Klargøringsvejledning til Cisco IP Phone 6800-serien af multiplatformstelefoner

Første gang udgivet: 2017-11-22

Senest ændret: 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.

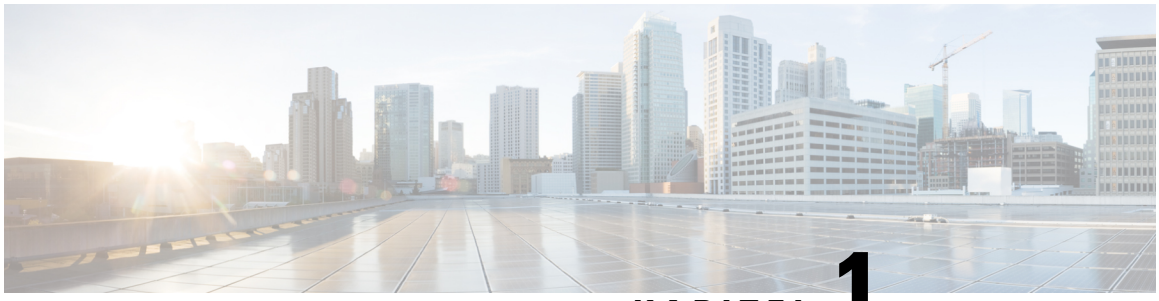
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

INDHOLD



KAPITEL 1

Installation og klargøring

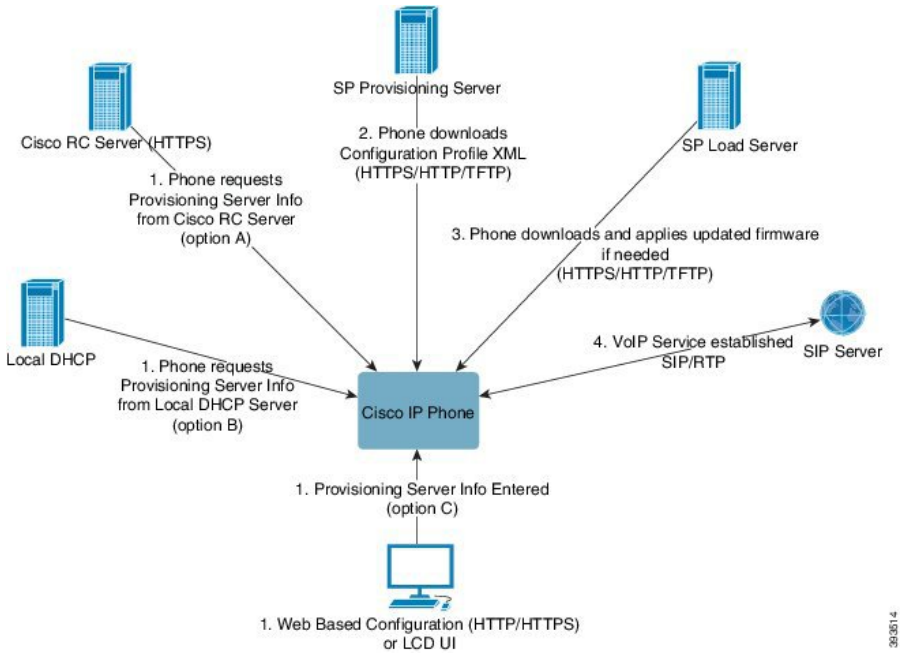
Klargøringsoversigt

Cisco IP Phone-telefoner er beregnet til store installationsmængder via Voice-over-IP (VoIP)-tjenesteudbydere til kunder i private hjem og små og store virksomhedsmiljøer. Klargøringen af telefonen via fjernadministration og konfiguration sikrer således, at telefonen fungerer korrekt hos kunden.

Cisco understøtter den tilpassede og løbende konfiguration af telefonens funktioner ved hjælp af:

- Pålidelig fjernbetjening af telefonen.
- Kryptering af den kommunikation, der styrer telefonen.
- Strømlinet telefonkontobinding.

Telefoner kan klargøres til at downloade konfigurationsfiler eller opdateret firmware fra en ekstern server. Overførsler kan ske, når telefonerne er tilsluttet til et netværk, når de tændes og efter angivne intervaller. Klargøring er typisk del af de store VoIP-baserede installationer, som tjenesteudbydere normalt foretager. Konfigurationsprofiler eller opdateret firmware overføres til enheden ved brug af TFTP, HTTP eller HTTPS.



Telefonens klargøringsproces på et højt niveau er som følger:

1. Hvis telefonen ikke er konfigureret, anvendes klargøringsserveroplysningerne på telefonen ved hjælp af en af følgende indstillinger:
   - **A** – downloadet fra RC-server (Remote Customization) til Cisco Enablement Data Orchestration System (EDOS) ved hjælp af HTTPS.
   - **B** – med forespørgsler fra en lokal DHCP-server.
   - **C** – indtastet manuelt via Cisco-telefonens webbaserede konfigurationsværktøj eller telefonens brugergrænseflade.
2. Telefonen henter serverens klargøringsoplysningerne og anvender konfigurations-XML'en ved hjælp af TFTP-, HTTP- eller HTTPS-protokollen.
3. Telefonen henter og anvender den opdaterede firmware, hvis det er nødvendigt, ved brug af TFTP, HTTP eller HTTPS.
4. VoIP-tjenesten er oprettet ved brug af den angivne konfiguration og firmware.

VoIP-tjenesteudbydere vil installere mange telefoner hos private kunder og små virksomhedskunder. I forretnings- eller virksomhedsmiljøer kan telefoner fungere som terminalnoder. Udbydere distribuerer disse enheder bredt ud på tværs af internettet, som er forbundet via routere og firewalls hos kunden.

Telefonen kan bruges som en ekstern udvidelse af tjenesteudbyderens backend-udstyr. Fjernadministration og konfiguration sikrer, at telefonen fungerer korrekt hos kunden.

TR69-klargøring

Cisco IP Phone hjælper administratoren med at konfigurere TR69-parametrene ved hjælp af webbrugergrænsefladen. Se administrationsvejledning til den tilsvarende telefonserie for at finde oplysninger vedrørende parametrene, herunder en sammenligning af XML- og TR69-parametrene.

Telefonerne understøtter ACS-registrering (Auto Configuration Server) af DHCP-indstilling 43, 60 og 125.

- Indstilling 43 – leverandørspecifikke oplysninger om ACS-URL-adressen.
- Indstilling 60 – leverandørklasse-id, så telefonen kan identificere sig selv med `dslforum.org` til ACS.
- Indstilling 125 – leverandørspecifikke oplysninger om gatewaytilknytningen.

RPC-metoder

Understøttede RPC-metoder

Telefonerne understøtter kun et begrænset sæt RPC-metoder (Remote Procedure Call) på følgende måde:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Oplys
- Download: Hent RPC-metoden, følgende filtyper understøttes:
  - Firmwareopgraderingsafbildning
  - Leverandørkonfigurationsfil
  - Brugerdefineret nøglecenterfil
- Overførsel fuldført

Understøttede hændelsestyper

Telefonerne understøtter hændelsestyper, der er baseret på understøttede funktioner og metoder. Kun følgende hændelsestyper understøttes:

- Bootstrap
- Start
- værdiændring
- forbindelsesanmodning
- Periodisk
- Overførsel fuldført
- M-download
- M-genstart

Telefonens virkemåde i tilfælde af netværksforsinkelse

- Administrative opgaver, som f.eks. interne portscanninger eller sikkerhedsscanninger
- Angreb på netværket i form af f.eks. Denial of Service-angreb

Installation

Cisco IP Phone-telefoner har praktiske mekanismer til klargøring, der er baseret på disse installationsmodeller:

- Massedistribution – tjenesteudbyderen køber Cisco IP Phone-telefoner i store mængder og forhåndsklargør dem enten internt eller køber RC-enheder (Remote Customization) fra Cisco. Enhederne udleveres derefter til kunderne som en del af en VoIP-serviceaftale.
- Detaildistribution – kunden køber en Cisco IP Phone i en detailbutik og anmoder om VoIP-tjeneste fra tjenesteudbyderen. Tjenesteudbyderen skal derefter understøtte den sikre fjernkonfiguration af enheden.

Massedistribution

I denne model udleverer tjenesteudbyderen telefoner til dennes kunder som en del af en VoIP-serviceaftale. Enhederne er enten RC-enheder eller forhåndsklargjort internt.

Cisco klargør RC-enheder til at gensynkronisere med en Cisco-server, der henter enhedsprofilen og firmwareopdateringerne.

En tjenesteudbyder kan forhåndsklargøre telefoner med de ønskede parametre, herunder de parametre, der styrer gensynkroniseringen, på forskellige måder:

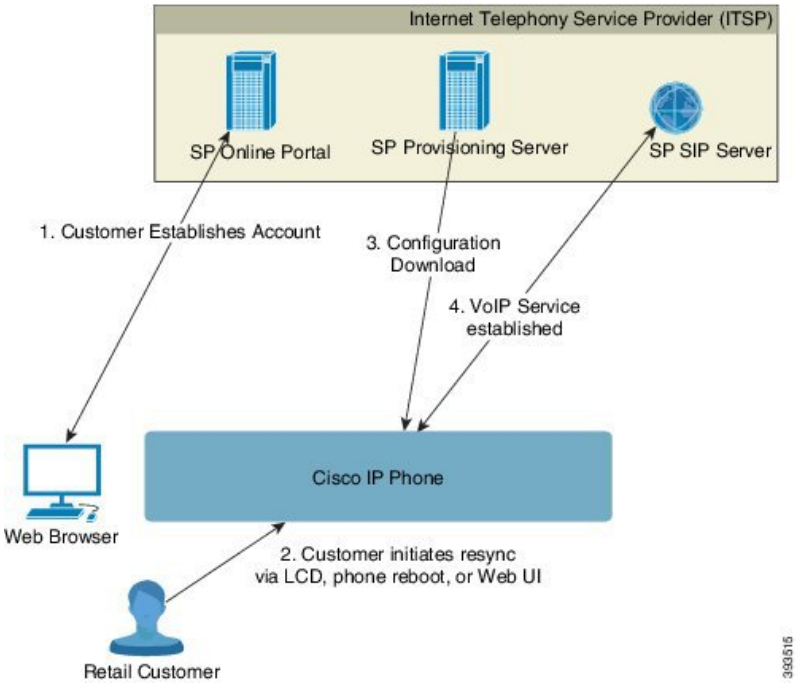
- Internt ved hjælp af DHCP og TFTP
- Eksternt ved hjælp af TFTP, HTTP eller HTTPS

- En kombination af intern og ekstern klargøring

Detailhandeldistribution

Ved en distributionsmodel til detailhandlen køber en kunde en telefon og abonnerer på en bestemt tjeneste. ITSP (Internet Telephony Service Provider) konfigurerer og vedligeholder en klargøringsserver og forhåndsklargør telefonen til at blive gensynkroniseret med tjenesteudbyderens server.

Figur 1: Detailhandeldistribution



Telefonen omfatter det webbaserede konfigurationsværktøj, der viser intern konfiguration og accepterer nye konfigurationsparameterværdier. Serveren accepterer også en speciel syntaks for URL-kommandoer til at udføre eksterne handlinger i forhold til gensynkronisering af profil og firmwareopgradering.

Kunden logger på tjenesten og opretter en VoIP-konto, eventuelt via en onlineportal, og knytter enheden til den tildelte tjenestekonto. Telefonen, der ikke er klargjort, instrueres i at gensynkronisere med en bestemt klargøringsserver via en URL-baseret kommando til gensynkronisering. Den URL-baserede kommando omfatter typisk et kontokunde-id-nummer eller en alfanumerisk kode for at kunne knytte enheden til den nye konto.

I det følgende instrueres en enhed på den DHCP-tildelte IP-adresse 192.168.1.102 i at klargøres sig selv til selve SuperVoIP-tjenesten:

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

I dette eksempel er kunde-id-nummeret 1234abcd for den nye konto. Den eksterne klargøringsserver tilknytter den telefon, der udfører gensynkroniseringsanmodningen, til den nye konto, baseret på URL-adressen og det medfølgende kunde-id. Via denne indledende gensynkroniseringshandling konfigureres telefonen i et enkelt trin. Derefter dirigeres telefonen automatisk til gensynkronisering til en permanent URL-adresse på serveren. For eksempel:

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

Både når det gælder den indledende og permanente adgang benytter klargøringsserveren sig af telefonklientcertifikatet til godkendelse. Klargøringsserveren leverer korrekte konfigurationsparameterværdier, der er baseret på den tilknyttede tjenestekonto.

Når enheden er tændt, eller der er gået et bestemt stykke tid, gensynkroniserer telefonen igen og downloader de nyeste parametre. Disse parametre kan håndtere mål som f.eks. opsætning af en søgegruppe, indstille hurtigopkaldsnumre og begrænse de funktioner, en bruger kan ændre.

Lignende emner

Klargøring af enheder internt, på side 39

Gensynkroniseringsproces

Firmwaren til hver telefon indeholder en administrationswebserver, der accepterer nye konfigurationsparameterværdier. Telefonen kan blive bedt om at gensynkronisere konfiguration efter genstart eller efter planlagte intervaller med en bestemt klargøringsserver via en URL-baseret gensynkroniseringskommando i enhedsprofilen.

Webserveren er aktiveret som standard. Hvis du vil deaktivere eller aktivere webserveren, skal du bruge den URL-baserede gensynkroniseringskommando.

Hvis det er nødvendigt, kan du bede om øjeblikkelig gensynkronisering via en URL-adresse til "gensynkroniseringshandling". URL-adressen til gensynkroniseringskommandoen kan omfatte et kontokunde-id-nummer eller en alfanumerisk kode, så enheden kan knyttes til brugerens konto på en entydig måde.

Eksempel

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

I dette eksempel instrueres en enhed på den DHCP-tildelte IP-adresse 192.168.1.102 i at klargøre sig selv til SuperVoIP-tjenesten på prov.supervoip.com. Kunde-id-nummeret for den nye konto er 1234abcd. Den eksterne klargøringsserver tilknytter den telefon, der udfører gensynkroniseringsanmodningen, til kontoen, basereret på URL-adressen og kunde-id'et.

Via denne indledende gensynkroniseringshandling konfigureres telefonen i et enkelt trin. Derefter dirigeres telefonen automatisk til gensynkronisering til en permanent URL-adresse på serveren.

Både når det gælder den indledende og permanente adgang benytter klargøringsserveren sig af klientcertifikatet til godkendelse. Serveren leverer konfigurationsparameterværdier, der er baseret på den tilknyttede tjenestekonto.

Klargøring

En telefon kan konfigureres til periodisk at gensynkronisere dens interne konfigurationstilstand for at matche en ekstern profil periodisk, og når den tændes. Telefonen kontakter en NPS (normal provisioning server) eller en ACS (access control server).

Som standard forsøges en profilgensynkronisering kun, når telefonen er inaktiv. Denne fremgangsmåde forhindrer en opgradering, der ville udløse en softwaregenstart og afbryde et opkald. Hvis mellemliggende

opgraderinger kræves for at nå en aktuel opgraderingstilstand fra en ældre frigivelse, kan opgraderingslogikken automatisere flertrinsopgraderinger.

Normal klargøringsserver

Den normale klargøringsserver kan være en TFTP-, HTTP- eller HTTPS-server. En ekstern firmwareopgradering opnås ved hjælp af TFTP eller HTTP eller HTTPS, fordi firmwaren ikke indeholder følsomme oplysninger.

Selvom HTTPS anbefales, kræver kommunikation med NPS ikke brug af en sikker protokol, fordi den opdaterede profil kan krypteres med en delt hemmelig nøgle. Få flere oplysninger om brug af HTTPS under Kryptering af kommunikation, på side 8. Sikker klargøring første gang sikres gennem en mekanisme, der bruger SSL-funktionalitet. En telefon, der ikke er klargjort, kan modtage en 256-bit symmetrisk nøglekrypteret profil, der er målrettet til den pågældende enhed.

Adgangskontrol for konfiguration

Telefonens firmware giver en mekanisme til at begrænse slutbrugeradgang til visse parametre. Firmware giver specifikke rettigheder til at logge på en **administrator**- eller **bruger**-konto. Hver især kan uafhængigt af hinanden være beskyttet med adgangskode.

- Administratorkonto – giver tjenesteudbyderen fuld adgang til alle parametre for administrationswebserveren.
- Brugerkonto – giver brugeren mulighed at konfigurere et undersæt af parametre for administrationswebserveren.

Tjenesteudbyderen kan begrænse brugerkontoen i klargøringsprofilen på følgende måder:

- Angiv, hvilke konfigurationsparametre der er tilgængelige til brugerkontoen ved oprettelse af konfigurationen.
- Deaktiver brugeradgang til administrationswebserveren.
- Deaktiver brugeradgang til LCD-brugergrænseflade.
- Omgå skærmen **Angiv adgangskode** for brugeren.
- Begræns de internetdomæner, som enheden kan tilgå til gensynkronisering, opgraderinger eller SIP-registrering, for linje 1.

Lignende emner

Egenskaber for elementkoder, på side 14
Adgangskontrol, på side 16

Gå til telefonens webside

Få adgang til telefonens webside fra en webbrowser på en computer, der kan få forbindelse til telefonen på undernetværket.

Hvis din serviceudbyder har deaktiveret adgang til konfigurationsværktøjet, skal du kontakte tjenesteudbyderen, før du fortsætter.

Fremgangsmåde

Trin 1 Sørg for, at computeren kan kommunikere med telefonen. Ingen VPN i brug.

Trin 2 Start en webbrowser.

Trin 3 Angiv IP-adressen på telefonen på adresselinjen i webbrowseren.

- Brugeradgang: **`http://<ip-adresse>/user`**
- Administratoradgang: **`http://<ip-adresse>/admin/advanced`**
- Administratoradgang: **`http://<ip-adresse>`**, klik på **Administratorlogoón**, og klik på **Avanceret**

F.eks.: `http://10.64.84.147/admin/`

Tillad webadgang til Cisco IP Phone

Hvis du vil vise telefonparametrene, skal du aktivere konfigurationsprofilen. Hvis du vil ændre nogle af disse parametre, skal du kunne ændre konfigurationsprofilen. Din systemadministrator kan have deaktiveret telefonindstillingen, der gør telefonens webbrugergrænseflade synlig eller skrivbar.

Hvis du ønsker yderligere oplysninger, kan du se *Klargøringsvejledningen til Cisco IP Phone 6800-serien af multiplatformstelefoner*.

Inden du begynder

Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Fremgangsmåde

Trin 1 Klik på **Tale** > **System**.

Trin 2 I sektionen **Systemkonfiguration** skal du indstille **Aktivér webserver** til **Ja**.

Trin 3 Hvis du vil opdatere konfigurationsprofilen, skal du klikke på **Send alle ændringer**, når du ændrer felterne i telefonens webbrugergrænseflade.

Telefonen genstartes, og ændringerne anvendes.

Trin 4 Hvis du vil rydde alle de ændringer, du har foretaget, i løbet af den aktuelle session (eller når du senest har klikket på **Send alle ændringer**), skal du klikke på **Fortryd alle ændringer**. Værdierne går tilbage til deres tidligere indstillinger.

Kryptering af kommunikation

De konfigurationsparametre, der er videregivet til enheden, kan indeholde godkendelseskoder eller andre oplysninger, der beskytter systemet mod uautoriseret adgang. Det er i serviceudbyderens interesse at forhindre uautoriseret kundeaktivitet. Det er i kundens interesse at forhindre uautoriseret brug af kontoen. Serviceudbyderen kan kryptere konfigurationsprofilkommunikationen mellem klargøringsserveren og enheden ud over at begrænse adgangen til administrationswebserveren.

Fremgangsmåder til klargøring af telefoner

Cisco IP Phone er typisk konfigureret til klargøring, når den forbindes til netværket første gang. Telefonen klargøres også ved de planlagte intervaller, der angives, når serviceudbyderen eller VAR-forhåndsklargør (konfigurerer) telefonen. Serviceudbydere kan godkende, at VAR'er eller avancerede brugere manuelt kan klargøre telefonen ved at bruge telefonens tastatur. Du kan også konfigurere klargøring ved hjælp af telefonens webbrugergrænseflade.

Marker **Status** > **Telefonstatus** > **Klargøring** i telefonens LCD-brugergrænseflade eller klargøringsstatussen under **Status** i det webbaserede konfigurationsværktøj.

Lignende emner

Manuel klargøring af en telefon på tastaturet, på side 9

Manuel klargøring af en telefon på tastaturet

Fremgangsmåde

Trin 1 Tryk på **Programmer** .

Trin 2 Vælg **Enhedsadministration** > **Profilregel**.

Trin 3 Angiv profilreglen i følgende format:

```
protokol://server[:port]/profil_stinavn
```

F.eks.:

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

Hvis der ikke er angivet en protokol, antages det, at TFTP skal bruges. Hvis der ikke er angivet et servernavn, vil den vært, der anmoder om URL-adressen, blive brugt som servernavnet. Hvis der ikke er angivet en port, bruges standardporten (69 for TFTP, 80 for HTTP eller 443 for HTTPS).

Trin 4 Tryk på **Gensynkroniser**.

Lignende emner

Fremgangsmåder til klargøring af telefoner, på side 9

Peer-firmwaredeling

PFS (Peer Firmware Sharing) er en distributionsmodel for firmware, der giver en Cisco IP Phone mulighed for at finde andre telefoner i samme model eller serie på undernettet og dele opdaterede firmwarefiler, når du har flere telefoner, der alle skal opgraderes på samme tid. PFS bruger CPPDP (Cisco Peer-to-Peer-Distribution Protocol), der er en beskyttet Cisco-protokol. Med CPPDP danner alle enheder i undernettet et peer to peer-hierarki og kopierer derefter firmware eller andre filer fra peer-enheder til enheder i nærheden. For at optimere firmwareopgraderinger downloader en rodtelefon firewareafbildningen fra belastningsserver og overfører derefter firmware til andre telefoner på det undernet ved brug af TCP-forbindelser.

Peer-firmwaredeling:

- Begrænser overbelastning på TFTP-overførsler til centraliserede eksterne belastningsservere.

- Fjerner behovet for manuelt at styre firmwareopgraderinger.
- Reducerer telefonens nedetid under opgradering, når et stort antal telefoner nulstilles samtidigt.

Bemærk

- Peer-firmwaredeling fungerer ikke, medmindre flere telefoner er indstillet til at opgradere på samme tid. Når der sendes en NOTIFY med Event:resync, starter den en gensynkronisering på telefonen. Eksempel på en XML-streng, der kan indeholde konfigurationerne til at starte opgraderingen:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Når du indstiller logserveren til peer-firmwaredeling til en IP-adresse og port, sendes de PFS-specifikke logfiler til den pågældende server som UDP-meddelelser. Denne indstilling skal foretages på hver telefon. Du kan derefter bruge logmeddelelserne, når du fejlfinder problemer, der er relateret til PFS.

Peer_Firmware_Sharing_Log_Server angiver værtsnavnet og porten for den eksterne UDPsyslog-server. Porten anvender syslog 514 som standard.

For eksempel:

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

Du kan bruge denne funktion ved at aktivere PFS på telefonerne.

Omgå skærmen Angiv adgangskode

Du kan omgå skærmen **Angiv adgangskode** ved den første start eller efter en fabriksnulstilling baseret på disse klargøringshandlinger:

- DHCP-konfiguration
- EDOS-konfiguration
- Konfiguration af brugeradgangskode, der bruges i telefonens XML-konfigurationsfil.

Tabel 1: Klargøringshandlinger, der fastlægger, om skærmen Angiv adgangskode vises

DHCP konfigureret	EDOS konfigureret	Brugeradgangskode konfigureret	Omgå skærmen Angiv adgangskode
Ja	I/T	Ja	Ja
Ja	I/T	Nej	**Nej**
Nej	Ja	Ja	Ja
Nej	Ja	Nej	**Nej**
Nej	Nej	I/T	**Nej**

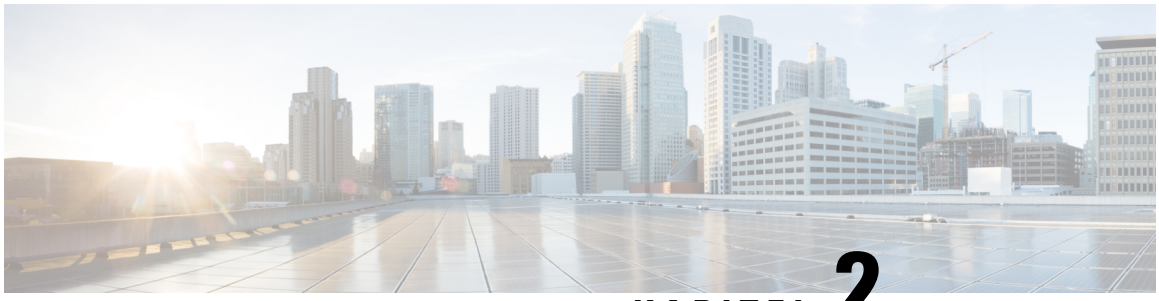
Fremgangsmåde

Trin 1 Rediger telefonfilen `config.xml` i en tekstfil eller XML-redigeringsprogram.

Trin 2 Indsæt koden **<User_Password>** ved hjælp af en af disse indstillinger.

- **Ingen adgangskode (start- og slutkode)**–**<User_Password></User_Password>**
- **Adgangskodeværdi (4 til 127 tegn)**–**<User_Password ua="rw">abc123</User_Password>**
- **Ingen adgangskode (kun start kode)**–**<User_Password />**

Trin 3 Gem ændringerne i filen `config.xml`.



KAPITEL 2

Klargøringsscripts

Klargøringsscripts

Telefonen accepterer konfiguration i et XML-format.

Få detaljerede oplysninger om din telefon ved at se i administrationsvejledningen for den specifikke enhed. Hver vejledning beskriver de parametre, der kan konfigureres via administrationswebserveren.

Formater til konfigurationsprofiler

Konfigurationsprofilen definerer parameterværdierne for telefonen.

Konfigurationsprofilens XML-format bruger XML-oprettelsesværktøjer til at kompilere parametrene og værdierne.

Bemærk UTF-8 tegnsættet er det eneste, der understøttes. Hvis du ændrer profilen i en editor, må du ikke ændre kodeformat; ellers kan telefonen ikke genkende filen.

Hver enkelt telefon har et forskelligt sæt funktioner og derfor et forskelligt sæt parametre.

XML-formatprofil (XML)

Open-formatprofilen er en tekstfil med XML-lignende syntaks i et hierarki af elementer, med elementattributter og værdier. Dette format gør det muligt at bruge standardværktøjer til at oprette konfigurationsfilen. En konfigurationsfil i dette format kan sendes fra klargøringsserveren til telefonen under en gensynkronisering. Filen kan sendes som et binært objekt uden kompilering.

Telefonen kan acceptere konfigurationsformater, der oprettes af standardværktøjer. Denne funktion forenkler udviklingen af backend-klargøringsserversoftware, der genererer konfigurationsprofiler fra eksisterende databaser.

For at beskytte fortrolige oplysninger i konfigurationsprofilen leverer klargøringsserveren denne type fil til telefonen via en kanal sikret med TLS. Filen kan eventuelt komprimeres ved hjælp af gzip-deflate-algoritmen (RFC1951).

Filen kan krypteres med en af disse krypteringsmetoder:

- AES-256-CBC-kryptering
- RFC-8188-baseret kryptering af HTTP-indhold med AES-128-GCM-beregning

Eksempel: Open-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 genkender.

Lignende emner

Komprimering og kryptering af Open-profil (XML), på side 17

Komponenter i konfigurationsfil

En konfigurationsfil kan indeholde disse komponenter:

- Elementkoder
- Attributter
- Parametre
- Formateringsfunktioner
- XML-kommentarer

Egenskaber for elementkoder

- XML-klargøringsformatet og webbrugergrænseflade giver mulighed for konfiguration af de samme indstillinger. XML-mærkenavn og feltnavnene i webbrugergrænsefladen ligner, men varierer på grund af begrænsninger i XML-elementnavne. For eksempel understregningstegn (_) i stedet for " ".
- Telefonen genkender elementer, der har de rigtige parameternavne, der er omsluttet af det særlige <flat-profile>-element.
- Elementnavne sættes i vinkelparenteser.
- De fleste elementnavne svarer til feltnavnene på enhedens administrationswebsider med følgende ændringer:

- Elementnavne kan ikke indeholde mellemrum eller specialtegn. For at aflede elementnavnet fra administrationswebfeltnavnet skal alle understregningstegning udskiftes med et mellemrumstegn eller specialtegnene `[`, `]`, `(`, `)` eller `/`.

  Eksempel: Elementet <Resync_On_Reset> repræsenterer feltet **Gensynkroniser ved nulstilling**.

- Hvert elementnavn skal være entydigt. På administrationswebsiderne kan de samme felter vises på mange sider, f.eks. linje-, bruger og lokalnummersiderne. Føj `[n]` til elementnavnet for at angive det nummer, der er vist under sidefanen.

  Eksempel: Elementet <Dial_Plan_1_> repræsenterer **Opkaldsplan** for linje 1.

- Hver åbningskode for element skal have et matchende lukningskode for element. For 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>
```

- Der skelnes mellem store og små bogstaver i elementkoder.
- Tomme elementkoder er tilladte og fortolkes, som at værdien konfigureres som tom. Angiv åbningskoden for elementet uden en tilsvarende elementkode, og indsæt et mellemrumstegn og en skråstreg før den afsluttende vinkelparentes (>). I dette eksempel er Profile Rule B (Profilregel B) tom:

```
<Profile_Rule_B />
```

- En tom elementkode kan bruges til at forhindre, at overskrivning af værdier, som brugeren måtte have angivet, under en gensynkroniseringshandling. I det følgende eksempel er brugerindstillingerne for hurtigkald uændret:

```
<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>
```

- Brug en tom værdi til at angive den tilhørende parameter til en tom streng. Angiv et åbnings- og lukningselement uden en værdi mellem dem. I følgende eksempel er parameteren GPP_A indstillet til en tom streng.

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

- Elementnavne, der ikke genkendes, ignoreres.

Lignende emner

Adgangskontrol for konfiguration, på side 7

Brugeradgangsattribut

Kontrolelementerne i brugeradgangsattributten (**ua**) kan bruges til at ændre adgangen af brugerkontoen. Hvis attributten **ua** ikke er angivet, bevares indstillingen for den eksisterende brugeradgang. Denne attribut påvirker ikke administratorkontoens adgang.

Attributten **ua** skal have en af følgende værdier:

- na – ingen adgang
- ro – skrivebeskyttet
- rw – læse/skrive

I følgende eksempel vises attributten **ua**:

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

Dobbelte anførselstegn skal sættes om værdien i indstillingen **ua**.

Adgangskontrol

Hvis parameteren <Phone-UI-User-Mode> er aktiveret, overholder telefonen brugergrænsefladeattributten for de relevante parametre, når brugergrænsefladen viser et menupunkt.

For menuposter, der er tilknyttet en enkelt konfigurationsparameter:

- Klargøring af parameteren med attributten "ua = na" ("ua" betyder "brugeradgang") får posten til at forsvinde.
- Klargøring af parameteren med attributten "ua = ro" gør posten skrivebeskyttet og ikke-redigerbar.

For menuposter, der er tilknyttet flere konfigurationsparametre:

- Klargøring af alle relevante parametre med attributten "ua = na" får posterne til at forsvinde.

Lignende emner

Adgangskontrol for konfiguration, på side 7

Parameteregenskaber

Disse egenskaber gælder for parametrene:

- De parametre, der ikke er angivet af en profil, ændres ikke på telefonen.
- Parametre, der ikke kan genkendes, ignoreres.
- Hvis profilen i Open-format indeholder flere forekomster af den samme parameterkode, tilsidesætter den sidste af en sådan forekomst eventuelle tidligere forekomster. For at undgå ved et uheld at tilsidesætte

konfigurationsværdier for en parameter anbefaler vi, at hver profil angiver mindst én forekomst af en parameter.

- Den sidste profil, der er behandlet, får forrang. Hvis flere profiler angiver den samme konfigurationsparameter, får værdien af den sidste profil forrang.

Strengformater

Disse egenskaber gælder for formateringen af strengene:

- Kommentarer, der er tilladt via standard-XML-syntaks.

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

- Blanktegn før og efter er tilladt for at øge læsbarheden, men fjernes fra parameterværdien.
- Nye linjer i en værdi konverteres til mellemrum.
- En XML-header i formatet `<? ?>` er tilladt, men det ignoreres af telefonen.
- Brug grundlæggende XML-tegn-escapes, hvis du vil bruge specialtegn. Det er vist i følgende tabel.

Specialtegn	Sekvens af XML-escape
& (ampersand)	&
< (mindre end)	<
> (større end)	>
' (apostrof)	'
” (dobbelt anførselstegn)	"

I følgende eksempel indtastes tegn-escapes for at repræsentere symboler for større end og mindre end, der kræves i en opkaldsplanregel. Dette eksempel definerer en opkaldsplan for informationshotline, der indstiller parameteren <Dial_Plan_1_> (**Administratorlogon** > **Avanceret** > **Tale** > **Lokal (nr.)**) til at være lig med (S0 < :18005551212>).

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

- Numeriske tegn-escapes med decimaler og hexadecimale værdier (f.eks. `&#40;` og `&#x2e;`), er oversat.
- Telefonens firmware understøtter kun ASCII-tegn.

Komprimering og kryptering af Open-profil (XML)

Open-konfigurationsprofilen kan komprimeres for at reducere netværksbelastningen på klargøringsserveren. Profilen kan også krypteres for at beskytte fortrolige oplysninger. Komprimering kræves ikke, men den skal ske før kryptering.

Lignende emner

Formater til konfigurationsprofiler, på side 13

Komprimering af Open-profil

Den understøttede komprimeringsmetode er en gzip-deflate-algoritme (RFC1951). Hjælpeværktøjet gzip og komprimeringsbiblioteket, der implementerer den samme algoritme (zlib), er tilgængelige på websteder på internettet.

For at identificere komprimering forventer telefonen, at den komprimerede fil indeholder en header, der er kompatibel med gzip. Aktivering af hjælpeprogrammet gzip i den oprindelige Open-profil genererer headeren. Telefonen undersøger den downloadede filheader for at bestemme filformatet.

Hvis f.eks. `profile.xml` er en gyldig profil, accepteres filen `profile.xml.gz` også. En af følgende kommandoer kan generere denne profiltype:

- `>gzip profile.xml`

  Erstatter den oprindelige fil med en komprimeret fil.

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

  Lader den oprindelige fil være på placeringen og producerer ny komprimeret fil.

Se et selvstudium i komprimering i afsnittet Komprimer en Open-profil med Gzip, på side 60.

Lignende emner

Komprimer en Open-profil med Gzip, på side 60

Kryptering af Open-profil

Symmetrisk nøglekryptering kan bruges til at kryptere en Open-konfigurationsprofil, uanset om filen er komprimeret eller ej. Hvis der anvendes komprimering, skal det gøres før krypteringen.

Klargøringsserveren bruger HTTPS til at håndtere den indledende klargøring af telefonen efter installation. Hvis konfigurationsprofilerne forhåndskrypteres, kan du efterfølgende bruge HTTP til at synkronisere profilerne. Dette reducerer belastningen på HTTPS-serveren ved store installationer.

Telefonen understøtter to metoder til kryptering af konfigurationsfiler:

- AES-256-CBC-kryptering
- RFC 8188-baseret kryptering af HTTP-indhold med AES-128-GCM-beregning

Nøglen eller IKM (Input Keying Material) skal allerede være klargjort i enheden. Bootstrap af den hemmelige nøgle kan udføres sikkert ved hjælp af HTTPS.

Navnet på konfigurationsfilen kræver ikke et specifikt format, men et filnavn med filtypenavnet `.cfg` vil som regel indikere, at det er en konfigurationsprofil.

AES-256-CBC-kryptering

Telefonen understøtter AES-256-CBC-kryptering af konfigurationsfilerne.

Værktøjet til OpenSSL-krypteringsværktøjet, der kan hentes forskellige steder på internettet, kan udføre kryptering. Understøttelse af AES 256-bit-kryptering kan kræve ny kompilering af værktøjet for at aktivere AES-koden. Firmwaren er blevet testet i forhold til version openssl-0.9.7c.

Krypter en profil med OpenSSL, på side 61 indeholder et selvstudium i kryptering.

Når det gælder en krypteret fil, forventer profilen, at filen har samme format, som genereres af 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
```

Et -k med små bogstaver kommer før den hemmelige nøgle, som kan være en almindelig tekst, og som bruges til at generere en vilkårlig 64-bit salt. Når den hemmelige del er angivet med argumentet -k, afleder krypteringsværktøjet en vilkårlig 128-bit startvektor og den faktiske 256-bit krypteringsnøgle.

Når denne form for kryptering bruges i en konfigurationsprofil, skal telefonen oplyses om den hemmelige nøgleværdi for at kunne dekryptere filen. Denne værdi er angivet som en kvalifikator i profilens URL-adresse. Syntaksen er som følger, hvor der bruges en eksplicit URL-adresse:

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

Denne værdi programmeres ved hjælp af en af Profile_Rule-parametrene.

Lignende emner

Krypter en profil med OpenSSL, på side 61

Makroudvidelse

Flere klargøringsparametre bliver udsat for en makroudvidelse internt, før de bliver evalueret. Dette forhåndsevalueringstrin giver større fleksibilitet i forhold til at styre aktiviteterne med telefonens gensynkronisering og opgradering.

Disse parametergrupper udsættes for en makroudvidelse før evaluering:

- Resync_Trigger_* (Udløser 1 af gensynkronisering_*)
- Profile_Rule* (Profilregel*)
- Log_xxx_Msg (Meddelelse om log xxx)
- Opgraderingsregel

Under visse betingelser udsættes nogle parametre for generelle formål (GPP_ *) også for en makroudvidelse, hvilket udtrykkeligt er angivet i Valgfri argumenter til gensynkronisering, på side 23.

Under en makroudvidelse udskiftes indholdet af de navngivne variable udtrykkene for formen $NAME og $(NAME). Disse variabler omfatter parametre for generelle formål, flere produkt-id'er, visse hændelsestidsindstillinger og værdier for klargøringstilstand. Få en fuldstændig liste under Makroudvidelsesvariabler, på side 72.

I følgende eksempel bruges udtrykket $(MAU) til at indsætte MAC-adressen 000E08012345.

Administratoren angiver: **$(MAU)config.cfg**

Den resulterende makroudvidelse for en enhed med MAC-adressen 000E08012345 er:
`000E08012345config.cfg`

Hvis et makronavn ikke genkendes, sker der ikke en udvidelse. Navnet STRANGE genkendes f.eks. ikke som et gyldig makronavn, mens MAU genkendes som et gyldigt makronavn.

Administratoren angiver: **$STRANGE$MAU.cfg**

Den resulterende makroudvidelse for en enhed med MAC-adressen 000E08012345 er:
`$STRANGE000E08012345.cfg`

Makroudvidelse anvendes ikke rekursivt. $$MAU" udvides f.eks. til $MAU" ($$ udvides) og resulterer ikke i MAC-adressen.

Indholdet af parametrene for specielle formål, GPP_SA til og med GPP_SD, knyttes til makroudtrykkene $SA til og med $SD. Disse parametre bliver kun makroudvidet som argumentet for indstillingerne **--key** , **--uid** og **--pwd** i en URL-adresse til gensynkronisering.

Betingede udtryk

Betingede udtryk kan udløse gensynkroniseringshændelser og vælge mellem alternative URL-adresser til gensynkroniserings- og opgraderingshandlinger.

Betingede udtryk består af en liste over sammenligninger, der er adskilt af med operatoren **og**. Alle sammenligninger skal være opfyldt, hvis betingelsen skal være sand.

Hver enkelt sammenligning relatere til en af følgende tre typer konstanter:

- Heltalsværdier
- Software- eller hardwareversionsnumre
- Streng med dobbelte anførselstegn

Versionsnumre

Softwareversionen for multiplatformstelefoners formelle frigivelsesversion anvender dette format, hvor BN==buildnummer:

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

Den sammenlignende streng skal bruge det samme format. Ellers vil det resultere i en fejl ved parsing af format.

I softwareversionen kan v1-v2-v3-v4 kan angive forskellige cifre eller tegn, men skal starte med et numeriske ciffer. Ved sammenligning af softwareversionen sammenlignes v1-v2-v3-v4 efter hinanden, og cifrene længst til venstre har forrang i forhold til de efterfølgende.

Hvis v[x] kun indeholder numeriske cifre, sammenlignes cifrene, hvis v[x] indeholder cifre + alfanumeriske tegn, sammenlignes cifre først, og derefter sammenlignes tegn i alfabetisk rækkefølge.

Eksempel på gyldigt versionsnummer

sipyyyy.11-0-0MPP-BN

Modsat: 11.0.0 er et ugyldigt format.

Sammenligning

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

Strenge i anførselstegn kan sammenlignes for lighed eller ulighed. Heltal og versionsnumre kan også sammenlignes regnemæssigt. Sammenligningsoperatorerne kan udtrykkes som symboler eller akronymer. Akronymer er praktiske til at udtrykke betingelsen i en Open-formatprofil.

Operatør	Alternativ syntaks	Beskrivelse	Gælder for heltal og versionsoperander	Gælder for operander til strenge i anførselstegn
=	eq	lig med	Ja	Ja
!=	ne	ikke lig med	Ja	Ja
<	lt	mindre end	Ja	Nej
<=	le	mindre end eller lig med	Ja	Nej
>	gt	større end	Ja	Nej
>=	ge	større end eller lig med	Ja	Nej
OG		og	Ja	Ja

Det er vigtigt at sætte makrovariabler i dobbelte anførselstegn, hvis der forventes en strengkonstant. Hvis det ikke sker, forventes et tal eller versionsnummer.

Når betingede udtryk bruges sammen med parametrene Profile_Rule* (Profilregel*) og Upgrade_Rule (Opgraderingsregel), skal der sættes anførselstegn om betingede udtryk med syntaksen "(expr)?" som i dette eksempel på en opgraderingsregel. Husk, at BN betyder buildnummer.

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

Brug ikke den forudgående syntaks med parenteser til at konfigurere parametrene Resync_Trigger_ * (Gensynkroniseringsudløser).

URL-syntaks

Brug standard-URL-syntaksen til at angive, hvordan du henter konfigurationsfiler og firmware henholdsvis i parametrene Profile_Rule* (Profilregel) og Upgrade_Rule (Opgraderingsregel). Syntaksen er som følger:

`[ skema:// ] [ server [:port]] filsti`

Hvor **`skema`** er en af disse værdier:

- tftp
- http
- https

Hvis **skema** er udeladt, antages tftp. Serveren kan være et DNS-genkendt værtsnavn eller en numerisk IP-adresse. Porten er destinations-UDP eller TCP-portnummeret. Filstien skal begynde med rodmappen (/); det skal være en absolut sti.

Hvis **server** mangler, bruges den tftp-server, der er angivet via DHCP (indstilling 66).

Bemærk Når det gælder opgraderingsregler, skal serveren angives.

Hvis **port** mangler, bruges standardporten for det angivne skema. Tftp anvender UDP-port 69, http bruger TCP-port 80, https anvender TCP-port 443.

Der skal være en filsti. Den behøver ikke nødvendigvis henvise til en statisk fil, men kan angive dynamisk indhold, der hentes via CGI.

Makroudvidelse gælder 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 bruger DHCP-indstilling 66, understøttes tom syntaks ikke af opgraderingsreglerne. Dette gælder kun for profilregel*.

RFC 8188-baseret kryptering af HTTP-indhold

Telefonen understøtter RFC 8188-baseret kryptering af HTTP-indhold med AES-128-GCM-beregning for konfigurationsfiler. Med denne krypteringsmetode kan enhver enhed læse HTTP-meddelelsesheaderne. Det er dog kun de enheder, der kender IKM (Input Keying Material), som også kan læse selve meddelelsen. Når telefonen er klargjort med IKM, kan telefonen og klargøringsserveren udveksle konfigurationsfilerne på sikker vis. Det giver netværkselementer fra tredjeparter mulighed for at bruge meddelelsesheaderne til analyse og overvågning.

XML-konfigurationsparameteren **IKM_HTTP_Encrypt_Content** indeholder IKM på telefonen. Denne parameter er af sikkerhedsmæssige årsager ikke tilgængelig på websiden til administration af telefonen. Den kan heller ikke ses i telefonens konfigurationsfil, som du kan få adgang til fra telefonens IP-adresse, eller fra telefonens konfigurationsrapporter, som sendes til klargøringsserveren.

Hvis du vil bruge RFC 8188-baseret kryptering, skal du sikre følgende:

- Klargør telefonen med IKM ved at angive IKM med XML-parameteren **IKM_HTTP_Encrypt_Content** i konfigurationsfilen, der sendes fra klargøringsserveren til telefonen.
- Hvis denne kryptering anvendes på de konfigurationsfiler, der sendes fra klargøringsserveren til telefonen, skal du sikre, at HTTP-headeren *Content-Encoding* i konfigurationsfilen er "aes128gcm".

  Hvis headeren ikke findes, får metoden AES-256-CBC førsteprioritet. Telefonen anvender AES-256-CBC-kryptering, hvis der findes en AES-256-CBC-nøgle i en profilregel, uanhængigt af IKM.
- Hvis telefonen skal anvende denne kryptering til de konfigurationsrapporter, der sendes til klargøringsserveren, skal du sikre, at der ikke er angivet en AES-256-CBC-nøgle i rapportreglen.

Valgfri argumenter til gensynkronisering

Valgfri argumenter, **key**, **uid** og **pwd**, kan komme før de URL-adresser, der er angivet i parameteren Profile_Rule* (Profilregel), der samlet er omsluttet af kantede parenteser.

Nøgle

Indstillingen **--key** angiver, at den konfigurationsfil, som telefonen modtager fra klargøringsserveren, er krypteret med AES-256-CBC kryptering, medmindre headeren *Content-Encoding* i filen angiver "aes128gcm"-kryptering. Selve nøglen er angivet som en streng efter **--key**. Nøglen kan eventuelt angives i dobbelte anførselstegn ("). Telefonen bruger nøglen til at dekryptere konfigurationsfilen.

Eksempler på brug

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

De valgfri argumenter i kantede parenteser er makroudvidet. Parametrene for specielle formål GPP_SA til og med GPP_SD er kun makroudvidede ind i makrovariabler $SA til og med $SD, når de bruges som nøgleindstillingsargumenter. Se disse eksempler:

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

I åbne formatprofiler skal argumentet til **--key** skal være det samme som argumentet til den indstilling **-k**, der er givet til **openssl**.

uid og pwd

Indstillingerne **uid** og **pwd** kan bruges til at angive bruger-id og adgangskodegodkendelse for den angivne URL-adresse. De valgfri argumenter i kantede parenteser er makroudvidet. Parametrene for specielle formål GPP_SA til og med GPP_SD er kun makroudvidede ind i makrovariabler $SA til og med $SD, når de bruges som nøgleindstillingsargumenter. Se disse eksempler:

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

[--uid $SA -pwd $SB] https://klargøringsserver_url/sti_til_din_konfiguration/din_konfiguration.xml

ville derefter blive udvidet til:

[--uid MyUserID -pwdMinHemmeligeAdgangskode]
https://klargøringsserver_url/sti_til_din_konfiguration/din_konfiguration.xml

Anvend en brugerprofil på enheden med IP-telefoni

Når du opretter et XML-script til konfiguration, skal den videregives til telefonen for at blive anvendt. For at anvende konfigurationen kan du enten downloade konfigurationsfilen på telefonen fra en TFTP-, HTTP- eller HTTPS-server via en webbrowser eller ved hjælp af kommandolinjeværktøjet cURL.

Download konfigurationsfilen til telefonen fra en TFTP-Server

Benyt følgende fremgangsmåde til at downloade konfigurationsfilen til et TFTP-serverprogram på din pc.

Fremgangsmåde

Trin 1 Tilslut din pc til telefon-LAN'et:

Trin 2 Kør et TFTP-serverprogram på pc'en, og sørg for, at konfigurationsfilen findes i TFTP-rodmappen.

Trin 3 Gå til en webbrowser, angiv telefonens LAN-IP-adresse, IP-adressen på computeren, filnavnet og logonlegitimationsoplysningerne. Brug dette format:

http://<WAN_IP_Adresse>/admin/resync?tftp://<PC_IP_Address>/<filnavn>&xuser=admin&xpassword=<password>

Eksempel:

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

Download konfigurationsfilen til telefonen med cURL

Benyt følgende fremgangsmåde for at hente konfigurationen til telefonen ved hjælp af cURL. Dette kommandolinjeværktøj bruges til at overføre data med en URL-syntaks. Du kan downloade cURL på:

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

Bemærk Vi anbefaler, at du ikke bruger cURL til at sende konfigurationen til telefonen, da brugernavnet og adgangskoden måske kan blive opfanget under brug af cURL.

Fremgangsmåde

Trin 1 Slut pc'en til LAN-porten på telefonen.

Trin 2 Download konfigurationsfil til telefonen ved at indtaste følgende cURL-kommando:

```
curl -d @my_config.xml
"http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin"
```

Klargøringsparametre

Dette afsnit beskriver de klargøringsparametre, der i store træk er organiseret efter funktion:

Disse typer klargøringsparametre findes:

- Generelle formål
- Aktiveringsfunktioner

- Udløsere
- Konfigurerbare tidsplaner
- Profilregler
- Opgraderingsregel

Parametre for generelle formål

Parametrene for generelle formål GPP_* (**Administratorlogon** > **Adanceret** > **Tale** > **Klargøring**) bruges som fri strenge og registreres ved konfiguration af telefonen for at interagere med en bestemt klargøringsserverløsning. Parametrene GPP_ * er som standard tomme. De kan konfigureres til at indeholde forskellige værdier, herunder følgende:

- Krypteringsnøgler
- URL-adresser
- Oplysninger om status ved klargøring i flere faser
- Skabeloner for Post-anmodninger
- Tilknytninger til alias for parameternavn
- Delvise strengværdier, eventuelt samlet til komplette parameterværdier.

GPP_ * parametrene kan bruges til makroudvidelse i andre klargøringsparametre. Til dette formål er makronavne på ét bogstav (A til og med P) nok til at identificere indholdet af GPP_A til og med GPP_P. Derudover identificerer makronavne med to store bogstaver SA til og med SD GPP_SA som GPP_SD som et specialtilfælde ved brug som argumenter i følgende URL-adresseindstillinger:

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

Disse parametre kan bruges som variabler i klargørings- og opgraderingsregler. Der refereres til dem ved at foranstille variabelnavnet med et '$'-tegn, f.eks. $GPP_A.

Brug parametre for generelle formål

Hvis GPP_A f.eks. indeholder strengen ABC, og GPP_B indeholder 123, udvides AB-makroen til ABC123.

Inden du begynder

Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Fremgangsmåde

Trin 1 Vælg **Tale** > **Klargøring**.

Trin 2 Rul ned til afsnittet **Parametre for generelle formål**.

Trin 3 Angiv gyldige værdier i felterne GPP A til og med GPP P.

Trin 4 Klik på **Send alle ændringer**.

Aktiveringsfunktioner

Parametrene Provision_Enable (Aktivér klargøring) og Upgrade_Enable (Aktivér opgradering) styrer alle handlinger med gensynkronisering af profiler og firmwareopgraderinger. Disse parametre styrer gensynkroniseringer og opgraderinger uafhængigt af hinanden. Disse parametre styrer også UTL-kommandoer for gensynkronisering og opgradering, der udstedes gennem administrationswebserveren. Begge disse parametre er indstillet til **Ja** som standard.

Parameteren Resync_From_SIP (Gensynkroniser fra SIP) styrer anmodninger om gensynkronisering. En SIP NOTIFY-hændelse sendes fra tjenesteudbyderens proxyserver til telefonen. Hvis indstillingen er aktiveret, kan proxyen anmode om en gensynkronisering. For at kunne gøre dette sender proxyen en SIP NOTIFY-meddelelse, der indeholder hændelsen: gensynkroniser header til enheden.

Enheden udfordrer anmodningen med et 401-svar (godkendelse nægtet for anvendte legitimationsoplysninger). Enheden forventer en efterfølgende anmodning, der er godkendt, før den oveholder gensynkroniseringsanmodning fra proxyen. Headerne Hændelse: reboot_now (reboot nu) og Hændelse: restart_now (genstart nu) giver henholdsvis kolde og varme, hvilket også udfordres.

De to resterende aktiveringsfunktioner er Resync_On_Reset (Gensynkroniser ved nulstilling) og Resync_After_Upgrade_Attempt (Gensynkroniser efter opgraderingsforsøg). Disse parametre afgør, om enheden udfører en gensynkroniseringshandling, når den tændes, softwaren rebooter og efter hvert opgraderingsforsøg.

Når Resync_On_Reset (Gensynkroniser ved nulstilling) er aktiveret, introducerer enheden en vilkårlig forsinkelse, der følger startsekvensen, før nulstillingen udføres. Forsinkelsen er et vilkårligt tidspunkt op til den værdi, som Resync Random Delay (Vilkårlig forsinkelse på gensynkronisering) (i sekunder) angiver. I en gruppe af telefoner, der tændes samtidigt, spreder denne forsinkelse starttidspunkterne for gensynkroniseringsanmodningerne ud for hver enhed. Denne funktion kan være nyttig ved installationer i stort boligområde, hvis der skulle ske et strømnedbrud.

Udløsere

Telefonen giver dig mulighed at gensynkronisere efter bestemte intervaller eller på et bestemt tidspunkt.

Gensynkroniser efter bestemte intervaller

Telefonen er designet til periodisk at gensynkronisere med klargøringsserveren. Gensynkroniseringsintervallet er konfigureret i Resync_Periodic (Gensynkroniser periodisk) (sekunder). Hvis denne værdi er tom, gensynkroniseres enheden ikke periodisk.

Gensynkroniseringen sker typisk, når talelinjerne er inaktive. Når en talelinje er aktiv, når der skal ske en gensynkronisering, forsinker telefonen gensynkroniseringsproceduren, indtil linjen bliver inaktiv igen. En gensynkronisering kan medføre, at værdier i konfigurationsparametre ændres.

En gensynkroniseringshandling kan mislykkes, fordi telefonen ikke er i stand til at hente en profil fra serveren, den downloadede fil er beskadiget, eller der er opstået en intern fejl. Enheden forsøger at gensynkronisere igen efter et tidsrum, der er angivet i Resync Error Retry Delay (Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl) (sekunder). Hvis Resync Error Retry Delay (Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl) er indstillet til 0, forsøger enheden ikke at synkronisere igen efter et mislykket forsøg på gensynkronisering.

Hvis en opgradering mislykkes, udføres der et nyt forsøg efter en retry efter Upgrade Error Retry Delay (Forsinkelse på forsøg ved opgraderingsfejl) sekunder.

To konfigurerbare parametre er tilgængelige til betinget at udløse en gensynkronisering: Resync_Trigger_1 (Udløser 1 af gensynkronisering) og Resync_Trigger_2 (Udløser 2 af gensynkronisering). Hver parameter kan programmeres med et betinget udtryk, der udsættes for en makroudvidelse. Når gensynkroniseringsintervallet udløber (tid til den næste gensynkronisering), vil udløserne forhindre gensynkronisering, medmindre en eller flere udløsere evalueres som sande, hvis de er indstillet.

Det følgende eksempel udløser en betinget gensynkronisering. I eksemplet har det seneste forsøg på opgradering af telefonen varet mere end 5 minutter (300 sekunder), og mindst 10 minutter (600 sekunder) er gået, siden det sidste forsøg på gensynkronisering.

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

Gensynkroniser på et bestemt tidspunkt

Parameteren Resync_At (Gensynkroniser kl.) giver telefonen mulighed for at gensynkronisere på et bestemt tidspunkt. Denne parameter bruger 24-timers formatet (ttmm) til at angive tid.

Parameteren Resync_At_Random_Delay (Vilkår forsinkelse på gensynkroniseringstidspunkt) giver telefonen mulighed for at gensynkronisere med en ukendt forsinkelse i tid. Denne parameter bruger et positivt heltalsformat til at angive tiden.

Det skal undgås at oversvømme serveren med gensynkroniseringsanmodninger fra flere telefoner, der er angivet til blive gensynkroniseret på samme tidspunkt. For at gøre det udløser telefonen gensynkroniseringen op til 10 minutter efter det angivne tidspunkt.

Hvis du f.eks. indstiller gensynkroniseringstiden til 1000 (10 om morgenen), udløser telefonen gensynkronisering på et hvilket som helst tidspunkt 10:00 og 10:10 om morgenen.

Denne funktion er som standard deaktiveret. Hvis parameteren Resync_At (Gensynkroniser kl.) er klargjort, ignoreres parameteren Resync_Periodic (Gensynkroniser periodisk).

Konfigurerbare tidsplaner

Du kan konfigurere tidsplaner for periodiske gensynkroniseringer, og du kan angive intervaller for nye forsøg på gensynkronisering og opgraderingsfejl ved hjælp af disse klargøringsparametre:

- Resync Periodic (Gensynkroniser periodisk)
- Resync Error Retry Delay (Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl)
- Upgrade Error Retry Delay (Forsinkelse på forsøg ved opgraderingsfejl)

Hver parameter accepterer en enkelt forsinkelsesværdi (sekunder). Den nye udvidede syntaks giver mulighed for en kommasepareret liste over på hinanden følgende forsinkelseselementer. Det sidste element i rækkefølgen vil implicit blive gentaget uden tidsbegrænsning.

Du kan også vælge at bruge et plustegn til at angive en anden numerisk værdi, der tilføjer en vilkårlig ekstra forsinkelse.

Eksempel 1

I dette eksempel gensynkroniserer telefonen periodisk hver 2. time. Hvis en gensynkronisering giver fejl, forsøger enheden efter følgende intervaller: 30 minutter, 1 time, 2 timer, 4 timer. Enheden fortsætter med at prøve efter 4-timers intervaller, indtil gensynkroniseringen lykkes.

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

Eksempel 2

I dette eksempel gensynkroniserer enheden hver time (plus en ekstra vilkårlig forsinkelse på op til 10 minutter). I tilfælde af en gensynkroniseringsfejl forsøger enheden efter disse følgende intervaller: 30 minutter (plus op til 5 minutter). 1 time (plus op til 10 minutter), 2 timer (plus op til 15 minutter). Enheden fortsætter med at prøve efter 2-timers intervaller (plus op til 15 minutter), indtil gensynkroniseringen lykkes.

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

Eksempel 3

I dette eksempel prøver enheden opgradering igen efter 30 minutter, hvis et eksternt forsøg på opgradering mislykkes, og derefter en gang mere efter en time og derefter efter to timer. Hvis opgraderingen stadig mislykkes, forsøges hver fjerde til femte time, indtil opgraderingen lykkes.

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

Profilregler

Telefonen har flere parametre for eksterne konfigurationsprofiler (Profile_Rule*) (Profilregel*). Hver enkelt gensynkronisering kan således hente flere filer, som administreres af forskellige servere.

I det mest enkle scenarie gensynkroniserer enheden periodisk til en enkelt brugerprofil på en central server, der opdaterer alle relevante interne parametre. Alternativt kan profilen blive delt mellem forskellige filer. En fil er fælles for alle telefoner i en installation. En separat entydig fil er angivet for hver konto. Krypteringsnøgler og certifikatoplysninger kan leveres af en helt anden stadig profil, der gemmes på en separat server.

Hver gang en gensynkronisering forfalder, evaluerer telefonen de fire Profile_Rule*-parametre efter hinanden:

1. Profile_Rule (Profilregel)
2. Profile_Rule_B (Profilregel_B)
3. Profile_Rule_C (Profilregel_C)
4. Profile_Rule_D (Profilregel_D)

Hver evaluering kan resultere i, at der hentes en profil fra en ekstern klargøringsserver og mulighed for opdatering af et antal interne parametre. Hvis en evaluering mislykkes, afbrydes sekvensen af gensynkroniseringer og forsøges igen forfra, hvilket er angivet i parameteren Resync Error Retry Delay (Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl) (sekunder). Hvis alle evalueringer gennemføres, venter enheden på den anden, der er angivet ved hjælp af parameteren Resync_Periodic (Gensynkroniser periodisk), og udfører derefter en anden gensynkronisering.

Indholdet af hver parameter Profile_Rule* (Profilregel) består af et sæt alternativer. Alternativerne adskilles med tegnet| (pipe). Hvert alternativ består af et betinget udtryk, et tildelingsudtryk, en profil-URL-adresse og eventuelle tilknyttede URL-indstillinger. Alle disse komponenter er valgfri inden for de enkelte alternativer. Følgende er de gyldige kombinationer samt den rækkefølge, de skal vises i, hvis de findes:

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

Inden for hver Profile_Rule*-parameter skal alle alternativer, med undtagelse af den sidste, indeholde et betinget udtryk. Dette udtryk evalueres og behandles på følgende måde:

1. Betingelser evalueres fra venstre mod højre, indtil der findes en, der evalueres som sand (eller indtil der findes et alternativ uden et betinget udtryk).
2. Et eventuelt medfølgende tildelingsudtrykket evalueres, hvis det findes.
3. Hvis en URL-adresse er angivet som en del af det pågældende alternativ, gøres der et forsøg på at hente den profil, der er placeret ved den angivne URL-adresse. Systemet forsøger at opdatere de interne parametre i overensstemmelse hermed.

Hvis alle alternativer har betingede udtryk, og ingen evalueres til at være sand (eller hvis det hele profilreglen er tom), ignoreres hele Profile_Rule*-parameteren. Den næste profilregelparameter i sekvensen er evalueres.

Eksempel 1

Dette eksempel gensynkroniserer ubetinget til profilen på den angivne URL-adresse og udfører en HTTP GET-anmodning til den eksterne klargøringsserver:

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

Eksempel 2

I dette eksempel gensynkroniserer enheden til to forskellige URL-adresser, afhængigt af registreringstilstanden for linje 1. Hvis registreringen er gået tabt, udfører enhederne en HTTP POST til et CGI-script. Enheden sender indholdet af den makroudvidede udvidet GPP_A, hvilket kan angive yderligere oplysninger om enhedens tilstand:

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

Eksempel 3

I dette eksempel gensynkroniserer enheden til den samme server. Enheden giver yderligere oplysninger, hvis et certifikat ikke er installeret på enheden (for ældre enheder før 2.0):

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

Eksempel 4

I dette eksempel er linje 1 deaktiveret, indtil GPP_A indstilles til lig med klargjort via den første URL-adresse. Derefter gensynkroniseres den til den anden URL-adresse:

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

Eksempel 5

I dette eksempel antages det, at den profil, som serveren returnerer, indeholder XML-elementkoder. Disse mærker skal gentilknyttes til de rigtige parameternavne af den aliastilknytning, der er gemt i GPP_B:

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

En gensynkronisering anses typisk for at være mislykket, hvis en anmodet profil ikke modtages fra serveren. Parameteren Resync_Fails_On_FNF (Gensynkronisering mislykkes ved FNF) kan tilsidesætte denne standardvirkemåde. Hvis Resync_Fails_On_FNF (Gensynkronisering mislykkes ved FNF) er indstillet til Nej, accepterer enheden svaret "fil ikke fundet" fra serveren som en gennemført gensynkronisering. Standardværdien for Resync_Fails_On_FNF (Gensynkronisering mislykkes ved FNF) er Ja.

Opgraderingsregel

Opgraderingsregel fortæller enheden, at en ny load skal aktiveres, og hvor loaden kan hentes, hvis det er nødvendigt. Hvis loaden allerede er på enheden, forsøger den ikke at hente loaden. Det betyder altså, at gyldigheden af loadplaceringen ikke har nogen betydning, når de ønskede loads er i den inaktive partition.

Upgrade_Rule (Opgraderingsregel) angiver en firmwareload, der overføres og anvendes, hvis den er forskellig fra den aktuelle load, medmindre den er begrænset af et betinget udtryk, eller Upgrade_Enable (Aktivér opgradering) er indstillet til **Nej**.

Telefonen har en konfigurerbar ekstern opgraderingsparameter, Upgrade_Rule (Opgraderingsregel). Denne parameter accepterer syntaks svarende til profilregelparametrene. Indstillinger for URL-adresser understøttes ikke for opgraderinger, men betingede udtryk og tildelingsudtryk kan bruges. Hvis der bruges betingede udtryk, kan parameteren udfyldes med flere alternativer adskilt af tegnet |. Syntaksen for hvert alternativ er som følger:

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

Som det også var tilfældet med parametrene Profile_Rule* (Profilregel*), evaluerer parameteren Upgrade_Rule (Opgraderingsregel) hvert enkelt alternativ, indtil det betingede udtryk er opfyldet, eller et alternativ ikke har et betinget udtryk. Det medfølgende tildelingsudtryk evalueres, hvis det angives. Derefter forsøges en opgradering til den angivne URL-adresse.

Hvis Upgrade_Rule (Opgraderingsregel) indeholder en URL-adresse uden et betinget udtryk, opgraderer enheden til den firewareafbildning, der angiver URL-adressen. Efter makroudvidelse og evaluering af reglen forsøger enheden ikke på at opgradere igen, før reglen ændres eller den gældende kombination af skemaet + server + port + filsti ændres.

Enheden deaktiverer lyden i starten af proceduren for at forsøge en opgradering af firmware og genstarter i slutningen af proceduren. Enheden starter kun en opgradering, der styres af indholdet af i Upgrade_Rule (Opgraderingsregel) automatisk, hvis alle talelinjerne er inaktive i øjeblikket.

F.eks.

- For Cisco IP 6800-serien:

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

  where BN==Build Number
  ```

I dette eksempel opgraderer Upgrade_Rule (Opgraderingsregel) firmwaren til den afbildning, der er lagret på den angivne URL-adresse.

Her er et andet 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 eksempel får enheden til at indlæse et af to billeder, baseret på indholdet af en parameter for generelle formål GPP_F.

Enheden kan gennemtvinge en nedgraderingsgrænse med hensyn til firmwarens versionsnummer, som kan være en nyttig tilpasningsindstilling. Hvis et gyldigt firmwareversionsnummer er konfigureret i parameteren Downgrade_Rev_Limit (Grænse for nedgraderingsrevision), afviser enheden opgraderingsforsøg for firmwareversioner, der ligger før den angivne grænse.

Datatyper

Følgende datatyper anvendes med konfigurationsprofilparametre:

- {a,b,c,…} – et valg mellem a, b, c, …
- Boolesk – boolesk værdi med enten "ja" eller "nej".
- CadScript – et miniscript, der angiver kadanceparametrene for et signal. Op til 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 kaldes en sektion.
  - $on_{i,j}$ og $off_{i,j}$ er til/fra-varigheden i sekunder af et *segment*. i = 1 eller 2 og j = 1 til 6.
  - D_i er den samlede varighed af sektionen i sekunder.

  Alle varigheder kan have op til tre decimaler for at give trin på 1 ms. Jokertegnet "*" betyder tidsubegrænset varighed. Segmenter i en sektion afspilles i rækkefølge og gentages, indtil den samlede varighed er blevet afspillet.

  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 – karakteristisk 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 – scriptingsyntaks, der bruges til at angive opkaldsplanerne Linje 1 og Linje 2.
- Float<n> – en flydende punktværdi med op til n decimaler.
- FQDN – Fully Qualified Domain Name. Det kan indeholde op til 63 tegn. Der er følgende eksempler:
  - sip.Cisco.com:5060 eller 109.12.14.12:12345
  - sip.Cisco.com eller 109.12.14.12
- FreqScript – et miniscript, som angiver parametrene for frekvens og niveau for en tone. Indeholder op til 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 (kun heltal uden fortegn).
  - L_1– L_6 er tilsvarende niveauer i dBm (med op til en decimal).

  Mellemrum før og efter et komma er tilladt, men anbefales ikke.

  Eksempel 1 – tone for ventende opkald:

```
440@-10

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

  Eksempel 2 – ringetone:

```
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 form af x.x.x.x, hvor x er mellem 0 og 255. Eksempel: 10.1.2.100.
- Bruger-id – bruger-id, som det vises i en URL-adresse; op til 63 tegn.
- Telefon – en telefonnummerstreng, f.eks. 14081234567, * 69, * 72, 345678; eller en generisk URL-adresse, f.eks. 1234@10.10.10.100:5068 eller jsmith@Cisco.com. Strengen kan indeholde op til 39 tegn.
- PhTmplt – en telefonnummerskabelon. Hver skabelon kan indeholde et eller flere mønstre, der er adskilt med komma (,). Mellemrum i begyndelsen af hvert mønster ignoreres. "?" og "*" repræsenterer jokertegn. Brug % xx til at repræsentere konstanter. %2a repræsenterer f.eks. *. Skabelonen kan indeholde op til 39 tegn. Eksempler: “1408*, 1510*”, “1408123????, 555?1.”.
- Port – TCP/UDP-portnummer (0-65535). Det kan angives i decimal- eller hex-format.

- ProvisioningRuleSyntax – scriptingsyntaks, der bruges til at definere regler for konfigurationsgensynkronisering og firmwareopgraderinger.
- PwrLevel – strømniveau udtrykt i dBm med en decimal, f.eks. -13,5 eller 1,5 (dBm).
- RscTmplt – en skabelon for SIP-svarstatuskoden, f.eks. “404, 5*”, “61?”, “407, 408, 487, 481”. Det kan indeholde op til 39 tegn.
- Sig<n> – n-bitværdi med fortegn. Det kan angives i decimal- eller hex-format. Et "-"-tegn skal stå før negative værdier. Et +-tegn kan sættes før positive værdier.
- Stjernekoder – aktiveringskode til en supplerende tjeneste, f.eks. * 69. Koden kan indeholde op til 7 tegn.
- Str<n> – en generisk streng med op til n ikke-reserverede tegn.
- Time<n> – tidsvarighed i sekunder, med op til n decimalpladser. Ekstra angivne decimaler ignoreres.
- ToneScript – et miniscript, der angiver frekvens, niveau og kadenceparametrene for en tone i et igangværende opkald. Script kan indeholde op til 127 tegn.

  Syntaks: FreqScript;Z_1[;Z_2].

  Z_1-sektionen svarer til S_1-sektionen i et CadScript, med undtagelse af at hvert til/fra segment efterfølges af en parameter for frekvenskomponenter: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$ hvor:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ angiver frekvenskomponenterne i det FreqScript, der bruges i dette segment.

  Hvis der bruges end én frekvenskomponent i et segment, summeres komponenterne sammen.

  Eksempel 1 – ringetone:

```
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 – hakkende tone:

```
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-bitværdi uden fortegn, hvor n = 8, 16 eller 32. Det kan angives i decimal- eller hex-format, f.eks. 12 eller 0x18, så længe værdien kan være i n bit.

Bemærk Overvej disse:

- <Par Name> repræsenterer et navn på en konfigurationsparameter. I en profil dannes den tilhørende kode ved at erstatte mellemrummet med et understregningstegn "_", f.eks. **Par_Name**.
- Et tomt standardværdifeltet indebærer en tom streng < "" >.
- Telefonen fortsætter med at bruge de sidste konfigurerede værdier for koder, der ikke findes i en bestemt profil.
- Skabeloner sammenlignes i den angivne rækkefølge. Det første, *ikke tætteste*, match vælges. Parameternavnet skal matche helt nøjagtigt.
- Hvis der er angivet mere end én definition for en parameter i en profil, vil en sådan sidste definition i filen være den, der aktiveres på telefonen.
- En parameterspecifikation med en tom parameterværdi tvinger parameteren tilbage til dens standardværdi. For i stedet at angive en tom streng skal du bruge en tom streng "" som parameterværdien.

Profilopdateringer og firmwareopgradering

Telefonen understøtter sikker fjernklargøring (konfiguration) og firmwareopgraderinger. En telefon, der ikke er klargjort, kan modtage en krypteret profil, der er målrettet til den pågældende enhed. Telefonen kræver ikke en eksplicit nøgle på grund af en sikker førstegangsmekanisme til klargøring, der bruger SSL-funktionalitet.

Brugeren skal ikke enten starte eller udføre en profilopdatering eller firmwareopgradering, eller hvis mellemliggende opgraderinger kræves for at nå en fremtidig opgraderingstilstand fra en ældre version. En profilgensynkronisering forsøges kun, når telefonen er inaktiv, fordi en gensynkronisering kan udløse en softwaregenstart og afbryde et opkald.

Parametre for generelle formål administrerer klargøringsprocessen. Hver enkelt telefon kan konfigureres til at kontakte en NPS (normal provisioning server) regelmæssigt. Kommunikationen med NPS kræver ikke brug af en sikker protokol, fordi den opdaterede profil er krypteret med en delt hemmelig nøgle. NPS kan være en standard-TFTP, HTTP- eller HTTPS-server med klientcertifikater.

Administratoren kan opgradere, reboote, genstarte eller gensynkronisere telefoner ved hjælp af telefonens webbrugergrænseflade. Administratoren kan også udføre disse opgaver ved hjælp af en SIP-beskedmeddelelse.

Konfigurationsprofiler genereres ved hjælp af almindeligt forekommende open source-værktøjer, der integreres med tjenesteudbyderens klargøringssystemer.

Lignende emner

Tillad og konfigurer profilopdateringer, på side 34

Tillad og konfigurer profilopdateringer

Profilopdateringer kan tillades ved angivne intervaller. Opdaterede profiler sendes fra en server til telefonen ved hjælp af TFTP, HTTP eller HTTPS.

Inden du begynder

Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Fremgangsmåde

Trin 1 Vælg **Tale** > **Klargøring**.
Trin 2 I sektionen **Konfigurationsprofil** skal du vælge **Ja** på rullelisten **Aktivér klargøring**.
Trin 3 Angiv parametrene.
Trin 4 Klik på **Send alle ændringer**.

Lignende emner

Profilopdateringer og firmwareopgradering, på side 34

Tillad og konfigurer firmwareopgraderinger

Firmwareopdateringer kan tillades ved angivne intervaller. Opdateret firmware sendes fra en server til telefonen ved hjælp af TFTP eller HTTP. Sikkerhed er et mindre problem i forhold til en firmwareopgradering, fordi firmware ikke indeholder personlige oplysninger.

Inden du begynder

Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Fremgangsmåde

Trin 1 Vælg **Tale** > **Klargøring**.
Trin 2 I sektionen **Firmwareopgradering** skal du vælge **Ja** på rullelisten **Aktivér opgradering**.
Trin 3 Angiv parametrene.
Trin 4 Klik på **Send alle ændringer**.

Firmwareopgradering af TFTP, HTTP eller HTTPS

Telefonen understøtter opgradering af én enkelt afbildning af TFTP, HTTP eller HTTPS.

Bemærk Nedgraderinger til tidligere versioner er muligvis ikke tilgængelige for alle enheder. Få flere oplysninger i telefonens release-notes og firmwareversion.

Inden du begynder

Firmwaredownload filen skal overføres til en tilgængelig server.

Fremgangsmåde

Trin 1 Omdøb billedet på følgende måde:

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

hvor:

`x8xx` r telefonserien, f.eks. 6841.

`AA-b-c` er frigivelsesnummeret, f.eks. 10-4-1

Trin 2 Brug kommandoen **`tar-- xzvf`** til at udpakke tar-pakken.

Trin 3 Kopier mappen til en TFTP-, HTTP-, eller HTTPS-downloadmappe.

Trin 4 Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Trin 5 Vælg **Tale** > **Klargøring**.

Trin 6 Find loadfilnavnet, der slutter med **.loads**, og føj det til den gyldige URL-adresse.

Trin 7 Klik på **Send alle ændringer**.

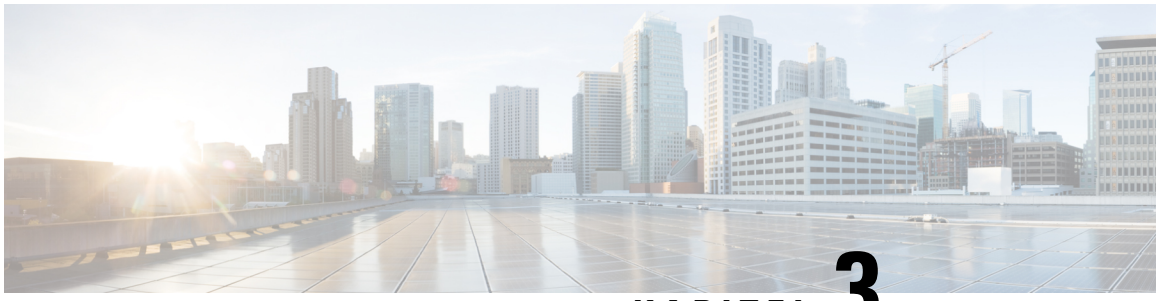
Opgrader firmware med en browserkommando

En opgraderingskommando, der er indtastet i browserens adresselinje, kan bruges til at opgradere firmware på en telefon. Telefonen opdateres kun, når den er inaktiv. Opdateringen forsøges automatisk, når opkaldet er afsluttet.

Fremgangsmåde

Hvis du vil opgradere telefonen med en URL-adresse i en webbrowser, skal du skrive følgende kommando:

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



KAPITEL 3

Forhåndsklargøring og klargøringsservere internt

Forhåndsklargøring og klargøringsservere internt

Tjenesteudbyderen forhåndsklargør telefoner, bortset fra RC-enheder, med en profil. Forhåndsklargøringsprofilen kan omfatte et begrænset sæt parametre, der gensynkroniserer telefonen. Profilen kan også bestå af et komplet sæt parametre, som fjernserveren leverer. Som standard synkroniseres telefonen igen, når den tændes, og efter intervaller, der er konfigureret i profilen. Når brugeren forbinder telefonen hos kunden, downloader enheden den opdaterede profil og eventuelle firmwareopdateringer.

Denne proces med forhåndsklargøring, installation og ekstern klargøring kan udføres på mange måder.

Serverforberedelse og softwareværktøjer

Eksemplerne i dette kapitel kræver, at en eller flere servere er tilgængelige. Disse servere kan være installeret og køre på en lokal pc:

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

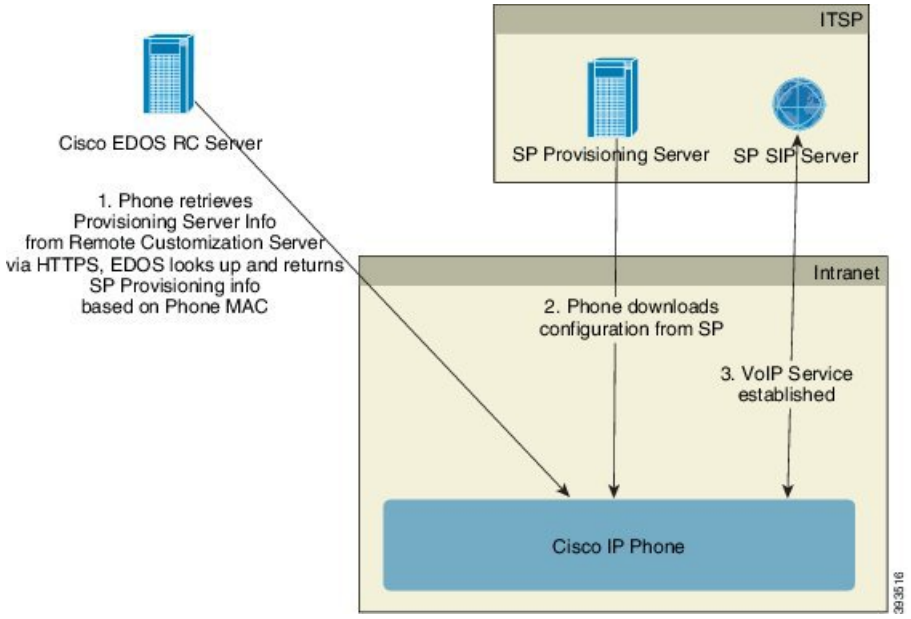
Hvis du vil foretage en fejlfinding af serverkonfigurationen, er det nyttigt at installere klienter for hver type server på en separat servermaskine. Denne fremgangsmåde sikrer, at serveren fungerer korrekt, uafhængigt af interaktionen med telefonerne.

Vi anbefaler også, at du installerer disse softwareværktøjer:

- Hvis du vil generere konfigurationsprofiler, skal du installere komprimeringsværktøjet gzip, der er open source.

- Når det gælder profilkryptering og HTTPS-funktioner, skal du installere OpenSSL-programpakken, der er open source.
- For at teste den dynamiske profiloprettelse 1-trins ekstern klargøring ved hjælp af HTTPS anbefaler vi et scriptsprog med understøttelse af CGI-scripting. Perl-sprogværktøjerne, der er open source, er et eksempel på et scriptingsprog.
- For at kontrollere sikre udvekslinger mellem klargøringsservere og telefonerne skal du installere en Ethernet-pakkesniffer (som f.eks. Ethereal/Wireshark), der frit kan downloades. Registrer en Ethernet-pakkesporing af interaktionen mellem telefonen og klargøringsserveren. Det gør du ved at køre pakkesnifferen på en pc, der er tilknyttet til en switch med portspejling aktiveret. Du kan bruge værktøjet ssldump til HTTPS-transaktioner.

RC-distribution (Remote Customization)



Alle telefoner kontakter Cisco EDOS RC-serveren, indtil de først er blevet klargjort.

I en RC-distributionsmodel køber kunder en telefon, der allerede er knyttet til en bestemt tjenesteudbyder på Cisco EDOS RC-serveren. ITSP (Internet telefoni Service Provider) konfigurerer og vedligeholder en klargøringsserver og registrerer oplysninger om klargøringsserveren på Cisco EDOS RC-serveren.

Når telefonen er tændt og har en internetforbindelse, er tilpasningstilstanden af den ikke klargjorte telefon **åben**. Telefonen laver først en forespørgsel til den lokale DHCP-server for at få oplysninger om klargøringsserveren og indstiller telefonens tilpasningstilstand. Hvis DHCP-forespørgslen gennemføres, indstilles tilpasningstilstanden til **afbrudt**, og RC forsøges ikke, og det skyldes, at DHCP leverer de nødvendige oplysninger om klargøringsserveren.

Når en telefon opretter forbindelse til et netværk for første gang eller efter en fabriksnulstilling, og hvis der er ingen konfiguration af DHCP-indstillinger, kontakter den en enhedsaktiveringsserver for klargøring uden berøring. Nye telefoner bruger “activate.cisco.com” i stedet for “webapps.cisco.com” til klargøring. Telefoner med firmwareversion 11.2 (1) bruger fortsat webapps.cisco.com. Cisco anbefaler, at begge domænenavne får adgang via din firewall.

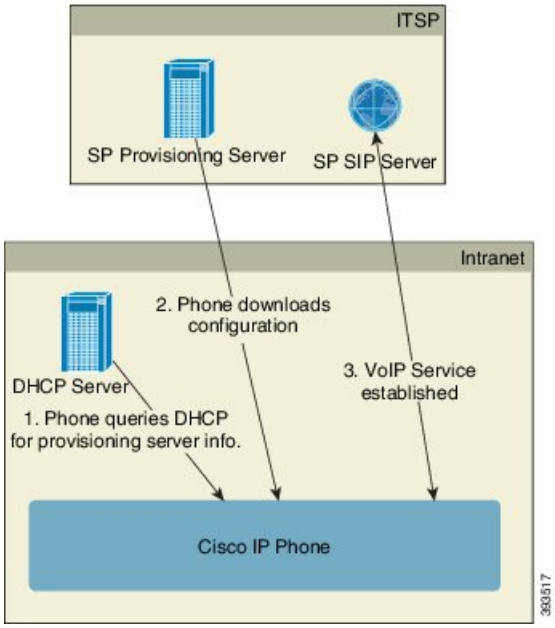
Hvis DHCP-serveren ikke giver oplysninger om klargøringsserveren, sender telefonen en forespørgsel til Cisco EDOS RC og giver dens MAC-adresse og model, og tilpasningstilstand indstilles til **ventende**. Cisco EDOS-serveren svarer med den tilknyttede tjenesteudbyders klargøringsserveroplysninger, herunder URL-adresse til klargøringsserver, og telefonens tilpasningstilstand indstilles **brugerdefineret ventende**. Telefonen udfører derefter en kommando med gensynkroniserings-URL-adresse til tjenesteudbyderens konfiguration og, hvis den lykkes, indstilles tilpasningstilstanden til **erhvervet**.

Hvis Cisco EDOS RC-serveren ikke har en tjenestebyder tilknyttet telefonen, indstilles telefonens tilpasningstilstand til **ikke tilgængelig**. Telefonen kan konfigureres manuelt, eller der føjes en tilknytning for telefonens tjenesteudbyder til Cisco EDOS-serveren.

Hvis en telefon klargøres enten via LCD-skærm eller webkonfigurationsværktøjet, før tilpasningstilstanden bliver **erhvervet**, indstilles tilpasningstilstanden til **afbrudt**, og der sendes ikke en forespørgsel til Cisco EDOS-serveren, medmindre telefonen er blevet nulstillet til fabriksindstillingerne.

Når telefonen er blevet klargjort, benyttes Cisco EDOS RC-serveren ikke, medmindre telefonen nulstilles til fabriksindstillingerne.

Klargøring af enheder internt



Med Ciscos standardfabriksnulstillingkonfiguration forsøger telefonen automatisk at gensynkronisere til en profil på en TFTP-server. En administreret DHCP-server på et LAN leverer oplysninger om den profil og TFTP-server, der er konfigureret til forhåndsklargøring til enheden. Tjenesteudbyderen forbinder hver ny telefon til LAN'et. Telefonen gensynkroniserer automatisk til den lokale TFTP-server og initialiserer dens interne tilstand med henblik på installation. Denne forhåndsklargøringsprofil indeholder typisk URL-adressen for en ekstern klargøringsserver. Klargøringsserveren holder enheden opdateret, når enheden er installeret og tilsluttet til kundenetværket.

Den forhåndsklargjorte enhedsstregkode kan scannes for at registrere dens MAC-adresse eller serienummer, før telefonen leveres til kunden. Disse oplysninger kan bruges til at oprette en profil, som telefonen gensynkroniserer med.

Ved modtagelse af telefonen forbinder kunden den til bredbåndsforbindelsen. Telefonen opretter forbindelse til klargøringsserveren ved start via den URL-adresse, der er konfigureret via forhåndsklargøringen. Telefonen kan derfor gensynkronisere og opdatere profilen og firmwaren efter behov.

Lignende emner

Detailhandeldistribution, på side 5
TFTP-klargøring, på side 40

Opsætning af klargøringsserver

Dette afsnit beskriver konfigurationskravene til klargøring af en telefon ved hjælp af forskellige servere og forskellige scenarier. For så vidt angår dette dokument og til testformål installeres og køres klargøringsservere på en lokal pc. Derudover er generelt tilgængelige softwareværktøjer nyttige til klargøring af telefonerne.

TFTP-klargøring

Telefonerne understøtter TFTP for både handlinger med klargøringsgensynkronisering og firmwareopgradering. Når enheder er installeret via fjernadgang, anbefales HTTPS, men HTTP og TFTP kan også bruges. Dette kræver derefter klargøring af filkryptering for at tilføje sikkerhed, fordi det giver større pålidelighed, under forudsætning af mekanismer til NAT- og routerbeskyttelse. TFTP er nyttig til intern klargøring af et stort antal enheder, der ikke er klargjorte.

Telefonen er i stand til at hente en IP-adresse til TFTP-server direkte fra DHCP-serveren via DHCP-indstilling 66. Hvis en Profile_Rule (Profilregel) er konfigureret med filstien for den pågældende TFTP-server, downloader enheden dens profil fra TFTP-serveren. Downloaden sker, når enheden er forbundet til et LAN og tændes.

Den Profile_Rule (Profilregel), der fulgte med standardfabrikskonfigurationen, er *&PN*.cfg, hvor *&PN* repræsenterer telefonens modelnavn.

For en CP-6841-3PCC er filnavnet f.eks. CP-6841-3PCC.cfg.

Når det gælder en enhed med fabriksindstillet standardprofil, gensynkroniserer enheden, når den tændes, til denne fil på den lokale TFTP-server, som DHCP-indstillingen 66 angiver. Filstien er i forhold til den virtuelle rodmappe på TFTP-serveren.

Lignende emner

Klargøring af enheder internt, på side 39

Styring af eksterne slutpunkter og NAT

Telefonen er kompatibel med NAT (network address translation) for at få adgang til internettet via en router. For at øge sikkerheden kan routeren forsøge at blokere uautoriserede indgående pakker ved at implementere symmetrisk NAT, en pakkefiltreringsstrategi, der kraftigt begrænser de pakker, der har tilladelse til at komme ind i det beskyttet netværk fra internettet. Af denne årsag anbefales ekstern klargøring ved hjælp af TFTP ikke.

VoIP kan fungere sammen med NAT, når en form for NAT-tværfunktion leveres. Konfigurer STUN (Simple Traversal of UDP through NAT). Denne indstilling kræver, at brugeren har:

- En dynamisk ekstern (offentlig) IP-adresse fra din tjeneste
- En computer, der kører STUN-serversoftware
- En edge-enhed med en asymmetrisk NAT-mekanisme

HTTP-klargøring

Telefonen fungerer som en browser, der anmoder om websider fra et eksternt internetsted. Dette giver en pålidelig måde at få forbindelse til klargøringsserveren på, selv når en kunderouter implementerer symmetrisk NAT eller andre beskyttelsesmekanismer. HTTP og HTTPS arbejder mere pålideligt end TFTP ved fjerninstallationer, især når de installerede enheder er tilsluttet bag lokale firewalls eller NAT-aktiverede routere. HTTP og HTTPs er indbyrdes udskiftelige i følgende beskrivelser af anmodningstyper.

Grundlæggende HTTP-baseret klargøring benytter HTTP GET-metoden til at hente konfigurationsprofiler. Der oprettes typisk en konfigurationsfil for hver installeret telefon, og disse filer gemmes i en mappe på HTTP-serveren. Når serveren modtager GET-forespørgslen, returnerer den blot den fil, der er angivet i GET-anmodningsheaderen.

I stedet for en statisk profil kan konfigurationsprofilen genereres dynamisk ved forespørgsler til en kundedatabase og producere profilen løbende.

Når telefonen anmoder om en gensynkronisering, kan den bruge HTTP POST-metoden til at anmode om konfigurationsdataene for gensynkroniseringen. Enheden kan konfigureres til at videregive bestemte status- og identifikationsoplysninger til serveren i brødteksten i HTTP POST-anmodningen. Serveren bruger disse oplysninger til at generere en ønsket svarkonfigurationsprofil eller lagre statusoplysningerne til senere analyse- og sporingsbrug.

Som en del af både GET- og POST-anmodninger medtager telefonen automatisk grundlæggende identifikationsoplysninger i feltet Brugeragent i anmodningsheaderen. Disse oplysninger angiver producenten, produktnavnet, den aktuelle firmwareversion og produktets serienummer for enheden.

I følgende eksempel er feltet for brugeragentanmodning fra en CP-6841-3PCC:

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

Når telefonen er konfigureret til at gensynkronisere til en konfigurationsprofil ved hjælp af HTTP, anbefales det, HTTPS bruges, eller at profilen krypteres, for at beskytte fortrolige oplysninger. Krypterede profiler, som telefonen downloader ved hjælp af HTTP, undgår risikoen for afsløre fortrolige oplysninger, der er indeholdt i konfigurationsprofilen. Denne gensynkronisering producerer en lavere computerberegningsmæssig belastning på klargøringsserveren sammenlignet med brugen af HTTPS.

Telefonen kan dekryptere de profiler, der er krypteret med en af disse krypteringsmetoder:

- AES-256-CBC-kryptering
- RFC-8188-baseret kryptering med AES-128-GCM-beregning

Bemærk Telefonerne understøtter HTTP-Version 1.0-, HTTP-Version 1.1 og Chunk-kodning, når HTTP-Version 1.1 er den forhandlede transportprotokol.

Håndtering af HTTP-statuskoder ved gensynkronisering og opgradering

Telefonen understøtter HTTP-svar for fjernklargøring (gensynkronisering). Den aktuelle funktionsmåde af telefonen kan kategoriseres på tre måder:

- A – gennemført, hvor værdierne "gensynkroniser periodisk" og "gensynkronisering med vilkårlig forsinkelse" efterfølgende anmodninger.

- B – mislykket, når fil ikke blev fundet eller en beskadiget profil. Værdien "Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl" bestemmer efterfølgende anmodninger.
- C – andre fejl, når en ugyldig URL-adresse eller IP-adresse medfører en forbindelsesfejl. Værdien "Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl" bestemmer efterfølgende anmodninger.

Tabel 2: Telefonens funktionsmåde ved HTTP-svar

HTTP-statuskode	Beskrivelse	Telefonens funktionsmåde
301 Flyttet permanent	Denne og fremtidige forespørgsler skal sendes til en ny placering.	Prøv øjeblikkeligt anmodning igen med den nye placering.
302 Fundet	Kendt som Midlertidigt flyttet.	Prøv øjeblikkeligt anmodning igen med den nye placering.
3xx	Andre 3xx-svar ikke behandlet.	C
400 Ugyldig anmodning	Anmodningen kan ikke udføres på ugyldig syntaks.	C
401 Uautoriseret	Grundlæggende eller digest-godkendelsesudfordring.	Forsøg straks anmodning igen med godkendelsesoplysninger. Maksimalt 2 forsøg. Ved fejl er telefonens funktionsmåde C.
403 Forbudt	Serveren afviser at svare.	C
404 Ikke fundet	Anmodet ressource blev ikke fundet. Efterfølgende anmodninger fra klient tillades.	B
407 Proxygodkendelse kræves	Grundlæggende eller digest-godkendelsesudfordring.	Forsøg straks anmodning igen med godkendelsesoplysninger. Maksimalt to nye forsøg. Ved fejl er telefonens funktionsmåde C.
4xx	Andre klientefejlstatuskoder behandles ikke.	C
500 Fejl ved intern server	Generisk fejlmeddelelse.	Telefonens funktionsmåde er C.
501 Ikke implementeret	Serveren genkender ikke anmodningsmetoden eller kan ikke udføre anmodningen.	Telefonens funktionsmåde er C.
502 Ugyldig gateway	Serveren fungerer som en gateway eller proxy og modtager et ugyldigt svar fra den tidligere server.	Telefonens funktionsmåde er C.
503 Tjenesten ikke tilgængelig	Serveren er ikke tilgængelig i øjeblikket (overbelastet eller nede pga. vedligeholdelse). Dette er en midlertidig tilstand.	Telefonens funktionsmåde er C.

HTTP-statuskode	Beskrivelse	Telefonens funktionsmåde
504 Gatewaytimeout	Serveren fungerer som en gateway eller proxy og modtager et rettidigt svar fra den tidligere server.	C
5xx	Andre serverfejl	C

HTTPS-klargøring

Telefonen understøtter HTTPS til klargøring for at få øget sikkerhed ved administration af fjerninstallerede enheder. Hver enkelt telefon har et entydigt SLL-klientcertifikat (og tilknyttet privat nøgle) ud over CA Sipura-serverrodcertifikat. Sidstnævnte giver telefonen mulighed for at registrere godkendte klargøringsservere og afvise servere, der ikke er godkendt. På den anden side giver klientcertifikatet klargøringsserveren mulighed for at identificere den enkelte enhed, der sender anmodningen.

Hvis en tjenesteudbyder skal kunne administrere installationen ved hjælp af HTTPS, skal der for hver klargøringsserver genereres et servercertifikat, som en telefon gensynkroniserer med ved hjælp af HTTPS. Servercertifikatet skal være signeret af Cisco Server CA Root Key, hvis certifikat er placeret på alle installerede enheder. For at få et signeret servercertifikat skal tjenesteudbyderen videresende en anmodning om certifikatsignering til Cisco, der signerer og returnerer servercertifikatet til installation på klargøringsserveren.

Klargøringservercertifikatet skal indeholde feltet CN (Common Name) og FQDN for den vært, der kører på den relevante server. Det kan eventuelt indeholde oplysninger om følgende værts FQDN adskilt med en skråstreg (/). Følgende eksempler er CN-poster, som telefonen accepterer som gyldige:

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

Ud over at kontrollere servercertifikatet tester telefonen serverens IP-adresse mod et DNS-opslag af det servernavn, der er angivet i servercertifikatet.

Få et signeret servercertifikat

Værktøjet OpenSSL kan generere en anmodning om signering af certifikat. Følgende eksempel viser kommandoen **openssl**, der producerer et 1024-bit RSA offentligt/privat nøglepar og en anmodning om signering af certifikat:

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

Denne kommando genererer serverens private nøgle i **privkey.pem** og en tilhørende anmodning og signering af certifikat i **provserver.csr**. Serviceudbyderen holder **privkey.pem** hemmelig og sender **provserver.csr** til Cisco til signering. Ved modtagelse af filen **provserver.csr** genererer Cisco**provserver.crt**, der er det signerede servercertifikat.

Fremgangsmåde

Trin 1 Gå til https://software.cisco.com/software/edos/home, og log på med dine CCO-legitimationsoplysninger.

Bemærk Når en telefon opretter forbindelse til et netværk for første gang eller efter en fabriksnulstilling, og der ikke er nogen konfiguration af DHCP-indstillinger, kontakter den en enhedsaktiveringsserver for klargøring uden berøring. Nye telefoner bruger "activate.cisco.com" i stedet for "webapps.cisco.com" til klargøring. Telefoner med firmwareversion før 11.2(1) bruger fortsat "webapps.cisco.com". Vi anbefaler, at begge domænenavne får adgang via din firewall.

Trin 2 Vælg **Certifikatstyring**.

Under fanen **Signer CSR** overføres CSR'en fra det tidligere trin til signering.

Trin 3 På rullelisten **Vælg produkt** skal du vælge **SPA1xx firmware 1.3.3 og nyere/SPA232D firmware 1.3.3 og nyere/SPA5xx firmware 7.5.6 og nyere/CP-78xx-3PCC/CP-88xx-3PCC**.

Bemærk Dette produkt indeholder Cisco IP Phone-serien af multiplatformstelefoner.

Trin 4 Gå til feltet **CSR-fil**, klik på **Gennemse**, og vælg den CSR, der skal signeres.

Trin 5 Vælg krypteringsmetoden:

- MD5
- SHA1
- SHA256

Cisco anbefaler, at du vælger SHA256-kryptering.

Trin 6 Vælg den gældende varighed (f.eks. 1 år) på rullelisten **Varighed af signering**.

Trin 7 Klik på **Signer certifikatanmodning**.

Trin 8 Vælg en af følgende muligheder for at modtage det signerede certifikat:

- **Angiv modtagerens e-mailadresse** – Hvis du ønsker at modtage certifikatet på e-mail, skal du indtaste din e-mailadresse i dette felt.
- **Download** – Vælg denne indstilling, hvis du vil downloade det signerede certifikat.

Trin 9 Klik på **Send**.

Det signerede servercertifikat bliver enten sendt på e-mail til den e-mailadresse, der tidligere er angivet, eller downloadet.

Nøglecenterrodscertifikat for multiplatformstelefoner

Cisco leverer også et klientrodscertifikat til multiplatformstelefoner til tjenesteudbyderen. Dette rodcertifikat certificerer ægtheden af det klientcertifikat, der er på hver telefon. Multiplatformstelefoner understøtter også fra tredjeparts signerede certifikater som f.eks. dem, der leveres af Verisign, Cybertrust osv.

Det entydige klientcertifikat, som hver enkelt enhed har under en HTTPS-session, indeholder identificerede oplysninger, der er indlejret i dets emnefelt. Disse oplysninger kan gøres tilgængelige af HTTPS-serveren til et CGI-script, der kaldes for at håndtere sikre anmodninger. Certifikatemnet angiver især enhedens produktnavn (OU-element), MAC-adresse (S-element) og serienummer (L-element).

I følgende eksempel fra klientcertifikatets emnefelt til Cisco IP Phone 6841-multiplatformstelefoner vises disse elementer:

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

For at fastlægge om en telefon har et individualiseret certifikat skal du bruge klargøringsmakrovariablen $CCERT. Variablens værdi udvides til enten installeret eller ikke installeret, alt efter om der findes eller ikke findes et entydigt klientcertifikat. Er der tale om et generisk certifikat, er det muligt at få enhedens serienummer via HTTP-anmodningsheaderen i feltet Brugeragent.

HTTPS-servere kan konfigureres til at anmode om SSL-certifikater fra tilsluttede klienter. Hvis indstillingen er aktiveret, kan serveren bruge det klientrodscertifikat til multiplatformstelefoner, som Cisco leverer, for at bekræfte klientcertifikatet. Serveren kan derefter give oplysningerne om certifikatet til et CGI til viderebehandling.

Placeringen af certifikatstorage kan variere. På en Apache-installation er filstierne til lagring af det klargøringsserversignerede certifikat, dens tilknyttede private nøgle og nøglecenterklientrodscertifikatet til multiplatformstelefoner følgende:

```
# 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
```

Få mere specifikke oplysninger i dokumentationen til en HTTPS-server.

Cisco Client Certificate Root Authority signerer hver entydigt certifikat. Det tilhørende rodcertifikat er gjort tilgængeligt for tjenesteudbydere, som bruger den til klientgodkendelse.

Redundante klargøringsservere

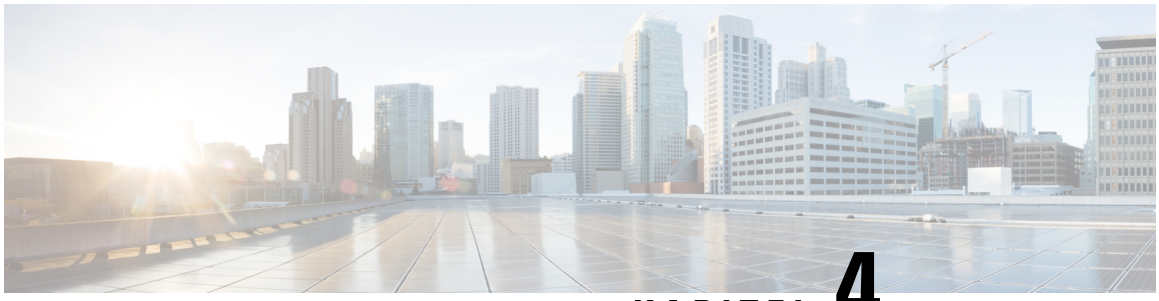
Klargøringsserveren kan angives som en IP-adresse eller som et fuldt kvalificeret domænenavn (FQDN). Brug af et FQDN muliggør implementering af redundante klargøringsservere. Når klargøringsserveren er identificeret gennem en FQDN, forsøger telefonen at oversætte FQDN til en IP-adresse via DNS. Det er kun DNS-poster, der understøttes til klargøring; DNS SRV-adresser er ikke tilgængelige til klargøring. Telefonen fortsætter med at behandle A-poster, indtil en server svarer. Hvis ingen server, der er knyttet til A-poster, svarer, logger telefonen en fejl på syslog-serveren.

Syslog-server

Hvis en syslog-server er konfigureret på telefonen ved hjælp af <Syslog-Server>-parametrene, sender gensynkroniserings- og opgraderingshandlingerne meddelelser til syslog-serveren. En meddelelse kan oprettes ved starten af en ekstern filanmodning (konfigurationsprofil eller firmware) og ved afslutningen af handlingen (hvor den enten angiver gennemført eller mislykket).

De loggede meddelelser konfigureres i følgende parametre og makroudvides i de faktiske syslog-meddelelser:

- Log Request Msg (Meddelelse om logføringsanmodning)
- Log Success Msg (Meddelelse om logføring gennemført)
- Log Failure Msg (Meddelelse om logføring mislykket)



KAPITEL 4

Klargøringseksempler

Oversigt over klargøringseksempler

Dette kapitel indeholder eksempler på procedurer til overførelse af konfigurationsprofiler mellem telefonen og klargøringsserveren.

Få oplysninger om oprettelse af konfigurationsprofiler ved at se under Klargøringsscripts, på side 13.

Grundlæggende gensynkronisering

Denne sektion viser telefonernes grundlæggende gensynkroniseringsfunktion.

TFTP-gensynkronisering

Telefonen understøtter flere netværksprotokoller til at hente konfigurationsprofiler. Den mest grundlæggende profiloverførselsprotokol er TFTP (RFC1350). TFTP bruges i stor udstrækning til klargøring af netværksenheder inden for private LAN-netværk. Selvom det ikke anbefales for installation af eksterne slutpunkter på tværs af internettet, kan TFTP være praktisk til installation inden for små virksomheder, forhåndsklargøring internt og udvikling og test. Se Klargøring af enheder internt, på side 39for flere oplysninger om intern forhåndsklargøring. I følgende procedure ændres en profil, efter at der er downloadet en fil fra en TFTP-server.

Fremgangsmåde

Trin 1 I et LAN-miljø skal du tilslutte en pc og en telefon til en hub, switch eller lille router.

Trin 2 På pc'en skal du installere og aktivere en TFTP-server.

Trin 3 Brug en teksteditor til at oprette en konfigurationsprofil, der indstiller værdien for GPP_A til 12345678 som vist i eksemplet.

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

Trin 4 Gem profilen med navnet `basic.txt` i rodmappen på TFTP-serveren.

Du kan kontrollere, at TFTP-serveren er konfigureret korrekt: anmod om filen `basic.txt` ved hjælp af en anden TFTP-klient end telefonen. Brug helst en TFTP-klient, der kører på en separat vært, fra klargøringsserveren.

Trin 5 Åbn webbrowseren på pc'en, og gå til konfigurationssiden administrator/avanceret. Hvis IP-adressen til telefonen f.eks. er 192.168.1.100:

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

Trin 6 Vælg fanen **Tale** > **Klargøring**, og kontrollér værdierne af parametrene for generelle formål GPP_A til og med GPP_P. De burde være tomme.

Trin 7 Gensynkroniser testtelefonen til konfigurationsfilen `basic.txt` ved at åbne gensynkroniserings-ULR-adressen i et webbrowservindue.

Hvis IP-adressen på TFTP-serveren er 192.168.1.200, skal kommandoen svarer til følgende eksempel:

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

Når telefonen modtager denne kommando, anmoder enheden på adressen 192.168.1.100 om filen `basic.txt` fra TFTP-serveren på IP-adresse 192.168.1.200. Telefonen parser derefter den downloadede fil og opdaterer parameteren GPP_A med værdien 12345678.

Trin 8 Kontrollér, at parameteren blev opdateret korrekt: opdater konfigurationssiden i pc'ens webbrowser, og vælg den fanen **Tale** > **Klargøring**.

Parameteren GPP_A burde nu indeholde værdien 12345678.

Brug Syslog til logmeddelelser

Telefonen sender en syslog-meddelelse til den angivne syslog-server, når enheden er ved at gensynkronisere til en klargøringsserver, og når gensynkronisering er enten fuldført eller mislykket. For at identificere denne server har du gå til telefonens administrationswebside (se Gå til telefonens webside, på side 7), vælge **Tale** > **systemet** og identificere serveren i parameteren **Syslog-serveren** for sektion **Valgfri netværkskonfiguration**. Konfigurer syslog-serverens IP-adressen på enheden, og hold øje med de meddelelser, der oprettes under de resterende procedurer.

Fremgangsmåde

Trin 1 Installér og aktivér en syslog-server på den lokale pc.

Trin 2 Programmér pc'ens IP-adresse i parameteren Syslog_Server i profilen, og send ændringen:

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

Trin 3 Klik fanen **System**, og angiv værdien af din lokale syslog-server i parameteren Syslog_Server.

Trin 4 Gentag gensynkroniseringshandlingen, som beskrevet i TFTP-gensynkronisering, på side 47.

Enheden genererer to syslog-meddelelser i løbet af gensynkroniseringen. Den første meddelelse angiver, at en anmodning er i gang. Den anden meddelelse angiver, om gensynkroniseringen er gennemført eller mislykket.

Trin 5 Kontrollér, at din syslog-server har modtaget meddelelser svarer til følgende:

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

Detaljerede meddelelser er tilgængelige ved programmering af parameteren Debug_Server (Fejlfind server) (i stedet for parameteren Syslog_Server) med syslog-serverens IP-adresse og ved at angive fejlfindingsniveauet til en værdi mellem 0 og 3 (hvor 3 er den mest detaljerede):

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

Indholdet af disse meddelelser kan konfigureres ved hjælp af følgende parametre:

- Log Request Msg (Meddelelse om logføringsanmodning)
- Log Success Msg (Meddelelse om logføring gennemført)
- Log Failure Msg (Meddelelse om logføring mislykket)

Hvis nogen af disse parametre er ryddet, genereres den tilsvarende syslog-meddelelse ikke.

Gensynkroniser en enhed automatisk

En enhed kan periodisk gensynkronisere med klargøringsserveren for at sikre, at eventuelle profilændringer, der er foretaget på serveren, overføres til slutpunktsenheden (i modsætning til afsendelse af en eksplicit anmodning om gensynkronisering til slutpunktet).

For at få telefonen til periodisk at gensynkronisere med en server defineres der en URL-adresse til en konfigurationsprofil ved hjælp af profilregelparameteren, og der defineres en gensynkroniseringsperiode ved hjælp af parameteren Resync_Periodic (Gensynkroniser periodisk).

Inden du begynder

Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Fremgangsmåde

Trin 1 Vælg **Tale** > **Klargøring**.

Trin 2 Angiv profilregelparameteren. I dette eksempel antages IP-adressen 192.168.1.200 til TFTP-serveren.

Trin 3 I feltet **Gensynkroniser periodisk** skal du angive en lille værdi som test, f.eks. **30** sekunder.

Trin 4 Klik på **Send alle ændringer**.

Med de nye parameterindstillinger gensynkroniserer telefonen to gange i minuttet til den konfigurationsfil, som URL-adressen angiver.

Trin 5 Se de resulterende meddelelser i syslog-sporet (som beskrevet i afsnittet Brug Syslog til logmeddelelser, på side 48).

Trin 6 Sørg for, at feltet **Gensynkronisering ved nulstilling** er indstillet til **Ja**.

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

Trin 7 Genstart telefonen for at tvinge den til at gensynkronisere med klargøringsserveren.

Hvis gensynkroniseringshandlingen af en eller anden grund mislykkes, f.eks. hvis serveren ikke reagerer, venter enheden (i det antal sekunder, der er konfigureret i **Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl**), før den forsøger at synkronisere igen. Hvis **Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl** er nul, forsøger telefonen ikke at synkronisere efter et mislykket forsøg på gensynkronisering.

Trin 8 (Valgfri) Angiv værdien i feltet **Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl** til et lille tal, f.eks. **30**.

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

Trin 9 Deaktiver TFTP-serveren, og se resultaterne i telefonens syslog-output.

Entydige profiler, makroudvidelse og HTTP

I en installation, hvor hver enkelt telefon skal være konfigureret med særskilte værdier for visse parametre, f.eks. bruger-id eller visningsnavn, kan tjenesteudbyderen oprette en entydig profil for hver installeret enhed og hoste disse profiler på en klargøringsserver. Hver enkelt telefon igen skal til gengæld konfigureres til at gensynkronisere dens egen profil ifølge en forudbestemt konvention for navngivning af profiler.

Profilens URL-syntaks kan omfatte id-oplysninger, der er specifikke for hver telefon, f.eks. MAC-adresse eller serienummer, ved hjælp af makroudvidelsen i indbyggede variabler. Makroudvidelse fjerner behovet for at angive disse værdier flere steder i hver profil.

En profilregel udsættes for en makroudvidelse, før reglen anvendes på telefonen. Makroudvidelse styrer et antal værdier, f.eks.:

- $MA udvides til enhedens 12-cifrede MAC-adresse (ved hjælp af hexadecimale cifre med små bogstaver). For eksempel: 000e08abcdef.
- $SN udvides til enhedens serienummer. For eksempel: 88012BA01234.

Andre værdier kan være blive makroudvidet på denne måde, herunder alle parametre for generelle formål, GPP_A til og med GPP_P. Et eksempel på denne proces kan ses i TFTP-gensynkronisering, på side 47. Makroudvidelse er ikke begrænset til URL-filnavnet, men kan også anvendes på enhver del af profilregelparameteren. Disse parametre kaldes $A til og med $P. Få en fuldstændig liste over variabler, der er tilgængelige for makroudvidelse, under Makroudvidelsesvariabler, på side 72.

I denne øvelse klargøres en profil, der er specifik for en telefon, på en TFTP-server.

Øvelse: Klargør en bestemt IP-telefonprofil på en TFTP-Server

Fremgangsmåde

Trin 1 Få telefonens MAC-adresse fra produktmærkatet. (MAC-adressen er nummeret med tal og hexadecimale cifre med små bogstaver, f.eks. 000e08aabbcc.

Trin 2 Kopiér konfigurationsfilen `basic.txt` (beskrevet i TFTP-gensynkronisering, på side 47) til en ny fil med navnet `CP-xxxx-3PCC macaddress.cfg` (erstatter `xxxx` med modelnummer og `MAC-adresse` med telefonens MAC-adresse).

Trin 3 Flyt den nye fil til den virtuelle rodmappe på TFTP-serveren.

Trin 4 Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Trin 5 Vælg **Tale** > **Klargøring**.

Trin 6 Angiv `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` i feltet **Profilregel**.

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

Trin 7 Klik på **Send alle ændringer**. Dette medfører en øjeblikkelig genstart og gensynkronisering.

Når den næste gensynkronisering forekommer, henter telefonen den nye fil ved at udvide $MA makroudtrykket i dens MAC-adresse.

HTTP GET-gensynkronisering

HTTP giver en mere pålidelig gensynkroniseringsmekanisme end TFTP, fordi HTTP opretter en TCP-forbindelse, og TFTP bruger den mindre pålidelige UDP. Derudover har HTTP-servere bedre filtrerings- og logføringsfunktioner end TFTP-servere.

På klientsiden kræver telefonen ikke en speciel konfigurationsindstilling på serveren for at kunne gensynkronisere ved hjælp af HTTP. Syntaksen for profilregelparameteren til brug med HTTP GET-metoden svarer til den syntaks, der bruges til TFTP. Hvis en almindelig webbrowser kan hente en profil fra din HTTP-server, burde telefonen også kunne gøre det.

Øvelse: HTTP GET-gensynkronisering

Fremgangsmåde

Trin 1 Installér en HTTP-server på den lokale pc eller en anden tilgængelig vært.

Apache-serveren, der er open source, kan hentes på internettet.

Trin 2 Kopiér konfigurationsprofilen `basic.txt` (beskrevet i TFTP-gensynkronisering, på side 47) over i den virtuelle rodmappe på den installerede server.

Trin 3 For at kontrollere serverinstallationen og filadgangen til `basic.txt` ordentligt skal du have adgang til profilen via en webbrowser.

Trin 4 Rediger testtelefonens Profile_Rule (Profilregel), så den peger på HTTP-serveren i stedet for TFTP-serveren, for at hente dens profil med jævne mellemrum.

Hvis det f.eks. antages, at HTTP-serveren er 192.168.1.300, skal du indtaste følgende værdi:

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

Trin 5 Klik på **Send alle ændringer**. Dette medfører en øjeblikkelig genstart og gensynkronisering.

Trin 6 Se de syslog-meddelelser, som telefonen sender. De periodiske gensynkroniseringer skulle nu hente profilen fra HTTP-serveren.

Trin 7 I HTTP-serverens logfiler kan du se, hvordan oplysninger, der identificerer testtelefonen, vises i loggen for brugeragenter.

Disse oplysninger skal omfatte producenten, produktnavnet, den aktuelle firmwareversion og serienummeret.

Klargøring via Cisco XML

For hver enkelt telefon, der er angivet som xxxx her, kan du foretage en klargøring via Cisco XML-funktioner.

Du kan sende et XML-objekt til telefonen med en SIP-beskedpakke eller en HTTP-post til telefonens CGI-grænseflade: `http://IP-adressetelefon/CGI/Execute`.

CP-xxxx-3PCC udvider Cisco XML-funktionen for at understøtte klargøring via et XML-objekt:

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

Når telefonen har modtaget XML-objektet, hentes klargøringsfilen fra [profile-rule]. Denne regel bruger makroer til at forenkle installationen af programmet til XML-tjenester.

URL-fortolkning med makroudvidelse

Undermapper med flere profiler på serveren giver en praktisk metode til håndtering af et stort antal installerede enheder. Profilens URL-adresse kan indeholde:

- Navnet på en klargøringsserver eller en eksplicit IP-adresse. Hvis profilen identificerer klargøringsserveren efter navn, udfører telefonen et DNS-opslag for at fortolke navnet.
- En serverport, der ikke er standard, og som er angivet i URL-adressen ved hjælp af standardsyntaksen `:port` efter navnet på serveren.
- Undermappen til serverens virtuelle rodmappe, hvor profilen er gemt, er angivet ved hjælp af standard-URL-notation og administreres med makroudvidelse.

F.eks. anmoder følgende Profile_Rule (Profilregel) om profilfilen ($PN.cfg) i serverundermappen `/cisco/config` fra den TFTP-server, der kører på værten prov.telco.com, hvor der lyttes efter en forbindelse på port 6900:

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

En profil for hver telefon kan identificeres i en parameter for generelle formål, hvor der henvises til dens værdi i en almindelig profilregel ved hjælp af makroudvidelse.

Antag f.eks., at GPP_B er defineret som `Dj6Lmp23Q`.

Profile_Rule (Profilregel) har værdien:

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

Når enheden gensynkroniserer, og makroerne udvides, beder telefonen med MAC-adressen 000e08012345 om profilen med det navn, der indeholder enhedens MAC-adresse, på følgende webadresse:

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

Sikker HTTPS-gensynkronisering

Disse mekanismer er tilgængelige på telefonen til gensynkronisering ved hjælp af en sikker kommunikationsproces:

- Grundlæggende HTTPS-gensynkronisering
- HTTPS med klientcertifikatgodkendelse
- HTTPS-klientfiltrering og dynamisk indhold

Grundlæggende HTTPS-gensynkronisering

HTTPS tilføjer SSL til HTTP til ekstern klargøring, så:

- Telefonen kan godkende klargøringsserveren.
- Klargøringsserveren kan godkende telefonen.
- Fortroligheden af oplysninger, der udveksles mellem telefonen og klargøringsserveren, er sikret.

SSL genererer og udveksler hemmelige (symmetriske) nøgler for hver forbindelse mellem telefonen og serveren ved hjælp af sæt af offentlige/private nøglepar, der er forudinstalleret på telefonen og klargøringsserveren.

På klientsiden kræver telefonen ikke en speciel konfigurationsindstilling på serveren for at kunne gensynkronisere ved hjælp af HTTPS. Syntaksen for profilregelparameteren til brug af HTTPS med GET-metoden svarer til den syntaks, der bruges til HTTP eller TFTP. Hvis en almindelig webbrowser kan hente en profil fra en HTTPS-server, burde telefonen også kunne gøre det.

Ud over at installere en HTTPS-server skal der være installeret et SSL-servercertifikat, som Cisco signerer, på klargøringsserveren. Enhederne kan ikke gensynkronisere til en server, der bruger HTTPS, medmindre serveren leverer et Cisco-signeret servercertifikat. Se instruktioner til oprettelse af signerede SSL-certifikater for taleprodukter på https://supportforums.cisco.com/docs/DOC-9852.

Øvelse: Grundlæggende HTTPS-gensynkronisering

Fremgangsmåde

Trin 1 Installér en HTTPS-server på en vært, hvis IP-adresse er kendt for netværkets DNS-server via normal værtsnavnoversættelse.

Apache-serveren, der er open source, kan konfigureres til at fungere som en HTTPS-server, når den installeres med open source-pakken mod_ssl.

Trin 2 Generer en servercertifikatsignering for serveren. I dette trin kan du få brug for at installere open source-pakken OpenSSL eller tilsvarende software. Hvis du bruger OpenSSL, er den kommando, der bruges til at generere den grundlæggende CSR-fil, som følger:

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

Denne kommando genererer et offentlig/privat nøglepar, som er gemt i filen `privkey.pem`.

Trin 3 Send CSR-filen (provserver.csr) til Cisco til med henblik på signering.

Et signeret servercertifikat returneres (provserver.cert) sammen med en Sipura CA-klientrodscertifikat, spacroot.cert.

Se https://supportforums.cisco.com/docs/DOC-9852 for at få flere oplysninger

Trin 4 Gem det signerede servercertifikat, filen med de private nøglepar og klientrodscertifikatet på de relevante placeringer på serveren.

I tilfælde af en Apache-installation på Linux vil disse placeringer typisk være følgende:

```
# 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
```

Trin 5 Genstart serveren.

Trin 6 Kopiér konfigurationsfilen `basic.txt` (beskrevet i TFTP-gensynkronisering, på side 47) over i den virtuelle rodmappe på HTTPS-serveren.

Trin 7 Kontrollér, at serverhandlingen sker korrekt, ved at downloade `basic.txt` fra HTTPS-serveren via en standardbrowser på den lokale pc.

Trin 8 Undersøg det servercertifikat, serveren leverer.

Browseren genkender sandsynligvis ikke certifikatet som gyldigt, medmindre browseren er blevet konfigureret til at acceptere Cisco som et rodnøglecenter. Telefonerne forventer imidlertid, at certifikatet er signeret på denne måde.

Rediger Profile_Rule (Profilregel) for testenheden, så den indeholder en reference til HTTPS-serveren, f.eks.:

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

```
</Profile_Rule>
```

I dette eksemplet antages det, at navnet på HTTPS-serveren er **my.server.com**.

Trin 9 Klik på **Send alle ændringer**.

Trin 10 Se syslog-sporet, som telefonen sender.

Syslog-meddelelsen skulle gerne angive, at gensynkroniseringen hentede profilen fra HTTPS-serveren.

Trin 11 (Valgfri) Brug en funktion til analyse af Ethernet-protokoller på telefonens undernet til at kontrollere, at pakkerne er krypteret.

I denne øvelse blev verificering af klientcertifikat ikke aktiveret. Forbindelsen mellem telefonen og serveren er krypteret. Overførslen er dog ikke sikker, fordi enhver klient kan oprette forbindelse til serveren og anmode om filen og på den måde få kendskab til filnavnet og mappeplaceringen. For at få en sikker gensynkronisering skal serveren også godkende klienten, som vist i den øvelse, der er beskrevet i HTTPS med klientcertifikatgodkendelse, på side 55.

HTTPS med klientcertifikatgodkendelse

I den fabriksindstillede standardkonfiguration anmoder serveren ikke om et SSL-klientcertifikat fra en klient. Overførsel af profilen er ikke sikker, fordi en klient kan oprette forbindelse til serveren og anmode om profilen. Du kan redigere konfigurationen for at aktivere klientgodkendelse. Serveren kræver et klientcertifikat for at godkende telefonen, før den accepterer en anmodning om forbindelse.

På grund af dette krav kan gensynkroniseringshandlingen ikke testes uafhængigt ved hjælp af en browser, der mangler de korrekte legitimationsoplysninger. Udvekslingen af SSL-nøglen inden for HTTPS-forbindelsen mellem testtelefonen og serveren kan være ses med hjælpeværktøjet ssldump. Hjælpeværktøjet til sporing viser interaktionen mellem klient og server.

Øvelse: HTTPS med klientcertifikatgodkendelse

Fremgangsmåde

Trin 1 Aktivér klientcertifikatgodkendelse på HTTPS-serveren.

Trin 2 På Apache (v.2) skal du indstille følgende i serverkonfigurationsfilen:

```
SSLVerifyClient  require
```

Sørg også for, at spacroot.cert har været lagret som vist i øvelsen Grundlæggende HTTPS-gensynkronisering, på side 53.

Trin 3 Genstart HTTPS-serveren, og se syslog-sporet fra telefonen.

Hver enkelt gensynkronisering til serveren foretager nu symmetrisk godkendelse, så både servercertifikatet og klientcertifikatet bekræftes, før profilen overføres.

Trin 4 Brug ssldump til at registrere en gensynkroniseringsforbindelse mellem telefonen og HTTPS-serveren.

Hvis verificeringen af klientcertifikat er aktiveret korrekt på serveren, viser ssldump-sporet den symmetriske udveksling af certifikater (først server-klient og derefter klient-server), før de krypterede pakker, der indeholder profilen.

Når klientgodkendelse er aktiveret, er det kun en telefon med en MAC-adresse, der svarer til et gyldigt klientcertifikat, der kan anmode om profil fra klargøringsserveren. Serveren afviser en anmodning fra en almindelig webbrowser eller anden uautoriseret enhed.

HTTPS-klientfiltrering og dynamisk indhold

Hvis HTTPS-serveren er konfigureret til at kræve et klientcertifikatet, identificerer oplysningerne i certifikatet gensynkroniseringstelefonen og giver den de korrekte konfigurationsoplysninger.

HTTPS-serveren gør certifikatoplysningerne tilgængelige for CGI-scripts (eller kompilerede CGI-programmer), der kaldes som en del af gensynkroniseringsanmodningen. Som eksempel bruger denne øvelse Perl-scriptsproget, der er open source, og det antages, at Apache (v.2) bruges som HTTPS-serveren.

Fremgangsmåde

Trin 1 Installér Perl på den vært, der kører på HTTPS-serveren.

Trin 2 Generer følgende Perl-reflectorscript:

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

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

Trin 3 Gem denne fil med filnavnet `reflect.pl`, med tilladelse til eksekvering (chmod 755 på Linux), i CGI-scriptmappen på HTTPS-serveren.

Trin 4 Kontrollér tilgængelighed af CGI-scripts på serveren (dvs. `/cgi bin /...`).

Trin 5 Rediger Profile_Rule (Profilregel) på testenheden for at gensynkronisere til reflectorscriptet, som i følgende eksempel:

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

Trin 6 Klik på **Send alle ændringer**.

Trin 7 Se syslog-sporet for at sikre, at gensynkronisering gennemføres.

Trin 8 Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Trin 9 Vælg **Tale** > **Klargøring**.

Trin 10 Kontrollér, at parameteren GPP_D indeholder de oplysninger, scriptet har registreret.

Disse oplysninger indeholder produktnavnet, MAC-adressen og serienummeret, hvis testenheden har et entydigt certifikat fra producenten. Oplysningerne indeholder generiske strenge, hvis enheden var produceret før firmwareversion 2.0.

Et lignende script kan bestemme oplysninger om gensynkroniseringsenheden og derefter forsyne enheden med relevante konfigurationsparameterværdier.

HTTPS-certifikater

Telefonen har en pålidelig og sikker klargøringsstrategi, der er baseret på HTTPS-anmodninger fra enheden til klargøringsserveren. Både et servercertifikat og et klientcertifikat bruges til at godkende telefonen til serveren og serveren til telefonen.

Hvis du vil bruge HTTPS med telefonen, skal du generere en CSR (Certificate Signing Request) og sende den til Cisco. Telefonen genererer et certifikat til installation på klargøringsserveren. Telefonen accepterer certifikatet, når den forsøger at oprette en HTTPS-forbindelse til klargøringsserveren.

HTTPS-metode

HTTPS krypterer kommunikationen mellem en klient og en server og beskytter derved meddelelsesindholdet fra andre netværksenheder. Krypteringsmetoden for kommunikationens brødtekst mellem en klient og en server er baseret på kryptografi med symmetrisk nøgle. Med kryptografi med symmetrisk nøgle deler en klient og en server en enkelt hemmelig nøgle via en sikker kanal, der beskyttes af kryptering med offentlig/privat nøgle.

Meddelelser, der er krypteret af den hemmelige nøgle, kan kun dekrypteres ved hjælp af den samme nøgle. HTTPS understøtter en bred vifte af algoritmer til symmetrisk kryptering. Telefonen implementerer op til 256-bit symmetrisk kryptering ved hjælp af EAS (American Encryption Standard) ud over 128-bit RC4.

HTTPS giver også mulighed for autentificering af en server og en klient, der indgår i en sikker transaktion. Denne funktion sikrer, at en klargøringsserver og en individuel klient ikke kan efterlignes af andre enheder på netværket. Denne funktion er vigtig i forbindelse med klargøring af eksterne slutpunkter.

Der udføres server- og klientautentificering ved hjælp af kryptering med offentlig/privat nøgle med et certifikat, der indeholder den offentlige nøgle. Tekst, der er krypteret med en offentlig nøgle, kan kun dekrypteres med dens tilsvarende private nøgle (og omvendt). Telefonen understøtter RSA-algoritmen (Rivest-Shamir-Adleman) til kryptering med offentlig/privat nøgle.

SSL-servercertifikat

Hver sikker klargøringsserveren er forsynet med et SSL-servercertifikat (secure sockets layer), som Cisco signerer direkte. Den firmware, der kører på telefonen, genkender kun et Cisco-certifikat som gyldigt. Når en klient opretter forbindelse til en server ved hjælp af HTTPS, afviser den ethvert servercertifikat, der ikke er signeret af Cisco.

Denne mekanisme beskytter tjenesteudbyderen mod uautoriseret adgang til telefonen eller ethvert forsøg på at efterligne klargøringsserveren. Uden denne beskyttelse kan en hacker muligvis klargøre telefonen igen for at få konfigurationsoplysninger eller for at bruge en anden VoIP-tjeneste. Uden den private nøgle, der svarer til et gyldigt servercertifikatet, kan hackeren ikke kommunikere med en telefon.

Få et servercertifikat

Fremgangsmåde

Trin 1 Kontakt en Cisco-supportperson, der vil arbejde sammen med dig om certifikatprocessen. Hvis du ikke arbejder sammen med en bestemt supportperson, kan du sende en anmodning på e-mail ciscosb-certadmin@cisco.com.

Trin 2 Opret en private nøgle, der skal bruges i en CSR (Certificate Signing Request). Denne nøgle er privat, og du behøver ikke at angive denne nøgle til Cisco-supporten. Brug open source "openssl" til at generere nøglen. For eksempel:

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

Trin 3 Generer en CSR, der indeholder felter, der identificerer din organisation og placering. For eksempel:

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

Du skal have følgende oplysninger:

- Emnefelt – Angiv CN (Common Name), der skal have en FQDN-syntaks (Fully Qualified Domain Name). Under SSL-godkendelseshandshaket kontrollerer telefonen, at det certifikat, den modtager, er fra den computer, der viste det.
- Serverværtsnavn – f.eks. provserv.domain.com.
- E-mailadresse – Indtast en e-mailadresse, så kundesupport kan kontakte dig, hvis det er nødvendigt. Denne e-mail-adresse er synlig i CSR.

Trin 4 Send en e-mail med CSR (i zip-filformat) til Cisco-supportmedarbejderen eller til ciscosb-certadmin@cisco.com. Certifikatet signeres af Cisco. Cisco sender certifikatet til dig, så du kan installere det på dit system.

Klientcertifikat

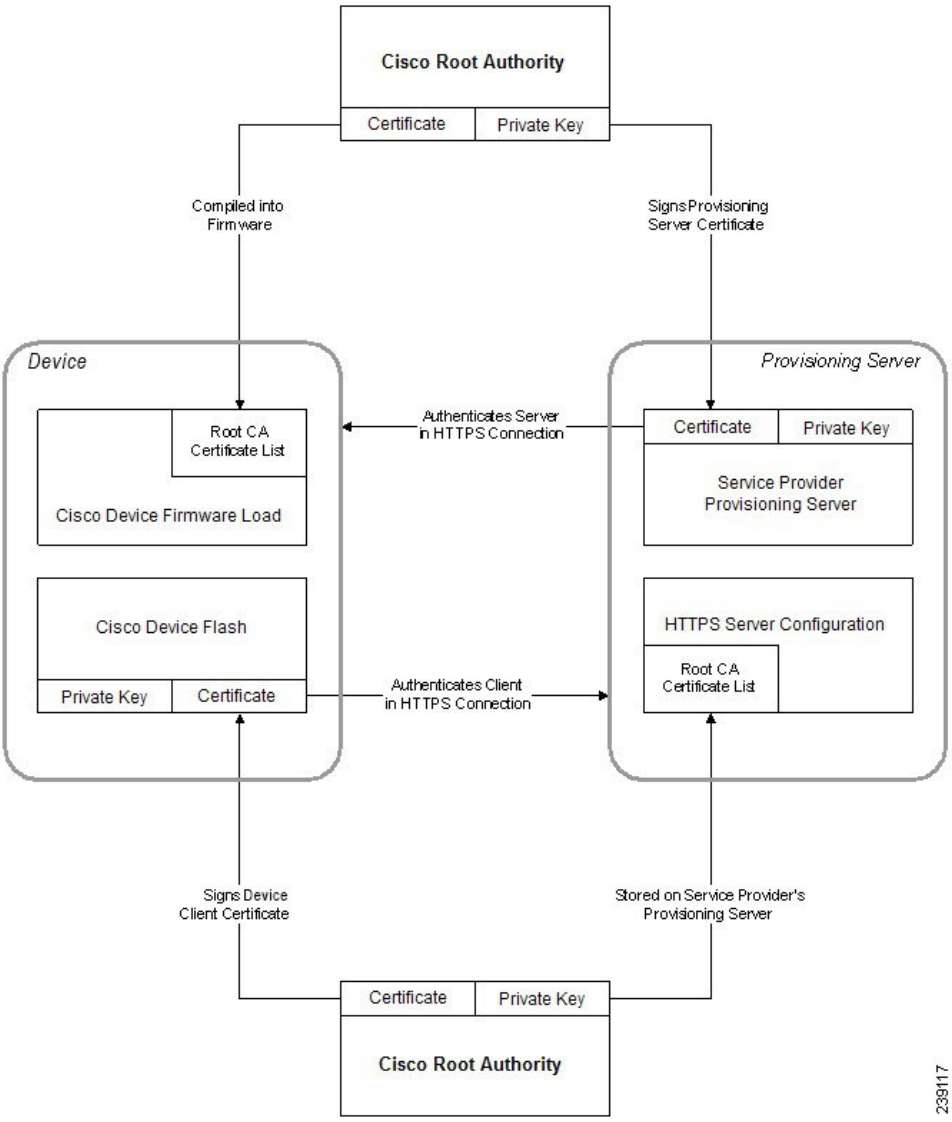
Ud over et direkte angreb på en telefon kan en hacker forsøge at kontakte en klargøringsserver via en almindelig webbrowser eller en anden HTTPS-klient for at hente konfigurationsprofilen fra klargøringsserveren. For at forhindre denne type angreb er der på hver enkelt telefon også et entydigt klientcertifikatet, der er signeret Cisco, og som indeholder oplysninger om hver enkelt slutpunkt. Et nøglecenterrodcertifikat, der kan godkende enhedens klientcertifikat, gives til hver tjenesteudbyder. Denne godkendelsessti tillader, at klargøringsserveren kan afvise uautoriserede anmodninger om konfigurationsprofiler.

Certifikatopbygning

Kombinationen af et servercertifikat og et klientcertifikat giver sikker kommunikationen mellem en ekstern telefon og dens klargøringsserver. Figuren herunder viser relationen og placeringen af certifikater, offentlige/private nøglepar og signeringsnøglecentre mellem Cisco-klienten, klargøringsserveren og nøglecentret.

Den øverste halvdel af diagrammet viser nøglecentret for klargøringsserveren, der bruges til at signere det individuelle klargøringsservercertifikat. Det tilhørende rodcertifikat er kompileret ind i firmwaren, hvilket giver telefonen mulighed for at godkende autoriserede klargøringsservere.

Figur 2: Flow af nøglecenter



Konfigurer et brugerdefineret nøglecenter

Digitale certifikater kan bruges til at godkende netværksenheder og brugere på netværket. De kan bruges til at forhandle IPSec-sessioner mellem netværksnoder.

En tredjepart bruger et nøglecentercertifikat til at validere og godkende to eller flere noder, der forsøger at kommunikere. Hver node har en offentlig og privat nøgle. Den offentlige nøgle krypterer data. Den private nøgle dekrypterer data. Da noderne har fået deres certifikater fra den samme kilde, er de sikre på deres respektive identitet.

Enheden kan bruge digitale certifikater, der er leveret af et tredjepartsnøglecenter, til at godkende IPSec-forbindelser.

Telefonerne understøtter en række forudinstallerede rodnøglecenter, der er integreret i firmwaren:

- Cisco Small Business-nøglecentercertifikat

- CyberTrust-nøglecentercertifikat
- VeriSign-nøglecentercertifikat
- Sipura Root-nøglecentercertifikat
- Linksys Root-nøglecentercertifikat

Inden du begynder

Gå til websiden til telefonadministration Se Gå til telefonens webside, på side 7.

Fremgangsmåde

Trin 1 Vælg **Info** > **Status**.

Trin 2 Rul til **Brugerdefineret nøglecenterstatus**, og se følgende felter:

- Status på klargøring af brugerdefineret nøglecenter – angiver klargøringsstatus.
  - Seneste klargøring gennemført den mm/dd/åååå TT:MM:SS eller
  - Seneste klargøring mislykket den mm/dd/åååå TT:MM:SS
- Oplysninger om brugerdefineret nøglecenter – viser oplysninger om det brugerdefinerede nøglecenter.
  - Installed (Installeret) – viser "CN-værdien", hvor "CN-værdien" er værdien for CN-parameteren i emnefeltet i det første certifikat.
  - Not Installed (Ikke installeret) – viser, hvis der ikke er installeret et brugerdefineret CA.

Profiladministration

Dette afsnit viser dannelsen af konfigurationsprofiler med henblik på download. Funktionaliteten kan forklares ved, at TFTP fra en lokal PC bruges som gensynkroniseringsmetoden, selvom HTTP eller HTTPS også kan bruges.

Komprimer en Open-profil med Gzip

En konfigurationsprofil i XML-format kan blive ret stor, hvis profilen angiver alle parametre individuelt. For at reducere belastningen på klargøringsserveren understøtter telefonen komprimering af XML-filen ved hjælp af deflate-komprimeringsformatet, som gzip-hjælpeprogrammet (RFC 1951) understøtter.

Bemærk Komprimering skal ske før kryptering, hvis telefonen skal kunne registrere en komprimeret og krypteret XML-profil.

Du kan sikre integration i tilpassede backend-klargøringsserverløsninger ved at bruge open source-zlib-komprimeringsbiblioteket i stedet for det separate gzip-hjælpeprogram til at udføre profilkomprimeringen. Telefonen forventer imidlertid den fil, der indeholder en gyldig gzip-header.

Fremgangsmåde

Trin 1 Installér gzip på den lokale pc.

Trin 2 Komprimer konfigurationsprofilen `basic.txt` (beskrevet i TFTP-gensynkronisering, på side 47) ved at kalde gzip på kommandolinjen:

```
gzip basic.txt
```

Dette genererer den deflatede fil `basic.txt.gz`.

Trin 3 Gem filen `basic.txt.gz` i den virtuelle rodmappe på TFTP-serveren.

Trin 4 Rediger Profile_Rule (Profilregel) på testenheden for at gensynkronisere til den deflatede fil i stedet for den oprindelige XML-fil, sådan som det er vist i følgende eksempel:

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

Trin 5 Klik på **Send alle ændringer**.

Trin 6 Se syslog-sporet fra telefonen.

Ved gensynkronisering downloader telefonen den nye fil og bruger den til at opdatere dens parametre.

Lignende emner

Komprimering af Open-profil, på side 18

Krypter en profil med OpenSSL

En komprimeret eller ikke-komprimeret profil kan krypteres (men en fil skal være komprimeret, før den krypteres). Kryptering er nyttig, når fortroligheden af profiloplysninger har stor betydning, f.eks. når en TFTP eller HTTP bruges til kommunikationen mellem telefonen og klargøringsserveren.

Telefonen understøtter symmetrisk nøglekryptering ved hjælp af 256-bit AES-algoritmen. Denne kryptering kan udføres ved hjælp af open source OpenSSL-pakken.

Fremgangsmåde

Trin 1 Installér OpenSSL på en lokal pc. Dette kan kræve, at OpenSSL-programmet kompileres igen for at aktivere AES.

Trin 2 Hvis konfigurationsfilen `basic.txt` (beskrevet i TFTP-gensynkronisering, på side 47) bruges, genereres der en krypteret fil med den følgende kommando:

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

Den komprimerede `basic.txt.gz`-fil, der er oprettet i Komprimer en Open-profil med Gzip, på side 60, kan også bruges, fordi XML-profilen både kan være komprimeret og krypteret.

Trin 3 Gem den krypterede `basic.cfg`-fil i den virtuelle rodmappe på TFTP-serveren.

Trin 4 Rediger Profile_Rule (Profilregel) på testenheden for at synkronisere den krypterede fil i stedet for den oprindelige XML-fil. Krypteringsnøglen gøres kendt for telefonen med følgende URL-indstilling:

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

Trin 5 Klik på **Send alle ændringer**.

Trin 6 Se syslog-sporet fra telefonen.

Ved gensynkronisering downloader telefonen den nye fil og bruger den til at opdatere dens parametre.

Lignende emner

AES-256-CBC-kryptering, på side 18

Opret partitionerede profiler

En telefon downloader flere separate profiler under hver enkelt gensynkronisering. Denne fremgangsmåde gør det muligt at administrere forskellige typer profiloplysninger på separate servere og vedligeholdelse af fælles konfigurationsparameterværdier, der er adskilt fra kontospecifikke værdier.

Fremgangsmåde

Trin 1 Opret en ny XML-profil, `basic2.txt`, der angiver en værdi for en parameter, der får den til at adskille sig fra de tidligere øvelser. Føj f.eks. følgende til profilen `basic.txt`:

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

Trin 2 Gem profilen `basic2.txt` i den virtuelle rodmappe på TFTP-serveren.

Trin 3 Lad den første profilregel fra tidligere øvelser være i mappen, men konfigurer den anden profilregel (Profile_Rule_B) til at pege på den nye fil:

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

Trin 4 Klik på **Send alle ændringer**.

Telefonen gensynkroniserer nu både til den første og anden profil og i den rækkefølge, hver gang en gensynkronisering forfalder.

Trin 5 Se syslog-sporet for at bekræfte den forventede funktionsmåde.

Angiv header til beskyttelse af personlige oplysninger for telefon

En header til beskyttelse af brugerens personlige oplysninger i SIP-meddelelsen indstiller behovet for beskyttelsen af brugernes personlige oplysninger fra det pålidelige netværk.

Du kan angive headerværdien for beskyttelse af brugernes personlige oplysninger for hvet linjenummer ved hjælp af en XML-kode i filen `config.xml`.

Indstillingerne for header med beskyttelse af personlige oplysninger er:

- Deaktiveret (standard)
- Ingen – brugeren anmoder om, at en tjeneste til beskyttelse af personlige oplysninger ikke anvender nogen funktioner til beskyttelse af personlige oplysninger på denne SIP-meddelelse.
- Header – brugeren har brug for en tjeneste til beskyttelse af personlige oplysninger for at skjule headere, som identificerende oplysninger ikke kan slettes fra.
- Session – brugeren anmoder om, at en tjeneste til beskyttelse af personlige oplysninger sikrer anonymitet for sessionerne.
- Bruger – brugeren anmoder om et niveau af beskyttelse af personlige oplysninger, der kun varetages af mellemmænd.
- Id – brugeren anmoder om, at systemet erstatter et id, der ikke viser IP-adressen eller værtsnavnet.

Fremgangsmåde

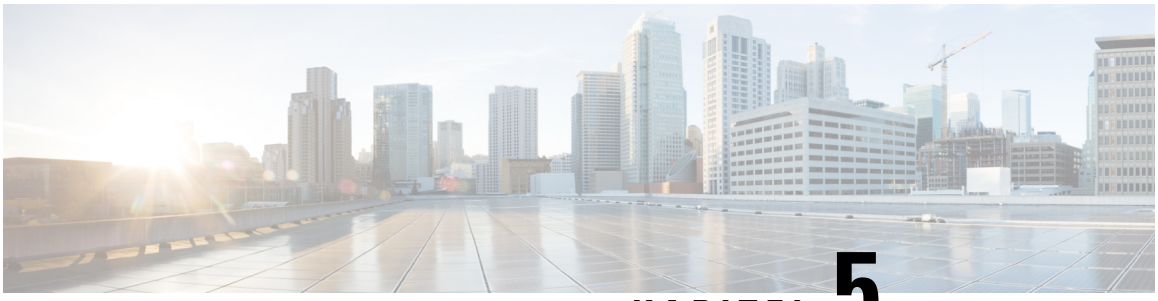
Trin 1 Rediger telefonfilen `config.xml` i en tekstfil eller XML-redigeringsprogram.

Trin 2 Indsæt **<Privacy_Header_N_ ua = "na">*Værdi*</ Privacy_Header_N_>**-koden, hvor N er linjelokalnummeret tal (1-10), og benyt en af følgende værdier.

- Standardværdi: **Deaktiveret**
- **ingen**
- **header**
- **session**
- **bruger**
- **id**

Trin 3 (Valgfri) Klargør eventuelle ekstra linjelokalnumre, der bruger den samme kode, med det krævede linjelokalnummer.

Trin 4 Gem ændringerne i filen `config.xml`.



KAPITEL 5

Klargøringsparametre

Oversigt over klargøringsparametre

Dette kapitel beskriver de klargøringsparametre, der kan bruges i scripts til konfigurationsprofiler.

Konfigurationsprofilparametre

Følgende tabel definerer funktionen og brugen af hver parameter i afsnittet **Konfigurationsprofilparametre** under fanen **Klargøring**.

Parameternavn	Beskrivelse og standardværdi
Provision Enable (Aktivér klargøring)	Styrer alle gensynkroniseringshandlinger uafhængigt af firmwareopgraderingshandlinger. Indstil til **Ja** for at aktivere ekstern klargøring. Standardværdien er Ja.
Resync On Reset (Gensynkronisering ved nulstilling)	Udløser en gensynkronisering efter hver genstart, bortset ved genstarter, der skyldes parameteropdateringer og firmwareopgraderinger. Standardværdien er Ja.

Parameternavn	Beskrivelse og standardværdi
Resync Random Delay (Vilkårlig forsinkelse på gensynkronisering)	En vilkårlig forsinkelse efter startsekvensen før nulstillingen udføres; angivet i sekunder. I en gruppe enheder med IP-telefoni, der er planlagt til at skulle starte samtidigt, giver dette en spredning i de tidspunkter, hvor hver enkelt enhed sender en gensynkroniseringsanmodning til klargøringsserveren. Denne funktion kan være nyttig ved installationer i stort boligområde, hvis der skulle ske et strømnedbrud. Værdien for dette felt skal være et heltal mellem 0 og 65535. Standardværdien er 2.
Resync At (HHmm) (Gensynkroniser kl. (TTmm))	Tiden (TTmm), hvor enheden igen synkroniseres med klargøringsserveren. Værdien for dette felt skal være et tal på fire cifre lige fra 0000 til 2400, der angiver tiden i TTmm-formatet. 0959 angiver f.eks. 09:59. Standardværdien er tom. Hvis værdien er ugyldig, ignoreres parameteren. Hvis denne parameter er angivet med en gyldig værdi, ignoreres parameteren Resync Periodic (Gensynkroniser periodisk).
Resync At Random Delay (Gensynkronisering ved vilkårlig forsinkelse)	Forhindrer en overbelastning af klargøringsserveren, når et stort antal enheder tændes samtidigt. For at undgå at oversvømme serveren med gensynkroniseringsanmodninger fra flere telefoner, gensynkroniseres telefonen i intervallet mellem timerne og minutter, og timerne og minutter plus vilkårlig forsinkelse (ttmm, ttmm+random_delay (vilkårlig forsinkelse)). Hvis f.eks. den vilkårlige forsinkelse = (synkroniser igen ved vilkårlig forsinkelse + 30)/60 minutter, konverteres inputværdien i sekunder til minutter og afrundes til næste minut for at beregne det endelige vilkårlige forsinkelsesinterval. Gyldig værdi er i intervallet mellem 0 og 65535. Denne funktion er deaktiveret, når denne parameter er indstillet til nul. Standardværdien er 600 sekunder (10 minutter).

Parameternavn	Beskrivelse og standardværdi
Resync Periodic (Gensynkroniser periodisk)	Tidsintervallet mellem periodiske gensynkroniseringer med klargøringsserveren. Den tilknyttede tidsindstilling for gensynkronisering er kun aktiv, efter den første synkronisering med serveren er gennemført. De gyldige formater er som følger: • Et heltal Eksempel: Et input på `3000` angiver, at næste gensynkroniseringen sker om 3000 sekunder. • Flere heltal Eksempel: Input af `600,1200,300` angiver, at den første gensynkronisering sker om 600 sekunder, den anden gensynkronisering sker 1200 sekunder efter den første, og den tredje gensynkronisering sker 300 sekunder efter den anden. • Et tidsinterval Et input på `2400+30` angiver, at den næste gensynkronisering sker mellem 2400 og 2430 sekunder efter en gennemført gensynkronisering. Indstil denne parameter til nul for at deaktivere periodisk gensynkroniseringen. Standardværdien er 3600 sekunder.

Parameternavn	Beskrivelse og standardværdi
Resync Error Retry Delay (Forsinkelse ved nyt forsøg efter gensynkroniseringsfejl)	Hvis en gensynkronisering mislykkes, fordi enheden med IP-telefon ikke kunne hente en profil fra serveren, eller den downloadede fil er beskadiget, eller der sker en intern fejl, forsøger enheden at synkronisere igen efter et tidsrum, der er angivet i sekunder. De gyldige formater er som følger: • Et heltal Eksempel: Et input på `300` angiver, at næste forsøg på gensynkronisering sker om 300 sekunder. • Flere heltal Eksempel: Et input på `600,1200,300` angiver, at det første forsøg sker 600 sekunder efter fejlen, det andet forsøg sker 1200 sekunder efter fejlen i det første forsøg, og det tredje forsøg sker 300 sekunder efter fejlen i det andet forsøg. • Et tidsinterval Et input på `2400+30` angiver, at det næste forsøg sker mellem 2400 og 2430 sekunder efter en mislykket gensynkronisering. Hvis forsinkelsen er indstillet til 0, forsøger enheden ikke at synkronisere igen efter et mislykket forsøg på gensynkronisering.
Forced Resync Delay (Tvungen forsinkelse på gensynkronisering)	Maksimal forsinkelse (i sekunder), telefonen venter, før der udføres en gensynkronisering. Enheden gensynkroniserer igen, når en af dens telefonlinjer er aktiv. Da en gensynkronisering kan tage adskillige sekunder, er det bedst at vente, indstil enheden har været inaktiv i længere tid før gensynkronisering. Dette giver en bruger mulighed for at foretage opkald efter hinanden uden afbrydelse. Enheden har en tidsindstilling, der begynder at tælle ned, når alle dens linjer bliver ledige. Denne parameter er startværdien for tælleren. Gensynkroniseringshændelser forsinkes, før denne tæller når nul. Gyldig værdi er i intervallet mellem 0 og 65535. Standardværdien er 14.400 sekunder.

Parameternavn	Beskrivelse og standardværdi
Resync From SIP (Gensynkronisering fra SIP)	Giver mulighed for, at en gensynkronisering kan udløses via en SIP NOTIFY-meddelelse. Standardværdien er Ja.
Resync efter forsøg på opgradering (Synkroniser igen efter opgraderingsforsøg)	Aktiverer eller deaktiverer gensynkroniseringshandlingen, når der opstår en opgradering. Hvis Ja er valgt, udløses synkronisering. Standardværdien er Ja.
Resync Trigger 1 (Udløser 1 af gensynkronisering), Resync Trigger 2 (Udløser 2 af gensynkronisering)	Konfigurerbare betingelser for udløsning af gensynkronisering. En gensynkronisering udløses, når den logiske ligning i disse parameter giver SAND. Standardværdien er (tom).
Resync Fails On FNF (Gensynkronisering mislykkes ved FNF)	En gensynkronisering anses for at være mislykket, hvis en anmodet profil ikke modtages fra serveren. Parameteren kan tilsidesætte dette. Når den er indstillet til **Nej**, accepterer enheden svaret `fil ikke fundet` fra serveren som en gennemført gensynkronisering. Standardværdien er Ja.
Profilregel Profile Rule B (Profilregel B) Profile Rule C (Profilregel C) Profile Rule D (Profilregel D)	Hver profilregel giver telefonen besked om den kilde, der skal hentes en profil (konfigurationsfilen) fra. For hver gensynkronisering anvender telefonen alle profilerne i rækkefølge. Standard: **`/$PSN.xml`** Hvis du anvender AES-256-CBC-kryptering til konfigurationsfilerne, skal du angive krypteringsnøglen med nøgleordet **`--key`** på følgende måde: **`[--key <krypteringsnøgle>]`** Nøglen kan eventuelt angives i dobbelte anførselstegn (").
DHCP Option To Use (DHCP-indstilling i brug)	DHCP-indstillinger, adskilt med kommaer, bruges til at hente firmware og profiler. Standardværdien er 66,160,159,150,60,43,125.
Log Request Msg (Meddelelse om logføringsanmodning)	Denne parameter indeholder den meddelelse, der sendes til syslog-serveren ved start af forsøg på gensynkronisering. Standardværdien er `$PN $MAC – anmoder % $SCHEME://$SERVIP:$PORT$PATH`.

Parameternavn	Beskrivelse og standardværdi
Log Success Msg (Meddelelse om logføring gennemført)	Den syslog-meddelelse, der udstedes ved gennemførelse af forsøg på gensynkronisering. Standardværdien er `$PN $MAC – gennemført gensynkronisering % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Log Failure Msg (Meddelelse om logføring mislykket)	Den syslog-meddelelse, der udstedes efter mislykket forsøg på gensynkronisering. Standardværdien er `$PN $MAC – gensynkronisering mislykkedes: $ERR`.
User Configurable Resync (Gensynkronisering, bruger kan konfigurere)	Giver en bruger mulighed for gensynkronisere telefonen via IP-telefonskærmen. Standardværdien er Ja.

Firmwareopgraderingsparametre

Følgende tabel definerer funktionen og brugen af hver parameter i afsnittet **Firmwareopgradering** under fanen **Klargøring**.

Parameternavn	Beskrivelse og standardværdi
Upgrade Enable (Opgradering aktiveret)	Giver mulighed for firmwareopgradering uafhængigt af gensynkroniseringshandlinger. Standardværdien er Ja.
Upgrade Error Retry Delay (Forsinkelse på forsøg ved opgraderingsfejl)	Intervallet for nyt forsøg på opgradering (i sekunder), der benyttes ved en opgraderingsfejl. Enheden har en tidsindstilling for firmwareopgradering, der aktiveres efter et mislykket forsøg på firmwareopgradering. Tidsindstillingen initialiseres med værdien i denne parameter. Det næste forsøg på firmwareopgradering sker, når denne tidsindstilling tæller ned til nul. Standardværdien er 3600 sekunder.

Parameternavn	Beskrivelse og standardværdi
Opgraderingsregel	Et script til firmwareopgradering, der definerer opgraderingsbetingelser og tilknyttede firmware-URL-adresser. Den bruger samme syntaks som profilreglen. Brug følgende format til at angive opgraderingsreglen: **<tftp|http|https>://<ip-adresse>/image/<load-navn>** For eksempel: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Hvis der ikke er angivet en protokol, antages det, at TFTP skal bruges. Hvis der ikke er angivet et servernavn, vil den vært, der anmoder om URL-adressen, blive brugt som servernavnet. Hvis der ikke er angivet en port, bruges standardporten (69 for TFTP, 80 for HTTP eller 443 for HTTPS). Standardværdien er tom.
Log Upgrade Request Msg (Meddelelse om logføring af opgraderingsanmodning)	Syslog-meddelelse, der udstedes ved start af et forsøg på opgradering af firmware. Standard: `$PN $MAC – anmoder om opgradering $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg (Meddelelse om logføring af gennemført opgradering)	Syslog-meddelelse, der udstedes, efter at et forsøg på opgradering af firmwaren er gennemført. Standardværdien er `$PN $MAC – gennemført opgradering $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg (Meddelelse om logføring af mislykket opgradering)	Syslog-meddelelse, der udstedes efter mislykket forsøg på opgradering af firmware. Standardværdien er `$PN $MAC – opgraderingen er mislykket: $ERR`
Peer-firmwaredeling	Aktiverer eller deaktiverer funktionen til peer-firmwaredeling. Vælg **Ja** eller **Nej** for at aktivere eller deaktivere funktionen. Standard: ja
Logserver for peer-firmwaredeling	Angiver IP-adressen og porten, som UDP-meddelelsen sendes til. For eksempel: 10.98.76.123:514, hvor 10.98.76.123 er IP-adressen og 514 portnummeret.

Parametre for generelle formål

Følgende tabel definerer funktionen og brugen af hver parameter i afsnittet **Parametre for generelle formål** under fanen **Klargøring**.

Parameternavn	Beskrivelse og standardværdi
GPP A - GPP P	Parametrene for generelle formål (GPP_*) bruges som frie strengregistre, når telefonerne konfigureres til at interagere med en bestemt klargøringsserverløsning. De kan konfigureres til at indeholde forskellige værdier, herunder følgende: • Krypteringsnøgler. • URL-adresser. • Oplysninger om status ved klargøring i flere faser. • Skabeloner for Post-anmodninger. • Tilknytninger til alias for parameternavn • Delvise strengværdier, eventuelt samlet til komplette parameterværdier. Standardværdien er tom.

Makroudvidelsesvariabler

Visse makrovariabler genkendes i følgende klargøringsparametre:

- Profile_Rule (Profilregel)
- Profile_Rule_* (Profilregel_*)
- Resync_Trigger_* (Udløser 1 af gensynkronisering_*)
- Opgraderingsregel
- Log_*
- GPP_* (under visse betingelser)

I disse parametre genkendes og udvides syntakstyper som f.eks. $NAME eller $(NAME).

Understrenge i makrovariable kan angives med notationen $(NAME:p) og $(NAME:p:q), hvor p og q er ikke-negative heltal (tilgængelig i revision 2.0.11 og derover). Den resulterende makroudvidelse i understrengen, startende ved tegnforskydning p, med længde q (eller indtil afslutningen af streng, hvis q ikke er angivet). Hvis GPP_A f.eks. indeholder ABCDEF, så udvides $(A:2) til CDEF, og $(A:2:3) udvides til CDE.

En ukendt navn er ikke oversat, og formen $NAME eller $(NAME) forbliver uændret i parameterværdien efter udvidelse.

Parameternavn	Beskrivelse og standardværdi
$	Formen $$ udvides til et enkelt $-tegn.
A til og med P	Erstattet af indholdet af parametrene for generelle formål GPP_A til og med GPP_P.
SA til og med SD	Erstattes af parametrene GPP_SA til og med GPP_SD til særlige formål. Disse parametre opbevarer nøgler eller adgangskoder, der bruges ved klargøring. **Bemærk** $SA til og med $SD genkendes som argumenter til den valgfri URL-kvalifikationer til gensynkronisering, --key.
MA	MAC-adresse, der bruger hexidecimale cifre med små bogstaver, f.eks. (000e08aabbcc).
MAU	MAC-adresse, der bruger hexidecimale cifre med store bogstaver, f.eks. (000E08AABBCC).
MAC	MAC-adresse, der bruger hexidecimale cifre med små bogstaver og koloner for at adskille par af hexidecimale cifre. For eksempel 00:0e:08:aa:bb:cc.
PN	Produktnavn. For eksempel CP-6841-3PCC.
PSN	Produktserienummer. For eksempel 6841-3PCC.
SN	Serienummerstreng, f.eks. 88012BA01234.
CCERT	Status for SSL-klientcertifikat: installeret eller ikke installeret.
IP	IP-adressen på telefonen i det lokale undernet. For eksempel 192.168.1.100.
EXTIP	Ekstern IP for telefonen som set på internettet. For eksempel 66.43.16.52.
SWVER	Softwareversionsstreng. For eksempel sip68xx.11-0-1MPP.
HWVER	Hardwareversionsstreng. For eksempel 2.0.1
PRVST	Klargøringstilstand (en numerisk streng): -1 = eksplicit anmodning om gensynkronisering 0 = gensynkronisering ved start 1 = periodisk gensynkronisering 2 = gensynkronisering er mislykket, antal nye forsøg

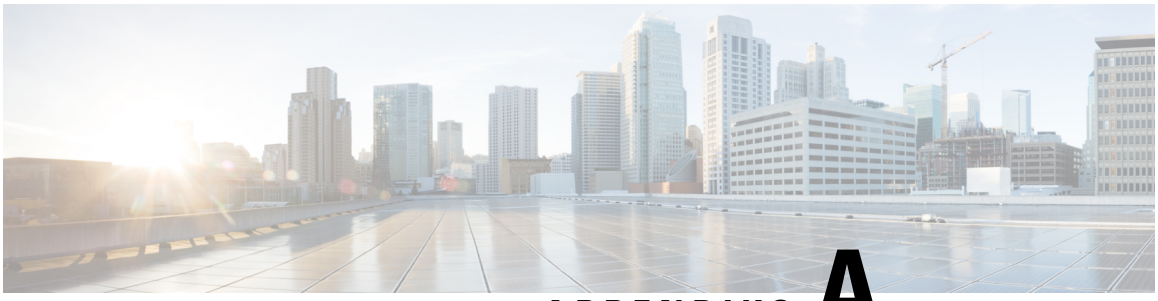
Parameternavn	Beskrivelse og standardværdi
UPGST	Opgraderingstilstand (en numerisk streng): 1 = første opgraderingsforsøg 2 = opgradering er mislykket, antal nye forsøg
UPGERR	Resulterende meddelelse (ERR) om tidligere opgraderingsforsøg; f.eks. http_get er mislykket.
PRVTMR	Sekunder siden sidste forsøg gensynkronisering.
UPGTMR	Sekunder siden sidste forsøg opgradering
REGTMR1	Sekunder siden linje 1 mistede registrering med SIP-server.
REGTMR2	Sekunder siden linje 2 mistede registrering med SIP-server.
UPGCOND	Tidligere makronavn.
SCHEME	Filadgangsskema, en af TFTP, HTTP eller HTTPS, som hentet efter parsing af URL-adresse til gensynkronisering eller opgradering.
SERV	Anmod om destinationservers værtsnavn, som hentet efter under parsing af URL-adresse til gensynkronisering eller opgradering.
SERVIP	Anmod om destinationservers IP-adresse, som hentet efter parsing af URL-adresse til gensynkronisering eller opgradering, muligvis efter DNS-opslag.
PORT	Anmod om destinations-UDP/TCP-port, som hentet efter parsing af URL-adresse til gensynkronisering eller opgradering.
PATH	Anmod om filsti, som hentet efter under parsing af URL-adresse til gensynkronisering eller opgradering.
ERR	Resulterende meddelelse om forsøg på gensynkronisering eller opgradering. Kun nyttig ved generering af resulterende syslog-meddelelser. Værdien bevares i variablen UPGERR i tilfælde af forsøg på opgradering.
UIDn	Indholdet af linje UserID-konfigurationsparameteren for linje n.
EMS	Extension Mobility Status (status for mobilitet af lokalnummer)

Parameternavn	Beskrivelse og standardværdi
MUID	Extension Mobility User ID (Bruger-id for mobilitet af lokalnummer)
MPWD	Extension Mobility Password (Adgangskode for mobilitet af lokalnummer)

Koder for interne fejl

Telefonen definerer et antal interne fejlkoder (X00 – X 99) for at lette konfigurationen ved at give en finere styring af enhedens funktionsmåde under visse fejlbetingelser.

Parameternavn	Beskrivelse og standardværdi
X00	Transportlagsfejl (eller ICMP) ved afsendelse af en SIP-anmodning.
X20	Timeout for SIP-anmodning, mens der ventes på et svar.
X40	Generel SIP-protokolfejl (f.eks. et ikke-acceptabelt codec i SDP i 200 og kvitteringsmeddelelser, eller der er timeout, mens der ventes på kvittering).
X60	Det opkaldt nummer er ugyldigt i henhold til den angivne opkaldsplan.



APPENDIKS A

Eksempel på konfigurationsprofiler

Eksempel på XML Open 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 konfigurationsprofiler

```
<!--  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 konfigurationsprofiler

```
<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 konfigurationsprofiler

```
<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 konfigurationsprofiler

```
<!--
 available options:
-12:00|-11:00|-10:00|-09:00|-08:00|-07:00|-06:00|-05:00|-04:00|-03:30|-03:00|-02:00|-01:00|+00:00|+01:00|+02:00|+03:00|+03:30|+04:00|+04:30|+05:00|+05:30|+05:45|+06:00|+06:30|+07:00|+08:00|+08:45|+09:00|+09:30|+10:00|+10:30|+11:00|+12:00|+12:45|+13:00|+14:00

-->
<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 konfigurationsprofiler

```
<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>
```

Eksempel på konfigurationsprofiler

```
<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 konfigurationsprofiler

```
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 konfigurationsprofiler

```
<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 konfigurationsprofiler

```
<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 konfigurationsprofiler

```
<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 konfigurationsprofiler

```
<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"/>
```

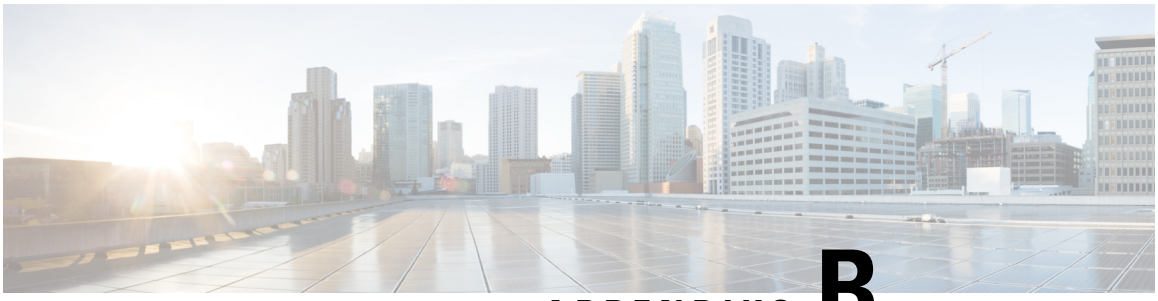
Eksempel på konfigurationsprofiler

```
<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 konfigurationsprofiler

```
 <!--  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>
```



APPENDIKS B

Akronymer

Akronymer

Vekselstrøm	Vekselstrøm
ACS	Adgangskontrolserver
A/D	Analog To Digital Converter
AES	Avanceret krypteringsstandard
ANC	Anonymous Call
AP	Access point
ASCII	Amerikansk standardkode til udveksling af oplysninger
B2BUA	Back to Back User Agent (Brugeragent fra start til slut)
Optagetmarkering	Optagetlys (BLF)
Bool	Boolean Values (Booleske værdier). Angivet som ja og nej eller 1 og 0 i en profil
BootP	Bootprotokol
CA	Certificate Authority
CAS	CPE Alert Signal
CDP	Cisco Discovery Protocol
CDR	Call Detail Record
CGI	Computergenereret Mmagery
CID	Caller ID
CIDCW	Call Waiting Caller ID

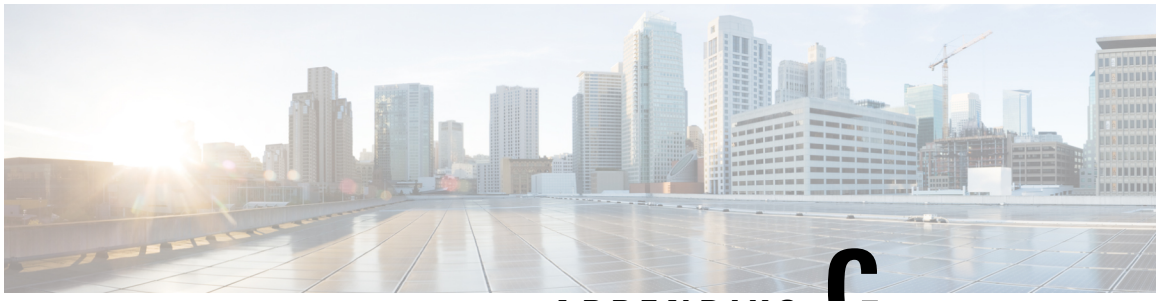
CNG	Comfort Noise Generation
CPC	Calling Party Control
CPE	Customer Premises Equipment
CSV	Kommasepareret værdi
CWCID	Call Waiting Caller ID
CWT	Call Waiting Tone
D/A	Digital to Analog Converter
dB	decibel
dBm	dB med hensyn til 1 milliwatt
DHCP	Dynamic Host Configuration Protocol
DND	Forstyr ikke
DNS	Domain Name System (DNS)
□DoS	DoS (Denial of Service)
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Loop
DSP	Digital Signal Processor
Sommertid	Sommertid
DTAS	Data Terminal Alert Signal (samme som CAS)
DTMF	Dual Tone Multiple Frequency
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
Vs:	Firmware
FXS	Foreign eXchange Station
GMT	GMT (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	Internet Protocol
IPv4	Internetprotokol version 4
IPv6	Internetprotokol version 6
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
ITU	International Telecommunication Union
IVR	Interactive Voice Response
LAN	Local Area Network
LBR	Low Bit Rate
LBRC	Low Bit Rate Codec
LCD	Liquid Crystal Display; også kendt som LCD-skærm
LDAP	Lightweight Directory Access Protocol
LED-indikator	LED (Light-Emiting Diode)
MAC-adresse	MAC-adresse
MC	Mini-Certificate
MGCP	Media Gateway Control Protocol
MOH	Music On Hold
MOS	Mean Opinion Score (1-5, jo højere jo bedre)
MPP	Multiplatform Phones
ms	Millisecond
MSA	Music Source Adaptor
MWI	Message Waiting Indication
NAT	Network Address Translation
NPS	Normal klargøringsserver
NTP	NTP (Network Transport Protocol)
OOB	Out-of-band
OSI	Open Switching Interval

PBX	Privat omstillingssystem
PCB	Printed Circuit Board
PoE	Power over Ethernet (PoE)
PR	Polarity Reversal
PS	Provisioning Server
PSQM	Perceptual Speech Quality Measurement (1-5, jo lavere jo bedre)
PSTN	Public Switched Telephone Network
QoS	Tjenestekvalitet
RC	Fjern tilpasning
REQT	(SIP) Request Message
RESP	(SIP) Response Message
RSC	(SIP) Response Status Code, f.eks. 404, 302, 600
RTP	Real Time Protocol
RTT	Round Trip Time
SAS	Streaming Audio Server
SDP	Session Description Protocol
SDRAM	Synchronous DRAM
sec	sekunder
SIP	Session Initiation Protocol
SLA	Shared line appearance
SLIC	Subscriber Line Interface Circuit
SP	Service provider
SSL	Secure Socket Layer
STUN	Session Traversal UDP for NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	TLS (Transport Layer Security)
TTL	Tid til aktiv
ToS	Typen af tjeneste

UA	User Agent
uC	Micro-controller
UDP	User Datagram Protocol
URI	URI (Uniform Resource Identifier)
URL	Uniform Resource Locator
UTC	CUT (Coordinated Universal Time)
VAR	Value Added Reseller (forhandler)
VLAN	Stemme-LAN
VM	Voicemail
VMWI	Visual Message Waiting Indication/Indicator
VoIP	Internetprotokol
VQ	Talekvalitet
WAN	Wide Area Network
XML	Extensible Markup Language

Akronymer



APPENDIKS C

Relateret dokumentation

Relateret dokumentation

Du kan bruge følgende afsnit til at finde relaterede oplysninger.

Dokumentation til Cisco IP Phone 6800-serien

Se de publikationer, der er specifikke for dit sprog, din telefonmodel og version af multiplatformfirmware. Naviger fra den følgende URL (Uniform Resource Locator):

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

Supportpolitik for firmware til Cisco IP Phone

Få oplysninger om supportpolitikken for telefoner under https://cisco.com/go/phonefirmwaresupport.