsvare nøyaktig.
- Hvis det gis mer enn én definisjon for en parameter i en profil, er det den siste definisjonen i filen som blir tatt i bruk i telefonen.
- En parameterspesifikasjon med en tom parameterverdi tvinger parameteren tilbake til standardverdien. Hvis du vil angi en tom streng i stedet, kan du bruke den tomme strengen "" som parameterverdi.

Profiloppdateringer og fastvareoppgraderinger

Telefonen støtter sikker ekstern klargjøring (konfigurasjon) og fastvareoppgraderinger. En uklargjort telefon kan motta en kryptert profil som er beregnet på den enheten. En sikker metode for førstegangsklargjøring som bruker SSL-funksjonalitet, gjør at telefonen ikke krever eksplisitt nøkkel.

Brukermedvirkning er ikke nødvendig for å starte eller fullføre en profiloppdatering, en fastvareoppgradering eller hvis det kreves mellomliggende oppgraderinger for å nå en fremtidig oppgraderingstilstand fra en eldre versjon. Det gjøres bare forsøk på resynkronisering av profiler når telefonen er inaktiv, fordi en resynkronisering kan utløse en programvareomstart og koble fra en samtale.

Generelle parametre administrerer klargjøringsprosessen. Hver telefon kan konfigureres til å kontakte en normal klargjøringsserver (NPS) regelmessig. Kommunikasjon med NPS krever ikke bruk av sikre protokoller fordi den oppdaterte profilen krypteres med en delt hemmelig nøkkel. NPS kan være en standard TFTP-, HTTP- eller HTTPS-server med klientsertifikater.

Administratoren kan oppgradere, starte opp på nytt (reboot), starte på nytt (restart) eller resynkronisere telefoner ved hjelp av telefonens nettbrukergrensesnitt. Administratoren kan også utføre disse oppgavene ved hjelp av en SIP-varslingsmelding.

Konfigurasjonsprofiler genereres ved hjelp av vanlige verktøy med åpen kildekode som integreres med tjenesteleverandørens klargjøringssystemer.

Beslektede emner

Tillate og konfigurere profiloppdateringer, på side 34

Tillate og konfigurere profiloppdateringer

Profiloppdateringer kan utføres ved bestemte intervaller. Oppdaterte profiler sendes fra en server til telefonen ved hjelp av TFTP, HTTP eller HTTPS.

Før du begynner

Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Prosedyre

Trinn 1 Velg **Voice (Tale)** > **Provisioning (Klargjøring)**.

Trinn 2 I delen **Configuration Profile** (Konfigurasjonsprofil) velger du **Yes** (Ja) i rullegardinlisten **Provision Enable** (Aktiver klargjøring).

Trinn 3 Skriv inn parametrene.

Trinn 4 Klikk på **Godta alle endringer**.

Beslektede emner

Profiloppdateringer og fastvareoppgraderinger, på side 34

Tillate og konfigurere fastvareoppgraderinger

Fastvareoppdateringer kan utføres ved bestemte intervaller. Oppdatert fastvare sendes fra en server til telefonen ved hjelp av TFTP eller HTTP. Sikkerheten har mindre betydning ved en fastvareoppgradering fordi fastvaren ikke inneholder personlig informasjon.

Før du begynner

Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Prosedyre

Trinn 1 Velg **Tale** > **Klargjøring**.

Trinn 2 I delen **Fastvareoppgradering** velger du **Ja** i rullegardinlisten **Aktiver oppgradering**.

Trinn 3 Skriv inn parametrene.

Trinn 4 Klikk på **Godta alle endringer**.

Oppgradere fastvare via TFTP, HTTP eller HTTPS

Telefonen støtter enkle ettbildesoppgraderinger via TFTP, HTTP eller HTTPS.

Merk Nedgradering til tidligere versjoner er kanskje ikke mulig for alle enheter. Du finner mer informasjon under produktmerknadene for telefonen og fastvareversjonen din.

Før du begynner

Innlastingsfilen for fastvaren må lastes ned til en tilgjengelig server.

Prosedyre

Trinn 1 Gi bildet nytt navn på denne måten:

`cp-x8xx-sip.aa-b-cMPP.cop` til **`cp-x8xx-sip.aa-b-cMPP.tar.gz`**

hvor:

`x8xx` er telefonserien, for eksempel 6841.

`aa-b-c` er versjonsnummeret, for eksempel 10-4-1

Trinn 2 Bruk kommandoen **`tar -xzvf`** til å pakke opp tar-pakken.

Trinn 3 Kopier mappen til en nedlastingskatalog for TFTP, HTTP eller HTTPS.

Trinn 4 Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Trinn 5 Velg **Voice (Tale)** > **Provisioning (Klargjøring)**.

Trinn 6 Finn innlastingsfilens filnavn, som ender på **.loads**, og føy det til den gyldige URL-adressen.

Trinn 7 Klikk på **Godta alle endringer**.

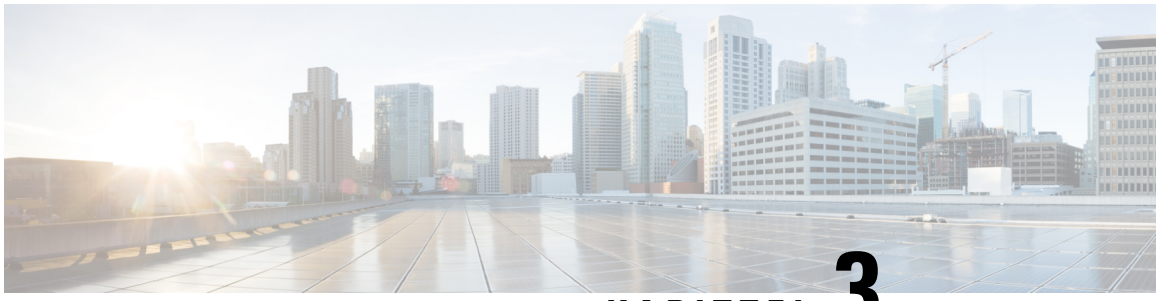
Oppgradere fastvare med en kommando i nettleseren

Fastvaren på en telefon kan oppgraderes ved hjelp av en oppgraderingskommando skrevet på nettleserens adresselinje. Telefonen oppdateres bare når den er ledig. Det gjøres automatisk forsøk på oppdatering etter at samtalen er fullført.

Prosedyre

Du kan oppgradere telefonen med en URL-adresse i en nettleser ved å skrive inn denne kommandoen:

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```



KAPITTEL 3

Intern forhåndsklargjøring og klargjøringsservere

Intern forhåndsklargjøring og klargjøringsservere

Tjenesteleverandøren forhåndsklargjør telefoner, med unntak av RC-enheter, med en profil. Forhåndsklargjøringsprofilen kan omfatte et begrenset sett med parametre som resynkroniserer telefonen. Profilen kan også omfatte et fullstendig sett av parametre som leveres av den eksterne serveren. Som standard resynkroniserer telefonen ved oppstart og ved intervaller konfigurert i profilen. Når brukeren kobler til telefonen i kundens lokaler, laster enheten ned den oppdaterte profilen og eventuelle fastvareoppdateringer.

Denne prosessen med forhåndsklargjøring, distribusjon og ekstern klargjøring kan utføres på mange måter.

Serverforberedelse og programvareverktøy

Eksemplene i dette kapitlet krever at én eller flere servere er tilgjengelige. Serverne kan være installert og kjøre på en lokal datamaskin:

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

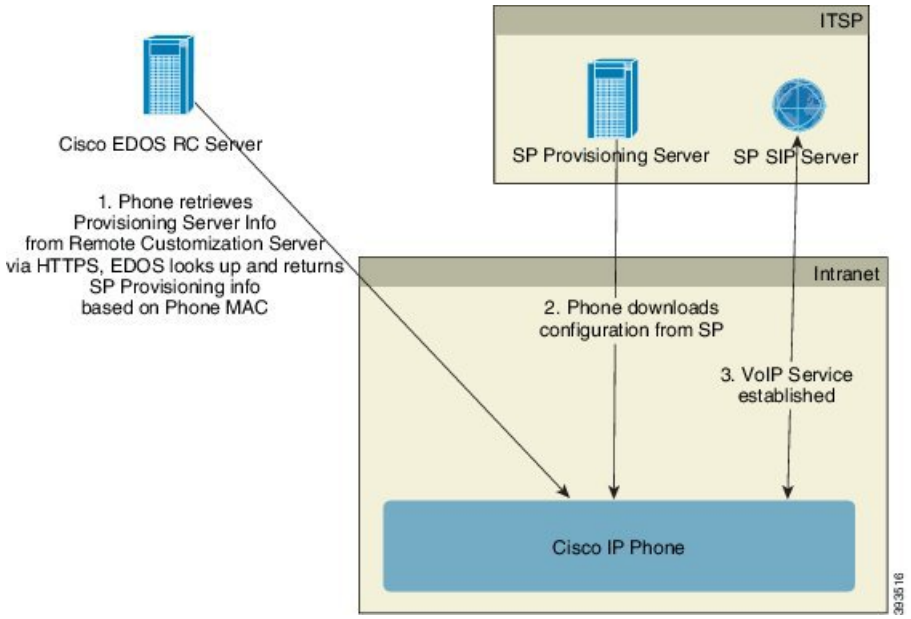
Når man skal feilsøke serverkonfigurasjonen, kan det være nyttig å installere klienter for hver type server på en separat servermaskin. Denne fremgangsmåten etablerer riktig serverdrift, uavhengig av samhandlingen med telefonene.

Vi anbefaler også at du installerer disse programvareverktøyene:

- Installer gzip-komprimeringsverktøyet med åpen kildekode, slik at du kan generere konfigurasjonsprofiler.
- Til profilkryptering og HTTPS-operasjoner installerer du OpenSSL-programvarepakken med åpen kildekode.

- Til å teste dynamisk generering av profiler og ett-trinns ekstern klargjøring ved hjelp av HTTPS anbefaler vi et skriptspråk som har støtte for CGI-skripting. Perl-språkverktøy med åpen kildekode er eksempler på et slikt skriptspråk.
- Hvis du vil bekrefte sikker utveksling mellom klargjøringsservere og telefoner, kan du installere en Ethernet-pakkesniffer (som fritt nedlastbare Ethereal/Wireshark). Registrer en Ethernet-pakkesporing av samhandlingen mellom telefonen og klargjøringsserveren. Dette gjør du ved å kjøre pakkesnifferen på en datamaskin som er koblet til en svitsj med portspeiling aktivert. Til HTTPS-transaksjoner kan du bruke ssldump-verktøyet.

Distribusjon gjennom ekstern tilpasning (RC)



Alle telefoner kontakter Cisco EDOS RC-serveren helt til de blir klargjort første gang.

I en RC-distribusjonsmodell kjøper kunden en telefon som allerede har blitt knyttet til en bestemt tjenesteleverandør i Cisco EDOS RC Server. Leverandøren av Internett-telefoni (ITSP) konfigurerer og vedlikeholder en klargjøringsserver, og registrerer klargjøringsserverinformasjonen deres med Cisco EDOS RC Server.

Når telefonen slås på med Internett-tilkobling, er tilpasningstilstanden for den uklargjorte telefonen **Open** (Åpen). Telefonen spør først den lokale DHCP-serveren om klargjøringsserverinformasjon og angir telefonens tilpasningstilstand. Hvis DHCP-spørringen er vellykket, angis tilpasningstilstanden til **Aborted** (avbrutt), og det gjøres ikke forsøk på ekstern tilpasning (RC) fordi DHCP gir den klargjøringsserverinformasjonen som er nødvendig.

Hvis det ikke finnes noen konfigurasjon av DHCP-oppsett når en telefon kobler til et nettverk for første gang eller etter tilbakestilling til fabrikkinnstillinger, kontaktes en enhetsaktiveringsserver for nullberøringsklargjøring. Nye telefoner bruker “activate.cisco.com” i stedet for “webapps.cisco.com” for klargjøring. Telefoner med fastvareversjon før 11.2 (1), vil fortsette å bruke webapps.cisco.com. Cisco anbefaler at du tillater begge domenenavn gjennom brannmuren.

Hvis DHCP-serveren ikke gir klargjøringsserverinformasjon, spør telefonen Cisco EDOS RC Server og oppgir sin MAC-adresse og modell, og tilpasningstilstanden settes til **Pending** (Ventende). Cisco EDOS-serveren

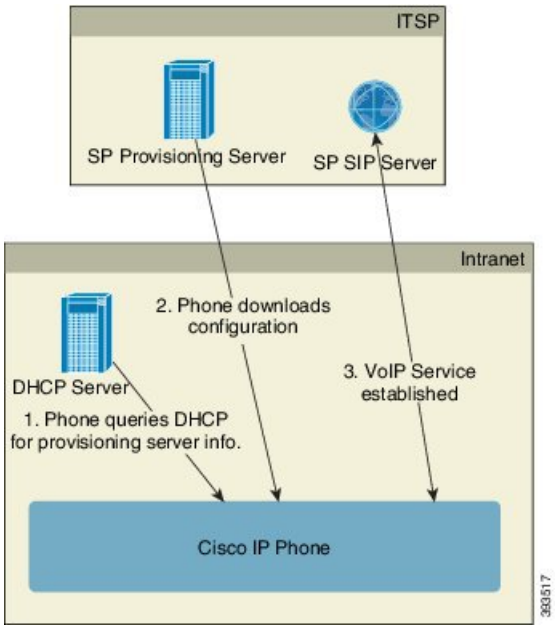
svarer med den tilhørende tjenesteleverandørens klargjøringsserverinformasjon, inkludert URL-adressen til klargjøringsserveren, og telefonens tilpasningstilstand angis til **Custom Pending** (Ventende tilpasning). Telefonen utfører deretter en ny resynkroniserings-URL-kommando for å hente tjenesteleverandørens konfigurasjon, og dersom dette lykkes, angis tilpasningstilstanden til **Acquired** (Lastet inn).

Hvis Cisco EDOS RC-serveren ikke har en tjenesteleverandør som er knyttet til telefonen, angis telefonens tilpasningstilstand til **Unavailable** (Utilgjengelig). Telefonen kan konfigureres manuelt, eller det kan legges til en tilknytning for tjenesteleverandøren til telefonen til Cisco EDOS-serveren.

Hvis en telefon klargjøres via LCD- eller nettkonfigurasjonsverktøyet før tilpasningstilstanden blir **Acquired** (Lastet inn), angis tilpasningstilstanden til **Aborted** (Avbrutt), og Cisco EDOS-serveren blir ikke spurt med mindre telefonen tilbakestilles til fabrikkinnstillinger.

Når telefonen har blitt klargjort, brukes ikke Cisco EDOS RC-serveren med mindre telefonen tilbakestilles til fabrikkinnstillinger.

Intern forhåndsklargjøring av enheter



Med Ciscos standardkonfigurasjon forsøker telefonen automatisk å resynkronisere til en profil på en TFTP-server. En administrert DHCP-server på et lokalnett gir informasjon til enheten om profilen og TFTP-serveren som er konfigurert for forhåndsklargjøring. Tjenesteleverandøren kobler alle nye telefoner til lokalnettet. Telefonen resynkroniserer automatisk til den lokale TFTP-serveren og initialiserer sin interne tilstand som forberedelse til distribusjon. Denne forhåndsklargjøringsprofilen inneholder normalt URL-adressen til en ekstern klargjøringsserver. Klargjøringsserveren holder enheten oppdatert når enheten har blitt distribuert og koblet til kundenettverket.

Strekkoden på den forhåndsklargjorte enheten kan skannes for å registrere dens MAC-adresse eller serienummer før telefonen sendes til kunden. Denne informasjonen kan brukes til å opprette profilen som telefonen resynkroniserer til.

Etter å ha mottatt telefonen kobler kunden den til en bredbåndskobling. Ved oppstart kontakter telefonen klargjøringsserveren via URL-adressen som konfigureres under forhåndsklargjøringen. Telefonen kan dermed resynkronisere og oppdatere profilen og fastvaren når det er behov for det.

Beslektede emner

Distribusjon via forhandler, på side 5
Klargjøring via TFTP, på side 40

Konfigurasjon av klargjøringsserver

Denne delen beskriver konfigurasjonskrav når telefoner skal klargjøres ved hjelp av forskjellige servere og scenarioer. Med tanke på dette dokumentet og testing installeres og kjøres klargjøringsservere på en lokal PC. I tillegg er allment tilgjengelige programvareverktøy nyttige når telefoner skal klargjøres.

Klargjøring via TFTP

Telefonen støtter TFTP for klargjøring av så vel resynkronisering som oppgradering av fastvare. Når enheter distribueres eksternt, anbefales HTTPS, men HTTP og TFTP kan også brukes. Dette krever i sin tur at klargjøringsfilen krypteres for å øke sikkerheten, da dette gir større pålitelighet med tanke på NAT og beskyttelsesmekanismene for rutere. TFTP kan være nyttig ved intern forhåndsklargjøring av mange uklargjorte enheter.

Telefonen kan hente IP-adresse for TFTP-serveren direkte fra DHCP-serveren via DHCP-alternativ 66. Hvis en Profile_Rule er konfigurert med filbanen for den TFTP-serveren, laster enheten ned profilen sin fra TFTP-serveren. Nedlastingen skjer når enheten er koblet til et lokalnett og påslått.

Profile_Rule-parameteren som følger med standardkonfigurasjonen fra fabrikken, er *&PN*.cfg, hvor *&PN* representerer telefonens modellnavn.

For en CP-6841-3PCC er for eksempel filnavnet CP-6841-3PCC.cfg.

Ved oppstart resynkroniserer en enhet ned standardprofilen fra fabrikken med denne filen på den lokale TFTP-serveren som angis av DHCP-alternativ 66. Filbanen viser til den virtuelle rotkatalogen på TFTP-serveren.

Beslektede emner

Intern forhåndsklargjøring av enheter, på side 39

Ekstern endepunktkontroll og NAT

Telefonen er kompatibel med oversettelse av nettverksadresser (NAT), slik at den kan få tilgang til Internett via en ruter. For å øke sikkerheten kan ruteren forsøke å blokkere uautoriserte innkommende pakker ved å implementere symmetrisk NAT, en pakkefiltreringsstrategi som sterkt begrenser hvilke pakker som skal få lov til å komme inn i det beskyttede nettverket fra Internett. Ekstern klargjøring gjennom TFTP anbefales derfor ikke.

VoIP kan fungere med NAT bare når det gis en form for NAT-gjennomgang. Konfigurere enkel gjennomgang av UDP via NAT (STUN). Dette alternativet krever at brukeren har:

- en dynamisk ekstern (offentlig) IP-adresse fra tjenesten
- en datamaskin som kjører STUN-serverprogramvare
- en grenseenhet med en asymmetrisk NAT-mekanisme

Klargjøring via HTTP

Telefonen fungerer som en nettleser som ber om nettsider fra et eksternt Internett-nettsted. Dette gir en pålitelig måte å nå klargjøringsserveren på, selv når en kunderuter implementerer symmetrisk NAT eller andre beskyttelsesmekanismer. HTTP og HTTPS fungerer mer pålitelig enn TFTP ved eksterne distribusjoner, særlig når de distribuerte enhetene er tilkoblet bak private brannmurer eller NAT-aktiverte rutere. HTTP og HTTPs brukes om hverandre ved følgende forespørselstypebeskrivelser.

Grunnleggende HTTP-basert klargjøring er avhengig av HTTP GET-metoden for å hente konfigurasjonsprofiler. Vanligvis opprettes det en konfigurasjonsfil for hver distribuerte telefon, og disse filene lagres i en katalog på HTTP-serveren. Når serveren mottar GET-forespørselen, returnerer den ganske enkelt filen som er angitt i GET-forespørselshodet.

I motsetning til en statisk profil kan konfigurasjonsprofilen genereres dynamisk ved å sende forespørsel til en kundedatabase og lage profilen i farten.

Når telefonen ber om en resynkronisering, kan den bruke HTTP POST-metoden til å be om konfigurasjonsdataene for resynkronisering. Enheten kan konfigureres til å formidle visse status- og identifikasjonsopplysninger til serveren i teksten i HTTP POST-forespørselen. Serveren bruker disse opplysningene til å generere en ønsket konfigurasjonsprofil som svar, eller til å lagre statusinformasjonen for senere analyse og sporing.

Som en del av både GET og POST-forespørsler inkluderer telefonen automatisk grunnleggende ID-informasjon i feltet User-Agent (Bruker-agent) i forespørselshodet. Denne informasjonen beskriver produsent, produktnavn, gjeldende fastvareversjon og produktserienummer for enheten.

Følgende eksempel er User-Agent-forespørselsfeltet fra en CP-6841-3PCC:

```
User-Agent: Cisco-CP-6841-3PCC/11.0 (00562b043615)
```

Når telefonen konfigureres til å resynkronisere til en konfigurasjonsprofil ved hjelp av HTTP, anbefales bruk av HTTPS eller at profilen krypteres, for å beskytte konfidensiell informasjon. Krypterte profiler som telefonen laster ned ved hjelp av HTTP, hindrer eksponering av konfidensiell informasjon som finnes i konfigurasjonsprofilen. Denne resynkroniseringsmodusen gir lavere databehandlingsbelastning på klargjøringsserveren sammenlignet med bruk av HTTPS.

Telefonen kan dekryptere profiler som er kryptert med en av følgende krypteringsmetoder:

- AES-256-CBC-kryptering
- RFC 8188-basert kryptering med AES-128-GCM-kryptering

Merk Telefonene støtter HTTP versjon 1.0, HTTP versjon 1.1 og chunk-koding når HTTP versjon 1.1 er forhandlet transportprotokoll.

Håndtering av HTTP-statuskode ved resynkronisering og oppgradering

Telefonen støtter HTTP-svar for ekstern klargjøring (resynkronisering). Telefonens gjeldende virkemåte klassifiseres i tre kategorier:

- A – vellykket, der verdiene "Resync Periodic" (resynkroniser regelmessig) og "Resync Random Delay" (Resynkroniser med tilfeldig forsinkelse" styrer etterfølgende forespørsler.

- B – mislykket, når filen ikke blir funnet, eller profilen er skadet. Verdien "Resync Error Retry Delay" (Resynkroniseringsfeil – forsinkelse før nytt forsøk) styrer etterfølgende forespørsler.
- C – andre feil, når en ugyldig URL-adresse eller IP-adresse fører til en tilkoblingsfeil. Verdien "Resync Error Retry Delay" (Resynkroniseringsfeil – forsinkelse før nytt forsøk) styrer etterfølgende forespørsler.

Tabell 2: Telefonens virkemåte ved HTTP-svar

HTTP-statuskode	Beskrivelse	Telefonens virkemåte
301 Moved Permanently	Denne og fremtidige forespørsler bør rettes mot en ny plassering.	Prøv forespørsel på nytt umiddelbart med ny plassering.
302 Found	Kjent som "midlertidig flyttet".	Prøv forespørsel på nytt umiddelbart med ny plassering.
3xx	Andre 3xx-svar blir ikke behandlet.	C
400 Bad Request	Forespørselen kan ikke oppfylles på grunn av ugyldig syntaks.	C
401 Unauthorized	Utfordring knyttet til grunnleggende (basic) eller sammensatt (digest) tilgangsgodkjenning.	Prøv forespørsel på nytt med godkjenningslegitimasjon umiddelbart. Maksimalt 2 forsøk. Hvis dette mislykkes, er telefonens virkemåte C.
403 Forbidden	Serveren nekter å svare.	C
404 Not Found	Finner ikke den forespurte ressursen. Etterfølgende forespørsler fra klient er tillatt.	B
407 Proxy Authentication Required	Utfordring knyttet til grunnleggende (basic) eller sammensatt (digest) tilgangsgodkjenning.	Prøv forespørsel på nytt med godkjenningslegitimasjon umiddelbart. Maksimalt to forsøk. Hvis dette mislykkes, er telefonens virkemåte C.
4xx	Andre statuskoder knyttet til klientfeil behandles ikke.	C
500 Internal Server Error	Generisk feilmelding.	Telefonens virkemåte er C.
501 Not Implemented	Serveren gjenkjenner ikke forespørselsmetoden, eller den har ikke mulighet til å oppfylle forespørselen.	Telefonens virkemåte er C.
502 Bad Gateway	Serveren fungerer som en gateway eller proxy og mottar et ugyldig svar fra en overordnet server.	Telefonens virkemåte er C.

HTTP-statuskode	Beskrivelse	Telefonens virkemåte
503 Service Unavailable	Serveren er for øyeblikket ikke tilgjengelig (overbelastet eller nede for vedlikehold). Dette er en midlertidig tilstand.	Telefonens virkemåte er C.
504 Gateway Timeout	Serveren opptrer som en gateway eller proxy og mottar ikke et rettidig svar fra en overordnet server.	C
5xx	Andre serverfeil	C

Klargjøring via HTTPS

Telefonen støtter klargjøring med HTTPS, som gir økt sikkerhet ved administrasjon av eksternt distribuerte enheter. Hver telefon har et unikt SLL-klientsertifikat (og tilhørende privat nøkkel), i tillegg til rotsertifikatet en Sipura CA serverrotsertifikat. Sistnevnte gjør det mulig for telefonen å gjenkjenne godkjente klargjøringsservere og avvise servere som ikke er godkjent. På den annen side gjør klientsertifikatet det mulig for klargjøringsserveren å identifisere de enkelte enhetene som sender forespørselen.

Når tjenesteleverandører skal håndtere distribusjon ved hjelp av HTTPS, må det genereres et serversertifikatet for hver klargjøringsserver som en telefon resynkroniserer med via HTTPS. Serversertifikatet må være signert med Ciscos Server CA-rotnøkkelen, og dette sertifikatet er på alle distribuerte enheter. For å få et signert serversertifikatet må tjenesteleverandøren videresende en sertifikatsigneringsforespørsel til Cisco, som signerer og returnerer serversertifikatet for installasjonen på klargjøringsserveren.

Klargjøringsserversertifikatet må inneholde feltet Vanlig navn (Common Name – CN), og FQDN-et til verten som kjører på serveren i emnet. Det kan eventuelt inneholde informasjon etter vertens FQDN, atskilt med skråstrek (/). Følgende eksempler er CN-oppføringer som godtas som gyldige av telefonen:

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

I tillegg til å verifisere serversertifikatet tester telefonen serverens IP-adresse mot et DNS-oppslag av servernavnet som er angitt i serversertifikatet.

Skaffe signerte serversertifikater

OpenSSL-verktøyet kan generere sertifikatsigneringsforespørsler. Følgende eksempel viser **`openssl`**-kommandoen som gir et 1024-biters offentlig/privat RSA-nøkkelpar og en sertifikatsigneringsforespørsel:

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

Kommandoen genererer den private nøkkelen for serveren i **`privkey.pem`** og en tilsvarende sertifikatsigneringsforespørsel i **`provserver.csr`**. Tjenesteleverandøren holder **`privkey.pem`** hemmelig og sender **`provserver.csr`** til Cisco for signering. Når Cisco mottar **`provserver.csr`**-filen, genererer Cisco **`provserver.crt`**, det signerte serversertifikatet.

Prosedyre

Trinn 1 Naviger til https://software.cisco.com/software/edos/home, og logg på med CCO-påloggingsopplysningene din.

Merk Hvis det ikke finnes noen konfigurasjon av DHCP-oppsett når en telefon kobler til et nettverk for første gang eller etter tilbakestilling til fabrikkinnstillinger, kontaktes en enhetsaktiveringsserver for nullberøringsklargjøring. Nye telefoner bruker "activate.cisco.com" i stedet for "webapps.cisco.com" til klargjøring. Telefoner med fastvareversjon før 11.2(1) fortsetter å bruke "webapps.cisco.com". Vi anbefaler at du tillater begge domenenavn gjennom brannmuren.

Trinn 2 Velg **Certificate Management** (Sertifikatbehandling).

I fanen **Sign CSR** (Signer sertifikatsigneringsforespørsel) lastes CSR-en i det forrige trinnet opp for signering.

Trinn 3 Fra rullegardinlisten **Select Product** (Velg produkt) velger du **SPA1xx firmware 1.3.3 and newer/SPA232D firmware 1.3.3 and newer/SPA5xx firmware 7.5.6 and newer/CP-78xx-3PCC/CP-88xx-3PCC**.

Merk Dette produktet inkluderer Cisco IP Phone 6800-serien av telefoner for flere plattformer.

Trinn 4 I **CSR File**-feltet (CSR-fil) klikker du **Browse** (Bla gjennom) og velger CSR-en som skal signeres.

Trinn 5 Velg krypteringsmetode:

- MD5
- SHA1
- SHA256

Cisco anbefaler at du velger SHA256-kryptering.

Trinn 6 I rullegardinlisten **Sign in Duration** (Påloggingsvarighet) velger du den aktuelle varigheten (for eksempel 1 år).

Trinn 7 Klikk **Sign Certificate Request** (Signer sertifikatforespørsel).

Trinn 8 Velg ett av følgende alternativer for å motta det signerte sertifikatet:

- **Skriv inn mottakerens e-postadresse** – Hvis du ønsker å motta sertifikatet via e-post, angir du e-postadressen i dette feltet.
- **Download** (Last ned): Velg dette alternativet hvis du vil laste ned det signerte sertifikatet.

Trinn 9 Klikk på **Bekreft**.

Det signerte serversertifikatet sendes med e-post til e-postadressen som er oppgitt, eller det blir lastet ned.

CA-klientrotsertifikat for telefoner for flere plattformer

Cisco tilbyr i tillegg tjenesteleverandører et klientrotsertifikat for telefoner for flere plattformer. Dette rotsertifikatet bekrefter autentisiteten til klientsertifikatet som er på hver telefon. Telefonene for flere plattformer støtter også sertifikater signert av tredjeparter, som de fra Verisign, Cybertrust og så videre.

Det unike klientsertifikatet som hver enhet tilbyr i løpet av en HTTPS-økt, inneholder identifiseringsinformasjon innebygd i emnefeltet sitt. Denne informasjonen kan gjøres tilgjengelig av HTTPS-serveren for et CGI-skript som aktiveres for å håndtere sikre forespørsler. Sertifikatemnet angir spesielt enhetens produktnavn (OU-element), MAC-adresse (S-element), og serienummer (L-element).

Følgende eksempel fra emnefeltet i klientsertifikatene til Cisco IP Phone 6841 telefoner for flere plattformer viser disse elementene:

```
OU=CP-6841-3PCC, L=88012BA01234, S=000e08abcdef
```

Bruk klargjøringsmakrovariabelen $CCERT til å bestemme om en telefon har et individualisert sertifikat. Variabelverdien utvides til enten Installed (Installert) eller Not Installed (Ikke installert), avhengig av om det er et unikt klientsertifikat på telefonen. Ved generiske sertifikater er det mulig å hente enhetens serienummer fra HTTP-forespørselshodet i feltet User-Agent (Bruker-agent).

HTTPS-servere kan konfigureres til å be om SSL-sertifikater fra påkoblende klienter. Hvis dette er aktivert, kan serveren bruke klientrotsertifikatet for telefoner for flere plattformer levert av Cisco til å verifisere klientsertifikatet. Serveren kan deretter gi sertifikatinformasjonen til en CGI for videre behandling.

Plasseringen for sertifikatlagring kan variere. I en Apache-installasjon er for eksempel filbanene for lagring av serversignerte klargjøringssertifikater, tilhørende private nøkler og CA-klientrotsertifikatet for telefoner for flere plattformer som følger:

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

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

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

Du finner mer detaljerte opplysninger i dokumentasjonen for HTTPS-serveren.

Cisco rotinstans for klientsertifikat signerer hvert unike sertifikat. Det tilhørende rotsertifikatet gjøres tilgjengelig for tjenesteleverandørene til klientgodkjenningsformål.

Redundante klargjøringsservere

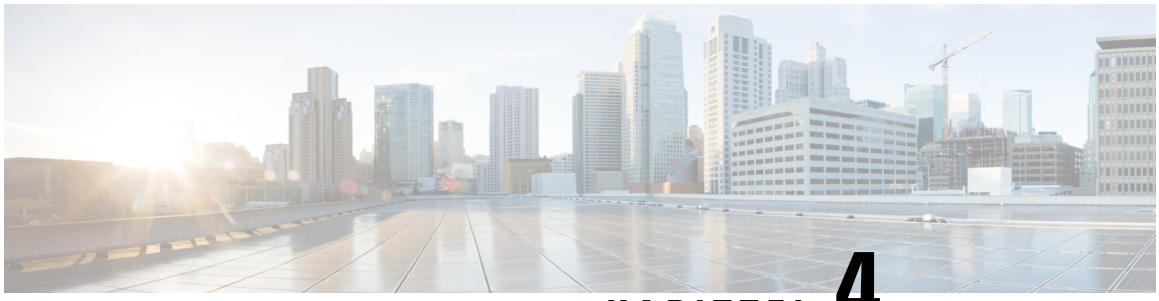
Klargjøringsservere kan angis som en IP-adresse eller som et fullstendig kvalifisert domenenavn (FQDN). Bruk av FQDN legger til rette for distribusjon av redundante klargjøringsservere. Når klargjøringsserveren identifiseres gjennom et FQDN, forsøker telefonen å løse FQDN-et til en IP-adresse gjennom DNS. Bare DNS A-poster støttes for klargjøring; DNS SRV-adresseoppløsning er ikke tilgjengelig for klargjøring. Telefonen fortsetter å behandle A-poster helt til en server svarer. Hvis ingen servere knyttet til A-postene svarer, logger telefonen en feil på syslog-serveren.

Syslog-server

Hvis det er konfigurert en syslog-server på telefonen gjennom <Syslog Server>-parametrene, sender resynkroniserings- og oppgraderingsoperasjonene meldinger til syslog-serveren. Det kan bli generert en melding ved starten av en ekstern filforespørsel (konfigurasjonsprofil eller fastvarelast) og når operasjonen avsluttes (angir om den har lykkes eller ei).

Loggførte meldinger konfigureres i følgende parametre og makroutvides til faktiske syslog-meldinger:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



KAPITTEL 4

Eksempler på klargjøring

Oversikt over eksempler på klargjøring

Dette kapitlet gir eksempelprosedyrer for overføring av konfigurasjonsprofiler mellom telefoner og klargjøringsservere.

Du finner informasjon om hvordan du oppretter konfigurasjonsprofiler, under Klargjøringsskript, på side 13.

Grunnleggende resynkronisering

Denne delen beskriver de grunnleggende resynkroniseringsfunksjonene i telefonene.

Resynkronisering via TFTP

Telefonen støtter flere nettverksprotokoller for henting av konfigurasjonsprofiler. Den mest grunnleggende profiloverføringsprotokollen er TFTP (RFC1350). TFTP brukes i stor grad til klargjøring av nettverksenheter i private lokalnett. Selv om den ikke anbefales til klargjøring av eksterne endepunkter over Internett, kan TFTP være praktisk til distribusjon i små organisasjoner, til intern forhåndsklargjøring og til utvikling og testing. Du finner mer informasjon om intern forhåndsklargjøring under Intern forhåndsklargjøring av enheter, på side 39. I prosedyren nedenfor endres en profil etter nedlasting av en fil fra en TFTP-server.

Prosedyre

Trinn 1 I et lokalnett kobler du til en datamaskin og en telefon til en hub, svitsj eller liten ruter.

Trinn 2 Installer og aktiver en TFTP-server på datamaskinen.

Trinn 3 Bruk et tekstredigeringsprogram til å opprette en konfigurasjonsprofil som angir verdien for GPP_A til 12345678, som vist i eksemplet.

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

Trinn 4 Lagre profilen med navnet `basic.txt` i rotkatalogen på TFTP-serveren.

Du kan kontrollere at TFTP-serveren er riktig konfigurert: be om filen `basic.txt` gjennom en annen TFTP-klient enn telefonen. Bruk helst en TFTP-klient som kjører på en separat vert fra klareringsserveren.

Trinn 5 Åpne siden for administrator / avansert konfigurasjon i en nettleser på datamaskinen. Hvis for eksempel IP-adressen til telefonen er 192.168.1.100:

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

Trinn 6 Velg fanen **Voice (Tale)** > **Provisioning (Klargjøring)** og sjekk verdiene for de generelle parameterne fra GPP_A til GPP_P. Disse skal være tomme.

Trinn 7 Resynkroniser testtelefonen med konfigurasjonsprofilen `basic.txt` ved å åpne resynkroniserings-URL-adressen i et nettleservindu.

Hvis IP-adressen til TFTP-serveren er 192.168.1.200, skal kommandoen være lik følgende eksempel:

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

Når telefonen mottar denne kommandoen, ber enheten på adressen 192.168.1.100 ber om filen `basic.txt` fra TFTP-serveren på IP-adressen 192.168.1.200. Telefonen analyserer deretter den nedlastede filen og oppdaterer parameteren GPP_A med verdien 12345678.

Trinn 8 Kontroller at parameteren har blitt riktig oppdatert: Oppdater konfigurasjonssiden på nettleseren på datamaskinen, og velg fanen **Voice (Tale)** > **Provisioning (Klargjøring)**.

Parameteren GPP_A skal nå inneholde verdien 12345678.

Bruke syslog til loggmeldinger

Telefonen sender en syslog-melding til den angitte syslog-serveren når enheten skal til å resynkronisere med en klargjøringsserver, og etter at resynkroniseringen har blitt fullført eller mislyktes. Du kan identifisere denne serveren ved å åpne telefonens administrasjonsnettside (se Få tilgang til telefonens nettside, på side 7), velge **Voice (Tale)** > **System** og identifisere serveren i **Syslog Server**-parameteren i delen **Optional Network Configuration** (Valgfri nettverkskonfigurasjon). Konfigurer IP-adressen til syslog-serveren i enheten og se meldingene som genereres under de gjenværende prosedyrene.

Prosedyre

Trinn 1 Installer og aktiver en syslog-server på den lokale datamaskinen.

Trinn 2 Programmer IP-adressen til datamaskinen i profilens Syslog_Server-parameter, og godta endringen:

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

Trinn 3 Klikk på **System**-fanen, og skriv inn verdien for den lokale syslog-serveren i parameteren Syslog_Server.

Trinn 4 Gjenta resynkroniseringen som beskrevet i Resynkronisering via TFTP, på side 47.

Enheten genererer to syslog-meldinger under resynkroniseringen. Den første meldingen angir at en forespørsel er under behandling. Den andre meldingen varsler om fullført eller mislykket resynkronisering.

Trinn 5 Kontroller at syslog-serveren har mottatt meldinger som ligner på følgende:

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

Du kan få tilgang til detaljerte meldinger ved å programmere parameteren Debug_Server (i stedet for parameteren Syslog_Server) med IP-adressen til syslog-serveren, ved å angi Debug_Level til en verdi mellom 0 og 3 (3 gir mest detaljer):

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

Du kan konfigurere innholdet i disse meldingene ved hjelp av følgende parametre:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Hvis noen av disse parameterne tømmes, blir ikke den tilsvarende syslog-meldingen generert.

Resynkronisere enheter automatisk

En enhet kan resynkronisere regelmessig med klargjøringsserveren for å sikre at eventuelle profilendringer foretatt på serveren spres til endepunktenheten (i stedet for å sende en eksplisitt resynkroniseringsforespørsel til endepunktet).

Du kan få telefonen til å resynkronisere regelmessig med en server ved å angi en konfigurasjonsprofil-URL ved hjelp av parameteren Profile_Rule og et resynkroniseringsintervall ved hjelp av parameteren Resync_Periodic.

Før du begynner

Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Prosedyre

Trinn 1 Velg **Voice (Tale)** > **Provisioning (Klargjøring)**.

Trinn 2 Angi parameteren Profile_Rule. Dette eksemplet forutsetter IP-adressen 192.168.1.200 for TFTP-serveren.

Trinn 3 I feltet **Resync Periodic** (Resynkroniser regelmessig) skriver du inn en liten testverdi, for eksempel **30** sekunder.

Trinn 4 Klikk på **Submit all Changes** (Godta alle endringer).

Med de nye parameterinnstillingene resynkroniserer telefonen to ganger i minuttet med konfigurasjonsfilen som URL-adressen angir.

Trinn 5 Se syslog-meldingene (som beskrevet i delen Bruke syslog til loggmeldinger, på side 48).

Trinn 6 Sjekk at feltet **Resync On Reset** (Resynkroniser ved tilbakestilling) er angitt til **Yes** (Ja).

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

Trinn 7 Slå telefonen av og på for å tvinge den til å resynkronisere med klargjøringsserveren.

Hvis resynkronisering av en eller annen grunn mislykkes – for eksempel hvis serveren ikke svarer –, venter enheten (i antallet sekunder som er konfigurert i **Resync Error Retry Delay** (Resynkroniseringsfeil – forsinkelse før nytt forsøk)) før den forsøker å resynkronisere på nytt. Hvis **Resync Error Retry Delay** er null, prøver ikke telefonen å resynkronisere på nytt etter et mislykket resynkroniseringsforsøk.

Trinn 8 (Valgfritt) Angi et lite tall som verdi for feltet **Resync Error Retry Delay**, for eksempel **30**.

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

Trinn 9 Deaktiver TFTP-serveren, og se resultatene i syslog-meldingen.

Unike profiler, makroutvidelse og HTTP

I en distribusjon der hver telefon må konfigureres med ulike verdier for enkelte parametre, for eksempel User_ID eller Display_Name, kan tjenesteleverandøren opprette en unik profil for hver distribuerte enhet og være vert for disse profilene på en klargjøringsserver. Hver telefon må på sin side konfigureres til å resynkronisere med sin egen profil i samsvar med en forhåndsbestemt navngivingskonvensjon for profiler.

Syntaksen for profil-URL-adressen kan inkludere identifiserende opplysninger som er spesifikke for hver telefon – som MAC-adresse eller serienummer –, gjennom makroutvidelse av innebygde variabler. Makroutvidelse eliminerer behovet for å angi disse verdiene på flere steder i hver profil.

En profilregel gjennomgår makroutvidelse før regelen tas i bruk på telefonen. Makroutvidelse styrer mange verdier, for eksempel:

- $MA utvides til enhetens 12-sifrede MAC-adresse (ved hjelp av heksadesimale sifre med små bokstaver). For eksempel 000e08abcdef.
- $SN utvides til enhetens serienummer. For eksempel 88012BA01234.

Andre verdier kan makroutvides på denne måten, inkludert alle generelle parametre, fra GPP_A til GPP_P. Du kan se et eksempel på denne prosessen under Resynkronisering via TFTP, på side 47. Makroutvidelse er ikke begrenset til URL-filnavnet, men kan også brukes på en hvilken som helst del av profilregelparameteren. Disse parameterne refereres til som $A til $P. Du finner en fullstendig liste over variabler som er tilgjengelige for makroutvidelse, under Makroutvidelsesvariabler, på side 72.

I denne øvelsen klargjøres en profil som er spesifikk for en telefon, på en TFTP-server.

Øvelse: Klargjøre en bestemt IP-telefonprofil på en TFTP-server

Prosedyre

Trinn 1 Hent telefonens MAC-adresse fra produktetiketten. (MAC-adressen er nummeret som består av tall og heksadesimale sifre med små bokstaver, for eksempel 000e08aabbcc.

Trinn 2 Kopier konfigurasjonsfilen `basic.txt` (beskrevet i Resynkronisering via TFTP, på side 47) til en ny fil kalt `CP-xxxx-3PCC macaddress.cfg` (erstatt `xxxx` med modellnummeret og `macaddress` med telefonens MAC-adresse.)

Trinn 3 Flytt den nye filen til TFTP-serverens virtuelle rotkatalog.

Trinn 4 Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Trinn 5 Velg **Voice (Tale)** > **Provisioning (Klargjøring)**.

Trinn 6 Skriv inn `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` i **Profile Rule**-feltet (Profilregel).

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

Trinn 7 Klikk på **Godta alle endringer**. Dette utløser en umiddelbar omstart og resynkronisering.

Når den neste resynkroniseringen utføres, henter telefonen den nye filen ved å utvide $MA-makrouttrykket i MAC-adressen sin.

Resynkronisering via HTTP GET

HTTP gir en mer pålitelig resynkroniseringsmetode enn TFTP fordi HTTP etablerer en TCP-tilkobling, og fordi TFTP bruker UDP, som er mindre pålitelig. I tillegg gir HTTP-servere bedre filtrerings- og loggingsfunksjoner sammenlignet med TFTP-servere.

På klientsiden krever ikke telefonen noen bestemt konfigurasjonsinnstilling på serveren for at den skal kunne resynkronisere via HTTPS. Syntaksen til Profile_Rule-parameteren for bruk av HTTP med GET-metoden ligner på syntaksen som brukes til TFTP. Hvis en standard nettleser kan hente en profil fra en HTTP-server, skal en telefon også kunne gjøre det.

Øvelse: Resynkronisering via HTTP GET

Prosedyre

Trinn 1 Installer en HTTP-server på den lokale datamaskinen eller på en annen tilgjengelig vert.

En Apache-server med åpen kildekode kan lastes ned fra Internett.

Trinn 2 Kopier konfigurasjonsprofilen `basic.txt` (beskrevet i Resynkronisering via TFTP, på side 47) til den virtuelle rotkatalogen på den installerte serveren.

Trinn 3 Sjekk serverinstallasjon og filtilgang til `basic.txt` ved å åpne profilen med en nettleser.

Trinn 4 Endre Profile_Rule for testtelefonen slik at den peker til HTTP-serveren i stedet for til TFTP-serveren, slik at profilen kan lastes ned regelmessig.

Forutsett for eksempel at HTTP-serveren er på 192.168.1.300, og angi følgende verdi:

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

Trinn 5 Klikk på **Godta alle endringer**. Dette utløser en umiddelbar omstart og resynkronisering.

Trinn 6 Se syslog-meldingene som telefonen sender. De regelmessige resynkroniseringene skal nå hente profilen fra HTTP-serveren.

Trinn 7 I HTTP-serverloggen ser du hvordan informasjonen som identifiserer testtelefonen, vises i loggen til brukeragenter.

Denne informasjonen skal inneholde produsent, produktnavn, gjeldende fastvareversjon og serienummer.

Klargjøring gjennom Cisco XML

Hver av telefonene, her angitt som xxxx, kan klargjøres ved hjelp av Cisco XML-funksjoner.

Du kan sende et XML-objekt til telefonen via en SIP-varslingspakke eller en HTTP Post til telefonens CGI-grensesnitt: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC utvider Cisco XML-funksjonen slik at den støtter klargjøring via et XML-objekt:

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

Etter at telefonen mottar XML-objektet, laster den ned klargjøringsfilen fra [profile-rule]. Denne regelen bruker makroer til å forenkle utviklingen av XML-tjenesteprogrammet.

URL-oppløsning med makroutvidelse

Underkataloger med flere profiler på serveren gir en praktisk måte å administrere mange distribuerte enheter. Profil-URL-adressen kan inneholde:

- Navnet på en klargjøringsserver eller en eksplisitt IP-adresse. Hvis profilen identifiserer klargjøringsserveren på grunnlag av navn, utfører telefonen et DNS-oppslag for å løse navnet.
- En ikke-standard serverport som angis i URL-adressen ved hjelp av standardsyntaksen `:port` etter navnet på serveren.
- Underkatalogen i serverens virtuelle rotkatalog hvor profilen er lagret, angitt ved hjelp av standard URL-notasjon og administrert gjennom makroutvidelse.

Følgende Profile_Rule ber for eksempel om profilfilen ($PN.cfg), i serverens underkatalog `/cisco/config`, fra TFTP-serveren som kjører på vertens prov.telco.com og lytter etter en tilkobling på port 6900:

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

Det kan identifiseres en profil for hver telefon i en generell parameter, med verdien referert i en felles profilregel ved hjelp av makroutvidelse.

Forutsett for eksempel at GPP_B er angitt som `Dj6Lmp23Q`.

Profile_Rule har verdien:

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

Når enheten resynkroniserer og makroene utvides, ber telefonen med MAC-adressen 000e08012345 om profilen som har et navn som inneholder enhetens MAC-adresse, på følgende URL-adresse:

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

Sikker resynkronisering med HTTPS

Disse metodene er tilgjengelige på telefonen for resynkronisering med sikker kommunikasjonsprosess:

- Grunnleggende resynkronisering med HTTPS
- HTTPS med klientsertifikatgodkjenning
- HTTPS klientfiltrering og dynamisk innhold

Grunnleggende resynkronisering med HTTPS

HTTPS legger til SSL i HTTP for ekstern klargjøring, slik at:

- telefonen kan godkjenne klargjøringsserveren
- klargjøringsserveren kan godkjenne telefonen
- man har trygghet for at informasjon som utveksles mellom telefonen og klargjøringsserveren, holdes fortrolig

SSL genererer og utveksler hemmelige (symmetriske) nøkler for hver tilkobling mellom telefonen og serveren, ved hjelp av offentlige/private nøkkelpar som er forhåndsinstallert på telefonen og klargjøringsserveren.

På klientsiden krever ikke telefonen noen bestemt konfigurasjonsinnstilling på serveren for å kunne resynkronisere med HTTPS. Syntaksen til Profile_Rule-parameteren for bruk av HTTPS med GET-metoden ligner på syntaksen som brukes for HTTP eller TFTP. Hvis en standard nettleser kan hente en profil fra en HTTPS-server, skal en telefon også kunne gjøre det.

I tillegg til å installere en HTTPS-server må det installeres et SSL-serversertifikat som signeres av Cisco, på klargjøringsserveren. Enhetene kan ikke resynkronisere med en server som bruker HTTPS, med mindre serveren legger frem et Cisco-signert serversertifikatet. Du finner instruksjoner for hvordan du oppretter signerte SSL-sertifikater for taleprodukter, på https://supportforums.cisco.com/docs/DOC-9852.

Øvelse: Grunnleggende resynkronisering med HTTPS

Prosedyre

Trinn 1 Installer en HTTPS-server på en vert som har en IP-adresse som er kjent for nettverkets DNS-server gjennom vanlig vertsnavnoversettelse.

Apache-servere med åpen kildekode kan konfigureres til å fungere som HTTPS-server når de installeres mod_ssl-pakken med åpen kildekode.

Trinn 2 Generer en server-sertifikatsigneringsforespørsel for serveren. Her må du kanskje installere OpenSSL-pakken med åpen kildekode eller tilsvarende programvare. Hvis du bruker OpenSSL, er kommandoen for å generere den grunnleggende CSR-filen som følger:

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

Kommandoen genererer et offentlig/privat nøkkelpar, som lagres i filen `privkey.pem`.

Trinn 3 Send CSR-filen (provserver.csr) til Cisco for signering.

Et signert serversertifikatet returneres (provserver.cert) sammen med en Sipura CA-klientrotsertifikat, spacroot.cert.

Hvis du vil ha mer informasjon, se https://supportforums.cisco.com/docs/DOC-9852.

Trinn 4 Lagre det signerte serversertifikatet, filen med det private nøkkelparet og klientrotsertifikatet på egnede plasseringer på serveren.

Hvis det er en Apache-installasjon på Linux, vil plasseringene vanligvis være:

```
# 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
```

Trinn 5 Start serveren på nytt.

Trinn 6 Kopier konfigurasjonsfilen `basic.txt` (beskrevet i Resynkronisering via TFTP, på side 47) til den virtuelle rotkatalogen på HTTPS-serveren.

Trinn 7 Kontroller at serveren fungerer som den skal, ved å laste ned `basic.txt` fra HTTPS-serveren ved å bruke en standard nettleser på den lokale datamaskinen.

Trinn 8 Inspiser serversertifikatet som serveren gir.

Nettleseren gjenkjenner sannsynligvis ikke sertifikatet som gyldig med mindre nettleseren er forhåndskonfigurert til å godta Cisco som en rotsertifikatutsteder. Telefonene forventer imidlertid at sertifikatet skal være signert på denne måten.

Endre Profile_Rule i testenheten slik at den inneholder en referanse til HTTPS-serveren, for eksempel:

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

Eksemplet forutsetter at navnet på HTTPS-serveren er **`my.server.com`**.

Trinn 9 Klikk på **Godta alle endringer**.

Trinn 10 Se syslog-meldingen som telefonen sender.

Syslog-meldingen skal angi at resynkroniseringen har hentet profilen fra HTTPS-serveren.

Trinn 11 (Valgfritt) Bruk Ethernet-protokollanalyse på telefonens subnett til å bekrefte at pakkene krypteres.

I denne øvelsen har ikke verifisering av klientsertifikat blitt aktivert. Forbindelsen mellom telefonen og serveren er kryptert. Overføringen er imidlertid ikke sikker fordi en hvilken som helst klient kan koble til serveren og be om filen dersom de vet filnavnet og katalogplasseringen. For å oppnå sikker resynkronisering må serveren også godkjenne klienten, som vist i øvelsen beskrevet under HTTPS med klientsertifikatgodkjenning, på side 55.

HTTPS med klientsertifikatgodkjenning

I standardkonfigurasjonen fra fabrikken ber ikke serveren om et SSL-klientsertifikat fra en klient. Overføring av profilen er ikke trygt fordi en hvilken som helst klient kan koble til serveren og be om profilen. Du kan redigere konfigurasjonen for å aktivere klientgodkjenning; serveren krever et klientsertifikat for å godkjenne telefonen før den godtar en tilkoblingsforespørsel.

På grunn av dette kravet kan ikke resynkronisering testes uavhengig ved hjelp av en nettleser som mangler legitimasjon. Du kan følge med på SSL-nøkkelutvekslingen innenfor HTTPS-forbindelsen mellom testtelefonen og serveren ved hjelp av ssldump-verktøyet. Verktøyet viser samhandlingen mellom klienten og serveren.

Øvelse: HTTPS med klientsertifikatgodkjenning

Prosedyre

Trinn 1 Aktiver klientsertifikatgodkjenning på HTTPS-serveren.

Trinn 2 I Apache (v.2) angir du følgende i serverens konfigurasjonsfil:

```
SSLVerifyClient  require
```

Sjekk også at spacroot.cert har blitt lagret som vist i Grunnleggende resynkronisering med HTTPS, på side 53-øvelsen.

Trinn 3 Start HTTPS-serveren på nytt, og se syslog-meldingen fra telefonen.

Hver resynkronisering til serveren utløser nå symmetrisk godkjenning, slik at både serversertifikatet og klientsertifikatet bekreftes før profilen overføres.

Trinn 4 Bruk ssldump til å registrere en ny synkroniseringstilkobling mellom telefonen og HTTPS-serveren.

Hvis klientsertifikatverifisering er riktig aktivert på serveren, viser ssldump-sporet den symmetriske utvekslingen av sertifikater (første server-til-klient og deretter klient-til-server) før de krypterte pakkene som inneholder profilen.

Med klientgodkjenning aktivert kan bare en telefon med en MAC-adresse som samsvarer med et gyldig klientsertifikat, be om profilen fra klargjøringsserveren. Serveren avviser forespørsler fra en vanlig nettleser eller en annen enhet som ikke er godkjent.

HTTPS klientfiltrering og dynamisk innhold

Hvis HTTPS-serveren er konfigurert til å kreve et klientsertifikat, identifiserer informasjonen i sertifikatet resynkroniseringstelefonen og gir den riktig konfigurasjonsinformasjon.

HTTPS-serveren gjør sertifikatinformasjonen tilgjengelig for CGI-skript (eller kompilerte CGI-programmer) som aktiveres under resynkroniseringsforespørselen. Av illustrasjonsformål bruker denne øvelsen skriptspråket Perl med åpen kildekode, og den forutsetter at Apache (v.2) brukes som HTTPS-server.

Prosedyre

Trinn 1 Installer Perl på verten som kjører HTTPS-serveren.

Trinn 2 Generer følgende reflektorskript i Perl:

```
#!/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>";
```

Trinn 3 Lagre filen med filnavnet `reflect.pl`, med kjøretillatelse (chmod 755 på Linux), i CGI-skriptkatalogen til HTTPS-serveren.

Trinn 4 Kontroller tilgjengeligheten til CGI-skript på serveren (det vil si `/cgi-bin/...`).

Trinn 5 Endre Profile_Rule på testenheten slik at den resynkroniserer med reflektorskriptet, som i eksemplet nedenfor:

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

Trinn 6 Klikk på **Godta alle endringer**.

Trinn 7 Se syslog-meldingen for å sjekke at resynkroniseringen gjennomføres.

Trinn 8 Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Trinn 9 Velg **Voice (Tale)** > **Provisioning (Klargjøring)**.

Trinn 10 Kontroller at parameteren GPP_D inneholder informasjonen som skriptet har registrert.

Denne informasjonen inneholder produktnavnet, MAC-adressen og serienummeret dersom testenheten kommer med et unikt sertifikat fra produsenten. Informasjonen inneholder generiske strenger hvis enheten har blitt produsert før fastvareversjon 2.0.

Et lignende skript kan se informasjon om resynkroniseringsenheten og deretter gi enheten passende konfigurasjonsparameterverdier.

HTTPS-sertifikater

Telefonen har en pålitelig og sikker klargjøringsstrategi som er basert på HTTPS-forespørsler fra enheten til klargjøringsserveren. Både et serversertifikatet og et klientsertifikat brukes til å godkjenne telefonen for serveren og serveren for telefonen.

Hvis du vil bruke HTTPS med telefonen, må du generere en sertifikatsigneringsforespørsel (CSR) og sende den til Cisco. Telefonen genererer et sertifikat for installasjon på klargjøringsserveren. Telefonen godkjenner sertifikatet når den prøver å etablere en HTTPS-tilkobling med klargjøringsserveren.

HTTPS-metode

HTTPS krypterer kommunikasjonen mellom en klient og en server, og beskytter dermed meldingsinnhold fra andre nettverksenheter. Krypteringsmetoden for teksten i kommunikasjonen mellom en klient og en server er basert på symmetrisk nøkkelkryptografi. Ved symmetrisk nøkkelkryptografi deler en klient og en server en enkelt hemmelig nøkkel via en sikker kanal som beskyttes med offentlig/privat nøkkelkryptering.

Meldinger som er kryptert med den hemmelige nøkkelen, kan bare dekrypteres med den samme nøkkelen. HTTPS støtter en rekke algoritmer for symmetrisk kryptering. Telefonen implementerer opptil 256-biters symmetrisk kryptering, ved hjelp av den amerikansk krypteringsstandarden AES, i tillegg til 128-biters RC4.

HTTPS legger også til rette for godkjenning av servere og klienter som deltar i sikre transaksjoner. Denne funksjonen sikrer at en klargjøringsserver og en enkelt klient ikke kan bli lurt av andre enheter i nettverket. Denne funksjonen har stor betydning i forbindelse med ekstern klargjøring av endepunkter.

Server- og klientgodkjenning utføres ved hjelp av offentlig/privat nøkkelkryptering med et sertifikat som inneholder den offentlige nøkkelen. Tekst som krypteres med en offentlig nøkkel, kan bare dekrypteres med den tilsvarende private nøkkelen (og omvendt). Telefonen støtter RSA-algoritmen (Rivest-Shamir-Adleman) for offentlig/privat nøkkelkryptografi.

SSL-serversertifikat

Hver sikre klargjøringsserver får utstedt et SSL-serversertifikat som Cisco signerer direkte. Fastvaren som kjører på telefonen, gjenkjenner bare Cisco-sertifikater som gyldige. Når en klient kobler til en server ved hjelp av HTTPS, forkaster den alle serversertifikatet som ikke er signert av Cisco.

Denne mekanismen beskytter tjenesteleverandøren mot uautorisert tilgang til telefonen og mot forsøk på å lure klargjøringsserveren. Uten slik beskyttelse kan det være mulig for en angriper å klargjøre telefonen på nytt for å få konfigurasjonsinformasjon eller for å bruke en annen VoIP-tjeneste. Uten den private nøkkelen som svarer til et gyldig serversertifikatet, kan ikke angriperen etablere kommunikasjon med en telefon.

Skaffe et serversertifikat

Prosedyre

Trinn 1 Kontakt en Cisco-støttemedarbeider som vil samarbeide med deg om sertifikatprosessen. Hvis du ikke jobber med en bestemt støttemedarbeider, sender du forespørselen via e-post til ciscosb-certadmin@cisco.com.

Trinn 2 Generer en privat nøkkel som skal brukes i en CSR (Sertifikatsigneringsforespørsel). Nøkkelen er privat, og du trenger ikke oppgi den til Ciscos kundestøtte. Bruk "openssl" med åpen kildekode til å generere nøkkelen. Eksempel:

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

Trinn 3 Generer en CSR som inneholder felter som identifiserer organisasjonen og plasseringen din. Eksempel:

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

Du må ha følgende informasjon:

- Emnefelt – skriv inn et vanlig navn (CN), som må ha FQDN-syntaks (fullstendig kvalifisert domenenavn). Under SSL-godkjenningen bekrefter telefonen at sertifikatet som den mottar, kommer fra maskinen som har vist det.
- Serververtsnavn – for eksempel provserv.domain.com.
- E-postadresse – skriv inn en e-postadresse, slik at kundestøtten om nødvendig kan kontakte deg. Denne e-postadressen er synlig i CSR.

Trinn 4 Send CSR-en (i zip-filformat) i en e-post til Cisco-støttemedarbeideren eller til ciscosb-certadmin@cisco.com. Sertifikatet signeres av Cisco. Cisco sender sertifikatet til deg for installasjon på systemet ditt.

Klientsertifikat

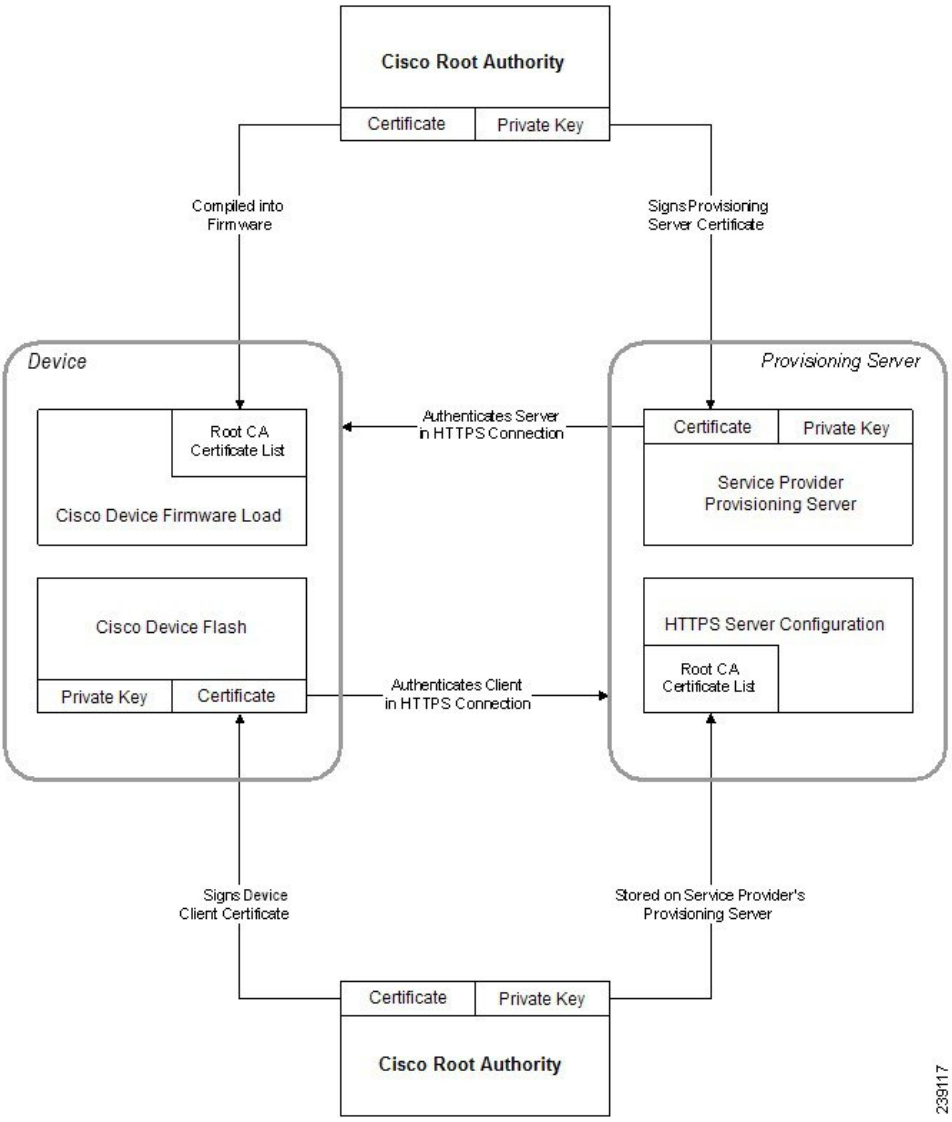
I tillegg til å foreta et direkte angrep på en telefon, kan en angriper forsøke å kontakte en klargjøringsserver gjennom en standard nettleser eller en annen HTTPS-klient for å hente konfigurasjonsprofilen fra klargjøringsserveren. For å hindre denne typen angrep har hver telefon i tillegg et unikt klientsertifikat, signert av Cisco, som inneholder ID-informasjon om hvert enkelt endepunkt. En rotsertifikat fra en sertifikatutsteder (CA) som kan godkjenne enhetens klientsertifikat, gis til hver tjenesteleverandør. Godkjenningsbanen gjør at klargjøringsserveren kan avvise uautoriserte forespørsler om konfigurasjonsprofiler.

Sertifikatstruktur

Kombinasjonen av et serversertifikatet og et klientsertifikat sørger for sikker kommunikasjon mellom en ekstern telefon og klargjøringsserveren dens. Illustrasjonen nedenfor viser forholdet og plasseringen av sertifikater, offentlige/private nøkkelpar og signerende rotinstanser mellom Cisco-klienten, klargjøringsserveren og sertifiseringsutstederen.

Den øvre delen av diagrammet viser rotinstansen for klargjøringsserveren, som brukes til å signere de enkelte klargjøringsserversertifikatene. Det tilsvarende rotsertifikatet kompileres i fastvaren, noe som gjør det mulig for telefonen å godkjenne godkjente klargjøringsservere.

Figur 2: Sertifikatutstederflyt



Konfigurere en egendefinert sertifikatutsteder (CA)

Digitale sertifikater kan brukes til å godkjenne nettverksenheter og brukere på nettverket. De kan brukes til å forhandle IPSec-økter mellom nettverksnoder.

En tredjepart bruker et sertifikat fra en sertifikatutsteder til å validere og godkjenne to eller flere noder som prøver å kommunisere. Hver node har en offentlig og en privat nøkkel. Den offentlige nøkkelen krypterer data. Den private nøkkelen dekrypterer data. Siden nodene har skaffet sine sertifikater fra samme kilde, kan de være sikre på hverandres identitet.

Enheten kan bruke digitale sertifikater som er levert av en tredjeparts sertifikatutsteder (CA), til å godkjenne IPSec-tilkoblinger.

Telefonen støtter et utvalg utstedere av rotsertifikater innebygd i fastvaren på forhånd:

- Cisco Small Business CA Certificate

- CyberTrust CA Certificate
- Verisign CA certificate
- Sipura Root CA Certificate
- Linksys Root CA Certificate

Før du begynner

Åpne telefonens administrasjonsnettside. Se Få tilgang til telefonens nettside, på side 7.

Prosedyre

Trinn 1 Velg **Info** > **Status**.

Trinn 2 Bla til **Custom CA Status** (Egendefinerte sertfikatutstedere – status), og se følgende felt:

- Custom CA Provisioning Status (Egendefinerte sertfikatutstedere – klargjøringsstatus) – viser klargjøringsstatus.
  - Last provisioning succeeded on mm/dd/yyyy HH:MM:SS (Siste klargjøring fullført mm/dd/åååå TT:MM:SS); eller
  - Last provisioning failed on mm/dd/yyyy HH:MM:SS (Siste klargjøring mislykket mm/dd/åååå TT:MM:SS)
- Custom CA Info (Egendefinerte sertfikatutstedere – info) – viser informasjon om egendefinerte sertifikatutstedere.
  - Installed (Installert) – viser "CN Value" (CN-verdi), der "CN Value" er verdien til CN-parameteren for Subject-feltet (Emne) i det første sertifikatet.
  - Not Installed (Ikke installert) – vises dersom ingen sertifikater fra egendefinerte sertifikatutstedere er installert.

Profiladministrasjon

Denne delen beskriver opprettelse av konfigurasjonsprofiler som forberedelse til nedlasting. Funksjonen kan beskrives slik: TFTP fra en lokal datamaskin brukes som resynkroniseringsmetode, selv om HTTP eller HTTPS også kan brukes.

Komprimere en åpen profil med Gzip

En konfigurasjonsprofil i XML-format kan bli ganske stor hvis profilen angir alle parametre enkeltvis. For å redusere belastningen på klargjøringsserveren støtter telefonen komprimering av XML-filer ved hjelp av deflate-komprimeringsformatet som gzip-verktøyet (RFC 1951) støtter.

Merk Komprimering må skje før kryptering for at telefonen skal gjenkjenne en komprimert og kryptert XML-profil.

For å gi mulighet for integrasjon i tilpassede klargjøringsserver-bakgrunnsløsninger kan zlib-komprimeringsbiblioteket med åpen kildekode brukes i stedet for det frittstående gzip-verktøyet til å utføre komprimering av profiler. Telefonen forventer imidlertid at filen skal inneholde et gyldig gzip-hode.

Prosedyre

Trinn 1 Installer gzip på den lokale datamaskinen.

Trinn 2 Komprimer konfigurasjonsprofilen `basic.txt` (beskrevet i Resynkronisering via TFTP, på side 47) ved å aktivere gzip fra kommandolinjen:

```
gzip basic.txt
```

Dette genererer den deflate-komprimerte filen `basic.txt.gz`.

Trinn 3 Lagre filen `basic.txt.gz` i den virtuelle rotkatalogen på TFTP-serveren.

Trinn 4 Endre Profile_Rule på testenheten slik at den resynkroniserer med den deflate-komprimerte filen i stedet for den opprinnelige XML-filen, som vist i eksemplet nedenfor:

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

Trinn 5 Klikk på **Submit All Changes** (Godta alle endringer).

Trinn 6 Se syslog-meldingen fra telefonen.

Ved en resynkronisering laster telefonen ned den nye filen og bruker den til å oppdatere parametrene.

Beslektede emner

Komprimering av åpne profiler, på side 18

Kryptere en profil med OpenSSL

Komprimerte eller ikke-komprimerte profiler kan krypteres (filer må imidlertid komprimeres før de krypteres). Kryptering er nyttig når man ønsker å beskytte profilinformasjon, for eksempel når det brukes TFTP eller HTTP til kommunikasjon mellom telefonen og klargjøringsserveren.

Telefonen støtter symmetrisk kryptering ved hjelp av den 256-biters AES-algoritmen. Slik kryptering kan utføres ved hjelp av OpenSSL-pakken med åpen kildekode.

Prosedyre

Trinn 1 Installer OpenSSL på en lokal datamaskin. Dette kan kreve at OpenSSL-programmet kompileres på nytt for å aktivere AES.

Trinn 2 Ved hjelp `basic.txt`-konfigurasjonsfilen (beskrevet i Resynkronisering via TFTP, på side 47) genererer du en kryptert fil med følgende kommando:

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

Den komprimerte `basic.txt.gz`-filen som ble opprettet i Komprimere en åpen profil med Gzip, på side 60, kan også brukes, fordi XML-profilen kan være både komprimert og kryptert.

Trinn 3 Lagre den krypterte `basic.cfg`-filen i den virtuelle rotkatalogen på TFTP-serveren.

Trinn 4 Endre Profile_Rule på testenheten slik at den resynkroniserer med den krypterte filen i stedet for med den opprinnelige XML-filen. Krypteringsnøkkelen gjøres kjente til telefonen med følgende URL-alternativ:

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

Trinn 5 Klikk på **Godta alle endringer**.

Trinn 6 Se syslog-meldingen fra telefonen.

Ved en resynkronisering laster telefonen ned den nye filen og bruker den til å oppdatere parametrene.

Beslektede emner

AES-256-CBC-kryptering, på side 18

Opprette delte profiler

En telefon laster ned flere separate profiler i løpet av hver resynkronisering. Denne fremgangsmåten gjør det mulig å administrere ulike typer profilinformasjon på separate servere og å bevare felles konfigurasjonsparameterverdier som er atskilt fra de kontospesifikke verdiene.

Prosedyre

Trinn 1 Opprett en ny XML-profil, `basic2.txt`, som angir en verdi for en parameter som gjør at den skiller seg fra de tidligere øvelsene. Legg for eksempel til følgende i `basic.txt`-profilen:

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

Trinn 2 Lagre `basic2.txt`-profilen i TFTP-serverens virtuelle rotkatalog.

Trinn 3 La den første profilregelen fra de tidligere øvelsene være i mappen, men konfigurer den andre profilregelen (Profile_Rule_B) slik at den peker til den nye filen:

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

Trinn 4 Klikk på **Godta alle endringer**.

Telefonen resynkroniserer nå med både den første og den andre profilen – i den rekkefølgen – ved senere resynkroniseringsoperasjoner.

Trinn 5 Se syslog-meldingen for å bekrefte at virkemåten er som forventet.

Angi personvernhode for telefonen

En brukers personvernhode i SIP-meldingen angir brukerens personvernbehov fra det klarerte nettverket.

Du kan angi en verdi for brukerens personvernhode for hvert internnummer ved hjelp av en XML-kode i `config.xml`-filen.

Alternativene for personvernhode er:

- Deaktivert (Disabled) (standard).
- none (ingen) – Brukeren ber om at en personverntjeneste ikke bruker noen personvernfunksjoner i denne SIP-meldingen.
- header (hode) – brukeren trenger en personverntjeneste til å skjule hoder som ikke kan renses for identifiserbar informasjon.
- session (økt) – brukeren ber om at en personverntjeneste sørger for anonymitet under øktene.
- user (bruker) – brukeren ber om personvern bare for mellomledd.
- id – brukeren ber om at systemet bytter ut en id som ikke viser IP-adressen eller vertsnavnet.

Prosedyre

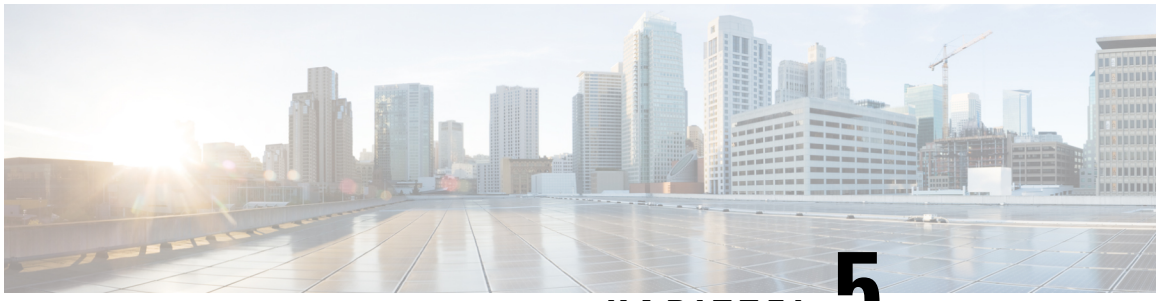
Trinn 1 Rediger `config.xml`-filen til telefonen i et tekst- eller XML-redigeringsprogram.

Trinn 2 Sett inn koden **`< Privacy_Header_N_ ua = "IT" >`*`Value`*`< / Privacy_Header_N_ >`**, der N er internnummeret (1–10), og bruk en av følgende verdier:

- Standardverdi: **`Disabled`** (Deaktivert)
- **`ingen`**
- **`header (hode)`**
- **`session (økt)`**
- **`user (bruker)`**
- **`id`**

Trinn 3 (Valgfritt) Klargjør alle internnumre på tilleggslinjer ved å bruke den samme koden med det ønskede internnummeret.

Trinn 4 Lagre endringene i `config.xml`-filen.



KAPITTEL 5

Klargjøringsparametre

Oversikt over klargjøringsparametre

Dette kapitlet beskriver klargjøringsparametrene som kan brukes i konfigurasjonsprofilskript.

Parametre for konfigurasjonsprofiler

Følgende tabell definerer funksjon og bruk av hver parameter i delen **Configuration Profile Parameters** (Konfigurasjonsprofilparametre) på fanen **Provisioning** (Klargjøring).

Parameternavn	Beskrivelse og standardverdi
Provision Enable	Styrer alle resynkroniseringer uavhengig av fastvareoppgraderinger. Angitt til **Yes** (Ja) for å aktivere ekstern klargjøring. Standardverdien er Yes (Ja).
Resync On Reset	Utløser en resynkronisering etter hver omstart, unntatt etter omstarter forårsaket av parameteroppdateringer og fastvareoppgraderinger. Standardverdien er Yes (Ja).

Parameternavn	Beskrivelse og standardverdi
Resync Random Delay	En tilfeldig forsinkelse etter oppstartssekvensen før tilbakestillingen utføres, angitt i sekunder. I en samling IP-telefonienheter med planlagt samtidig oppstart gir dette en spredning av tidspunktene da hver enhet sender resynkroniseringsforespørsel til klargjøringsserveren. Funksjonen kan være nyttig ved store distribusjoner i boligområder hvis det oppstår strømbrudd. Verdien for dette feltet må være et heltall mellom 0 og 65535. Standardverdien er 2.
Resync At (TTmm)	Klokkeslettet (TTmm) da enheten resynkroniserer med klargjøringsserveren. Verdien i dette feltet må være et firesifret tall mellom 0000 til 2400 som angir klokkeslettet i formatet TTmm. 0959 angir for eksempel 09:59. Standardverdien er tom. Hvis verdien er ugyldig, ignoreres parameteren. Hvis parameteren angis med en gyldig verdi, ignoreres Resync Periodic-parameteren (Resynkroniser regelmessig).
Resync At Random Delay	Forhindrer overbelastning av klargjøringsserveren når et stort antall enheter slås på samtidig. For å unngå at serveren oversvømmes med resynkroniseringsforespørsler fra flere telefoner, resynkroniserer telefonen i perioden mellom timer og minutter og timer og minutter pluss den tilfeldige forsinkelsen (hhmm, hhmm + random_delay). Hvis for eksempel den tilfeldige forsinkelsen = (Resync At Random Delay + 30)/60 minutter, konverteres den angitte verdien i sekunder til minutter og avrundes til neste minutt for å beregne det endelige random_delay-intervallet. Verdier i området mellom 0 og 65535 er gyldige. Funksjonen deaktiveres når parameteren angis til null. Standardverdien er 600 sekunder (10 minutter).

Parameternavn	Beskrivelse og standardverdi
Resync Periodic	Tidsintervallet mellom regelmessige resynkroniseringer med klargjøringsserveren. Den tilhørende resynkroniseringstidtakeren aktiveres bare etter den første vellykkede synkroniseringen med serveren. Følgende formater er gyldige: • Et heltall Eksempel: Verdien **3000** betyr at den neste resynkroniseringen finner sted om 3000 sekunder. • Flere heltall Eksempel: Verdien **600,1200,300** betyr at den første resynkroniseringen finner sted om 600 sekunder, den andre resynkroniseringen finner sted 1200 sekunder etter den første, og den tredje resynkroniseringen finner sted 300 sekunder etter den andre. • En tidsperiode Eksempel: Verdien **2400+30** betyr at den neste resynkroniseringen finner sted mellom 2400 og 2430 sekunder etter en vellykket resynkronisering. Hvis du vil deaktivere regelmessig resynkronisering, angir du parameteren til null. Standardverdien er 3600 sekunder.

Parameternavn	Beskrivelse og standardverdi
Resync Error Retry Delay	Hvis en resynkroniseringsoperasjon mislykkes fordi IP-telefonienheten ikke kan hente en profil fra serveren, eller fordi den nedlastede filen er skadet, eller det har oppstått en intern feil, prøver enheten å resynkronisere på nytt etter en tidsperiode som er angitt i sekunder. Følgende formater er gyldige: • Et heltall Eksempel: Verdien **300** betyr at det neste forsøket på resynkronisering finner sted om 300 sekunder. • Flere heltall Eksempel: Verdien **600,1200,300** betyr at det første nye forsøket på resynkronisering finner sted 600 sekunder etter en mislykket resynkronisering, det andre forsøket finner sted 1200 sekunder etter at det første nye forsøket mislykkes, og det tredje forsøket finner sted 300 sekunder etter at det andre nye forsøket mislykkes. • En tidsperiode Eksempel: Verdien **2400+30** betyr at det neste nye forsøket finner sted mellom 2400 og 2430 sekunder etter en mislykket resynkronisering. Hvis forsinkelsen angis til 0, prøver ikke enheten å resynkronisere på nytt etter et mislykket resynkroniseringsforsøk.
Forced Resync Delay	Maksimumsintervallet (i sekunder) som telefonen venter før den utfører en resynkronisering. Enheten resynkroniserer ikke mens noen av dens telefonlinjer er aktive. Siden en resynkronisering kan ta flere sekunder, er det ønskelig å vente til enheten har vært ledig en stund, før resynkroniseringen utføres. På denne måten kan en bruker foreta anrop etter hverandre uten avbrudd. Enheten har en tidtaker begynner nedtellingen når alle linjene blir ledige. Denne parameteren er den første verdien til telleren. Resynkroniseringer utsettes til tidtakeren har telt ned til null. Verdier i området mellom 0 og 65535 er gyldige. Standardverdien er 14 400 sekunder.

Parameternavn	Beskrivelse og standardverdi
Resync From SIP	Gjør det mulig å utløse en resynkronisering via en SIP-varslingsmelding. Standardverdien er Yes (Ja).
Resync After Upgrade Attempt	Aktiverer eller deaktiverer resynkronisering etter en oppgradering. Hvis Yes (Ja) velges, utløses synkronisering. Standardverdien er Yes (Ja).
Resync Trigger 1, Resync Trigger 2	Konfigurerbare betingelser for utløsing av resynkronisering. En resynkronisering utløses når logikkformelen i disse parametrene beregnes til SANN. Standardverdien er (tom).
Resync Fails On FNF	En resynkronisering regnes som mislykket hvis det ikke mottas en forespurt profil fra serveren. Dette kan overstyres av denne parameteren. Når den angis til **no** (nei), godtar enheten et `finner ikke filen`-svar fra serveren som en vellykket resynkronisering. Standardverdien er Yes (Ja).
Profilregel Profile Rule B Profile Rule C Profile Rule D	Hver profilregel informerer telefonen om en kilde som den kan hente en profil (konfigurasjonsfil) fra. Under hver ny synkroniseringsoperasjon tar telefonen i bruk alle profiler i rekkefølge. Standard: **`/$PSN.xml`** Hvis du tar i bruk AES-256-CBC-kryptering på konfigurasjonsfilene, angir du krypteringsnøkkel med **`--key`**-nøkkelordet på følgende måte: **`[--key <krypteringsnøkkel>]`** Krypteringsnøkkelen kan eventuelt settes i doble anførselstegn (").
DHCP Option To Use	DHCP-alternativer, atskilt med komma, brukes til å hente fastvare og profiler. Standardverdien er 66,160,159,150,60,43,125.
Log Request Msg	Denne parameteren inneholder meldingen som sendes til syslog-serveren ved starten av et nytt resynkroniseringsforsøk. Standardverdien er `$PN $MAC -Requesting % $SCHEME://$SERVIP:$PORT$PATH`.

Parameternavn	Beskrivelse og standardverdi
Log Success Msg	Syslog-melding som genereres når et resynkroniseringsforsøk lykkes. Standardverdien er `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Log Failure Msg	Syslog-melding som genereres etter et mislykket forsøk på resynkronisering. Standardverdien er `$PN $MAC -- Resync failed: $ERR`.
User Configurable Resync	Gjør det mulig for en bruker å resynkronisere telefonen fra IP-telefonskjermen. Standardverdien er Yes (Ja).

Parametre for fastvareoppgraderinger

Følgende tabell definerer funksjon og bruk av hver parameter i delen **Firmware Upgrade** (Fastvareoppgradering) på fanen **Provisioning** (Klargjøring).

Parameternavn	Beskrivelse og standardverdi
Upgrade Enable	Aktiverer fastvareoppgraderinger uavhengig av resynkroniseringer. Standardverdien er Yes (Ja).
Upgrade Error Retry Delay	Forsinkelsesintervallet før nytt oppgraderingsforsøk (i sekunder) ved en mislykket oppgradering. Enheten har en tidtaker for fastvareoppgraderingsfeil som aktiveres etter et mislykket forsøk på å oppgradere fastvaren. Tidtakeren er initialisert med verdien i denne parameteren. Det neste forsøket på fastvareoppgradering finner sted når tidtakeren teller ned til null. Standardverdien er 3600 sekunder.

Parameternavn	Beskrivelse og standardverdi
Upgrade Rule	Et fastvareoppgraderingsskript som angir betingelsene for oppgradering og de tilhørende URL-adressene for fastvare. Den bruker den samme syntaksen som Profile Rule (Profilregel). Bruk følgende format til å angi oppgraderingsregelen: **<tftp|http|https>://<ip-adresse>/bilde/<navn på innlasting>** Eksempel: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Hvis ingen protokoll angis, antas TFTP. Hvis ingen servernavn angis, brukes verten som ber om URL-adressen, som servernavn. Hvis ingen port angis, brukes standardporten (69 for TFTP, 80 for HTTP eller 443 for HTTPS). Standardverdien er tom.
Log Upgrade Request Msg	Syslog-melding som genereres ved starten av et forsøk på fastvareoppgradering. Standard: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Syslog-melding som genereres etter at en fastvareoppgradering er fullført. Standardverdien er `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg	Syslog-melding som genereres etter et mislykket forsøk på fastvareoppgradering. Standardverdien er `$PN $MAC -- Upgrade failed: $ERR`
Peer Firmware Sharing	Aktiverer eller deaktiverer funksjonen peer-fastvaredeling. Velg **Ja** (Yes) eller **Nei** (No) for å aktivere eller deaktivere funksjonen. Standard: Ja
Peer Firmware Sharing Log Server	Angir IP-adressen og porten som UDP-meldingen sendes til. For eksempel: 10.98.76.123:514, der 10.98.76.123 er IP-adressen og 514 er portnummeret.

Generelle parametre

Følgende tabell definerer funksjon og bruk av hver parameter i delen **General Purpose Parameters** (Generelle parametre) på fanen **Provisioning** (Klargjøring).

Parameternavn	Beskrivelse og standardverdi
GPP A til GPP P	De generelle parametrene GPP_* brukes som frie strengregistre når telefoner konfigureres til å samhandle med en bestemt klargjøringsserverløsning. De kan konfigureres til å inneholde forskjellige verdier, inkludert følgende: • krypteringsnøkler • URL-er • statusinformasjon om flertrinnsklargjøring • POST-forespørselsmaler • aliasmatriser for parameternavn • delvise strengverdier, eventuelt satt sammen til fullstendige parameterverdier Standardverdien er tom.

Makroutvidelsesvariabler

Enkelte makrovariabler gjenkjennes i følgende klargjøringsparametre:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (i bestemte situasjoner)

Innenfor disse parametrene gjenkjennes og utvides syntakstyper, som $NAME eller $(NAME).

Makrovariabeldelstrenger kan angis med notasjonen $(NAME:p) og $(NAME:p:q), der p og q er positive heltall (tilgjengelig i revisjon 2.0.11 og høyere). Makroutvidelsen blir delstrengen som starter med tegnforskyvning p, med lengden q (eller til slutten av strengen hvis q ikke er angitt). Hvis for eksempel GPP_A inneholder ABCDEF, utvides $(A:2) til CDEF, og $(A:2:3) utvides til CDE.

En navn som ikke gjenkjennes, oversettes ikke, og $NAME- eller $(NAME)-skjemaet forblir uendret i parameterverdien etter utvidelsen.

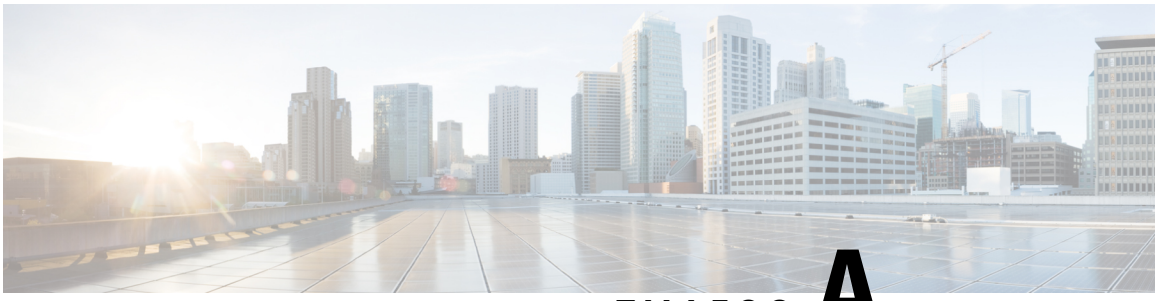
Parameternavn	Beskrivelse og standardverdi
$	Skjemaet $$ utvides til et enkelt $-tegn.
A til P	Erstattes av innholdet i de generelle parametrene GPP_A til GPP_P.
SA til SD	Erstattes med spesialparametrene GPP_SA til GPP_SD. Disse parametrene inneholder nøkler eller passord som brukes i klargjøringen. **Merk** $SA til $SD gjenkjennes som argumenter til den valgfrie kvalifikatoren for resynkroniserings-URL-en, --nøkkel.
MA	MAC-adresse som bruker heksadesimale sifre med små bokstaver, for eksempel 000e08aabbcc.
MAU	MAC-adresse som heksadesimale sifre med store bokstaver, for eksempel 000E08AABBCC.
MAC	MAC-adresse som bruker heksadesimale sifre med små bokstaver og kolon til å skille heksadesimale sifferpar. For eksempel 00:0e:08:aa:bb:cc.
PN	Produktnavn. For eksempel CP-6841-3PCC.
PSN	Produktets serienummer. For eksempel 6841-3PCC.
SN	Serienummerstreng. For eksempel 88012BA01234.
CCERT	Status for SSL-klientsertifikat: installert eller ikke installert.
IP	IP-adressen til telefonen i det lokale subnettet. For eksempel 192.168.1.100.
EXTIP	Telefonens eksterne IP-adresse, som vist på Internett. For eksempel 66.43.16.52.
SWVER	Programvareversjonsstreng. For eksempel sip68xx.11-0-1MPP.
HWVER	Maskinvareversjonsstreng. For eksempel 2.0.1
PRVST	Klargjøringstilstand (numerisk streng): -1 = eksplisitt resynkroniseringsforespørsel 0 = resynkronisering ved oppstart 1 = regelmessig resynkronisering 2 = mislykket synkronisering, nytt forsøk

Parameternavn	Beskrivelse og standardverdi
UPGST	Oppgraderingstilstand (numerisk streng): 1 = første oppgraderingsforsøk 2 = mislykket oppgradering, nytt forsøk
UPGERR	Resultatmelding (ERR) for forrige oppgraderingsforsøk; for eksempel http_get mislyktes.
PRVTMR	Sekunder siden forrige resynkroniseringsforsøk.
UPGTMR	Sekunder siden forrige oppgraderingsforsøk.
REGTMR1	Sekunder siden linje 1 mistet registrering med SIP-server.
REGTMR2	Sekunder siden linje 2 mistet registrering med SIP-server.
UPGCOND	Eldre makronavn.
SKJEMA	Filtilgangsskjema, enten TFTP, HTTP eller HTTPS, som hentes etter analyse av resynkroniserings- eller oppgraderings-URL-en.
SERV	Vertsnavnet til målserver for forespørsler, som hentes etter analyse av resynkroniserings- eller oppgraderings-URL-en.
SERVIP	IP-adressen til målserver for forespørsler, som hentes etter analyse av resynkroniserings- eller oppgraderings-URL-en, muligens etter DNS-oppslag.
PORT	UDP/TCP-porten til målserver for forespørsler, som hentes etter analyse av resynkroniserings- eller oppgraderings-URL-en.
PATH	Filbanen til målserver for forespørsler, som hentes etter analyse av resynkroniserings- eller oppgraderings-URL-en.
ERR	Resultatmelding for resynkroniserings- eller oppgraderingsforsøk. Benyttes bare til å generere syslog-meldinger. Verdien beholdes i variabelen UPGERR til bruk ved oppgraderingsforsøk.
UIDn	Innholdet i konfigurasjonsparameteren Line n UserID.
EMS	Extension Mobility-status
MUID	Bruker-ID for Extension Mobility
MPWD	Extension Mobility-passord

Intern feil-koder

Telefonen definerer en rekke internfeilkoder (X00–X99) for å forenkle konfigurasjonen gjennom å gi mer detaljert kontroll over virkemåten til enheten i visse feilsituasjoner.

Parameternavn	Beskrivelse og standardverdi
X00	Transportlagfeil (eller ICMP) under sending av SIP-forespørsel.
X20	SIP-forespørselen får tidsavbrudd under venting på svar.
X40	Generelle SIP-protokollfeil (for eksempel uakseptabel kodek i SDP i 200- og ACK-meldinger, eller tidsavbrudd under venting på ACK).
X60	Det oppringte nummeret er ugyldig ifølge den angitte oppringingsplanen.



TILLEGG A

Eksempel på konfigurasjonsprofiler

Eksempel på XML åpent format

```
<flat-profile>
 <!--  System Configuration  -->
<Restricted_Access_Domains ua="na"/>
<Enable_Web_Server ua="na">Yes</Enable_Web_Server>
<Enable_Protocol ua="na">Http</Enable_Protocol>
<!--  available options: Http|Https  -->
<Enable_Direct_Action_Url ua="na">Yes</Enable_Direct_Action_Url>
<Session_Max_Timeout ua="na">3600</Session_Max_Timeout>
<Session_Idle_Timeout ua="na">3600</Session_Idle_Timeout>
<Web_Server_Port ua="na">80</Web_Server_Port>
<Enable_Web_Admin_Access ua="na">Yes</Enable_Web_Admin_Access>
 <!--  <Admin_Password ua="na"/>  -->
 <!--  <User_Password ua="rw"/>  -->
<Phone-UI-readonly ua="na">No</Phone-UI-readonly>
<Phone-UI-User-Mode ua="na">No</Phone-UI-User-Mode>
<User_Password_Prompt ua="na">Yes</User_Password_Prompt>
<Block_Nonproxy_SIP ua="na">No</Block_Nonproxy_SIP>
 <!--  Power Settings  -->
<PoE_Power_Required ua="na">Normal</PoE_Power_Required>
<!--  available options: Normal|Maximum  -->
 <!--  Network Settings  -->
<IP_Mode ua="rw">Dual Mode</IP_Mode>
<!--  available options: IPv4 Only|IPv6 Only|Dual Mode  -->
 <!--  IPv4 Settings  -->
<Connection_Type ua="rw">DHCP</Connection_Type>
<!--  available options: DHCP|Static IP  -->
<Static_IP ua="rw"/>
<NetMask ua="rw"/>
<Gateway ua="rw"/>
<Primary_DNS ua="rw"/>
<Secondary_DNS ua="rw"/>
 <!--  IPv6 Settings  -->
<IPv6_Connection_Type ua="rw">DHCP</IPv6_Connection_Type>
<!--  available options: DHCP|Static IP  -->
<IPv6_Static_IP ua="rw"/>
<Prefix_Length ua="rw">1</Prefix_Length>
<IPv6_Gateway ua="rw"/>
<IPv6_Primary_DNS ua="rw"/>
<IPv6_Secondary_DNS ua="rw"/>
<Broadcast_Echo ua="rw">Disabled</Broadcast_Echo>
```

Eksempel på konfigurasjonsprofiler

```
<!--  available options: Disabled|Enabled  -->
<Auto_Config ua="rw">Enabled</Auto_Config>
<!--  available options: Disabled|Enabled  -->
 <!--  802.1X Authentication  -->
<Enable_802.1X_Authentication ua="rw">No</Enable_802.1X_Authentication>
 <!--  Optional Network Configuration  -->
<Host_Name ua="rw"/>
<Domain ua="rw"/>
<DNS_Server_Order ua="na">Manual,DHCP</DNS_Server_Order>
<!--  available options: Manual|Manual,DHCP|DHCP,Manual  -->
<DNS_Query_Mode ua="na">Parallel</DNS_Query_Mode>
<!--  available options: Parallel|Sequential  -->
<DNS_Caching_Enable ua="na">Yes</DNS_Caching_Enable>
<Switch_Port_Config ua="na">AUTO</Switch_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_Port_Config ua="na">AUTO</PC_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_PORT_Enable ua="na">Yes</PC_PORT_Enable>
<Enable_PC_Port_Mirror ua="na">No</Enable_PC_Port_Mirror>
<Syslog_Server ua="na"/>
<Syslog_Identifier ua="na">None</Syslog_Identifier>
<!--  available options: None|$MA|$MAU|$MAC|$SN  -->
<Debug_Level ua="na">NOTICE</Debug_Level>
<!--
 available options: EMERGENCY|ALERT|CRITICAL|ERROR|WARNING|NOTICE|INFO|DEBUG
-->
<Primary_NTP_Server ua="rw"/>
<Secondary_NTP_Server ua="rw"/>
<Enable_SSLv3 ua="na">No</Enable_SSLv3>
<Use_Config_TOS ua="na">No</Use_Config_TOS>
 <!--  VLAN Settings  -->
<Enable_VLAN ua="rw">No</Enable_VLAN>
<VLAN_ID ua="rw">1</VLAN_ID>
<PC_Port_VLAN_ID ua="na">1</PC_Port_VLAN_ID>
<Enable_CDP ua="na">Yes</Enable_CDP>
<Enable_LLDP-MED ua="na">Yes</Enable_LLDP-MED>
<Network_Startup_Delay ua="na">3</Network_Startup_Delay>
<DHCP_VLAN_Option ua="na"/>
 <!--  Wi-Fi Settings  -->
 <!--  Wi-Fi Profile 1  -->
 <!--  Wi-Fi Profile 2  -->
 <!--  Wi-Fi Profile 3  -->
 <!--  Wi-Fi Profile 4  -->
 <!--  Inventory Settings  -->
<Asset_ID ua="na"/>
 <!--  SIP Parameters  -->
<Max_Forward ua="na">70</Max_Forward>
<Max_Redirection ua="na">5</Max_Redirection>
<Max_Auth ua="na">2</Max_Auth>
<SIP_User_Agent_Name ua="na">$VERSION</SIP_User_Agent_Name>
<SIP_Server_Name ua="na">$VERSION</SIP_Server_Name>
<SIP_Reg_User_Agent_Name ua="na"/>
<SIP_Accept_Language ua="na"/>
<DTMF_Relay_MIME_Type ua="na">application/dtmf-relay</DTMF_Relay_MIME_Type>
<Hook_Flash_MIME_Type ua="na">application/hook-flash</Hook_Flash_MIME_Type>
<Remove_Last_Reg ua="na">No</Remove_Last_Reg>
<Use_Compact_Header ua="na">No</Use_Compact_Header>
<Escape_Display_Name ua="na">No</Escape_Display_Name>
<Talk_Package ua="na">No</Talk_Package>
<Hold_Package ua="na">No</Hold_Package>
```

```
<Conference_Package ua="na">No</Conference_Package>
<RFC_2543_Call_Hold ua="na">Yes</RFC_2543_Call_Hold>
<Random_REG_CID_on_Reboot ua="na">No</Random_REG_CID_on_Reboot>
<SIP_TCP_Port_Min ua="na">5060</SIP_TCP_Port_Min>
<SIP_TCP_Port_Max ua="na">5080</SIP_TCP_Port_Max>
<Caller_ID_Header ua="na">PAID-RPID-FROM</Caller_ID_Header>
<!--
 available options: PAID-RPID-FROM|PAID-FROM|RPID-PAID-FROM|RPID-FROM|FROM
-->
<Hold_Target_Before_Refer ua="na">No</Hold_Target_Before_Refer>
<Dialog_SDP_Enable ua="na">No</Dialog_SDP_Enable>
<Keep_Referee_When_Refer_Failed ua="na">No</Keep_Referee_When_Refer_Failed>
<Display_Diversion_Info ua="na">No</Display_Diversion_Info>
<Display_Anonymous_From_Header ua="na">No</Display_Anonymous_From_Header>
<Sip_Accept_Encoding ua="na">none</Sip_Accept_Encoding>
<!--  available options: none|gzip  -->
<SIP_IP_Preference ua="na">IPv4</SIP_IP_Preference>
<!--  available options: IPv4|IPv6  -->
<Disable_Local_Name_To_Header ua="na">No</Disable_Local_Name_To_Header>
 <!--  SIP Timer Values (sec)  -->
<SIP_T1 ua="na">.5</SIP_T1>
<SIP_T2 ua="na">4</SIP_T2>
<SIP_T4 ua="na">5</SIP_T4>
<SIP_Timer_B ua="na">16</SIP_Timer_B>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
<SIP_Timer_H ua="na">16</SIP_Timer_H>
<SIP_Timer_D ua="na">16</SIP_Timer_D>
<SIP_Timer_J ua="na">16</SIP_Timer_J>
<INVITE_Expires ua="na">240</INVITE_Expires>
<ReINVITE_Expires ua="na">30</ReINVITE_Expires>
<Reg_Min_Expires ua="na">1</Reg_Min_Expires>
<Reg_Max_Expires ua="na">7200</Reg_Max_Expires>
<Reg_Retry_Intvl ua="na">30</Reg_Retry_Intvl>
<Reg_Retry_Long_Intvl ua="na">1200</Reg_Retry_Long_Intvl>
<Reg_Retry_Random_Delay ua="na">0</Reg_Retry_Random_Delay>
<Reg_Retry_Long_Random_Delay ua="na">0</Reg_Retry_Long_Random_Delay>
<Reg_Retry_Intvl_Cap ua="na">0</Reg_Retry_Intvl_Cap>
<Sub_Min_Expires ua="na">10</Sub_Min_Expires>
<Sub_Max_Expires ua="na">7200</Sub_Max_Expires>
<Sub_Retry_Intvl ua="na">10</Sub_Retry_Intvl>
 <!--  Response Status Code Handling  -->
<Try_Backup_RSC ua="na"/>
<Retry_Reg_RSC ua="na"/>
 <!--  RTP Parameters  -->
<RTP_Port_Min ua="na">16384</RTP_Port_Min>
<RTP_Port_Max ua="na">16482</RTP_Port_Max>
<RTP_Packet_Size ua="na">0.030</RTP_Packet_Size>
<Max_RTP_ICMP_Err ua="na">0</Max_RTP_ICMP_Err>
<RTCP_Tx_Interval ua="na">0</RTCP_Tx_Interval>
<SDP_IP_Preference ua="na">IPv4</SDP_IP_Preference>
<!--  available options: IPv4|IPv6  -->
 <!--  SDP Payload Types  -->
<G711u_Codec_Name ua="na">PCMU</G711u_Codec_Name>
<G711a_Codec_Name ua="na">PCMA</G711a_Codec_Name>
<G729a_Codec_Name ua="na">G729a</G729a_Codec_Name>
<G729b_Codec_Name ua="na">G729ab</G729b_Codec_Name>
<G722_Codec_Name ua="na">G722</G722_Codec_Name>
<G722.2_Codec_Name ua="na">AMR-WB</G722.2_Codec_Name>
<iLBC_Codec_Name ua="na">iLBC</iLBC_Codec_Name>
<OPUS_Codec_Name ua="na">OPUS</OPUS_Codec_Name>
<AVT_Codec_Name ua="na">telephone-event</AVT_Codec_Name>
<G722.2_Dynamic_Payload ua="na">96</G722.2_Dynamic_Payload>
<G722.2_OA_Dynamic_Payload ua="na">103</G722.2_OA_Dynamic_Payload>
<iLBC_Dynamic_Payload ua="na">97</iLBC_Dynamic_Payload>
```

Eksempel på konfigurasjonsprofiler

```
<iLBC_30ms_Dynamic_Payload ua="na">105</iLBC_30ms_Dynamic_Payload>
<OPUS_Dynamic_Payload ua="na">99</OPUS_Dynamic_Payload>
<AVT_Dynamic_Payload ua="na">101</AVT_Dynamic_Payload>
<AVT_16kHz_Dynamic_Payload ua="na">107</AVT_16kHz_Dynamic_Payload>
<AVT_48kHz_Dynamic_Payload ua="na">108</AVT_48kHz_Dynamic_Payload>
<INFOREQ_Dynamic_Payload ua="na"/>
 <!--  NAT Support Parameters  -->
<Handle_VIA_received ua="na">No</Handle_VIA_received>
<Handle_VIA_rport ua="na">No</Handle_VIA_rport>
<Insert_VIA_received ua="na">No</Insert_VIA_received>
<Insert_VIA_rport ua="na">No</Insert_VIA_rport>
<Substitute_VIA_Addr ua="na">No</Substitute_VIA_Addr>
<Send_Resp_To_Src_Port ua="na">No</Send_Resp_To_Src_Port>
<STUN_Enable ua="na">No</STUN_Enable>
<STUN_Test_Enable ua="na">No</STUN_Test_Enable>
<STUN_Server ua="na"/>
<EXT_IP ua="na"/>
<EXT_RTP_Port_Min ua="na">0</EXT_RTP_Port_Min>
<NAT_Keep_Alive_Intvl ua="na">15</NAT_Keep_Alive_Intvl>
<Redirect_Keep_Alive ua="na">No</Redirect_Keep_Alive>
 <!--  Configuration Profile  -->
<Provision_Enable ua="na">Yes</Provision_Enable>
<Resync_On_Reset ua="na">Yes</Resync_On_Reset>
<Resync_Random_Delay ua="na">2</Resync_Random_Delay>
<Resync_At__HHmm_ ua="na"/>
<Resync_At_Random_Delay ua="na">30</Resync_At_Random_Delay>
<Resync_Periodic ua="na">60</Resync_Periodic>
<Resync_Error_Retry_Delay ua="na">360</Resync_Error_Retry_Delay>
<Forced_Resync_Delay ua="na">1440</Forced_Resync_Delay>
<Resync_From_SIP ua="na">Yes</Resync_From_SIP>
<Resync_After_Upgrade_Attempt ua="na">Yes</Resync_After_Upgrade_Attempt>
<Resync_Trigger_1 ua="na"/>
<Resync_Trigger_2 ua="na"/>
<User_Configurable_Resync ua="na">Yes</User_Configurable_Resync>
<Resync_Fails_On_FNF ua="na">Yes</Resync_Fails_On_FNF>
<Profile_Authentication_Type ua="na">Basic Http Authentication</Profile_Authentication_Type>
<!--
 available options: Disabled|Basic Http Authentication|XSI Authentication
-->
<Profile_Rule ua="na">/$PSN-a.xml</Profile_Rule>
<Profile_Rule_B ua="na">/$PSN-b.xml</Profile_Rule_B>
<Profile_Rule_C ua="na"/>
<Profile_Rule_D ua="na"/>
<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>
<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>
<Log_Request_Msg ua="na">
$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH
</Log_Request_Msg>
<Log_Success_Msg ua="na">
$PN $MAC -- Successful resync $SCHEME://$SERVIP:$PORT$PATH
</Log_Success_Msg>
<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed: $ERR</Log_Failure_Msg>
 <!--  Upload Configuration Options  -->
<Report_Rule ua="na"/>
<HTTP_Report_Method ua="na">POST</HTTP_Report_Method>
<!--  available options: POST|PUT  -->
<Report_To_Server ua="na">On Request</Report_To_Server>
<!--
 available options: On Request|On Local Change|Periodically
-->
<Periodic_Upload_To_Server ua="na">3600</Periodic_Upload_To_Server>
<Upload_Delay_On_Local_Change ua="na">60</Upload_Delay_On_Local_Change>
 <!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
```

```
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na"/>
<Log_Upgrade_Request_Msg ua="na">
$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH
</Log_Upgrade_Request_Msg>
<Log_Upgrade_Success_Msg ua="na">
$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR
</Log_Upgrade_Success_Msg>
<Log_Upgrade_Failure_Msg ua="na">$PN $MAC -- Upgrade failed: $ERR</Log_Upgrade_Failure_Msg>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Peer_Firmware_Sharing_Log_Server ua="na"/>
 <!--  CA Settings  -->
<Custom_CA_Rule ua="na"/>
 <!--  HTTP Settings  -->
<HTTP_User_Agent_Name ua="na">$VERSION ($MA)</HTTP_User_Agent_Name>
 <!--  Problem Report Tool  -->
<PRT_Upload_Rule ua="na"/>
<PRT_Upload_Method ua="na">POST</PRT_Upload_Method>
<!--  available options: POST|PUT  -->
<PRT_Max_Timer ua="na"/>
<PRT_Name ua="na"/>
 <!--  General Purpose Parameters  -->
<GPP_A ua="na"/>
<GPP_B ua="na"/>
<GPP_C ua="na"/>
<GPP_D ua="na"/>
<GPP_E ua="na"/>
<GPP_F ua="na"/>
<GPP_G ua="na"/>
<GPP_H ua="na"/>
<GPP_I ua="na"/>
<GPP_J ua="na"/>
<GPP_K ua="na"/>
<GPP_L ua="na"/>
<GPP_M ua="na"/>
<GPP_N ua="na"/>
<GPP_O ua="na"/>
<GPP_P ua="na"/>
 <!--  Call Progress Tones  -->
<Dial_Tone ua="na">350@-19,440@-19;10(*/0/1+2)</Dial_Tone>
<Outside_Dial_Tone ua="na">420@-16;10(*/0/1)</Outside_Dial_Tone>
<Prompt_Tone ua="na">520@-19,620@-19;10(*/0/1+2)</Prompt_Tone>
<Busy_Tone ua="na">480@-19,620@-19;10(.5/.5/1+2)</Busy_Tone>
<Reorder_Tone ua="na">480@-19,620@-19;10(.25/.25/1+2)</Reorder_Tone>
<Off_Hook_Warning_Tone ua="na">480@-10,620@0;10(.125/.125/1+2)</Off_Hook_Warning_Tone>
<Ring_Back_Tone ua="na">440@-19,480@-19;*(2/4/1+2)</Ring_Back_Tone>
<Call_Waiting_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Waiting_Tone>
<Confirm_Tone ua="na">600@-16;1(.25/.25/1)</Confirm_Tone>
<MWI_Dial_Tone ua="na">350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)</MWI_Dial_Tone>
<Cfwd_Dial_Tone ua="na">350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2)</Cfwd_Dial_Tone>
<Holding_Tone ua="na">600@-19;25(.1/.1/1,.1/.1/1,.1/9.5/1)</Holding_Tone>
<Conference_Tone ua="na">350@-19;20(.1/.1/1,.1/9.7/1)</Conference_Tone>
<Secure_Call_Indication_Tone
ua="na">397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2)</Secure_Call_Indication_Tone>
<Page_Tone ua="na">600@-16;.3(.05/0.05/1)</Page_Tone>
<Alert_Tone ua="na">600@-19;.2(.05/0.05/1)</Alert_Tone>
<Mute_Tone ua="na">600@-19;.2(.1/0.1/1)</Mute_Tone>
<Unmute_Tone ua="na">600@-19;.3(.1/0.1/1)</Unmute_Tone>
<System_Beep ua="na">600@-16;.1(.05/0.05/1)</System_Beep>
<Call_Pickup_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Pickup_Tone>
 <!--  Distinctive Ring Patterns  -->
<Cadence_1 ua="na">60(2/4)</Cadence_1>
<Cadence_2 ua="na">60(.3/.2,1/.2,.3/4)</Cadence_2>
<Cadence_3 ua="na">60(.8/.4,.8/4)</Cadence_3>
```

Eksempel på konfigurasjonsprofiler

```
<Cadence_4 ua="na">60(.4/.2,.3/.2,.8/4)</Cadence_4>
<Cadence_5 ua="na">60(.2/.2,.2/.2,.2/.2,1/4)</Cadence_5>
<Cadence_6 ua="na">60(.2/.4,.2/.4,.2/4)</Cadence_6>
<Cadence_7 ua="na">60(4.5/4)</Cadence_7>
<Cadence_8 ua="na">60(0.25/9.75)</Cadence_8>
<Cadence_9 ua="na">60(.4/.2,.4/2)</Cadence_9>
 <!--  Control Timer Values (sec)  -->
<Reorder_Delay ua="na">255</Reorder_Delay>
<Interdigit_Long_Timer ua="na">10</Interdigit_Long_Timer>
<Interdigit_Short_Timer ua="na">3</Interdigit_Short_Timer>
 <!--  Vertical Service Activation Codes  -->
<Call_Return_Code ua="na">*69</Call_Return_Code>
<Blind_Transfer_Code ua="na">*95</Blind_Transfer_Code>
<Cfwd_All_Act_Code ua="na">*72</Cfwd_All_Act_Code>
<Cfwd_All_Deact_Code ua="na">*73</Cfwd_All_Deact_Code>
<Cfwd_Busy_Act_Code ua="na">*90</Cfwd_Busy_Act_Code>
<Cfwd_Busy_Deact_Code ua="na">*91</Cfwd_Busy_Deact_Code>
<Cfwd_No_Ans_Act_Code ua="na">*92</Cfwd_No_Ans_Act_Code>
<Cfwd_No_Ans_Deact_Code ua="na">*93</Cfwd_No_Ans_Deact_Code>
<CW_Act_Code ua="na">*56</CW_Act_Code>
<CW_Deact_Code ua="na">*57</CW_Deact_Code>
<CW_Per_Call_Act_Code ua="na">*71</CW_Per_Call_Act_Code>
<CW_Per_Call_Deact_Code ua="na">*70</CW_Per_Call_Deact_Code>
<Block_CID_Act_Code ua="na">*61</Block_CID_Act_Code>
<Block_CID_Deact_Code ua="na">*62</Block_CID_Deact_Code>
<Block_CID_Per_Call_Act_Code ua="na">*81</Block_CID_Per_Call_Act_Code>
<Block_CID_Per_Call_Deact_Code ua="na">*82</Block_CID_Per_Call_Deact_Code>
<Block_ANC_Act_Code ua="na">*77</Block_ANC_Act_Code>
<Block_ANC_Deact_Code ua="na">*87</Block_ANC_Deact_Code>
<DND_Act_Code ua="na">*78</DND_Act_Code>
<DND_Deact_Code ua="na">*79</DND_Deact_Code>
<Secure_All_Call_Act_Code ua="na">*16</Secure_All_Call_Act_Code>
<Secure_No_Call_Act_Code ua="na">*17</Secure_No_Call_Act_Code>
<Secure_One_Call_Act_Code ua="na">*18</Secure_One_Call_Act_Code>
<Secure_One_Call_Deact_Code ua="na">*19</Secure_One_Call_Deact_Code>
<Paging_Code ua="na">*96</Paging_Code>
<Call_Park_Code ua="na">*68</Call_Park_Code>
<Call_Pickup_Code ua="na">*97</Call_Pickup_Code>
<Call_Unpark_Code ua="na">*88</Call_Unpark_Code>
<Group_Call_Pickup_Code ua="na">*98</Group_Call_Pickup_Code>
<Referral_Services_Codes ua="na"/>
<Feature_Dial_Services_Codes ua="na"/>
 <!--  Vertical Service Announcement Codes  -->
<Service_Annc_Base_Number ua="na"/>
<Service_Annc_Extension_Codes ua="na"/>
 <!--  Outbound Call Codec Selection Codes  -->
<Prefer_G711u_Code ua="na">*017110</Prefer_G711u_Code>
<Force_G711u_Code ua="na">*027110</Force_G711u_Code>
<Prefer_G711a_Code ua="na">*017111</Prefer_G711a_Code>
<Force_G711a_Code ua="na">*027111</Force_G711a_Code>
<Prefer_G722_Code ua="na">*01722</Prefer_G722_Code>
<Force_G722_Code ua="na">*02722</Force_G722_Code>
<Prefer_G722.2_Code ua="na">*01724</Prefer_G722.2_Code>
<Force_G722.2_Code ua="na">*02724</Force_G722.2_Code>
<Prefer_G729a_Code ua="na">*01729</Prefer_G729a_Code>
<Force_G729a_Code ua="na">*02729</Force_G729a_Code>
<Prefer_iLBC_Code ua="na">*01016</Prefer_iLBC_Code>
<Force_iLBC_Code ua="na">*02016</Force_iLBC_Code>
<Prefer_OPUS_Code ua="na">*01056</Prefer_OPUS_Code>
<Force_OPUS_Code ua="na">*02056</Force_OPUS_Code>
 <!--  Time  -->
<Set_Local_Date__mm_dd_yyyy_ ua="na"/>
<Set_Local_Time__HH_mm_ ua="na"/>
<Time_Zone ua="na">GMT-06:00</Time_Zone>
```

Eksempel på konfigurasjonsprofiler

```
<!--
 available options:
[illegible]

-->
<Time_Offset__HH_mm_ ua="na">-00/08</Time_Offset__HH_mm_>
<Ignore_DHCP_Time_Offset ua="na">Yes</Ignore_DHCP_Time_Offset>
<Daylight_Saving_Time_Rule
ua="na">start=3/-1/7/2;end=10/-1/7/2;save=1</Daylight_Saving_Time_Rule>
<Daylight_Saving_Time_Enable ua="na">Yes</Daylight_Saving_Time_Enable>
 <!--  Language  -->
<Dictionary_Server_Script ua="na"/>
<Language_Selection ua="na">English-US</Language_Selection>
<Locale ua="na">en-US</Locale>
<!--
 available options:
en-US|en-CA|en-AU|en-GB|fr-FR|fr-CA|es-ES|it-IT|de-DE|nn-NO|pt-PT|nl-NL|sv-SE|pt-BZ|es-MX|en-NZ|da-DK|ru-RU|pl-PL|tr-TR|cs-CZ|hu-HU|fi-FI|sk-SK|bg-BG|hr-HR|ja-JP|ko-KR|zh-CN|zh-HK

-->
 <!--  General  -->
<Station_Name ua="na">arupiSSomSok</Station_Name>
<Station_Display_Name ua="na">RCDN Time</Station_Display_Name>
<Voice_Mail_Number ua="na"/>
<WideBand_Handset_Enable ua="na">No</WideBand_Handset_Enable>
 <!--  Video Configuration  -->
 <!--  Handsfree  -->
<Bluetooth_Mode ua="na">Phone</Bluetooth_Mode>
<!--  available options: Phone|Handsfree|Both  -->
<Line ua="na">5</Line>
<!--
 available options: 1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|Disabled
-->
<Extension_1_ ua="na">1</Extension_1_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_1_ ua="na">$USER hot</Short_Name_1_>
<Share_Call_Appearance_1_ ua="na">private</Share_Call_Appearance_1_>
<!--  available options: private|shared  -->
<Extended_Function_1_ ua="na"/>
<Extension_2_ ua="na">2</Extension_2_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_2_ ua="na">$USER</Short_Name_2_>
<Share_Call_Appearance_2_ ua="na">private</Share_Call_Appearance_2_>
<!--  available options: private|shared  -->
<Extended_Function_2_ ua="na"/>
<Extension_3_ ua="na">3</Extension_3_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_3_ ua="na">$USER</Short_Name_3_>
<Share_Call_Appearance_3_ ua="na">private</Share_Call_Appearance_3_>
<!--  available options: private|shared  -->
<Extended_Function_3_ ua="na"/>
<Extension_4_ ua="na">4</Extension_4_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_4_ ua="na">$USER</Short_Name_4_>
<Share_Call_Appearance_4_ ua="na">private</Share_Call_Appearance_4_>
<!--  available options: private|shared  -->
<Extended_Function_4_ ua="na"/>
 <!--  Miscellaneous Line Key Settings  -->
<Line_ID_Mapping ua="na">Vertical First</Line_ID_Mapping>
<!--  available options: Horizontal First|Vertical First  -->
<SCA_Barge-In-Enable ua="na">No</SCA_Barge-In-Enable>
<SCA_Sticky_Auto_Line_Seize ua="na">No</SCA_Sticky_Auto_Line_Seize>
<Call_Appearances_Per_Line ua="na">2</Call_Appearances_Per_Line>
<!--  available options: 2|3|4|5|6|7|8|9|10  -->
 <!--  Supplementary Services  -->
```

Eksempel på konfigurasjonsprofiler

```
<Conference_Serv ua="na">Yes</Conference_Serv>
<Attn_Transfer_Serv ua="na">Yes</Attn_Transfer_Serv>
<Blind_Transfer_Serv ua="na">Yes</Blind_Transfer_Serv>
<DND_Serv ua="na">Yes</DND_Serv>
<Block_ANC_Serv ua="na">Yes</Block_ANC_Serv>
<Block_CID_Serv ua="na">Yes</Block_CID_Serv>
<Secure_Call_Serv ua="na">Yes</Secure_Call_Serv>
<Cfwd_All_Serv ua="na">Yes</Cfwd_All_Serv>
<Cfwd_Busy_Serv ua="na">Yes</Cfwd_Busy_Serv>
<Cfwd_No_Ans_Serv ua="na">Yes</Cfwd_No_Ans_Serv>
<Paging_Serv ua="na">Yes</Paging_Serv>
<Call_Park_Serv ua="na">Yes</Call_Park_Serv>
<Call_Pick_Up_Serv ua="na">Yes</Call_Pick_Up_Serv>
<ACD_Login_Serv ua="na">No</ACD_Login_Serv>
<Group_Call_Pick_Up_Serv ua="na">Yes</Group_Call_Pick_Up_Serv>
<Service_Annc_Serv ua="na">No</Service_Annc_Serv>
<Call_Recording_Serv ua="na">No</Call_Recording_Serv>
<Reverse_Phone_Lookup_Serv ua="na">Yes</Reverse_Phone_Lookup_Serv>
 <!--  Ringtone  -->
<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>
<Ring2 ua="na">n=Chirp 1;w=file://chirp1.raw;c=1</Ring2>
<Ring3 ua="na">n=Chirp 2;w=file://chirp2.raw;c=1</Ring3>
<Ring4 ua="na">n=Delight;w=file://Delight.rwb;c=1</Ring4>
<Ring5 ua="na">n=Evolve;w=file://Evolve.rwb;c=1</Ring5>
<Ring6 ua="na">n=Mellow;w=file://Mellow.rwb;c=1</Ring6>
<Ring7 ua="na">n=Mischief;w=file://Mischief.rwb;c=1</Ring7>
<Ring8 ua="na">n=Reflections;w=file://Reflections.rwb;c=1</Ring8>
<Ring9 ua="na">n=Ringer;w=file://Ringer.rwb;c=1</Ring9>
<Ring10 ua="na">n=Ascent;w=file://Ascent.rwb;c=1</Ring10>
<Ring11 ua="na">n=Are you there;w=file://AreYouThereF.raw;c=1</Ring11>
<Ring12 ua="na">n=Chime;w=file://Chime.raw;c=1</Ring12>
<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>
 <!--  Extension Mobility  -->
<EM_Enable ua="na">No</EM_Enable>
<EM_User_Domain ua="na"/>
<Session_Timer_m_ ua="na">480</Session_Timer_m_>
<Countdown_Timer_s_ ua="na">10</Countdown_Timer_s_>
<Preferred_Password_Input_Mode ua="na">Alpha-numeric</Preferred_Password_Input_Mode>
<!--  available options: Alphanumeric|Numeric  -->
 <!--  XSI Phone Service  -->
<XSI_Host_Server ua="na"/>
<XSI_Authentication_Type ua="na">Login Credentials</XSI_Authentication_Type>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID ua="na"/>
 <!--  <Login_Password ua="na"/>  -->
<SIP_Auth_ID ua="na"/>
 <!--  <SIP_Password ua="na"/>  -->
<Directory_Enable ua="na">No</Directory_Enable>
<Directory_Name ua="na"/>
<Directory_Type ua="na">Enterprise</Directory_Type>
<!--
 available options: Enterprise|Group|Personal|Enterprise Common|Group Common
-->
<CallLog_Enable ua="na">No</CallLog_Enable>
<CallLog_Associated_Line ua="na">1</CallLog_Associated_Line>
<!--  available options: 1|2|3|4  -->
<Display_Recents_From ua="na">Phone</Display_Recents_From>
<!--  available options: Phone|Server  -->
 <!--  Broadsoft XMPP  -->
<XMPP_Enable ua="na">No</XMPP_Enable>
<XMPP_Server ua="na"/>
<XMPP_Port ua="na">5222</XMPP_Port>
```

```
<XMPP_User_ID ua="na"/>
 <!--  <XMPP_Password ua="na"/>  -->
<Login_Invisible ua="na">No</Login_Invisible>
<XMPP_Retry_Interval ua="na">30</XMPP_Retry_Interval>
 <!--  Informacast  -->
<Page_Service_URL ua="na"/>
 <!--  XML Service  -->
<XML_Directory_Service_Name ua="na"/>
<XML_Directory_Service_URL ua="na"/>
<XML_Application_Service_Name ua="na"/>
<XML_Application_Service_URL ua="na"/>
<XML_User_Name ua="na"/>
 <!--  <XML_Password ua="na"/>  -->
<CISCO_XML_EXE_Enable ua="na">No</CISCO_XML_EXE_Enable>
<CISCO_XML_EXE_Auth_Mode ua="na">Local Credential</CISCO_XML_EXE_Auth_Mode>
<!--
 available options: Trusted|Local Credential|Remote Credential
-->
 <!--  Multiple Paging Group Parameters  -->
<Group_Paging_Script ua="na">
pggrp=224.168.168.168:34560;name=All;num=800;listen=yes;
</Group_Paging_Script>
 <!--  LDAP  -->
<LDAP_Dir_Enable ua="na">No</LDAP_Dir_Enable>
<LDAP_Corp_Dir_Name ua="na"/>
<LDAP_Server ua="na"/>
<LDAP_Search_Base ua="na"/>
<LDAP_Client_DN ua="na"/>
<LDAP_Username ua="na"/>
 <!--  <LDAP_Password ua="na"/>  -->
<LDAP_Auth_Method ua="na">None</LDAP_Auth_Method>
<!--  available options: None|Simple|DIGEST-MD5  -->
<LDAP_Last_Name_Filter ua="na"/>
<LDAP_First_Name_Filter ua="na"/>
<LDAP_Search_Item_3 ua="na"/>
<LDAP_Item_3_Filter ua="na"/>
<LDAP_Search_Item_4 ua="na"/>
<LDAP_Item_4_Filter ua="na"/>
<LDAP_Display_Attrs ua="na"/>
<LDAP_Number_Mapping ua="na"/>
 <!--  Programmable Softkeys  -->
<Programmable_Softkey_Enable ua="na">No</Programmable_Softkey_Enable>
<Idle_Key_List ua="na">
em_login;acd_login;acd_logout;astate;avail;unavail;redial;recents;cfwd;dnd;lcr;pickup;gpickup;unpark;em_logout;guestin;guestout;
</Idle_Key_List>
<Missed_Call_Key_List ua="na">lcr|1;miss|4;</Missed_Call_Key_List>
<Off_Hook_Key_List ua="na">
option;redial;cancel;dir;cfwd;dnd;lcr;unpark;pickup;gpickup;
</Off_Hook_Key_List>
<Dialing_Input_Key_List
ua="na">option|1;call|2;delchar|3;cancel|4;left|5;right|6;</Dialing_Input_Key_List>
<Progressing_Key_List ua="na">endcall|2;</Progressing_Key_List>
<Connected_Key_List ua="na">
hold|1;endcall|2;conf|3;xfer|4;bxfer;confLx;xferLx;park;phold;crdstart;crdpause;crdresume;crdstop;dnd;
</Connected_Key_List>
<Start-Xfer_Key_List ua="na">hold|1;endcall|2;xfer|3;dnd;</Start-Xfer_Key_List>
<Start-Conf_Key_List ua="na">hold|1;endcall|2;conf|3;dnd;</Start-Conf_Key_List>
<Conferencing_Key_List ua="na">
hold|1;endcall|2;join|4;phold;crdstart|5;crdpause|5;crdresume|5;crdstop|6;dnd;
</Conferencing_Key_List>
<Releasing_Key_List ua="na">endcall|2;</Releasing_Key_List>
<Hold_Key_List ua="na">resume|1;endcall|2;newcall|3;redial;dir;cfwd;dnd;</Hold_Key_List>
<Ringing_Key_List ua="na">answer|1;ignore|2;</Ringing_Key_List>
<Shared_Active_Key_List
```

Eksempel på konfigurasjonsprofiler

```
ua="na">newcall|1;barge|2;bargesilent|3;cfwd|4;dnd|5;</Shared_Active_Key_List>
<Shared_Held_Key_List ua="na">resume|1;barge|2;cfwd|3;dnd|4;</Shared_Held_Key_List>
<PSK_1 ua="na"/>
<PSK_2 ua="na"/>
<PSK_3 ua="na"/>
<PSK_4 ua="na"/>
<PSK_5 ua="na"/>
<PSK_6 ua="na"/>
<PSK_7 ua="na"/>
<PSK_8 ua="na"/>
<PSK_9 ua="na"/>
<PSK_10 ua="na"/>
<PSK_11 ua="na"/>
<PSK_12 ua="na"/>
<PSK_13 ua="na"/>
<PSK_14 ua="na"/>
<PSK_15 ua="na"/>
<PSK_16 ua="na"/>
 <!--  General  -->
<Line_Enable_1_ ua="na">Yes</Line_Enable_1_>
 <!--  Share Line Appearance  -->
<Share_Ext_1_ ua="na">No</Share_Ext_1_>
<Shared_User_ID_1_ ua="na"/>
<Subscription_Expires_1_ ua="na">3600</Subscription_Expires_1_>
<Restrict_MWI_1_ ua="na">No</Restrict_MWI_1_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_1_ ua="na">No</NAT_Mapping_Enable_1_>
<NAT_Keep_Alive_Enable_1_ ua="na">No</NAT_Keep_Alive_Enable_1_>
<NAT_Keep_Alive_Msg_1_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_1_>
<NAT_Keep_Alive_Dest_1_ ua="na">$PROXY</NAT_Keep_Alive_Dest_1_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_1_ ua="na">0x68</SIP_TOS_DiffServ_Value_1_>
<RTP_TOS_DiffServ_Value_1_ ua="na">0xb8</RTP_TOS_DiffServ_Value_1_>
 <!--  SIP Settings  -->
<SIP_Transport_1_ ua="na">UDP</SIP_Transport_1_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_1_ ua="na">5060</SIP_Port_1_>
<SIP_100REL_Enable_1_ ua="na">No</SIP_100REL_Enable_1_>
<EXT_SIP_Port_1_ ua="na">0</EXT_SIP_Port_1_>
<Auth_Resync-Reboot_1_ ua="na">Yes</Auth_Resync-Reboot_1_>
<SIP_Proxy-Require_1_ ua="na"/>
<SIP_Remote-Party-ID_1_ ua="na">No</SIP_Remote-Party-ID_1_>
<Referor_Bye_Delay_1_ ua="na">4</Referor_Bye_Delay_1_>
<Refer-To_Target_Contact_1_ ua="na">No</Refer-To_Target_Contact_1_>
<Referee_Bye_Delay_1_ ua="na">0</Referee_Bye_Delay_1_>
<Refer_Target_Bye_Delay_1_ ua="na">0</Refer_Target_Bye_Delay_1_>
<Sticky_183_1_ ua="na">No</Sticky_183_1_>
<Auth_INVITE_1_ ua="na">No</Auth_INVITE_1_>
<Ntfy_Refer_On_1xx-To-Inv_1_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_1_>
<Set_G729_annexb_1_ ua="na">yes</Set_G729_annexb_1_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_1_ ua="na"/>
<VQ_Report_Interval_1_ ua="na">0</VQ_Report_Interval_1_>
<User_Equal_Phone_1_ ua="na">No</User_Equal_Phone_1_>
<Call_Recording_Protocol_1_ ua="na">SIPREC</Call_Recording_Protocol_1_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_1_ ua="na">Disabled</Privacy_Header_1_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_1_ ua="na">No</P-Early-Media_Support_1_>
 <!--  Call Feature Settings  -->
```

```
<Blind_Attn-Xfer_Enable_1_ ua="na">No</Blind_Attn-Xfer_Enable_1_>
<Message_Waiting_1_ ua="na">No</Message_Waiting_1_>
<Auth_Page_1_ ua="na">No</Auth_Page_1_>
<Default_Ring_1_ ua="rw">1</Default_Ring_1_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_1_ ua="na"/>
<Conference_Bridge_URL_1_ ua="na"/>
<Conference_Single_Hardkey_1_ ua="na">No</Conference_Single_Hardkey_1_>
 <!--  <Auth_Page_Password_1_ ua="na"/>  -->
<Mailbox_ID_1_ ua="na"/>
<Voice_Mail_Server_1_ ua="na"/>
<Voice_Mail_Subscribe_Interval_1_ ua="na">86400</Voice_Mail_Subscribe_Interval_1_>
<Auto_Ans_Page_On_Active_Call_1_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_1_>
<Feature_Key_Sync_1_ ua="na">No</Feature_Key_Sync_1_>
<Call_Park_Monitor_Enable_1_ ua="na">No</Call_Park_Monitor_Enable_1_>
<Enable_Broadsoft_Hoteling_1_ ua="na">No</Enable_Broadsoft_Hoteling_1_>
<Hoteling_Subscription_Expires_1_ ua="na">3600</Hoteling_Subscription_Expires_1_>
<Secure_Call_Option_1_ ua="na">Optional</Secure_Call_Option_1_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_1_ ua="na">No</Broadsoft_ACD_1_>
<Call_Information_Enable_1_ ua="na">No</Call_Information_Enable_1_>
<Disposition_Code_Enable_1_ ua="na">No</Disposition_Code_Enable_1_>
<Trace_Enable_1_ ua="na">No</Trace_Enable_1_>
<Emergency_Escalation_Enable_1_ ua="na">No</Emergency_Escalation_Enable_1_>
<Queue_Status_Notification_Enable_1_ ua="na">No</Queue_Status_Notification_Enable_1_>
 <!--  Proxy and Registration  -->
<Proxy_1_ ua="na">as1bsoft.sipurash.com</Proxy_1_>
<Outbound_Proxy_1_ ua="na"/>
<Alternate_Proxy_1_ ua="na"/>
<Alternate_Outbound_Proxy_1_ ua="na"/>
<Use_OB_Proxy_In_Dialog_1_ ua="na">Yes</Use_OB_Proxy_In_Dialog_1_>
<Register_1_ ua="na">Yes</Register_1_>
<Make_Call_Without_Reg_1_ ua="na">No</Make_Call_Without_Reg_1_>
<Register_Expires_1_ ua="na">3600</Register_Expires_1_>
<Ans_Call_Without_Reg_1_ ua="na">No</Ans_Call_Without_Reg_1_>
<Use_DNS_SRV_1_ ua="na">No</Use_DNS_SRV_1_>
<DNS_SRV_Auto_Prefix_1_ ua="na">Yes</DNS_SRV_Auto_Prefix_1_>
<Proxy_Fallback_Intvl_1_ ua="na">3600</Proxy_Fallback_Intvl_1_>
<Proxy_Redundancy_Method_1_ ua="na">Normal</Proxy_Redundancy_Method_1_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_1_ ua="na">No</Dual_Registration_1_>
<Auto_Register_When_Failover_1_ ua="na">No</Auto_Register_When_Failover_1_>
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
 <!--  Subscriber Information  -->
<Display_Name_1_ ua="na"/>
<User_ID_1_ ua="na">4085263127</User_ID_1_>
 <!--  <Password_1_ ua="na">**********</Password_1_>  -->
<Auth_ID_1_ ua="na">AUN3127</Auth_ID_1_>
<Reversed_Auth_Realm_1_ ua="na"/>
<SIP_URI_1_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_1_ ua="na"/>
<XSI_Authentication_Type_1_ ua="na">Login Credentials</XSI_Authentication_Type_1_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_1_ ua="na"/>
 <!--  <Login_Password_1_ ua="na"/>  -->
<Anywhere_Enable_1_ ua="na">No</Anywhere_Enable_1_>
<Block_CID_Enable_1_ ua="na">No</Block_CID_Enable_1_>
<DND_Enable_1_ ua="na">No</DND_Enable_1_>
```

Eksempel på konfigurasjonsprofiler

```
<CFWD_Enable_1_ ua="na">No</CFWD_Enable_1_>
 <!--  Audio Configuration  -->
<Preferred_Codec_1_ ua="na">G711u</Preferred_Codec_1_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_1_ ua="na">No</Use_Pref_Codec_Only_1_>
<Second_Preferred_Codec_1_ ua="na">Unspecified</Second_Preferred_Codec_1_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_1_ ua="na">Unspecified</Third_Preferred_Codec_1_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_1_ ua="na">Yes</G711u_Enable_1_>
<G711a_Enable_1_ ua="na">Yes</G711a_Enable_1_>
<G729a_Enable_1_ ua="na">Yes</G729a_Enable_1_>
<G722_Enable_1_ ua="na">Yes</G722_Enable_1_>
<G722.2_Enable_1_ ua="na">Yes</G722.2_Enable_1_>
<iLBC_Enable_1_ ua="na">Yes</iLBC_Enable_1_>
<OPUS_Enable_1_ ua="na">Yes</OPUS_Enable_1_>
<Silence_Supp_Enable_1_ ua="na">No</Silence_Supp_Enable_1_>
<DTMF_Tx_Method_1_ ua="na">Auto</DTMF_Tx_Method_1_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_1_ ua="na">Default</Codec_Negotiation_1_>
<!--  available options: Default|List All  -->
<Encryption_Method_1_ ua="na">AES 128</Encryption_Method_1_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_1_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_1_>
<Caller_ID_Map_1_ ua="na"/>
<Enable_URI_Dialing_1_ ua="na">No</Enable_URI_Dialing_1_>
<Emergency_Number_1_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_1_ ua="na"/>
<Primary_Request_URL_1_ ua="na"/>
<Secondary_Request_URL_1_ ua="na"/>
 <!--  General  -->
<Line_Enable_2_ ua="na">Yes</Line_Enable_2_>
 <!--  Share Line Appearance  -->
<Share_Ext_2_ ua="na">No</Share_Ext_2_>
<Shared_User_ID_2_ ua="na"/>
<Subscription_Expires_2_ ua="na">3600</Subscription_Expires_2_>
<Restrict_MWI_2_ ua="na">No</Restrict_MWI_2_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_2_ ua="na">No</NAT_Mapping_Enable_2_>
<NAT_Keep_Alive_Enable_2_ ua="na">No</NAT_Keep_Alive_Enable_2_>
<NAT_Keep_Alive_Msg_2_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_2_>
<NAT_Keep_Alive_Dest_2_ ua="na">$PROXY</NAT_Keep_Alive_Dest_2_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_2_ ua="na">0x68</SIP_TOS_DiffServ_Value_2_>
<RTP_TOS_DiffServ_Value_2_ ua="na">0xb8</RTP_TOS_DiffServ_Value_2_>
 <!--  SIP Settings  -->
<SIP_Transport_2_ ua="na">UDP</SIP_Transport_2_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_2_ ua="na">5061</SIP_Port_2_>
<SIP_100REL_Enable_2_ ua="na">No</SIP_100REL_Enable_2_>
<EXT_SIP_Port_2_ ua="na">0</EXT_SIP_Port_2_>
```

```
<Auth_Resync-Reboot_2_ ua="na">Yes</Auth_Resync-Reboot_2_>
<SIP_Proxy-Require_2_ ua="na"/>
<SIP_Remote-Party-ID_2_ ua="na">No</SIP_Remote-Party-ID_2_>
<Referor_Bye_Delay_2_ ua="na">4</Referor_Bye_Delay_2_>
<Refer-To_Target_Contact_2_ ua="na">No</Refer-To_Target_Contact_2_>
<Referee_Bye_Delay_2_ ua="na">0</Referee_Bye_Delay_2_>
<Refer_Target_Bye_Delay_2_ ua="na">0</Refer_Target_Bye_Delay_2_>
<Sticky_183_2_ ua="na">No</Sticky_183_2_>
<Auth_INVITE_2_ ua="na">No</Auth_INVITE_2_>
<Ntfy_Refer_On_1xx-To-Inv_2_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_2_>
<Set_G729_annexb_2_ ua="na">yes</Set_G729_annexb_2_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_2_ ua="na"/>
<VQ_Report_Interval_2_ ua="na">0</VQ_Report_Interval_2_>
<User_Equal_Phone_2_ ua="na">No</User_Equal_Phone_2_>
<Call_Recording_Protocol_2_ ua="na">SIPREC</Call_Recording_Protocol_2_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_2_ ua="na">Disabled</Privacy_Header_2_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_2_ ua="na">No</P-Early-Media_Support_2_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_2_ ua="na">No</Blind_Attn-Xfer_Enable_2_>
<Message_Waiting_2_ ua="na">No</Message_Waiting_2_>
<Auth_Page_2_ ua="na">No</Auth_Page_2_>
<Default_Ring_2_ ua="rw">1</Default_Ring_2_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_2_ ua="na"/>
<Conference_Bridge_URL_2_ ua="na"/>
<Conference_Single_Hardkey_2_ ua="na">No</Conference_Single_Hardkey_2_>
 <!--  <Auth_Page_Password_2_ ua="na"/>  -->
<Mailbox_ID_2_ ua="na"/>
<Voice_Mail_Server_2_ ua="na"/>
<Voice_Mail_Subscribe_Interval_2_ ua="na">86400</Voice_Mail_Subscribe_Interval_2_>
<Auto_Ans_Page_On_Active_Call_2_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_2_>
<Feature_Key_Sync_2_ ua="na">No</Feature_Key_Sync_2_>
<Call_Park_Monitor_Enable_2_ ua="na">No</Call_Park_Monitor_Enable_2_>
<Enable_Broadsoft_Hoteling_2_ ua="na">No</Enable_Broadsoft_Hoteling_2_>
<Hoteling_Subscription_Expires_2_ ua="na">3600</Hoteling_Subscription_Expires_2_>
<Secure_Call_Option_2_ ua="na">Optional</Secure_Call_Option_2_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_2_ ua="na">No</Broadsoft_ACD_2_>
<Call_Information_Enable_2_ ua="na">No</Call_Information_Enable_2_>
<Disposition_Code_Enable_2_ ua="na">No</Disposition_Code_Enable_2_>
<Trace_Enable_2_ ua="na">No</Trace_Enable_2_>
<Emergency_Escalation_Enable_2_ ua="na">No</Emergency_Escalation_Enable_2_>
<Queue_Status_Notification_Enable_2_ ua="na">No</Queue_Status_Notification_Enable_2_>
 <!--  Proxy and Registration  -->
<Proxy_2_ ua="na">10.74.51.158</Proxy_2_>
<Outbound_Proxy_2_ ua="na"/>
<Alternate_Proxy_2_ ua="na"/>
<Alternate_Outbound_Proxy_2_ ua="na"/>
<Use_OB_Proxy_In_Dialog_2_ ua="na">Yes</Use_OB_Proxy_In_Dialog_2_>
<Register_2_ ua="na">Yes</Register_2_>
<Make_Call_Without_Reg_2_ ua="na">No</Make_Call_Without_Reg_2_>
<Register_Expires_2_ ua="na">360</Register_Expires_2_>
<Ans_Call_Without_Reg_2_ ua="na">No</Ans_Call_Without_Reg_2_>
<Use_DNS_SRV_2_ ua="na">No</Use_DNS_SRV_2_>
```

Eksempel på konfigurasjonsprofiler

```
<DNS_SRV_Auto_Prefix_2_ ua="na">Yes</DNS_SRV_Auto_Prefix_2_>
<Proxy_Fallback_Intvl_2_ ua="na">3600</Proxy_Fallback_Intvl_2_>
<Proxy_Redundancy_Method_2_ ua="na">Normal</Proxy_Redundancy_Method_2_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_2_ ua="na">No</Dual_Registration_2_>
<Auto_Register_When_Failover_2_ ua="na">No</Auto_Register_When_Failover_2_>
<TLS_Name_Validate_2_ ua="na">Yes</TLS_Name_Validate_2_>
 <!--  Subscriber Information  -->
<Display_Name_2_ ua="na"/>
<User_ID_2_ ua="na">158165</User_ID_2_>
 <!--  <Password_2_ ua="na"/>  -->
<Auth_ID_2_ ua="na"/>
<Reversed_Auth_Realm_2_ ua="na"/>
<SIP_URI_2_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_2_ ua="na"/>
<XSI_Authentication_Type_2_ ua="na">Login Credentials</XSI_Authentication_Type_2_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_2_ ua="na"/>
 <!--  <Login_Password_2_ ua="na"/>  -->
<Anywhere_Enable_2_ ua="na">No</Anywhere_Enable_2_>
<Block_CID_Enable_2_ ua="na">No</Block_CID_Enable_2_>
<DND_Enable_2_ ua="na">No</DND_Enable_2_>
<CFWD_Enable_2_ ua="na">No</CFWD_Enable_2_>
 <!--  Audio Configuration  -->
<Preferred_Codec_2_ ua="na">G711u</Preferred_Codec_2_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_2_ ua="na">No</Use_Pref_Codec_Only_2_>
<Second_Preferred_Codec_2_ ua="na">Unspecified</Second_Preferred_Codec_2_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_2_ ua="na">Unspecified</Third_Preferred_Codec_2_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_2_ ua="na">Yes</G711u_Enable_2_>
<G711a_Enable_2_ ua="na">Yes</G711a_Enable_2_>
<G729a_Enable_2_ ua="na">Yes</G729a_Enable_2_>
<G722_Enable_2_ ua="na">Yes</G722_Enable_2_>
<G722.2_Enable_2_ ua="na">Yes</G722.2_Enable_2_>
<iLBC_Enable_2_ ua="na">Yes</iLBC_Enable_2_>
<OPUS_Enable_2_ ua="na">Yes</OPUS_Enable_2_>
<Silence_Supp_Enable_2_ ua="na">No</Silence_Supp_Enable_2_>
<DTMF_Tx_Method_2_ ua="na">Auto</DTMF_Tx_Method_2_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_2_ ua="na">Default</Codec_Negotiation_2_>
<!--  available options: Default|List All  -->
<Encryption_Method_2_ ua="na">AES 128</Encryption_Method_2_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_2_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_2_>
<Caller_ID_Map_2_ ua="na"/>
<Enable_URI_Dialing_2_ ua="na">No</Enable_URI_Dialing_2_>
<Emergency_Number_2_ ua="na"/>
```

```
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_2_ ua="na"/>
<Primary_Request_URL_2_ ua="na"/>
<Secondary_Request_URL_2_ ua="na"/>
 <!--  General  -->
<Line_Enable_3_ ua="na">Yes</Line_Enable_3_>
 <!--  Share Line Appearance  -->
<Share_Ext_3_ ua="na">No</Share_Ext_3_>
<Shared_User_ID_3_ ua="na"/>
<Subscription_Expires_3_ ua="na">3600</Subscription_Expires_3_>
<Restrict_MWI_3_ ua="na">No</Restrict_MWI_3_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_3_ ua="na">No</NAT_Mapping_Enable_3_>
<NAT_Keep_Alive_Enable_3_ ua="na">No</NAT_Keep_Alive_Enable_3_>
<NAT_Keep_Alive_Msg_3_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_3_>
<NAT_Keep_Alive_Dest_3_ ua="na">$PROXY</NAT_Keep_Alive_Dest_3_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_3_ ua="na">0x68</SIP_TOS_DiffServ_Value_3_>
<RTP_TOS_DiffServ_Value_3_ ua="na">0xb8</RTP_TOS_DiffServ_Value_3_>
 <!--  SIP Settings  -->
<SIP_Transport_3_ ua="na">UDP</SIP_Transport_3_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_3_ ua="na">5062</SIP_Port_3_>
<SIP_100REL_Enable_3_ ua="na">No</SIP_100REL_Enable_3_>
<EXT_SIP_Port_3_ ua="na">0</EXT_SIP_Port_3_>
<Auth_Resync-Reboot_3_ ua="na">Yes</Auth_Resync-Reboot_3_>
<SIP_Proxy-Require_3_ ua="na"/>
<SIP_Remote-Party-ID_3_ ua="na">No</SIP_Remote-Party-ID_3_>
<Referor_Bye_Delay_3_ ua="na">4</Referor_Bye_Delay_3_>
<Refer-To_Target_Contact_3_ ua="na">No</Refer-To_Target_Contact_3_>
<Referee_Bye_Delay_3_ ua="na">0</Referee_Bye_Delay_3_>
<Refer_Target_Bye_Delay_3_ ua="na">0</Refer_Target_Bye_Delay_3_>
<Sticky_183_3_ ua="na">No</Sticky_183_3_>
<Auth_INVITE_3_ ua="na">No</Auth_INVITE_3_>
<Ntfy_Refer_On_1xx-To-Inv_3_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_3_>
<Set_G729_annexb_3_ ua="na">yes</Set_G729_annexb_3_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_3_ ua="na"/>
<VQ_Report_Interval_3_ ua="na">0</VQ_Report_Interval_3_>
<User_Equal_Phone_3_ ua="na">No</User_Equal_Phone_3_>
<Call_Recording_Protocol_3_ ua="na">SIPREC</Call_Recording_Protocol_3_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_3_ ua="na">Disabled</Privacy_Header_3_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_3_ ua="na">No</P-Early-Media_Support_3_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_3_ ua="na">No</Blind_Attn-Xfer_Enable_3_>
<Message_Waiting_3_ ua="na">No</Message_Waiting_3_>
<Auth_Page_3_ ua="na">No</Auth_Page_3_>
<Default_Ring_3_ ua="rw">1</Default_Ring_3_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_3_ ua="na"/>
<Conference_Bridge_URL_3_ ua="na"/>
<Conference_Single_Hardkey_3_ ua="na">No</Conference_Single_Hardkey_3_>
 <!--  <Auth_Page_Password_3_ ua="na"/>  -->
<Mailbox_ID_3_ ua="na"/>
<Voice_Mail_Server_3_ ua="na"/>
<Voice_Mail_Subscribe_Interval_3_ ua="na">86400</Voice_Mail_Subscribe_Interval_3_>
```

Eksempel på konfigurasjonsprofiler

```
<Auto_Ans_Page_On_Active_Call_3_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_3_>
<Feature_Key_Sync_3_ ua="na">No</Feature_Key_Sync_3_>
<Call_Park_Monitor_Enable_3_ ua="na">No</Call_Park_Monitor_Enable_3_>
<Enable_Broadsoft_Hoteling_3_ ua="na">No</Enable_Broadsoft_Hoteling_3_>
<Hoteling_Subscription_Expires_3_ ua="na">3600</Hoteling_Subscription_Expires_3_>
<Secure_Call_Option_3_ ua="na">Optional</Secure_Call_Option_3_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_3_ ua="na">No</Broadsoft_ACD_3_>
<Call_Information_Enable_3_ ua="na">No</Call_Information_Enable_3_>
<Disposition_Code_Enable_3_ ua="na">No</Disposition_Code_Enable_3_>
<Trace_Enable_3_ ua="na">No</Trace_Enable_3_>
<Emergency_Escalation_Enable_3_ ua="na">No</Emergency_Escalation_Enable_3_>
<Queue_Status_Notification_Enable_3_ ua="na">No</Queue_Status_Notification_Enable_3_>
 <!--  Proxy and Registration  -->
<Proxy_3_ ua="na"/>
<Outbound_Proxy_3_ ua="na"/>
<Alternate_Proxy_3_ ua="na"/>
<Alternate_Outbound_Proxy_3_ ua="na"/>
<Use_OB_Proxy_In_Dialog_3_ ua="na">Yes</Use_OB_Proxy_In_Dialog_3_>
<Register_3_ ua="na">Yes</Register_3_>
<Make_Call_Without_Reg_3_ ua="na">No</Make_Call_Without_Reg_3_>
<Register_Expires_3_ ua="na">3600</Register_Expires_3_>
<Ans_Call_Without_Reg_3_ ua="na">No</Ans_Call_Without_Reg_3_>
<Use_DNS_SRV_3_ ua="na">No</Use_DNS_SRV_3_>
<DNS_SRV_Auto_Prefix_3_ ua="na">Yes</DNS_SRV_Auto_Prefix_3_>
<Proxy_Fallback_Intvl_3_ ua="na">3600</Proxy_Fallback_Intvl_3_>
<Proxy_Redundancy_Method_3_ ua="na">Normal</Proxy_Redundancy_Method_3_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_3_ ua="na">No</Dual_Registration_3_>
<Auto_Register_When_Failover_3_ ua="na">No</Auto_Register_When_Failover_3_>
<TLS_Name_Validate_3_ ua="na">Yes</TLS_Name_Validate_3_>
 <!--  Subscriber Information  -->
<Display_Name_3_ ua="na"/>
<User_ID_3_ ua="na"/>
 <!--  <Password_3_ ua="na"/>  -->
<Auth_ID_3_ ua="na"/>
<Reversed_Auth_Realm_3_ ua="na"/>
<SIP_URI_3_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_3_ ua="na"/>
<XSI_Authentication_Type_3_ ua="na">Login Credentials</XSI_Authentication_Type_3_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_3_ ua="na"/>
 <!--  <Login_Password_3_ ua="na"/>  -->
<Anywhere_Enable_3_ ua="na">No</Anywhere_Enable_3_>
<Block_CID_Enable_3_ ua="na">No</Block_CID_Enable_3_>
<DND_Enable_3_ ua="na">No</DND_Enable_3_>
<CFWD_Enable_3_ ua="na">No</CFWD_Enable_3_>
 <!--  Audio Configuration  -->
<Preferred_Codec_3_ ua="na">G711u</Preferred_Codec_3_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_3_ ua="na">No</Use_Pref_Codec_Only_3_>
<Second_Preferred_Codec_3_ ua="na">Unspecified</Second_Preferred_Codec_3_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_3_ ua="na">Unspecified</Third_Preferred_Codec_3_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
```

```
-->
<G711u_Enable_3_ ua="na">Yes</G711u_Enable_3_>
<G711a_Enable_3_ ua="na">Yes</G711a_Enable_3_>
<G729a_Enable_3_ ua="na">Yes</G729a_Enable_3_>
<G722_Enable_3_ ua="na">Yes</G722_Enable_3_>
<G722.2_Enable_3_ ua="na">Yes</G722.2_Enable_3_>
<iLBC_Enable_3_ ua="na">Yes</iLBC_Enable_3_>
<OPUS_Enable_3_ ua="na">Yes</OPUS_Enable_3_>
<Silence_Supp_Enable_3_ ua="na">No</Silence_Supp_Enable_3_>
<DTMF_Tx_Method_3_ ua="na">Auto</DTMF_Tx_Method_3_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_3_ ua="na">Default</Codec_Negotiation_3_>
<!--  available options: Default|List All  -->
<Encryption_Method_3_ ua="na">AES 128</Encryption_Method_3_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_3_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_3_>
<Caller_ID_Map_3_ ua="na"/>
<Enable_URI_Dialing_3_ ua="na">No</Enable_URI_Dialing_3_>
<Emergency_Number_3_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_3_ ua="na"/>
<Primary_Request_URL_3_ ua="na"/>
<Secondary_Request_URL_3_ ua="na"/>
 <!--  General  -->
<Line_Enable_4_ ua="na">Yes</Line_Enable_4_>
 <!--  Share Line Appearance  -->
<Share_Ext_4_ ua="na">No</Share_Ext_4_>
<Shared_User_ID_4_ ua="na"/>
<Subscription_Expires_4_ ua="na">3600</Subscription_Expires_4_>
<Restrict_MWI_4_ ua="na">No</Restrict_MWI_4_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_4_ ua="na">No</NAT_Mapping_Enable_4_>
<NAT_Keep_Alive_Enable_4_ ua="na">No</NAT_Keep_Alive_Enable_4_>
<NAT_Keep_Alive_Msg_4_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_4_>
<NAT_Keep_Alive_Dest_4_ ua="na">$PROXY</NAT_Keep_Alive_Dest_4_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_4_ ua="na">0x68</SIP_TOS_DiffServ_Value_4_>
<RTP_TOS_DiffServ_Value_4_ ua="na">0xb8</RTP_TOS_DiffServ_Value_4_>
 <!--  SIP Settings  -->
<SIP_Transport_4_ ua="na">UDP</SIP_Transport_4_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_4_ ua="na">5063</SIP_Port_4_>
<SIP_100REL_Enable_4_ ua="na">No</SIP_100REL_Enable_4_>
<EXT_SIP_Port_4_ ua="na">0</EXT_SIP_Port_4_>
<Auth_Resync-Reboot_4_ ua="na">Yes</Auth_Resync-Reboot_4_>
<SIP_Proxy-Require_4_ ua="na"/>
<SIP_Remote-Party-ID_4_ ua="na">No</SIP_Remote-Party-ID_4_>
<Referor_Bye_Delay_4_ ua="na">4</Referor_Bye_Delay_4_>
<Refer-To_Target_Contact_4_ ua="na">No</Refer-To_Target_Contact_4_>
<Referee_Bye_Delay_4_ ua="na">0</Referee_Bye_Delay_4_>
<Refer_Target_Bye_Delay_4_ ua="na">0</Refer_Target_Bye_Delay_4_>
<Sticky_183_4_ ua="na">No</Sticky_183_4_>
<Auth_INVITE_4_ ua="na">No</Auth_INVITE_4_>
<Ntfy_Refer_On_1xx-To-Inv_4_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_4_>
<Set_G729_annexb_4_ ua="na">yes</Set_G729_annexb_4_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
```

Eksempel på konfigurasjonsprofiler

```
<Voice_Quality_Report_Address_4_ ua="na"/>
<VQ_Report_Interval_4_ ua="na">0</VQ_Report_Interval_4_>
<User_Equal_Phone_4_ ua="na">No</User_Equal_Phone_4_>
<Call_Recording_Protocol_4_ ua="na">SIPREC</Call_Recording_Protocol_4_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_4_ ua="na">Disabled</Privacy_Header_4_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_4_ ua="na">No</P-Early-Media_Support_4_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_4_ ua="na">No</Blind_Attn-Xfer_Enable_4_>
<Message_Waiting_4_ ua="na">No</Message_Waiting_4_>
<Auth_Page_4_ ua="na">No</Auth_Page_4_>
<Default_Ring_4_ ua="rw">1</Default_Ring_4_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_4_ ua="na"/>
<Conference_Bridge_URL_4_ ua="na"/>
<Conference_Single_Hardkey_4_ ua="na">No</Conference_Single_Hardkey_4_>
 <!--  <Auth_Page_Password_4_ ua="na"/>  -->
<Mailbox_ID_4_ ua="na"/>
<Voice_Mail_Server_4_ ua="na"/>
<Voice_Mail_Subscribe_Interval_4_ ua="na">86400</Voice_Mail_Subscribe_Interval_4_>
<Auto_Ans_Page_On_Active_Call_4_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_4_>
<Feature_Key_Sync_4_ ua="na">No</Feature_Key_Sync_4_>
<Call_Park_Monitor_Enable_4_ ua="na">No</Call_Park_Monitor_Enable_4_>
<Enable_Broadsoft_Hoteling_4_ ua="na">No</Enable_Broadsoft_Hoteling_4_>
<Hoteling_Subscription_Expires_4_ ua="na">3600</Hoteling_Subscription_Expires_4_>
<Secure_Call_Option_4_ ua="na">Optional</Secure_Call_Option_4_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_4_ ua="na">No</Broadsoft_ACD_4_>
<Call_Information_Enable_4_ ua="na">No</Call_Information_Enable_4_>
<Disposition_Code_Enable_4_ ua="na">No</Disposition_Code_Enable_4_>
<Trace_Enable_4_ ua="na">No</Trace_Enable_4_>
<Emergency_Escalation_Enable_4_ ua="na">No</Emergency_Escalation_Enable_4_>
<Queue_Status_Notification_Enable_4_ ua="na">No</Queue_Status_Notification_Enable_4_>
 <!--  Proxy and Registration  -->
<Proxy_4_ ua="na">as1bsoft.sipurash.com</Proxy_4_>
<Outbound_Proxy_4_ ua="na"/>
<Alternate_Proxy_4_ ua="na"/>
<Alternate_Outbound_Proxy_4_ ua="na"/>
<Use_OB_Proxy_In_Dialog_4_ ua="na">Yes</Use_OB_Proxy_In_Dialog_4_>
<Register_4_ ua="na">Yes</Register_4_>
<Make_Call_Without_Reg_4_ ua="na">No</Make_Call_Without_Reg_4_>
<Register_Expires_4_ ua="na">3600</Register_Expires_4_>
<Ans_Call_Without_Reg_4_ ua="na">No</Ans_Call_Without_Reg_4_>
<Use_DNS_SRV_4_ ua="na">No</Use_DNS_SRV_4_>
<DNS_SRV_Auto_Prefix_4_ ua="na">Yes</DNS_SRV_Auto_Prefix_4_>
<Proxy_Fallback_Intvl_4_ ua="na">3600</Proxy_Fallback_Intvl_4_>
<Proxy_Redundancy_Method_4_ ua="na">Normal</Proxy_Redundancy_Method_4_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_4_ ua="na">No</Dual_Registration_4_>
<Auto_Register_When_Failover_4_ ua="na">No</Auto_Register_When_Failover_4_>
<TLS_Name_Validate_4_ ua="na">Yes</TLS_Name_Validate_4_>
 <!--  Subscriber Information  -->
<Display_Name_4_ ua="na"/>
<User_ID_4_ ua="na">4085263128</User_ID_4_>
 <!--  <Password_4_ ua="na">**********</Password_4_>  -->
<Auth_ID_4_ ua="na">AUN3128</Auth_ID_4_>
<Reversed_Auth_Realm_4_ ua="na"/>
<SIP_URI_4_ ua="na"/>
```

```
 <!--  XSI Line Service  -->
<XSI_Host_Server_4_ ua="na"/>
<XSI_Authentication_Type_4_ ua="na">Login Credentials</XSI_Authentication_Type_4_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_4_ ua="na"/>
 <!--  <Login_Password_4_ ua="na"/>  -->
<Anywhere_Enable_4_ ua="na">No</Anywhere_Enable_4_>
<Block_CID_Enable_4_ ua="na">No</Block_CID_Enable_4_>
<DND_Enable_4_ ua="na">No</DND_Enable_4_>
<CFWD_Enable_4_ ua="na">No</CFWD_Enable_4_>
 <!--  Audio Configuration  -->
<Preferred_Codec_4_ ua="na">G711u</Preferred_Codec_4_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_4_ ua="na">No</Use_Pref_Codec_Only_4_>
<Second_Preferred_Codec_4_ ua="na">Unspecified</Second_Preferred_Codec_4_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_4_ ua="na">Unspecified</Third_Preferred_Codec_4_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_4_ ua="na">Yes</G711u_Enable_4_>
<G711a_Enable_4_ ua="na">Yes</G711a_Enable_4_>
<G729a_Enable_4_ ua="na">Yes</G729a_Enable_4_>
<G722_Enable_4_ ua="na">Yes</G722_Enable_4_>
<G722.2_Enable_4_ ua="na">Yes</G722.2_Enable_4_>
<iLBC_Enable_4_ ua="na">Yes</iLBC_Enable_4_>
<OPUS_Enable_4_ ua="na">Yes</OPUS_Enable_4_>
<Silence_Supp_Enable_4_ ua="na">No</Silence_Supp_Enable_4_>
<DTMF_Tx_Method_4_ ua="na">Auto</DTMF_Tx_Method_4_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_4_ ua="na">Default</Codec_Negotiation_4_>
<!--  available options: Default|List All  -->
<Encryption_Method_4_ ua="na">AES 128</Encryption_Method_4_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_4_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_4_>
<Caller_ID_Map_4_ ua="na"/>
<Enable_URI_Dialing_4_ ua="na">No</Enable_URI_Dialing_4_>
<Emergency_Number_4_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_4_ ua="na"/>
<Primary_Request_URL_4_ ua="na"/>
<Secondary_Request_URL_4_ ua="na"/>
 <!--  Hold Reminder  -->
<Hold_Reminder_Timer ua="rw"/>
<Hold_Reminder_Ring ua="rw">2</Hold_Reminder_Ring>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12
-->
 <!--  Call Forward  -->
<Cfwd_Setting ua="rw">Yes</Cfwd_Setting>
<Cfwd_All_Dest ua="rw"/>
<Cfwd_Busy_Dest ua="rw"/>
```

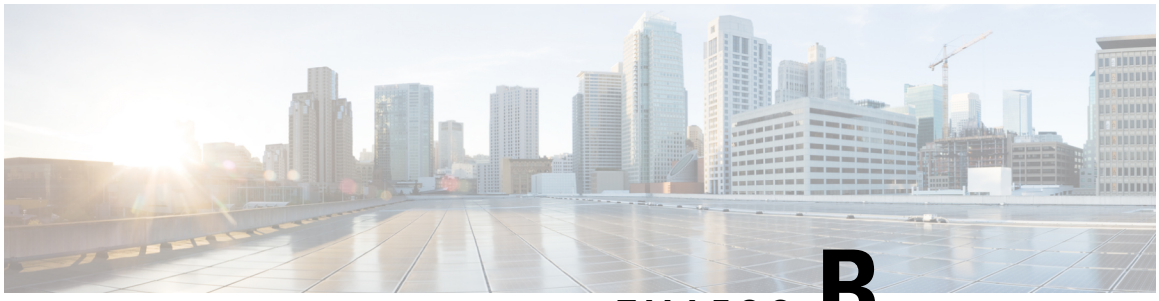
Eksempel på konfigurasjonsprofiler

```
<Cfwd_No_Ans_Dest ua="rw"/>
<Cfwd_No_Ans_Delay ua="rw">20</Cfwd_No_Ans_Delay>
 <!--  Speed Dial  -->
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name ua="rw"/>
<Speed_Dial_5_Number ua="rw"/>
<Speed_Dial_6_Name ua="rw"/>
<Speed_Dial_6_Number ua="rw"/>
<Speed_Dial_7_Name ua="rw"/>
<Speed_Dial_7_Number ua="rw"/>
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
<Speed_Dial_9_Number ua="rw"/>
 <!--  Supplementary Services  -->
<CW_Setting ua="rw">Yes</CW_Setting>
<Block_CID_Setting ua="rw">No</Block_CID_Setting>
<Block_ANC_Setting ua="rw">No</Block_ANC_Setting>
<DND_Setting ua="rw">No</DND_Setting>
<Secure_Call_Setting ua="na">No</Secure_Call_Setting>
<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>
<Preferred_Audio_Device ua="na">None</Preferred_Audio_Device>
<!--  available options: Speaker|Headset|None  -->
<Time_Format ua="na">12hr</Time_Format>
<!--  available options: 12hr|24hr  -->
<Date_Format ua="na">month/day</Date_Format>
<!--  available options: month/day|day/month  -->
<Miss_Call_Shortcut ua="na">No</Miss_Call_Shortcut>
<Handset_LED_Alert ua="rw">Voicemail</Handset_LED_Alert>
<!--
 available options: Voicemail|Voicemail, Missed Call
-->
<Alert_Tone_Off ua="rw">No</Alert_Tone_Off>
<Log_Missed_Calls_for_EXT_1 ua="na">Yes</Log_Missed_Calls_for_EXT_1>
<Log_Missed_Calls_for_EXT_2 ua="na">Yes</Log_Missed_Calls_for_EXT_2>
<Log_Missed_Calls_for_EXT_3 ua="na">Yes</Log_Missed_Calls_for_EXT_3>
<Log_Missed_Calls_for_EXT_4 ua="na">Yes</Log_Missed_Calls_for_EXT_4>
<Shared_Line_DND_Cfwd_Enable ua="na">Yes</Shared_Line_DND_Cfwd_Enable>
 <!--  Camera Profile 1  -->
 <!--  Camera Profile 2  -->
 <!--  Camera Profile 3  -->
 <!--  Camera Profile 4  -->
 <!--  Audio Volume  -->
<Ringer_Volume ua="rw">5</Ringer_Volume>
<Speaker_Volume ua="rw">7</Speaker_Volume>
<Handset_Volume ua="rw">15</Handset_Volume>
<Headset_Volume ua="rw">10</Headset_Volume>
<Ehook_Enable ua="na">No</Ehook_Enable>
 <!--  Audio Compliance  -->
<Compliant_Standard ua="rw">TIA</Compliant_Standard>
<!--  available options: TIA|ETSI  -->
 <!--  Screen  -->
<Screen_Saver_Enable ua="rw">Yes</Screen_Saver_Enable>
<Screen_Saver_Type ua="rw">Clock</Screen_Saver_Type>
<!--  available options: Clock|Download Picture|Logo  -->
<Screen_Saver_Wait ua="rw">60</Screen_Saver_Wait>
<Screen_Saver_Refresh_Period ua="rw">10</Screen_Saver_Refresh_Period>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<!--  available options: Off|10s|20s|30s|Always On  -->
```

```
<LCD_Contrast ua="rw">9</LCD_Contrast>
<Boot_Display ua="na">Default</Boot_Display>
<!--
 available options: Default|Download Picture|Logo|Text
-->
<Text_Logo ua="na"/>
<Phone_Background ua="rw">Default</Phone_Background>
<!--  available options: Default|Logo  -->
<Picture_Download_URL ua="rw"/>
<Logo_URL ua="rw"/>
 <!--  Video Configuration  -->
 <!--  General  -->
<Subscribe_Expires ua="na">1800</Subscribe_Expires>
<Subscribe_Retry_Interval ua="na">30</Subscribe_Retry_Interval>
<Number_of_Units ua="na">0</Number_of_Units>
<!--  available options: 0|1  -->
<Subscribe_Delay ua="na">1</Subscribe_Delay>
<Server_Type ua="na">Broadsoft</Server_Type>
<!--
 available options: Broadsoft|SPA9000|Asterisk|RFC3265_4235|Sylantro
-->
<BLF_List_URI ua="na"/>
<Use_Line_Keys_For_BLF_List ua="na">No</Use_Line_Keys_For_BLF_List>
<Customizable_PLK_Options ua="na">sd;</Customizable_PLK_Options>
<BLF_List ua="na">Show</BLF_List>
<!--  available options: Show|Hide  -->
<Call_Pickup_Audio_Notification ua="na">No</Call_Pickup_Audio_Notification>
<Attendant_Console_LCD_Contrast ua="na">8</Attendant_Console_LCD_Contrast>
<BXfer_To_Starcode_Enable ua="na">No</BXfer_To_Starcode_Enable>
<BXfer_On_Speed_Dial_Enable ua="na">No</BXfer_On_Speed_Dial_Enable>
<BXfer_To_Remote_Party_Number_Enable ua="na">No</BXfer_To_Remote_Party_Number_Enable>
<BLF_Label_Display_Mode ua="na">Both</BLF_Label_Display_Mode>
<!--  available options: Name|Ext|Both  -->
<Wake_up_phone_screen_when_BLF_pickup_is_ringing
ua="na">No</Wake_up_phone_screen_when_BLF_pickup_is_ringing>
 <!--  Unit 1  -->
<Unit_1_Key_1_ ua="na"/>
<Unit_1_Key_2_ ua="na"/>
<Unit_1_Key_3_ ua="na"/>
<Unit_1_Key_4_ ua="na"/>
<Unit_1_Key_5_ ua="na"/>
<Unit_1_Key_6_ ua="na"/>
<Unit_1_Key_7_ ua="na"/>
<Unit_1_Key_8_ ua="na"/>
<Unit_1_Key_9_ ua="na"/>
<Unit_1_Key_10_ ua="na"/>
<Unit_1_Key_11_ ua="na"/>
<Unit_1_Key_12_ ua="na"/>
<Unit_1_Key_13_ ua="na"/>
<Unit_1_Key_14_ ua="na"/>
<Unit_1_Key_15_ ua="na"/>
<Unit_1_Key_16_ ua="na"/>
<Unit_1_Key_17_ ua="na"/>
<Unit_1_Key_18_ ua="na"/>
<Unit_1_Key_19_ ua="na"/>
<Unit_1_Key_20_ ua="na"/>
<Unit_1_Key_21_ ua="na"/>
<Unit_1_Key_22_ ua="na"/>
<Unit_1_Key_23_ ua="na"/>
<Unit_1_Key_24_ ua="na"/>
<Unit_1_Key_25_ ua="na"/>
<Unit_1_Key_26_ ua="na"/>
<Unit_1_Key_27_ ua="na"/>
<Unit_1_Key_28_ ua="na"/>
```

Eksempel på konfigurasjonsprofiler

```
 <!--  TR-069  -->
<Enable_TR-069 ua="na">No</Enable_TR-069>
<ACS_URL ua="na"/>
<ACS_Username ua="na"/>
 <!--  <ACS_Password ua="na"/>  -->
<Connection_Request_Username ua="na"/>
 <!--  <Connection_Request_Password ua="na"/>  -->
<Periodic_Inform_Interval ua="na">20</Periodic_Inform_Interval>
<Periodic_Inform_Enable ua="na">Yes</Periodic_Inform_Enable>
<TR-069_Traceability ua="na">No</TR-069_Traceability>
<CWMP_V1.2_Support ua="na">Yes</CWMP_V1.2_Support>
<TR-069_VoiceObject_Init ua="na">Yes</TR-069_VoiceObject_Init>
<TR-069_DHCPOption_Init ua="na">Yes</TR-069_DHCPOption_Init>
<TR-069_Fallback_Support ua="na">No</TR-069_Fallback_Support>
<BACKUP_ACS_URL ua="na"/>
<BACKUP_ACS_User ua="na"/>
 <!--  <BACKUP_ACS_Password ua="na"/>  -->
</flat-profile>
```



TILLEGG B

Akronymer

Akronymer

AC	Vekselstrøm
ACS	Tilgangskontrollserver
A/D	Analog til digital-omformer
AES	AES, Avansert krypteringsstandard
ANC	Anonymt anrop
AP	Tilgangspunkt
ASCII	Amerikansk standardkode for informasjonsutveksling
B2BUA	Back to Back User Agent (brukeragent)
BLF	Opptattlampefelt
Bool	Boolske verdier. Angis som yes (ja) og no (nei), eller 1 og 0 i profilen
BootP	Bootstrap-protokoll (Bootstrap Protocol)
CA	Sertifikatutsteder
CAS	Varselsignal i CPE
CDP	Cisco Discovery Protocol
CDR	Samtaleinformasjon
CGI	Datamaskingenererte bilder
CID	Oppringer-ID
CIDCW	Anroper-ID for samtale venter

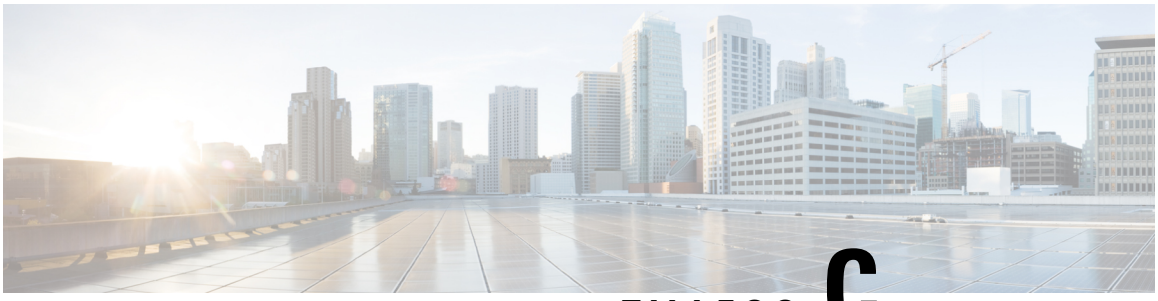
CNG	Generering av komfortstøy
CPC	Oppringerkontroll
CPE	Utstyr i kundens lokaler
CSV	Kommadelt verdi
CWCID	Anroper-ID for samtale venter
CWT	Samtale venter-tone
D/A	Digital til analog-omformer
dB	desibel
dBm	dB ved 1 milliwatt
DHCP	Dynamic Host Configuration Protocol
DND	Ikke forstyrr
DNS	Domenenavnsystem
DoS	Tjenestenekt (Denial of service)
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Loop
DSP	Digital signalprosessor
DST	Sommertid
DTAS	Varselsignal for dataterminal (samme som CAS)
DTMF	Tonekodesignalering (Dual Tone Multiple Frequency)
FQDN	Fullstendig kvalifisert domenenavn
FSK	Frequency Shift Keying
FW	Fastvare
FXS	Foreign eXchange Station
GMT	Vesteuropeisk tid (Greenwich Mean Time)
GW	Gateway
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
ICMP	Internet Control Message Protocol

IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internett-protokoll
IPv4	Internet Protocol versjon 4
IPv6	Internet Protocol versjon 6
ISP	Internett-leverandør
ITSP	Leverandør av Internett-telefoni
ITU	Den internasjonale telekommunikasjonsunion
IVR	Interactive Voice Response
LAN	Lokalnett
LBR	Lav bitrate
LBRC	Kodek for lav bitrate
LCD	Flytende krystall-skjerm; også kalt LCD-skjerm
LDAP	Lightweight Directory Access Protocol
LED	Lysdiode; LED-lampe
MAC-adresse	Kontrolladresse for nettverkstilgang
MC	Minisertifikat
MGCP	Media Gateway Control Protocol
MOH	Ventemusikk
MOS	Mean Opinion Score (1–5, jo høyere, jo bedre)
MPP	Telefoner for flere plattformer
ms	Millisekund
MSA	Musikkildeadapter
MWI	Melding venter-indikasjon
NAT	Oversettelse av nettverksadresse
NPS	Normal klargjøringsserver
NTP	Network Time Protocol
OOB	Out-of-band
OSI	Open Switching Interval

PBX	Private branch exchange
PCB	Kretskort
PoE	Fungerer med Ethernet
PR	Polaritetsveksling
PS	Klargjøringsserver
PSQM	Mål på oppfattet talekvalitet (1–5, jo lavere, jo bedre)
PSTN	Svitsjet telefonnettverk
QoS	Tjenestekvalitet (Quality of service)
RC	Fjern tilpasning
REQT	(SIP) Forespørselsmelding
RESP	(SIP) Svarmelding
RSC	(SIP) Svarstatuskode, for eksempel 404, 302, 600
RTP	Sanntidsprotokoll (Real Time Protocol)
RTT	Round Trip Time
SAS	Lydserver for streaming
SDP	Session Description Protocol
SDRAM	Synkron DRAM
sek	sekunder
SIP	Session Initiation Protocol
SLA	Shared line appearance
SLIC	Subscriber Line Interface Circuit
SP	Tjenesteleverandør
SSL	Secure Socket Layer
STUN	Session Traversal UDP for NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security; kryptografisk protokoll
TTL	Levetid (Time to live)
ToS	Tjenestetype

UA	Brukeragent (User Agent)
uC	Mikrokontroller
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Koordinert universaltid
VAR	Value Added Reseller; videreforhandler
VLAN	Voice LAN
VM	Talepost
VMWI	Visuell melding venter-indikasjon/indikator
VoIP	Voice over Internet Protocol
VQ	Talekvalitet
WAN	Vidstrakt nettverk (Wide Area Network)
XML	Extensible Markup Language

Akronymer



TILLEGG C

Beslektet dokumentasjon

Beslektet dokumentasjon

Bruk de følgende avsnittene til å få relevant informasjon.

Dokumentasjon for Cisco IP Phone 6800-serien

Se publikasjonene som er spesifikke for ditt språk, telefonmodellen du bruker, og versjonen for multiplattformfastvaren. Naviger fra følgende Uniform Resource Locator (URL-adresse):

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/tsd-products-support-series-home.html

Kundestøttepolicy for Cisco IP Phone-telefonfastvare

Du finner informasjon om kundestøttepolicyer for telefoner under https://cisco.com/go/phonefirmwaresupport.