Etableringshandbok för Cisco IP Phone 6800-seriens multiplattformstelefoner

Först publicerad: 2017-11-22

Senast ändrad: 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.

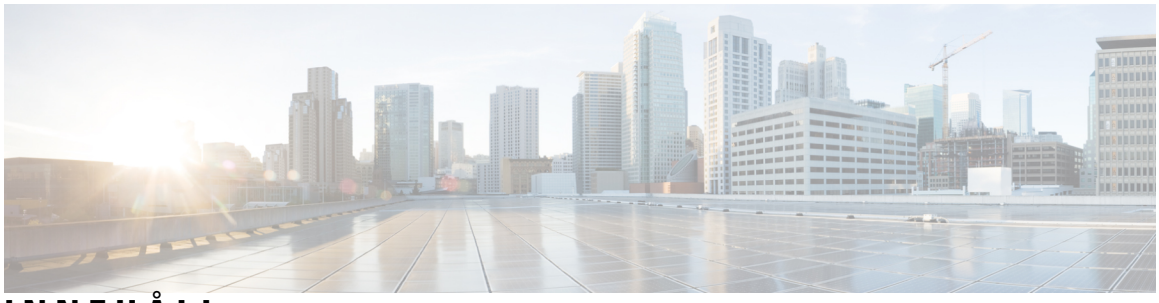
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

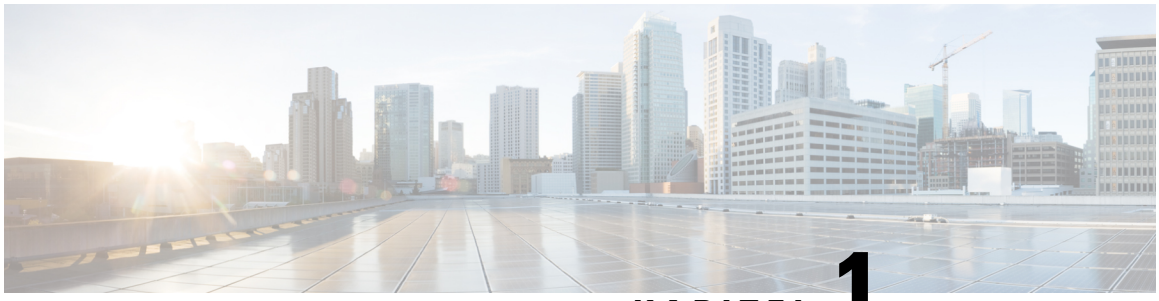
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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)



INNEHÅLL



KAPITEL 1

Distribution och etablering

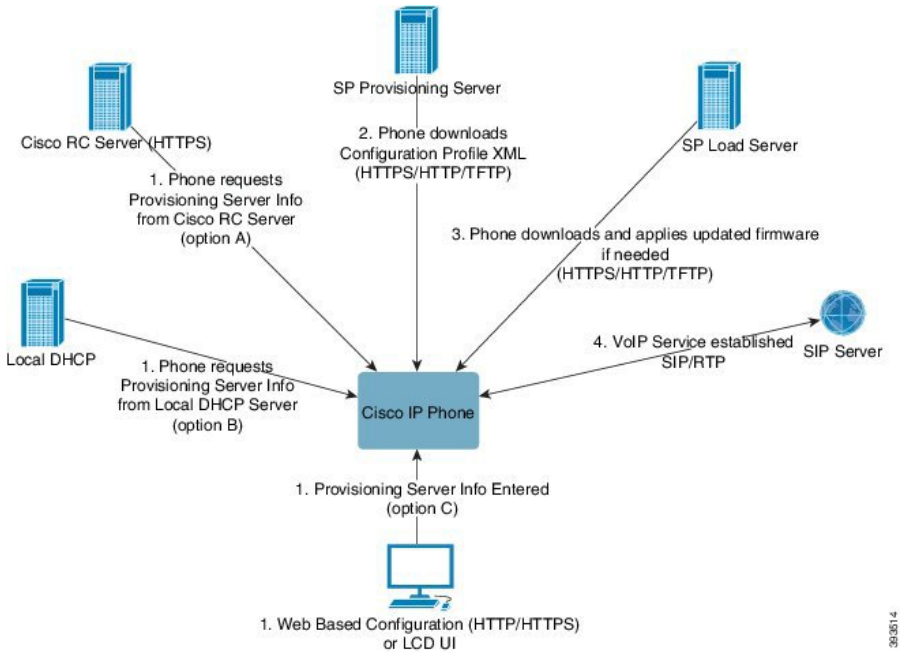
Etableringsöversikt

Cisco IP Phones är avsedda för storskaliga distributioner av VoIP-tjänstleverantörer (Voice-over-IP) till kunder i hem-, företags- eller storföretagsmiljöer. Etablering av telefonen via fjärrhantering och fjärrkonfiguration säkerställer därför korrekt drift hos kunden.

Cisco tillhandahåller anpassad och löpande konfiguration av telefonens funktioner genom:

- Tillförlitlig fjärrstyrning av telefonen.
- Kryptering av kommunikationen som styr telefonen.
- Effektiv bindning av telefonkonton.

Telefoner kan etableras för att hämta konfigurationsprofiler eller uppdaterad fast programvara från en fjärrserver. Hämtningar kan ske när telefonerna är anslutna till ett nätverk, när de är påslagna och enligt bestämda intervall. Etablering är vanligtvis en del av de storskaliga VoIP-distributioner som tjänsteleverantörer ofta genomför. Konfigurationsprofiler eller uppdaterad fast programvara överförs till enheten via TFTP, HTTP eller HTTPS.



På högre nivå ser telefonetableringsprocessen ut så här:

1. Om telefonen inte har konfigurerats används informationen från etableringsservern på telefonen med hjälp av någon av följande metoder:
   - **A**– Hämtas från Ciscos EDOS-server (Enablement Data Orchestration System) med fjärranpassning (RC) via HTTPS.
   - **B**– En fråga skickas från en lokal DHCP-server.
   - **C**– Anges manuellt med hjälp av Ciscos webbaserade konfigurationsverktyg för telefoner eller telefonanvändargränssnittet.
2. Telefonen hämtar informationen från etableringsservern och tillämpar XML-konfigurationsfilen via HTTPS-, HTTP- eller TFTP-protokollet.
3. Telefonen hämtar och tillämpar den uppdaterade fasta programvaran, om det behövs, via HTTPS, HTTP eller TFTP.
4. VoIP-tjänsten upprättas med hjälp av den angivna konfigurationen och fasta programvaran.

VoIP-tjänstleverantörer distribuerar ett stort antal telefoner till hemanvändare och små företagskunder. I företags- eller storföretagsmiljöer kan telefoner fungera som terminalnoder. Dessa enheter distribueras ofta av leverantörerna över Internet och ansluts till kunden via routrar och brandväggar.

Telefonen kan användas som en fjärransluten förlängning av tjänstleverantörens backend-utrustning. Fjärrhantering och fjärrkonfiguration säkerställer att telefonen fungerar korrekt hos kunden.

TR69-etablering

Cisco IP Phone hjälper administratören att konfigurera TR69-parametrarna via det webbaserade användargränssnittet. Information om parametrarna, inklusive en jämförelse av XML- och TR69-parametrarna, finns i administrationsguiden för motsvarande telefonserie.

Telefonerna har stöd för ACS-identifiering (Auto Configuration Server) från DHCP-alternativ 43, 60 och 125.

- Alternativ 43 – Leverantörsspecifik information för ACS-URL:en.
- Alternativ 60 – Leverantörsklass-ID som telefonen använder för att identifiera sig med `dslforum.org` till ACS.
- Alternativ 125 – Leverantörsspecifik information för gateway-associationen.

RPC-metoder

RPC-metoder som stöds

Telefonerna har endast stöd för följande begränsade uppsättning RPC-metoder (Remote Procedure Call):

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Informera
- Download: RPC-hämtningsmetod; följande filtyper stöds:
    - Avbildning för uppgradering av fast programvara
    - Leverantörskonfigurationsfil
    - Anpassad CA-fil (Certificate Authority)
- Transfer Complete

Typer av händelser som stöds

Telefonerna stöder händelsetyper baserat på vilka funktioner och metoder som stöds. Endast följande händelsetyper stöds:

- Bootstrap
- Boot
- Value change
- Connection request
- Periodic
- Transfer Complete
- M Download
- M Reboot

Telefonbeteende under överbelastning av nätverket

- Administrativa åtgärder, t.ex. skanning av en intern port eller en säkerhetsskanning.
- Om ditt nätverk attackeras, t.ex. med en DoS-attack.

Implementering

Cisco IP Phones tillhandahåller smidiga etableringsmekanismer, baserat på följande distributionsmodeller:

- Massdistribution – Tjänsteleverantören införskaffar ett stort antal Cisco IP Phones och företablerar dem internt eller köper RC-enheter för fjärranpassning från Cisco. Enheterna utfärdas sedan till kunderna som en del av ett VoIP-servicekontrakt.
- Återförsäljardistribution – Kunden köper en Cisco IP Phone i en butik och beställer VoIP-tjänster från tjänsteleverantören. Tjänsteleverantören ansvarar sedan för en säker fjärrkonfiguration av enheten.

Massdistribution

I den här modellen skickar tjänsteleverantören telefoner till sina kunder som en del av ett VoIP-servicekontrakt. Enheterna är antingen RC-enheter eller företablerade internt.

Cisco företablerar RC-enheter för omsynkronisering med en Cisco-server som hämtar enhetsprofilen och uppdateringar av den fasta programvaran.

En tjänsteleverantör kan företablera telefoner med önskade parametrar, inklusive de parametrar som styr omsynkroniseringen, på olika sätt:

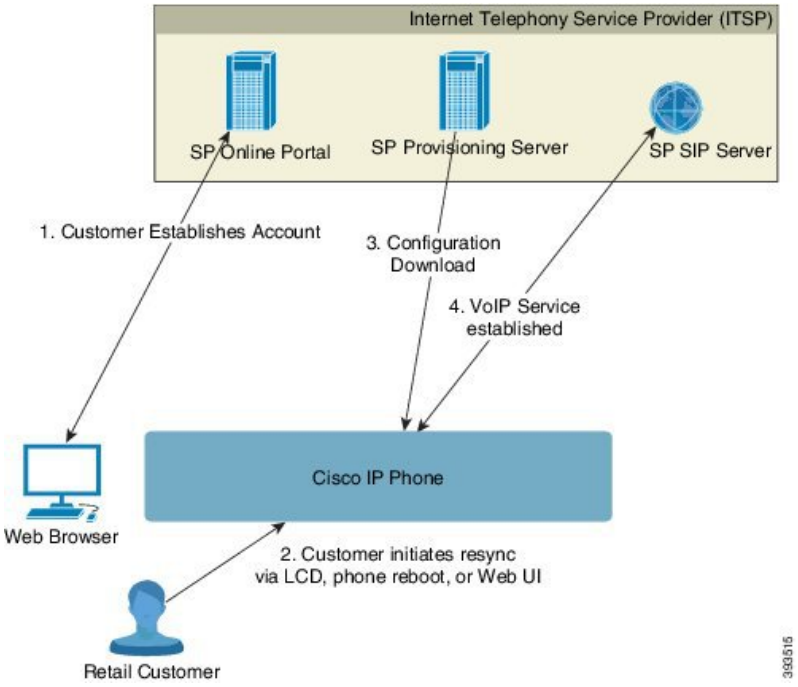
- Internt med hjälp av DHCP och TFTP
- Från en fjärrplats med hjälp av TFTP, HTTP eller HTTPS

- En kombination av intern etablering och fjärretablering

Distribution inom detaljhandeln

I en distributionsmodell för detaljhandeln köper en kund en telefon och prenumererar på en viss tjänst. En ITSP (Internet telefoni Service Provider) konfigurerar och underhåller en etableringsserver och företablerar telefonen för synkronisering med tjänstleverantörens server.

Figur 1. Distribution inom detaljhandeln



Telefonen innehåller det webbaserade konfigurationsverktyget som visar den interna konfigurationen och som tar emot nya konfigurationsparametervärden. Servern stöder även en speciell URL-kommandosyntax för profilomsynkronisering och uppgradering av fast programvara via en fjärranslutning.

Kunden loggar in till tjänsten och skapar ett VoIP-konto, t.ex. via en onlineportal, och kopplar enheten till det tilldelade tjänstkontot. Den icke-etablerade telefonen uppmanas att synkronisera med en specifik etableringsserver via ett URL-omsynkroniseringskommando. URL-kommandot innehåller vanligtvis kund-ID:t eller den alfanumeriska koden för ett konto som unikt associerar enheten med det nya kontot.

I följande exempel uppmanas en enhet på den DHCP-tilldelade IP-adressen 192.168.1.102 att etablera sig mot SuperVoIP-tjänsten:

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

I det här exemplet är 1234abcd kund-ID:t för det nya kontot. Den fjärranslutna etableringsservern associerar telefonen som utför omsynkroniseringsbegäran med det nya kontot, baserat på URL:en och det angivna kund-ID:t. Med den här första omsynkroniseringen konfigureras telefonen i ett enda steg. Telefonen uppmanas sedan att synkronisera om till en permanent URL på servern. Till exempel:

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

För både initial och permanent åtkomst behöver etableringsservern telefonens klientcertifikat för autentisering. Etableringsservern tillhandahåller rätt konfigurationsparametervärden baserat på det associerade tjänstkontot.

När enheten startas eller när en viss tid förflutit synkroniserar telefonen och hämtar de senaste parametrarna. Dessa parametrar kan exempelvis användas för att konfigurera en svarsgrupp, ställa in snabbvalsnummer eller för att begränsa vilka funktioner som en användare kan ändra.

Relaterade ämnen

Intern företablering på enheter, på sidan 39

Omsynkroniseringsprocessen

Den fasta programvaran för varje telefon innehåller en administrationswebbserver som accepterar nya konfigurationsparametervärden. Telefonen kan uppmanas att synkronisera om konfigurationen efter en omstart eller enligt schemalagda intervall mot en angiven etableringsserver via ett URL-omsynkroniseringskommando i enhetsprofilen.

Webbservern är aktiverad som standard. Du inaktiverar eller aktiverar webbservern med hjälp av URL-omsynkroniseringskommandot.

Om det behövs kan du begära en omedelbar omsynkronisering via en URL-omsynkroniseringsåtgärd. URL-omsynkroniseringskommandot kan innehålla kund-ID:t eller den alfanumeriska koden för ett konto som unikt associerar enheten med användarens konto.

Exempel

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

I detta exempel uppmanas en enhet på den DHCP-tilldelade IP-adressen 192.168.1.102 att etablera sig mot SuperVoIP-tjänsten på prov.supervoip.com. Kund-ID:t för det nya kontot är 1234abcd. Den fjärranslutna etableringsservern associerar telefonen som utför omsynkroniseringsbegäran med kontot, baserat på URL:en och kund-ID:t.

Med den här första omsynkroniseringen konfigureras telefonen i ett enda steg. Telefonen uppmanas sedan att synkronisera om till en permanent URL på servern.

För både initial och permanent åtkomst behöver etableringsservern klientcertifikatet för autentisering. Servern tillhandahåller konfigurationsparametervärden baserat på det associerade tjänstkontot.

Etablering

En telefon kan konfigureras att regelbundet, eller när den startar, synkronisera sin interna konfigurationsstatus så att den matchar en fjärrprofil. Telefonen kontakter en normal etableringsserver (NPS) eller en åtkomstkontrollserver (ACS).

Som standard utförs profilomsynkroniseringar endast när telefonen är inaktiv. På så sätt förhindras uppgraderingar som annars skulle utlösa en omstart av programvaran och avbryta ett pågående samtal. Om mellanliggande uppgraderingar krävs för att uppnå en aktuell uppgraderingsstatus från en äldre version, kan uppgraderingslogiken automatisera uppgraderingar i flera steg.

Normal etableringsserver

Den normala etableringsservern (NPS, Normal Provisioning Server) kan vara en TFTP-, HTTP- eller HTTPS-server. Fjärruppgraderingar av den fasta programvaran utförs via TFTP, HTTP eller HTTPS eftersom den fasta programvaran inte innehåller känslig information.

Även om HTTPS rekommenderas kräver inte kommunikationen med NPS-servern användning av ett säkert protokoll eftersom den uppdaterade profilen kan krypteras med en delad hemlig nyckel. Mer information om hur du använder HTTPS finns i Kryptering av kommunikation, på sidan 8. Säker förstagångsetablering tillhandahålls med en mekanism som använder SSL-funktioner. En icke-etablerad telefon kan ta emot en krypterad profil med en 256-bitars symmetrisk nyckel som är avsedd för enheten.

Åtkomstkontroll för konfigurationsinställningar

Telefonens fasta programvara innehåller mekanismer som begränsar slutanvändarens åtkomst till vissa parametrar. Den fasta programvaran tillhandahåller särskilda behörigheter för inloggning till ett **administratörskonto** eller ett **användarkonto**. Dessa kan lösenordsskyddas separat.

- Administratörskonto – ger tjänstleverantören fullständig åtkomst till alla parametrar för administrationswebbservern.
- Användarkonto – tillåter att användaren konfigurerar en deluppsättning av parametrarna för administrationswebbservern.

Tjänsteleverantören kan begränsa användarkontot i etableringsprofilen på följande sätt:

- Ange vilka konfigurationsparametrar som är tillgängliga för användarkontot när konfigurationen skapas.
- Inaktivera användaråtkomst till administrationswebbservern.
- Inaktivera användaråtkomst till LCD-användargränssnittet.
- Kringgå skärmen **Ange lösenord** för användaren.
- Begränsa vilka Internetdomäner som används av enheten för omsynkronisering, uppgraderingar och SIP-registrering för linje 1.

Relaterade ämnen

Taggegenskaper för element, på sidan 14
Åtkomstkontroll, på sidan 16

Åtkomst till webbsidan för telefonen

Gå till telefonens webbsida från en webbläsare på en dator som kan nå telefonen i subnätverket.

Om din tjänstleverantör har inaktiverat åtkomst till konfigurationsverktyget kontaktar du tjänstleverantören innan du fortsätter.

Arbetsordning

Steg 1 Kontrollera att datorn kan kommunicera med telefonen. Inget VPN används.

Steg 2 Starta en webbläsare.

Steg 3 Ange IP-adressen till telefonen i webbläsarens adressfält.

- Användaråtkomst: **`http://<ip-adress>/user`**
- Administratörsåtkomst: **`http://<ip-adress>/admin/advanced`**
- Administratörsåtkomst: **`http://<ip-adress>`**, klicka på **ADMIN-inloggning** och sedan på **Avancerat**

Till exempel `http://10.64.84.147/admin`

Tillåt webbåtkomst till en Cisco IP Phone

Om du vill visa telefonparametrarna aktivera du konfigurationsprofilen. Om du vill ändra någon av parametrarna, måste du kunna ändra konfigurationsprofilen. Systemadministratören kan ha inaktiverat telefonalternativet för att göra telefonens webbgränssnitt synligt eller redigeringsbart.

Mer information finns i *Etableringshandbok för Cisco IP Phone 6800-seriens multiplattformstelefoner*.

Innan du börjar

Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Arbetsordning

Steg 1 Klicka på **Röst** > **System**.

Steg 2 Gå till **Systemkonfiguration** och ange **Aktivera webbserver** som **Ja**.

Steg 3 Om att uppdatera konfigurationsprofilen klickar du på **Verkställ alla ändringar** när du har ändrat fälten i telefonens webbanvändargränssnitt.

Telefonen startar om och ändringarna tillämpas.

Steg 4 Om du vill rensa alla ändringar som du har gjort under den aktuella sessionen (eller efter att du senast klickade på **Verkställ alla ändringar**) klickar du på **Ångra alla ändringar**. Värdena återställs till sina tidigare inställningar.

Kryptering av kommunikation

Konfigurationsparametrarna som överförs till enheten kan innehålla behörighetskoder eller annan information som skyddar systemet mot obehörig åtkomst. Det ligger i tjänsteleverantörens intresse att förhindra otillåten kundaktivitet. Det ligger i kundens intresse att förhindra obehörig användning av kontot. Tjänsteleverantören kan kryptera överföringen av konfigurationsprofilen mellan etableringsservern och enheten, samt begränsa åtkomsten till administrationswebbservern.

Telefonenetableringsmetoder

Cisco IP Phone konfigureras normalt för etablering första gången telefonen ansluter till nätverket. Telefonen etableras även enligt de schemalagda intervall som definieras när tjänsteleverantören eller en mervärdesåterförsäljare (VAR) företablerar (konfigurerar) telefonen. Tjänsteleverantörer kan tillåta att

mervärdesåterförsäljare eller avancerade användare etablerar telefonen manuellt via telefonens knappsats. Du kan också konfigurera etablering via telefonens webbaserade användargränssnitt.

Gå till **Status** > **Telefonstatus** > **Etablering** från användargränssnittet på telefonens LCD-skärm eller till Etableringsstatus på fliken **Status** i det webbaserade konfigurationsverktyget.

Relaterade ämnen

Etablera en telefon manuellt från knappsatsen, på sidan 9

Etablera en telefon manuellt från knappsatsen

Arbetsordning

Steg 1 Tryck på **Program**  .

Steg 2 Välj **Enhetsadministration** > **Profilregel**.

Steg 3 Ange profilregeln i följande format:

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

Till exempel:

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

Om inget protokoll anges, antas TFTP. Om inget servernamn anges används värden som begär webbadressen som servernamn. Om ingen port anges används standardporten (69 för TFTP, 80 för HTTP eller 443 för HTTPS).

Steg 4 Tryck på **Återsynka**.

Relaterade ämnen

Telefonenetableringsmetoder, på sidan 8

Utdelning av firmware

PFS (Peer Firmware Sharing) är en distributionsmodell för fast programvara som gör att en Cisco IP Phone kan hitta andra telefoner av samma modell eller serie i subnätet och dela uppdaterade filer av den fasta programvaran när du vill uppgradera flera telefoner på samma gång. PFS använder Cisco Peer-to-Peer Distribution Protocol (CPPDP) som är ett tillverkarspecifikt Cisco-protokoll. Med CPPDP bildar alla enheter i samma subnät en peer-to-peer-hierarki där den fasta programvaran eller de andra filerna kopieras från peer-enheter till närliggande enheter. För att optimera uppgraderingen av den fasta programvaran hämtar en rottelefon avbildningen av den fasta programvaran från laddningsservern och överför sedan den fasta programvaran till andra telefoner i subnätet med hjälp av TCP-anslutningar.

Peer-delning av firmware:

- Begränsar trängsel vid TFTP-överföringar till centraliserade fjärrladdningsservrar.
- Eliminerar behovet av att manuellt kontrollera firmwareuppgraderingar.
- Minskar telefondriftstopp vid uppgraderingar när ett stort antal telefoner återställs samtidigt.

OBS!

- Peer-delning av fast programvara fungerar inte om flera telefoner har konfigurerats att uppgraderas på samma gång. När NOTIFY skickas med Event:resync initieras en omsynkronisering på telefonen. Exempel på en XML-sträng som kan innehålla konfigurationer som initierar uppgraderingen:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- När du konfigurerar PFS-loggservern (Peer Firmware Sharing) till en IP-adress och port skickas de PFS-specifika loggarna till den servern som UDP-meddelanden. Den här inställningen måste göras på varje telefon. Sedan kan du använda loggmeddelandena när du felsöker problem relaterade till PFS.

Peer_Firmware_Sharing_Log_Server anger värdnamnet och porten för den UDP-baserade syslog-fjärrservern. Portens standard-syslog är 514.

Till exempel:

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

Om du vill använda den här funktionen aktiverar du PFS på telefonerna.

Kringgå skärmen Ange lösenord

Du kan kringgå skärmen **Ange lösenord** första gången telefonen startar eller efter en fabriksåterställning baserat på dessa etableringsåtgärder:

- DHCP-konfiguration
- EDOS-konfiguration
- Konfiguration av användarlösenord via telefonens XML-konfigurationsfil.

Tabell 1. Etableringsåtgärder som avgör om skärmen Ange lösenord visas eller inte

DHCP har konfigurerats	EDOS har konfigurerats	Användarlösenord har konfigurerats	Kringgå skärmen Ange lösenord
Ja	Ej tillg.	Ja	Ja
Ja	Ej tillg.	Nej	**Nej**
Nej	Ja	Ja	Ja
Nej	Ja	Nej	**Nej**
Nej	Nej	Ej tillg.	**Nej**

Arbetsordning

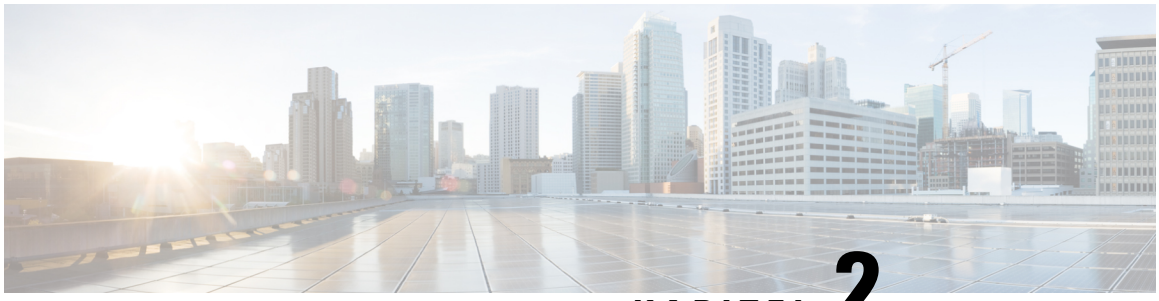
Steg 1 Redigera telefonens `config.xml`-fil i en XML- eller textredigerare.

Steg 2 Infoga taggen **<User_Password>** med något av följande alternativ.

- **Inget lösenord (start- och sluttagg)** – **<User_Password></User_Password>**

- **Lösenordsvärde (4 till 127 tecken)** – **`<User_Password ua="rw">abc123</User_Password>`**
- **Inget lösenord (endast starttagg)** – **`<User_Password />`**

Steg 3 Spara ändringarna i `config.xml`-filen.



KAPITEL 2

Etableringsskript

Etableringsskript

Telefonen stöder konfiguration i XML-format.

Detaljerad information om telefonen finns i administrationshandboken för din enhet. I varje handbok beskrivs de parametrar som kan konfigureras via administrationswebbservern.

Format för konfigurationsprofilen

Konfigurationsprofilen definierar parametervärdena för telefonen.

XML-formatet för konfigurationsprofiler använder XML-standardverktyg för att kompilera parametrarna och värdena.

OBS! Endast UTF-8 teckenuppsättningen stöds. Om du ändrar profilen i en redigerare är det viktigt att du inte ändrar kodningsformatet. I så fall kan telefonen inte identifiera filen.

Varje telefon har en egen funktionsuppsättning och därför även en egen uppsättning parametrar.

Profil i XML-format

En profil med öppet format är en textfil med XML-liknande syntax i en elementhierarki med elementattribut och elementvärden. Med det här formatet kan du använda standardverktyg för att skapa konfigurationsfilen. En konfigurationsfil i det här formatet kan skickas från etableringsservern till telefonen under en omsynkronisering. Filen kan skickas utan kompilering som ett binärt objekt.

Telefonen stöder konfigurationsformat som genereras av standardverktyg. Den här funktionen underlättar utvecklingen av program för backend-etableringsservrar som genererar konfigurationsprofiler från befintliga databaser.

För att skydda konfidentiell information i konfigurationsprofilen skickar etableringsservern den här typen av fil till telefonen via en TLS-skyddad kanal. Filen kan också komprimeras med hjälp av gzip-komprimeringsalgoritmen (RFC1951).

Filen kan krypteras med någon av dessa krypteringsmetoder:

- AES-256-CBC kryptering
- RFC-8188 baserat HTTP innehåll kryptering med AES-128-GCM chiffrering

Exempel: Öppet 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>
```

Elementtaggen <flat-profile> innesluter alla parameterelement som kan identifieras av telefonen.

Relaterade ämnen

Komprimering och kryptering av öppen profil (XML), på sidan 17

Komponenter i konfigurationsfilen

En konfigurationsfil kan innehålla följande komponenter:

- Elementtaggar
- Attribut
- Parametrar
- Formateringsfunktioner
- XML-kommentarer

Taggegenskaper för element

- XML-etableringsformatet och webbanvändargränssnittet stöder konfiguration av samma inställningar. XML-taggnamnet och fältnamnen i webbanvändargränssnittet liknar varandra, men varierar på grund av begränsningarna i XML-elementnamn. Till exempel understreck (_) i stället för " ".
- Telefonen identifierar element med rätt parameternamn som är inkapslade i det speciella <flat-profile>-elementet.
- Elementnamn omges av vinkelparenteser.
- De flesta elementnamnen liknar fältnamnen på administrationswebbsidorna för en enheten, med följande variationer:

- Elementnamn får inte innehålla blanksteg eller specialtecken. För att härleda elementnamnet från fältnamnet på administrationswebbsidorna ersätter du alla blanksteg eller specialtecknen `[`, `]`, `(`, `)` eller `/` med ett understreck.

  Exempel: Elementet <Resync_On_Reset> representerar fältet **Resync On Reset**.

- Alla elementnamn måste vara unika. På administrationswebbsidorna kan samma fält visas på flera webbsidor, till exempel på sidorna Linje, Användare och Anknytning. Lägg till `[n]` i elementnamnet för att indikera numret som visas på sidfliken.

  Exempel: Elementet <Dial_Plan_1_> representerar **uppringningsplanen** (Dial Plan) för linje 1.

- Varje inledande elementtagg måste ha en matchande avslutande elementtagg. Till exempel:

```
<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>
```

- Elementtaggar är skiftlägeskänsliga.
- Tomma elementtaggar tillåts och tolkas som att värdet ska vara tomt. Infoga den inledande elementtaggen utan en matchande elementtagg och infoga ett blanksteg och ett snedstreck innan du stänger vinkelparentesen (>). I det här exemplet är profilregel B tom:

```
<Profile_Rule_B />
```

- En tom elementtagg kan användas för att förhindra överskrivning av värden som anges av användaren under en omsynkronisering. I följande exempel förblir användarens snabbvalsinställningar oförändrade:

```
<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>
```

- Använd ett tomt värde om du vill att den associerade parametern ska vara en tom sträng. Infoga ett inledande och ett avslutande element utan något värde mellan dem. I följande exempel är parametern GPP_A en tom sträng.

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

- Elementnamn som inte kan identifieras ignoreras.

Relaterade ämnen

Åtkomstkontroll för konfigurationsinställningar, på sidan 7

Attribut för användaråtkomst

Attributkontrollerna för användaråtkomst (**ua**) kan användas för att ändra användarkontots åtkomst. Om **ua**-attributet inte anges bevaras den befintliga inställningen för användaråtkomst. Det här attributet påverkar inte åtkomst från administratörskontot.

Attributet **ua** måste ha något av följande värden:

- na – ingen åtkomst
- ro – skrivskyddad
- rw – läs-/skrivbehörighet

Följande exempel illustrerar **ua**-attributet:

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

ua-alternativets värde måste omges av dubbla citattecken.

Åtkomstkontroll

Om parametern <Phone-UI-User-Mode> har aktiverats används attributet för användaråtkomst för relevanta parametrar när en menypost visas i det grafiska gränssnittet på telefonen.

För menyposter som är associerade med en enda konfigurationsparameter:

- Om parametern etableras med attributet ”ua = na” (”ua” står för ”användaråtkomst”) försvinner posten.
- Om parametern etableras med attributet ”ua = ro” skrivskyddas posten, så att den inte kan redigeras.

För menyposter som är associerade med flera konfigurationsparametrar:

- Om någon av parametrarna etableras med attributet ”ua = na” försvinner posterna.

Relaterade ämnen

Åtkomstkontroll för konfigurationsinställningar, på sidan 7

Parameteregenskaper

Dessa egenskaper gäller för följande parametrar:

- Parametrar som inte anges i en profil lämnas oförändrade på telefonen.
- Okända parametrar ignoreras.
- Om profilen med öppet format innehåller flera förekomster av samma parametertagg åsidosätter den sista förekomsten tidigare förekomster. För att undvika oavsiktlig åsidosättning av en parameters konfigurationsvärden rekommenderar vi att högst en instans av en parameter anges i en profil.
- Den sista profilen som bearbetas prioriteras. Om flera profiler definierar samma konfigurationsparameter prioriteras den sista profilens värde.

Strängformat

Följande gäller för formateringen av strängarna:

- Kommentarer som följer XML-standardsyntax tillåts.

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

- Inledande och avslutande blanksteg tillåts för att underlätta läsningen, men tas bort från parametervärdet.
- Nya rader inuti ett värde omvandlas till blanksteg.
- Ett XML-sidhuvud med format `<? ?>` tillåts, men ignoreras av telefonen.
- Om du vill infoga specialtecken använder du vanliga escape-tecken för XML (se tabellen nedan).

Specialtecken	XML-escape-sekvens
& (et-tecken)	&
< (mindre än)	<
> (större än)	>
’ (apostrof)	'
” (dubbelt citattecken)	"

I följande exempel används escape-tecken för att representera symbolerna för större än och mindre än, som krävs i en regel för en uppringningsplan. I det här exemplet definieras en uppringningsplan för en hotline som konfigurerar parametern <Dial_Plan_1_> (**Admininloggning** > **Avancerat** > **Röst** > **Ankn (n)**) som (S0 <:18005551212>).

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

- Numeriska escape-tecken, som använder decimala och hexadecimala värden (`&#` och `&#x`), är översatta.
- Telefonens fasta programvara stöder endast ASCII-tecken.

Komprimering och kryptering av öppen profil (XML)

Du kan komprimera den öppna konfigurationsprofilen för att minska nätverksbelastningen på etableringsservern. Profilen kan också krypteras för att skydda hemlig information. Komprimering är inte obligatoriskt, men måste ske före kryptering.

Relaterade ämnen

Format för konfigurationsprofilen, på sidan 13

Komprimering av öppen profil

Den komprimeringsmetod som stöds är gzip-komprimeringsalgoritmen (RFC1951). Verktyget gzip och komprimeringsbiblioteket som implementerar samma algoritm (zlib) är tillgängliga från webbplatser på Internet.

För att kunna identifiera komprimering förväntar sig telefonen att den komprimerade filen innehåller ett huvud som är kompatibelt med gzip. Huvudet genereras via ett anrop till gzip-verktyget i den ursprungliga öppna profilen. Telefonen kontrollerar filhuvudet som hämtats för att fastställa filformatet.

Om till exempel `profil.xml` är en giltig profil, så accepteras även filen `profil.xml.gz`. Den här profiltypen kan genereras med något av följande kommandon:

- `>gzip profil.xml`

  Ersätter den ursprungliga filen med den komprimerade filen.

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

  Den ursprungliga filen lämnas kvar och en ny komprimerad fil genereras.

En genomgång om komprimering finns i avsnittet Komprimera en öppen profil med Gzip, på sidan 60.

Relaterade ämnen

Komprimera en öppen profil med Gzip, på sidan 60

Kryptering av öppen profil

Kryptering med symmetriska nycklar kan användas för att kryptera en öppen konfigurationsprofil oavsett om filen är komprimerad eller inte. Komprimering, om tillämpad, måste tillämpas före kryptering.

Etableringsservern använder HTTPS för att hantera den första etableringen av telefonen efter distributionen. Konfigurationsprofiler offline som krypterats i förväg tillåter användning av HTTP för att återsynka profiler senare. Det här minskar belastningen på HTTPS-servern i storskaliga distributioner.

Telefonen stöder två metoder av kryptering för konfigurationsfiler:

- AES-256-CBC kryptering
- RFC 8188-baserat HTTP-innehållskryptering med AES-128-GCM chiffrering

Nyckeln eller Input Keying Material (IKM) måste ha blivit företablerad till enheten vid en tidigare tidpunkt. Initieringen (bootstrap) av den hemliga nyckeln kan utföras på ett säkert sätt med HTTPS.

Namnet för konfigurationsfilen kräver inte ett speciellt format, men ett filnamn som slutar med tillägget `.cfg` indikerar normalt att det rör sig om en konfigurationsprofil.

AES-256-CBC Kryptering

Telefonen stöder AES-256-CBC kryptering för konfigurationsfiler.

Krypteringen kan utföras med krypteringsverktyget OpenSSL, som kan hämtas från olika webbplatser på Internet. Stöd för 256-bitars AES-kryptering kan kräva omkompilering av verktyget för att aktivera AES-koden. Den fasta programvaran har testats mot openssl-0.9.7c-versionen.

Kryptera en profil med OpenSSL, på sidan 61 innehåller en genomgång om kryptering.

För en krypterad fil förväntar sig profilen att filen har samma format som det format som genereras med följande 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
```

Ett gement -k föregår den hemliga nyckeln, som kan vara en oformaterad textfras, och som används för att generera en slumpmässig 64-bitars saltsträng. Med hemligheten som anges av argumentet -k hämtar krypteringsverktyget en slumpmässig första 128-bitarsvektor och själva 256-bitarskrypteringsnyckeln.

När den här formen av kryptering används med en konfigurationsprofil måste telefonen informeras om den hemliga nyckelns värde för att kunna dekryptera filen. Det här värdet anges som en kvalificerare i profil-URL:en. Syntaxen är som följer, och använder en explicit URL:

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

Det här värdet programmeras med hjälp av någon av Profile_Rule-parametrarna.

Relaterade ämnen

Kryptera en profil med OpenSSL, på sidan 61

Makroexpandering

Flera etableringsparametrar genomgår intern makroexpandering innan de utvärderas. Det här förutvärderingssteget ger större flexibilitet vid omsynkroniserings- och uppgraderingsaktiviteter på telefonen.

Följande parametergrupper genomgår makroexpandering före utvärderingen:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

Under vissa omständigheter genomgår även vissa allmänna parametrar (GPP_*) makroexpandering, vilket beskrivs i Valfria omsynkroniseringsargument, på sidan 22.

Under makroexpanderingen ersätter innehållet i de namngivna variablerna uttryck i formatet $NAME och $(NAME). Dessa variabler omfattar allmänna parametrar, flera produktidentifierare, vissa händelsetimers och värden för etableringsstatus. En fullständig lista finns i Variabler för makroexpandering, på sidan 72.

I följande exempel används uttrycket $(MAU) för att infoga MAC-adressen 000E08012345.

Administratören anger: **`$(MAU)config.cfg`**

Den resulterande makroexpanderingen för en enhet med MAC-adressen 000E08012345 är: `000E08012345config.cfg`

Om ett makronamn inte kan identifieras, sker ingen expandering. Exempelvis identifieras inte namnet STRANGE som ett giltigt makronamn, men det gör däremot MAU.

Administratören anger: **$STRANGE$MAU.cfg**

Den resulterande makroexpanderingen för en enhet med MAC-adressen 000E08012345 är: `$STRANGE000E08012345.cfg`

Makroexpandering tillämpas inte rekursivt. Exempelvis expanderas $$MAU” till $MAU” ($$ expanderas) och resulterar inte i MAC-adressen.

Innehållet i specialparametrarna, GPP_SA till och med GPP_SD, mappas till makrouttrycken $SA till och med $SD. Dessa parametrar makroexpanderas endast som argumentet för alternativen **--key** , **--uid** och **--pwd** i en omsynkroniserings-URL.

Villkorsuttryck

Villkorsuttryck kan utlösa omsynkroniseringshändelser och välja bland alternativa URL:er för omsynkroniserings- och uppgraderingsåtgärder.

Ett villkorsuttryck består av en lista med jämförelser, avgränsade med **och** operatorn. Alla jämförelser måste uppfyllas för att villkoret ska vara sant.

Varje jämförelse kan relatera till någon av följande tre typer av litteraler:

- Heltalsvärden
- Versionsnummer för program- eller maskinvara
- Strängar inom dubbla citattecken

Versionsnummer

Officiella utgåvor av programvaruversioner för multiplattformstelefoner (MPP) använder detta format, där BN = versionsnummer:

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

Jämförelsesträngen måste använda samma format. Annars returneras ett formatparsningsfel.

I programvaruversionen kan v1-v2-v3-v4 innehålla olika siffror och tecken, men strängen måste börja med en numerisk siffra. När programvaruversionen jämförs, jämförs v1-v2-v3-v4 i följd, och siffrorna längst till vänster ges företräde framför de till höger.

Om v[x] endast innehåller numeriska siffror, jämförs siffrorna. Om v[x] innehåller numeriska siffror och alfanumeriska tecken, jämförs siffrorna först och sedan tecknen i alfabetisk ordning.

Exempel på giltigt versionsnummer

sipyyyy.11-0-0MPP-BN

Däremot är 11.0.0 ett ogiltigt format.

Jämförelse

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

Strängar inom citattecken kan jämföras för att identifiera likheter eller olikheter. Heltal och versionsnummer kan även jämföras aritmetiskt. Jämförelseoperatorerna kan anges som symboler eller som akronymer. Akronymer är praktiska för att ange villkoret i en profil med öppet format.

Operatör	Alternativ syntax	Beskrivning	Gäller för heltals- och versionsoperander	Gäller för strängoperander inom citattecken
=	eq	lika med	Ja	Ja
!=	ne	inte lika med	Ja	Ja
<	lt	mindre än	Ja	Nej
<=	le	mindre än eller lika med	Ja	Nej
>	gt	större än	Ja	Nej
>=	ge	större än eller lika med	Ja	Nej
AND		och	Ja	Ja

Det är viktigt att makrovariabler omges med dubbla citattecken där en stränglitteral förväntas. Gör inte det om ett nummer eller versionsnummer förväntas.

När villkorsuttryck används med Profile_Rule*- och Upgrade_Rule-parametrar måste de inneslutas i syntaxen ”(expr)?” som i det här exemplet på en uppgraderingsregel. Kom ihåg att BN (Build Number) betyder versionsnummer.

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

Använd inte föregående syntax med parenteser för att konfigurera Resync_Trigger_*-parametrar.

URL-syntax

Använd URL-standardsyntax för att ange hur konfigurationsfiler och fast programvara ska hämtas i Profile_Rule*- respektive Upgrade_Rule-parametrar. Syntaxen ser ut så här:

`[ scheme:// ] [ server [:port]] filsökväg`

Där **`scheme`** är något av följande värden:

- tftp
- http
- https

Om **`scheme`** utelämnas används tftp. Servern kan vara ett DNS-identifierat värdnamn eller en numerisk IP-adress. Porten är UDP- eller TCP-målportnumret. Filsökvägen måste börja med rotkatalogen (/) och måste vara en absolut sökväg.

Om **`server`** saknas används tftp-servern som angetts via DHCP (alternativ 66).

OBS! Servern måste anges för uppgraderingsregler.

Om **port** saknas används standardporten för det angivna schemat. Tftp använder UDP-port 69, http använder TCP-port 80 och https använder TCP-port 443.

En filsökväg måste anges. Den måste inte nödvändigtvis referera till en statisk fil, utan kan ange dynamiskt innehåll som hämtas via CGI.

Makroexpandering används i URL:er. Följande är exempel på giltiga URL:er:

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

När du använder DHCP-alternativ 66 stöds inte tom syntax av några uppgraderingsregler. Det är bara tillämpligt för profilregel*.

RFC 8188-baserad HTTP-innehållskryptering

Telefonen stöder RFC 8188-baserat HTTP-innehållskryptering med AES-128-GCM chiffrering för konfigurationsfiler. Med den här metoden för kryptering kan alla enheter läsa sidhuvudena för HTTP-meddelandena. Dock kan endast de enheter som känner till Input Keying Material (IKM) läsa lasten. När telefonen är etablerad med IKM kan telefonen och etableringsservern utbyta konfigurationsfiler på ett säkert sätt, samtidigt som nätverkselement från tredje part tillåts använda meddelandenas sidhuvuden för analytiska syften och övervakningssyften.

Parametern för XML-konfiguration **IKM_HTTP_Encrypt_Content** innehåller IKM på telefonen. Den här parametern är inte tillgänglig på websidan för telefonadministration av säkerhetsskäl. Det är inte heller synligt i telefonens konfigurationsfil vilken du kan komma åt från telefonens IP-adress eller från telefonens konfigurationsrapporter som skickats till etableringsservern.

Om du vill använda den RFC 8188-baserade krypteringen ska du kontrollera följande:

- Förse telefonen med IKM genom att specificera IKM med XML-parametern **IKM_HTTP_Encrypt_Content** i konfigurationsfilen som skickats från etableringsservern till telefonen.
- Om den här krypteringen appliceras på konfigurationsfilerna som skickats från etableringsservern till telefonen, kan du kontrollera att HTTP-sidhuvudet för *Innehålls-Kodning* i konfigurationsfilen har ”aes128gcm”.

  I avsaknad av detta sidhuvud får metoden AES-256-CBC prioritet. Telefonen tillämpar AES-256-CBC dekryptering om en AES-256-CBC-nyckel finns i en profilregel, oavsett IKM.
- Se till att det inte finns någon specificerad AES-256-CBC-nyckel i rapportregeln om du vill att telefonen ska applicera denna kryptering till de konfigurationsrapporter som skickas till etableringsservern.

Valfria omsynkroniseringsargument

Valfria argument – **key**, **uid** och **pwd** – kan föregå URL:erna som anges i Profile_Rule*-parametrar och omges av hakparenteser.

key

Alternativet **– key** instruerar telefonen att konfigurationsfilen den tar emot från etableringsservern är krypterad med AES-256-CBC kryptering, såvida inte sidhuvudet i filen för *Innehålls-Kodning* anger ”aes128gcm” kryptering. Själva nyckeln anges som en sträng efter termen **--key**. Nyckeln kan också omslutas med dubbla citattecken (”). Telefonen använder nyckeln för att dekryptera konfigurationsfilen.

Användningsexempel

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

De valfria argumenten inom hakparenteser makroexpanderas. Specialparametrar, GPP_SA till och med GPP_SD, makroexpanderas endast till makrovariabler, $SA till och med $SD, om de används som argument till alternativet key. Se följande exempel:

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

I profiler med öppet format måste argumentet för **--key** vara samma som argumentet för alternativet **-k** som skickas till **openssl**.

uid och pwd

Alternativen **uid** och **pwd** kan användas för att definiera autentisering med användar-ID och lösenord för den angivna URL:en. De valfria argumenten inom hakparenteser makroexpanderas. Specialparametrar, GPP_SA till och med GPP_SD, makroexpanderas endast till makrovariabler, $SA till och med $SD, om de används som argument till alternativet key. Se följande exempel:

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

[--uid $SA -pwd $SB] https://etableringsserverns_url/sökväg_till_din_konfiguration/din_konfiguration.xml

expanderas till:

[--uid MyUserID -pwdMySecretPassword]
https://etableringsserverns_url/sökväg_till_din_konfiguration/din_konfiguration.xml

Koppla en profil till IP-telefonenheten

När du har skapat ett XML-konfigurationsskript måste det skickas till telefonen för att tillämpas. Du kan tillämpa konfigurationen antingen genom att hämta konfigurationsfilen till telefonen från en TFTP-, HTTP- eller HTTPS-server via en webbläsare eller genom att använda kommandoradsverktyget cURL.

Hämta konfigurationsfilen till telefonen från en TFTP-server

Följ stegen nedan för att hämta konfigurationsfilen till ett TFTP-serverprogram på datorn.

Arbetsordning

Steg 1 Anslut datorn till telefonens lokala nätverk.

Steg 2 Kör ett TFTP-serverprogram på datorn och kontrollera att konfigurationsfilen finns i TFTP-rotkatalogen.

Steg 3 Öppna en webbläsare och ange IP-adressen för telefonens lokala nätverk, datorns IP-adress, filnamnet och inloggningsuppgifterna. Använd det här formatet:

`http://<WAN_IP-adress>/admin/resync?tftp://<Datorns_IP-adress>/<filnamn>&xuser=admin&xpassword=<lösenord>`

Exempel:

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

Hämta konfigurationsfilen till telefonen med cURL

Följ stegen nedan för att hämta konfigurationen till telefonen med hjälp av cURL. Det här kommandoradsverktyget används för att överföra data med URL-syntax. Om du vill hämta cURL går du till:

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

OBS! Vi rekommenderar att du inte använder cURL för att publicera konfigurationen till telefonen eftersom användarnamnet och lösenordet kan fångas upp när du använder cURL.

Arbetsordning

Steg 1 Anslut datorn till LAN-porten på telefonen.

Steg 2 Hämta konfigurationsfilen till telefonen genom att ange följande cURL-kommando:

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

Etableringsparametrar

Det här avsnittet beskriver etableringsparametrarna ordnade i breda kategorier efter funktion:

Följande typer av etableringsparametrar är tillgängliga:

- Allmänna
- Aktivering
- Utlösare
- Konfigurerbara scheman

- Profilregler
- Uppgraderingsregel

Allmänna parametrar

De allmänna GPP_*-parametrarna (**Admininloggning** > **Avancerat** > **Röst** > **Etablering**) används som fria strängregister när du konfigurerar telefonen för interaktion med en viss etableringsserverlösning. GPP_*-parametrarna är tomma som standard. De kan konfigureras för att innehålla olika värden, bland annat följande:

- Krypteringsnycklar
- Webbadresser
- Statusinformation för multietablering
- Postbegärandemallar
- Mappningar mellan parameternamn och alias
- Partiella strängvärden som så småningom kopplas ihop till kompletta parametervärden.

GPP_*-parametrarna stöder makroexpandering inuti andra etableringsparametrar. För detta ändamål räcker det att använda makronamn med en versal bokstav (A till P) för att identifiera innehållet i GPP_A till och med GPP_P. Makronamnen med två versala bokstäver, SA till och med SD, identifierar också GPP_SA till och med GPP_SD i särskilda fall när de används som argument för följande URL-alternativ:

key, **uid** och **pwd**

Dessa parametrar kan användas som variabler i etablerings- och uppgraderingsregler. Du kan refererar till dem genom att lägga till ett ”$”-tecken först i variabelnamnet, t.ex. $GPP_A.

Använda allmänna parametrar

Om GPP_A exempelvis innehåller strängen ABC, och GPP_B innehåller 123, så makroexpanderas uttrycket AB till ABC123.

Innan du börjar

Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Arbetsordning

Steg 1 Välj **Röst** > **Etablering**.

Steg 2 Gå till avsnittet om **allmänna parametrar**.

Steg 3 Ange giltiga värden i fälten, GPP A till och med GPP P.

Steg 4 Klicka på **Verkställ alla ändringar**.

Aktivering

Parametrarna Provision_Enable och Upgrade_Enable styr alla åtgärder relaterade till profilomsynkronisering och uppgradering av fast programvara. Dessa parametrar styr omsynkroniseringar och uppgraderingar oberoende av varandra. Dessa parametrar styr även kommandon för omsynkroniserings- och uppgraderings-URL:er som skickas via administrationswebbservern. Standardinställningen för båda parametrarna är **Yes**.

Parametern Resync_From_SIP kontrollerar åtgärder relaterade till omsynkroniseringsförfrågningar. En SIP NOTIFY-händelse skickas från tjänsteleverantörens proxyserver till telefonen. Om den är aktiverad kan proxyservern begära en omsynkronisering. För att göra det skickar proxyservern ett SIP NOTIFY-meddelande som innehåller Event: resync-huvudet till enheten.

Enheten svarar på begäran med ett 401-svar (auktoriseringen avvisas för angivna inloggningsuppgifter). Enheten förväntar sig en autentiserad efterföljande begäran innan den godkänner omsynkroniseringsbegäran från proxyservern. Event: reboot_now- och Event: restart_now-huvudena utför kalla respektive varma omstarter, vilket också kräver autentiseringssvar.

De två återstående enable-parametrarna är Resync_On_Reset och Resync_After_Upgrade_Attempt. Dessa parametrar avgör om enheten utför en omsynkronisering efter en omstart av programvara och efter varje uppgraderingsförsök.

När Resync_On_Reset används lägger enheten till en slumpmässig fördröjning efter startsekvensen innan återställningen utförs. Fördröjningen är en slumpmässig tid upp till värdet som anges i Resync_Random_Delay (i sekunder). I en grupp med telefoner som startas samtidigt fördelar fördröjningen starttiderna för omsynkroniseringsförfrågningarna från varje enhet. Denna funktion kan vara bra i ett stort bostadsområde om det inträffar lokalt strömavbrott.

Utlösare

Telefonen stöder omsynkronisering vid specifika intervall eller vid en viss tid.

Omsynkronisering vid specifika intervall

Telefonen är utformad att med jämna mellanrum synkronisera med etableringsservern. Omsynkroniseringsintervallet konfigureras i Resync_Periodic (sekunder). Om det här värdet lämnas tomt synkroniseras inte enheten regelbundet.

Omsynkronisering sker typiskt när linjer är inaktiv. Om en röstlinje är aktiv när en omsynkronisering ska utföras, skjuter telefonen upp omsynkroniseringen tills linjen är ledig igen. En omsynkronisering kan resultera i att konfigurationsparametervärden ändras.

En omsynkronisering kan misslyckas om telefonen inte kan hämta en profil från servern, om den nedladdade filen är skadad eller på grund av ett internt fel. Enheten försöker synkronisera igen efter det antal sekunder som anges i Resync_Error_Retry_Delay (sekunder). Om Resync_Error_Retry_Delay har angetts till 0 försöker enheten inte synkronisera igen efter ett misslyckat omsynkroniseringsförsök.

Om en uppgradering misslyckas görs ett nytt försök efter det antal sekunder som anges i Upgrade_Error_Retry_Delay.

Det finns två parametrar som kan konfigureras för villkorsstyrd omsynkronisering: Resync_Trigger_1 och Resync_Trigger_2. Båda parametrarna kan programmeras med ett villkorsuttryck som makroexpanderas. När omsynkroniseringsintervallet går ut (tidpunkten för nästa omsynkronisering) förhindrar utlösarna, om sådana har angetts, omsynkroniseringen om inte en eller flera utlösare utvärderas som sanna.

Följande exempelvillkor utlöser en omsynkronisering. I exemplet har det senaste telefonuppgraderingsförsöket pågått i mer än 5 minuter (300 sekunder), och det har gått minst 10 minuter (600 sekunder) sedan det senaste omsynkroniseringsförsöket.

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

Omsynkronisering vid en specifik tid

Parametern Resync_At gör att telefonen kan synkronisera vid en specifik tidpunkt. Den här parametern använder 24-timmarsformat (hhmm) för att ange tiden.

Parametern Resync_At_Random_Delay gör att telefonen kan synkronisera vid en ospecificerad tidfördröjning. I den här parametern används ett positivt heltal för att ange tiden.

Överbelastning av servern på grund av omsynkroniseringsförfrågningar från flera telefoner som konfigurerats att synkronisera samtidigt bör undvikas. För att göra det utlöser telefonen omsynkroniseringen upp till 10 minuter efter den angivna tiden.

Om du till exempel ställer in omsynkroniseringstiden på 1000 (dvs. kl. 10) utlöser telefonen omsynkroniseringen någon gång mellan 10:00 och 10:10.

Den här funktionen är inaktiverad som standard. Om parametern Resync_At har etablerats, ignoreras Resync_Periodic-parametern.

Konfigurerbara scheman

Du kan konfigurera scheman för regelbundna omsynkroniseringar och du kan ange intervall för omförsök vid omsynkroniserings- och uppdateringsfel genom att använda följande etableringsparametrar:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Varje parameter stöder ett enskilt fördröjningsvärde (sekunder). Den nya utökade syntaxen stöder en kommateckenavgränsad lista med flera efterföljande fördröjningselement. Det sista elementet i sekvensen upprepas implicit för alltid.

Om du vill kan du infoga ett plustecken för att ange ett till numeriskt värde som lägger till en extra slumpmässig fördröjning.

Exempel 1

I detta exempel synkroniseras telefonen regelbundet varannan timme. Om det uppstår ett omsynkroniseringsfel gör enheten nya försök enligt följande intervall: 30 minuter, 1 timme, 2 timmar, 4 timmar. Enheten fortsätter att försöka i 4-timmarsintervall tills omsynkroniseringen lyckas.

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

Exempel 2

I det här exemplet synkroniseras enheten regelbundet varje timme (plus en extra slumpmässig fördröjning på upp till 10 minuter). Om en omsynkronisering misslyckas gör enheten nya försök enligt följande intervall: 30 minuter (plus upp till 5 minuter). 1 timme (plus upp till 10 minuter), 2 timmar (plus upp till 15 minuter). Enheten fortsätter att försöka i 2-timmarsintervall (plus upp till 15 minuter) tills omsynkroniseringen lyckas.

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

Exempel 3

I det här exemplet, om en fjärruppgradering misslyckas, så gör enheten ett nytt uppgraderingsförsök 30 minuter senare, och sedan efter 1 timme och därefter efter 2 timmar. Om uppgraderingen fortfarande misslyckas gör enheten nya uppgraderingsförsök var fjärde till var femte timme tills uppgraderingen lyckas.

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

Profilregler

Telefonen tillhandahåller flera profilparametrar för fjärrkonfiguration (Profile_Rule*). Det betyder att varje omsynkronisering kan hämta flera filer som hanteras av olika servrar.

I det enklaste scenariot synkroniseras enheten regelbundet mot en profil på en central server, som uppdaterar alla relevanta interna parametrar. Alternativt kan profilen delas upp mellan olika filer. En fil är gemensam för alla telefoner i en distribution. En separat, unik fil tillhandahålls för varje konto. Krypteringsnycklar och certifikatinformation kan tillhandahållas av en annan profil, som lagras på en separat server.

När det är dags för en omsynkronisering utvärderar telefonen de fyra Profile_Rule*-parametrarna i ordning:

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

Varje utvärdering kan resultera i att en profil hämtas från en fjärransluten etableringsserver, och kan leda till att vissa interna parametrar uppdateras. Om en utvärdering misslyckas avbryts omsynkroniseringssekvensen och ett nytt försök görs från början baserat på parametern Resync_Error_Retry_Delay (sekunder). Om alla utvärderingar lyckas väntar enheten det antal sekunder som anges i parametern Resync_Periodic och utför sedan en till omsynkronisering.

Innehållet i varje Profile_Rule*-parameter består av en uppsättning alternativ. Alternativen avgränsas med ett |-tecken (lodrätt streck). Varje alternativ består av ett villkorsuttryck, ett tilldelningsuttryck, en profil-URL och eventuella associerade URL-alternativ. Alla dessa komponenter är valfria inom varje alternativ. Följande är de giltiga kombinationerna, och den ordning som de måste anges i, om de används:

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

Inom varje Profile_Rule*-parameter måste alla alternativ utom det sista ange ett villkorsuttryck. Det här uttrycket utvärderas och bearbetas på följande sätt:

1. Villkoren utvärderas från vänster till höger tills ett villkor hittas som utvärderas som sant (eller tills ett alternativ utan villkorsuttryck hittas).
2. Associerade tilldelningsuttryck utvärderas, om sådana finns.
3. Om en URL anges som en del av alternativet görs ett försök att hämta profilen som finns på den angivna URL:en. Systemet försöker uppdatera de interna parametrarna i enlighet.

Om alla alternativ har villkorsuttryck och inget utvärderas som sant (eller om hela profilregeln är tom) ignoreras hela Profile_Rule*-parametern. Nästa profilregelparameter i sekvensen utvärderas.

Exempel 1

Det här exemplet synkroniserar ovillkorligt till profilen på den angivna URL:en och utför en HTTP GET-begäran till den fjärranslutna etableringsservern:

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

Exempel 2

I det här exemplet synkroniserar enheten till två olika URL:er, beroende på registreringsstatusen för linje 1. Om registreringen har gått förlorad kör enheten en HTTP POST-begäran till ett CGI-skript. Enheten skickar innehållet i den makroexpanderade GPP_A-parametern, som kan ge ytterligare information om enhetens status:

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

Exempel 3

I det här exemplet synkroniserar enheten om till samma server. Enheten tillhandahåller ytterligare information om ett certifikat inte finns installerat på enheten (för äldre enheter före version 2.0):

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

Exempel 4

I det här exemplet är linje 1 inaktiverad tills GPP_A anges till Provisioned via den första URL:en. Sedan synkroniserar enheten till den andra URL:en:

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

Exempel 5

I det här exemplet förväntas profilen som servern returnerar innehålla XML-elementtaggar. Dessa taggar måste mappas om till rätt parameternamn baserat på aliasmappningen i GPP_B:

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

En omsynkronisering anses normalt misslyckad om en begärd profil inte tas emot från servern. Parametern Resync_Fails_On_FNF kan åsidosätta detta standardbeteende. Om Resync_Fails_On_FNF har värdet No accepterar enheten ett ”file-not-found”-svar från servern som en lyckad omsynkronisering. Standardvärdet för Resync_Fails_On_FNF är Yes.

Uppgraderingsregel

Uppgraderingsregeln uppmanar enheten att aktivera en ny inläsning och anger var den finns, om det behövs. Om inläsningsfilen redan finns på enheten, försöker enheten inte hämta den. Inläsningsplatsens giltighet har därför ingen betydelse om inläsningen finns i den inaktiva partitionen.

Upgrade_Rule anger att fast programvara, om den skiljer sig från den befintliga, ska hämtas och användas om åtgärden inte begränsas av ett villkorsuttryck eller om Upgrade_Enable är inställt på **Nej**.

Telefonen tillhandahåller en konfigurerbar parameter för fjärruppgradering, Upgrade_Rule. Den här parametern stöder ungefär samma syntax som parametrarna för profilregeln. URL-alternativ stöds inte för uppgraderingar, men villkorsuttryck och tilldelningsuttryck kan användas. Om villkorsuttryck används kan flera alternativ, avgränsade med |-tecknet, anges i parametern. Syntaxen för respektive alternativ är som följer:

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

Som i fallet med Profile_Rule*-parametrar utvärderar Upgrade_Rule-parametern varje alternativ tills ett villkorsuttryck uppfylls eller tills ett alternativet utan villkorsuttryck hittas. Associerade tilldelningsuttryck utvärderas om sådana finns. Sedan görs ett försök att uppgradera till den angivna URL:en.

Om Upgrade_Rule innehåller en URL utan något villkorsuttryck, uppgraderar enheten till den avbildning av den fasta programvaran som URL:en anger. Efter makroexpandering och utvärdering av regeln försöker enheten inte att uppgradera igen förrän regeln ändras eller kombinationen av schema + server + port + filsökväg ändras.

När enheten försöker uppgradera den fasta programvaran inaktiverar den ljudet i början av processen och startar om i slutet av processen. Enheten startar endast automatiska uppgraderingar baserat på innehållet i Upgrade_Rule om alla röstlinjer är inaktiva (lediga).

Till exempel,

- För Cisco IP 6800-serien:

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

  where BN==Build Number
  ```

I det här exemplet uppgraderar Upgrade_Rule den fasta programvaran till avbildningen som finns på den angivna URL:en.

Här är ett till exempel för 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
```

Det här exemplet uppmanar enheten att läsa in en av två avbildningar, baserat på innehållet i en allmän parameter, GPP_F.

Enheten kan framtvinga en nedgraderingsgräns vad gäller den fasta programvarans revisionsnummer, vilket kan vara ett användbart anpassningsalternativ. Om ett giltigt revisionsnummer för den fasta programvaran har konfigurerats i parametern Downgrade_Rev_Limit, avvisar enheten uppgraderingsförsök för versioner av den fasta programvaran som är äldre än den angivna gränsen.

Datatyper

Följande datatyper används med konfigurationsprofilparametrar:

- {a, b, c, ...} – Val mellan a, b, c ...
- Bool – Ett booleskt värde, antingen ”yes” eller ”no”.
- CadScript – Ett miniskript som anger kadensparametrarna för en signal. Upp till 127 tecken.

  Syntax: $S_1[;S_2]$, där:

  - $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ och kallas för ett avsnitt.
  - $on_{i,j}$ och $off_{i,j}$ är on/off-varaktigheten i sekunder för ett *segment*. i = 1 eller 2, och j = 1 till 6.
  - D_i är avsnittets totala varaktighet i sekunder.

  Alla varaktigheter kan ha upp till tre decimaler för en precision på 1 ms. Jokertecknet ”*” representerar en oändlig varaktighet. Segmenten i ett avsnitt körs i ordning och upprepas tills värdet för den totala varaktigheten nås.

  Exempel 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
```

  Exempel 2 – Olika ringsignaler (kort, kort, kort, lång):

```
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 – Skriptsyntax som används för att ange uppringningsplaner för linje 1 och linje 2.
- Float <n> – Ett flyttalsvärde med upp till n decimaler.
- FQDN – Fullständigt kvalificerat domännamn. Det kan innehålla upp till 63 tecken. Några exempel är:
  - sip.Cisco.com:5060 eller 109.12.14.12:12345
  - sip.Cisco.com eller 109.12.14.12
- FreqScript – Ett miniskript som anger parametrarna för frekvens och nivå för en ton. Innehåller upp till 127 tecken.

  Syntax: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, där:
  - F_1–F_6 är frekvensen i Hz (endast osignerade heltal).
  - L_1–L_6 är motsvarande nivåer i dBm (med upp till en decimal).

  Blanksteg före och efter kommatecknet är tillåtet men rekommenderas inte.

  Exempel 1 – Signal för samtal väntar:

```
440@-10

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

  Exempel 2 – Kopplingston:

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

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

- IP – Giltig IPv4-adress i formatet x.x.x.x, där x är ett värde mellan 0 och 255. Exempel: 10.1.2.100.
- UserID – Användar-ID:t så som det visas i en URL. Kan innehålla upp till 63 tecken.
- Phone – En telefonnummersträng, till exempel 14081234567, *69, *72 eller 345678, eller en allmän URL, till exempel 1234@10.10.10.100:5068 eller jsmith@Cisco.com. Strängen kan innehålla upp till 39 tecken.
- PhTmplt – En telefonnummermall. Varje mall kan innehålla ett eller flera mönster som avgränsas med komma (,). Blanksteg i början av varje mönster ignoreras. ”?” och ”*” representerar jokertecken. Använd %xx för att representera litteraler. Exempelvis representerar %2a *. Mallen kan innehålla upp till 39 tecken. Exempel: “1408*, 1510*”, “1408123???, 555?1.”.
- Port – TCP/UDP-portnummer (0-65535). Det kan anges i decimalformat eller i hexadecimalt format.
- ProvisioningRuleSyntax – Skriptsyntax som används för att definiera regler för konfigurationsomsynkronisering och uppgraderingsregler för fast programvara.
- PwrLevel – Strömnivå uttryckt i dBm med en decimal, till exempel –13.5 eller 1.5 (dBm).
- RscTmplt – En mall för statuskoder för SIP-svar, t.ex. “404, 5*”, “61?”, “407, 408, 487, 481”. Den kan innehålla upp till 39 tecken.

- Sig<n> – Signerat n-bitars värde. Den kan anges i decimalformat eller i hexadecimalt format. Negativa värden måste föregås av ett ”-”-tecken. Ett ”+”-tecken före positiva värden är valfritt.
- Stjärnkoder – Aktiveringskod för en extra tjänst, t.ex. *69. Koden kan innehålla upp till 7 tecken.
- Str<n> – En allmän sträng med upp till n icke-reserverade tecken.
- Time<n> – Tid i sekunder, med upp till n decimaler. Extra decimaler ignoreras.
- ToneScript – Ett miniskript som anger frekvens-, nivå- och kadensparametrarna för en samtalsförloppston. Skriptet kan innehålla upp till 127 tecken.

  Syntax: FreqScript;Z_1[;Z_2].

  Avsnitt Z_1 liknar avsnitt S_1 i ett CadScript, förutom att varje on/off-segment åtföljs av en parameter för frekvenskomponenter: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$ där:

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

  Om mer än en frekvenskomponent används i ett segment summeras komponenterna.

  Exempel 1 – Kopplingston:

```
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
```

  Exempel 2 – Oregelbunden ton:

```
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> – Osignerat n-bitars värde, där n = 8, 16 eller 32. Det kan anges i decimalformat eller i hexadecimalt format, t.ex. 12 eller 0x18, så länge värdet får plats i n bitar.

OBS! Ha följande i åtanke:

- <Par Name> representerar namnet på en konfigurationsparameter. I en profil skapas den associerade taggen genom att blanksteget ersätts med ett understreck (”_”), t.ex. **Par_Name**.
- Ett tomt standardvärdefält innebär en tom sträng, < “” >.
- Telefonen fortsätter att använda de senaste konfigurerade värdena för taggar som inte finns i en viss profil.
- Mallar jämförs i den angivna ordningen. Den första, *inte den närmaste*, matchningen väljs. Parameternamnet måste matcha exakt.
- Om flera definitioner för en parameter anges i en profil, används den sista av dessa definitioner i filen på telefonen.
- En parameterspecifikation med ett tomt parametervärde återställer parametern till dess standardvärde. Om du i stället vill ange en tom sträng, använder du den tomma strängen ”” som parametervärdet.

Profiluppdateringar och uppgraderingar av fast programvara

Telefonen stöder säker fjärrbaserad etablering (konfiguration) och uppgradering av den fasta programvaran. En icke-etablerad telefon kan ta emot en krypterade profil som är avsedd för enheten. En säker förstagångsetablering som använder SSL-funktioner gör att telefonen inte kräver en explicit nyckel.

Användaren behöver varken starta eller slutföra en profiluppdatering eller en uppgradering av den fasta programvaran. Detsamma gäller om mellanliggande uppgraderingar krävs för att uppnå en framtida uppgraderingsstatus från en äldre version. Profilomsynkroniseringsförsök görs endast när telefonen är inaktiv eftersom omsynkroniseringar kan utlösa en omstart av programvaran och koppla från pågående samtal.

Allmänna parametrar hanterar etableringsprocessen. Varje telefon kan konfigureras att regelbundet kontakta en normal etableringsserver (NPS). Kommunikation med den normala etableringsservern kräver inte användning av ett säkert protokoll eftersom den uppdaterade profilen krypteras med en delad hemlig nyckel. NPS-servern kan vara en vanlig TFTP-, HTTP- eller HTTPS-server med klientcertifikat.

Administratören kan uppgradera, starta om eller synkronisera om telefoner med hjälp av telefonens webbanvändargränssnitt. Administratören kan även utföra dessa uppgifter med hjälp av ett SIP-meddelande.

Konfigurationsprofiler genereras med hjälp av vanliga verktyg med öppen källkod som integrerar med tjänsteleverantörens etableringssystem.

Relaterade ämnen

Tillåta och konfigurera profiluppdateringar, på sidan 34

Tillåta och konfigurera profiluppdateringar

Profiluppdateringar kan tillåtas vid angivna intervall. Uppdaterade profiler skickas från en server till telefonen med hjälp av TFTP, HTTP eller HTTPS.

Innan du börjar

Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Arbetsordning

Steg 1 Välj **Röst** > **Provisionering**.
Steg 2 Gå till avsnittet **Konfigurationsprofil** och välj **Ja** i listrutan **Provision Enable**.
Steg 3 Ange parametrarna.
Steg 4 Klicka på **Verkställ alla ändringar**.

Relaterade ämnen

Profiluppdateringar och uppgraderingar av fast programvara, på sidan 34

Tillåta och konfigurera uppgraderingar av fast programvara

Uppdateringar av den fasta programvaran kan tillåtas vid angivna intervall. Uppdaterad fast programvara skickas från en server till telefonen via TFTP eller HTTP. Säkerheten är inte ett lika stort problem när det gäller uppgraderingen av fast programvara eftersom fast programvara inte innehåller personlig information.

Innan du börjar

Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Arbetsordning

Steg 1 Välj **Röst** > **Etablering**.
Steg 2 Gå till avsnittet **Uppgradera firmware** och välj **Ja** i listrutan **Upgrade Enable**.
Steg 3 Ange parametrarna.
Steg 4 Klicka på **Verkställ alla ändringar**.

Uppgradera fast programvara via TFTP, HTTP eller HTTPS

Telefonen stöder uppgraderingar med en enstaka avbildning via TFTP, HTTP eller HTTPS.

OBS! Nedgraderingar till tidigare versioner kanske inte är tillgängligt för alla enheter. Mer information finns i filen med viktig information för din telefon och din version av den fasta programvaran.

Innan du börjar

Inläsningsfilen för den fasta programvaran måste hämtas till en tillgänglig server.

Arbetsordning

Steg 1 Byt namn på avbildningen så här:

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

där:

x8xx är telefonserien, t.ex. 6841.

aa-b-c är versionsnumret, t.ex. 10-4-1

Steg 2 Använd kommandot **tar -xzvf** för att ta bort .tar-formatet.

Steg 3 Kopiera mappen till en TFTP-, HTTP- eller HTTPS-hämtningskatalog.

Steg 4 Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Steg 5 Välj **Röst** > **Provisionering**.

Steg 6 Leta upp namnet på inläsningsfilen som slutar med **.loads** och lägga till det i den giltiga URL:en.

Steg 7 Klicka på **Verkställ alla ändringar**.

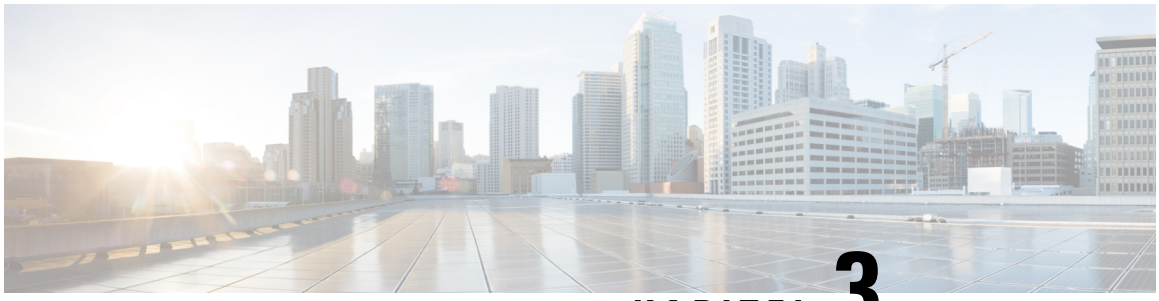
Uppgradera fast programvara med ett webbläsarkommando

Ett uppgraderingskommando som anges i webbläsarens adressfält kan användas för att uppgradera den fasta programvaran på en telefon. Telefonen uppdateras endast om den är inaktiv. Uppdateringsförsöket görs automatiskt när ett pågående samtal har avslutats.

Arbetsordning

Om du vill uppgradera telefonen med en URL i en webbläsare anger du följande kommando:

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



KAPITEL 3

Intern företablering och etableringsservrar

Intern företablering och etableringsservrar

Tjänstleverantören företablerar telefoner, förutom RC-enheter, med en profil. Företableringsprofilen kan innehålla en begränsad uppsättning parametrar som synkroniserar om telefonen. Profilen kan även innehålla en fullständig uppsättning parametrar som tillhandahålls av fjärrservern. Som standard synkroniserar telefonen när den startar och enligt intervall som konfigureras i profilen. När användaren ansluter telefonen i kundens system hämtar enheten den uppdaterade profilen och eventuella uppdateringar av den fasta programvaran.

Du kan utföra den här företablerings-, distributions- och fjärretableringsprocessen på många olika sätt.

Serverförberedelser och programverktyg

Exemplen i det här kapitlet kräver att en eller flera servrar är tillgängliga. Dessa servrar kan installeras och köras på en lokal dator:

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

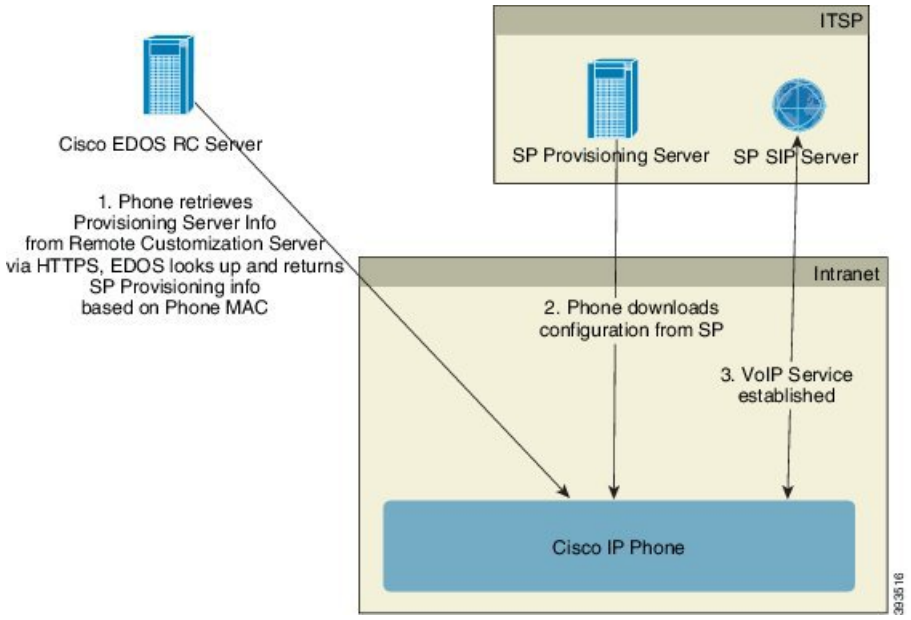
För att underlätta eventuell felsökning av serverkonfigurationen är det bra att installera klienter för varje typ av server på en separat serverdator. På så sätt påverkas inte serverns drift av interaktionen med telefonerna.

Vi rekommenderar att du installerar följande programverktyg:

- För att skapa konfigurationsprofiler installerar du komprimeringsverktyget gzip (öppen källkod).
- För profilkryptering och HTTPS-åtgärder installerar du OpenSSL-programpaketet (öppen källkod).

- För att testa den dynamiska profilgenereringen och snabbt fjärretablera via HTTPS rekommenderar vi ett skriptspråk med CGI-skriptstöd. Perl med öppen källkod är ett exempel på den här typen av skriptspråk.
- För att bekräfta att utbytet mellan etableringsservrarna och telefonerna är säkert installerar du en Ethernet-paketspårare (till exempel Ethereal/Wireshark, som du kan hämta gratis). Du kan sedan spåra interaktionen mellan telefonen och etableringsservern. Det gör du genom att köra paketspåraren på en dator som är ansluten till en växel som använder portspegling. För HTTPS-transaktioner kan du använda verktyget ssldump.

Distribution med fjärranpassning (RC)



Alla telefoner kontaktar Cisco EDOS RC-servern tills de etablerats.

I en RC-distributionsmodell köper kunden en telefon som redan har kopplats till en specifik tjänsteleverantör på Cisco EDOS RC-servern. ITSP-leverantören (Internet Telephony Service Provider) konfigurerar och underhåller en etableringsserver och registrerar sin information om etableringsservern på Cisco EDOS RC-servern.

När telefonen är påslagen och uppkopplad mot Internet är den icke-etablerade telefonens anpassningsstatus **Öppen**. Telefonen frågar den lokala DHCP-servern efter information om etableringsservern och anger telefonens anpassningsstatus. Om DHCP-frågan lyckas ändras anpassningsstatusen till **Avbruten** och inga RC-försök görs eftersom DHCP tillhandahåller den nödvändiga informationen om etableringsservern.

När en telefon ansluter till ett nätverk för första gången eller efter en fabriksåterställning, och om inga DHCP-alternativ har konfigurerats, kontaktar den en enhetsaktiveringsserver för ZTP (Zero Touch Provisioning). Nya telefoner använder ”activate.cisco.com” i stället för ”webapps.cisco.com” för etablering. Telefoner med en tidigare version av den fasta programvaran än 11.2(1) använder fortfarande webapps.cisco.com. Cisco rekommenderar att du tillåter båda domännamnen via din brandvägg.

Om DHCP-servern inte tillhandahåller information om etableringsservern frågar telefonen Cisco EDOS RC-servern och uppger sin MAC-adress, och anpassningsstatusen ändras till **Väntar**. Cisco EDOS-servern svarar med den associerade tjänsteleverantörens information om etableringsservern, inklusive etableringsserverns URL, och telefonens anpassningsstatus ändras till **Anpassad väntan**. Telefonen kör sedan

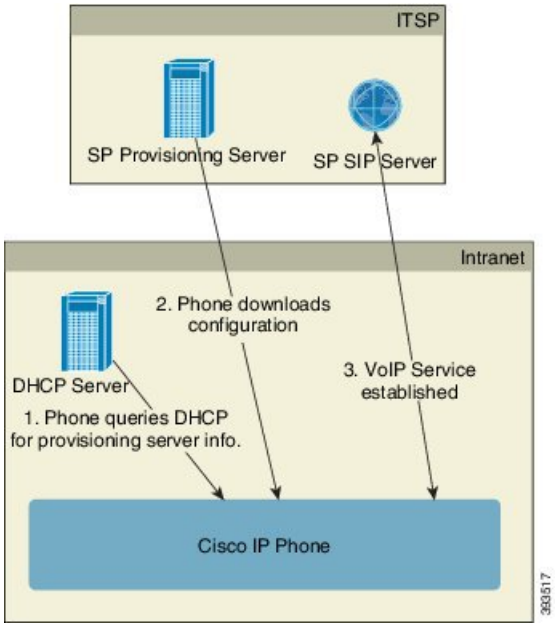
ett URL-omsynkroniseringskommando för att hämta tjänsteleverantörens konfiguration och, om det lyckas, ändras anpassningsstatusen till **Mottagen**.

Om ingen tjänsteleverantör är kopplad till telefonen på Cisco EDOS RC-servern ändras telefonens anpassningsstatus till **Ej tillgänglig**. Telefonen kan konfigureras manuellt eller så kan en association med telefonens tjänstleverantör skapas på Cisco EDOS-servern.

Om en telefon etableras via antingen LCD eller webbkonfigurationsverktyget innan anpassningsstatusen ändras till **Mottagen**, ändras anpassningsstatusen till **Avbruten** och Cisco EDOS-servern får inga fler frågor såvida inte telefonen återställs till fabriksinställningarna.

När telefonen har etablerats används inte Cisco EDOS RC-servern såvida inte telefonen återställs till fabriksinställningarna.

Intern företablering på enheter



Med Ciscos standardkonfiguration försöker telefonen automatiskt synkronisera till en profil på en TFTP-server. En hanterad DHCP-server i ett lokalt nätverk skickar informationen om profilen och TFTP-servern som konfigureras för företablering till enheten. Tjänsteleverantören ansluter varje ny telefon till det lokala nätverket. Telefonen synkroniserar automatiskt till den lokala TFTP-servern och initierar sitt interna tillstånd som en förberedelse inför distributionen. Den här företableringsprofilen innehåller vanligtvis URL:en till en fjärransluten etableringsserver. Etableringsservern ser till att enheten är uppdaterad när den har distribuerats och anslutits till kundnätverket.

Den företablerade enhetens streckkod kan skannas för att registrera enhetens MAC-adress eller serienummer innan telefonen skickas till kunden. Den här informationen kan användas för att skapa profilen som telefonen synkroniserar till.

När kunden har tagit emot telefonen ansluter han eller hon telefonen till bredbandslänken. När telefonen startas kontaktar den etableringsservern via URL:en som konfigurerades i företableringsprocessen. Telefonen kan på så sätt synkronisera om och uppdatera profilen och den fasta programvaran om det behövs.

Relaterade ämnen

Distribution inom detaljhandeln, på sidan 5
TFTP-etablering, på sidan 40

Konfiguration av etableringsserver

Det här avsnittet beskriver konfigurationskraven för etablering av en telefon med hjälp av olika servrar och olika scenarier. I exemplen i det här dokumentet installeras och körs etableringsservrarna på en lokal dator. Allmänt tillgängliga verktyg kan användas för etablering av telefonerna.

TFTP-etablering

Telefonerna stöder TFTP både för etableringsåtgärder relaterade till omsynkronisering och till uppgradering av fast programvara. HTTPS rekommenderas om enheterna fjärrdistribueras, men HTTP och TFTP kan också användas. Detta kräver i så fall att etableringsfilen skyddas genom kryptering eftersom det ökar tillförlitligheten med NAT- och routerbaserade skyddsmekanismer. TFTP är användbart vid intern företablering av ett stort antal icke-etablerade enheter.

Telefonen kan skaffa en IP-adress för TFTP-servern från DHCP-servern med hjälp av DHCP-alternativ 66. Om en Profile_Rule konfigureras med filsökvägen för TFTP-servern, hämtar enheten sin profil från TFTP-servern. Hämtningen sker när enheten startar och ansluter till ett lokalt nätverk.

Den Profile_Rule som ingår i fabrikskonfigurationen är *&PN*.cfg, där *&PN* representerar namnet på telefonmodellen.

För en CP-6841-3PCC är filnamnet exempelvis CP-6841-3PCC.cfg.

När en enhet som använder standardprofilen startar synkroniserar den till den här filen på den lokala TFTP-servern som anges i DHCP-alternativ 66. Filsökvägen är relativ till TFTP-serverns virtuella rotkatalog.

Relaterade ämnen

Intern företablering på enheter, på sidan 39

Fjärrslutpunktskontroll och NAT

Telefonen är kompatibel med NAT (Network Address Translation) för åtkomst till Internet via en router. För att öka säkerheten kanske routern försöker blockera obehöriga inkommande paket genom att implementera symmetrisk NAT, en paketfiltreringsstrategi som kraftigt begränsar vilka paket som kan komma åt det skyddade nätverket från Internet. Av den anledningen rekommenderas inte fjärretablering via TFTP.

VoIP kan endast användas med NAT om någon form av NAT-transversering tillhandahålls. Konfigurera enkel transversering av UDP via NAT (STUN, Simple Traversal of UDP through NAT). Det här alternativet kräver att användaren har:

- En dynamisk extern (offentlig) IP-adress från din tjänst
- En dator som kör STUN-serverprogramvara
- En edge-enhet med en asymmetrisk NAT-mekanism

HTTP-etablering

Telefonen fungerar som en webbläsare som begär webbsidor från en fjärrplats på Internet. Detta innebär att etableringsservern kan nås på ett tillförlitligt sätt, även om en kunds router implementerar symmetrisk NAT eller andra skyddsmekanismer. HTTP och HTTPS är mer tillförlitliga än TFTP i fjärrdistributioner, särskilt om de distribuerade enheterna är anslutna bakom privata brandväggar eller NAT-aktiverade routrar. HTTP och HTTPs används synonymt i följande beskrivningar av olika typer av begäranden.

Vid grundläggande HTTP-baserad etablering hämtas konfigurationsprofilerna med HTTP GET-metoden. Vanligtvis skapas en konfigurationsfil för varje distribuerad telefon, och filerna lagras i en HTTP-serverkatalog. När servern tar emot GET-begäran returnerar den bara filen som anges i huvudet i GET-begäran.

Konfigurationsprofilen behöver inte vara statisk, utan kan genereras dynamiskt och skapas direkt baserat på data som hämtas från en kunddatabas.

När telefonen begär en omsynkronisering kan den använda metoden HTTP POST för att begära konfigurationsdata för omsynkroniseringen. Enheten kan konfigureras att skicka status- och identifikationsinformation till servern inuti HTTP POST-begäran. Servern använder den här informationen för att generera en konfigurationsprofil, eller för att lagra statusinformationen för senare analys och spårning.

Som en del av både GET- och POST-begäranden lägger telefonen automatiskt till grundläggande identifierande information i fältet User-Agent i huvudet i begäran. Den här informationen innehåller tillverkaren, produktnamnet, den aktuella versionen av den fasta programvaran och serienumret för enheten.

Följande exempel illustrerar User-Agent-fältet i en begäran från en CP-6841-3PCC:

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

Om telefonen konfigureras att synkronisera till en konfigurationsprofil via HTTP, rekommenderar vi att HTTPS användas eller att profilen krypteras för att skydda konfidentiellt information. Krypterade profiler som telefonen hämtar via HTTP förhindrar att konfidentiell information i konfigurationsprofilen exponeras. Det här omsynkroniseringsläget innebär en mindre beräkningsbelastning på etableringsservern jämfört med HTTPS.

Telefonen kan dekryptera profiler krypterade med någon av dessa krypteringsmetoder:

- AES-256-CBC kryptering
- RFC-8188 baserad kryptering med AES-128-GCM chiffrering

OBS! Telefonerna stöder HTTP Version 1.0 och HTTP Version 1.1 samt segmentkodning om HTTP Version 1.1 används som transportprotokoll.

Hantering av HTTP-statuskoder vid omsynkronisering och uppgradering

Telefonen har stöd för HTTP-svar för fjärretablering (omsynkronisering). Telefonens beteende kategoriseras på tre sätt:

- A – Åtgärden lyckades, och värdena för ”Resync Periodic” och ”Resync Random Delay” styr efterföljande begäranden.
- B – Ett fel uppstod på grund av att filen saknas eller att profilen är skadad. Värdet för “Resync Error Retry Delay” styr efterföljande begäranden.

- C – Ett annat fel uppstod, t.ex. en ogiltig URL eller IP-adress som resulterar i ett anslutningsfel. Värdet för "Resync Error Retry Delay" styr efterföljande begäranden.

Tabell 2. Telefonbeteende för HTTP-svar

HTTP-statuskod	Beskrivning	Telefonbeteende
301: Permanent flyttad	Den här och kommande förfrågningar måste dirigeras till en ny plats.	Försök igen direkt med den nya platsen.
302: Hittades	Även kallat Tillfälligt flyttad.	Försök igen direkt med den nya platsen.
3xx	Andra 3xx-svar som inte hanteras.	C
400: Ogiltig begäran	Begäran kan inte uppfyllas på grund av felaktig syntax.	C
401: Obehörig	Enkel eller sammanfattad åtkomstautentiseringsfråga.	Försök igen direkt med giltiga inloggningsuppgifter. Högst två omförsök. Om ett fel uppstår är telefonbeteendet C.
403: Nekad	Servern vägrar att svara.	C
404: Saknas	Det gick inte att hitta den begärda resursen. Efterföljande begäranden av klienten tillåts.	B
407: Proxyautentisering krävs	Enkel eller sammanfattad åtkomstautentiseringsfråga.	Försök igen direkt med giltiga inloggningsuppgifter. Högst två omförsök. Om ett fel uppstår är telefonbeteendet C.
4xx	Andra statuskoder för klientfel bearbetas inte.	C
500: Internt serverfel	Allmänt felmeddelande.	Telefonbeteendet är C.
501: Inte implementerad	Servern känner inte igen förfrågningsmetoden, eller kan inte uppfylla begäran.	Telefonbeteendet är C.
502: Ogiltig gateway	Servern fungerar som en gateway eller proxyserver och tar emot ett ogiltigt svar från den överordnade servern.	Telefonbeteendet är C.
503: Tjänsten är inte tillgänglig	Servern är inte tillgänglig för närvarande (överbelastad eller frånkopplad för underhåll). Det här är ett tillfälligt tillstånd.	Telefonbeteendet är C.
504: Gateway-timeout	Servern fungerar som en gateway eller proxyserver och tar inte emot svar från den överordnade servern inom en bestämd tidsram.	C
5xx	Annat serverfel.	C

HTTPS-etablering

Telefonen stöder HTTPS-baserad etablering för ökad säkerhet vid hantering av fjärrdistribuerade enheter. Varje telefon har ett unikt SSL-klientcertifikat (och en associerad privat nyckel), förutom ett Sipura CA-serverrotcertifikat. Det senare gör att telefonen kan identifiera auktoriserade etableringsservrar och avvisa icke-auktoriserade servrar. Klientcertifikatet gör å andra sidan att etableringsservern kan identifiera den enskilda enhet som skickar begäran.

För att en tjänstleverantör ska kunna hantera distributioner med HTTPS måste ett servercertifikat genereras för varje etableringsserver som en telefon synkroniserar till med hjälp av HTTPS. Servercertifikatet måste signeras av Cisco Server CA-rotnyckeln, som alla distribuerade enheter har. För att erhålla ett signerat servercertifikat måste tjänstleverantören skicka en certifikatsigneringsförfrågan till Cisco, som signerar och returnerar servercertifikatet för installation på etableringsservern.

Certifikatet på etableringsservern måste innehålla fältet för vanligt namn (CN, Common Name) och det fullständigt kvalificerade domännamnet (FQDN) för värden som kör servern i ämnesfältet. Information kan läggas till efter värdens fullständigt kvalificerade domännamn, och avgränsas i så fall med ett snedstreck (/). Följande exempel illustrerar CN-poster som telefonen accepterar som giltiga:

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

Förutom att verifiera servercertifikatet kontrollerar telefonen serverns IP-adress mot en DNS-sökning av servernamnet som anges i servercertifikatet.

Skaffa ett signerat servercertifikat

Verktyget OpenSSL kan generera en certifikatsigneringsförfrågan. Följande exempel visar **openssl**-kommandot som genererar ett par med offentliga och privata nycklar med 1024-bitars RSA och en certifikatsigneringsbegäran:

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

Det här kommandot genererar serverns privata nyckel i **privkey.pem** och en associerad certifikatsigneringsbegäran i **provserver.csr**. Tjänsteleverantören håller **privkey.pem** hemlig och skickar **provserver.csr** till Cisco för signering. När filen **provserver.csr** har mottagits genererar Cisco **provserver.crt**, dvs. det signerade servercertifikatet.

Arbetsordning

Steg 1 Gå till https://software.cisco.com/software/edos/home och logga in med dina CCO-inloggningsuppgifter.

OBS! När en telefon ansluter till ett nätverk för första gången eller efter en fabriksåterställning, och inga DHCP-alternativ har konfigurerats, kontaktar den en enhetsaktiveringsserver för Zero Touch Provisioning. Nya telefoner använder ”activate.cisco.com” i stället för ”webapps.cisco.com” för etablering. Telefoner med en tidigare version av den fasta programvaran än 11.2(1) använder fortfarande ”webapps.cisco.com”. Vi rekommenderar att du tillåter båda domännamnen via din brandvägg.

Steg 2 Välj **Certifikathantering**.

Certifikatsigneringsbegäran i det föregående steget laddas upp för signering på fliken **Signera CSR** (Sign CSR).

Steg 3 Välj **SPA1xx firmware 1.3.3 och senare/SPA232D firmware 1.3.3 och senare/SPA5xx firmware 7.5.6 och senare/CP-78xx-3PCC/CP-88xx-3PCC** i listrutan **Välj produkt**.

OBS! Den här produkten omfattar Cisco IP Phone 6800-seriens multiplattformstelefoner.

Steg 4 Klicka på **Bläddra** i fältet **CSR-fil** och välj CSR-filen som ska signeras.

Steg 5 Välj krypteringsmetod:

- MD5
- SHA1
- SHA256

Cisco rekommenderar att du väljer SHA256-kryptering.

Steg 6 Välj lämplig tidslängd (t.ex. 1 år) i listrutan **Inloggningslängd** (Sign in Duration).

Steg 7 Klicka på **Signera certifikatbegäran** (Sign Certificate Request).

Steg 8 Välj något av följande alternativ för att ta emot det signerade certifikatet:

- **Ange mottagarens e-postadress** (Enter Recipient's Email Address) – Ange din e-postadress om du vill ta emot certifikatet via e-post.
- **Hämta** – Välj det här alternativet om du vill hämta det signerade certifikatet.

Steg 9 Klicka på **Skicka**.

Det signerade servercertifikatet skickas antingen via e-post till den angivna e-postadressen eller laddas ned.

CA-klientrotcertifikat för multiplattformstelefoner

Cisco erbjuder även ett klientrotcertifikat för multiplattformstelefoner till tjänstleverantörer. Det här rotcertifikatet intygar äktheten i klientcertifikatet som varje telefon har. Multiplattformstelefonerna har även stöd för signerade certifikat från tredje part, till exempel från Verisign, Cybertrust och så vidare.

Det unika klientcertifikat som varje enhet tillhandahåller under en HTTPS-session innehåller identifierande information som är inbäddad i certifikatets ämnesfält. HTTPS-servern kan göra den här informationen tillgänglig för ett CGI-skript som anropas för att hantera säkra förfrågningar. Mer specifikt innehåller certifikatets ämnesfält enhetens produktnamn (OU-element), MAC-adress (S-element) och serienummer (L-element).

I följande exempel innehåller ämnesfältet i klientcertifikat för Cisco IP Phone 6841-seriens multiplattformstelefoner följande element:

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

För att avgöra om en telefon har ett eget anpassat certifikat använder du etableringsmakrovariabeln $CCERT. Variabelns värde expanderas till Installed eller Not Installed, beroende på om ett unikt klientcertifikat finns eller inte. Om det rör sig om ett allmänt certifikat hittar du enhetens serienummer i fältet User-Agent i huvudet i HTTP-begäran.

HTTPS-servrar kan konfigureras att begära SSL-certifikat från anslutande klienter. Om den här konfigurationen har aktiverats kan servern använda Ciscos klientrotcertifikat för multiplattformstelefoner för att verifiera

klientcertifikatet. Servern kan sedan göra certifikatinformationen tillgänglig för ett CGI-skript för vidare bearbetning.

Platsen för certifikatslagring kan variera. Följande exempel visar filsökvägarna för lagring av certifikat som signerats av etableringsservern, den associerade privata nyckeln och CA-klientrotcertifikatet för multiplattformstelefoner i en Apache-installation:

```
# 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
```

Specifik information finns i dokumentationen för HTTPS-servrar.

Ciscos klientrotcertifikatutfärdare signerar varje unikt certifikat. Det associerade rotcertifikatet görs tillgängligt för tjänsteleverantörer för klientautentisering.

Redundanta etableringsservrar

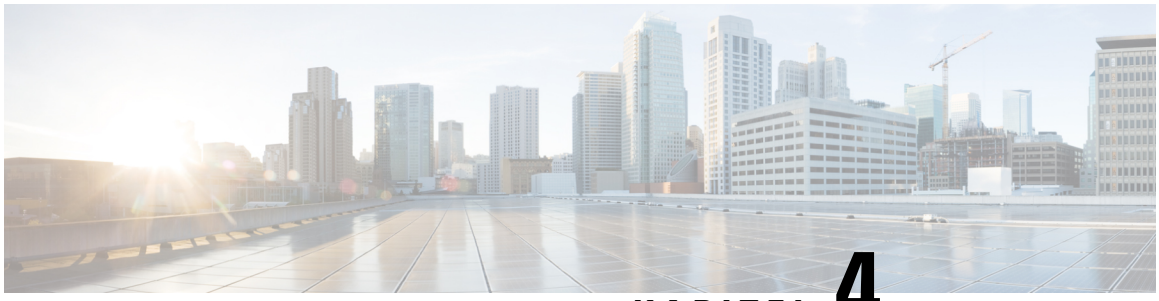
Etableringsservern kan anges som en IP-adress eller som ett fullständigt kvalificerat domännamn (FQDN). Användningen av ett fullständigt kvalificerat domännamn underlättar distributionen av redundanta etableringsservrar. När etableringsservern identifieras med ett fullständigt kvalificerat domännamn försöker telefonen matcha namnet med en IP-adress via DNS. Endast DNS A-poster stöds för etablering. DNS SRV-adressmatchning kan inte användas för etablering. Telefonen fortsätter att bearbeta A-poster tills en server svarar. Om ingen server som är associerad med A-posterna svarar, loggar telefonen ett fel till syslog-servern.

Syslog-server

Om en syslog-servern har konfigurerats på telefonen med hjälp av <Syslog Server>-parametrarna skickar omsynkroniseringen och uppgraderingsåtgärderna meddelanden till syslog-servern. Ett meddelande kan genereras i början av en begäran för en fjärransluten fil (konfigurationsprofil eller fast programvara) och i slutet av åtgärden (anger om åtgärden lyckades eller misslyckades).

De loggade meddelandena konfigureras i följande parametrar och makroexpanderas i själva syslog-meddelandena:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



KAPITEL 4

Etableringsexempel

Översikt över etableringsexempel

Det här kapitlet innehåller exempelprocedurer som beskriver hur konfigurationsprofiler överförs mellan telefonen och etableringsservern.

Information om hur du skapar konfigurationsprofiler finns i Etableringsskript, på sidan 13.

Grundläggande omsynkronisering

I det här avsnittet beskrivs de grundläggande omsynkroniseringsfunktionerna för telefonerna.

TFTP-omsynkronisering

Telefonen stöder flera nätverksprotokoll för att hämta konfigurationsprofiler. De mest grundläggande profilöverföringsprotokollet är TFTP (RFC1350). TFTP används ofta för etablering av nätverksenheter i privata, lokala nätverk. Även om det inte rekommenderas för distribution av fjärrslutpunkter via Internet kan TFTP vara användbart för distribution inom små organisationer, för intern företablering och för utveckling och testning. Mer information om intern företablering finns i Intern företablering på enheter, på sidan 39. I följande procedur ändras en profil när en fil har hämtats från en TFTP-server.

Arbetsordning

Steg 1 I en LAN-miljö ansluter du en dator och en telefon till ett nav, en växel eller en liten router.

Steg 2 Installera och aktivera en TFTP-server på datorn.

Steg 3 Använd en textredigerare för att skapa en konfigurationsprofil som konfigurerar värdet för GPP_A till 12345678 som i exemplet.

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

Steg 4 Spara profilen med namnet `basic.txt` i TFTP-serverns rotkatalog.

Du kan kontrollera att TFTP-servern är rätt konfigurerad genom att begära `basic.txt`-filen via en annan TFTP-klient än telefonen. Använd helst en TFTP-klient som körs på en annan värd än etableringsservern.

Steg 5 Öppna sidan för administratörskonfiguration/avancerad konfiguration i webbläsaren på datorn. Om telefonens IP-adress exempelvis är 192.168.1.100:

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

Steg 6 Gå till **Röst** > **Etablering** och kontrollera värdena för de allmänna parametrarna GPP_A till och med GPP_P. De bör vara tomma.

Steg 7 Synkronisera om testtelefonen till `basic.txt`-konfigurationsprofilen genom att öppna omsynkroniserings-URL:en i ett webbläsarfönster.

Om TFTP-serverns IP-adress är 192.168.1.200 bör kommandot likna det i följande exempel:

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

När telefonen tar emot det här kommandot begär enheten på adressen 192.168.1.100 `basic.txt`-filen från TFTP-servern på IP-adressen 192.168.1.200. Telefonen parsar sedan den hämtade filen och uppdaterar parametern GPP_A med värdet 12345678.

Steg 8 Kontrollera att parametern har uppdaterats korrekt genom att uppdatera konfigurationssidan i webbläsaren på datorn och gå till **Röst** > **Etablering**.

Nu bör parametern GPP_A innehålla värdet 12345678.

Använda Syslog för att logga meddelanden

Telefonen skickar ett syslog-meddelande till den angivna syslog-servern när enheten är på väg att synkronisera till en etableringsservern och när omsynkroniseringen har slutförts eller misslyckats. Du kan identifiera den här servern genom att gå till telefonens administrationswebbsida (se Åtkomst till webbsidan för telefonen, på sidan 7), välja **Röst** > **System** och identifiera servern i parametern **Syslog Server** i avsnittet **Valfri nätverkskonfiguration**. Konfigurera syslog-serverns IP-adress på enheten och observera meddelandena som genereras under de återstående procedurerna.

Arbetsordning

Steg 1 Installera och aktivera en syslog-server på den lokala datorn.

Steg 2 Programmera datorns IP-adress i parametern Syslog_Server i profilen och skicka ändringen:

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

Steg 3 Klicka på fliken **System** och ange värdet för din lokala syslog-server i parametern Syslog_Server.

Steg 4 Upprepa omsynkroniseringsåtgärden genom att följa anvisningarna i TFTP-omsynkronisering, på sidan 47.

Enheten genererar två syslog-meddelanden under omsynkroniseringen. Det första meddelandet anger att en begäran bearbetas. Det andra meddelandet anger att omsynkroniseringen har lyckats eller misslyckats.

Steg 5 Kontrollera att syslog-servern har tagit emot meddelanden liknande följande:

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

Du kan få detaljerade meddelanden genom att programmera en Debug_Server-parameter (i stället för parametern Syslog_Server) med syslog-serverns IP-adress och genom att ställa in Debug_Level till ett värde mellan 0 och 3 (där 3 representerar den mest utförliga nivån):

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

Innehållet i dessa meddelanden kan konfigureras med hjälp av följande parametrar:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Om någon av dessa parametrar tas bort genereras inte det associerade syslog-meddelandet.

Synkronisera om en enhet automatiskt

En enhet kan regelbundet synkroniseras mot etableringsservern för att säkerställa att eventuella profiländringar på servern distribueras till slutpunktsenheten (i stället för att en uttrycklig omsynkroniseringsbegäran skickas till slutpunkten).

Du kan konfigurera telefonen så att den regelbundet synkroniseras med en server genom att definiera en URL för konfigurationsprofilen med hjälp av parametern Profile_Rule, och en omsynkroniseringsperiod med hjälp av parametern Resync_Periodic.

Innan du börjar

Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Arbetsordning

Steg 1 Välj **Röst** > **Provisionering**.

Steg 2 Definiera parametern Profile_Rule. I det här exemplet är TFTP-serverns IP-adress 192.168.1.200.

Steg 3 Ange ett lågt värde för testning i fältet **Resync Periodic**, t.ex. **30** sekunder.

Steg 4 Klicka på **Verkställ alla ändringar**.

Med de nya parameterinställningarna synkroniserar telefonen två gånger per minut med konfigurationsfilen som anges i URL:en.

Steg 5 Observera de resulterande meddelandena i syslog-spårningen (som beskrivs i avsnittet Använda Syslog för att logga meddelanden, på sidan 48).

Steg 6 Kontrollera att värdet i fältet **Resync On Reset** är **Yes**.

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

Steg 7 Stäng av telefonen för att framtvinga en omsynkronisering till etableringsservern.

Om omsynkroniseringen misslyckas av någon anledning, t.ex. om servern inte svarar, så väntar enheten (det antal sekunder som konfigurerats i **Resync Error Retry Delay**) innan den försöker synkronisera igen. Om **Resync Error Retry Delay** är 0 försöker telefonen inte synkronisera igen efter ett misslyckat omsynkroniseringsförsök.

Steg 8 (Valfritt) Ange ett lågt värde i fältet **Resync Error Retry Delay**, t.ex. **30**.

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

Steg 9 Inaktivera TFTP-servern och observera resultatet som returneras av syslog.

Unika profiler, makroexpandering och HTTP

I en implementering där vissa parametrar, till exempel User_ID eller Display_Name, måste konfigureras med unika värden för varje telefon, kan tjänsteleverantören skapa en unik profil för varje distribuerad enhet och lagra dessa profiler på en etableringsservern. Varje telefon måste sedan konfigureras att synkronisera mot sin egen profil baserat på en förbestämd namngivningskonvention för profiler.

Profilens URL-syntax kan innehålla identifierande information som är specifik för varje telefon, till exempel MAC-adressen eller serienumret, genom makroexpandering av inbyggda variabler. När makroexpandering används behöver inte dessa värden anges på flera platser i varje profil.

En profilregel makroexpanderas innan regeln tillämpas på telefonen. Makroexpanderingen styr flera värden, till exempel:

- $MA expanderas till enhetens 12-siffriga MAC-adress (med gemena hexadecimala tecken). Till exempel 000e08abcdef.
- $SN expanderas till enhetens serienummer. Till exempel 88012BA01234.

Andra värden kan makroexpanderas på det här sättet, inklusive alla allmänna parametrar, dvs. GPP_A till och med GPP_P. Ett exempel på den här processen finns i TFTP-omsynkronisering, på sidan 47. Makroexpandering kan tillämpas på valfri del av parametern för profilregeln och är inte begränsat till URL-filnamnet. Du refererar till dessa parametrar som $A till och med $P. En fullständig lista över variabler som är tillgängliga för makroexpandering finns i Variabler för makroexpandering, på sidan 72.

I den här övningen etableras en profil som är specifik för en telefon på en TFTP-server.

Övning: Etablera en specifik IP-telefonprofil på en TFTP-server

Arbetsordning

Steg 1 Leta upp telefonens MAC-adress på produktetiketten för telefonen. (MAC-adressen är numret som innehåller siffror och gemena hexadecimala siffror, t.ex. 000e08aabbcc.)

Steg 2 Kopiera `basic.txt`-konfigurationsfilen (beskrivs i TFTP-omsynkronisering, på sidan 47) till en ny fil med namnet `CP-xxxx-3PCC macaddress.cfg` (där du ersätter `xxxx` med modellnumret och `macaddress` med telefonens MAC-adress).

Steg 3 Spara den nya filen i TFTP-serverns virtuella rotkatalog.

Steg 4 Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Steg 5 Välj **Röst** > **Provisionering**.

Steg 6 Ange `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` i fältet **Profilregel**.

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

Steg 7 Klicka på **Verkställ alla ändringar**. Detta utlöser en omedelbar omstart och omsynkronisering.

När nästa omsynkronisering utförs hämtar telefonen den nya filen genom att expandera $MA-makrouttrycket till MAC-adressen.

HTTP GET-omsynkronisering

HTTP tillhandahåller en mer tillförlitlig omsynkroniseringsmekanism än TFTP eftersom HTTP upprättar en TCP-anslutning och TFTP använder det mindre tillförlitliga UDP. Dessutom erbjuder HTTP-servrar bättre filtrerings- och loggningsfunktioner jämfört med TFTP-fjärrservrar.

På klientsidan kräver inte telefonen någon särskild konfigurationsinställning på servern för att kunna synkronisera med hjälp av HTTP. Profile_Rule-parametersyntaxen vid användning av HTTPS med GET-metoden liknar syntaxen som används för TFTP. Om en standardwebbläsare kan hämta en profil från din HTTP-server, bör telefonen kunna göra det också.

Övning: HTTP GET-omsynkronisering

Arbetsordning

Steg 1 Installera en HTTP-server på den lokala datorn eller en annan tillgänglig värd.

Apache-servern med öppen källkod kan hämtas från Internet.

Steg 2 Kopiera konfigurationsprofilen `basic.txt` (beskrivs i TFTP-omsynkronisering, på sidan 47) i den installerade serverns virtuella rotkatalog.

Steg 3 Kontrollera att serverinstallationen slutförts korrekt och att du kan komma åt `basic.txt`-filen genom att öppna profilen i en webbläsare.

Steg 4 Ändra Profile_Rule för testtelefonen så att den pekar på HTTP-servern i stället för på TFTP-servern, så att profilen hämtas regelbundet.

Om vi antar att HTTP-servern till exempel är 192.168.1.300, anger du följande värde:

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

Steg 5 Klicka på **Verkställ alla ändringar**. Detta utlöser en omedelbar omstart och omsynkronisering.

Steg 6 Observera syslog-meddelandena som telefonen skickar. Nu bör profilen hämtas från HTTP-servern vid de regelbundna omsynkroniseringarna.

Steg 7 Granska HTTP-serverloggarna och se hur informationen som identifierar testtelefonen visas i användaragentloggen.

Informationen bör innehålla tillverkaren, produktnamnet, den aktuella versionen av den fasta programvaran och serienumret.

Etablering via Cisco XML

För var och en av telefonerna, som här anges som xxxx, kan du etablera med hjälp av Cisco XML-funktioner.

Du kan skicka ett XML-objekt till telefonen via ett SIP Notify-paket eller HTTP POST till telefonens CGI-gränssnitt: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC utökar Cisco XML-funktionen för att ge stöd för etablering via ett XML-objekt:

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

När telefonen tar emot XML-objektet hämtar den etableringsfilen från [profile-rule]. Den här regeln använder makron för att underlätta utvecklingen av XML-tjänstprogrammet.

URL-matchning med makroexpandering

Underkataloger med flera profiler på servern gör det enkelt att hantera ett stort antal distribuerade enheter. Profilens URL kan innehålla:

- Etableringsserverns namn eller en explicit IP-adress. Om profilen identifierar etableringsservern baserat på dess namn utför telefonen en DNS-sökning för att matcha namnet.
- En annan serverport än standardporten som anges i URL:en, som anges med standardsyntaxen `:port` efter servernamnet.
- Underkatalogen i serverns virtuella rotkatalog där profilen lagras, som anges med URL-standardnotation och som hanteras med makroexpandering.

Exempelvis begär följande Profile_Rule profilfilen ($PN.cfg), i underkatalogen `/cisco/config` på servern, från TFTP-servern som körs på värden prov.telco.com och som lyssnar efter en anslutning på port 6900:

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

```
</Profile_Rule>
```

En profil för varje telefon kan identifieras i en allmän parameter, där makroexpandering används för att referera till dess värde i en gemensam profilregel.

Anta till exempel att GPP_B definierats som `Dj6Lmp23Q`.

Profile_Rule har värdet:

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

När enheten synkroniseras och makrona expanderas begär telefonen med MAC-adressen 000e08012345 profilen med namnet som innehåller enhetens MAC-adress på följande URL:

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

Säker HTTPS-omsynkronisering

Följande funktioner är tillgängliga på telefonen för omsynkronisering via en säker kommunikationsprocess:

- Grundläggande HTTPS-omsynkronisering
- HTTPS med klientcertifikatautentisering
- HTTPS-klientfiltrering och dynamiskt innehåll

Grundläggande HTTPS-omsynkronisering

HTTPS lägger till SSL till HTTP vid fjärretablering så att:

- Telefonen kan autentisera etableringsservern.
- Etableringsservern kan autentisera telefonen.
- Integriteten i information som kommuniceras mellan telefonen och etableringsservern säkerställs.

SSL genererar och utbyter hemliga (symmetriska) nycklar för varje anslutning mellan telefonen och servern med hjälp av nyckelpar med offentliga och privata nycklar som är förinstallerade på telefonen och på etableringsservern.

På klientsidan kräver inte telefonen någon särskild konfigurationsinställning på servern för att kunna synkronisera med hjälp av HTTPS. Profile_Rule-parametersyntaxen vid användning av HTTPS med GET-metoden liknar syntaxen som används för HTTP och TFTP. Om en standardwebbläsare kan hämta en profil från en HTTPS-server, bör telefonen kunna göra det också.

Förutom att installera en HTTPS-server måste ett SSL-servercertifikat som Cisco signerar installeras på etableringsservern. Enheterna kan inte synkronisera till en server som använder HTTPS om inte servern tillhandahåller ett Cisco-signerat servercertifikat. Instruktioner för hur du skapar signerade SSL-certifikat för röstprodukter finns på https://supportforums.cisco.com/docs/DOC-9852.

Övning: Grundläggande HTTPS-omsynkronisering

Arbetsordning

Steg 1 Installera en HTTPS-server på en värd vars IP-adress kan identifieras av nätverkets DNS-server genom normal värdnamnsöversättning.

Apache-servern med öppen källkod kan konfigureras att fungera som en HTTPS-server när den installeras med mod_ssl-paketet med öppen källkod.

Steg 2 Generera en begäran om servercertifikatsignering för servern. I det här steget kan du behöva installera OpenSSL-paketet med öppen källkod eller likvärdig programvara. Om du använder OpenSSL använder du följande kommando för att generera den grundläggande CSR-filen:

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

Det här kommandot genererar ett nyckelpar med offentliga och privata nycklar, som sparas i filen `privkey.pem`.

Steg 3 Skicka CSR-filen (provserver.csr) till Cisco för signering.

Ett signerat servercertifikat returneras (provserver.cert) tillsammans med ett Sipura CA-klientrotcertifikat, spacroot.cert.

Mer information finns i https://supportforums.cisco.com/docs/DOC-9852

Steg 4 Spara det signerade servercertifikatet och filen med nyckelparen samt klientrotcertifikatet på lämpliga platser på servern.

Om du har en Apache-installation i Linux används vanligtvis följande platser:

```
# 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
```

Steg 5 Starta om servern.

Steg 6 Kopiera `basic.txt`-konfigurationsfilen (beskrivs i TFTP-omsynkronisering, på sidan 47) till HTTPS-serverns virtuella rotkatalog.

Steg 7 Kontrollera att servern fungerar som den ska genom att hämta `basic.txt` från HTTPS-servern via en webbläsare från den lokala datorn.

Steg 8 Kontrollera servercertifikatet som du får från servern.

Webbläsaren identifierar antagligen inte certifikatet som giltigt om inte webbläsaren har förkonfigurerats att godkänna Cisco som rotcertifikatutfärdare. Men telefonerna förväntar sig att certifikatet signeras på det här sättet.

Ändra Profile_Rule för testenheten så att den innehåller en referens till HTTPS-servern, till exempel:

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

```
</Profile_Rule>
```

I det här exemplet är namnet på HTTPS-servern **my.server.com**.

Steg 9 Klicka på **Verkställ alla ändringar**.

Steg 10 Observera syslog-spårningen som telefonen skickar.

Syslog-meddelandet bör ange att profilen hämtades från HTTPS-servern vid omsynkroniseringen.

Steg 11 (Valfritt) Kör ett Ethernet-protokollanalysverktyg i telefonens subnät för att verifiera att paketen krypteras.

I den här övningen aktiverades inte klientcertifikatsverifiering. Anslutningen mellan telefonen och servern krypteras. Överföringen är dock inte säker eftersom alla klienter kan ansluta till servern och begära filen om de känner till filnamnet och katalogens sökväg. För en säker omsynkronisering måste servern även autentisera klienten, som du såg i övningen som beskrivs i HTTPS med klientcertifikatautentisering, på sidan 55.

HTTPS med klientcertifikatautentisering

I den ursprungliga fabrikskonfigurationen begär inte servern ett SSL-klientcertifikat från en klient. Överföringen av profilen är inte säker eftersom alla klienter kan ansluta till servern och begära profilen. Du kan aktivera klientautentisering genom att redigera konfigurationen så att servern kräver ett klientcertifikat för att autentisera telefonen innan den godkänner en anslutningsbegäran.

Detta krav innebär att omsynkroniseringen inte kan testas separat via en webbläsare som saknar rätt autentiseringsuppgifter. SSL-nyckelutbytet i HTTPS-anslutningen mellan testtelefonen och servern kan övervakas med verktyget ssldump. Verktygsspårningen visar interaktionen mellan klienten och servern.

Övning: HTTPS med klientcertifikatautentisering

Arbetsordning

Steg 1 Aktivera klientcertifikatautentisering på HTTPS-servern.

Steg 2 I Apache (v.2) anger du följande i serverkonfigurationsfilen:

```
SSLVerifyClient  require
```

Kontrollera också att spacroot.cert har lagrats korrekt (se övningen Grundläggande HTTPS-omsynkronisering, på sidan 53).

Steg 3 Starta om HTTPS-servern och kontrollera syslog-spårningen från telefonen.

Nu utförs symmetrisk autentisering vid varje omsynkronisering till servern, så att både servercertifikatet och klientcertifikatet verifieras innan profilen överförs.

Steg 4 Använd ssldump om du vill visa omsynkroniseringsanslutningen mellan telefonen och HTTPS-servern.

Om klientcertifikatsverifieringen har aktiverats korrekt på servern visar ssldump-spårningen det symmetriska certifikatutbytet (först server-till-klient och sedan klient-till-server) före de krypterade paketen som innehåller profilen.

När klientautentisering är aktiverat kan bara en telefon med en MAC-adress som matchar ett giltigt klientcertifikat begära profilen från etableringsservern. Servern avvisar förfrågningar från vanliga webbläsare eller andra obehöriga enheter.

HTTPS-klientfiltrering och dynamiskt innehåll

Om HTTPS-servern har konfigurerats att begära ett klientcertifikat identifierar informationen i certifikatet telefonen som synkroniseras och förser den med rätt konfigurationsinformation.

HTTPS-servern gör certifikatinformationen tillgänglig för CGI-skript (eller kompilerade CGI-program) som anropas som en del av omsynkroniseringsbegäran. Den här övningen bygger på skriptspråket Perl (öppen källkod) och förutsätter att Apache (v.2) används som HTTPS-servern.

Arbetsordning

Steg 1 Installera Perl på värden som kör HTTPS-servern.

Steg 2 Generera följande Perl-reflektorskript:

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

Steg 3 Spara filen med filnamnet `reflect.pl`, med körningsbehörighet (chmod 755 i Linux) i katalogen med CGI-skript på HTTPS-servern.

Steg 4 Kontrollera att CGI-skripten är tillgängliga på servern (dvs. `/cgi bin /...`).

Steg 5 Ändra Profile_Rule på testenheten så att den synkroniserar mot reflektorskriptet, som i följande exempel:

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

Steg 6 Klicka på **Verkställ alla ändringar**.

Steg 7 Kontrollera syslog-spårningen för att försäkra dig om att omsynkroniseringen lyckades.

Steg 8 Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Steg 9 Välj **Röst** > **Provisionering**.

Steg 10 Kontrollera att parametern GPP_D innehåller informationen som hämtades av skriptet.

Den här informationen innehåller produktens namn, MAC-adress och serienummer om testenheten har ett unikt certifikat från tillverkaren. Informationen innehåller allmänna strängar om enheten tillverkades före version 2.0 av den fasta programvaran.

Ett liknande skript kan hämta information om enheten som synkroniseras och sedan förse enheten med lämpliga konfigurationsparametervärden.

HTTPS-certifikat

Telefonen tillhandahåller en tillförlitlig och säker etableringsstrategi som baseras på HTTPS-förfrågningar från enheten till etableringsservern. Både ett servercertifikat och ett klientcertifikat används för att autentisera telefonen mot servern och servern mot telefonen.

För att använda HTTPS med telefonen måste du generera en certifikatsigneringsbegäran (CSR) och skicka den till Cisco. Telefonen genererar ett certifikat för installation på etableringsservern. Telefonen accepterar certifikatet när den försöker upprätta en HTTPS-anslutning med etableringsservern.

HTTPS-metod

HTTPS krypterar kommunikationen mellan en klient och en server och skyddar på så sätt meddelandeinnehållet från andra nätverksenheter. Krypteringsmetoden för själva innehållet i kommunikationen mellan en klient och en server baseras på kryptografi med symmetriska nycklar. Med kryptering med symmetriska nycklar delar en klient och en server en hemlig nyckel via en säker kanal som skyddas av kryptering med offentliga och privata nycklar.

Meddelanden som krypterats med den privata nyckeln kan endast dekrypteras med samma nyckel. HTTPS stöder flera olika algoritmer för symmetrisk kryptering. Telefonen stöder symmetrisk kryptering på upp till 256 bitar med AES (American Encryption Standard), förutom 128-bitars RC4.

HTTPS har även stöd för server- och klientautentisering i säkra transaktioner. Den här funktionen förhindrar att andra enheter i nätverket imiterar en etableringsserver eller en klient. Den här funktionen är nödvändig vid etablering av fjärrslutpunkter.

Server- och klientautentiseringar utförs via kryptering med offentliga och privata nycklar med ett certifikat som innehåller den offentliga nyckeln. Text som krypteras med en offentlig nyckel kan endast dekrypteras av den associerade privata nyckeln (och vice versa). Telefonen stöder RSA-algoritmen (Rivest-Shamir-Adleman) för kryptering med offentliga och privata nycklar.

SSL-servercertifikat

Alla säkra etableringsservrar tilldelas ett SSL-servercertifikat (Secure Sockets Layer) som Cisco signerar direkt. Endast Cisco-certifikat identifieras som giltiga certifikat av den fasta programvaran som körs på telefonen. När en klient ansluter till en server via HTTPS avvisar den alla servercertifikat som inte signerats av Cisco.

Den här mekanismen förhindrar obehörig åtkomst på telefonen, eller försök att imitera etableringsservern. Utan den här typen av skydd kan en illvillig användare etablera om telefonen för att därigenom få tag i konfigurationsinformation eller komma åt en annan VoIP-tjänst. Utan den privata nyckeln som är associerad med ett giltigt servercertifikat kan en illvillig användare inte upprätta kommunikation med en telefon.

Skaffa ett servercertifikat

Arbetsordning

Steg 1 Kontakta Cisco support så hjälper vi dig med certifikatprocessen. Om du inte redan har en personlig supportkontakt kan du skicka din förfrågan till ciscosb-certadmin@cisco.com.

Steg 2 Generera en privat nyckel som du sedan ska använda i en certifikatsigneringsbegäran (CSR). Den här nyckeln är privat och du behöver inte uppge den till Cisco support. Använd ”openssl” med öppen källkod för att generera nyckeln. Till exempel:

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

Steg 3 Generera en CSR som innehåller fält som identifierar din organisation och plats. Till exempel:

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

Du behöver följande information:

- Ämnesfält – Ange det vanliga namnet (CN, Common Name). Namnet måste ha FQDN-syntax (fullständigt kvalificerat domännamn). I handskakningsfasen i SSL-autentiseringsprocessen kontrollerar telefonen att certifikatet som tas emot kommer från den dator som skickade det.
- Serverns värdnamn – Till exempel provserv.domain.com.
- E-postadress – Ange en e-postadress så att kundsupporten kan kontakta dig om det behövs. Den här e-postadressen visas i certifikatsigneringsbegäran (CSR).

Steg 4 Skicka CSR via e-post (i ZIP-format) till kontaktpersonen på Cisco support eller till ciscosb-certadmin@cisco.com. Certifikatet signeras av Cisco. Cisco skickar certifikatet till dig så att du kan installera det i ditt system.

Klientcertifikat

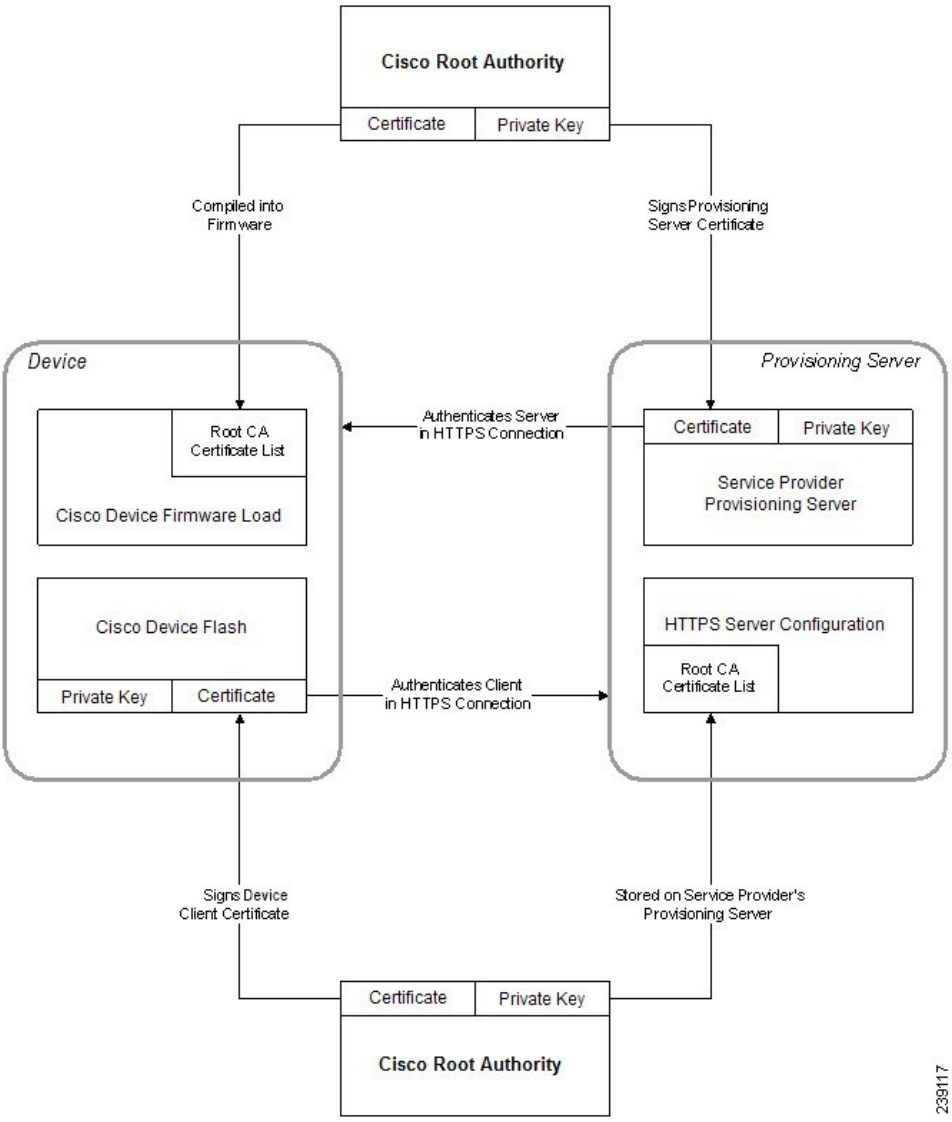
Förutom att utföra en direkt attack på en telefon kan en illvillig användare försöka kontakta en etableringsserver via en vanlig webbläsare eller en annan HTTPS-klient för att komma åt konfigurationsprofilen på etableringsservern. För att förhindra den här typen av attacker har varje telefon även ett unikt Cisco-signerat klientcertifikat, som innehåller information om varje enskild slutpunkt. Ett CA-rotcertifikat (Certificate Authority) som kan autentisera enhetens klientcertifikat utfärdas till varje tjänsteleverantör. Den här autentiseringsmetoden gör att etableringsservern kan avvisa obehöriga begäranden om konfigurationsprofiler.

Certifikatstruktur

Kombinationen av ett servercertifikat och ett klientcertifikat säkerställer en säker kommunikation mellan en fjärransluten telefon och dess etableringsserver. Bilden nedan illustrerar förhållandet mellan och placeringen av certifikat, par med offentliga och privata nycklar, rotutfärdare för signering, t.ex. Ciscos klientcertifikat, etableringsservern och certifikatutfärdaren.

Den övre halvan av diagrammet visar rotcertifikatutfärdaren för etableringsservern som används för att signera det enskilda etableringsservercertifikatet. Det associerade rotcertifikatet kompileras i den fasta programvaran, vilket gör att telefonen kan autentisera auktoriserade etableringsservrar.

Figur 2. CA-flöde (Certificate Authority)



Konfigurera en anpassad CA (Certificate Authority)

Digitala certifikat kan användas för att autentisera nätverksenheter och användare i nätverket. De kan användas för att förhandla IPSec-sessioner mellan nätverksnoder.

En tredje part använder ett certifikat från en certifikatutfärdare (CA, Certificate Authority) för att validera och autentisera två eller flera noder som försöker kommunicera. Varje nod har en offentlig och privat nyckel. Den offentliga nyckeln krypterar data. Den privata nyckeln dekrypterar data. Eftersom noderna har erhållit certifikaten från samma källa, är deras identiteter säkerställda.

Enheten kan använda digitala certifikat från en tredje parts certifikatutfärdare för att autentisera IPSec-anslutningar.

Telefonerna har stöd för en uppsättning förinstallerade rotcertifikatutfärdare som är inbyggda i den fasta programvaran:

- Cisco Small Business CA-certifikat
- CyberTrust CA-certifikat
- Verisign CA-certifikat
- Sipura Root CA-certifikat
- Linksys Root CA-certifikat

Innan du börjar

Öppna webbsidan för telefonadministration. Se Åtkomst till webbsidan för telefonen, på sidan 7.

Arbetsordning

Steg 1 Välj **Info** > **Status**.

Steg 2 Gå till **Anpassad CA-status** och notera följande fält:

- Anpassad CA-etableringsstatus – Anger etableringsstatusen.
  - Senaste etableringen lyckades mm/dd/yyyy HH:MM:SS eller
  - Senaste etableringen misslyckades mm/dd/yyyy HH:MM:SS
- Info om anpassad CA – Visar information om den anpassade certifikatutfärdaren.
  - Installerat – Visar "CN-värde" där "CN-värde" är värdet på CN-parametern i fältet Ämne i det första certifikatet.
  - Inte installerat – Visas om inget anpassat CA-certifikat har installerats.

Profilhantering

Det här avsnittet beskriver hur konfigurationsprofiler skapas inför hämtningen. För att illustrera funktionerna används TFTP från en lokal dator som omsynkroniseringsmetod, men även HTTP och HTTPS kan användas.

Komprimera en öppen profil med Gzip

En konfigurationsprofil i XML-format kan bli mycket stor om alla parametrar anges separat i profilen. För att minska belastningen på etableringsservern stöder telefonen komprimering av XML-filen med hjälp av Deflate-komprimeringsformatet, som kan användas i verktyget gzip (RFC 1951).

OBS! Komprimeringen måste utföras innan krypteringen för att telefonen ska kunna identifiera den komprimerade och krypterade XML-profilen.

För integrering med anpassade lösningar för backend-etableringsservrar kan profilkomprimeringen utföras med zlib-komprimeringsbiblioteket med öppen källkod i stället för med det fristående gzip-verktyget. Telefonen förväntar sig dock att filen innehåller ett giltigt gzip-huvud.

Arbetsordning

Steg 1 Installera gzip på den lokala datorn.

Steg 2 Komprimera konfigurationsfilen `basic.txt` (beskrivs i TFTP-omsynkronisering, på sidan 47) genom att anropa gzip från kommandoraden:

```
gzip basic.txt
```

När du gör det genereras den komprimerade filen `basic.txt.gz`.

Steg 3 Spara filen `basic.txt.gz` i TFTP-serverns virtuella rotkatalog.

Steg 4 Ändra Profile_Rule på testenheten så att den synkroniseras mot den komprimerade filen i stället för den ursprungliga XML-filen, som du ser i följande exempel:

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

Steg 5 Klicka på **Verkställ alla ändringar.**

Steg 6 Observera syslog-spårningen från telefonen.

Vid omsynkroniseringen hämtar telefonen den nya filen och använder den för att uppdatera sina parametrar.

Relaterade ämnen

Komprimering av öppen profil, på sidan 18

Kryptera en profil med OpenSSL

Komprimerade och okomprimerade profiler kan krypteras (observera att en fil måste komprimeras innan den krypteras). Kryptering är användbart när det är viktigt att profilinformationen skyddas, t.ex. om TFTP eller HTTP används för kommunikation mellan telefonen och etableringsservern.

Telefonen stöder kryptering med symmetriska nycklar med hjälp av 256-bitars AES-algoritmen. Den här krypteringen kan utföras med hjälp av OpenSSL-paketet med öppen källkod.

Arbetsordning

Steg 1 Installera OpenSSL på en lokal dator. OpenSSL-programmet kanske måste kompileras för att aktivera AES.

Steg 2 Använd konfigurationsfilen `basic.txt` (beskrivs i TFTP-omsynkronisering, på sidan 47) och generera en krypterad fil med följande kommando:

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

Den komprimerade `basic.txt.gz`-filen som skapades i Komprimera en öppen profil med Gzip, på sidan 60 kan också användas eftersom XML-profilen kan vara både komprimerad och krypterad.

Steg 3 Spara den krypterade `basic.txt.gz`-filen i TFTP-serverns virtuella rotkatalog.

Steg 4 Ändra Profile_Rule på testenheten för att synkronisera till den krypterade filen i stället för till den ursprungliga XML-filen. Krypteringsnyckeln tillgängliggörs till telefonen med följande URL-alternativ:

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

Steg 5 Klicka på **Verkställ alla ändringar**.

Steg 6 Observera syslog-spårningen från telefonen.

Vid omsynkroniseringen hämtar telefonen den nya filen och använder den för att uppdatera sina parametrar.

Relaterade ämnen

AES-256-CBC Kryptering, på sidan 18

Skapa partitionerade profiler

En telefon hämtar många olika profiler vid varje omsynkronisering. Med den här metoden kan du hantera olika typer av profilinformation på separata servrar och använda andra konfigurationsparametervärden än de kontospecifika värdena.

Arbetsordning

Steg 1 Skapa en ny XML-profil, `basic2.txt`, som anger ett annat värde för en parameter än de i de tidigare övningarna. Lägg exempelvis till följande i `basic.txt`-profilen:

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

Steg 2 Spara `basic2.txt`-profilen i TFTP-serverns virtuella rotkatalog.

Steg 3 Lämna den första profilregeln från de tidigare övningarna i mappen, men konfigurera den andra profilregeln (Profile_Rule_B) så att den pekar på den nya filen:

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

Steg 4 Klicka på **Verkställ alla ändringar**.

Nu synkroniserar telefonen om till både den första och den andra profilen, i den ordningen, så fort en omsynkronisering körs.

Steg 5 Kontrollera syslog-spårningen för att bekräfta att beteendet är som förväntat.

Ställa in telefonens sekretesshuvud

Ett huvud för användarsekretess i SIP-meddelandet anger krav på användarsekretess från det betrodda nätverket.

Du kan ange värdet för huvudet för användarsekretess för varje anknytning med en XML-tagg i `config.xml`-filen.

Alternativen för sekretesshuvudet är:

- Inaktiverat (standard)
- none – Användaren begär att en privat tjänst inte använder några sekretessfunktioner i det här SIP-meddelandet.
- header – Användaren vill att en privat tjänst döljer huvuden där identifierande information inte kan tas bort.
- session – Användaren begär att en privat tjänst ger anonymitet i sessionerna.
- user – Användaren begär en sekretessnivå endast av mellanhänder.
- id – Användaren begär att systemet ska byta till ett ID som inte visar IP-adressen eller värdnamnet.

Arbetsordning

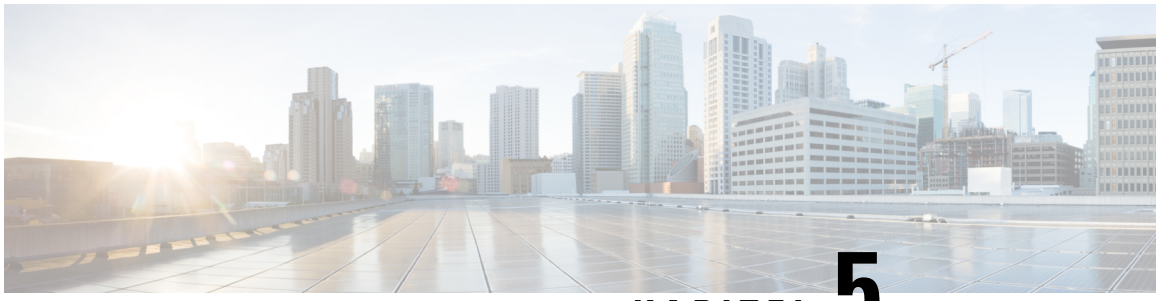
Steg 1 Redigera telefonens `config.xml`-fil i en XML- eller textredigerare.

Steg 2 Infoga **<Privacy_Header_N_ ua="na">*värde*</Privacy_Header_N_>**-taggen, där N är anknytningens nummer (1–10) och använd något av följande värden.

- Standardvärde: **Inaktiverat**
- **none**
- **header**
- **session**
- **user**
- **id**

Steg 3 (Valfritt) Etablera eventuella ytterligare anknytningar med hjälp av samma tagg med önskat anknytningsnummer.

Steg 4 Spara ändringarna i `config.xml`-filen.



KAPITEL 5

Etableringsparametrar

Översikt över etableringsparametrar

I det här kapitlet beskrivs etableringsparametrarna som kan användas i skript för konfigurationsprofiler.

Parametrar för konfigurationsprofilen

Följande tabell beskriver hur parametrarna i avsnittet **Parametrar för konfigurationsprofil** (Configuration Profile Parameters) på fliken **Etablering** fungerar och används.

Parameternamn	Beskrivning och standardvärde
Provision Enable	Kontrollerar alla omsynkroniseringsåtgärder oberoende av uppgraderingar av den fasta programvaran. Använd värdet **Ja** om du vill aktivera fjärretablering. Standardvärdet är Ja.
Resync On Reset	Utlöser en omsynkronisering efter varje omstart utom för omstarter orsakade av parameteruppdateringar och uppgraderingar av den fasta programvaran. Standardvärdet är Ja.

Parameternamn	Beskrivning och standardvärde
Resync Random Delay	En slumpmässig fördröjning efter startsekvensen innan du utför återställningen anges i sekunder. I en pool av IP-telefonienheter som är schemalagda att starta samtidigt införs en spridning i tider där varje enhet skickar en omsynkroniseringsbegäran till etableringsservern. Denna funktion kan vara bra i ett stort bostadsområde om det inträffar lokalt strömavbrott. Värdet för det här fältet måste vara ett heltal mellan 0 och 65 535. Standardvärdet är 2.
Resync At (HHmm)	Antalet timmar och minuter (HHmm) som enheten synkroniserar med etableringsservern. Värdet för det här fältet måste vara fyra siffror mellan 0000 till 2 400 att ange tiden i HHmm mm. 0959 anger till exempel 09:59. Värdet är tomt som standard. Om värdet är ogiltigt ignoreras parametern. Om den här parametern anges med ett giltigt värde ignoreras Resync Periodic-parametern.
Resync At Random Delay	Förhindrar en överbelastning av etableringsservern när ett stort antal enheter startas samtidigt. För att undvika att servern överbelastas med omsynkroniseringsförfrågningar från flera telefoner synkroniserar telefonen i intervallet mellan timmarna och minuterna, och timmarna och minuterna plus den slumpmässiga fördröjningen (hhmm, hhmm + random_delay). Till exempel, om den slumpmässiga fördröjningen = (Återsynka vid Slumpmässig fördröjning + 30)/60 minuter, omvandlas indatavärdet i sekunder till minuter och avrundas uppåt till nästa minut för att beräkna det slutliga random_delay-intervallet. Det giltiga värdet är i intervallet mellan 0 och 65 535. Den här funktionen inaktiveras om den här parametern anges till noll. Standardvärdet är 600 sekunder (10 minuter).

Parameternamn	Beskrivning och standardvärde
Resync Periodic	Tidsintervallet mellan periodiska omsynkroniseringar med etableringsservern. Den associerade omsynkroniseringstimern aktiveras efter den första lyckade synkroniseringen med servern. Giltiga format är följande: • Ett heltal Exempel: En inmatning av `3000` anger att nästa omsynkronisering sker om 3 000 sekunder. • Flera heltal Exempel: En inmatning av `600,1200,300` anger att första omsynkroniseringen inträffar efter 600 sekunder, andra omsynkronisering sker 1 200 sekunder efter den första, och den tredje omsynkroniseringen äger rum 300 sekunder efter den andra. • Ett tidsintervall Exempel, en inmatning av `2400 + 30` anger att nästa omsynkronisering sker mellan 2400 och 2430 sekunder efter en godkänd omsynkning. Ange den här parametern till noll om du vill inaktivera periodisk omsynkronisering. Standardvärdet är 3600 sekunder.

Parameternamn	Beskrivning och standardvärde
Resync Error Retry Delay	Om en omsynkronisering misslyckas, t.ex. om IP-telefonenheten inte kunde hämta en profil från servern, om den hämtade filen är skadad eller om det har uppstått ett internt fel, försöker enheten synkronisera igen efter en viss tid som anges i sekunder. Giltiga format är följande: • Ett heltal Exempel: En inmatning av **300** anger att nästa försök för omsynkronisering inträffar om 300 sekunder. • Flera heltal Exempelvis: En inmatning av **600,1200,300** anger att det första försöket inträffar efter 600 sekunder efter misslyckandet, det andra försöket 1200 sekunder efter misslyckandet av det första försöket, och det tredje försöket äger rum 300 sekunder efter misslyckandet av det andra försöket. • Ett tidsintervall Exempelvis, en inmatning av **2400 + 30** anger att nästa försök sker mellan 2400 och 2 430 sekunder efter en misslyckad omsynkronisering. Om förseningen är 0 försöker enheten inte synkronisera igen efter ett misslyckat omsynkroniseringsförsök.
Forced Resync Delay	Den längsta fördröjning (i sekunder) som telefonen väntar innan den utför en omsynkronisering. Enheten påbörjar inte omsynkroniseringen om någon av dess telefonlinjer är aktiv. Eftersom en omsynkronisering kan ta flera sekunder är det bäst att vänta tills enheten har varit inaktiv en längre tid innan omsynkroniseringen utförs. På så sätt kan användaren ringa samtal utan avbrott. Enheten har en timer som börjar nedräkningen när alla telefonens linjer blivit inaktiva. Den här parametern är räknarens första värde. Omsynkroniseringshändelser skjuts upp tills räknaren når noll. Det giltiga värdet är i intervallet mellan 0 och 65 535. Standardvärdet är 14 400 sekunder.

Parameternamn	Beskrivning och standardvärde
Resync From SIP	Tillåter att ett SIP NOTIFY-meddelande utlöser en omsynkronisering. Standardvärdet är Ja.
Resync After Upgrade Attempt	Aktiverar eller inaktiverar omsynkroniseringsåtgärden när en uppgradering har inträffat. Om Ja väljs utlöses synkronisering. Standardvärdet är Ja.
Resync Trigger 1, Resync Trigger 2	Konfigurerbara omsynkroniseringsutlösningsvillkor. En omsynkronisering utlöses när den logiska ekvationen i dessa parametrar utvärderas till TRUE. Standardvärdet är (tomt).
Resync Fails On FNF	En omsynkronisering anses misslyckad om en begärd profil inte tas emot från servern. Detta kan åsidosättas av den här parametern. Om värdet anges till **Nej** godtar enheten ett `file-not-found`-svar från servern som en lyckad omsynkronisering. Standardvärdet är Ja.
Profile Rule Profile Rule B Profilregel C Profile Rule D	Varje profilregel informerar telefonen om en källa från vilken den kan erhålla en profil (konfigurationsfil). Under varje återsynkronisering applicerar telefonen alla profiler i följd. Standard: **`/$PSN.xml`** Om du applicerar CBC-AES-256-kryptering till konfigurationsfilerna, specificera krypteringsnyckel med nyckelordet till **`– key`** på följande sätt: **`[--key <krypteringsnyckel>]`** Du kan också omsluta krypteringsnyckeln med dubbla citattecken (”).
DHCP Option To Use	DHCP-alternativ, avgränsade med kommatecken, som används för att hämta firmware och profiler. Standardvärdet är 66,160,159,150,60,43,125.
Log Request Msg	Den här parametern innehåller meddelandet som skickas till syslog-servern i början av ett omsynkroniseringsförsök. Standardvärdet är `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`.

Parameternamn	Beskrivning och standardvärde
Log Success Msg	Syslog-meddelandet som returneras efter ett lyckat omsynkroniseringsförsök. The default value is `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Log Failure Msg	Syslog-meddelandet som returneras efter ett misslyckat omsynkroniseringsförsök. Standardvärdet är `$PN $MAC -- Resync failed: $ERR`.
User Configurable Resync	Tillåter en användare att synkronisera telefonen från IP-telefonens skärm. Standardvärdet är Ja.

Parametrar för uppgradering av fast programvara

Följande tabell beskriver hur parametrarna i avsnittet **Uppgradera firmware** på fliken **Etablering** fungerar och används.

Parameternamn	Beskrivning och standardvärde
Upgrade Enable	Tillåter uppgradering av fast programvara oberoende av omsynkroniseringsåtgärder. Standardvärdet är Ja.
Upgrade Error Retry Delay	Intervallet för nya uppgraderingsförsök (i sekunder) tillämpas om uppgraderingen misslyckas. Enheten har en feltimer för uppgradering av fast programvara som aktiveras efter en misslyckad uppgradering av den fasta programvaran. Timern initieras med värdet i den här parametern. Nästa uppgradering av firmware uppstår när denna timer räknar ner till noll. Standardvärdet är 3 600 sekunder.

Parameternamn	Beskrivning och standardvärde
Upgrade Rule	Ett firmwareuppgraderingsskript som definierar uppgraderingsvillkor och tillhörande firmwareadresser. Den använder samma syntax som profilregeln. Använd följande format för att ange uppgraderingsregeln: **<tftp|http|https>://<ip-adress>/image/<inläsningsfilens namn>** Till exempel: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Om inget protokoll anges, antas TFTP. Om inget servernamn anges används värden som begär webbadressen som servernamn. Om ingen port anges används standardporten (69 för TFTP, 80 för HTTP och 443 för HTTPS). Värdet är tomt som standard.
Log Upgrade Request Msg	Syslog-meddelande som skickas vid början av ett firmware-uppgraderingsförsök. Standard: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Syslog-meddelande som utfärdas efter att ett lyckat firmwareuppgraderingsförsök har slutförts. Standardvärdet är `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg	Syslog-meddelande som utfärdas efter att ett misslyckat firmwareuppgraderingsförsök har slutförts. Standardvärdet är `$PN $MAC -- Upgrade failed: $ERR`
Peer Firmware Sharing	Aktiverar eller inaktiverar PFS-funktionen (Peer Firmware Sharing). Välj **Ja** eller **Nej** för att aktivera eller inaktivera funktionen. Standard: Ja
Peer Firmware Sharing Log Server	Anger IP-adressen och porten som UDP-meddelandet skickas till. Till exempel: 10.98.76.123:514 där 10.98.76.123 är IP-adressen och 514 är portnumret.

Allmänna parametrar

Följande tabell beskriver hur parametrarna i avsnittet **Allmänna parametrar** på fliken **Etablering** fungerar och används.

Parameternamn	Beskrivning och standardvärde
GPP A - GPP P	De allmänna GPP_*-parametrarna används som fria strängregister när telefonerna konfigureras för interaktion med en viss etableringsserverlösning. De kan konfigureras för att innehålla olika värden, bland annat följande: • Krypteringsnycklar. • Webbadresser. • Statusinformation för multietablering. • Postbegärandemallar. • Mappningar mellan parameternamn och alias. • Partiella strängvärden som så småningom kopplas ihop till kompletta parametervärden. Värdet är tomt som standard.

Variabler för makroexpandering

Vissa makrovariabler identifieras i följande etableringsparametrar:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (under särskilda omständigheter)

I dessa parametrar identifieras och expanderas syntaxtyper som $NAME eller $(NAME).

Understrängar i makrovariabler kan anges med notationen $(NAME:p) och $(NAME:p:q), där p och q är positiva heltal (tillgängligt i uppdatering 2.0.11 och senare). Den resulterande makroexpanderingen är delsträngen som börjar vid teckenförskjutning p, med längd q (eller till strängslutet om inte q har angetts). Om GPP_A exempelvis innehåller ABCDEF expanderar $(A:2) till CDEF och $(A:2:3) till CDE.

Ett okänt namn översätts inte och $NAME- eller $(NAME)-formatet ändras inte i parametervärdet efter expanderingen.

Parameternamn	Beskrivning och standardvärde
$	Formatet $$ expanderas till ett enda $-tecken.
A till och med P	Ersätts med innehållet i de allmänna parametrarna GPP_A till och med GPP_P.
SA till och med SD	Ersätts med specialparametrarna GPP_SA till och med GPP_SD. Dessa parametrar innehåller knappar eller lösenord som används i etableringen. **OBS!** $SA till och med $SD känns igen som argument för den valfria URL-kvalificeraren för omsynkronisering, --knapp.
MA	MAC-adress med gemena hexadecimala tecken, t.ex. 000e08aabbcc.
MAU	MAC-adress med versala hexadecimala tecken, t.ex. 000E08AABBCC.
MAC	MAC-adress med gemena hexadecimala tecken och kolon som avgränsar hexadecimala sifferpar. Till exempel 00:0e:08:aa:bb:cc.
PN	Produktnamn. Till exempel CP-6841-3PCC.
PSN	Produktserienummer. Till exempel 6841-3PCC.
SN	Serienummersträng. Till exempel 88012BA01234.
CCERT	SSL-klientcertifikatstatus: installerat eller inte installerat.
IP	Telefonens IP-adress i det lokala subnätet. Till exempel 192.168.1.100.
EXTIP	Telefonens externa IP-adress, så som den visas på Internet. Till exempel 66.43.16.52.
SWVER	Programvaruversionssträng. Till exempel sip68xx.11-0-1MPP.
HWVER	Maskinvaruversionssträng. Till exempel 2.0.1
PRVST	Etableringsstatus (en numerisk sträng): -1 = explicit omsynkroniseringsbegäran 0 = omsynkronisering vid start 1 = periodisk omsynkronisering 2 = omsynkronisering misslyckades, nytt försök

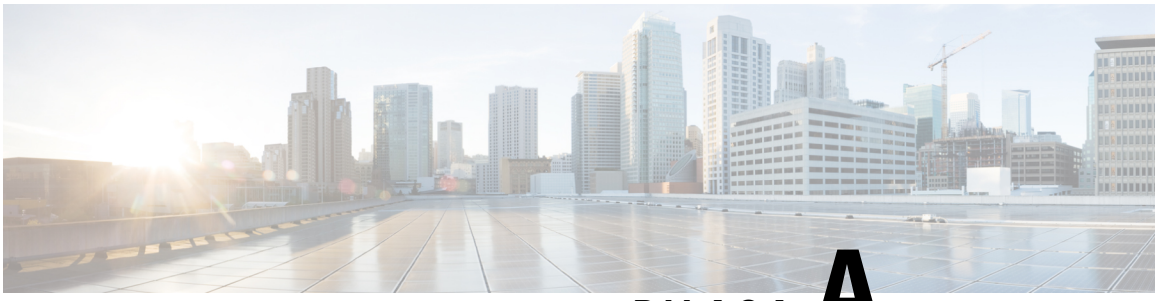
Parameternamn	Beskrivning och standardvärde
UPGST	Uppgraderingsstatus (en numerisk sträng): 1 = första uppgraderingsförsöket 2 = uppgradering misslyckades, nytt försök
UPGERR	Resultatmeddelande (ERR) för föregående uppgraderingsförsök, till exempel http_get misslyckades.
PRVTMR	Sekunder sedan senaste omsynkroniseringsförsök.
UPGTMR	Sekunder sedan senaste uppgraderingsförsök.
REGTMR1	Sekunder sedan linje 1 förlorade registrering hos SIP-servern.
REGTMR2	Sekunder sedan linje 2 förlorade registrering hos SIP-servern.
UPGCOND	Äldre makronamn.
SCHEME	Filåtkomstschemat (TFTP, HTTP eller HTTPS), så som det erhålls efter parsning av omsynkroniserings- eller uppgraderings-URL:en.
SERV	Begäran om målserverns värdnamn, så som det erhålls efter parsning av omsynkroniserings- eller uppgraderings-URL:en.
SERVIP	Begäran om målserverns IP-adress, så som den erhålls efter parsning av omsynkroniserings- eller uppgraderings-URL:en, möjligen efter en DNS-sökning.
PORT	Begäran om UDP-/TCP-målporten, så som den erhålls efter parsning av omsynkroniserings- eller uppgraderings-URL:en.
PATH	Begäran om målfilens sökväg, så som den erhålls efter parsning av omsynkroniserings- eller uppgraderings-URL:en.
ERR	Resultatmeddelande för omsynkroniserings- eller uppgraderingsförsök. Endast användbart vid generering av syslog-resultatmeddelanden. Värdet sparas i variabeln UPGERR vid uppgraderingsförsök.
UIDn	Innehållet i konfigurationsparametern Line n UserID.
EMS	Extension Mobility-status
MUID	Extension Mobility-användar-ID

Parameternamn	Beskrivning och standardvärde
MPWD	Extension Mobility-lösenord

Interna felkoder

Telefonen definierar ett antal interna felkoder (X00–X99) som gör det enklare att styra enhetens beteende i samband med vissa feltillstånd.

Parameternamn	Beskrivning och standardvärde
X00	Transportskiktsfel (eller ICMP-fel) när du skickar en SIP-begäran.
X20	Tidsgränsen för SIP-begäran går ut i väntan på ett svar.
X40	Allmänt SIP-protokollfel (till exempel ogiltig codec i SDP i 200 och ACK-meddelanden, eller timeout i väntan på ACK).
X60	Ogiltigt uppringt nummer enligt den angivna uppringningsplanen.



BILAGA A

Exempelkonfigurationsprofiler

Exempel 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>
```

Exempelkonfigurationsprofiler

```
<!--  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>
```

Exempelkonfigurationsprofiler

```
<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>
```

Exempelkonfigurationsprofiler

```
<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>
```

Exempelkonfigurationsprofiler

```
<!--
 available options:
-12|-11|-10|-9|-8|-7|-6|-5|-4|-3|-2|-1|0|1|2|3|4|5|6|7|8|9|10|11|12|13|14

-->
<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  -->
```

Exempelkonfigurationsprofiler

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

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

Exempelkonfigurationsprofiler

```
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_>
```

Exempelkonfigurationsprofiler

```
<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_>
```

Exempelkonfigurationsprofiler

```
<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_>
```

Exempelkonfigurationsprofiler

```
<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
-->
```

Exempelkonfigurationsprofiler

```
<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"/>
```

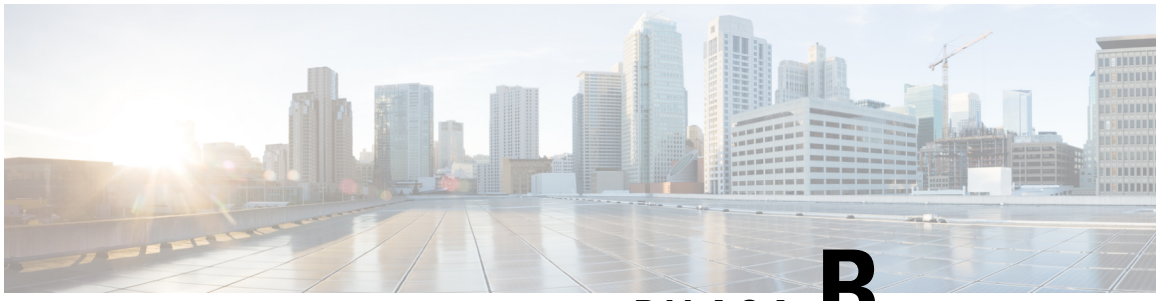
Exempelkonfigurationsprofiler

```
<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"/>
```

Exempelkonfigurationsprofiler

```
 <!--  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>
```



BILAGA B

Akronymer

Akronymer

AC	Växelström
ACS	Åtkomstkontrollserver
A/D	Analog till digital-omvandlare
AES	Advanced Encryption Standard
ANC	Anonymous Call (anonymt samtal)
Accesspunkt	Accesspunkt
ASCII	American Standard Code for Information Interchange
B2BUA	Back to Back User Agent (användaragent från slutpunkt till slutpunkt)
Lampfältet för Upptagen	Lampfältet för Upptagen
Bool	Booleska värden. Anges som yes och no, eller 1 och 0 i profilen
BootP	Bootstrap Protocol
CA	Certifikatsauktoritet
CAS	CPE Alert Signal
CDP	Cisco Discovery Protocol
CDR	Call Detail Record (post med samtalsdetaljer)
CGI	Datorgenererade bilder
CID	Samtals-ID

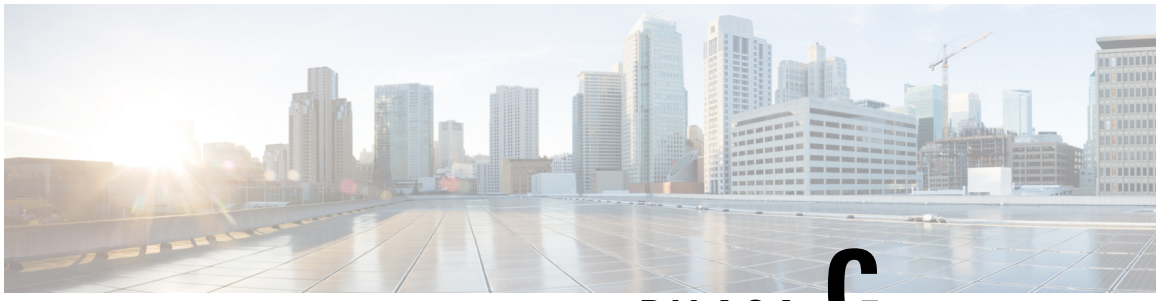
CIDCW	Call Waiting Caller ID (nummerpresentation för väntande samtal)
CNG	Comfort Noise Generation (generering av behagligt bakgrundsljud)
CPC	Calling Party Control (samtalskontroll för uppringande part)
CPE	Customer Premises Equipment (utrustning på kundens sida)
CSV	Kommaavgränsat värde
CWCID	Call Waiting Caller ID (nummerpresentation för väntande samtal)
CWT	Ton för samtal väntar
D/A	Digital till analog-omvandlare
dB	decibel
dBm	dB för 1 milliwatt
DHCP	Dynamic Host Configuration Protocol
Stör ej	Stör ej
DNS	DNS (Domain Name System)
DoS	Denial of Service
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Loop
DSP	Digital Signal Processor
SOMMARTID	Sommartid
DTAS	Data Terminal Alert Signal (samma som CAS)
DTMF	Dual Tone Multiple Frequency (tonval)
FQDN	Fully Qualified Domain Name (fullständigt kvalificerat domännamn)
FSK	Frequency Shift Keying (frekvensmodulering)
FW	fast programvara
FXS	Foreign eXchange Station
GMT	Greenwich Mean Time
GW	Gateway
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP över SSL

ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	Internetprotokoll version 4
IPv6	Internetprotokoll version 6
ISP	Internet Service Provider (Internetleverantör)
ITSP	Internet Telephony Service Provider (Internettelefonileverantör)
ITU	International Telecommunication Union
IVR	Interactive Voice Response
LAN	Local Area Network (lokalt nätverk)
LBR	Low Bit Rate (låg bitfrekvens)
LBRC	Low Bit Rate Codec
LCD	Flytande kristalldisplay; även kallat LCD-skärm
LDAP	Lightweight Directory Access Protocol
Lysdiod	LED
MAC-adressen	Åtkomstadress för mediakontroll
MC	Minicertifikat
MGCP	Media Gateway Control Protocol
MOH	Musik i vänteläge
MOS	Mean Opinion Score (mått på talkvalitet) (1–5, ju högre desto bättre)
MPP	Multiplattformstelefoner
ms	Millisekund
MSA	Music Source Adaptor (adapter för musikkälla)
MWI	Message Waiting Indication (indikator för väntande meddelande)
NAT	Adressöversättning
NPS	Normal etableringsserver
NTP	Nätverkstidsprotokoll
OOB	Out-of-band (utanför nätverket)

OSI	Open Switching Interval
PBX	Privat branschväxel
PCB	Printed Circuit Board (tryckt kretskort)
PoE	Power-over-Ethernet (PoE)
PR	Polarity Reversal (polaritetsväxling)
PS	Provisioning Server (etableringsserver)
PSQM	Perceptual Speech Quality Measurement (mått på perceptuell talkvalitet) (1–5, ju lägre desto bättre)
PSTN	Public Switched Telephone Network (publikt telenät)
QoS	Tjänstkvalitet
RC	Ta bort anpassning
REQT	(SIP) Request Message (förfrågningsmeddelande)
RESP	(SIP) Response Message (svarsmeddelande)
RSC	(SIP) Response Status Code (svarskod), t.ex. 404, 302, 600
RTP	Real Time Protocol
RTT	Round Trip Time (tidsfördröjning)
SAS	Streaming Audio Server (strömmande ljudserver)
SDP	Session Description Protocol
SDRAM	Synchronous DRAM
sek	sekunder
SIP	Session Initiation Protocol
SLA	Shared line appearance (utseende för delad linje)
SLIC	Subscriber Line Interface Circuit (krets för prenumerantens linjegränssnitt)
SP	Tjänsteleverantör
SSL	Secure Socket Layer
STUN	Sessions-överträdelse UDP för NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

TTL	Time to live
ToS	Typ av tjänst
UA	User Agent (användaragent)
uC	Mikrostyrenhet
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	UTC-tid
VAR	mervärdegivande återförsäljare
VLAN	Röst LAN
VM	Röstmeddelanden
VMWI	Visual Message Waiting Indication/Indicator (visuell indikator för väntande meddelande)
VoIP	Voice over Internetprotokoll
VQ	Röstkvalitet
WAN	Wide Area Network
XML	Extensible Markup Language

Akronymer



BILAGA C

Relaterad dokumentation

Relaterad dokumentation

Läs följande avsnitt om du vill ha mer relevant information.

Dokumentation för Cisco IP Phone 6800-serien

Se de publikationer som gäller för ditt språk, din telefonmodell och din version av den fasta multiplattformsprogramvaran. Navigera från följande 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

Supportpolicy för fast programvara för Cisco IP Phones

Information om supportpolicyn för telefoner finns i https://cisco.com/go/phonefirmwaresupport.