



Inrichtingshandleiding Cisco IP Phone 6800-serie voor meerdere platforms

Eerste publicatie: 2017-11-22

Laatste wijziging: 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 NON-INFRINGEMENT 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)

© 2019 Cisco Systems, Inc. Alle rechten voorbehouden.



INHOUD

HOOFDSTUK 1

Implementatie en inrichting 1

- Overzicht inrichting 1
- TR69-inrichting 3
 - RPC-methoden 3
 - Ondersteunde RPC-methoden 3
 - Ondersteunde gebeurtenistypen 4
 - Telefoongedrag tijdens netwerkcongestie 4
- Implementatie 4
 - Bulksgewijze distributie 4
 - Verkoopdistributie 5
 - Proces van hersynchronisatie 6
- Inrichten 6
 - Normale inrichtingserver 7
 - Toegangsbeheer configureren 7
 - Telefoonwebpagina openen 7
 - Webtoegang tot Cisco IP Phone toestaan 8
 - Communicatiecodering 8
 - Werkwijzen telefooninrichting 9
 - Handmatig een telefoon inrichten vanuit het toetsenblok 9
 - Peer firmware delen 9
 - Het scherm Wachtwoord instellen overslaan 10

HOOFDSTUK 2

Inrichtingscripts 13

- Inrichtingscripts 13
- Indelingen van het configuratieprofiel 13
 - Onderdelen van het configuratiebestand 14

Eigenschappen van de element-tag	14
Gebruikerstoegangattribuut	16
Toegangsbeheer	16
Parametereigenschappen	16
Indelingen van tekenreeksen	17
Compressie en codering van een open profiel (XML)	18
Compressie van een open profiel	18
Codering open profiel	18
AES-256-CBC-codering	19
HTTP-inhoudcodering op basis van RFC-8188	22
Argumenten voor optioneel hersynchroniseren	23
sleutel	23
uid en pwd (gebruikers-id en wachtwoord)	24
Een profiel toepassen op het IP-telefonie-apparaat	24
Het configuratiebestand downloaden naar de IP-telefoon vanuit een TFTP-server	24
Het configuratiebestand downloaden naar de telefoon met cURL	25
Inrichtingsparameters	25
Parameters voor algemene doeleinden	25
Gebruik parameters voor algemene doeleinden	26
Schakelt in	26
Actie	27
Hersynchroniseren op specifieke intervallen	27
Hersynchroniseren op een specifiek tijdstip	27
Configureerbare plannings	28
Profielregels	29
Upgrade Rule (Upgraderegel)	31
Gegevenstypen	32
Profielupdates en firmware-upgrades	35
Profielupdates toestaan en configureren	36
Firmware-upgrades toestaan en configureren	36
Firmware upgraden met TFTP, HTTP of HTTPS	36
Firmware upgraden met een browseropdracht	37

HOOFDSTUK 3 **Voorinrichting op kantoor en inrichtingsservers** 39

Voorinrichting op kantoor en inrichtingsservers	39
Servervoorbereiding en hulpprogramma's	39
RC-distributie (externe aanpassing)	40
Voorinrichting van apparaten op kantoor	41
Instellen van de inrichtingsserver	42
TFTP-inrichting	42
Extern eindpuntbeheer en NAT	42
HTTP-inrichting	43
HTTP-statuscode verwerken bij hersynchronisatie en upgraden	44
HTTPS-inrichting	45
Een ondertekend servercertificaat verkrijgen	46
CA-clientbasiscertificaat voor telefoons voor meerdere platforms	47
Redundante inrichtingsservers	48
Syslog-server	48

HOOFDSTUK 4
Voorbeelden van inrichting 49

Overzicht voorbeelden van inrichten	49
Standaard hersynchroniseren	49
Hersynchroniseren via TFTP	49
Syslog gebruiken om berichten op te slaan	50
Een apparaat automatisch hersynchroniseren	51
Unieke profielen, macro-uitbreiding en HTTP	52
Oefening: een specifiek IP-telefoonprofiel inrichten op een TFTP-server	53
Inrichten via Cisco XML	54
URL-oplossing met macro-uitbreiding	54
Hersynchroniseren via beveiligde HTTPS	55
Standaard hersynchroniseren via HTTPS	55
Oefening: standaard hersynchroniseren via HTTPS	56
HTTPS met clientcertificaatverificatie	57
Oefening: HTTPS met clientcertificaatverificatie	58
HTTPS-clientfiltering en dynamische inhoud	58
HTTPS-certificaten	59
HTTPS-methodologie	59
SSL-servercertificaat	60

Een servercertificaat verkrijgen	60
Clientcertificaat	61
Certificaatstructuur	61
Een aangepaste Certificate Authority configureren	62
Profielbeheer	63
Een open profiel met Gzip comprimeren	63
Een profiel coderen met OpenSSL	64
Gepartitioneerde profielen maken	65
Privacykopetekest telefoon instellen	66

HOOFDSTUK 5	Inrichtingsparameters	69
	Overzicht van inrichtingsparameters	69
	Configuratieprofielparameters	69
	Firmware-upgradeparameters	74
	Parameters voor algemene doeleinden	76
	Variabelen voor macro-uitbreiding	76
	Interne foutcodes	79

BIJLAGE A:	Voorbeeld configuratieprofielen	81
	Voorbeeld van open XML-indeling	81

BIJLAGE B:	Acroniemen	103
	Acroniemen	103

BIJLAGE C:	Verwante documentatie	109
	Verwante documentatie	109
	Documentatie van de Cisco IP Phone 6800-serie	109
	Ondersteuningsbeleid voor Cisco IP Phone-firmware	109



HOOFDSTUK 1

Implementatie en inrichting

- [Overzicht inrichting, op pagina 1](#)
- [TR69-inrichting, op pagina 3](#)
- [Telefoongedrag tijdens netwerkcongestie, op pagina 4](#)
- [Implementatie, op pagina 4](#)
- [Inrichten, op pagina 6](#)

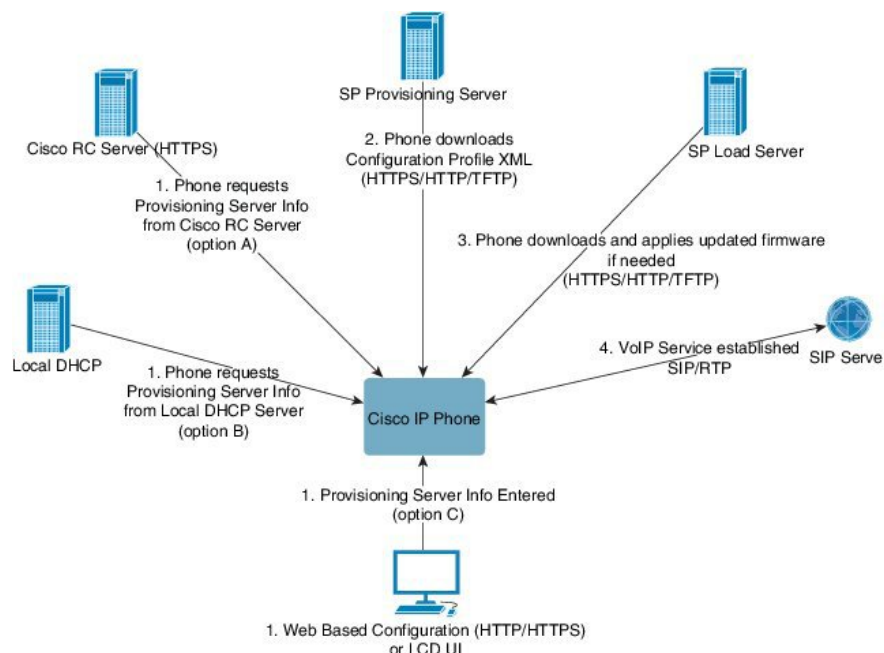
Overzicht inrichting

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

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

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

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



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

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

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

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

TR69-inrichting

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

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

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

RPC-methoden

Ondersteunde RPC-methoden

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

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

Ondersteunde gebeurtenistypen

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

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

Telefoongedrag tijdens netwerkcongestie

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

Implementatie

Cisco IP Phones bieden handige mechanismen voor inrichting, op basis van deze implementatiemodellen:

- Bulksgewijze distributie: de serviceprovider verwerft Cisco IP Phones in grote hoeveelheden en richt deze op locatie in of koopt RC-toestellen (Remote Customization) in bij Cisco. De apparaten worden vervolgens aan de klanten uitgegeven als onderdeel van een VoIP-serviceovereenkomst.
- Verkoopdistributie: de klant koopt de Cisco IP Phone bij een verkoper en vraagt de VoIP-service aan bij de serviceprovider. De serviceprovider moet vervolgens de beveiligde externe configuratie van het apparaat ondersteunen.

Bulksgewijze distributie

In dit model geeft de serviceprovider telefoons aan zijn klanten als onderdeel van een VoIP-serviceovereenkomst. De apparaten zijn ofwel RC-toestellen of intern vooringericht.

Cisco richt RC-toestellen vooraf in om te hersynchroniseren met een Cisco-server die het apparaatprofiel en de firmware-updates downloadt.

Een serviceprovider kan telefoons voorinrichten met de gewenste parameters, waaronder de parameters die hersynchronisatie beheren, op verschillende methoden:

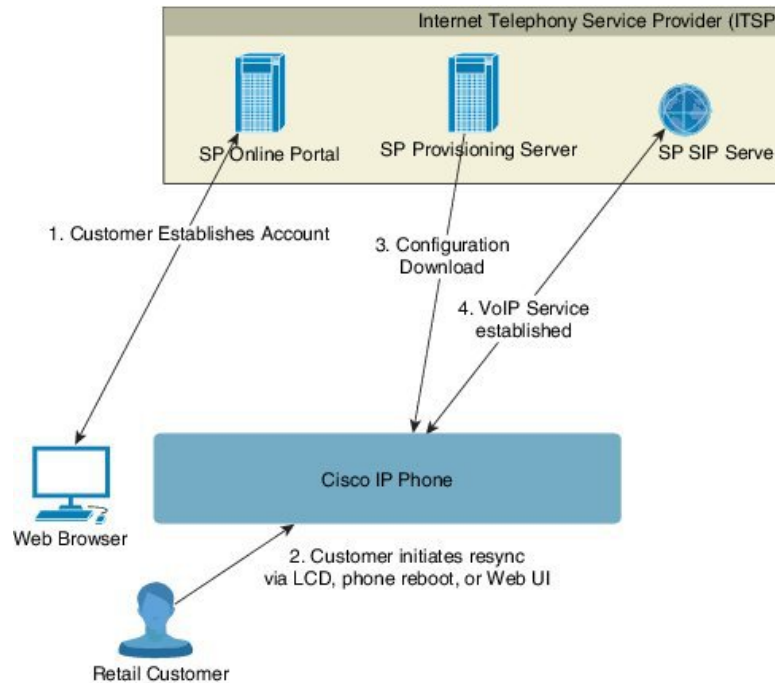
- Op kantoor met DHCP en TFTP
- Op afstand met TFTP, HTTP of HTTPS

- Een combinatie van interne en externe inrichting

Verkoopdistributie

Bij een verkoopdistributiemodel koopt een klant een telefoon en neemt deze een abonnement op een bepaalde service. De internettelefonie-serviceprovider (ITSP) stelt een inrichtingsserver in en onderhoudt deze, en richt de telefoon vooraf in om te hersynchroniseren met de server van de serviceprovider.

Figuur 1: Verkoopdistributie



De telefoon bevat het webgebaseerde configuratiehulpprogramma waarmee interne configuratie wordt weergegeven en nieuwe configuratieparameterwaarden worden geaccepteerd. De server accepteert ook een speciale URL-opdrachtsyntaxis voor het uitvoeren van externe hersynchronisatie van het profiel en firmware-upgrades.

De klant meldt zich aan bij de service en zorgt voor een VoIP-account, mogelijk via een online portal, en koppelt het apparaat aan het toegewezen serviceaccount. De niet-ingerichte telefoon wordt opgedragen om te hersynchroniseren met een specifieke inrichtingsserver via een URL-opdracht voor hersynchronisatie. De URL-opdracht bevat meestal een klant-id-nummer van een account of een alfanumerieke code, om het apparaat te koppelen met het nieuwe account.

In het volgende voorbeeld is een apparaat op het DHCP-toegewezen IP-adres 192.168.1.102 gevraagd om zichzelf in te richten naar de SuperVoIP-service:

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

In dit voorbeeld is 1234abcd het klant-id-nummer van het nieuwe account. De externe inrichtingsserver koppelt de telefoon die het verzoek voor hersynchroniseren uitvoert met het nieuwe account, op basis van de URL en de opgegeven klant-id. Via deze eerste hersynchronisatie wordt de telefoon in één stap geconfigureerd. De

telefoon wordt automatisch aangestuurd om vanaf dat moment te hersynchroniseren naar een permanente URL op de server. Bijvoorbeeld:

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

Voor zowel eerste als permanente toegang, is de inrichtingsserver voor verificatie afhankelijk van het clientcertificaat van de telefoon. De inrichtingsserver levert de juiste configuratieparameterwaarden op basis van het gekoppelde serviceaccount.

Wanneer het apparaat is ingeschakeld of wanneer een bepaalde periode is verstreken, wordt de telefoon gehersynchroniseerd en worden de meest recente parameters gedownload. Deze parameters kunnen doelen adresseren zoals het instellen van een zoekgroep, het instellen van snelkiesnummers en het beperken van de functies die een gebruiker kan wijzigen.

Verwante onderwerpen

[Voorinrichting van apparaten op kantoor](#), op pagina 41

Proces van hersynchronisatie

De firmware voor elke telefoon bevat een beheerwebserver die nieuwe configuratieparameterwaarden accepteert. De telefoon kan worden gevraagd de configuratie te hersynchroniseren na het opnieuw opstarten of op geplande intervallen, met een gespecificeerde inrichtingsserver via een URL-opdracht voor hersynchronisatie in het apparaatprofiel.

De webserver is standaard ingeschakeld. Als u de webserver in of uit wilt schakelen, gebruikt u de URL-opdracht voor hersynchronisatie.

Indien nodig kan direct hersynchroniseren worden verzocht via een actie-URL voor hersynchronisatie. De URL-opdracht voor hersynchronisatie kan een klant-id-nummer van een account of een alfanumerieke code bevatten, om het unieke apparaat te koppelen met het account van de gebruiker.

Voorbeeld

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

In dit voorbeeld is een apparaat op het DHCP-toegewezen IP-adres 192.168.1.102 gevraagd om zichzelf in te richten naar de SuperVoIP-service op prov.supervoip.com. Het klant-id-nummer van het nieuwe account is 1234abcd. De externe inrichtingsserver koppelt de telefoon die het verzoek voor hersynchronisatie uitvoert met het account, op basis van de URL en de klant-id.

Via deze eerste hersynchronisatie wordt de telefoon in één stap geconfigureerd. De telefoon wordt automatisch aangestuurd om vanaf dat moment te hersynchroniseren naar een permanente URL op de server.

Voor zowel eerste als permanente toegang, is de inrichtingsserver voor verificatie afhankelijk van het clientcertificaat. De server levert configuratieparameterwaarden op basis van het gekoppelde serviceaccount.

Inrichten

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

Standaard wordt een profiel alleen gehersynchroniseerd als de telefoon inactief is. Dit voorkomt dat de software door de upgrade opnieuw wordt opgestart en een gesprek wordt afgebroken. Als tussentijdse upgrades zijn

vereist om een actuele upgradestatus vanuit een oudere versie te bereiken, kan de upgradeloga getrapte upgrades automatiseren.

Normale inrichtingsserver

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

Hoewel HTTPS wordt aanbevolen, hoeft er bij communicatie met de NPS geen beveiligd protocol te worden gebruikt omdat het bijgewerkte profiel kan worden gecodeerd met een gedeelde geheime sleutel. Zie voor meer informatie over het gebruik van HTTPS [Communicatiecodering, op pagina 8](#). Beveiligde eerste inrichting wordt aangeboden via een mechanisme dat SSL-functionaliteit gebruikt. Een telefoon zonder inrichting kan een profiel dat is gecodeerd met een 256-bits symmetrische sleutel ontvangen dat aan dat apparaat is gericht.

Toegangsbeheer configureren

De firmware van de telefoon biedt methoden voor het beperken van eindgebruikerstoegang tot de enkele parameters. De firmware biedt specifieke bevoegdheden voor aanmelden bij een **beheerders**account of een **gebruikers**account. Elk kan onafhankelijk met een wachtwoord worden beveiligd.

- Beheerdersaccount: biedt de serviceprovider volledige toegang tot alle beheerwebserverparameters.
- Gebruikersaccount: biedt de gebruiker toegang om een selectie van de beheerwebserverparameters te configureren.

De serviceprovider kan het gebruikersaccount op de volgende manieren beperken in het inrichtingsprofiel:

- Aangeven welke configuratieparameters beschikbaar zijn voor het gebruikersaccount bij het maken van de configuratie.
- Gebruikerstoegang tot de beheerwebserver uitschakelen.
- Gebruikerstoegang tot de LCD-gebruikersinterface uitschakelen.
- Het scherm **Wachtwoord instellen** overslaan voor de gebruiker.
- De internetdomeinen beperken die door het worden apparaat geopend voor hersynchronisatie, upgrades of SIP-registratie voor lijn 1.

Verwante onderwerpen

[Eigenschappen van de element-tag](#), op pagina 14

[Toegangsbeheer](#), op pagina 16

Telefoonwebpagina openen

Open de webpagina van de telefoon via een webbrowser op een computer die de telefoon in het subnetwerk kan bereiken.

Als uw serviceprovider toegang tot het configuratiehulpprogramma heeft uitgeschakeld, neemt u contact op met de serviceprovider voordat u verder gaat.

Procedure

- Stap 1** Zorg ervoor dat de computer met de telefoon kan communiceren. Er is geen VPN in gebruik.
- Stap 2** Start een webbrowser.
- Stap 3** Voer het IP-adres van de telefoon op de adresbalk van uw webbrowser in.
- Gebruikerstoegang: **http://<ip-adres>/gebruiker**
 - Beheerderstoegang: **http://<ip-adres>/admin/geavanceerd**
 - Beheerderstoegang: **http://<ip-adres>**, klik op **Beheerdersaanmelding** en klik op **Geavanceerd**
- Bijvoorbeeld: `http://10.64.84.147/admin/`
-

Webtoegang tot Cisco IP Phone toestaan

Als u de telefoonparameters wilt bekijken, schakelt u het configuratieprofiel in. Als u wijzigingen wilt aanbrengen in een van de parameters, moet u het configuratieprofiel kunnen wijzigen. Uw systeembeheerder heeft de telefoonoptie om te lezen van en te schrijven naar de webgebruikersinterface van de telefoon mogelijk uitgeschakeld.

Zie voor meer informatie de *Inrichtingshandleiding voor Cisco IP Phone 6800-serie voor meerdere platforms*.

Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).

Procedure

- Stap 1** Klik op **Spraak > Systeem**.
- Stap 2** Stel in de sectie **Systeemconfiguratie Webserver inschakelen** in op **Ja**.
- Stap 3** Als u het configuratieprofiel wilt bijwerken, klikt u op **Alle wijzigingen verzenden** nadat u de velden in de webgebruikersinterface voor de telefoon hebt gewijzigd.
- De telefoon wordt opnieuw gestart en de wijzigingen worden toegepast.
- Stap 4** Als u alle in de huidige sessie aangebrachte wijzigingen wilt wissen (of nadat u voor het laatst hebt geklikt op **Alle wijzigingen verzenden**), klikt u op **Alle wijzigingen ongedaan maken**. Waarden worden weer op de vorige instellingen ingesteld.
-

Communicatiecodering

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

Werkwijzen telefooninrichting

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


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

Verwante onderwerpen

[Handmatig een telefoon inrichten vanuit het toetsenblok](#), op pagina 9

Handmatig een telefoon inrichten vanuit het toetsenblok

Procedure

- Stap 1** Druk op **Toepassingen** .
- Stap 2** Selecteer **Apparaatbeheer > Profielregel**.
- Stap 3** Voer de profielregel in met de volgende indeling:
- ```
protocol://server[:poort]/profile_pathname
```

Bijvoorbeeld:

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

Als er geen protocol wordt opgegeven, wordt TFTP verondersteld. Als er geen servernaam wordt opgegeven, wordt de host die de URL aanvraagt, gebruikt als de servernaam. Als er geen poort wordt opgegeven, wordt de standaardpoort gebruikt (69 voor TFTP, 80 voor HTTP of 443 voor HTTPS).

- Stap 4** Druk op **Opnieuw synchroniseren**.

### Verwante onderwerpen

[Werkwijzen telefooninrichting](#), op pagina 9

## Peer firmware delen

Peer firmware delen (PFS) is een firmwaredistributiemodel waarmee een Cisco IP Phone andere telefoons van hetzelfde model of uit dezelfde serie kan vinden op het subnet en de bijgewerkte firmwarebestanden daarmee kan delen als u meerdere telefoons tegelijk wilt upgraden. PFS maakt gebruik van het Cisco Peer-to-Peer-Distribution Protocol (CPPDP) dat een eigen protocol is van Cisco. Met CPPDP vormen alle apparaten in het subnet een peer-to-peer-hiërarchie zodat u firmware of andere bestanden van peerapparaten kunt kopiëren naar aangrenzende apparaten. Als u firmwareupgrades wilt optimaliseren, wordt de firmware-image van de laadserver gedownload op een hoofdtelefoon en vervolgens naar andere telefoons in het subnet overgebracht via TCP-verbindingen.

Peer firmware delen:

- Beperkt congestie in TFTP-overdrachten naar gecentraliseerde externe laadserver.

- Elimineert de vereiste om firmware-upgrades handmatig te beheren.
- Reduceert telefoonuitvaltijd tijdens upgrades wanneer grote aantallen telefoons gelijktijdig worden gereset.



#### Opmerking

- Peer firmware delen werkt alleen als meerdere telefoons op dezelfde tijd zijn ingesteld voor bijwerken. Wanneer een NOTIFY-melding wordt verzonden met Event:resync, wordt de telefoon opnieuw gesynchroniseerd. Voorbeeld van XML met configuraties voor het starten van de upgrade:  
**"Event:resync;profile="http://10.77.10.141/profile.xml**
- Wanneer u de PFS-logserver instelt op een IP-adres en poort, worden de specifieke PFS-logboeken naar die server verzonden als UDP-berichten. Deze instelling moet op elke telefoon worden uitgevoerd. U kunt de logboekberichten vervolgens gebruiken bij het oplossen van problemen met PFS.

Peer\_Firmware\_Sharing\_Log\_Server: hiermee geeft u de hostnaam en de poort op van de externe UDP-syslogserver. De poort is standaard ingesteld op de syslog 514.

Bijvoorbeeld:

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

Schakel PFS in op de telefoons als u deze functie wilt gebruiken.

## Het scherm Wachtwoord instellen overslaan

U kunt het scherm **Wachtwoord instellen** overslaan bij de eerste keer opstarten of na het terugzetten van fabrieksinstellingen, op basis van deze inrichtingsacties:

- DHCP-configuratie
- EDOS-configuratie
- Configuratie van gebruikerswachtwoord met het XML-configuratiebestand in de telefoon.

**Tabel 1: Inrichtingsacties die bepalen of het scherm Wachtwoord instellen wordt weergegeven**

| DHCP geconfigureerd | EDOS geconfigureerd | Gebruikerswachtwoord geconfigureerd | ScherM Wachtwoord instellen overslaan |
|---------------------|---------------------|-------------------------------------|---------------------------------------|
| Ja                  | n.v.t.              | Ja                                  | Ja                                    |
| Ja                  | n.v.t.              | Nee                                 | <b>Nee</b>                            |
| Nee                 | Ja                  | Ja                                  | Ja                                    |
| Nee                 | Ja                  | Nee                                 | <b>Nee</b>                            |
| Nee                 | Nee                 | n.v.t.                              | <b>Nee</b>                            |



## Procedure

---

- Stap 1** Bewerk het bestand `config.xml` van de telefoon in een tekst- of XML-editor.
- Stap 2** Voeg de tag `<User_Password>` in met een van deze opties.
- Geen wachtwoord (begin- en eindtag): `<User_Password></User_Password>`
  - Wachtwoordwaarde (4 tot 127 tekens): `<User_Password ua="rw">abc123</User_Password>`
  - Geen wachtwoord (alleen begintag): `<User_Password/>`
- Stap 3** Sla de wijzigingen in het `config.xml`-bestand op.
-





## HOOFDSTUK 2

# Inrichtingsscripts

---

- [Inrichtingsscripts](#), op pagina 13
- [Indelingen van het configuratieprofiel](#), op pagina 13
- [Compressie en codering van een open profiel \(XML\)](#), op pagina 18
- [Een profiel toepassen op het IP-telefonie-apparaat](#), op pagina 24
- [Inrichtingsparameters](#), op pagina 25
- [Gegevenstypen](#), op pagina 32
- [Profielupdates en firmware-upgrades](#), op pagina 35

## Inrichtingsscripts

De telefoon accepteert configuratie in een XML-indeling.

Raadpleeg voor meer informatie over uw telefoon de beheerhandleiding voor uw specifieke apparaat. Elke handleiding beschrijft de parameters die kunnen worden geconfigureerd via de beheerwebserver.

## Indelingen van het configuratieprofiel

Het configuratieprofiel definieert de parameterwaarden voor de telefoon.

De XML-indeling van het configuratieprofiel gebruikt standaard-XML-ontwerpprogramma's bij het samenstellen van de parameters en waarden.



---

### Opmerking

Alleen de tekenset UTF-8 wordt ondersteund. Als u het profiel in een editor wijzigt, wijzig dan niet de indeling voor de codering, anders kan de telefoon het bestand niet herkennen.

---

Elke telefoon heeft een andere functieset en daarom een andere set parameters.

### Profiel met XML-indeling (XML)

Het profiel met open indeling is een tekstbestand met een XML-achtige syntaxis in een hiërarchie van elementen, met elementattributen en waarden. Met deze indeling kunt u standaard hulpprogramma's gebruiken om het configuratiebestand te maken. Een configuratiebestand met deze indeling kan tijdens hersynchronisatie worden

verzonden vanaf de inrichtingsserver naar de telefoon. Het bestand kan worden verzonden zonder compilatie als een binair object.

De telefoon kan configuratie-indelingen accepteren die door standaard hulpprogramma's worden gegenereerd. Deze functie vereenvoudigt de ontwikkeling van de back-end software voor de inrichtingsserver waarmee configuratieprofielen worden gegenereerd uit bestaande databases.

Om vertrouwelijke informatie in het configuratieprofiel te beveiligen, levert de inrichtingsserver dit type bestand aan de telefoon via een kanaal dat is beveiligd met TLS. Het bestand kan optioneel worden gecomprimeerd met behulp van het gzip-verkleiningsalgoritme (RFC1951).

Het bestand kan met een van de volgende coderingsmethoden worden gecodeerd:

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

### Voorbeeld: open profiel indeling

```
<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>
```

De element-tag <flat-profile> sluit alle parameterelementen in die door de telefoon worden herkend.

### Verwante onderwerpen

[Compressie en codering van een open profiel \(XML\)](#), op pagina 18

## Onderdelen van het configuratiebestand

Een configuratiebestand kan deze onderdelen bevatten:

- Element-tags
- Attributen
- Parameters
- Functies voor het opmaken
- XML-opmerkingen

### Eigenschappen van de element-tag

- Met de XML-inrichtingsindeling en de webgebruikersinterface kunt u dezelfde instellingen configureren. De XML-tagnaam en de veldnamen in de webgebruikersinterface zijn vergelijkbaar, maar wijken af vanwege naambeperkingen voor XML-elementen. Bijvoorbeeld onderstrepingstekens ( \_ ) in plaats van " " .
- De telefoon herkent elementen met de juiste parameternamen die worden ingesloten in het speciale element <flat-profile>.

- Elementnamen worden tussen punthaken ingesloten.
- De meeste elementnamen zijn vergelijkbaar met de veldnamen op de beheerwebpagina's van het apparaat, met de volgende aanpassingen:

- Elementnamen mogen geen spaties of speciale tekens bevatten. Als u de elementnaam wilt afleiden van de veldnaam op de beheerpagina, kunt u elke spatie of de speciale tekens [ , ], ( , ) of / vervangen voor een laag streepje.

**Voorbeeld:** het element <Resync\_On\_Reset> staat voor het veld **Resync On Reset**.

- Elke elementnaam moet uniek zijn. Op de beheerwebpagina's kunnen dezelfde velden op meerdere webpagina's worden weergegeven, zoals de pagina's Lijn, Gebruiker en Toestelnummer. Voeg [n] toe aan de elementnaam om het nummer aan te geven dat wordt weergegeven in het tabblad van de pagina.

**Voorbeeld:** Het element <Dial\_Plan\_1\_> element staat voor het **Kiesplan** voor lijn 1.

- Elke openende element-tag moet een overeenkomende sluitende element-tag hebben. Bijvoorbeeld:

```
<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>
```

- Element-tags zijn hoofdlettergevoelig.
- Lege element-tags zijn toegestaan en worden geïnterpreteerd als dat ze de waarde configureren als leeg. Voer de openende element-tag in zonder corresponderende element-tag, en plaats een spatie en een slash voor het sluitende punthaakje (>). In dit voorbeeld is Profile Rule B (profielregel B) leeg:

```
<Profile_Rule_B />
```

- Een lege element-tag kan worden gebruikt om het overschrijven van een door de gebruiker opgegeven waarde te voorkomen tijdens hersynchronisatie. In het volgende voorbeeld blijven de gebruikersinstellingen voor snelkiesnummers ongewijzigd:

```
<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>
```

- Gebruik een lege waarde om de corresponderende parameter in te stellen op een lege tekenreeks. Voer een openend en sluitend element in zonder waarde ertussen. In het volgende voorbeeld wordt de parameter GPP\_A ingesteld op een lege tekenreeks.

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

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

- Niet-herkende elementnamen worden genegeerd.

### Verwante onderwerpen

[Toegangsbeheer configureren](#), op pagina 7

## Gebruikerstoegangattribuut

De besturingselementen voor het gebruikerstoegangattribuut (**ua**) kunnen worden gebruikt om toegang door het gebruikersaccount te wijzigen. Als het attribuut **ua** niet wordt gespecificeerd, wordt de bestaande instelling voor gebruikerstoegang behouden. Dit attribuut is niet van invloed op toegang door het beheerdersaccount.

Het attribuut **ua** moet een van de volgende waarden hebben:

- na: geen toegang
- ro: alleen-lezen
- rw: lezen/schrijven

In het volgende voorbeeld ziet u het attribuut **ua**:

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

U moet dubbele aanhalingstekens plaatsen rondom de waarde van de optie **ua**.

## Toegangsbeheer

Als de parameter <Phone-UI-User-Mode> is ingeschakeld, houdt de GUI van de telefoon zich aan het gebruikerstoegangsattribuut van de relevante parameters wanneer de GUI een menu-item toont.

Voor menu-items die zijn gekoppeld aan een enkele configuratieparameter:

- Inrichting van de parameter met het attribuut 'ua=na' ('ua' betekent 'gebruikerstoegang') zorgt ervoor dat het item verdwijnt.
- Wanneer u de parameter inricht met het attribuut 'ua=ro' is het item alleen-lezen en niet-bewerkbaar.

Voor menu-items die zijn gekoppeld aan meerdere configuratieparameters:

- Wanneer u alle betrokken parameters inricht met het attribuut 'ua=na' verdwijnen alle items.

### Verwante onderwerpen

[Toegangsbeheer configureren](#), op pagina 7

## Parametereigenschappen

Deze eigenschappen zijn van toepassing op de parameters:

- Eventuele parameters die niet door een profiel zijn gespecificeerd blijven ongewijzigd in de telefoon.
- Onbekende parameters worden genegeerd.

- Als het profiel met open indeling meerdere exemplaren van dezelfde parametertag bevat, overschrijft het laatste exemplaar de eerdere. Als u wilt voorkomen dat u per ongeluk configuratiewaarden van een parameter overschrijft, raden we aan dat elk profiel maximaal één instantie van een parameter specificeert.
- Het laatste profiel dat wordt verwerkt heeft voorrang. Als meerdere profielen dezelfde configuratieparameter specificeren, heeft de waarde van het laatste profiel voorrang.

## Indelingen van tekenreeksen

Deze eigenschappen zijn van toepassing op de indeling van de tekenreeksen:

- Opmerkingen zijn toegestaan met de standaard XML-syntaxis.  

```
<!-- My comment is typed here -->
```
- Een spatie voor- en achteraan is toegestaan voor leesbaarheid, maar wordt verwijderd uit de parameterwaarde.
- Nieuwe regels binnen een waarde worden omgezet tot spaties.
- Een XML-koptekst met de vorm `<? ?>` is toegestaan, maar wordt door de telefoon genegeerd.
- Als u speciale tekens wilt invoeren, dient u de standaard XML-tekennotering te gebruiken, zoals u kunt zien in de volgende tabel.

Speciaal teken	XML-tekenvolgorde
& (ampersand)	&
< (minder dan)	<
> (meer dan)	>
' (apostrof)	'
” (dubbele aanhalingstekens)	”

In het volgende voorbeeld wordt de tekennotering gebruikt voor de symbolen voor meer dan en minder dan, zoals vereist voor een kiesplanregel. Dit voorbeeld definieert een kiesplan voor een informatietelefoonlijn waarbij de parameter `<Dial_Plan_1_>` (**Beheerdersaanmelding > Geavanceerd > Spraak > Toestelnummer (n)**) wordt ingesteld op gelijk aan (`S0 <:18005551212>`).

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

- Numerieke tekennotering, met decimale en hexadecimale waarden (s.a. ( en .) worden omgezet.
- De firmware van de telefoon ondersteunt alleen ASCII-tekens.

# Compressie en codering van een open profiel (XML)

Het open configuratieprofiel kan worden gecomprimeerd als u de netwerkbelasting van de inrichtingsserver wilt verlagen. Het profiel kan ook worden gecodeerd om vertrouwelijke informatie te beschermen. Compressie is niet vereist, maar moet voorafgaan aan codering.

## Verwante onderwerpen

[Indelingen van het configuratieprofiel](#), op pagina 13

## Compressie van een open profiel

De ondersteunde compressiemethode is het gzip-verkleiningsalgoritme (RFC1951). Het hulpprogramma gzip en de compressiebibliotheek die hetzelfde algoritme implementeert (zlib) zijn beschikbaar via het internet.

Voor het identificeren van de compressie verwacht de telefoon dat het bestand een gzip-compatibele koptekst bevat. Wanneer het gzip-hulpprogramma wordt aangeroepen op het oorspronkelijke open profiel, wordt de koptekst gegenereerd. De telefoon controleert de gedownloade bestandskoptekst om de bestandsindeling te bepalen.

Bijvoorbeeld, als `profile.xml` een geldig profiel is, wordt het bestand `profile.xml.gz` ook geaccepteerd. Een van de volgende opdrachten kan dit profieltype genereren:

```
• >gzip profile.xml
```

Hiermee wordt het oorspronkelijke bestand vervangen door het gecomprimeerde bestand.

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

Hiermee blijft het oorspronkelijke bestand intact en wordt er een nieuw gecomprimeerd bestand gemaakt.

In de sectie [Een open profiel met Gzip comprimeren, op pagina 63](#) vindt u een uitleg over compressie.

## Verwante onderwerpen

[Een open profiel met Gzip comprimeren](#), op pagina 63

## Codering open profiel

Codering met een symmetrische sleutel kan worden gebruikt om een open configuratieprofiel te coderen, ongeacht of het bestand is gecomprimeerd of niet. Als er een compressie wordt toegepast, moet dit voor de codering gebeuren.

De inrichtingsserver werkt met HTTPS om de eerste inrichting van de telefoon af te handelen na implementatie. Vooraf offline coderen van configuratieprofielen zorgt ervoor dat HTTP later kan worden gebruikt om profielen te hersynchroniseren. Deze functie vermindert de belasting van de HTTPS-server bij grootschalige implementaties.

De telefoon ondersteunt twee coderingsmethoden voor configuratiebestanden:

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

De sleutel of Input Keying Material (IKM) moet op een eerder moment worden vooringericht op het apparaat. Bootstrap van de geheime sleutel kan via HTTPS veilig worden uitgevoerd.



De naam van het configuratiebestand vereist geen specifieke indeling, maar een bestandsnaam die eindigt met de extensie `.cfg` wijst doorgaans op een configuratieprofiel.

## AES-256-CBC-codering

De telefoon ondersteunt de AES-256-CBC-codering voor configuratiebestanden.

Het coderingshulpprogramma OpenSSL, te downloaden van verschillende internetsites, kan de codering uitvoeren. Voor ondersteuning van 256-bits AES-codering is mogelijk hercompilatie van het hulpprogramma nodig om de AES-code in te schakelen. De firmware is getest tegen versie openssl-0.9.7c.

[Een profiel coderen met OpenSSL, op pagina 64](#) biedt een uitleg over codering.

Voor een gecodeerd bestand verwacht het profiel dat het bestand dezelfde indeling heeft zoals gegenereerd door de volgende opdracht:

```
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
```

Een kleine letter `-k` gaat vooraf aan de geheime sleutel, die tekst zonder opmaak moet zijn, en deze wordt gebruikt voor het genereren van een willekeurige 64-bits salt. Met het geheim gespecificeerd door het `-k`-argument, kan het coderingshulpprogramma een willekeurige 128-bits initiële vector en de werkelijke 256-bits codeersleutel afleiden.

Wanneer deze vorm van codering wordt gebruikt voor een configuratieprofiel, moet de telefoon op de hoogte worden gesteld van de geheime sleutelwaarde om het bestand te decoderen. Deze waarde wordt gespecificeerd als een kwalificatie in de URL van het profiel. De syntaxis is als volgt, met een expliciete URL:

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

Deze waarde wordt geprogrammeerd met behulp van één van de parameters `Profile_Rule`.

### Verwante onderwerpen

[Een profiel coderen met OpenSSL, op pagina 64](#)

## Uitbreiding van macro

Verskillende inrichtingsparameters ondergaan interne macro-uitbreiding voordat ze worden geëvalueerd. Deze stap voor evaluatie biedt meer flexibiliteit bij het beheren van de hersynchronisatie- en upgrade-activiteiten van de telefoon.

Deze parametergroepen ondergaan macro-uitbreiding voorafgaand aan evaluatie:

- `Resync_Trigger_*`
- `Profile_Rule*`
- `Log_xxx_Msg`
- `Upgrade_Rule`

Onder bepaalde omstandigheden ondergaan enkele parameters voor algemene doeleinden (GPP\_\*) ook macro-uitbreiding. Dit is expliciet aangegeven in [Argumenten voor optioneel hersynchroniseren, op pagina 23](#).

De inhoud van de benoemde variabelen vervangt tijdens macro-uitbreiding de expressies met de vorm \$NAME en \$(NAME). Deze variabelen zijn onder andere parameters voor algemene doeleinden, verschillende product-id's, bepaalde gebeurtenis timers en statuswaarden voor inrichting. Zie voor een volledige lijst [Variabelen voor macro-uitbreiding, op pagina 76](#).

In het volgende voorbeeld wordt de uitdrukking \$(MAU) gebruikt om het MAC-adres 000E08012345 in te voegen.

De beheerder voert het volgende in: **\$ (MAU) config.cfg**

De resulterende macro-uitbreiding voor een apparaat met MAC-adres 000E08012345 is:  
000E08012345config.cfg

Als de macronaam niet wordt herkend, blijft het niet-uitgebreid. De naam STRANGE wordt bijvoorbeeld niet herkend als een geldige macronaam, terwijl MAU wordt herkend als een geldige macronaam.

De beheerder voert het volgende in: **\$STRANGE\$MAU.cfg**

De resulterende macro-uitbreiding voor een apparaat met MAC-adres 000E08012345 is:  
\$STRANGE000E08012345.cfg

Macro-uitbreiding wordt niet recursief toegepast. Bijvoorbeeld, "\$MAU" wordt uitgebreid naar "\$MAU" (de "\$" wordt uitgebreid), en leidt niet tot het MAC-adres.

De inhoud van de parameters voor speciale doeleinden, GPP\_SA tot GPP\_SD, zijn toegewezen aan de macro-expressies \$SA tot \$SD. Deze parameters worden alleen macro-uitgebreid als het argument van de opties **--key**, **--uid** en **--pwd** in een URL voor hersynchronisatie.

## Voorwaardelijke expressies

Voorwaardelijke expressies kunnen hersynchronisatie activeren en selecteren uit alternatieve URL's voor hersynchronisatie- en upgradebewerkingen.

Voorwaardelijke expressies bestaan uit een lijst met vergelijkingen, gescheiden door de **en**-operator. Alle vergelijkingen moeten worden voldaan, anders is de voorwaarde niet waar.

Elke vergelijking kan betrekking hebben tot een van de volgende drie soorten letterlijke waarden:

- Integerwaarden
- Software- of hardwareversienummers
- Tekenreeksen met dubbele aanhalingstekens

### Versienummers

De formeel uitgebrachte softwareversie van telefoons voor meerdere platforms (MPP) gebruikt deze indeling, waarbij BN staat voor Build Number:

- Cisco IP Phone 6800-serie: sip68xx.v1-v2-v3MPP-BN

De vergelijkende tekenreeks moet dezelfde indeling gebruiken. Anders ontstaat er een fout bij het parseren van de indeling.

In de softwareversie kan v1-v2-v3-v4 verschillende cijfers en tekens specificeren, maar het moet beginnen met een numeriek cijfer. Wanneer u de softwareversie vergelijkt, wordt v1-v2-v3-v4 op volgorde vergeleken. De meest linkse cijfers hebben voorrang op de latere.

Als v[x] alleen numerieke cijfers bevat, worden de cijfers vergeleken; als v[x] numerieke cijfers + alfanumerieke tekens bevat, worden de cijfers eerst vergeleken en worden de tekens vervolgens in alfabetische volgorde vergeleken.

### Voorbeeld van een geldig versienummer

sipywww.11-0-0MPP-BN

Daarentegen: 11.0.0 is een ongeldige indeling.

### Vergelijking

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

Tekenreeksen tussen aanhalingstekens kunnen worden vergeleken voor gelijkheid of ongelijkheid. Gehele getallen en versienummers kunnen ook rekenkundig worden vergeleken. De vergelijkingsoperators kunnen worden uitgedrukt als symbolen of acroniemen. Acroniemen zijn handig om de voorwaarde in een profiel met open indeling uit te drukken.

Operator	Alternatieve syntaxis	Beschrijving	Van toepassing op gehele getallen en versie-operanden	Van toepassing op operanden met een tekenreeks tussen aanhalingstekens
=	eq	gelijk aan	Ja	Ja
!=	ne	niet gelijk aan	Ja	Ja
<	lt	minder dan	Ja	Nee
<=	le	minder dan of gelijk aan	Ja	Nee
>	gt	meer dan	Ja	Nee
>=	ge	meer dan of gelijk aan	Ja	Nee
EN		en	Ja	Ja

Het is belangrijk om macrovariabelen tussen dubbele aanhalingstekens te plaatsen wanneer een letterlijke tekenreeks wordt verwacht. Doe dit niet wanneer er een nummer of versienummer wordt verwacht.

In de context van de parameters Profile\_Rule\* en Upgrade\_Rule, moeten voorwaardelijke expressies binnen de syntaxis "(expr)?" worden geplaatst, zoals in dit voorbeeld van de upgraderegel. Houd er rekening mee dat BN voor Build Number staat.

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

Gebruik de voorafgaande syntaxis tussen haakjes niet om de parameters `Resync_Trigger_*` te configureren.

## URL-syntaxis

Gebruik de standaard URL-syntaxis om te specificeren hoe configuratiebestanden en firmwareversies moeten worden opgehaald in de parameters `Profile_Rule*` en `Upgrade_Rule`. De syntaxis is als volgt:

```
[schema://] [server [:poort]] bestandspad
```

Hierbij is **schema** een van deze waarden:

- tftp
- http
- https

Als **schema** niet is opgegeven, wordt tftp aangenomen. De server kan een hostnaam met DNS-herkenning of een numeriek IP-adres zijn. De poort is de bestemmings-UDP of het TCP-poortnummer. Het bestandspad moet beginnen met de hoofdmap (/). Dit moet een absoluut pad zijn.

Als **server** ontbreekt, wordt de tftp-server die is gespecificeerd via DHCP (optie 66) gebruikt.



### Opmerking

Voor upgraderegels moet de server worden opgegeven.

Als **poort** ontbreekt, wordt de standaardpoort voor het gespecificeerde schema gebruikt. Tftp gebruikt UDP-poort 69, http gebruikt TCP-poort 80, https gebruikt TCP-poort 443.

Er moet een bestandspad aanwezig zijn. Het moet niet noodzakelijk verwijzen naar een statisch bestand, maar kan ook dynamische inhoud aangeven die is verkregen via CGI.

Macro-uitbreiding is van toepassing binnen de URL's. Hieronder ziet u voorbeelden van geldige URL's:

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

Als u DHCP-optie 66 gebruikt, wordt lege syntaxis nu niet ondersteund door upgraderegels. Dit is alleen van toepassing op Profile Rule\*.

## HTTP-inhoudcodering op basis van RFC-8188

De telefoon ondersteunt de HTTP-inhoudcodering op basis van RFC 8188 met AES-128-GCM ciphering voor configuratiebestanden. Met deze coderingsmethode kan elke entiteit de HTTP-berichtkoppen lezen. Alleen de entiteiten die het Input Keying Material (IKM) kennen, kunnen echter de kern lezen. Wanneer de telefoon is ingericht met het IKM, kunnen de telefoon en de inrichtende server veilig configuratiebestanden uitwisselen, terwijl ze het voor derde netwerkelementen mogelijk maken om de berichtkoppen te gebruiken voor analyse- en monitoringdoeleinden.

De XML-configuratieparameter **IKM\_HTTP\_Encrypt\_Content** bevat het IKM op de telefoon. Deze parameter is om veiligheidsredenen niet toegankelijk op de telefoonbeheerwebpagina. Hij is ook niet zichtbaar

in het configuratiebestand van de telefoon dat u kunt bereiken via het IP-adres van de telefoon of via de configuratierapporten van de telefoon die naar de inrichtende server zijn gestuurd.

Als u de codering op basis van RFC 8188 wilt gebruiken, moet u de volgende zaken garanderen:

- Richt de telefoon in met het IKM door het IKM op te geven met de XML-parameter **IKM\_HTTP\_Encrypt\_Content** in het configuratiebestand dat van de inrichtende server naar de telefoon wordt gestuurd.
- Als deze codering wordt toegepast op de configuratiebestanden die van de inrichtende server naar de telefoon worden gestuurd, garandeer dan dat de HTTP-kop *Inhoudcodering* in het configuratiebestand "aes128gcm" aangeeft.

Als deze kop ontbreekt, krijgt de methode van AES-256-CBC voorrang. De telefoon past de AES-256-CBC-codering toe als er een AES-256-CBC-sleutel aanwezig is in een profielregel, ongeacht het IKM.

- Als u wilt dat de telefoon deze codering toepast op de configuratierapporten die het naar de inrichtende server stuurt, garandeer dan dat er geen AES-256-CBC-sleutel in de rapportregel is opgegeven.

## Argumenten voor optioneel hersynchroniseren

Optionele argumenten, **sleutel**, **gebruikers-id** en **wachtwoord**, kunnen voorafgaan aan de URL's die worden ingevoerd in Profile\_Rule\*-parameters, gezamenlijk ingesloten door vierkante haken.

### sleutel

De optie **--sleutel** vertelt de telefoon dat het ontvangen configuratiebestand van de inrichtende server is gecodeerd met de AES-256-CBC-codering tenzij de kop *Inhoudcodering* in het bestand de codering "aes128gcm" aangeeft. De sleutel zelf wordt opgegeven als een tekenreeks na de term **--sleutel**. De sleutel kan optioneel tussen dubbele aanhalingstekens (") worden geplaatst. De telefoon gebruikt de sleutel om het configuratiebestand te decoderen.

### Gebruiksvoorbeelden

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

De optionele argumenten tussen haakjes zijn macro-uitgebreid. Parameters voor speciale doeleinden, GPP\_SA tot GPP\_SD, worden macro-uitgebreid tot macro-variabelen \$SA tot \$SD, maar alleen wanneer ze worden gebruikt als sleuteloptie-argumenten. Zie de volgende voorbeelden:

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

In profielen met open indeling moet het argument voor **--key** hetzelfde zijn als het argument voor de optie **-k** die wordt toegekend aan **openssl**.

## uid en pwd (gebruikers-id en wachtwoord)

De opties **uid** en **pwd** kunnen worden gebruikt om gebruikersnaam- en wachtwoord-verificatie te specificeren voor de opgegeven URL. De optionele argumenten tussen haakjes zijn macro-uitgebreid. Parameters voor speciale doeleinden, GPP\_SA tot GPP\_SD, worden macro-uitgebreid tot macro-variabelen \$SA tot \$SD, maar alleen wanneer ze worden gebruikt als sleuteloptie-argumenten. Zie de volgende voorbeelden:

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

```
[--uid $SA -pwd $SB] https://inrichtingsserver_url/pad_naar_uw_config/uw_config.xml
```

wordt vervolgens uitgebreid naar:

```
[--uid MijnGebruikers-id -$SA -pwdMijnGeheimeWachtwoord]
https://inrichtingsserver_url/pad_naar_uw_config/uw_config.xml
```

## Een profiel toepassen op het IP-telefonie-apparaat

Nadat u een XML-configuratiescript hebt gemaakt, moet dit worden doorgegeven aan de telefoon voor toepassing. Als u de configuratie wilt toepassen, kunt u het configuratiebestand downloaden naar de telefoon vanaf een TFTP-, HTTP- of HTTPS-server via een webbrowser of met behulp van het hulpprogramma met de cURL-opdrachtregel.

## Het configuratiebestand downloaden naar de IP-telefoon vanuit een TFTP-server

Voltooi deze stappen om het configuratiebestand te downloaden naar aan TFTP-servertoepassing op uw computer.

### Procedure

- 
- Stap 1** Sluit uw computer aan op het LAN van de telefoon.
  - Stap 2** Voer een TFTP-servertoepassing uit op de computer en zorg ervoor dat het configuratiebestand beschikbaar is in de TFTP-hoofdmap.
  - Stap 3** Voer vanuit een webbrowser het LAN-IP-adres van de telefoon, het IP-adres van de computer, de bestandsnaam en de aanmeldingsgegevens in. Gebruik deze indeling:

```
http://<WAN_IP_adres>/admin/resync?tftp://<PC_IP_adres>/<bestandsnaam>&user=admin&password=<wachtwoord>
```

Voorbeeld:

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

---

## Het configuratiebestand downloaden naar de telefoon met cURL

Voer de volgende stappen uit om de configuratie naar de telefoon te downloaden met behulp van cURL. Dit opdrachtregelhulpprogramma wordt gebruikt om gegevens over te dragen met een URL-syntaxis. Als u cURL wilt downloaden, gaat u naar:

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



### Opmerking

We raden aan dat u cURL niet gebruikt om de configuratie naar de telefoon te verzenden, omdat de gebruikersnaam en het wachtwoord kunnen worden vastgelegd als u cURL gebruikt.

### Procedure

#### Stap 1

Sluit uw computer aan op de LAN-poort van de telefoon.

#### Stap 2

Download het configuratiebestand naar de telefoon door de volgende cURL-opdracht in te voeren:

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

## Inrichtingsparameters

Deze sectie beschrijft de inrichtingsparameter op volgorde van functie:

Deze typen inrichtingsparameters bestaan:

- Algemene doeleinden
- Schakelt in
- Actie
- Configureerbare planningen
- Profielregels
- Upgrade Rule (Upgraderegel)

## Parameters voor algemene doeleinden

De GPP\_\*-parameters voor algemene doeleinden (**Beheerdersaanmelding > Geavanceerd > Spraak > Inrichting**) worden gebruikt als vrije tekenreeks en worden geregistreerd bij het configureren van telefoon om met een bepaalde inrichtingsserveroplossing te werken. De GPP\_\*-parameters zijn standaard leeg. Ze kunnen zo worden geconfigureerd dat ze diverse waarden bevatten, zoals de volgende:

- Coderingsleutels
- URL's

- Statusinformatie voor inrichting met meerdere fasen
- Plaatsingsaanvraagjablonen
- Parameternaamaliastoewijzingen
- Gedeeltelijke tekenreekswaarden, uiteindelijk gecombineerd in complete parameterwaarden.

De parameters GPP\_\* zijn beschikbaar voor macro-uitbreiding binnen andere inrichtingsparameters. Voor dit doel zijn macronamen met één hoofdletter (A tot P) voldoende om de inhoud van GPP\_A tot GPP\_P te identificeren. De macronamen met twee hoofdletters, SA tot SD, identificeren bovendien GPP\_SA tot GPP\_SD als een speciaal geval wanneer deze worden gebruikt als argumenten van de volgende URL-opties:

#### key, uid en pwd

Deze parameters kunnen worden gebruikt als variabelen in inrichtings- en upgraderegels. Er wordt naar verwezen door een '\$'-teken toe te voegen voorafgaand aan de variabele naam, zoals \$GPP\_A.

## Gebruik parameters voor algemene doeleinden

Bijvoorbeeld, als GPP\_A de tekenreeks ABC bevat en GPP\_B bevat 123, zorgt de uitdrukking \$A\$B voor een macro-uitbreiding tot ABC123.

#### Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).

#### Procedure

- 
- Stap 1** Selecteer **Spraak > Inrichting**.
  - Stap 2** Blader naar de sectie **Parameters voor algemene doeleinden**.
  - Stap 3** Voer geldige waarden in voor de velden GPP A tot GPP P.
  - Stap 4** Klik op **Alle wijzigingen verzenden**.
- 

## Schakelt in

Met de parameters Provision\_Enable en Upgrade\_Enable worden alle bewerkingen voor profielhersynchronisatie en firmware-upgrade beheerd. Deze parameters beheren hersynchronisaties en upgrades onafhankelijk van elkaar. Deze parameters beheren ook URL-opdrachten voor hersynchronisatie en upgrades die worden uitgegeven via de beheerwebserver. Beide van deze parameters zijn standaard ingesteld op **Ja**.

De parameter Resync\_From\_SIP bepaalt verzoeken voor hersynchronisatie. Een SIP NOTIFY-gebeurtenis wordt vanuit de proxyserver van de serviceprovider naar de telefoon verzonden. Indien ingeschakeld kan de proxy een hersynchronisatie verzoeken. Hiervoor verzendt de proxy een SIP NOTIFY-bericht met 'Gebeurtenis: koptekst hersynchroniseren' naar het apparaat.

Het apparaat daagt het verzoek uit met een 401-antwoord (autorisatie geweigerd voor gebruikte referenties). Het apparaat verwacht een geverifieerd volgend verzoek voordat deze het verzoek tot hersynchronisatie van de proxy inwilligt. De kopteksten 'Gebeurtenis: reboot\_now' en 'Gebeurtenis: restart\_now' voeren koud en warm opnieuw opstarten uit, en worden ook uitgedaagd.



De twee overgebleven inschakelbare parameters zijn `Resync_On_Reset` en `Resync_After_Upgrade_Attempt`. Deze parameters bepalen of een apparaat hersynchroniseert na software opnieuw opstarten en na elke upgradepoging.

Als `Resync_On_Reset` is ingeschakeld, introduceert het apparaat een willekeurige vertraging die de opstartprocedure opvolgt voordat het opnieuw instellen wordt uitgevoerd. De vertraging is een willekeurige tijd tot maximaal de waarde die wordt gespecificeerd door `Resync_Random_Delay` (in seconden). In een pool met telefoons die tegelijkertijd opstarten, verspreidt deze vertraging de begintijd van de verzoeken tot hersynchronisatie van elk toestel. Deze functie kan handig zijn in een grote huisinstallatie, in het geval van een regionale stroomstoring.

## Actie

Met de telefoon kunt u op specifieke intervallen of op een bepaald tijdstip hersynchroniseren.

### Hersynchroniseren op specifieke intervallen

De telefoon is ontworpen om periodiek met de inrichtingsserver te hersynchroniseren. Het hersynchronisatie-interval wordt geconfigureerd in `Resync_Periodic` (seconden). Als deze waarde leeg wordt gelaten, hersynchroniseert het apparaat niet periodiek.

De hersynchronisatie vindt meestal plaats wanneer de spraaklijnen inactief zijn. Wanneer een spraaklijn actief is wanneer een hersynchronisatie moet plaatsvinden, vertraagt de telefoon de hersynchronisatieprocedure tot de lijn weer inactief wordt. Door een hersynchronisatie kunnen waarden van configuratieparameters worden veranderd.

Een hersynchronisatie kan mislukken omdat de telefoon een profiel niet kan ophalen van de server, omdat het gedownloade bestand corrupt is of omdat er een interne fout is opgetreden. Het apparaat probeert opnieuw te hersynchroniseren na de tijd die is gespecificeerd in `Resync_Error_Retry_Delay` (seconden). Als `Resync_Error_Retry_Delay` is ingesteld op 0, probeert het apparaat niet nogmaals te hersynchroniseren na een mislukte hersynchronisatiepoging.

Als een upgrade mislukt, wordt dit opnieuw geprobeerd na het aantal seconden dat is gespecificeerd met `Upgrade_Error_Retry_Delay`.

Er zijn twee configureerbare parameters beschikbaar om onder bepaalde voorwaarden een hersynchronisatie te veroorzaken: `Resync_Trigger_1` en `Resync_Trigger_2`. Elke parameter kan worden geprogrammeerd met een voorwaardelijke expressie die macro-uitbreiding ondergaat. Wanneer het hersynchronisatie-interval verloopt (de tijd tot de volgende hersynchronisatie) voorkomen deze parameters, indien ingesteld, de hersynchronisatie tenzij één of meerdere voorwaarden als waar wordt geëvalueerd.

In het volgende voorbeeld wordt er bij de voorwaarde een hersynchronisatie veroorzaakt. In het voorbeeld is de laatste poging om de telefoon te upgraden meer dan 5 minuten geleden (300 seconden) en is er tenminste 10 minuten (600 seconden) verstreken sinds de laatste hersynchronisatiepoging.

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

### Hersynchroniseren op een specifiek tijdstip

Met de parameter `Resync_At` kan de telefoon op een bepaald tijdstip hersynchroniseren. Deze parameter gebruikt de 24-uursnotatie (uumm) om de tijd te specificeren.

Met de parameter `Resync_At_Random_Delay` kan de telefoon op een niet-gespecificeerde vertraging in de tijd hersynchroniseren. Deze parameter gebruikt een positief geheel getal om de tijd te specificeren.

Overbelasting van de server met verzoeken voor hersynchronisatie van meerdere telefoons die zijn ingesteld om op dezelfde tijd te hersynchroniseren moet worden vermeden. Daarom zal de telefoon de hersynchronisatie tot 10 minuten na de gespecificeerde tijd activeren.

Bijvoorbeeld, als u de tijd voor hersynchronisatie instelt op 1000 (10:00 uur), activeert de telefoon de hersynchronisatie ergens tussen 10:00 en 10:10 uur.

Deze functie is standaard uitgeschakeld. Wanneer de parameter `Resync_At` wordt ingericht, wordt de parameter `Resync_Periodic` genegeerd.

## Configureerbare planningen

U kunt planningen voor periodiek hersynchroniseren configureren en u kunt de intervallen voor opnieuw proberen voor hersynchronisatie- en upgradefouten opgeven via deze inrichtingsparameters:

- `Resync_Periodic` (Periodiek hersynchroniseren)
- `Resync_Error_Retry_Delay` (Vertraging nieuwe poging na hersynchronisatiefout)
- `Upgrade_Error_Retry_Delay` (Vertraging nieuwe poging na upgradefout)

Elke parameter accepteert een enkele vertragingsswaarde (seconden). De nieuwe uitgebreide syntaxis maakt het mogelijk om een door komma's gescheiden lijst met opeenvolgende vertragingselementen te maken. Het laatste element in de reeks wordt impliciet eindeloos herhaald.

Indien gewenst, kunt u een plussteken (+) gebruiken om een andere numerieke waarde te specificeren die als een willekeurige extra vertraging wordt toegevoegd.

### Voorbeeld 1

In dit voorbeeld hersynchroniseert de telefoon regelmatig elke 2 uur. Als er een fout bij hersynchroniseren optreedt, probeert het apparaat het met deze intervallen opnieuw: 30 minuten, 1 uur, 2 uur, 4 uur. Het apparaat blijft het met intervallen van 4 uur proberen totdat het met succes hersynchroniseert.

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

### Voorbeeld 2

In dit voorbeeld hersynchroniseert het apparaat regelmatig elk uur (plus een extra willekeurige vertraging van maximaal 10 minuten). In het geval van een fout bij hersynchroniseren, probeert het apparaat het opnieuw met deze intervallen: 30 minuten (plus maximaal 5 minuten), 1 uur (plus maximaal 10 minuten), 2 uur (plus maximaal 15 minuten). Het apparaat blijft het met intervallen van 2 uur proberen (plus maximaal 15 minuten) totdat het met succes hersynchroniseert.

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

### Voorbeeld 3

In dit voorbeeld, als een externe upgrade mislukt, probeert het apparaat de upgrade opnieuw na 30 minuten, vervolgens na één uur, vervolgens na twee uur. Als de upgrade nog steeds mislukt, probeert het apparaat dit opnieuw elke vier tot vijf uur totdat de upgrade is gelukt.

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

## Profielregels

De telefoon biedt meerdere profielparameters voor externe configuratie (Profile\_Rule\*). Daardoor kunnen met elke hersynchronisatiebewerking meerdere bestanden worden opgehaald die door verschillende servers worden beheerd.

In het meeste eenvoudige scenario hersynchroniseert het apparaat periodiek naar een enkel profiel op een centrale server, waarmee alle belangrijke interne parameters worden bijgewerkt. Een profiel kan ook worden opgesplitst tussen verschillende bestanden. Eén bestand is gemeenschappelijk voor alle telefoons in een implementatie. Een ander, uniek bestand wordt aangeboden voor elk account. Coderings sleutels en certificaatinformatie kan door weer een ander profiel worden aangeboden, opgeslagen op een afzonderlijke server.

Wanneer er een hersynchronisatie moet worden uitgevoerd, evalueert de telefoon de vier Profile\_Rule\*-parameters op volgorde:

1. Profile\_Rule
2. Profile\_Rule\_B
3. Profile\_Rule\_C
4. Profile\_Rule\_D

Elke evaluatie kan resulteren in het ophalen van een profiel van een externe inrichtingsserver, met een mogelijke update van een aantal interne parameters. Als een evaluatie mislukt, wordt de hersynchronisatie onderbroken, en wordt dit opnieuw geprobeerd vanaf het begin dat is aangegeven met de parameter Resync\_Error\_Retry\_Delay (in seconden). Als alle evaluaties slagen, wacht het apparaat het aantal seconden dat is gespecificeerd door de parameter Resync\_Periodic en voert het nog een hersynchronisatie uit.

De inhoud van elke parameter Profile\_Rule\* bestaat uit een aantal alternatieven. De alternatieven worden gescheiden door het teken |. Elk alternatief bestaat uit een voorwaardelijke expressie, een toewijzingsexpressie, een profiel-URL en eventuele gekoppelde URL-opties. Al deze onderdelen zijn optioneel binnen elk alternatief. Hieronder ziet u geldige combinaties en de volgorde waarin deze moeten voorkomen indien ze aanwezig zijn:

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

Binnen elke parameter Profile\_Rule\* moeten alle alternatieven behalve de laatste een voorwaardelijke expressie aanbieden. Deze expressie wordt als volgt geëvalueerd en verwerkt:

1. Voorwaarden worden van links naar rechts geëvalueerd, tot er een is gevonden die als waar wordt geëvalueerd (of tot er een alternatief is gevonden zonder voorwaardelijke expressie).
2. Een eventuele bijgaande toewijzingsexpressie wordt geëvalueerd, indien aanwezig.
3. Als er een URL wordt gespecificeerd als onderdeel van dat alternatief, wordt geprobeerd het profiel te downloaden dat zich bevindt op de gespecificeerde URL. Het systeem probeert de interne parameters vervolgens bij te werken.

Als alle alternatieven voorwaardelijke expressies bevatten en er wordt er geen als waar geëvalueerd (of als de volledige profielregel leeg is) wordt de volledige parameter Profile\_Rule\* overgeslagen. De volgende profielregelparameter in de reeks wordt geëvalueerd.

### Voorbeeld 1

In dit voorbeeld wordt onvoorwaardelijk gehersynchroniseerd naar het profiel op de gespecificeerde URL en wordt een HTTP GET-verzoek uitgevoerd naar de externe inrichtingsserver:

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

### Voorbeeld 2

In dit voorbeeld hersynchroniseert het apparaat naar twee verschillende URL's, afhankelijk van de registratiestatus op Lijn 1. In het geval van verloren registratie, voert het apparaat een HTTP POST uit naar een CGI-script. Het apparaat verzendt de inhoud van GPP\_A na macro-uitbreiding. Deze inhoud kan aanvullende informatie over de apparaatstatus bevatten:

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

### Voorbeeld 3

In dit voorbeeld hersynchroniseert het apparaat naar dezelfde server. Het apparaat levert aanvullende informatie als een certificaat niet is geïnstalleerd op het toestel (voor oude toestellen vòòr 2.0):

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

### Voorbeeld 4

In dit voorbeeld is lijn 1 uitgeschakeld tot GPP\_A gelijk is ingesteld aan Ingericht via de eerste URL. Na afloop hersynchroniseert het naar de tweede URL:

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

### Voorbeeld 5

In dit voorbeeld wordt er aangenomen dat het profiel dat wordt teruggezonden door de server XML-element-tags bevat. Deze tags moeten opnieuw worden vastgelegd met correcte parameternamen in de map met aliassen die is opgeslagen in GPP\_B:

```
[--alias b] https://p.tel.com/account/PNMA.xml
```

Een hersynchronisatie wordt meestal als mislukt beschouwd als een aangevraagd profiel niet van de server wordt ontvangen. De parameter Resync\_Fails\_On\_FNF kan dit standaardgedrag overschrijven. Als Resync\_Fails\_On\_FNF is ingesteld op Nee, accepteert het apparaat File-Not-Found-antwoord van de server als een succesvolle hersynchronisatie. De standaardwaarde voor Resync\_Fails\_On\_FNF is Ja.

## Upgrade Rule (Upgraderegel)

De upgraderegel is om het apparaat te vertellen om een nieuwe versie te activeren en waar deze versie moet worden opgehaald, indien nodig. Als de versie al op het apparaat staat, wordt deze niet opgehaald. De geldigheid van de locatie van de versie is dus niet van belang wanneer de gewenste versie in de inactieve partitie is.

De Upgrade\_Rule (upgraderegel) specificeert een firmwareversie die, als deze verschilt van de huidige versie, wordt gedownload en wordt toegepast tenzij dit wordt beperkt door een voorwaardelijke expressie of als Upgrade\_Enable (upgrade inschakelen) is ingesteld op Nee.

De telefoon biedt een configureerbare externe upgradeparameter, Upgrade\_Rule. Deze parameter accepteert syntaxis die overeenkomt met de parameters van de profielregel. URL-opties worden niet ondersteund voor upgrades, maar voorwaardelijke expressies en toewijzingsexpressies kunnen worden gebruikt. Als voorwaardelijke expressies worden gebruikt, kan de parameter worden ingevuld met meerdere alternatieven, gescheiden door het |-teken. De syntaxis voor elk alternatief is als volgt:

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

Net als in het geval van Profile\_Rule\*-parameters evalueert de parameter Upgrade\_Rule elk alternatief totdat een voorwaardelijke expressie is voldaan of een alternatief geen voorwaardelijke expressie heeft. De bijbehorende toewijzingsexpressie wordt geëvalueerd, indien deze is gespecificeerd. Vervolgens wordt een upgrade naar de gespecificeerde URL geprobeerd.

Als de Upgrade\_Rule een URL zonder een voorwaardelijke expressie bevat, wordt het apparaat bijgewerkt naar de firmware-image die door de URL wordt gespecificeerd. Na macro-uitbreiding en evaluatie van de regel probeert het apparaat niet opnieuw te upgraden tot de regel is aangepast of tot de effectieve combinatie van schema + server + poort + bestandspad wordt gewijzigd.

Als u een firmware-upgrade wilt proberen, schakelt het apparaat audio uit aan het begin van de procedure en start het opnieuw op aan het einde van de procedure. Het apparaat begint automatisch een upgrade die wordt bepaald door de inhoud van Upgrade\_Rule, alleen als alle spraaklijnen momenteel inactief zijn.

Bijvoorbeeld:

- Voor de Cisco IP 6800-serie:

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

In dit voorbeeld zorgt de Upgrade\_Rule ervoor dat er een firmware-upgrade wordt uitgevoerd naar de image die is opgeslagen op de aangegeven URL.

Dit is een ander voorbeeld voor de Cisco IP Phone 6800-serie:

```
("$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
```

In dit voorbeeld wordt het toestel aangestuurd om een van de twee images te laden, op basis van de inhoud van een parameter voor algemene doeleinden, GPP\_F.

Het apparaat kan een downgradelimit afdwingen met betrekking tot het firmwarerevisienummer. Dit kan een nuttige aanpassingsoptie zijn. Als een geldig firmwarerevisienummer is geconfigureerd in de parameter

Downgrade\_Rev\_Limit, weigert het apparaat upgradepogingen voor firmware-versies lager dan de opgegeven limiet.

## Gegevenstypen

Deze gegevenstypen worden gebruikt met configuratieprofielparameters:

- {a,b,c,...}: een keuze uit a, b, c, ...
- Booleaans: booleaanse waarde van 'ja' of 'nee'.
- CadScript: een miniscript waarmee de cadansparameters van een signaal worden gespecificeerd. Maximaal 127 tekens.

Syntaxis: S<sub>1</sub>[;S<sub>2</sub>] waarbij:

- S<sub>i</sub>=D<sub>i</sub>(aan<sub>i,1</sub>/uit<sub>i,1</sub>[,aan<sub>i,2</sub>/uit<sub>i,2</sub>[,aan<sub>i,3</sub>/uit<sub>i,3</sub>[,aan<sub>i,4</sub>/uit<sub>i,4</sub>[,aan<sub>i,5</sub>/uit<sub>i,5</sub>[,aan<sub>i,6</sub>/uit<sub>i,6</sub>]]]]) en is bekend als een sectie.
- aan<sub>i,j</sub> en uit<sub>i,j</sub> zijn de aan/uit duur in seconden van een *segment*. i = 1 of 2 en j = 1 tot 6.
- D<sub>i</sub> is de totale duur van de sectie in seconden.

Alle duren kunnen tot drie decimaalplaatsen hebben om oplossing tot 1 ms te bieden. Een wildcardteken '\*' staat voor oneindige duur. De segmenten binnen een sectie worden op volgorde afgespeeld en herhaald tot de totale duur is afgespeeld.

Voorbeeld 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
```

Voorbeeld 2: afwijkende beltoon (kort, kort, kort, lang):

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

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

Total Ring Length = 60s
```

- Nummerplanscript: scriptsyntaxis die wordt gebruikt om nummerplannen voor lijn 1 en lijn 2 te specificeren.
- <n> zweven: een zwevende puntwaarde met maximaal n decimalen.

- FQDN: volledig gekwalificeerde domeinnaam. Dit kan maximaal 63 tekens bevatten. Hieronder ziet u enkele voorbeelden:
  - sip.Cisco.com:5060 of 109.12.14.12:12345
  - sip.Cisco.com of 109.12.14.12

- FreqScript: een miniscript dat de frequentie- en niveauparameters van een toon specificceert. Bevat maximaal 127 tekens.

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

- $F_1$ - $F_6$  frequentie in Hz zijn (alleen niet-ondertekende gehele getallen).
- $L_1$ - $L_6$  bijbehorende niveaus in dBm zijn (met maximaal één decimaal).

Spaties voor en na de komma zijn toegestaan, maar niet aanbevolen.

Voorbeeld 1: toon voor wachtend gesprek:

```
440@-10

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

Voorbeeld 2: kiestoon:

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

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

- IP: geldig IPv4-adres in de vorm van x.x.x.x, waarbij x tussen 0 en 255 is. Voorbeeld: 10.1.2.100.
- Gebruikers-id: gebruikers-id zoals deze wordt weergegeven in een URL; maximaal 63 tekens.
- Telefoon: een telefoonnummerreeks, zoals 14081234567, \*69, \*72, 345678; of een generieke URL zoals 1234@10.10.10.100:5068 of jsmith@Cisco.com. De tekenreeks kan maximaal 39 tekens bevatten.
- PhTmpl: een telefoonnummersjabloon. Elke sjabloon kan een of meer patronen bevatten die worden gescheiden door een komma (.). Spaties aan het begin van elk patroon worden genegeerd. '?' en '\*' vertegenwoordigen wildcard-tekens. Als u deze tekens letterlijk wilt aangeven, gebruikt u %xx. Zo staat %2a bijvoorbeeld voor \*. De sjabloon kan maximaal 39 tekens bevatten. Voorbeelden: "1408\*, 1510\*", "1408123????, 555?1.".
- Poort: TCP/UDP-poortnummer (0-65535). Deze kan worden gespecificeerd in decimale of hexadecimale indeling.
- ProvisioningRuleSyntax: scriptsyntaxis die wordt gebruikt voor het definiëren van configuratieregels, hersynchronisatieregels en firmware-upgraderegels.
- PwrLevel: stroomniveau uitgedrukt in dBm met één decimaal, zoals -13,5 of 1.5 (dBm).
- RscTmpl: een sjabloon van de SIP-antwoordstatuscode zoals "404, 5\*", "61?", "407, 408, 487, 481". Dit kan maximaal 39 tekens bevatten.

- **Sig<n>**: ondertekende n-bits-waarde. Deze kan worden gespecificeerd in decimale of hexadecimale indeling. Een '-' teken moet voorafgaan aan negatieve waarden. Een '+'-teken voorafgaand aan positieve waarden is optioneel.
- **Stercodes**: activeringscode voor een aanvullende service, zoals \*69. De code kan maximaal 7 tekens bevatten.
- **Str<n>**: een algemene tekenreeks met maximaal n niet-gereserveerde tekens.
- **Tijd<n>**: tijdsduur in seconden, met maximaal n decimalen. Extra gespecificeerde decimaalplaatsen worden genegeerd.
- **ToneScript**: een miniscript dat de frequentie-, niveau- en cadansparameters van een toon voor gespreksvoorgang specificeert. Script kan maximaal 127 tekens bevatten.

Syntaxis: FreqScript;Z<sub>1</sub>[:Z<sub>2</sub>].

De sectie Z<sub>1</sub> is vergelijkbaar met de sectie S<sub>1</sub> in een CadScript, behalve dat elk aan/uit-segment wordt gevolgd door een parameter met frequentiecomponenten: Z<sub>1</sub> = D<sub>1</sub>(aan<sub>i,1</sub>/uit<sub>i,1</sub>/f<sub>i,1</sub>[,aan<sub>i,2</sub>/uit<sub>i,2</sub>/f<sub>i,2</sub>[,aan<sub>i,3</sub>/uit<sub>i,3</sub>/f<sub>i,3</sub>[,aan<sub>i,4</sub>/uit<sub>i,4</sub>/f<sub>i,4</sub>[,aan<sub>i,5</sub>/uit<sub>i,5</sub>/f<sub>i,5</sub>[,aan<sub>i,6</sub>/uit<sub>i,6</sub>/f<sub>i,6</sub>]]]])) waarbij:

- $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]]$ .
- $1 < n_k < 6$  specificeert de frequentiecomponenten in FreqScript die worden gebruikt in dat segment.

Als meer dan één frequentiecomponent in een segment wordt gebruikt, worden de componenten bij elkaar opgeteld.

Voorbeeld 1: kiestoon:

```
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
```

Voorbeeld 2: stottertoon:

```
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>: niet-ondertekende n-bits-waarde, waarbij n = 8, 16 of 32. Dit kan worden gespecificeerd in decimale of hexadecimale indeling, zoals 12 of 0x18, zo lang de waarde in n bits past.



**Opmerking** Denk aan het volgende:

- <Par Name> vertegenwoordigt een configuratieparameternaam. In een profiel wordt de bijbehorende tag samengesteld door de spatie te vervangen met een onderstrepingsteken '\_', zoals **Par\_Name**.
- Een leeg standaardwaardeveld betekent een lege string <"" >.
- De telefoon blijft de laatst geconfigureerde waarden gebruiken voor tags die niet in een bepaald profiel aanwezig zijn.
- Sjablonen worden vergeleken in de aangegeven volgorde. De eerste, *niet de dichtstbijzijnde*, overeenkomst wordt geselecteerd. De parameternaam moet exact overeenkomen.
- Als er meer dan één definitie van een parameter wordt gegeven in een profiel, is de laatste dergelijke definitie in het bestand de definitie die wordt toegepast in de telefoon.
- Een parameterspecificatie met een lege parameterwaarde forceert de parameter terug op de standaardwaarde. Als u in plaats daarvan een lege tekenreeks wilt specificeren, gebruikt u de lege tekenreeks "" als de parameterwaarde.

## Profielupdates en firmware-upgrades

De telefoon ondersteunt veilige externe inrichting (configuratie) en firmware-upgrades. Een niet-ingerichte telefoon kan een gecodeerd profiel ontvangen dat aan dat apparaat is gericht. De telefoon vereist geen expliciete sleutel vanwege een beveiligd mechanisme voor de eerste inrichting waarbij SSL-functionaliteit wordt gebruikt.

Tussenkomen van de gebruiker is niet nodig om een profielupdate of firmware-upgrade te beginnen of te voltooien. Het is ook niet nodig wanneer tussentijdse upgrades nodig zijn om een volgende upgradestatus te bereiken vanuit een oudere versie. Een profiel wordt alleen gehersynchroniseerd wanneer de telefoon inactief is, omdat een hersynchronisatie kan veroorzaken dat de software opnieuw wordt opgestart, waardoor het gesprek wordt afgebroken.

Parameters voor algemene doeleinden beheren het inrichtingsproces. Elke telefoon kan worden geconfigureerd om periodiek contact te maken met een normale inrichtingsserver (NPS). Er hoeft bij communicatie met de NPS geen beveiligd protocol te worden gebruikt omdat het bijgewerkte profiel wordt gecodeerd met een gedeelde geheime sleutel. De NPS kan een standaard TFTP-, HTTP- of HTTPS-server met clientcertificaten zijn.

De beheerder kan telefoons upgraden, opnieuw opstarten, opnieuw starten of hersynchroniseren met behulp van de webgebruikersinterface van de telefoon. De beheerder kan deze taken ook uitvoeren met behulp van een SIP NOTIFY-bericht.

Configuratieprofielen worden gegenereerd met behulp van algemene, open-source-hulpmiddelen die integreren met inrichtingssystemen van de serviceprovider.

### Verwante onderwerpen

[Profielupdates toestaan en configureren](#), op pagina 36

## Profielupdates toestaan en configureren

Profielupdates kunnen op specifieke intervallen worden toegestaan. Bijgewerkte profielen worden vanaf een server naar de telefoon verzonden met behulp van TFTP, HTTP of HTTPS.

### Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).

### Procedure

- 
- Stap 1** Selecteer **Spraak > Inrichting**.
  - Stap 2** Kies in de sectie **Configuratieprofiel Ja** in de vervolgkeuzelijst **Inrichting inschakelen**.
  - Stap 3** Voer de parameters in.
  - Stap 4** Klik op **Alle wijzigingen verzenden**.

### Verwante onderwerpen

[Profielupdates en firmware-upgrades](#), op pagina 35

## Firmware-upgrades toestaan en configureren

Firmware-updates kunnen op specifieke intervallen worden toegestaan. Bijgewerkte firmware wordt vanaf een server naar de telefoon verzonden met behulp van TFTP of HTTP. Beveiliging is een minder groot probleem met een firmware-upgrade, omdat firmware geen persoonlijke informatie bevat.

### Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).

### Procedure

- 
- Stap 1** Selecteer **Spraak > Inrichting**.
  - Stap 2** Kies in de sectie **Firmware-upgrade Ja** in de vervolgkeuzelijst **Upgrade inschakelen**.
  - Stap 3** Voer de parameters in.
  - Stap 4** Klik op **Alle wijzigingen verzenden**.

## Firmware upgraden met TFTP, HTTP of HTTPS

De telefoon ondersteunt een upgrade met één image met TFTP, HTTP of HTTPS.



### Opmerking

Downgrades naar eerdere versies zijn mogelijk niet beschikbaar voor alle apparaten. Zie voor meer informatie de release notes voor uw telefoon- en firmwareversie.

### Voordat u begint

Het firmwareversiebestand moet worden gedownload naar een toegankelijke server.

### Procedure

---

- Stap 1** Wijzig de naam van de afbeelding als volgt:  
`cp-x8xx-sip.aa-b-cMPP.cop` naar `cp-x8xx-sip.aa-b-cMPP.tar.gz`  
Waarbij:  
`x8xx` is de telefoonserie, bijvoorbeeld 6841.  
`aa-b-c` is het versienummer, zoals 10-4-1
- Stap 2** Gebruik de opdracht `tar-xzvf` om de tar-bal uit te pakken.
- Stap 3** Kopieer de map naar een TFTP-, HTTP- of HTTPS-downloadmap.
- Stap 4** Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).
- Stap 5** Selecteer **Spraak > Inrichting**.
- Stap 6** Zoek de bestandsnaam van de versie, die eindigt op `.loads` en voeg deze toe aan de geldige URL.
- Stap 7** Klik op **Alle wijzigingen verzenden**.
- 

## Firmware upgraden met een browseropdracht

Een upgradeopdracht die wordt ingevoerd in de adresbalk van de browser kan worden gebruikt om de firmware op een telefoon te upgraden. De telefoon wordt alleen bijgewerkt als deze inactief is. De update wordt automatisch geprobeerd nadat het gesprek is voltooid.

### Procedure

---

Voer de volgende opdracht in om de telefoon bij te werken met een URL in een webbrowser:

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

---





## HOOFDSTUK 3

# Voorinrichting op kantoor en inrichtingsservers

- [Voorinrichting op kantoor en inrichtingsservers, op pagina 39](#)
- [Servervoorbereiding en hulpprogramma's, op pagina 39](#)
- [Voorinrichting van apparaten op kantoor, op pagina 41](#)
- [Instellen van de inrichtingsserver, op pagina 42](#)

## Voorinrichting op kantoor en inrichtingsservers

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

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

## Servervoorbereiding en hulpprogramma's

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

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

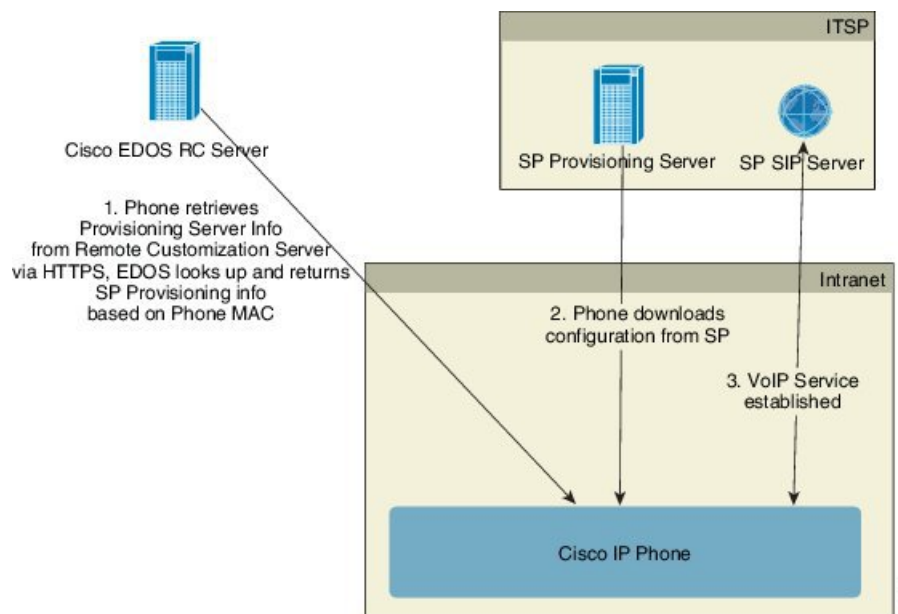
Als u problemen met de serverconfiguratie wilt oplossen, is het handig om clients voor elk type server te installeren op een afzonderlijke servercomputer. Daarmee maakt u een juiste serverwerking mogelijk, onafhankelijk van de interactie met de telefoons.

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

- Als u configuratieprofielen wilt genereren, kunt u het open-source gzip-compressiehulpprogramma installeren.

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

## RC-distributie (externe aanpassing)



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

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

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

Wanneer een telefoon voor de eerste keer verbinding maakt met een netwerk of nadat de fabrieksinstellingen zijn teruggezet en er geen DHCP-opties zijn ingesteld, maakt de telefoon contact met een apparaatactiveringsserver voor automatische inrichting. Nieuwe telefoons gebruiken “activate.cisco.com” in plaats van “webapps.cisco.com” voor het inrichten. Telefoons met een firmwarerelease van vóór 11.2(1) blijven webapps.cisco.com gebruiken. Cisco raadt aan om beide domeinnamen toe te staan via uw firewall.

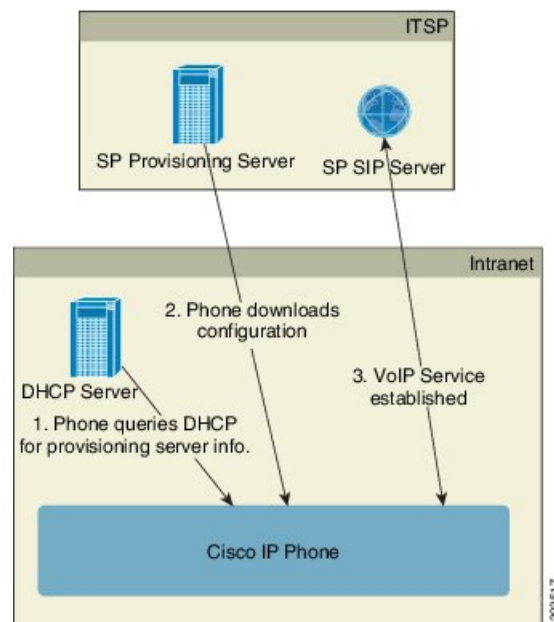
Als de DHCP-server geen informatie van de inrichtingsserver aanbiedt, vraagt de telefoon dit aan bij de Cisco EDOS RC-server en biedt deze het MAC-adres en het model aan. De aanpassingsstatus wordt ingesteld op **In behandeling**. De Cisco EDOS-server reageert met de gekoppelde informatie van de inrichtingsserver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

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

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

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

## Voorinrichting van apparaten op kantoor



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

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

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

#### Verwante onderwerpen

[Verkoopdistributie](#), op pagina 5

[TFTP-inrichting](#), op pagina 42

## Instellen van de inrichtingsserver

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

## TFTP-inrichting

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

De telefoon kan een IP-adres van de TFTP-server rechtstreeks verkrijgen van de DHCP-server via DHCP-optie 66. Als een Profile\_Rule is geconfigureerd met het bestandspad van die TFTP-server, downloadt het apparaat het profiel van de TFTP-server. Het downloaden vindt plaats wanneer het apparaat is verbonden met een LAN en wanneer het is opgestart.

De Profile\_Rule die wordt aangeboden bij de standaardfabrieksconfiguratie is `&PN.cfg`, waarbij `&PN` staat voor de telefoonmodelnaam.

Voor een CP-6841-3PCC is de bestandsnaam bijvoorbeeld CP-6841-3PCC.cfg.

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

#### Verwante onderwerpen

[Voorinrichting van apparaten op kantoor](#), op pagina 41

## Extern eindpuntbeheer en NAT

De telefoon is compatibel met netwerkadresomzetting (NAT) om het internet via een router te gebruiken. Voor betere beveiliging kan de router proberen ongeautoriseerde binnenkomende pakketten te blokkeren door symmetrisch NAT te implementeren, een strategie voor het filteren van pakketten waarmee de pakketten die zijn toegestaan om via het internet het beveiligde netwerk binnen te komen ernstig worden beperkt. Daarom wordt externe inrichting via TFTP niet aanbevolen.



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

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

## HTTP-inrichting

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

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

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

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

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

Het volgende voorbeeld is het verzoekveld User-Agent uit een CP-6841-3PCC:

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

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

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

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

**Opmerking**

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

## HTTP-statuscode verwerken bij hersynchronisatie en upgraden

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

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

**Tabel 2: Telefoongedrag voor HTTP-antwoorden**

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

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

## HTTPS-inrichting

De telefoon ondersteunt HTTPS voor inrichting voor betere beveiliging bij het extern beheer van geïmplementeerde toestellen. Elke telefoon heeft een uniek SSL-clientcertificaat (en de bijbehorende privé sleutel), naast een Sipura CA-basisservercertificaat. Het laatste zorgt ervoor dat de telefoon geverifieerde inrichtingsservers kan herkennen en niet-geverifieerde servers kan afwijzen. Aan de andere kant zorgt het clientcertificaat ervoor dat de inrichtingsserver het individuele toestel kan herkennen dat het verzoek verzendt.

Als een serviceprovider de implementatie wil beheren via HTTPS, moet een servercertificaat worden gegenereerd voor elke inrichtingsserver waarnaar een telefoon hersynchroniseert met behulp van HTTPS. Het servercertificaat moet zijn ondertekend door de Cisco Server CA-basisleutel. Alle geïmplementeerde toestellen hebben dit certificaat. Als u een ondertekend servercertificaat wilt verkrijgen, moet de serviceprovider een aanvraag voor certificaatondertekening indienen bij Cisco. Cisco ondertekent het servercertificaat en stuurt het terug voor installatie op de inrichtingsserver.

Het certificaat van de inrichtingsserver moet het veld Algemene naam (CN) en de FQDN van de host waarop de server wordt uitgevoerd in het onderwerp bevatten. Het kan optioneel ook informatie bevatten na de host-FQDN, gescheiden door een slash (/). De volgende voorbeelden zijn van CN-vermeldingen die door de telefoon als geldig worden geaccepteerd:

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

Naast het verifiëren van het servercertificaat, controleert de telefoon het IP-adres van de server tegen een DNS-zoekopdracht van de servernaam die is gespecificeerd in het servercertificaat.

## Een ondertekend servercertificaat verkrijgen

Het hulpprogramma OpenSSL kan een verzoek voor certificaatondertekening genereren. Het volgende voorbeeld toont de **openssl**-opdracht waarmee een RSA openbare/privé sleutelbaar van 1024-bits en een verzoek tot certificaatondertekening wordt geproduceerd:

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

Deze opdracht genereert de privé serversleutel in **privkey.pem** en een bijbehorend verzoek tot certificaatondertekening in **provserver.csr**. De serviceprovider houdt de **privkey.pem** geheim en dient **provserver.csr** in bij Cisco voor ondertekening. Na ontvangst van het bestand **provserver.csr**, genereert Cisco **provserver.crt**, het ondertekende servercertificaat.

### Procedure

- 
- Stap 1** Ga naar <https://software.cisco.com/software/edos/home> en meld u aan met uw CCO-referenties.
- Opmerking** Wanneer een telefoon voor de eerste keer verbinding maakt met een netwerk of nadat de fabrieksinstellingen zijn teruggezet en er geen DHCP-opties zijn ingesteld, maakt de telefoon contact met een apparaatactiveringsserver voor automatische inrichting. Nieuwe telefoons gebruiken “activate.cisco.com” in plaats van “webapps.cisco.com” voor het inrichten. Telefoons met een firmwarerelease van vóór 11.2(1) blijven “webapps.cisco.com” gebruiken. We raden aan om beide domeinnamen toe te staan door uw firewall.
- Stap 2** Selecteer **Certificate Management**.
- Op het tabblad **CSR ondertekenen** kunt u de CRS uit de vorige stap uploaden voor ondertekening.
- Stap 3** In de vervolgkeuzelijst **Product selecteren** selecteert u **SPA1xx-firmware 1.3.3 en hoger/SPA232D-firmware 1.3.3 en hoger/SPA5xx-firmware 7.5.6 en hoger/CP-78xx-3PCC/CP-88xx-3PCC**.
- Opmerking** Dit product bevat de Cisco IP Phone 6800-serie voor meerdere platforms.
- Stap 4** In het veld **CSR-bestand** klikt u op **Bladeren** en selecteert u de CSR voor ondertekening.
- Stap 5** De coderingsmethode selecteren:
- MD5
  - SHA1
  - SHA256
- Cisco beveelt aan om SHA256-codering te selecteren.
- Stap 6** In de vervolgkeuzelijst **Duur aanmelden** selecteert u de duur van toepassing (bijvoorbeeld 1 jaar).
- Stap 7** Klik op **Verzoek tot certificaatondertekening**.
- Stap 8** Selecteer een van de volgende opties om het ondertekende certificaat te ontvangen:
- **Voer e-mailadres van de ontvanger in:** als u het certificaat via e-mail wilt ontvangen, voert u uw e-mailadres in dit veld in.
  - **Downloaden:** selecteer deze optie als u het ondertekende certificaat wilt downloaden.
- Stap 9** Klik op **Verzenden**.

Het ondertekende servercertificaat wordt per e-mail verzonden naar het eerder opgegeven e-mailadres of gedownload.

## CA-clientbasiscertificaat voor telefoons voor meerdere platforms

Cisco biedt ook een clientbasiscertificaat voor telefoons voor meerdere platforms aan de serviceprovider. Dit basiscertificaat verklaart de betrouwbaarheid van het clientcertificaat dat elke telefoon heeft. De telefoons voor meerdere platforms ondersteunen ook certificaten die door externe partijen zijn ondertekend, zoals die van Verisign, Cybertrust, etc.

Het unieke clientcertificaat dat elk apparaat biedt tijdens een HTTPS-sessie draagt identificerende informatie die in het onderwerpveld wordt ingesloten. Deze informatie kan beschikbaar worden gesteld door de HTTPS-server aan een CGI-script dat wordt aangeroepen om beveiligde verzoeken af te handelen. Het certificaatonderwerp geeft in het bijzonder de productnaam (OU-element), het MAC-adres (S-element) en het serienummer (L-element) van het toestel aan.

Het volgende voorbeeld van het onderwerpveld van het clientcertificaat van Cisco IP Phone 6841 voor meerdere platforms toont deze elementen:

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

Om te bepalen of een telefoon een individueel certificaat draagt, gebruikt u de macrovariabele \$CCERT voor inrichting. De waarde van de variabele wordt uitgebreid tot geïnstalleerd of niet geïnstalleerd, afhankelijk van de aanwezigheid of afwezigheid van een uniek clientcertificaat. In het geval van een algemeen certificaat, is het mogelijk om het serienummer van het toestel te verkrijgen van de HTTP-aanvraagkopstekst in het veld User-Agent.

HTTPS-servers kunnen worden geconfigureerd om SSL-certificaten aan te vragen van clients die verbinding maken. Indien dit is ingeschakeld, kan de server het clienthoofdcertificaat voor telefoons voor meerdere platforms gebruiken dat door Cisco wordt geleverd om het clientcertificaat te verifiëren. De server kan de certificaatinformatie vervolgens aan een CGI aanbieden voor verdere verwerking.

De locatie voor opslag van certificaten kan variëren. Bij een Apache-installatie bijvoorbeeld, is het bestandspad voor de opslag van het door de inrichtingsserver ondertekende certificaat, de bijbehorende privé sleutel en het CA-clientbasiscertificaat voor telefoons voor meerdere platforms als volgt:

```
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
```

Raadpleeg de documentatie voor een HTTPS-server voor specifieke informatie.

De Cisco Client Certificate Root Authority ondertekent elk unieke certificaat. Het overeenkomstige hoofdcertificaat wordt beschikbaar gesteld aan serviceproviders ten behoeve van clientverificatie.

## Redundante inrichtingsservers

De inrichtingsserver kan worden gespecificeerd als een IP-adres of als een volledig gekwalificeerde domeinnaam (FQDN). Het gebruik van een FQDN faciliteert de implementatie van redundante inrichtingsservers. Wanneer de inrichtingsserver wordt geïdentificeerd via een FQDN, probeert de telefoon de FQDN om te zetten naar een IP-adres via DNS. Alleen DNS A-records worden ondersteund voor inrichting; DNS SRV-adresresolutie is niet beschikbaar voor inrichting. Totdat een server reageert, blijft de telefoon A-records verwerken. Als er geen server reageert die is gekoppeld aan de A-records, meldt de telefoon een fout bij de syslog-server.

## Syslog-server

Als een syslog-server is geconfigureerd op de telefoon door het gebruik van de parameters <Syslog Server>, worden er bij de bewerkingen hersynchroniseren en upgraden berichten naar de syslog-server verzonden. Een bericht kan worden gegenereerd aan het begin van een verzoek voor een extern bestand (configuratieprofiel of firmwareversie) en aan het eind van de bewerking (om succes of mislukking aan te geven).

Berichten in het logboek worden geconfigureerd in de volgende parameters en worden macro-uitgebreid tot de werkelijke syslog-berichten:

- Log\_Request\_Msg (Aanvraagbericht registreren)
- Log\_Success\_Msg (Succesbericht registreren)
- Log\_Failure\_Msg (Foutbericht registreren)



## HOOFDSTUK 4

# Voorbeelden van inrichting

---

- [Overzicht voorbeelden van inrichten, op pagina 49](#)
- [Standaard hersynchroniseren, op pagina 49](#)
- [Hersynchroniseren via beveiligde HTTPS, op pagina 55](#)
- [Profielbeheer, op pagina 63](#)
- [Privacytekst telefoon instellen, op pagina 66](#)

## Overzicht voorbeelden van inrichten

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

Voor meer informatie over het maken van configuratieprofielen raadpleegt u [Inrichtingsscripts, op pagina 13](#).

## Standaard hersynchroniseren

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

## Hersynchroniseren via TFTP

De telefoon ondersteunt meerdere netwerkprotocollen voor het ophalen van configuratieprofielen. Het meest eenvoudige profieloverdrachtsprotocol is TFTP (RFC1350). TFTP wordt veel gebruikt voor de inrichting van netwerkapparaten binnen privé LAN-netwerken. Hoewel het niet wordt aanbevolen voor de implementatie van externe eindpunten via het internet, kan TFTP nuttig zijn voor implementatie binnen kleine organisaties, voorinrichting op kantoor en het ontwikkelen en testen. Zie [Voorinrichting van apparaten op kantoor, op pagina 41](#) voor meer informatie over voorinrichting op kantoor. In de volgende procedure wordt een profiel aangepast na het downloaden van een bestand van een TFTP-server.

### Procedure

---

- Stap 1** Sluit een computer en een telefoon aan op een hub, switch of kleine router in een LAN-omgeving.
- Stap 2** Installeer en activeer een TFTP-server op de computer.

- Stap 3** Gebruik een tekstverwerker om een configuratieprofiel te maken waarin de waarde voor GPP\_A wordt ingesteld op 12345678 zoals weergegeven in het voorbeeld.

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

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

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

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

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

- Stap 6** Selecteer het tabblad **Spraak > Inrichting** en controleer de waarden van de parameters voor algemene doeleinden GPP\_A tot GPP\_P. Deze zouden leeg moeten zijn.

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

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

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

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

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

De parameter GPP\_A moet de waarde 12345678 nu bevatten.

---

## Syslog gebruiken om berichten op te slaan

De telefoon verzendt een syslog-bericht naar de toegewezen syslog-server wanneer het apparaat op het punt staat te hersynchroniseren naar een inrichtingsserver en nadat de hersynchronisatie is voltooid of mislukt. Om deze server te identificeren, opent u de beheerwebpagina van de telefoon (zie [Telefoonwebpagina openen, op pagina 7](#)) en selecteert u **Spraak > Systeem** en identificeert u de server in de parameter **Syslog-server** van de sectie **Optionele netwerkconfiguratie**. Configureer het IP-adres van de syslog-server in het apparaat en controleer de berichten die tijdens de resterende procedures worden gegenereerd.

### Procedure

---

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



**Stap 2** Programmeer het IP-adres van de computer in de parameter Syslog\_Server van het profiel en dien de wijziging in:

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

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

**Stap 4** Herhaal de hersynchronisatiebewerking zoals beschreven in [Hersynchroniseren via TFTP, op pagina 49](#).

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

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

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

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

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

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

- Log\_Request\_Msg (Aanvraagbericht registreren)
- Log\_Success\_Msg (Succesbericht registreren)
- Log\_Failure\_Msg (Foutbericht registreren)

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

---

## Een apparaat automatisch hersynchroniseren

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

Zodat de telefoon periodiek hersynchroniseert naar een server, wordt er een configuratieprofiel-URL gedefinieerd met de parameter Profile\_Rule en wordt er een hersynchronisatieperiode gedefinieerd met de parameter Resync\_Periodic.

### Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).

## Procedure

---

- Stap 1** Selecteer **Spraak > Inrichting**.
- Stap 2** Definieer de parameter `Profile_Rule`. In dit voorbeeld wordt verondersteld dat het IP-adres van de TFTP-server 192.168.1.200 is.
- Stap 3** Voer in het veld **Resync Periodic** een kleine waarde in om te testen, zoals **30** seconden.
- Stap 4** Klik op **Alle wijzigingen verzenden**.
- Met de nieuwe parameterinstellingen zal de telefoon twee keer per minuut hersynchroniseren naar het configuratiebestand dat de URL specificeert.
- Stap 5** Controleer de resulterende berichten in de syslog-tracering (zoals beschreven in de sectie [Syslog gebruiken om berichten op te slaan, op pagina 50](#)).
- Stap 6** Zorg ervoor dat het veld **Resync On Request** is ingesteld op **Ja**.
- ```
<Resync_On_Reset>Yes</Resync_On_Reset>
```
- Stap 7** Zet de telefoon uit en weer aan om een hersynchronisatie naar de inrichtingsserver af te dwingen.
- Als de hersynchronisatie mislukt om een bepaalde reden, zoals dat de server niet reageert, wacht het toestel (voor het aantal seconden dat is geconfigureerd in **Resync Error Retry Delay**) voordat deze opnieuw probeert te hersynchroniseren. Als de **Resync Error Retry Delay** wordt ingesteld op 0, probeert de telefoon niet nogmaals te hersynchroniseren na een mislukte hersynchronisatiepoging.
- Stap 8** (Optioneel) Stel de waarde van het veld **Resync Error Retry Delay** in op een klein nummer, zoals **30**.
- ```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```
- Stap 9** Schakel de TFTP-server uit en observeer de resultaten in de syslog-uitvoer.
- 

## Unieke profielen, macro-uitbreiding en HTTP

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

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

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

- `$MA` is een uitbreiding op het 12-cijferige MAC-adres van het toestel (met kleine hexadecimale tekens). Bijvoorbeeld `000e08abcdef`.

- \$SN is een uitbreiding op het serienummer van de eenheid. Bijvoorbeeld 88012BA01234.

Andere waarden kunnen op dezelfde wijze macro-uitbreiding ondergaan, inclusief alle parameters voor algemene doeleinden; GPP\_A tot GPP\_P. U kunt een voorbeeld van dit proces zien in [Hersynchroniseren via TFTP, op pagina 49](#). Macro-uitbreiding is niet beperkt tot de URL-bestandsnaam, maar kan ook worden toegepast op enig onderdeel van de profielregelparameter. Naar deze parameters wordt verwezen als \$A tot \$P. Zie voor een volledige lijst van variabelen die beschikbaar zijn voor macro-uitbreiding [Variabelen voor macro-uitbreiding, op pagina 76](#).

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

## Oefening: een specifiek IP-telefoonprofiel inrichten op een TFTP-server

### Procedure

- 
- Stap 1** Verkrijg het MAC-adres van de telefoon van het productlabel. (Het MAC-adres is het nummer, met cijfers en kleine hexadecimale tekens, zoals 000e08aabbcc.
- Stap 2** Kopieer het configuratiebestand `basic.txt` (zoals beschreven in [Hersynchroniseren via TFTP, op pagina 49](#)) naar een nieuw bestand met de naam `CP-xxxx-3PCC mac-adres.cfg` (vervang hierbij `xxxx` met het modelnummer en `mac-adres` met het MAC-adres van de telefoon).
- Stap 3** Verplaats het nieuwe bestand in de virtuele hoofdmap van de TFTP-server.
- Stap 4** Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).
- Stap 5** Selecteer **Spraak > Inrichting**.
- Stap 6** Voer `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` in het veld **Profielregel** in.

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

- Stap 7** Klik op **Alle wijzigingen verzenden**. Hierdoor wordt er direct opnieuw opgestart en gehersynchroniseerd. Wanneer de volgende hersynchronisatie wordt uitgevoerd, haalt de telefoon het nieuwe bestand op door de macro-expressie `$MA` uit te breiden tot het MAC-adres.
- 

### Hersynchroniseren via HTTP GET

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

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

*Oefening: hersynchroniseren via HTTP GET***Procedure**

- 
- Stap 1** Installeer een HTTP-server op de lokale computer of een andere toegankelijke host.  
De open-source Apache-server kan worden gedownload van internet.
- Stap 2** Kopieer het configuratieprofiel `basic.txt` (zoals beschreven in [Hersynchroniseren via TFTP, op pagina 49](#)) op de virtuele hoofdmap van de geïnstalleerde server.
- Stap 3** Als u de juiste serverinstallatie en toegang tot `basic.txt` wilt verifiëren, opent u het profiel met een webbrowser.
- Stap 4** Wijzig de `Profile_Rule` van de testtelefoon om naar de HTTP-server te verwijzen in plaats van de TFTP-server, zodat het profiel periodiek wordt gedownload.  
Bijvoorbeeld, ervan uitgaande dat de HTTP-server zich op 192.168.1.200 bevindt, voert u de volgende waarde in:
- ```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```
- Stap 5** Klik op **Alle wijzigingen verzenden**. Hierdoor wordt er direct opnieuw opgestart en gehersynchroniseerd.
- Stap 6** Bekijk de syslog-berichten die de telefoon verzendt. De periodieke hersynchronisaties zouden nu het profiel van de HTTP-server moeten ophalen.
- Stap 7** In de HTTP-serverlogboeken ziet u hoe de informatie die de testtelefoon identificeert in het logboek van gebruikersagenten verschijnt.
Deze informatie moet de fabrikant, de productnaam, de huidige firmwareversie en het serienummer bevatten.
-

Inrichten via Cisco XML

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

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

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

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

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

URL-oplossing met macro-uitbreiding

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

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

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

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

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

Stel bijvoorbeeld dat GPP_B wordt gedefinieerd als `Dj6Lmp23Q`.

De Profile_Rule heeft de waarde:

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

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

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

Hersynchroniseren via beveiligde HTTPS

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

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

Standaard hersynchroniseren via HTTPS

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

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

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

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

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

Oefening: standaard hersynchroniseren via HTTPS

Procedure

-
- Stap 1** Installeer een HTTPS-server op een host waarvan het IP-adres bekend is voor de DNS-netwerkserver via normale hostnaamvertaling.
- De open-source Apache-server kan worden geconfigureerd om te werken als een HTTPS-server wanneer het open-source `mod_ssl`-pakket is geïnstalleerd.
- Stap 2** Genereer een ondertekeningsverzoek voor het servercertificaat voor de server. Voor deze stap moet u mogelijk het open-source OpenSSL-pakket of gelijkwaardige software installeren. Indien u OpenSSL gebruikt, is de opdracht om het standaard CSR-bestand te genereren als volgt:
- ```
openssl req -new -out provserver.csr
```
- Deze opdracht genereert een gecombineerde openbare/privé sleutel, die wordt opgeslagen in het bestand `privkey.pem`.
- Stap 3** Stuur het CSR-bestand (`provserver.csr`) naar Cisco om het te laten ondertekenen.
- Een ondertekend servercertificaat wordt teruggezonden (`provserver.cert`) samen met een Sipura CA Client Root-certificaat, `spacroot.cert`.
- Zie <https://supportforums.cisco.com/docs/DOC-9852> voor meer informatie.
- Stap 4** Sla het ondertekende servercertificaat, het bestand met de gecombineerde privé sleutel en het clientbasiscertificaat op in de juiste locaties op de server.
- In het geval van een Apache-installatie op Linux zijn deze locaties meestal als volgt:

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

- Stap 5** Start de server opnieuw op.
- Stap 6** Kopieer het configuratiebestand `basic.txt` (zoals beschreven in [Hersynchroniseren via TFTP, op pagina 49](#)) naar de virtuele hoofdmap van de HTTPS-server.
- Stap 7** Controleer of de server correct werkt door `basic.txt` te downloaden van de HTTPS-server met een standaardbrowser vanuit de lokale computer.
- Stap 8** Controleer het servercertificaat dat de server levert.

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

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

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

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

- Stap 9** Klik op **Alle wijzigingen verzenden**.
- Stap 10** Bekijk de syslog-tracering die de telefoon verzendt.
- Het syslog-bericht zou moeten aangeven dat de hersynchronisatie het profiel van de HTTPS-server heeft verkregen.
- Stap 11** (Optioneel) Gebruik een Ethernet-protocolanalysator op het telefoonsubnet om te verifiëren dat de pakketten zijn gecodeerd.

In deze oefening is clientcertificaatverificatie niet ingeschakeld. De verbinding tussen de telefoon en de server is gecodeerd. De overdracht is echter niet beveiligd omdat elke client verbinding kan maken met de server en het bestand kan aanvragen, indien de bestandsnaam en maplocatie bekend zijn. Voor beveiligd hersynchroniseren moet de server de client ook verifiëren, zoals aangetoond in de oefening beschreven in [HTTPS met clientcertificaatverificatie, op pagina 57](#).

---

## HTTPS met clientcertificaatverificatie

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

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

## Oefening: HTTPS met clientcertificaatverificatie

### Procedure

---

**Stap 1** Clientcertificaatverificatie inschakelen op de HTTPS-server.

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

```
SSLVerifyClient require
```

Zorg er ook voor dat spacroot.cert is opgeslagen zoals u ziet in de oefening [Standaard hersynchroniseren via HTTPS, op pagina 55](#).

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

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

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

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

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

---

## HTTPS-clientfiltering en dynamische inhoud

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

De HTTPS-server stelt de certificaat-informatie beschikbaar aan CGI-scripts (of gecompileerde CGI-programma's) die worden opgeroepen als onderdeel van het verzoek voor hersynchronisatie. Deze oefening maakt ter illustratie gebruik van de open-source Perl-scripttaal en er wordt aangenomen dat Apache (v.2) wordt gebruikt als de HTTPS-server.

### Procedure

---

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

**Stap 2** Genereer het volgende Perl-reflectorscript:

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



```
print "<flat-profile><GPP_D>";

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

- Stap 3** Sla dit bestand op met de bestandsnaam `reflect.pl`, met uitvoeringstoestemming (`chmod 755` op Linux), in de map CGI-scripts van de HTTPS-server.
- Stap 4** Verifieer de toegankelijkheid van CGI-scripts op de server (dat wil zeggen `/cgi-bin/...`).
- Stap 5** Wijzig de `Profile_Rule` op het testapparaat zodat deze hersynchroniseert met het reflectorscript, zoals in het volgende voorbeeld:

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

- Stap 6** Klik op **Alle wijzigingen verzenden**.
- Stap 7** Bekijk de syslogtracering om te controleren dat hersynchroniseren lukt.
- Stap 8** Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).
- Stap 9** Selecteer **Spraak > Inrichting**.
- Stap 10** Verifieer dat de parameter `GPP_D` de informatie bevat die het script heeft vastgelegd.

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

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

## HTTPS-certificaten

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

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

## HTTPS-methodologie

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

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

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

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

## SSL-servercertificaat

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

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

## Een servercertificaat verkrijgen

### Procedure

- Stap 1** Neem contact op met iemand van Cisco Support die u kan helpen bij het certificaatproces. Als u geen ondersteuning krijgt van een specifiek persoon, kunt u uw verzoek e-mailen naar [ciscosb-certadmin@cisco.com](mailto:ciscosb-certadmin@cisco.com).
- Stap 2** Genereer een privé sleutel die wordt gebruikt in een CSR (certificaatondertekeningsverzoek). Deze sleutel is privé. U hoeft deze sleutel niet aan Cisco Support door te geven. Gebruik open-source "openssl" om de sleutel te genereren. Bijvoorbeeld:

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

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

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

U hebt de volgende informatie nodig:

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

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

## Clientcertificaat

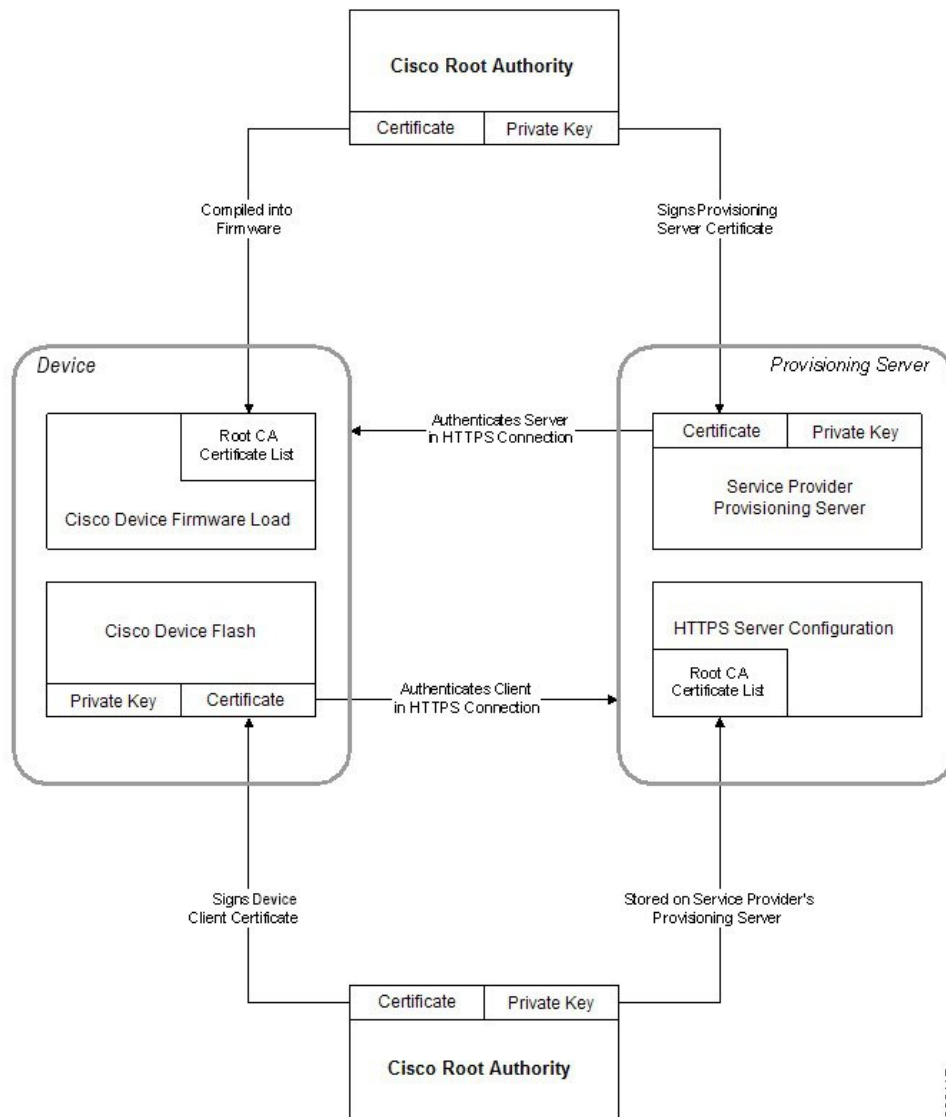
Naast een directe aanval op een telefoon, kan een aanvaller contact maken met een inrichtingsserver via een standaard webbrowser of een andere HTTPS-client om het configuratieprofiel van de inrichtingsserver te proberen te verkrijgen. Om dit soort aanvallen te voorkomen, heeft elke telefoon ook een uniek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

## Certificaatstructuur

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

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

Figuur 2: Certificate Authority-stroom



## Een aangepaste Certificate Authority configureren

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

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

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

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

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

### Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [Telefoonwebpagina openen, op pagina 7](#).

### Procedure

---

**Stap 1**

Selecteer **Info** > **Status**.

**Stap 2**

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

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

## Profielbeheer

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

### Een open profiel met Gzip comprimeren

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



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

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

### Procedure

**Stap 1** Installeer gzip op de lokale computer.

**Stap 2** Comprimeer het configuratieprofiel `basic.txt` (beschreven in [Hersynchroniseren via TFTP, op pagina 49](#)) door gzip te activeren vanaf de opdrachtregel:

```
gzip basic.txt
```

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

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

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

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

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

**Stap 6** Bekijk de syslog-tracering op de telefoon.

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

### Verwante onderwerpen

[Compressie van een open profiel](#), op pagina 18

## Een profiel coderen met OpenSSL

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

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

## Procedure

---

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

**Stap 2** Met het configuratiebestand `basic.txt` (zoals beschreven in [Hersynchroniseren via TFTP, op pagina 49](#)) kunt u een gecodeerd bestand met de volgende opdracht genereren:

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

Het gecomprimeerde `basic.txt.gz`-bestand dat is gemaakt in [Een open profiel met Gzip comprimeren, op pagina 63](#) kan ook worden gebruikt, omdat het XML-profiel zowel gecomprimeerd als gecodeerd kan zijn.

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

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

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

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

**Stap 6** Bekijk de syslog-tracering op de telefoon.

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

---

## Verwante onderwerpen

[AES-256-CBC-codering](#), op pagina 19

# Gepartitioneerde profielen maken

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

## Procedure

---

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

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

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

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

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

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

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

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

## Privacykopstekst telefoon instellen

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

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

De opties voor de privacykopstekst zijn:

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

### Procedure

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

**Stap 2** Voeg de tag `<Privacy_Header_N_ua="na">Waarde</Privacy_Header_N_>` in, waarbij N het toestelnummer is (1-10), en gebruik een van de volgende waarden.

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

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



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

---





## HOOFDSTUK 5

# Inrichtingsparameters

- [Overzicht van inrichtingsparameters, op pagina 69](#)
- [Configuratieprofielparameters, op pagina 69](#)
- [Firmware-upgradeparameters, op pagina 74](#)
- [Parameters voor algemene doeleinden, op pagina 76](#)
- [Variabelen voor macro-uitbreiding, op pagina 76](#)
- [Interne foutcodes, op pagina 79](#)

## Overzicht van inrichtingsparameters

Dit hoofdstuk beschrijft de inrichtingsparameters die kunnen worden gebruikt in configuratieprofielscripts.

## Configuratieprofielparameters

In de volgende tabel worden de functie en het gebruik van elke parameter in de sectie **Configuratieprofielparameters** van het tabblad **Inrichting** gedefinieerd.

| Naam van parameter                            | Beschrijving en standaardwaarde                                                                                                                                                                                       |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Provision Enable (Inrichting inschakelen)     | Hiermee worden alle acties voor hersynchronisatie onafhankelijk van acties voor firmware-upgrade beheerd. Ingesteld op <b>Ja</b> om externe inrichting in te schakelen.<br><br>De standaardwaarde is Ja.              |
| Resync On Reset (Hersynchroniseren bij reset) | Hiermee wordt hersynchronisatie geactiveerd na elke keer opnieuw opstarten, met uitzondering van opnieuw opstarten dat wordt veroorzaakt door parameterupdates en firmware-upgrades.<br><br>De standaardwaarde is Ja. |

| Naam van parameter                                              | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resync Random Delay (Willekeurige vertraging hersynchr.)        | <p>Een willekeurige vertraging na de opstartreeks alvorens de reset, opgegeven in seconden, uit te voeren. In een pool van IP-telefoonapparaten die zijn ingepland om tegelijkertijd te worden opgestart, zorgt dit voor een spreiding in de tijden waarop elk toestel een hersynchronisatieverzoek verzendt naar de inrichtingsserver. Deze functie kan handig zijn in een grote huisinstallatie, in het geval van een regionale stroomstoring.</p> <p>De waarde voor dit veld moet een geheel getal zijn tussen 0 en 65535.</p> <p>De standaardwaarde is 2.</p>                                                                                                                                                                                                                                                                                                                       |
| Resync At (HHmm) (Hersynchroniseren om (UUm))                   | <p>De tijd (UUm) waarop het apparaat hersynchroniseert met de inrichtingsserver.</p> <p>De waarde voor dit veld moet een viercijferig nummer zijn van 0000 tot 2400 om de tijd in de indeling UUm aan te geven. 0959 geeft bijvoorbeeld 09:59 aan.</p> <p>De standaardwaarde is leeg. Als de waarde ongeldig is, wordt de parameter genegeerd. Als deze parameter met een geldige waarde is ingesteld, wordt de parameter Resync Periodic (Periodiek hersynchroniseren) genegeerd.</p>                                                                                                                                                                                                                                                                                                                                                                                                  |
| Resync At Random Delay (Hersynchr. bij willekeurige vertraging) | <p>Hiermee wordt overbelasting van de inrichtingsserver voorkomen wanneer een groot aantal apparaten tegelijk opstart.</p> <p>Om te voorkomen dat de server overbelast raakt met verzoeken voor hersynchronisatie van meerdere telefoons, wordt de telefoon gehersynchroniseerd binnen het bereik van de uren en minuten, en de uren en minuten plus de willekeurige vertraging (hhmm, hhmm + random_delay). Bijvoorbeeld bij: willekeurige vertraging = (Hersynchroniseren bij willekeurige vertraging +30)/60 minuten, wordt de ingevoerde waarde in seconden geconverteerd naar minuten, met afronding naar boven tot de volgende minuut om het uiteindelijke random_delay-interval te berekenen.</p> <p>Geldige waarden zijn van 0 tot 65535.</p> <p>Deze functie is uitgeschakeld wanneer deze parameter is ingesteld op nul. De standaardwaarde is 600 seconden (10 minuten).</p> |

| Naam van parameter                            | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resync Periodic (Periodiek hersynchroniseren) | <p>Het tijdsinterval tussen periodieke hersynchronisatie met de inrichtingsserver. De gekoppelde hersynchronisatietimer is alleen actief na de eerste geslaagde synchronisatie met de server.</p> <p>De geldige indelingen zijn als volgt:</p> <ul style="list-style-type: none"> <li>• Een geheel getal<br/> Voorbeeld: een invoer van <b>3000</b> geeft aan dat de volgende hersynchronisatie over 3000 seconden optreedt.</li> <li>• Meerdere gehele getallen<br/> Voorbeeld: een invoer van <b>600 , 1200 , 300</b> geeft aan dat de eerste hersynchronisatie optreedt over 600 seconden, de tweede hersynchronisatie 1200 seconden na de eerste en de derde hersynchronisatie 300 seconden na de tweede.</li> <li>• Een tijdsbereik<br/> Bijvoorbeeld, een invoer van <b>2400+30</b> geeft aan dat de volgende hersynchronisatie tussen 2400 en 2430 seconden na een geslaagde hersynchronisatie optreedt.</li> </ul> <p>Stel deze parameter in op nul om periodieke hersynchronisatie uit te schakelen.</p> <p>De standaardwaarde is 3600 seconden.</p> |

| Naam van parameter                                                           | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resync Error Retry Delay (Vertraging nieuwe poging na hersynchronisatiefout) | <p>Als een hersynchronisatiebewerking mislukt omdat het IP-telefoonapparaat geen profiel van de server kan ophalen, omdat het gedownloade bestand beschadigd is of omdat er een interne fout optreedt, probeert het apparaat opnieuw te hersynchroniseren na een in seconden gespecificeerde tijd.</p> <p>De geldige indelingen zijn als volgt:</p> <ul style="list-style-type: none"> <li>• Een geheel getal<br/>Voorbeeld: een invoer van <b>300</b> geeft aan dat de volgende poging tot hersynchronisatie over 300 seconden optreedt.</li> <li>• Meerdere gehele getallen<br/>Voorbeeld: een invoer van <b>600 , 1200 , 300</b> geeft aan dat de eerste poging optreedt over 600 seconden na de fout, de tweede poging 1200 seconden nadat de eerste poging is mislukt en de derde poging 300 seconden nadat de tweede poging is mislukt.</li> <li>• Een tijdsbereik<br/>Bijvoorbeeld, een invoer van <b>2400+30</b> geeft aan dat de volgende poging tussen 2400 en 2430 seconden na een mislukte hersynchronisatie optreedt.</li> </ul> <p>Als de vertraging wordt ingesteld op 0, probeert het apparaat niet nogmaals te hersynchroniseren na een mislukte hersynchronisatiepoging.</p> |
| Forced Resync Delay (Geforceerde vertraging hersynchronisatie)               | <p>Maximale vertraging (in seconden) die de telefoon wacht voordat een hersynchronisatie wordt uitgevoerd.</p> <p>Het apparaat voert geen hersynchronisatie uit terwijl een van de telefoonlijnen actief is. Omdat een hersynchronisatie enkele seconden kan duren, is het gewenst om te wachten totdat het apparaat gedurende langere tijd inactief is voordat hersynchronisatie wordt uitgevoerd. Hierdoor kan een gebruiker zonder onderbreking oproepen blijven plaatsen.</p> <p>Het apparaat heeft een timer die begint af te tellen wanneer alle lijnen inactief worden. Deze parameter is de eerste waarde van de teller. Hersynchronisaties worden uitgesteld tot deze teller op nul staat.</p> <p>Geldige waarden zijn van 0 tot 65535.</p> <p>De standaardwaarde is 14400 seconden.</p>                                                                                                                                                                                                                                                                                                                                                                                              |

| Naam van parameter                                                 | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resync From SIP (Hersynchroniseren via SIP)                        | <p>Hiermee kan een hersynchronisatie worden geactiveerd via een SIP NOTIFY-bericht.</p> <p>De standaardwaarde is Ja.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Resync After Upgrade Attempt (Hersynchroniseren na upgradepoging)  | <p>Hiermee schakelt u of de hersynchronisatiebewerking in of uit nadat een upgrade is uitgevoerd. Als u Ja selecteert, wordt de synchronisatie gestart.</p> <p>De standaardwaarde is Ja.</p>                                                                                                                                                                                                                                                                                                                                                                           |
| Hersynchronisatietrigger 1, hersynchronisatietrigger 2             | <p>Configureerbare hersynchronisatietriggervoorwaarden. Een hersynchronisatie wordt geactiveerd wanneer de logische vergelijking in deze parameters TRUE retourneert.</p> <p>De standaardwaarde is (leeg).</p>                                                                                                                                                                                                                                                                                                                                                         |
| Resync Fails On FNF (Hersynchronisatie bij FNF)                    | <p>Een hersynchronisatie wordt als mislukt beschouwd als een aangevraagd profiel niet van de server wordt ontvangen. Dit kan door deze parameter worden opgeheven. Wanneer deze instelling wordt ingesteld op <b>nee</b>, accepteert het apparaat een <code>File-Not-Found</code>-antwoord van de server als een succesvolle hersynchronisatie.</p> <p>De standaardwaarde is Ja.</p>                                                                                                                                                                                   |
| Profielregel<br>Profielregel B<br>Profielregel C<br>Profielregel D | <p>Elke profielregel informeert de telefoon over een bron waarvan hij een profiel kan halen (configuratiebestand). Tijdens elke hersynchronisatie past de telefoon alle profielen achtereenvolgens toe.</p> <p>Standaard: <code>/\$PSN.xml</code></p> <p>Als u AES-256-CBC-codering op de configuratiebestanden toepast, geef de coderingssleutel dan als volgt op met het sleutelwoord <code>--sleutel:</code></p> <p><code>[--sleutel &lt;coderingssleutel&gt;]</code></p> <p>U kunt de coderingssleutel optioneel tussen dubbele aanhalingstekens (") plaatsen.</p> |
| DHCP Option To Use (Te gebruiken DHCP-optie)                       | <p>DHCP-opties, gescheiden door komma's, gebruikt om firmware en profielen op te halen.</p> <p>De standaardwaarde is 66,160,159,150,60,43,125.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Naam van parameter                                                          | Beschrijving en standaardwaarde                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Request Msg (Aanvraagbericht registreren)                               | Deze parameter bevat het bericht dat wordt verzonden naar de syslog-server bij de start van een poging tot hersynchroniseren.<br><br>De standaardwaarde is <code>1\$PN \$MAC -Aanvragen % \$SCHEME://\$SERVIP:\$PORT\$PATH</code> .    |
| Log Success Msg (Succesbericht registreren)                                 | Het Syslog-bericht dat wordt uitgegeven na een succesvolle voltooiing van een hersynchronisatiepoging.<br><br>De standaardwaarde is <code>\$PN \$MAC -Geslaagde hersynchronisatie % \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR</code> . |
| Log Failure Msg (Foutbericht registreren)                                   | Het Syslog-bericht dat wordt uitgegeven na een mislukte hersynchronisatiepoging.<br><br>De standaardwaarde is <code>\$PN \$MAC -- Hersynchronisatie mislukt: \$ERR</code> .                                                            |
| User Configurable Resync (Door gebruiker configureerbare hersynchronisatie) | Hiermee kan een gebruiker de telefoon hersynchroniseren via het scherm van de IP Phone.<br><br>De standaardwaarde is Ja.                                                                                                               |

## Firmware-upgradeparameters

In de volgende tabel worden de functie en het gebruik van elke parameter in de sectie **Firmware-upgrade** van het tabblad **Inrichting** gedefinieerd.

| Naam van parameter                                                  | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade Enable (Upgrade inschakelen)                                | Hiermee zijn firmware-upgradebewerkingen onafhankelijk van hersynchronisatieacties ingeschakeld.<br><br>De standaardwaarde is Ja.                                                                                                                                                                                                                                                                                                    |
| Upgrade Error Retry Delay (Vertraging nieuwe poging na upgradefout) | Het interval voor opnieuw proberen te upgraden (in seconden) wordt toegepast in het geval van een fout bij de upgrade. Het apparaat heeft een fouttimer voor de firmware-upgrade die wordt geactiveerd nadat een firmware-upgrade mislukt. De timer wordt met de waarde in deze parameter geïnitieerd. De volgende firmware-upgrade poging vindt plaats wanneer naar nul wordt afgeteld.<br><br>De standaardwaarde is 3600 seconden. |



| Naam van parameter                                                 | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade Rule (Upgraderegel)                                        | <p>Een firmware-upgradescript waarmee upgradevoorwaarden en gekoppelde firmware-URL's worden gedefinieerd. Hierbij wordt dezelfde syntaxis als bij profielregel gebruikt.</p> <p>Gebruik de volgende indeling om de upgraderegel in te voeren:</p> <pre>&lt;tftp http https&gt;://&lt;ip-adres&gt;/image/&lt;versienaam&gt;</pre> <p>Bijvoorbeeld:</p> <pre>tftp://192.168.1.5/image/sip68xx.11-0-IMP-EN.loads</pre> <p>Als er geen protocol wordt opgegeven, wordt TFTP verondersteld. Als er geen servernaam wordt opgegeven, wordt de host die de URL aanvraagt, gebruikt als de servernaam. Als er geen poort wordt opgegeven, wordt de standaardpoort gebruikt (69 voor TFTP, 80 voor HTTP of 443 voor HTTPS).</p> <p>De standaardwaarde is leeg.</p> |
| Log Upgrade Request Msg (Aanvraagbericht upgrade registreren)      | <p>Syslog-bericht dat wordt afgegeven bij de start van een firmware-upgradepoging.</p> <p>Standaard: \$PN \$MAC -- Upgradeverzoek<br/>\$SCHEME://\$SERVIP:\$PORT\$PATH</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Log Upgrade Success Msg (Succesbericht upgrade registreren)        | <p>Syslog-bericht dat wordt afgegeven nadat de firmware-upgradepoging met succes is voltooid.</p> <p>De standaardwaarde is \$PN \$MAC--<br/>Succesvolle upgrade \$SCHEME: / /<br/>\$SERVIP: \$PORT\$ pad--\$ERR</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Log Upgrade Failure Msg (Foutbericht upgrade registreren)          | <p>Syslog-bericht dat wordt afgegeven nadat de firmware-upgradepoging is mislukt.</p> <p>De standaardwaarde is \$PN \$MAC -- Upgrade<br/>mislukt: \$ERR</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Peer firmware delen                                                | <p>Hiermee schakelt u of de functie Peer firmware delen in of uit. Selecteer <b>Ja</b> of <b>Nee</b> om de functie in of uit te schakelen.</p> <p>Standaard: Ja</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Peer Firmware Sharing Log Server (Peer Firmware Sharing-logserver) | <p>Geeft het IP-adres en de poort aan waarnaar het UDP-bericht wordt verzonden.</p> <p>Bijvoorbeeld: 10.98.76.123:514 waarbij 10.98.76.123 het IP-adres is en 514 het poortnummer.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Parameters voor algemene doeleinden

In de volgende tabel worden de functie en het gebruik van elke parameter in de sectie **Parameters voor algemene doeleinden** van het tabblad **Inrichting** gedefinieerd.

| Naam van parameter | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GPP A - GPP P      | <p>De GPP_*-parameters voor algemene doeleinden worden gebruikt als vrije tekenreeks en worden geregistreerd bij het configureren van telefoons om met een bepaalde inrichtingsserveroplossing te werken. Ze kunnen zo worden geconfigureerd dat ze diverse waarden bevatten, zoals de volgende:</p> <ul style="list-style-type: none"> <li>• Coderingssleutels.</li> <li>• URL's.</li> <li>• Statusinformatie voor inrichting met meerdere fasen</li> <li>• Plaatsingsaanvraagjablonen.</li> <li>• Parameternaamaliastoewijzingen.</li> <li>• Gedeeltelijke tekenreekswaarden, uiteindelijk gecombineerd in complete parameterwaarden.</li> </ul> <p>De standaardwaarde is leeg.</p> |

## Variabelen voor macro-uitbreiding

Bepaalde macro-variabelen worden herkend binnen de volgende inrichtingsparameters:

- Profile\_Rule
- Profile\_Rule\_\*
- Resync\_Trigger\_\*
- Upgrade\_Rule
- Log\_\*
- GPP\_\* (onder bepaalde omstandigheden)

Syntaxistypen zoals \$NAME of \$(NAME), worden herkend en uitgebreid binnen deze parameters.

Macro-variabele subtekenreeksen kunnen worden opgegeven met de notatie \$(NAME:p) en \$(NAAM:p:q), waarbij p en q niet-negatieve gehele getallen zijn (beschikbaar in revisie 2.0.11 en hoger). De resulterende macro-uitbreiding is de subtekenreeks die begint bij tekenverschuiving p, met lengte q (of anders tot het einde van de tekenreeks als q niet is gespecificeerd). Bijvoorbeeld, als GPP\_A ABCDEF bevat, wordt \$(A:2) uitgebreid naar CDEF en wordt \$(A:2:3) uitgebreid naar CDE.

Een niet-herkende naam wordt niet vertaald en de vorm \$NAME of \$(NAME) blijft ongewijzigd in de parameterwaarde na uitbreiding.

| Naam van parameter | Beschrijving en standaardwaarde                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$                 | De vorm \$\$ wordt uitgebreid tot één teken \$.                                                                                                                                                                                                                                              |
| A tot en met P     | Vervangen door de inhoud van de parameters voor algemene doeleinden GPP_A tot GPP_P.                                                                                                                                                                                                         |
| SA tot SD          | Wordt vervangen door de speciale parameters GPP_SA tot en met GPP_SD. Deze parameters bevatten toetsen of wachtwoorden voor inrichting.<br><br><b>Opmerking</b> \$SA tot en met \$SD worden herkend als argumenten voor de optionele URL-kwalificatie voor opnieuw synchroniseren,--sleutel. |
| MA                 | MAC-adres met kleine letters hexadecimale tekens, bijvoorbeeld 000e08aabbcc.                                                                                                                                                                                                                 |
| MAU                | MAC-adres met grote hexadecimale tekens, bijvoorbeeld 000E08AABBCC.                                                                                                                                                                                                                          |
| MAC                | MAC-adres met kleine hexadecimale tekens en dubbele punten om hexadecimale tekenparen van elkaar te scheiden. Bijvoorbeeld 00:0e:08:aa:bb:cc.                                                                                                                                                |
| PN                 | Productnaam. Bijvoorbeeld CP-6841-3PCC.                                                                                                                                                                                                                                                      |
| PSN                | Productserienummer. Bijvoorbeeld 6841-3PCC.                                                                                                                                                                                                                                                  |
| SN                 | Tekenreeks voor serienummer, bijvoorbeeld 88012BA01234.                                                                                                                                                                                                                                      |
| CCERT              | Status SSL-clientcertificaat: geïnstalleerd of niet geïnstalleerd.                                                                                                                                                                                                                           |
| IP                 | IP-adres van de telefoon binnen het lokale subnet. Bijvoorbeeld 192.168.1.100.                                                                                                                                                                                                               |
| EXTIP              | Extern IP-adres van de telefoon, zoals weergegeven op het internet. Bijvoorbeeld 66.43.16.52.                                                                                                                                                                                                |
| SWVER              | Tekenreeks softwareversie. Bijvoorbeeld sip68xx.11-0-1MPP.                                                                                                                                                                                                                                   |
| HWVER              | Tekenreeks hardwareversie. Bijvoorbeeld 2.0.1                                                                                                                                                                                                                                                |

| Naam van parameter | Beschrijving en standaardwaarde                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PRVST              | Inrichtingsstatus (een reeks cijfers):<br>-1 = expliciete aanvraag hersynchroniseren<br>0 = opstarten hersynchroniseren<br>1 = periodiek hersynchroniseren<br>2 = synchroniseren is mislukt, nieuwe poging   |
| UPGST              | Status van upgrade (een reeks cijfers):<br>1 = eerste upgradepoging<br>2 = upgrade is mislukt, nieuwe poging                                                                                                 |
| UPGERR             | Resultaatbericht (ERR) van de vorige upgradepoging; bijvoorbeeld http_get is mislukt.                                                                                                                        |
| PRVTMR             | Seconden sinds de laatste hersynchronisatiepoging.                                                                                                                                                           |
| UPGTMR             | Seconden sinds de laatste upgradepoging.                                                                                                                                                                     |
| REGTMR1            | Seconden sinds registratie lijn 1 met SIP-server is verbroken.                                                                                                                                               |
| REGTMR2            | Seconden sinds registratie lijn 2 met SIP-server is verbroken.                                                                                                                                               |
| UPGCOND            | Oude macronaam                                                                                                                                                                                               |
| SCHEME             | Bestandstoegangsschema, TFTP, HTTP of HTTPS, zoals verkregen na het parseren van hersynchronisatie- of upgrade-URL.                                                                                          |
| SERV               | Aanvraag doelserverhostnaam, zoals verkregen na het parseren van de hersynchronisatie- of upgrade-URL.                                                                                                       |
| SERVIP             | Aanvraag doelserver IP-adres, zoals verkregen na het parseren van de hersynchronisatie- of upgrade-URL, mogelijk na een DNS-zoekopdracht.                                                                    |
| PORT               | Aanvraag doel UDP/TCP-poort, zoals verkregen na het parseren van de hersynchronisatie- of upgrade-URL.                                                                                                       |
| PATH               | Aanvraag doelbestandspad, zoals verkregen na het parseren van de hersynchronisatie- of upgrade-URL.                                                                                                          |
| ERR                | Resultaatbericht van hersynchronisatie- of upgradepoging. Alleen nuttig bij het genereren van resultaat syslog-berichten. De waarde wordt behouden in de variabele UPGERR in het geval van upgrade-pogingen. |

| Naam van parameter | Beschrijving en standaardwaarde                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| UIDn               | De inhoud van de configuratieparameter Line n UserID (gebruikers-id voor lijn n). |
| EMS                | Extension Mobility-status                                                         |
| MUID               | Extension Mobility-gebruikers-id                                                  |
| MPWD               | Extension Mobility-wachtwoord                                                     |

## Interne foutcodes

De telefoon definieert een aantal interne foutcodes (X00 - X99) om configuratie te faciliteren door betere controle over het gedrag van het toestel te bieden bij bepaalde foutomstandigheden.

| Naam van parameter | Beschrijving en standaardwaarde                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| X00                | Transportlaagfout (of ICMP-fout) bij het verzenden van een SIP-verzoek.                                                                               |
| X20                | Er ontstaat een time-out met het SIP-verzoek terwijl er wordt gewacht op antwoord.                                                                    |
| X40                | Algemene SIP-protocolfout (bijvoorbeeld een onacceptabele codec in SDP in 200- en ACK-berichten, of er ontstaat een time-out bij het wachten op ACK). |
| X60                | Gekozen nummer is ongeldig volgens het gegeven kiesplan.                                                                                              |





## BIJLAGE A

# Voorbeeld configuratieprofielen

- [Voorbeeld van open XML-indeling, op pagina 81](#)

## Voorbeeld van open XML-indeling

```
<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>
```

```

<!-- 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>

```

```

<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>

```

```

<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>

```

```

<!--
 available options:

-->
<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:

-->
 <!-- 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 -->

```

```

<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

```

```

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_lxx-To-Inv_1_ ua="na">Yes</Ntfy_Refer_On_lxx-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">aslbsoft.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_>

```

```

<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|lxxx[2-9]xxxxxxS0|xxxxxxxxxxxxx.)
</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_lxx-To-Inv_2_ ua="na">Yes</Ntfy_Refer_On_lxx-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_>

```

```

<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|xxxxxxxxxxxxxx.)
</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_lxx-To-Inv_3_ ua="na">Yes</Ntfy_Refer_On_lxx-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_>

```

```

<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]xxxxxS0|xxxxxxxxxxxxx.)
 </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_lxx-To-Inv_4_ ua="na">Yes</Ntfy_Refer_On_lxx-To-Inv_4_>
 <Set_G729_annexb_4_ ua="na">yes</Set_G729_annexb_4_>
 <!--
 available options: none|no|yes|follow silence supp setting
-->

```

```

<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">aslbsoft.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|xxxxxxxxxxxxx.)
</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"/>

```

```

<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"/>

```

```
<!-- 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>
```



## BIJLAGE **B**

# Acroniemen

---

- [Acroniemen, op pagina 103](#)

## Acroniemen

AC	Wisselstroom
ACS	Toegangsbeheerserver
A/D	Converteerder analoog naar digitaal
AES	Advanced Encryption Standard
ANC	Anoniem gesprek
AP	Access point
ASCII	Amerikaanse standaardcode voor de uitwisseling van informatie
B2BUA	Back to Back-gebruikersagent
BLF	Busy Lamp Field (BLF)
Boole	Booleaanse-waarden. Gespecificeerd als Ja en Nee of 1 en 0 in het profiel
BootP	Bootstrap Protocol
CA	Certificeringsinstantie
CAS	CPE-waarschuwingssignaal
CDP	Cisco Discovery Protocol
CDR	Gespreksdetailrecords
CGI	Door de computer gegenereerde Mmagery
CID	Beller-ID
CIDCW	Beller-id wachtend gesprek

CNG	Comfortabel ruis genereren
CPC	Beheer bellende partij
CPE	Klantapparatuur op kantoor
CSV	Comma-Separated Value (door komma gescheiden waarde)
CWCID	Beller-id wachtend gesprek
CWT	Call Waiting Tone (Toon wachtend gesprek)
D/A	Converter digitaal naar analoog
dB	decibel
dBm	dB met betrekking tot 1 milliwatt
DHCP	Dynamic Host Configuration Protocol
NST	Niet storen
DNS	Domain Name System
DoS	Denial of service
DRAM	Dynamic Random Access Memory (dynamisch geheugen met willekeurige toegang)
DSL	Digital Subscriber Loop
DSP	Digitale signaalprocessor
DST	Zomertijd
DTAS	Waarschuwingssignaal gegevensterminal (hetzelfde als CAS)
DTMF	Dubbele toon meerdere frequenties
FQDN	Volledig gekwalificeerde domeinnaam
FSK	Frequentie Shift Keying
Firewall	Firmware
FXS	Foreign eXchange Station
GMT	Greenwich Mean Time
GW	Gateway
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
ICMP	Internet Control Message Protocol

IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	Internet Protocol versie 4
IPv6	Internet Protocol versie 6
ISP	Internet-serviceprovider
ITSP	Internet Telefonie-serviceprovider
ITU	Internationale Telecommunicatie Unie
IVR	Interactive Voice Response (interactieve spraakrespons)
LAN	Local Area Network
LBR	Lage bitrate
LBRC	Lage bitratecodec
LCD	Liquid Crystal Display; ook bekend als scherm
LDAP	Lightweight Directory Access Protocol
Led	Light-Emiting Diode
MAC-adres	Media Access Control-adres
MC	Mini-certificaat
MGCP	Media Gateway Control Protocol (besturingsprotocol voor mediagateway)
MOH	Music On Hold
MOS	Mean Opinion Score (1-5, hoe hoger hoe beter)
MPP	Telefoons voor meerdere platforms
ms	Milliseconde
MSA	Adapter voor muziekbron
MWI	Indicatie voor wachtend bericht
NAT	Network Address Translation
NPS	Normale inrichtingsserver
NTP	Netwerktijdprotocol
OOB	Out-of-band
OSI	Open schakelinterval

PBX	Private branch exchange
PCB	Printplaat
PoE	Power over Ethernet
PR	Polariteitomkering
PS	Inrichtingsserver
PSQM	Perceptuele spraakkwaliteitsmeting (1-5, hoe lager hoe beter)
PSTN	Openbaar geschakeld telefoonnetwerk
QoS	Quality-of-service
Redencode	Aanpassing verwijderen
REQT	(SIP) verzoeksbericht
RESP	(SIP) antwoordbericht
RSC	(SIP) antwoordstatuscode, zoals 404, 302, 600
RTP	Real Time Protocol
RTT	Retourtijd
SAS	Streamingserver voor audio
SDP	Session Description Protocol
SDRAM	Synchroon DRAM
sec.	seconden
SIP	Session Initiation Protocol
SLA	Weergave van gedeelde lijn
SLIC	Interfacecircuit van abonneelijn
SP	Serviceprovider
SSL	Secure Socket Layer
STUN	Session Traversal UDP voor NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security (TLS)
TTL	Time to live
ToS	Type service



UA	Gebruikersagent
uC	Micro-controller
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Gecoördineerde wereldtijd
VAR	Value Added Reseller
VLAN	Voice LAN
VM	Voicemail
VMWI	Visuele indicatie/indicator voor wachtend bericht
VoIP	Voice over Internet Protocol (Sprak via IP)
VQ	Stemkwaliteit
WAN	WAN
XML	Extensible Markup Language





## BIJLAGE **C**

### Verwante documentatie

---

- [Verwante documentatie](#), op pagina 109
- [Ondersteuningsbeleid voor Cisco IP Phone-firmware](#), op pagina 109

### Verwante documentatie

Gebruik de volgende gedeelten om gerelateerde informatie te verkrijgen.

#### Documentatie van de Cisco IP Phone 6800-serie

Raadpleeg de publicaties voor uw taal, telefoonmodel en firmwarerelease voor meerdere platforms. Ga vanuit de volgende Uniform Resource Locator (URL):

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

#### Ondersteuningsbeleid voor Cisco IP Phone-firmware

Zie voor meer informatie over het ondersteuningsbeleid voor telefoons, <https://cisco.com/go/phonefirmwaresupport>.

