Vodnik za omogočanje uporabe telefonov Cisco IP Phone 6800 Series za več platform

Prvič objavljeno: 2017-11-22

Nazadnje spremenjeno: 2019-01-30

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

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

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

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

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

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

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

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

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

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

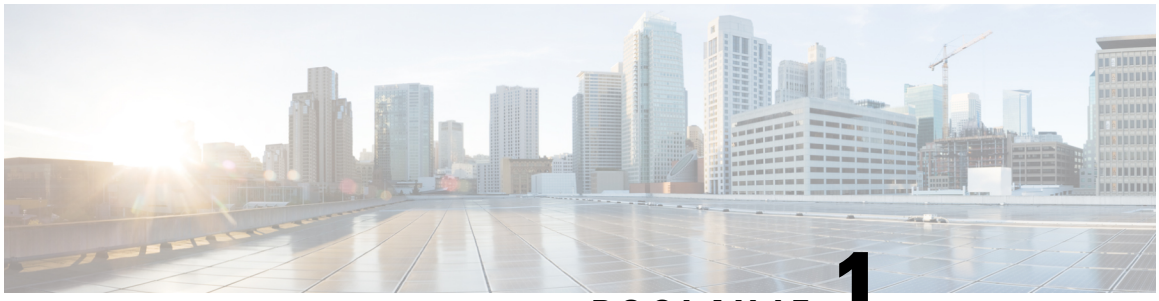
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

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

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

VSEBINA



POGLAVJE 1

Uvajanje in omogočanje uporabe

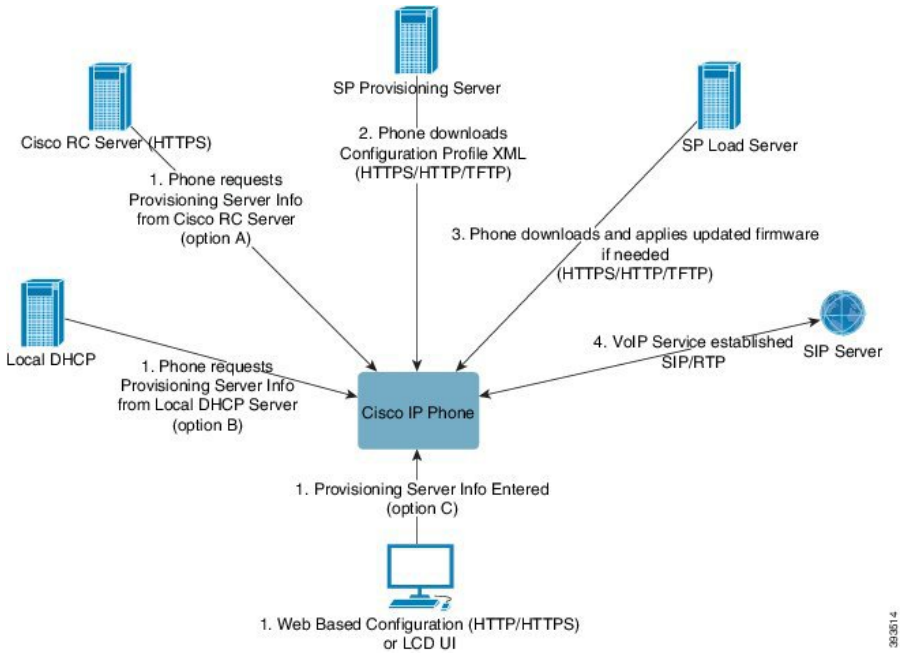
Pregled omogočanja uporabe

Telefoni Cisco IP Phone so namenjeni za množično uvajanje s strani ponudnikov storitev VoIP (Voice-over-IP) strankam v gospodinjskih, poslovnih in velikih poslovnih okoljih. Omogočanje uporabe telefona z oddaljenim upravljanjem in konfiguracijo zato zagotavlja pravilno delovanje telefona na strankinem mestu uporabe.

Cisco podpira prilagojeno stalno konfiguriranje funkcij telefona z uporabo:

- zanesljivega daljinskega upravljanja telefona,
- šifriranja komunikacijskega strežnika, ki nadzira telefon,
- učinkovitega povezovanja z računom telefona.

Telefone je mogoče pripraviti tako, da iz oddaljenega strežnika prenesejo konfiguracijske profile ali posodobljeno vdelano programsko opremo. Prenosi se lahko izvedejo ob priključitvi telefona v omrežje, ob vklopu in ob vnaprej določenih intervalih. Omogočanje uporabe je običajno za množično uvajanje sistemov VoIP, ki je pogosto pri ponudnikih storitev. Konfiguracijski profili ali posodobljena vdelana programska oprema se v napravo prenesejo s protokolom TFTP, HTTP ali HTTPS.



Postopek omogočanja uporabe telefona je na visoki ravni tak:

1. Če telefon ni konfiguriran, se podatki iz strežnika za omogočanje uporabe v telefonu uporabijo z eno od teh možnosti:
   - **A** – prenos iz strežnika Cisco Enablement Data Orchestration System (EDOS) Remote Customization (RC) z uporabo protokola HTTPS;
   - **B** – s poizvedbo lokalnemu strežniku DHCP;
   - **C** – z ročnim vnosom prek spletnega konfiguracijskega orodja Ciscovih telefonov ali uporabniškega vmesnika telefona.
2. Telefon s protokolom HTTPS, HTTP ali TFTP prenese podatke iz strežnika za omogočanje uporabe in konfiguracijski XML.
3. Telefon s protokolom HTTPS, HTTP ali TFTP po potrebi prenese posodobljeno vdelano programsko opremo in jo uporabi.
4. Storitev VoIP se vzpostavi z navedeno konfiguracijo in vdelano programsko opremo.

Ponudniki storitev VoIP želijo uvesti veliko število telefonov strankam v gospodinjstvih in malih podjetjih. V podjetjih ali velikih poslovnih okoljih lahko telefoni delujejo kot zaključna vozlišča. Ponudniki po internetu množično distribuirajo te naprave, ki so povezane prek usmerjevalnikov in požarnih zidov v prostorih strank.

Telefon je mogoče uporabiti kot oddaljeni podaljšek zaledne opreme ponudnika storitev. Oddaljeno upravljanje in konfiguracija zagotavljata pravilno delovanje telefona v prostorih strank.

Omogočanje za uporabo s parametri TR69

Cisco IP Phone pomaga skrbniku konfigurirati parametre TR69 prek spletnega uporabniškega vmesnika. Informacije, povezane s parametri, vključno s primerjavo parametrov XML in TR69, najdete v vodniku za skrbnike za ustrezno serijo telefonov.

Telefoni podpirajo odkrivanje ACS (Auto Configuration Server) iz možnosti DHCP 43, 60 in 125.

- Možnost 43 – podatki o URL-ju za ACS za posameznega dobavitelja.
- Možnost 60 – identifikator razreda dobavitelja, s katerim se telefon prek `dslforum.org` predstavi strežniku ACS.
- Možnost 125 – podatki za povezavo s prehodom za posameznega dobavitelja.

Metode RPC

Podprte metode RPC

Telefoni podpirajo samo omejen nabor metod RPC (Remote Procedure Call), ki so navedene v nadaljevanju:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: prenos metode RPC, podprte vrste datotek so:
  - Posnetek za nadgradnjo vdelane programske opreme
  - Dobaviteljeva konfiguracijska datoteka
  - Prilagojena datoteka overitelja potrdila (CA)
- Transfer Complete

Podprte vrste dogodkov

Telefoni podpirajo vrste dogodkov na podlagi podprtih funkcij in načinov. Podprte so samo te vrste dogodkov:

- prvi zagon
- zagon
- sprememba vrednosti
- zahteva za povezavo
- občasen
- prenos končan
- M-prenos
- M-vnovični zagon

Vedenje telefona ob zasedenem omrežju

- Skrbniške dejavnosti, kot je pregled notranjih vrat ali varnostni pregled
- Napadi na vaše omrežje, kot je napad DoS.

Uvajanje

Telefoni Cisco IP Phone ponujajo priročen mehanizem za omogočanje uporabe na podlagi teh modelov uvajanja:

- Množična distribucija – ponudnik storitev pridobi veliko število telefonov Cisco IP Phone in jih interno vnaprej omogoči za uporabo ali pa od Cisca kupi enote za oddaljeno prilagajanje (RC). Naprave se nato izdajo strankam v okviru pogodbe o storitvah VoIP.
- Maloprodajna distribucija – stranka kupi telefon Cisco IP Phone v maloprodaji in zahteva storitev VoIP od ponudnika storitev. Ponudnik storitev mora nato podpirati varno oddaljeno konfiguracijo naprave.

Množična distribucija

Pri tem modelu ponudnik storitev telefone izda svojim strankam v okviru pogodbe o storitvah VoIP. Naprave so enote RC ali interno vnaprej omogočene za uporabo.

Cisco enote RC vnaprej omogoči za uporabo tako, da se resinhronizirajo s Ciscovim strežnikom, ki prenese profil naprave in posodobitve vdelane programske opreme.

Ponudnik storitev lahko telefone na različne načine vnaprej omogoči za uporabo z želenimi parametri, vključno s parametri, ki nadzirajo resinhronizacijo:

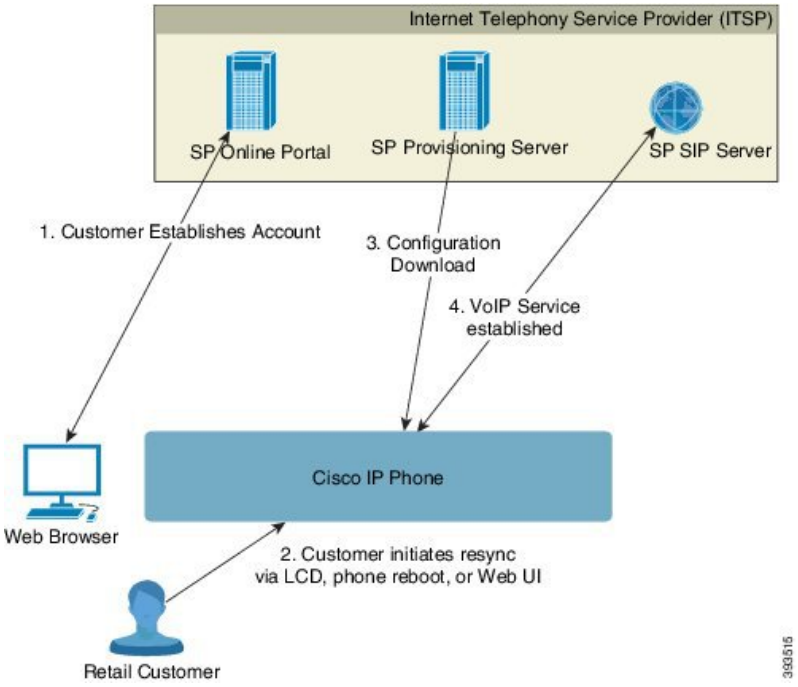
- Interno z uporabo protokolov DHCP in TFTP
- Na daljavo z uporabo protokolov TFTP, HTTP ali HTTPS

- S kombinacijo internega in oddaljenega omogočanja uporabe

Maloprodajna distribucija

V maloprodajnem distribucijskem modelu stranka kupi telefon in se naroči na določeno storitev. Ponudnik telefonskih storitev nastavi in vzdržuje strežnik za omogočanje uporabe in telefon vnaprej omogoči za uporabo tako, da se redno resinhronizira s strežnikom ponudnika storitev.

Slika 1: Maloprodajna distribucija



Telefon ima spletno konfiguracijsko orodje, ki prikaže notranjo konfiguracijo in sprejeme nove vrednosti konfiguracijskih parametrov. Strežnik sprejme tudi posebno sintakso ukazov URL za izvajanje postopkov resinhronizacije profila in nadgradnje vdelane programske opreme na daljavo.

Stranka se prijavi v storitev in vzpostavi račun VoIP, po možnosti prek spletnega portala, in napravo poveže z dodeljenim računom storitve. Telefon, ki še ni omogočen za uporabo, dobi ukaz za resinhronizacijo s strežnikom prek ukaza URL-ja za resinhronizacijo. Ukaz URL običajno vključuje strankino številko-ID-ja računa ali alfanumerično kodo, s katero se naprava poveže z novim računom.

V naslednjem primeru naprava na naslovu IP 192.168.1.102, ki ga dodeli DHCP, prejme ukaz, da se omogoči za uporabo s storitvijo SuperVoIP:

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

V tem primeru je 1234abcd strankina številka ID-ja za novi račun. Strežnik za oddaljeno omogočanje uporabe poveže telefon, ki izvaja zahtevo za resinhronizacijo, z novim računom na podlagi URL-ja in navedenega ID-ja stranke. Telefon se s tem začetnim postopkom resinhronizacije konfigurira v enem koraku. Od takrat naprej je telefon samodejno usmerjen, da se resinhronizira s trajnim URL-jem v strežniku. Na primer:

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

Strežnik za omogočanje uporabe uporablja odjemalsko potrdilo telefona za preverjanje pristnosti tako pri prvotnem kot tudi pri trajnem dostopu. Strežnik za omogočanje uporabe zagotovi pravilne vrednosti konfiguracijskega parametra na podlagi povezanega računa storitve.

Ob vklopu naprave ali po določenem časovnem obdobju, se telefon resinhronizira in prenese najnovejše parametre. Ti parametri so lahko uporabljeni za namene, kot je nastavitev iskalne skupine, nastavitev številk za hitro klicanje in omejevanje funkcij, ki jih lahko spremeni uporabnik.

Sorodne teme

Interno predomogočanje uporabe naprav, na strani 39

Postopek resinhronizacije

Vdelana programska oprema vsakega telefona vsebuje skrbniški spletni strežnik, ki sprejema nove vrednosti konfiguracijskih parametrov. Z ukazom URL-ja za resinhronizacijo v profilu naprave je mogoče določiti, da telefon po vnovičnem zagonu ali ob načrtovanih intervalih resinhronizira konfiguracijo z določenim strežnikom za omogočanje uporabe.

Spletni strežnik je privzeto omogočen. Spletni strežnik lahko onemogočite ali omogočite z ukazom URL-ja za resinhronizacijo.

Po potrebi je mogoče zahtevati takojšnjo resinhronizacijo z URL-jem za dejanje "resync". Ukaz URL za resinhronizacijo lahko vključuje strankino številko-ID-ja računa ali alfanumerično kodo, s katero se naprava enolično poveže z uporabnikovim računom.

Primer

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

V tem primeru naprava na naslovu IP 192.168.1.102, ki ga dodeli DHCP, prejme ukaz, da se omogoči za uporabo s storitvijo SuperVoIP na naslovu prov.supervoip.com. Strankina številka ID-ja za novi račun je 1234abcd. Strežnik za oddaljeno omogočanje uporabe poveže telefon, ki izvaja zahtevo za resinhronizacijo, z računom na podlagi URL-ja in ID-ja stranke.

Telefon se s tem začetnim postopkom resinhronizacije konfigurira v enem koraku. Od takrat naprej je telefon samodejno usmerjen, da se resinhronizira s trajnim URL-jem v strežniku.

Strežnik za omogočanje uporabe uporablja odjemalsko potrdilo za preverjanje pristnosti tako pri prvotnem kot tudi pri trajnem dostopu. Strežnik zagotovi vrednosti konfiguracijskega parametra na podlagi povezanega računa storitve.

Nadziranje

Telefon je mogoče konfigurirati tako, da stanje svoje notranje konfiguracije redno in ob vklopu resinhronizira tako, da se ujema z oddaljenim profilom. Telefon vzpostavi povezavo z navadnim strežnikom za omogočanje uporabe (NPS) ali strežnikom za nadzor dostopa (ACS).

Poskus resinhronizacije profila se privzeto izvede samo, ko je telefon nedejaven. To prepreči nadgradnjo, ki bi sprožila vnovični zagon programske opreme in prekinila klic. Če so za doseganje trenutnega stanja nadgradnje s starejše izdaje potrebne vmesne nadgradnje, lahko logika nadgradnje avtomatizira večstopenjske nadgradnje.

Običajni strežnik za omogočanje uporabe

Navaden strežnik za omogočanje uporabe (NPS) je lahko strežnik TFTP, HTTP ali HTTPS. Oddaljena nadgradnja vdelane programske opreme se izvede s protokolom TFTP, HTTP ali HTTPS, ker vdelana programska oprema ne vsebuje občutljivih podatkov.

Priporočamo sicer HTTPS, vendar za komunikacijo z NPS ni potreben varen protokol, ker je posodobljeni profil mogoče šifrirati s skrivnim ključem v skupni rabi. Za več informacij o uporabi protokola HTTPS si oglejte temo Šifriranje komunikacije, na strani 8. Varno prvo omogočanje uporabe je zagotovljeno z mehanizmom, ki uporablja funkcije SSL. Telefon, ki ni omogočen za uporabo, lahko prejme profil, šifriran z 256-bitnim simetričnim ključem, ki je ciljan prav za to napravo.

Konfiguriranje nadzora dostopa

Vdelana programska oprema telefona ponuja mehanizme za omejevanje dostopa končnih uporabnikov do nekaterih parametrov. Vdelana programska oprema omogoča določene pravice za prijavo v račun **skrbnika** ali **uporabnika**. Vsakega od teh računov je mogoče ločeno zaščiti z geslom.

- Skrbniški račun – ponudniku storitev omogoča poln dostop do vseh parametrov skrbniškega spletnega strežnika.
- Uporabniški račun – uporabniku omogoča konfiguriranje podskupine parametrov skrbniškega spletnega strežnika.

Ponudnik storitev lahko uporabniški račun na naslednje načine omeji v profilu za omogočanje uporabe:

- določi, kateri konfiguracijski parametri so na voljo uporabniškemu računu pri ustvarjanju konfiguracije;
- onemogoči uporabniški dostop do skrbniškega spletnega strežnika;
- onemogoči uporabniški dostop za uporabniški vmesnik na zaslonu LCD;
- obide zaslon **Nastavitev gesla** za uporabnika;
- omeji internetne domene, do katerih naprava dostopa za resinhronizacijo, nadgradnje ali registracijo SIP za linijo 1.

Sorodne teme

Lastnosti oznake elementa, na strani 14
Nadzor dostopa, na strani 16

Dostop do spletne strani telefona

Spletno stran telefona odprite iz brskalnika v računalniku, ki lahko telefon doseže v podomrežju.

Če je ponudnik storitev onemogočil dostop do konfiguracijskega orodja, se pred nadaljevanjem obrnite nanj.

Postopek

Korak 1 Poskrbite, da bo računalnik lahko komuniciral s telefonom. VPN se ne uporablja.

Korak 2 Odprite brskalnik.

Korak 3 V naslovno vrstico brskalnika vnesite naslov IP telefona.

- Uporabniški dostop: **http://<ip address>/user**
- Skrbniški dostop: **http://<ip address>/admin/advanced**
- Skrbniški dostop: **http://<ip address>**, kliknite **Prijava skrbnika** in kliknite **Dodatno**

Primer: `http://10.64.84.147/admin`

Omogočanje spletnega dostopa do telefona Cisco IP Phone

Če si želite ogledati parametre telefona, omogočite konfiguracijski profil. Če želite spremeniti katerega od parametrov, morate imeti možnost spreminjanja konfiguracijskega profila. Skrbnik sistema je v telefonu morda onemogočil možnost, da je spletni uporabniški vmesnik telefona viden ali omogoča zapisovanje.

Več informacij je na voljo v *Vodniku za omogočanje uporabe telefonov Cisco IP Phone 6800 Series za več platform*.

Preden začnete

Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Postopek

Korak 1 Kliknite **Glas** > **Sistem**.

Korak 2 V razdelku **Sistemska konfiguracija** nastavite možnost **Omogoči spletni strežnik** na **Da**.

Korak 3 Če želite posodobiti konfiguracijski profil, kliknite **Pošlji vse spremembe**, potem ko v spletnem uporabniškem vmesniku telefona spremenite polja.

Telefon se znova zažene in spremembe so uveljavljene.

Korak 4 Če želite počistiti vse spremembe, ki ste jih izvedli v trenutni seji (ali potem, ko ste zadnjič kliknili **Pošlji vse spremembe**), kliknite **Razveljavi vse spremembe**. Vrednosti se vrnejo na prejšnje nastavitve.

Šifriranje komunikacije

Konfiguracijski parametri, sporočeni napravi, lahko vsebujejo avtorizacijske kode ali druge podatke, ki sistem ščitijo pred nepooblaščenim dostopom. V interesu ponudnika storitev je, da prepreči nepooblaščeno dejavnost strank. V interesu stranke je, da prepreči nepooblaščeno uporabo računa. Ponudnik storitev lahko šifrira komunikacijo konfiguracijskega profila med strežnikom za omogočanje uporabe in napravo, poleg tega pa tudi omeji dostop do skrbniškega spletnega strežnika.

Postopki za omogočanje uporabe telefonov

Cisco IP Phone je običajno konfiguriran za omogočanje uporabe, ko se prvič poveže v omrežje. Telefon je omogočen za uporabo tudi ob vnaprej določenih intervalih, ki jih nastavi ponudnik storitev ali prodajalec z dodano vrednostjo, ko vnaprej omogoči uporabo (konfigurira) telefona. Ponudniki storitev lahko prodajalcem z dodano vrednostjo ali izkušenim uporabnikom dovolijo ročno omogočanje uporabe telefona s tipkovnico telefona. Omogočanje uporabe lahko konfigurirate tudi v spletnem uporabniškem vmesniku telefona.

V uporabniškem vmesniku na zaslonu LCD telefona preverite **Stanje** > **Stanje telefona** > **Omogočanje uporabe** oziroma na zavihku **Stanje** spletnega konfiguracijskega orodja preverite stanje omogočanja uporabe.

Sorodne teme

Ročno omogočanje uporabe telefona s tipkovnico, na strani 9

Ročno omogočanje uporabe telefona s tipkovnico

Postopek

Korak 1 Pritisnite **Aplikacije** .

Korak 2 Izberite **Skrbništvo naprave** > **Pravilo za profil**.

Korak 3 Pravilo za profil vnesite v tej obliki:

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

Na primer:

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

Če ni naveden protokol, se uporabi TFTP. Če ni navedeno ime strežnika, se uporabi ime gostitelja, ki zahteva URL. Če niso navedena vrata, se uporabijo privzeta vrata (69 za TFTP, 80 za HTTP ali 443 za HTTPS).

Korak 4 Pritisnite **PonSinh**.

Sorodne teme

Postopki za omogočanje uporabe telefonov, na strani 8

Skupna raba vdelane programske opreme med enakovrednimi

Peer Firmware Sharing (PFS) je model distribucije vdelane programske opreme, ki telefonu Cisco IP Phone omogoča iskanje drugih telefonov enakega modela ali serije v podomrežju in skupno rabo posodobljenih datotek z vdelano programsko opremo, ko morate hkrati nadgraditi več telefonov. PFS uporablja protokol CPPDP (Cisco Peer-to-Peer-Distribution Protocol), ki je Ciscov lastniški protokol. Pri uporabi CPPDP vse naprave v podomrežju ustvarijo hierarhijo enakovrednih naprav, nato pa prekopirajo vdelano programsko opremo ali druge datoteke iz enakovrednih naprav v sosednje. Za optimizacijo nadgradenj vdelane programske opreme korenski telefon prenese posnetek vdelane programske opreme s strežnika za nalaganje, nato pa prenese vdelano programsko opremo v druge telefone v podomrežju prek povezav TCP.

Skupna raba vdelane programske opreme med enakovrednimi:

- omeji zastoje pri prenosih TFTP na centralizirane strežnike za nalaganje;
- odstrani potrebo po ročnem nadzorovanju nadgradenj vdelane programske opreme;
- med nadgradnjami skrajša čas nedelovanja telefona, če hkrati ponastavljate večje število telefonov.

Opomba

- PFS ne deluje, razen če je več telefonov nastavljeno za hkratno nadgradnjo. Ko je z ukazom Event:resync poslan NOTIFY, se sproži vnovična sinhronizacija telefona. Primer kode xml, ki lahko vsebuje konfiguracije za sprožanje nadgradnje:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Ko nastavite strežnik dnevnika PFS (Peer Firmware Sharing) na naslov IP in vrata, so dnevniki, specifični za PFS, poslani temu strežniku kot sporočila UDP. Ta nastavitev je potrebna na vseh telefonih. Dnevniška sporočila lahko nato uporabite za odpravljanje težav, povezanih s PFS.

Peer_Firmware_Sharing_Log_Server določa ime gostitelja in vrata oddaljenega strežnika sistemskega dnevnika UDP. Vrata so privzeto nastavljena na privzeto vrednost za sistemski dnevnik 514.

Na primer:

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

Če želite uporabiti to funkcijo, na telefonu omogočite PFS.

Obidenje zaslona za nastavitev gesla

Zaslon **Nastavitev gesla** v telefonu lahko obidete ob prvem zagonu ali po tovarniški ponastavitvi, in sicer s temi postopki za omogočanje uporabe:

- Konfiguracija DHCP
- Konfiguracija EDOS
- Konfiguracija gesla uporabnika s konfiguracijsko datoteko XML v telefonu.

Tabela 1: Dejanja za omogočanje uporabe, ki določajo, ali je prikazan zaslon za nastavitev gesla

DHCP je konfiguriran	EDOS je konfiguriran	Geslo uporabnika je konfigurirano	Obidenje zaslona za nastavitev gesla
da	N/R	da	da
da	N/R	ne	**ne**
ne	da	da	da
ne	da	ne	**ne**
ne	ne	N/R	**ne**

Postopek

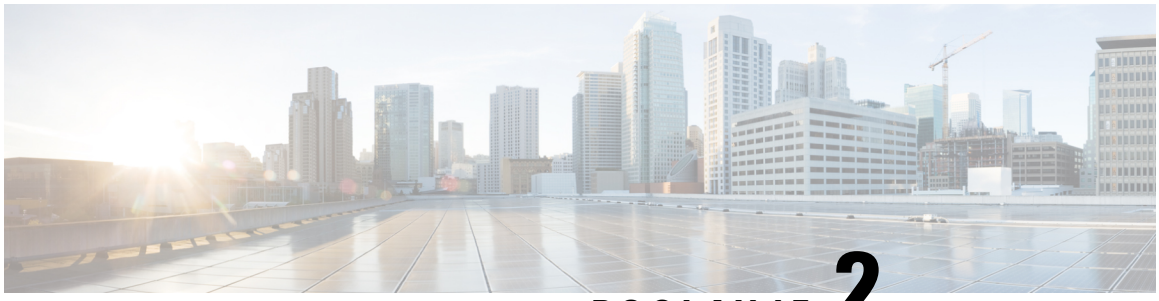
Korak 1 Uredite datoteko `config.xml` za telefon v urejevalniku besedila ali zapisov XML.

Korak 2 Z eno od teh možnosti vstavite oznako **<User_Password>**.

- **Brez gesla (začetna in končna oznaka)**–**<User_Password></User_Password>**

- **Vrednost gesla (4–127 znakov)**–`<User_Password ua="rw">abc123</User_Password>`
- **Brez gesla (samo začetna oznaka)**–`<User_Password />`

Korak 3 Spremembe shranite v datoteko `config.xml`.



POGLAVJE 2

Skripti za omogočanje uporabe

Skripti za omogočanje uporabe

Telefon sprejema konfiguracijo v obliki XML.

Če želite podrobne informacije o telefonu, si oglejte vodnik za skrbnike za svoj model naprave. V vsakem vodniku so opisani parametri, ki jih je mogoče konfigurirati prek skrbniškega spletnega strežnika.

Oblike konfiguracijskega profila

Konfiguracijski profil določa vrednosti parametrov za telefon.

Oblika XML konfiguracijskega profila uporablja standardna orodja za pripravo kode XML za prevajanje parametrov in vrednosti.

Opomba Podprt je samo nabor znakov UTF-8. Če profil spremenite v urejevalniku, ne spreminjajte oblike kodiranja, sicer telefon ne bo mogel prepoznati datoteke.

Vsak telefon ima drugačen nabor funkcij in posledično tudi drugačen nabor parametrov.

Profil v obliki XML (XML)

Odprta oblika profila je besedilna datoteka s sintakso, podobno XML-ju, v hierarhiji elementov z atributi in vrednostmi elementov. Ta oblika omogoča uporabo standardnih orodij za ustvarjanje konfiguracijske datoteke. Konfiguracijsko datoteko v tej obliki je mogoče med postopkom resinhronizacije poslati iz strežnika za omogočanje uporabe v telefon. Datoteko je mogoče poslati brez prevajanja v dvojiški predmet.

Telefon lahko sprejme oblike konfiguracije, ki jih generirajo standardna orodja. Ta funkcija poenostavlja razvoj programske opreme za zaledne strežnike za omogočanje uporabe, ki konfiguracijske profile generira iz obstoječih zbirk podatkov.

Strežnik za omogočanje uporabe to vrsto datoteke prenese telefonu prek kanala, zaščitenega s protokolom TLS, da zaščiti zaupne podatke v konfiguracijskem profilu. Datoteke je mogoče tudi stisniti z uporabo algoritma gzip deflate (RFC1951).

Datoteko je mogoče šifrirati z enim od teh načinov šifriranja:

- Šifriranje AES-256-CBC
- Šifriranje vsebine HTTP na podlagi RFC-8188 z uporabo AES-128-GCM

Primer: odprta oblika profila

```
<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>
```

Okoli vseh elementov parametrov, ki jih telefon prepozna, mora biti oznaka elementa <flat-profile>.

Sorodne teme

Stiskanje in šifriranje odprtega profila (XML), na strani 17

Komponente konfiguracijske datoteke

Konfiguracijska datoteka lahko vsebuje te komponente:

- Oznake elementov
- Atribute
- Parametre
- Oblikovne funkcije
- Komentarje XML

Lastnosti oznake elementa

- Oblika zapisa XML za omogočanje uporabe in spletni uporabniški vmesnik omogočata konfiguracijo istih nastavitev. Ime oznake XML in imena polj v spletnem uporabniškem vmesniku so podobna, vendar se razlikujejo zaradi omejitev imen elementov XML. Primer: podčrtaji (_) namesto narekovajev (" ").
- Telefon prepozna elemente s pravilnimi imeni parametrom, ki so enkapsulirani v posebnem elementu <flat-profile>.
- Imena elementov so med znakoma < in >.
- Večina imen elementov je podobnih imenom polj na skrbniških spletnih straneh za napravo s temi spremembami:

- Imena elementov ne smejo vsebovati presledkov ali posebnih znakov. Če želite iz imena polja skrbniških spletnih strani izpeljati ime elementa, vse presledke ali posebne zanke `[, ], (, )` ali `/` zamenjajte s podčrtaji.

  Primer: element <Resync_On_Reset> predstavlja polje **Resync On Reset**.

- Vsako ime elementa mora biti edinstveno. Na skrbniških spletnih straneh se lahko ista polja pojavijo na več spletnih straneh, na primer na straneh Linija, Uporabnik in Interna številka. Če želite navesti številko, ki je prikazana na zavihku strani, imenu elementa dodajte pripono `[n]`.

  Primer: element <Dial_Plan_1_> predstavlja **načrt klicanja** za linijo 1.

- Vsaka otvoritvena oznaka elementa mora imeti ustrezno zaključno oznako elementa. Na primer:

```
<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>
```

- Oznake elementov razlikujejo med velikimi in malimi črkami.
- Prazne oznake elementov so dovoljene in bodo razumljene, kot da določajo prazno vrednost. Vnesite otvoritveno oznako elementa brez ustrezne oznake elementa ter pred zaključni znak > vstavite presledek in poševnico naprej. V te, primeru je vrednost Profile Rule B prazna:

```
<Profile_Rule_B />
```

- Prazno oznako elementa lahko uporabite za preprečevanje prepisa morebitnih uporabniško določenih vrednosti med postopkom resinhronizacije. V naslednjem primeru so uporabniške nastavitve za hitro klicanje nespremenjene:

```
<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>
```

- Uporabite prazno vrednost za nastavitev ustreznega parametra na prazen niz. Vnesite otvoritveni in zaključni element brez vmesne vrednosti. V naslednjem primeru je parameter GPP_A nastavljen na prazen niz.

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

- Neprepoznana imena elementov so prezrta.

Sorodne teme

Konfiguriranje nadzora dostopa, na strani 7

Atribut za uporabniški dostop

Za spreminjanje dostopa za uporabniški račun je mogoče uporabiti kontrolnike atributa za uporabniški dostop (**ua**). Če atribut **ua** ni naveden, se ohrani obstoječa nastavitev uporabniškega dostopa. Ta atribut ne vpliva na dostop, ki ga ima skrbniški račun.

Če je nastavljen atribut **ua**, mora imeti eno od teh vrednosti:

- na – ni dostopa
- ro – samo za branje
- rw – branje in pisanje

Naslednji primer kaže uporabo atributa **ua**:

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

Vrednost možnosti **ua** mora biti v dvojnih narekovajih.

Nadzor dostopa

Če je omogočen parameter <Phone-UI-User-Mode>, grafični uporabniški vmesnik (GUI) telefona upošteva atribut za uporabniški dostop v ustreznih parametrih, ko GUI prikaže menijski element.

Za menijske vnose, ki so povezani z enim samim konfiguracijskim parametrom:

- Če parameter nastavite z atributom "ua=na" ("ua" pomeni "user access" – uporabniški dostop), vnos izgine.
- Če parameter nastavite z atributom "ua=ro", je vnos samo za branje in ga ni mogoče urejati.

Za menijske vnose, ki so povezani z več konfiguracijskimi parametri:

- Če vse zadevne parametre nastavite z atributom "ua=na", vnosi izginejo.

Sorodne teme

Konfiguriranje nadzora dostopa, na strani 7

Lastnosti parametrov

Te lastnosti veljajo za vse parametre:

- Morebitni parametri, ki niso določeni v profilu, v telefonu ostanejo nespremenjeni.
- Neprepoznani parametri se prezrejo.
- Če profil v odprti obliki vsebuje več pojavitev iste oznake parametra, zadnja taka pojavitev preglasi morebitne prejšnje. Zaradi preprečitve nenamerne preglasitve konfiguracijskih vrednosti parametra priporočamo, da je v vsakem profilu določen največ en primerek parametra.

- Prednost ima zadnji obdelani profil. Če več profilov določa enak konfiguracijski parameter, ima prednost vrednost zadnjega profila.

Oblike zapisa nizov

Za obliko zapisa nizov veljajo te lastnosti

- Komentarji so dovoljeni prek standardne sintakse XML.

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

- Začetni in končni presledek je dovoljen zaradi berljivosti, vendar se odstrani iz vrednosti parametra.
- Nove vrstice v vrednosti se pretvorijo v presledke.
- Glava XML v obliki `<? ?>` je dovoljena, vendar jo telefon prezre.
- Za vnos posebnih znakov uporabite osnovna ubežna zaporedja znakov XML, kot je prikazano v naslednji tabeli.

Posebni znak	Ubežno zaporedje XML
& (ampersand)	&
< (manj kot)	<
> (več kot)	>
’ (apostrof)	'
” (dvojni narekovaj)	"

V naslednjem primeru ubežni znaki predstavljajo znaka "več kot" in "manj kot", ki sta potrebna v pravilu načrta klicanja. V tem primeru opredelimo načrt klicanja za informacijsko klicno linijo, ki parameter <Dial_Plan_1_> (**Prijava skrbnika** > **dodatno** > **Glas** > **Int (n)**) nastavi tako, da je enak (S0 <:18005551212>).

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

- Ubežne vrednosti za številske znake, ki uporabljajo desetiške in šestnajstiške vrednosti (npr. `(` in `.`) so prevedeni.
- Vdelana programska oprema telefona podpira samo znake ASCII.

Stiskanje in šifriranje odprtega profila (XML)

Odprt konfiguracijski profil je mogoče stisniti, da se zmanjša omrežna obremenitev strežnika za omogočanje uporabe. Profil je mogoče tudi šifrirati za zaščito zaupnih podatkov. Stiskanje ni obvezno, vendar se mora izvesti pred šifriranjem.

Sorodne teme

Oblike konfiguracijskega profila, na strani 13

Stiskanje odprtega profila

Podprt način stiskanja je algoritem gzip deflate (RFC1951). Orodje gzip in knjižnica za stiskanje, ki uporablja isti algoritem (zlib), sta na voljo na internetnih mestih.

Telefon za prepoznavanje stiskanja pričakuje, da bo stisnjena datoteka imela glavo, združljivo s stiskanjem gzip. Glavo generirate z uporabo orodja gzip na izvirnem odprtem profilu. Telefon pregleda glavo prenesene datoteke, da bi ugotovil obliko zapisa.

Če je na primer `profile.xml` veljaven profil, je sprejeta tudi datoteka `profile.xml.gz`. To vrsto profila lahko generirate z enim od teh ukazov:

- `>gzip profile.xml`

  Prvotno datoteko zamenja s stisnjeno.

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

  Izvirna datoteka ostane nespremenjena, ustvari se nova stisnjena datoteka.

V razdelku Stiskanje odprtega profila z orodjem Gzip, na strani 60 je na voljo več informacij o stiskanju.

Sorodne teme

Stiskanje odprtega profila z orodjem Gzip, na strani 60

Šifriranje odprtega profila

Šifriranje s simetričnim ključem je mogoče uporabiti za šifriranje odprtega konfiguracijskega profila ne glede na to, ali je datoteka stisnjena ali ne. Če se uporablja stiskanje, ga je treba uporabiti pred šifriranjem.

Strežnik za omogočanje uporabe uporablja HTTPS za začetno omogočanje uporabe telefona po uvedbi. Če konfiguracijske profile vnaprej šifrirate, ko naprava ni povezana v omrežje, je mogoče za resinhronizacijo profilov uporabiti HTTP. S tem se zmanjša obremenitev strežnika HTTPS pri množičnem uvajanju.

Telefon podpira dva načina šifriranja za konfiguracijske datoteke:

- Šifriranje AES-256-CBC
- Šifriranje vsebine HTTP na podlagi RFC-8188 z uporabo AES-128-GCM

Ključ ali IKM je treba vnaprej predomogočiti za uporabo v enoti. Zagonsko uporabo skrivnega ključa je mogoče varno izvesti z uporabo HTTPS-ja.

Za ime konfiguracijske datoteke ni določena posebna oblika, vendar ime datoteke s pripono `.cfg` običajno označuje konfiguracijski profil.

Šifriranje AES-256-CBC

Telefon podpira šifriranje AES-256-CBC za konfiguracijske datoteke.

Za izvedbo šifriranja lahko uporabite orodje za šifriranje OpenSSL, ki ga lahko prenesete z različnih internetnih mest. Podpora za 256-bitno šifriranje AES lahko zahteva vnovično prevajanje orodja, da se omogoči koda AES. Vdelana programska oprema je bila preskušena z različico openssl-0.9.7c.

Šifriranje profila z OpenSSL-jem, na strani 61 vsebuje vadnico o šifriranju.

Profil za šifrirano datoteko pričakuje, da je datoteka v isti obliki, kot bi jo generiral ta ukaz:

```
# 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
```

Pred skrivnim ključem, ki je lahko poljubna besedna zveza v navadnem besedilu in se uporablja za generiranje naključne 64-bitne soli, je mala črka -k. Orodje za šifriranje s skrivnim ključem, ki ga določa argument -k, izpelje naključni 128-bitni zaletni vektor in dejanski 256-bitni šifrirni ključ.

Ko se ta oblika šifriranja uporabi za konfiguracijski profil, je treba telefon obvestiti o vrednosti skrivnega ključa, da bo lahko dešifriral datoteko. Ta vrednost je navedena kot kvalifikator v URL-ju profila. Sintaksa je opisana v nadaljevanju in uporablja eksplicitni URL:

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

Ta vrednost se programira z uporabo enega od parametrov Profile_Rule.

Sorodne teme

Šifriranje profila z OpenSSL-jem, na strani 61

Razširitev makrov

Za več parametrov za omogočanje uporabe se pred razreševanjem izvede interna razširitev makrov. Ta korak vnaprejšnjega ocenjevanja ponuja veliko prilagodljivost pri nadzoru dejavnosti resinhronizacije in nadgradnje telefona.

Za te skupine parametrov se razširitev makrov izvede pred razreševanjem:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

Pod določenimi pogoji se razširitev makrov izvede tudi za parametre splošnega namena (GPP_*), kot je izrecno navedeno v razdelku Izbirni argumenti za resinhronizacijo, na strani 22.

Pri razširitvi makrov vsebina poimenovanih spremenljivk zamenja izraze v obliki $NAME in $(NAME). Te spremenljivke vključujejo parametre splošnega namena, več identifikatorjev izdelkov, nekatere časovnike dogodkov in vrednosti stanja omogočanja uporabe. Popoln seznam je v razdelku Spremenljivke za razširitev makrov, na strani 72.

V naslednjem primeru se izraz $(MAU) uporabi za vstavljanje naslova MAC 000E08012345.

Skrbnik vnese: **`$(MAU)config.cfg`**

Nastala razširitev makrov za napravo, ki ima naslov MAC 000E08012345, je: `000E08012345config.cfg`

Če ime makra ni prepoznano, ostane nerazširjen. Primer: ime STRANGE ni prepoznano kot veljavno ime makra, MAU pa je.

Skrbnik vnese: **$STRANGE$MAU.cfg**

Nastala razširitev makrov za napravo, ki ima naslov MAC 000E08012345, je:
`$STRANGE000E08012345.cfg`

Razširitev makrov se ne uporablja rekurzivno. Primer: $$MAU" se razširi v $MAU" ($$ se razširi) in rezultat ni naslov MAC.

Vsebina parametrov za posebne namene od GPP_SA do GPP_SD se preslika na izraze makrov od $SA do $SD. Ti parametri se razširijo kot makri samo kot argumenti možnosti **--key** , **--uid** in **--pwd** v URL-ju za resinhronizacijo.

Pogojni izrazi

Pogojni izrazi lahko sprožijo dogodke resinhronizacije in izbirajo med alternativnimi URL-ji za postopke resinhronizacije in nadgradnje.

Pogojni izrazi so sestavljeni iz seznama primerjav, ločenih z operatorjem **and**. Pogoj bo imel vrednost "true", če so izpolnjene vse primerjave.

Vsaka primerjava se lahko nanaša na eno od naslednjih treh vrst vnosov:

- celoštevilske vrednosti
- številke različic programske ali strojne opreme
- nizi v dvojnih narekovajih

številke različic

Formalna različica izdaje programske opreme za telefone za več platform uporablja to obliko zapisa, pri čemer je BN==Build Number (številka delovne različice):

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

Primerjalni niz mora biti v enaki obliki zapisa. Sicer pride do napake razčlenjevanja oblike zapisa.

V različici programske opreme lahko v1-v2-v3-v4 določa različne številke in znake, vendar se mora začeti s številko. Pri primerjavi različice programske opreme se v1-v2-v3-v4 primerja zaporedno in skrajne leve številke imajo prednost pred poznejšimi.

Če v[x] vključuje samo številke, se te primerjajo, če v[x] vključuje številke + abecedne znake, se najprej primerjajo številk, nato pa znaki v abecednem redu.

Primer veljavne številke različice

sipyyyy.11-0-0MPP-BN

Primer neveljaven oblike: 11.0.0.

Primerjava

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

Nize v narekovajih je mogoče primerjati glede na enakost ali neenakost. Cela števila in številke različic je mogoče primerjati aritmetično. Primerjavo med operaterji je mogoče izraziti kot simbole ali kot kratice. Kratice so priročne za izražanje pogoja v profilu odprte oblike.

Operator	Alternativna sintaksa	Opis	Velja za celoštevilske operande in operande številk različice	Velja za operande nizov v narekovajih
=	eq	enako	da	da
!=	ne	ni enako	da	da
<	lt	manj kot	da	ne
<=	le	manj kot ali enako	da	ne
>	gt	več kot	da	ne
>=	ge	več kot ali enako	da	ne
AND		in	da	da

Pomembno je, da so spremenljivke makrov v dvojnih narekovajih, kjer je pričakovan vnos niza. Vendar pa tega ne storitev, kjer je pričakovano število ali številka različice.

Ko so pogojni izrazi uporabljeni v kontekstu parametrov Profile_Rule* in Upgrade_Rule, morajo biti v sintaksi “(expr)?” koz v tem primeru pravila za nadgradnjo. Upoštevajte, da BN pomeni Build Number (številka delovne različice).

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

Zgornje sintakse z oklepaji ne uporabljajte za konfiguriranje parametrov Resync_Trigger_*.

Sintaksa URL-jev

S standardno skladnjo URL lahko v parametru Profile_Rule* oziroma Upgrade_Rule podate, kako prenesti konfiguracijske datoteke in nalaganja vdelane programske opreme. Sintaksa je naslednja:

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

Pri čemer je **`scheme`** ena od teh vrednosti:

- tftp
- http
- HTTPS

Če **`scheme`** izpustite, se uporabi tftp. Vrednost "server" je lahko gostiteljsko ime, ki ga prepozna DNS, ali številski naslov IP. Vrednost "port" je številka ciljnih vrat UDP ali TCP. Vrednost"filepath" se mora začeti s korenskim imenikom (/) in mora biti absolutna pot.

Če vrednost **`server`** manjka, se uporabi strežnik tftp, določen z DHCP-jem (možnost 66).

Opomba Za pravila za nadgradnjo je treba določiti strežnik.

Če vrednost **port** manjka, se uporabijo standardna vrata za navedeno shemo. Tftp uporablja vrata UDP 69, http uporablja vrata TCP 80, https pa vrata TCP 443.

Pot datoteke je obvezna. Ni sicer nujno, da se nanaša na statično datoteko, temveč lahko kaže dinamično vsebino, pridobljeno prek CGI.

V URL-jih se uporablja razširitev makrov. Nekaj primerov veljavnih URL-jev:

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

Pri uporabi možnosti DHCP 66 pravila nadgradnje ne podpirajo prazne skladnje. To velja samo za pravilo profila*.

Šifriranje vsebine HTTP na podlagi RFC-8188

Telefon podpira šifriranje vsebine HTTP na podlagi RFC-8188 z uporabo AES-128-GCM za konfiguracijske datoteke. S tem način šifriranja, lahko vsaka oseba, preberite HTTP glave sporočil. Vendar pa laho vsebino preberejo samo entitete, ki poznajo IKM (Input Keying Material). Ko je za telefon omogočena uporaba z IKM, lahko telefon in strežnik za omogočanje uporabe varno izmenjata konfiguracijske datoteke, medtem ko lahko omrežni elementi drugih ponudnikov uporabijo glave sporočil za namene analiziranja in spremljanja.

Konfiguracijski parameter XML **IKM_HTTP_Encrypt_Content** vsebuje IKM v telefonu. Zaradi varnostnih razlogov ta parameter ni dostopen na spletnem mestu za skrbništvo telefona. Prav tako ni viden v konfiguracijski datoteki telefona, do katere lahko dostopate iz naslova IP telefona ali iz konfiguracijskih poročil, poslanih strežniku za omogočanje uporabe.

Če želite uporabiti šifriranje na podlagi RFC 8188, poskrbite za naslednje:

- Telefon omogočite za uporabo z IKM, tako da IKM določite s parametrom XML **IKM_HTTP_Encrypt_Content** v konfiguracijski datoteki, poslani iz strežnika za omogočanje uproabe v telefon.
- Če je to šifriranje uporabljeno za konfiguracijske datoteke, poslane iz strežnika za omogočanje uporabe v telefon, poskrbite, da bo glava HTTP *Content-Encoding* v konfiguracijski datoteki imela “aes128gcm”.

  Če te glave ni, ima prednost način AES-256-CBC. Telefon uporablja dešifriranje AES-256-CBC, če je v pravilu profila ključ AES-256-CBC, ne glede na IKM.
- Če želite, da telefon uporabi to šifriranje za konfiguracijska poročila, ki jih pošlje strežniku za omogočanje uporabe, poskrbite, da v pravilu za poročilo ne bo naveden ključ AES-256-CBC.

Izbirni argumenti za resinhronizacijo

Izbirni argumenti **key**, **uid** in **pwd** so lahko pred URL-ji, ki jih vnesete v parametre za Profile_Rule*, in vsi skupaj v oglatih oklepajih.

key

Možnost **--key** telefonu pove, da je konfiguracijska datoteka, ki jo prejme iz strežnika za omogočanje, šifrirana s šifriranjem AES-256-CBC, razen če glava *Content-Encoding* v datoteki določa šifriranje "aes128gcm". Sam ključ je naveden kot niz po izrazu **--key**. Ključ je lahko izbirno naveden v dvojnih narekovajih ("). Telefon uporablja ključ za dešifiranje konfiguracijske datoteke.

Primeri uporabe

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

Izbirni argumenti v oklepajih so razširjeni z makri. Parametri za posebne namene (od GPP_SA do GPP_SD) so z makri razširjeni v spremenljivke makra od $SA do $SD, samo ko se uporabljajo kot argumenti ključnih možnosti. Oglejte si te primere:

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

V profilih odprte oblike mora biti argument, ki je naveden za **--key**, enak kot argument za možnost **-k**, ki je naveden za **openssl**.

uid in pwd

Možnosti **uid** in **pwd** je mogoče uporabiti za določanje preverjanja pristnosti navedenega URL-ja z uporabniškim imenom in geslom. Izbirni argumenti v oklepajih so razširjeni z makri. Parametri za posebne namene (od GPP_SA do GPP_SD) so z makri razširjeni v spremenljivke makra od $SA do $SD, samo ko se uporabljajo kot argumenti ključnih možnosti. Oglejte si te primere:

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

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

se razširi v:

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

Uporaba profila za napravo za telefonijo IP

Ko ustvarite konfiguracijski skript XML, ga je treba prenesti v telefon, da ga bo lahko uporabil. Če želite uporabiti konfiguracijo, lahko konfiguracijsko datoteko prenesete v telefon iz strežnika TFTP, HTTP ali HTTPS z uporabo spletnega brskalnika ali orodja ukazne vrstice cURL.

Prenos konfiguracijske datoteke v telefon iz strežnika TFTP

Če želite konfiguracijsko datoteko prenesti v program strežnika TFTP v računalniku, uporabite ta postopek.

Postopek

Korak 1 Računalnik povežite s krajevnim omrežjem telefona.

Korak 2 V računalniku zaženite program strežnika TFTP in poskrbite, da bodo konfiguracijske datoteke v korenskem imeniku za TFTP.

Korak 3 V brskalnik vnesite naslov IP telefona v krajevnem omrežju, naslov IP računalnika, ime datoteke in poverilnice za prijavo. Uporabite to obliko:

http://<naslov_IP_prostranegaomrežja>/admin/resync?tftp://<naslov_IP_računalnika>/<ime_datoteke>&user=admin&password=<geslo>

Primer:

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

Prenos konfiguracijske datoteke v telefon z orodjem cURL

Če želite konfiguracijsko datoteko prenesti v telefon z orodjem cURL, uporabite ta postopek. To orodje ukazne vrstice se uporablja za prenos podatkov s sintakso URL-jev. Če želite prenesti cURL, obiščite:

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

Opomba Priporočamo, da orodja cURL ne uporabite za prenos konfiguracije v telefon, ker lahko pri tem pride do zajema uporabniškega imena in gesla.

Postopek

Korak 1 Računalnik priključite na omrežna vrata telefona.

Korak 2 Konfiguracijsko datoteko prenesite v telefon z uporabo tega ukaza cURL:

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

Parametri za omogočanje uporabe

V tem razdelku so opisani parametri za omogočanje uporabe, ki so na splošno razvrščeni glede na funkcijo:

Obstajajo ti parametri za omogočanje uporabe:

- Splošna uporaba
- Omogočanja
- Sprožilniki
- Nastavljivi urniki

- Pravila za profil
- Pravilo za nadgradnjo

Parametri splošnega namena

Parametri splošnega namena GPP_* (**Prijava skrbnika** > **Dodatno** > **Glas** > **Omogočanje uporabe**) se uporabljajo kot prosti registri za nize pri konfiguriranju telefona za interakcijo z določeno strežniško rešitvijo za omogočanje uporabe. Parametri GPP_* so privzeto prazni. Konfigurirati jih je mogoče z raznolikimi vrednostmi, vključno z naslednjimi:

- šifrirni ključi,
- URL-ji,
- podatki o stanju večstopenjskega omogočanja uporabe,
- predloge za objavo zahtev,
- preslikave vzdevkov imen parametrov,
- delne vrednosti nizov, ki so sčasoma kombinirane v celotne vrednosti parametrov.

Parametri GPP_* so na voljo za razširitev makrov z drugimi parametri za omogočanje uporabe. Za ta namen za identifikacijo vsebine GPP_A do GPP_P zadostujejo enomestna imena makrov z velikimi črkami (A do P). Dvomestna imena makrov z velikimi črkami od SA do SD določajo GPP_SA do GPP_SD kot poseben primer, če jih uporabite kot argumente naslednjih možnosti URL-jev:

key, **uid** in **pwd**

Te parametre je mogoče uporabiti kot spremenljivke v pravilih za omogočanje uporabe in nadgradnjo. Sklic nanje se izvede tako, da imenu spremenljivke dodate predpono z znakom "$", kot je $GPP_A.

Uporaba parametrov splošnega namena

Če GPP_A na primer vsebuje niz ABC in GPP_B vsebuje 123, bo izraz AB z makri razširjen v ABC123.

Preden začnete

Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Postopek

Korak 1 Izberite **Glas** > **Omogočanje uporabe**.

Korak 2 Pomaknite se do razdelka **Parametri splošnega namena**.

Korak 3 V polja GPP A do GPP P vnesite veljavne vrednosti.

Korak 4 Kliknite **Pošlji vse spremembe**.

Omogočanja

Parametra Provision_Enable in Upgrade_Enable nadzirata vse postopke resinhronizacije profilov in nadgradnje vdelane programske opreme. Ta parametra nadzirata resinhronizacije in nadgradnje neodvisno drug od drugega. Ta parametra nadzirata tudi ukaze URL-jev za resinhronizacijo in nadgradnjo, izdane prek skrbniškega spletnega strežnika. Oba ta parametra sta privzeto nastavljena na **Yes (Da)**.

Parameter Resync_From_SIP nadzira zahteve za postopke resinhronizacije. Iz strežnika proxy ponudnika storitev se v telefon pošlje dogodek SIP NOTIFY. Če je omogočen, lahko strežnik proxy zahteva resinhronizacijo. To strežnik proxy stori tako, da napravi pošlje sporočilo SIP NOTIFY, ki vsebuje glavo "Event: resync".

Naprava se na zahtevo odzove s pozivom 401 (avtorizacija zavrnjena za uporabljene poverilnice). Naprava nato pričakuje zahtevo s preverjeno pristnostjo, preden izvede zahtevo za resinhronizacijo iz strežnika proxy. Glavi Event: reboot_now in Event: restart_now izvedeta strojni oziroma programski vnovični zagon, ki sta prav tako zavrnjena s pozivom.

Preostali omogočanji sta Resync_On_Reset in Resync_After_Upgrade_Attempt. Ta parametra določata, ali naprava izvede postopek resinhronizacije po vnovičnem zagonu programske opreme ob vklopu in po vsakem poskusu nadgradnje.

Ko je omogočen parameter Resync_On_Reset, naprava vstavi naključno zakasnitev, ki sledi postopku zagona, preden izvede ponastavitev. Zakasnitev je naključen časovni interval do vrednosti, ki jo določa Resync_Random_Delay (v sekundah). V skupini telefonov, ki se hkrati vklopijo, ta zakasnitev porazdeli čase zagona in zahteve za resinhronizacijo iz posameznih enot. Ta funkcija je lahko koristna v velikem stanovanjskem sistemu, če pride do območnega izpada napajanja.

Sprožilniki

Telefon omogoča resinhronizacijo ob določenih intervalih ali ob določeni uri.

Resinhroniziranje ob določenih intervalih

Telefon je zasnovan tako, da se redno resinhronizira s strežnikom za omogočanje uporabe. Interval resinhronizacije je konfiguriran v Resync_Periodic (v sekundah). Če to vrednost pustite prazno, se naprava ne resinhronizira ob rednih intervalih.

Resinhroniziranje se običajno izvede, ko so glasovne linije nedejavne. Če je glasovna linija aktivna, ko naj bi se izvedla resinhronizacija, telefon resinhronizacijo odloži, dokler ni linija spet nedejavna. Resinhronizacija lahko povzroči spremembo vrednosti konfiguracijskih parametrov.

Postopek resinhronizacije lahko ne uspe, če telefon ne more prenesti profila iz strežnika, če je prenesena datoteka poškodovana ali če je prišlo do notranje napake. Naprava poskuša resinhronizacijo spet izvesti po času, navedenem v Resync_Error_Retry_Delay (v sekundah). Če je Resync_Error_Retry_Delay nastavljen na 0, naprava po neuspešnem poskusu resinhronizacije ne poskuša resinhronizirati.

Če nadgradnja ne uspe, se vnovični poskus izvede po številu sekund, določenem v Upgrade_Error_Retry_Delay.

Na voljo sta dva parametra, ki ju je mogoče konfigurirati in lahko pogojno sprožita resinhronizacijo: Resync_Trigger_1 in Resync_Trigger_2. Vsak parameter je mogoče programirati s pogojnim izrazom, za katerega se izvede razširitev makrov. Ko poteče interval za resinhronizacijo (čas za naslednjo resinhronizacijo), bodo morebitni nastavljeni sprožilniki razrešeni na vrednost "true".

Naslednji primer pogoja sproži resinhronizacijo. V tem primeru je minilo več kot 5 minut (300 sekund) od zadnjega poskusa nadgradnje telefona in vsaj 10 minut (600 sekund) od zadnjega poskusa resinhronizacije.

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

Resinhronizacija ob določeni uri

Parameter Resync_At, da telefon izvede resinhronizacijo ob določeni uri. Ta parameter uporablja 24-urno obliko (hhmm) za določanje ure.

Parameter Resync_At_Random_Delay telefonu omogoča izvedbo resinhronizacije z nenavedeno zakasnitvijo. Ta parameter uporablja obliko pozitivnega celega števila za določanje ure.

Preplavitvi telefona z zahtevami za resinhronizacijo iz več telefonov, ki so nastavljeni, da se resinhronizira ob istem času, se je treba izogibati. Telefon to stori tako, da resinhronizacijo sproži do 10 minut po navedenem času.

Če na primer nastavite, da je ura resinhronizacije 1000 (10 dopoldne), telefon resinhronizacijo sproži kadar koli med 10.00 in 10.10 dopoldan.

Ta funkcija je privzeto onemogočena. Če je nastavljen parameter Resync_At, se parameter Resync_Periodic prezre.

Nastavljivi urniki

S temi parametri za omogočanje uporabe lahko nastavite urnike za redne resinhronizacije in določite intervale, ob katerih naj se ob neuspešnih resinhronizacijah in nadgradnjah izvedejo vnovični poskusi:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Vsak parameter sprejme eno vrednost za zakasnitev (v sekundah). Nova razširjena sintaksa omogoča uporabo z vejicami ločenega seznama zaporednih elementov zakasnitve. Zadnji element v zaporedju se implicitno za vedno ponavlja.

Izbirno lahko uporabite znak plus (+), da določite drugo številsko vrednost, ki doda naključno dodatno zakasnitev.

Primer 1

V tem primeru se telefon redno resinhronizira vsaki 2 uri. Če resinhronizacija ne uspe, naprava poskuša znova ob teh intervalih: 30 minut, 1 ura, 2 uri, 4 ure. Naprava poskuse ponavlja v 4-urnih intervalih, dokler ne izvede uspešne resinhronizacije.

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

Primer 2

V tem primeru se telefon redno resinhronizira vsako uro (plus dodatna naključna zakasnitev do 10 minut). Če resinhronizacija ne uspe, naprava poskuša znova ob teh intervalih: 30 minut (plus največ 5 minut). 1 ura (plus največ 10 minut), 2 uri (plus največ 15 minut). Naprava poskuse ponavlja v 2-urnih intervalih (plus največ 15 minut), dokler ne izvede uspešne resinhronizacije.

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

Primer 3

Če v tem primeru poskus oddaljene nadgradnje ne uspe, naprava znova poskuša čez 30 minut, nato spet čez eno uro in nato spet čez dve. Če nadgradnja še vedno ne uspe, naprava poskuša vsakih štiri do pet ur, dokler ne uspe.

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

Pravila za profil

Telefon ponuja več parametrov oddaljenega konfiguracijskega profila (Profile_Rule*). Tako lahko vsak postopek resinhronizacije pridobi več datotek, ki jih upravljajo različni strežniki.

V najpreprostejšem primeru se naprava vsake toliko časa sinhronizira z enim samim profilom v osrednjem strežniku, ki posodobi vse ustrezne notranje parametre. Profil je mogoče razdeliti med različnimi datotekami. Ena datoteka je skupna za vse telefone v posameznem uvajanju. Za vsak račun je zagotovljena ločena edinstvena datoteka. Šifrirni ključi in podatki o potrdilih so lahko pridobljeni iz spet drugega profila, shranjenega v ločenem strežniku.

Telefon vsakič, ko naj se zgodi postopek resinhronizacije, v zaporedju oceni štiri parametre profile_Rule*:

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

Rezultat vsakega razreševanja je lahko prenos profila iz oddaljenega strežnika za omogočanje uporabe, možna pa je tudi posodobitev določenega števila notranjih parametrov. Če razreševanje ne uspe, je zaporedje resinhronizacije prekinjeno in se poskuša znova izvesti od začetka, navedenega v parametru Resync_Error_Retry_Delay (v sekundah). Če vsa razreševanja uspejo, naprava počaka toliko sekund, kot je določeno s parametrom Resync_Periodic, in nato izvede še eno resinhronizacijo.

Vsebina vsakega parametra Profile_Rule* je sestavljena iz več alternativ. Alternative so ločene z navpičnico (|). Vsaka alternativa je sestavljena iz pogojnega izraza, dodelitvenega izraza, URL-ja profila in morebitnih povezanih možnosti za URL. Vse te komponente so izbirne v vsaki alternativi. V nadaljevanju so veljavne kombinacije in vrstni red, v katerem morajo biti, če so prisotne:

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

V vsakem parametru Profile_Rule* morajo vse alternative razen zadnje navesti pogojni izraz. Ta izraz se oceni in obdela na naslednji način:

1. Pogoji se razrešujejo od leve proti desni, dokler ni najden tak, katerega rešitev je "true" (oziroma je najdena alternativa brez pogojnega izraza).
2. Če je prisoten povezan dodelitveni izraz, se prav tako razreši.

3. Če je v okviru zadevne alternative naveden URL, se izvede poskus prenosa profila, ki je na lokaciji navedenega URL-ja. Sistem poskuša ustrezno posodobiti notranje parametre.

Če imajo vse alternative pogojne izraze in ni rešitev nobenega "true" (ali če je celotno pravilo profila prazno), se preskoči celoten parameter Profile_Rule*. Nadaljuje se razreševanje naslednjega parametra pravila profila v zaporedju.

Primer 1

Ta primer se brezpogojno resinhronizira s profilom na navedenem URL-ju in izvede zahtevo HTTP GET oddaljenemu strežniku za omogočanje uporabe:

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

Primer 2

V tem primeru se naprava resinhronizira z dvema različnima URL-jema, kar je odvisno od stanja registracije linije 1. V primeru izgubljene registracije naprava izvede ukaz HTTP POST skriptu CGI. Naprava pošlje vsebino z makrom razširjenega GPP_A, ki lahko vsebuje dodatne podatke o stanju naprave:

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

Primer 3

V tem primeru se naprava resinhronizira z istim strežnikom. Naprava posreduje dodatne podatke, če v napravi ni nameščeno potrdilo (za starejše naprave pred različico 2.0):

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

Primer 4

V tem primeru je linija 1 onemogočena, dokler ni GPP_A prek prvega URL-ja nastavljen tako, da je enako "Provisioned". Potem se resinhronizira z drugim URL-jem:

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

Primer 5

V tem primeru se sklepa, da profil, ki ga vrne strežnik, vsebuje oznake elementa XML. Te oznake je treba preslikati v ustrezna imena parametrov s preslikavo vzdevkov, shranjeno v GPP_B:

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

Običajno se obravnava, da resinhronizacija ni uspešna, če iz strežnika ni prejet zahtevani profil. Parameter Resync_Fails_On_FNF lahko preglasi ta privzeti način delovanja. Če je Resync_Fails_On_FNF nastavljen

na "No" (Ne), naprava kot uspešno resinhronizacijo od strežnika sprejme odgovor, da datoteka ni najdena. Privzeta vrednost za Resync_Fails_On_FNF je "Yes" (Da).

Pravilo za nadgradnjo

Pravilo za nadgradnjo napravi pove, naj aktivira novo nalaganje, in po potrebi, kje ga dobiti. Če je nalaganje že v napravi, ga ne bo poskusila dobiti. Veljavnost mesta nalaganja torej ni pomembna, ko je želeno nalaganje v neaktivni particiji.

Upgrade_Rule določa nalaganje vdelane programske opreme. Če se to razlikuje od trenutnega nalaganja, bo preneseno in uporabljeno, razen če je omejeno s pogojnim izrazom ali je možnost Upgrade_Enable nastavljena na **Ne**.

Telefon ponuja en parameter za oddaljeno nadgradnjo, ki ga je mogoče konfigurirati: Upgrade_Rule. Ta parameter sprejema sintakso, podobno parametrom za pravila profila. Možnosti URL-ja niso podprte za nadgradnje, lahko pa uporabite pogojne in dodelitvene izraze. Če uporabite pogojni izraz, je parameter mogoče izpolniti z različnimi možnostmi, ločenimi z znakom |. Sintaksa za posamezne možnosti je naslednja:

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

Tako kot v primeru parametrov Profile_Rule* parameter Upgrade_Rule razrešuje posamezne možnosti, dokler ni izpolnjen pogojni izraz oziroma možnost nima pogojnega izraza. Če je naveden povezan dodelitveni izraz, se prav tako razreši. Nato se izvede poskus nadgradnje na navedeni URL.

Če Upgrade_Rule vsebuje URL brez pogojnega izraza, naprava nadgradi na posnetek vdelane programske opreme, ki jo določa URL. Po razširitvi makrov in razreševanju pravila naprava ne poskuša znova nadgraditi, dokler ni pravilo spremenjeno oziroma je spremenjena veljavna kombinacija sheme + strežnika + vrat + poti datoteke.

Pred poskusom nadgradnje vdelane programske opreme naprava onemogoči zvok, na koncu postopka pa se znova zažene. Naprava samodejno začne nadgradnjo, ki temelji na vsebini parametra Upgrade_Rule, samo če so vse glasovne linije trenutno nedejavne.

Primer:

- Za Cisco IP 6800 Series:

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

  where BN==Build Number
  ```

V tem primeru Upgrade_Rule nadgradi vdelano programsko opremo na posnetek, ki je shranjen na navedenem URL-ju.

Tu je še en primer za Cisco IP Phone 6800 Series:

```
("$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
```

V tem primeru enoti damo navodila, da naloži enega od dveh posnetkov, in sicer na podlagi vsebine parametra splošnega namena GPP_F.

Naprava lahko uveljavi omejitev vrnitve na starejšo različico vdelane programske opreme, kar je lahko koristna možnost za prilagajanje. Če je v parametru Downgrade_Rev_Limit konfigurirana veljavna številka različice

vdelane programske opreme, naprava zavrne poskuse nadgradnje na različice vdelane programske opreme, starejše od navedene omejitve.

Vrste podatkov

S parametri konfiguracijskega profila se uporabljajo te vrste podatkov:

- {a,b,c,…} – izbira med a, b, c, …
- Bool – logična vrednost "yes" (da) ali "no" (ne)
- CadScript – miniskript, ki določa parametre pogostosti signala (do 127 znakov)

  Sintaksa: $S_1[;S_2]$, pri čemer:

  - $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ in se imenuje razdelek.
  - $on_{i,j}$ in $off_{i,j}$ sta trajanje vklopa/izklopa (v sekundah) za *segment*. i = 1 ali 2 in j = 1 do 6.
  - D_i je skupno trajanje razdelka (v sekundah).

  Vsa trajanja imajo lahko največ tri decimalna mesta za 1 ms ločljivost. Nadomestni znak "*" označuje neskončno trajanje. Segmenti v razdelku se predvajajo v zaporedju in ponavljajo, dokler ni predvajano celotno skupno trajanje.

  Primer 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
  ```

  Primer 2 – značilno zvonjenje (kratko,kratko,kratko,dolgo):

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

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

  Total Ring Length = 60s
  ```

- DialPlanScript – skriptna sintaksa, ki se uporablja za določanje načrtov klicanja za liniji 1 in 2
- Float<n> – vrednost s plavajočo vejico z največ n decimalnimi mesti
- FQDN – popolnoma določeno ime domene; vsebuje lahko do 63 znakov. Nekaj primerov:
  - sip.Cisco.com:5060 ali 109.12.14.12:12345

- sip.Cisco.com ali 109.12.14.12

- FreqScript – miniskript, ki določa parametre za frekvenco in raven tona; vsebuje do 127 znakov.

  Sintaksa: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, pri čemer:

  - F_1–F_6 so frekvence v Hz (samo cela števila brez predznaka).
  - L_1–L_6 so ustrezne ravni v dBm (z največ enim decimalnim mestom).

  Presledki pred vejico in po njej so dovoljeni, vendar niso priporočeni.

  Primer 1 – ton za klic na čakanju:

```
440@-10

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

  Primer 2 – klicni ton:

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

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

- IP – veljaven naslov IPv4 v obliki x.x.x.x, pri čemer je x med 0 in 255 Primer 10.1.2.100.
- UserID – ID uporabnika, kot je prikazan v URL-ju; do 63 znakov
- Phone – niz telefonske številke, kot je 14081234567, *69, *72, 345678, ali splošen URL, kot je 1234@10.10.10.100:5068 ali jsmith@Cisco.com Niz ima lahko največ 39 znakov.
- PhTmplt – predloga za telefonsko številko Vsaka predloga lahko vsebuje enega ali več vzorcev, ki so ločeni z vejico (,). Presledki na začetku vzorcev se prezrejo. "?" in "*" predstavljata nadomestne znake. Če želite uporabiti sam znak, uporabite %xx. %2a na primer predstavlja znak *. Predloga lahko vsebuje največ 39 znakov. Primeri: "1408*, 1510*", "1408123????, 555?1.".
- Vrata – številka vrat TCP/UDP (0–65535) Navedena je lahko v desetiški ali šestnajstiški obliki.
- ProvisioningRuleSyntax – skriptna sintaksa, ki se uporablja za določanje pravil za konfiguracijsko resinhronizacijo nadgradnje vdelane programske opreme.
- PwrLevel – raven moči, izražena v dBm z enim decimalnim mestom, kot je –13,5 ali 1,5 (dBm).
- RscTmplt – predloga kode za stanja odziva SIP, kot so "404, 5*", "61?", "407, 408, 487, 481". vsebuje lahko do 39 znakov.
- Sig<n> – n-bitna vrednost s predznakom Navedena je lahko v desetiški ali šestnajstiški obliki. Pred negativnimi vrednostmi mora biti znak "–" (minus). Predznak "+" pred pozitivnimi vrednostmi ni obvezen.
- Star Codes – koda za aktiviranje za dopolnilno storitev, na primer *69 Koda lahko ima največ 7 znakov.
- Str<n> – generičen niz z največ n nerezerviranimi znaki.
- Time<n> – trajanje (v sekundah) z največ n decimalnimi mesti Dodatna navedena decimalna mesta se prezrejo.

- ToneScript – miniskript, ki določa parametre za frekvenco, raven in pogostost tona za napredovanje klica Skript lahko vsebuje do 127 znakov.

  Sintaksa: FreqScript;Z_1[;Z_2].

  Razdelek Z_1 je podoben razdelku S_1 v skriptu CadScript, razen tega, da vsakemu segmentu "on/off" sledi parameter frekvenčne komponente: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$, pri čemer:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ določa frekvenčne komponente v skriptu FreqScript, ki se uporabljajo v tem segmentu.

  Če je v segmentu uporabljenih več frekvenčnih komponent, se komponente seštejejo.

  Primer 1 – klicni ton:

```
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
```

  Primer 2 – zaostali ton:

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

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

Total Tone Length = 12s
```

- Uns<n> – n-bitna vrednost brez predznaka, pri čemer je n = 8, 16 ali 32. Določena je lahko v desetiški ali šestnajstiški obliki, na primer 12 ali 0x18, pod pogojem, da je vrednost mogoče določiti z n biti.

Opomba Upoštevajte naslednje:

- <Par Name> predstavlja ime konfiguracijskega parametra. V profilu se ustrezna oznaka oblikuje tako, da se presledek zamenja s podčrtajem "_", na primer **Par_Name**.
- Prazno polje za privzeto vrednost označuje prazen niz < “” >.
- Telefon še naprej uporablja zadnje konfigurirane vrednosti za oznake, ki niso navedene v danem profilu.
- Predloge se primerjajo v navedenem vrstnem redu. Izbere se prvo ujemanje, *ne najbližje*. Ime parametra se mora natančno ujemati.
- Če je v profilu navedenih več definicij parametra, se v telefonu uporabi zadnja taka definicija v datoteki.
- Navedba parametra s prazno vrednostjo parametra mu vsili nazaj privzeto vrednost. Če želite namesto tega določiti prazen niz, kot vrednost parametra uporabite prazen niz "".

Posodobitve profila in nadgradnje vdelane programske opreme

Telefon podpira varno oddaljeno omogočanje uporabe (konfiguracijo) in posodobitve vdelane programske opreme. Telefon, ki ni omogočen za uporabo, lahko prejme šifriran profil, ciljan za to napravo. Telefon ne potrebuje eksplicitnega ključa zaradi varnega mehanizma za prvo omogočanje uporabe, ki uporablja funkcije SSL.

Za zagon ali dokončanje začetka ali konca posodobitve profila ali nadgradnje vdelane programske opreme ni potrebno nobeno ukrepanje uporabnika, prav tako pa tudi ne, če so potrebne vmesne nadgradnje za doseganje stanja prihodnje nadgradnje iz starejše izdaje. Poskus resinhronizacije profila se izvede samo, če je telefon nedejaven, ker lahko resinhronizacija sproži vnovični zagon programske opreme in prekine klic.

Postopek omogočanja uporabe upravljajo parametri splošnega namena. Vsak telefon je mogoče konfigurirati tako, da občasno vzpostavi povezavo z navadnim strežnikom za omogočanje uporabe (NPS). Za komunikacijo z NPS ni potreben varen protokol, ker je posodobljeni profil šifriran s skrivnim ključem v skupni rabi. NPS je lahko standardni strežnik TFTP, HTTP ali HTTPS z odjemalskimi potrdili.

Skrbnik lahko telefone nadgradi, znova zažene ali resinhronizira z uporabo spletnega uporabniškega vmesnika telefona. Skrbnik lahko ta opravila izvede tudi s sporočilom SIP NOTIFY.

Konfiguracijski profili se generirajo z uporabo običajnih odprtokodnih orodij, ki se vključijo v sisteme za omogočanje uporabe ponudnikov storitev.

Sorodne teme

Dovoljevanje in konfiguriranje posodobitev profila, na strani 34

Dovoljevanje in konfiguriranje posodobitev profila

Posodobitve profilov je mogoče dovoliti ob določenih intervalih. Posodobljeni profili se iz strežnika v telefon pošljejo s protokolom TFTP, HTTP ali HTTPS.

Preden začnete

Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Postopek

Korak 1 Izberite **Glas** > **Omogočanje uporabe**.

Korak 2 V razdelku **Configuration Profile (Konfiguracijski profil)** izberite možnost **Yes (Da)** na spustnem seznamu **Provision Enable (Omogoči omogočanje uporabe)**.

Korak 3 Vnesite parametre.

Korak 4 Kliknite **Pošlji vse spremembe**.

Sorodne teme

Posodobitve profila in nadgradnje vdelane programske opreme, na strani 34

Dovoljevanje in konfiguriranje nadgradenj vdelane programske opreme

Posodobitve vdelane programske opreme je mogoče dovoliti ob določenih intervalih. Posodobljena vdelana programska oprema je iz strežnika poslana v telefon z uporabo protokola TFTP ali HTTP. Pri nadgradnja vdelane programske opreme varnost ni tako pomembna, ker ta programska oprema ne vsebuje osebnih podatkov.

Preden začnete

Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Postopek

Korak 1 Izberite **Glas** > **Omogočanje uporabe**.

Korak 2 V razdelku **Firmware Upgrade (Nadgradnja vdelane programske opreme)** izberite možnost **Yes (Da)** na spustnem seznamu **Upgrade Enable (Omogoči nadgradnjo)**.

Korak 3 Vnesite parametre.

Korak 4 Kliknite **Pošlji vse spremembe**.

Nadgradnja programske opreme prek TFTP, HTTP ali HTTPS

Telefon podpira enotno nadgradnjo z enim posnetkom prek TFTP, HTTP ali HTTPS.

Opomba Prehodi na starejše izdaje morda ne bodo na voljo za vse naprave. Za več informacij si oglejte opombe ob izdaji za vašo različico telefona in vdelane programske opreme.

Preden začnete

Datoteko za nalaganje vdelane programske opreme je treba prenesti v dostopen strežnik.

Postopek

Korak 1 Posnetek preimenujte na naslednji način:

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

kjer:

`x8xx` je serija telefona, na primer 6841.

`aa-b-c` je številka izdaje, na primer 10-4-1

Korak 2 Stisnjeno datoteko tar razširite z ukazom **`tar -xzvf`**.

Korak 3 Mapo kopirajte v imenik za prenos TFTP, HTTP ali HTTPS.

Korak 4 Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Korak 5 Izberite **Glas** > **Omogočanje uporabe**.

Korak 6 Poiščite ime datoteke za nalaganje s pripono **.loads** in ga dodajte veljavnemu URL-ju.

Korak 7 Kliknite **Pošlji vse spremembe**.

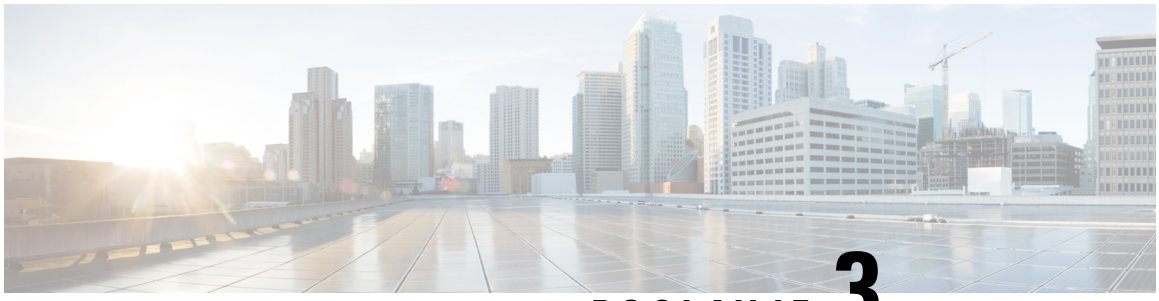
Nadgradnja vdelane programske opreme z ukazom iz brskalnika

Za izvedbo nadgradnje vdelane programske opreme v telefonu je mogoče uporabiti ukaz za nadgradnjo, ki ga vnesete v naslovno vrstico brskalnika. Telefon se posodobi samo, ko je nedejaven. Poskus posodobitve se izvede samodejno, ko je klic končan.

Postopek

Če želite telefon nadgraditi z URL-jem v brskalniku, vnesite ta ukaz:

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



POGLAVJE 3

Interni strežniki za predomogočanje uporabe in omogočanje uporabe

Interni strežniki za predomogočanje uporabe in omogočanje uporabe

Ponudnik storitev telefone, razen enot RC, vnaprej omogoči za uporabo s profilom. Profil za vnaprejšnje omogočanje uporabe je lahko sestavljen iz omejenega nabora parametrov, ki resinhronizirajo telefon. Profil lahko vključuje tudi popoln nabor parametrov, ki jih priskrbi oddaljeni strežnik. Telefon se privzeto resinhronizira ob vklopu in ob intervalih, ki so konfigurirani v profilu. Ko uporabnik v strankinih prostorih priključi telefon, naprava prenese posodobljen profil in morebitne posodobitve vdelane programske opreme.

Ta postopek vnaprejšnjega omogočanja uporabe, uvajanja in oddaljenega omogočanja uporabe je mogoče izvesti na več načinov.

Priprava strežnika in programska orodja

Za primere v tem poglavju mora biti na voljo en ali več strežnikov. V lokalnem računalniku je mogoče namestiti in izvajati te strežnike:

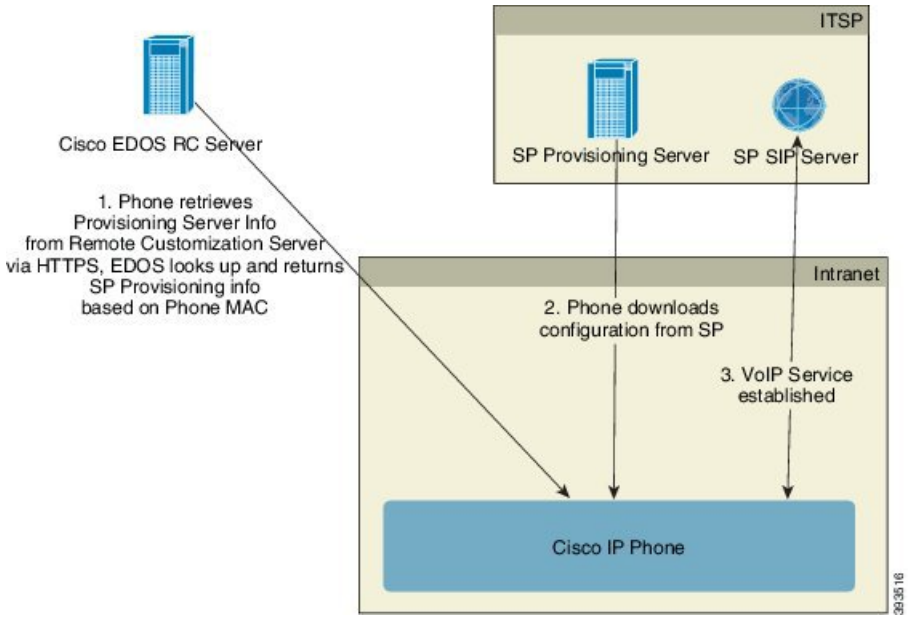
- TFTP (vrata UDP 69),
- syslog (vrata UDP 514),
- HTTP (vrata TCP 80),
- HTTPS (vrata TCP 443).

Za odpravljanje težav s konfiguracijo strežnika je koristno, če v ločenem računalniku namestite odjemalce za vsako vrsto strežnika. S tem postopkom preverite pravilno delovanje strežnika neodvisno od interakcije s telefoni.

Priporočamo tudi, da namestite ta orodja:

- za generiranje konfiguracijskih profilov namestite odprtokodno orodje za stiskanje gzip;
- za šifriranje profilov in postopke HTTPS namestite odprtokodni programski paket OpenSSL;
- za preskušanje dinamičnega generiranja profilov in oddaljeno omogočanje uporabe v enem koraku z uporabo HTTPS-ja priporočamo skriptni jezik s podporo za skripte CGI. Primer takega skriptnega jezika so odprtokodna jezikovna orodja Perl;
- za preverjanje varne izmenjave med strežniki za omogočanje uporabe in telefoni namestite orodje za sledenje ethernetnih paketov (packet sniffer), kot je prostodostopni Ethereal/Wireshark. Zajemite sled ethernetnih paketov interakcije med telefonom in strežnikom za omogočanje uporabe. To naredite tako, da orodje za sledenje paketov namestite v računalnik, ki je povezan s stikalom, ki ima omogočeno zrcaljenje vrat. Za transakcije HTTPS lahko uporabite orodje ssldump.

Distribucija za oddaljeno prilagajanje (RC)



Vsi telefoni vzpostavijo povezavo s Ciscovim strežnikom EDOS RC, dokler niso prvotno omogočeni za uporabo.

V distribucijskem modelu RC stranka kupi telefon, ki je že povezan z določenim ponudnikom storitev v Ciscovem strežniku EDOS RC. Ponudnik internetnih telefonskih storitev (Internet Telephony Service Provider oz. ITSP) nastavi in vzdržuje strežnik za omogočanje uporabe ter podatke tega strežnika registrira v Ciscovem strežniku EDOS RC.

Ob vklopu telefona z internetno povezavo je stanje prilagajanja za telefon, ki ni omogočen za uporabo, **Odprt**. Telefon lokalnemu strežniku DHCP najprej pošlje poizvedbo za podatke strežnika za omogočanje uporabe in nastavi stanje prilagajanja telefona. Če je poizvedba DHCP uspešna, je stanje prilagajanja nastavljeno na **Opuščeno** in ni poskusa RC, ker je DHCP zagotovil potrebne podatke strežnika za omogočanje uporabe.

Če pri prvi povezavi telefona v omrežje ali po tovarniški ponastavitvi ni nastavljena nobena možnost DHCP, vzpostavi povezavo s strežnikom za aktiviranje naprav za omogočanje uporabe brez ročnega ukrepanja. Novi

telefoni bodo za omogočanje uporabe uporabili “activate.cisco.com” namesto “webapps.cisco.com”. Telefoni z različicami vdelane programske opreme pred 11.2(1) bodo še naprej uporabljali webapps.cisco.com. Cisco priporoča, da v požarnem zidu dovolite obe imeni domen.

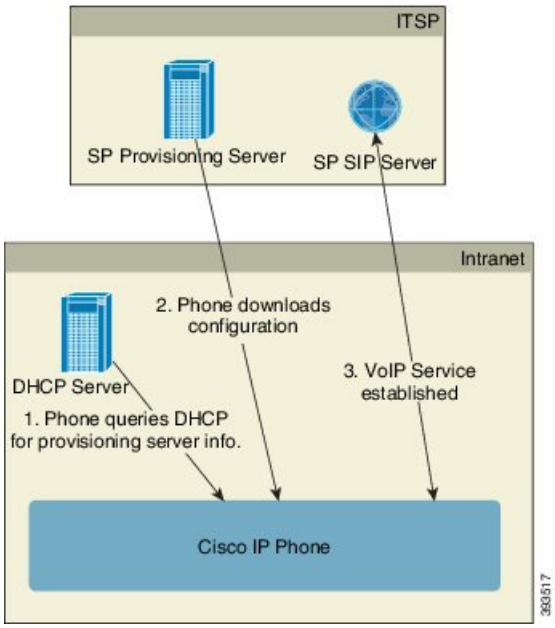
Če strežnik DHCP ne zagotovi podatkov strežnika za omogočanje uporabe, telefon pošlje poizvedbo Ciscovemu strežniku EDOS RC, navede svoj naslov MAC in model ter stanje prilagajanja nastavi na **Čakajoče**. Ciscov strežnik EDOS se odzove s podatki strežnika za omogočanje uporabe povezanega ponudnika storitev, vključno z URL-jem strežnika za omogočanje uporabe, stanje prilagajanja telefona pa je nastavljeno na **Po meri – čakanje**. Telefon nato izvede ukaz URL-ja za resinhronizacijo, da pridobi konfiguracijo ponudnika storitev. Če je uspešen, se stanje prilagoditve nastavi na **Pridobljeno**.

Če Ciscov strežnik EDOS RC nima ponudnika storitev, povezanega s telefonom, je stanje prilagajanja telefona nastavljeno na **Nedosegljiv**. Telefon je mogoče ročno konfigurirati oziroma v Ciscov strežnik EDOS dodati povezavo za ponudnika storitev za telefon.

Če je telefon omogočen za uporabo prek zaslona LCD ali s spletnim konfiguracijskim orodjem, preden stanje prilagajanja postane **Pridobljeno**, je stanje prilagajanja nastavljeno na **Opuščeno** in Ciscovemu strežniku EDOS se ne pošlje poizvedba, razen v primeru tovarniške ponastavitve telefona.

Ko je telefon omogočen za uporabo, se Ciscov strežnik EDOS RC ne uporablja, razen v primeru tovarniške ponastavitve telefona.

Interno predomogočanje uporabe naprav



S Ciscovo tovarniško privzeto konfiguracijo se telefon samodejno poskuša resinhronizirati s profilom v strežniku TFTP. Upravljani strežnik DHCP v krajevnem omrežju napravi posreduje podatke o profilu in strežniku TFTP, ki je konfiguriran za predomogočanje uporabe. Ponudnik storitev poveže vsak nov telefon v krajevno omrežje. Telefon se samodejno znova sinhronizira z lokalnim strežnikom TFTP in inicializira svoje interno stanje, tako da je pripravljen za uvajanje. Ta profil za predomogočanje uporabe običajno vključuje URL oddaljenega strežnika za omogočanje uporabe. Strežnik za omogočanje uporabe zagotovi, da je naprava posodobljena, potem ko je uvedena in povezana v omrežje stranke.

Pred pošiljanjem telefona, ki je vnaprej omogočen za uporabo, stranki je mogoče optično prebrati njegovo črtno kodo in zabeležiti njegov naslov MAC ali serijsko številko. Te podatke je mogoče uporabiti za ustvarjanje profila, s katerim se naprava resinhronizira.

Po prejemu telefona ga stranka poveže s širokopasovno povezavo. Telefon se ob vklopu poveže s strežnikom za omogočanje uporabe prek URL-ja, ki je bil določen v postopku predomogočanja uporabe. Telefon se lahko tako resinhronizira in po potrebi posodobi profil in vdelano programsko opremo.

Sorodne teme

Maloprodajna distribucija, na strani 5
Omogočanje za uporabo s parametri TFTP, na strani 40

Nastavitev strežnika za omogočanje uporabe

V tem razdelku opisujemo zahteve za omogočanje uporabe telefona z uporabo različnih strežnikov in različnih primerov uporabe. Za namene tega dokumenta in preskušanja se strežniki za omogočanje uporabe namestijo in izvajajo v lokalnem računalniku. Za omogočanje uporabe telefonov so koristna tudi splošno razpoložljiva programska orodja.

Omogočanje za uporabo s parametri TFTP

Telefoni podpirajo TFTP za postopke resinhronizacije profilov in nadgradnje vdelane programske opreme. Pri oddaljenem uvajanju naprav priporočamo HTTPS, vendar lahko uporabite tudi HTTP in TFTP. V tem primeru je nato potrebno šifriranje datotek za večjo varnost, saj ponuja večjo zanesljivost glede na zaščitne mehanizme protokola NAT in usmerjevalnikov. TFTP je koristen za interno predomogočanje uporabe velikega števila naprav, ki niso omogočene za uporabo.

Telefon lahko naslov IP strežnika TFTP pridobi neposredno od strežnika DHCP z možnostjo 66 za DHCP. Če je parameter Profile_Rule konfiguriran z datotečno potjo tega strežnika TFTP, naprava svoj profil prenese iz strežnika TFTP. Prenos se izvede, ko je naprava povezana v omrežje in vklopljena.

Profile_Rule, naveden s privzeto tovarniško konfiguracijo, je *&PN*.cfg, pri čemer *&PN* predstavlja vrednost modela telefona.

Za enoto CP-6841-3PCC je na primer ime datoteke CP-6841-3PCC.cfg.

Ob vklopu naprave s privzetim tovarniškim profilom se ta resinhronizira s to datoteko v lokalnem strežniku TFTP , ki ga določa možnost 66 za DHCP. Pot datoteke je relativna na navidezni korenski imenik strežnika TFTP.

Sorodne teme

Interno predomogočanje uporabe naprav, na strani 39

Oddaljeni nadzor končnih točk in NAT

Telefon je združljiv s protokolom NAT (network address translation) za dostop do interneta prek usmerjevalnika. Usmerjevalnik lahko zaradi večje varnosti poskuša preprečiti nedovoljene dohodne pakete z uvedbo simetričnega NAT-a. To je strategija za filtriranje paketov, ki zelo omeji pakete, ki jim je iz interneta dovoljen vstop v zaščiteno omrežje. Oddaljeno omogočanje uporabe z uporabo TFTP-ja zato ni priporočeno.

VoIP lahko soobstaja s protokolom NAT samo, ko je na voljo neka vrsta prečkanja NAT-a. Konfiguriranje preprostega prečkanja protokola UDP prek NAT-a (STUN). Uporabnik za to možnost potrebuje:

- dinamični zunanji (javni) naslov IP od vaše storitve;
- računalnik, v katerem se izvaja strežniška programska oprema STUN;
- robno napravo z mehanizmom asimetričnega NAT-a.

Omogočanje za uporabo s parametri HTTP

Telefon deluje kot brskalnik, ki zahteva spletne strani od oddaljenega internetnega mesta. To zagotavlja zanesljiv mehanizem za doseganje strežnika za omogočanje uporabe, ko strankin usmerjevalnik uporablja simetrični NAT ali druge zaščitne mehanizme. HTTP in HTTPS v oddaljenih namestitvah delujeta zanesljiveje kot TFTP, zlasti če so uvedene enote povezane z gospodinjskimi požarnimi zidovi ali usmerjevalniki, ki imajo omogočen NAT. HTTP in HTTPs se v naslednjih opisih vrst zahtev uporabljata izmenljivo.

Osnovno omogočanje uporabe na podlagi HTTP uporablja metodo HTTP GET za pridobivanje konfiguracijskih profilov. Običajno se za vsak uveden telefon ustvari konfiguracijska datoteka in te datoteke so shranjene v imeniku strežnika HTTP. Ko strežnik prejme zahtevo GET, preprosto vrne datoteko, ki je navedena v glavi zahteve GET.

Namesto statičnega profila je mogoče konfiguracijski profil generirati dinamično s pošiljanjem poizvedb strankini zbirki podatkov in sprotnim ustvarjanjem profila.

Ko telefon zahteva resinhronizacijo, lahko za zahtevanje konfiguracijskih podatkov za resinhronizacijo uporabi metodo HTTP POST. Napravo je mogoče konfigurirati tako, da v telesu zahteve HTTP POST strežniku pošilja določene podatke o stanju in identifikacijske podatke. Strežnik te podatke uporabi za generiranje želenega konfiguracijskega profila odgovora ali shranjevanje podatkov o stanju za poznejše analiziranje in sledenje.

Telefon v okviru zahtev GET in POST samodejno vključi osnovne identifikacijske podatke v polje User-Agent v glavi zahteve. To so podatki o proizvajalcu, imenu izdelka, trenutni različici vdelane programske opreme in serijski številki naprave.

Naslednji primer je polje zahteve User-Agent iz enote CP-6841-3PCC:

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

Ko je telefon konfiguriran tako, da se s konfiguracijskim profilom resinhronizira z uporabo protokola HTTP, zaradi zaščite zaupnih podatkov priporočamo, da uporabite HTTPS ali da je profil šifriran. Z uporabo šifriranih profilov, ki jih telefon prenese z uporabo protokola HTTP, je mogoče preprečiti razkritje zaupnih podatkov, vsebovanih v konfiguracijskem profilu. Način resinhronizacije predstavlja manjšo računsko obremenitev strežnika za omogočanje uporabe kot uporaba protokola HTTPS.

Telefon lahko dešifrira profile, šifrirane z enim od teh načinov šifriranja:

- Šifriranje AES-256-CBC
- šifriranje na podlagi RFC-8188 z uporabo AES-128-GCM

Opomba Telefoni podpirajo HTTP različice 1.0, HTTP različice 1.1 in način Chunk Encoding, ko se HTTP različice 1.1 pogaja glede transportnega protokola.

Obravnava kod stanja HTTP pri resinhronizaciji in nadgradnji

Telefon podpira odziv HTTP za oddaljeno omogočanje uporabe (resinhronizacija). Trenuten način delovanja telefona je kategoriziran na tri načine:

- A – uspeh, pri čemer vrednosti "Resync Periodic" in "Resync Random Delay" določata nadaljnje zahteve.
- B – neuspeh, če datoteka ni najdena ali je profil poškodovan. Vrednost "Resync Error Retry Delay" določa nadaljnje zahteve.
- C – drug neuspeh, ko napačen URL ali naslov IP povzroči napako povezave. Vrednost "Resync Error Retry Delay" določa nadaljnje zahteve.

Tabela 2: Način delovanja telefona za odzive HTTP

Koda stanja HTTP	Opis	Način delovanja telefona
301 Moved Permanently	To in prihodnje zahteve je treba usmeriti na novo lokacijo.	Zahtevo takoj znova poskusite z drugo lokacijo.
302 Found	Poznano kot začasno premaknjeno.	Zahtevo takoj znova poskusite z drugo lokacijo.
3xx	Druge zahteve 3xx niso obdelane.	U
400 Bad Request	Zahteve ni mogoče izpolniti zaradi napačne sintakse.	U
401 Unauthorized	Osnovni izziv preverjanja pristnosti ali odziv z dostopom do povzetka.	Zahtevo takoj znova poskusite s poverilnicami za preverjanje pristnosti – največ 2 poskusa. Ob neuspehu je način delovanja telefona C.
403 Forbidden	Strežnik se noče odzvati.	U
404 Not Found	Zahtevano sredstvo ni najdeno. Nadaljnje zahteve odjemalca so dovoljene.	B
407 Proxy Authentication Required	Osnovni izziv preverjanja pristnosti ali odziv z dostopom do povzetka.	Zahtevo takoj znova poskusite s poverilnicami za preverjanje pristnosti – največ dva vnovična poskusa. Ob neuspehu je način delovanja telefona C.
4xx	Druge kode stanja odjemalca niso obdelane.	U
500 Internal Server Error	Splošno sporočilo o napaki.	Način delovanja telefona je C.
501 Not Implemented	Strežnik ne prepozna načina zahteve ali je ne more izpolniti.	Način delovanja telefona je C.
502 Bad Gateway	Strežnik deluje kot prehod ali proxy in prejme neveljaven odziv nadrejenega strežnika.	Način delovanja telefona je C.

Koda stanja HTTP	Opis	Način delovanja telefona
503 Service Unavailable	Strežnik trenutno ni na voljo (preobremenjen ali nedosegljiv zaradi vzdrževanja). To je začasno stanje.	Način delovanja telefona je C.
504 Gateway Timeout	Strežnik deluje kot prehod ali proxy in ne prejme pravočasnega odziva nadrejenega strežnika.	U
5xx	Druga napaka strežnika	U

Omogočanje uporabe za HTTPS

Telefon podpira uporabo protokola HTTPS za omogočanje uporabe, ker zagotavlja večjo varnost pri upravljanju enot, ki se uvajajo na daljavo. Vsak telefon ima poleg strežniškega korenskega potrdila Sipura CA edinstveno odjemalsko potrdilo SLL (in povezan zasebni ključ). To telefonu omogoča prepoznavanje dovoljenih strežnikov za omogočanje uporabe in zavrnitev nedovoljenih. Po drugi strani odjemalsko potrdilo omogoča strežniku za omogočanje uporabe prepoznavanje posamezne naprave, ki je poslala zahtevo.

Če želi ponudnik storitev upravljati uvajanje z uporabo HTTPS-ja, mora generirati strežniško potrdilo za vsak strežnik za omogočanje uporabe, s katerim se telefon resinhronizira z uporabo HTTPS-ja. Strežniško potrdilo mora biti podpisano s korenskim ključem Ciscovega overitelja strežniških potrdil. Njegovo potrdilo je vdelano v vse uvedene enote. Ponudnik storitev, ki želi pridobiti podpisano strežniško potrdilo, mora Ciscu poslati zahtevo za podpis potrdila, Cisco pa strežniško potrdilo podpiše in ga vrne za namestitev v strežniku za omogočanje uporabe.

Potrdilo strežnika za omogočanje uporabe mora v zadevi vsebovati polje za skupno ime (CN) in popolnoma določeno ime domene gostitelja, v katerem se izvaja strežnik. Izbirno lahko po popolnoma določenem imenu domene gostitelja vsebuje podatke, ki so ločeni s poševnico (/). Naslednji primeri kažejo vnose CN, ki jih telefon sprejme kot veljavne:

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

Telefon poleg preverjanja strežniškega potrdila preskusi tudi strežnikov naslov IP, tako da v sistemu DNS poišče ime strežnika, ki je naveden v strežniškem potrdilu.

Pridobitev podpisanega strežniškega potrdila

Orodje OpenSSL lahko generira zahtevo za podpis potrdila. Naslednji primer prikazuje ukaz **openssl**, ki generira 1024-bitni par javnih/zasebnih ključev RSA in zahtevo za podpis potrdila:

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

Ta ukaz generira zasebni ključ strežnika v datoteki **privkey.pem** in ustrezno zahtevo za podpis potrdila v datoteki **provserver.csr**. Ponudnik storitev zadrži skrivnost **privkey.pem** in pošlje **provserver.csr** Ciscu v podpis. Po prejemu datoteke **provserver.csr** Cisco generira podpisano strežniško potrdilo **provserver.crt**.

Postopek

Korak 1 Pojdite na https://software.cisco.com/software/edos/home in se prijavite s poverilnicami za CCO.

Opomba Če pri prvi povezavi telefona v omrežje ali po tovarniški ponastavitvi ni nastavljena nobena možnost DHCP, vzpostavi povezavo s strežnikom za aktiviranje naprav za omogočanje uporabe brez ročnega ukrepanja. Novi telefoni bodo za omogočanje uporabe uporabili “activate.cisco.com” namesto “webapps.cisco.com”. Telefoni z izdajo vdelane programske opreme pred 11.2(1) še naprej uporabljajo “webapps.cisco.com”. Priporočamo, da v požarnem zidu dovolite obe imeni domen.

Korak 2 Izberite **Certificate Management (Upravljanje potrdil)**.

Na zavihku **Sign CSR (Podpis CSR-ja)** je naložen CRS iz prejšnjega koraka za podpisovanje.

Korak 3 Na spustnem seznamu **Select Product (Izberite izdelek)** izberite **SPA1xx firmware 1.3.3 and newer/SPA232D firmware 1.3.3 and newer/SPA5xx firmware 7.5.6 and newer/CP-78xx-3PCC/CP-88xx-3PCC**.

Opomba Ta izdelek vključuje telefone Cisco IP Phone 6800 Series za več platform.

Korak 4 V polju **CSR File (Datoteka CSR)** kliknite **Browse (Prebrskaj)** in izberite datoteko CSR za podpis.

Korak 5 Izberite način šifriranja:

- MD5
- SHA1
- SHA256

Cisco priporoča, da izberete šifriranje SHA256.

Korak 6 Na spustnem seznamu **Sign in Duration (Trajanje prijave)** izberite ustrezno trajanje (npr. 1 leto).

Korak 7 Kliknite **Sign Certificate Request (Podpiši zahtevo za potrdilo)**.

Korak 8 Za prejem podpisanega potrdila izberite eno od teh možnosti:

- **Enter Recipient’s Email Address (Vnesite e-poštni naslov prejemnika)** – če želite potrdilo prejeti po e-pošti, v to polje vnesite e-poštni naslov.
- **Download (Prenos)** – če želite podpisano potrdilo prenesti, izberite to možnost.

Korak 9 Kliknite **Submit (Pošlji)**.

Podpisano strežniško potrdilo vam bo po e-pošti poslano na prej navedeni e-poštni naslov ali preneseno.

Korensko odjemalsko potrdilo overitelja potrdil za telefone za več platform

Cisco ponudnikom storitev ponuja tudi korensko odjemalsko potrdilo za telefone za več platform. To korensko potrdilo potrjuje pristnost odjemalskega potrdila, ki ga ima vsak telefon. Telefoni za več platform podpirajo tudi potrdila, ki jih podpišejo tretje osebe, kot so tista od Verisigna, Cybertrusta in drugih.

Edinstveno odjemalsko potrdilo, ki ga naprava ponudi med sejo HTTPS, vsebuje identifikacijske podatke, ki so vdelani v polje z zadevo potrdila. Te podatke lahko strežniku HTTPS posreduje skript CGI, sprožen za obravnavo varnih zahtev. Natančneje, zadeva potrdila vsebuje ime izdelka enote (element OU), naslov MAC (element S) in serijsko številko (element L).

Naslednji primer iz polja z zadevo odjemalskega potrdila telefonov Cisco IP Phone 6841 za več platform prikazuje te elemente:

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

Če želite ugotoviti, ali ima telefon posamezno potrdilo, uporabite spremenljivko makra za omogočanje $CCERT. Vrednost spremenljivke se razširi v vrednost "Nameščeno" ali "Nenameščeno", odvisno od tega, ali je prisotno ali odstotno edinstveno odjemalsko potrdilo. V primeru splošnega potrdila je serijsko številko enote mogoče dobiti iz glave zahteve HTTP v polju User-Agent.

Strežnike HTTPS je mogoče konfigurirati tako, da zahtevajo potrdila SSL od odjemalcev, ki se povezujejo. Če je to omogočeno, lahko strežnik uporabi korensko odjemalsko potrdilo za telefone za več platform, ki ga Cisco priskrbi za preverjanje odjemalskega potrdila. Strežnik lahko podatke o potrdilu nato posreduje skriptu CGI za nadaljnjo obdelavo.

Mesto shrambe potrdila se lahko razlikuje. V namestitvi strežnika Apache so na primer datotečne poti za shrambo potrdila, ki ga podpiše strežnik za omogočanje uporabe, zasebnega ključa, povezanega z njim, in korenskega odjemalskega potrdila overitelja potrdil za telefone za več platform naslednje:

```
# 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
```

Za podrobnejše informacije glejte dokumentacijo za strežnik HTTPS.

Ciscov korenski overitelj odjemalskih potrdil podpiše vsako edinstveno potrdilo. Ustrezno korensko potrdilo je na voljo ponudniku storitev za namene preverjanja pristnosti odjemalcev.

Redundantni strežniki za omogočanje uporabe

Strežnik za omogočanje uporabe lahko navedete kot naslov IP ali kot popolnoma določeno ime domene (Fully Qualified Domain Name oz. FQDN). Uporaba FQDN-ja poenostavi uvajanje redundantnih strežnikov za omogočanje uporabe. Ko je strežnik za omogočanje uporabe prepoznan prek FQDN-ja, telefon poskuša FQDN razrešiti na naslov IP prek DNS-ja. Za omogočanje uporabe so podprti samo zapisi DNS A; razreševanje naslovov DNS SRV ni na voljo za omogočanje uporabe. Telefon nadaljuje obdelavo zapisov A, dokler se strežnik ne odzove. Če se ne odzove noben strežnik, povezan z zapisi A, telefon v strežniku sistemskega dnevnika zabeleži napako.

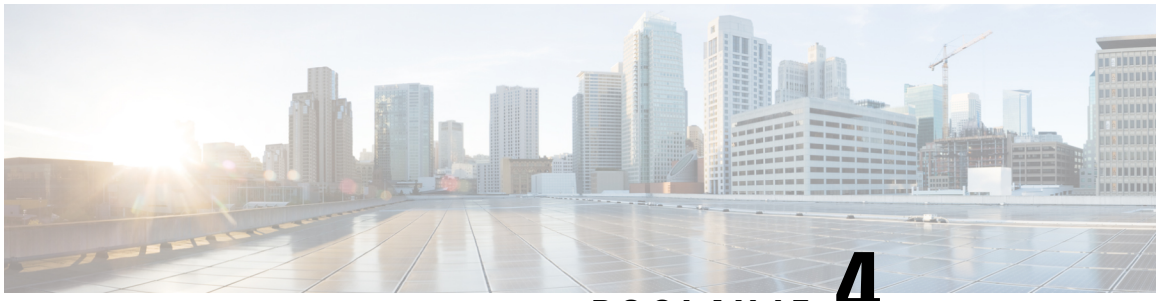
Strežnik sistemskega dnevnika

Če je v telefonu z uporabo parametrov <Syslog Server> konfiguriran strežnik sistemskega dnevnika, postopki resinhronizacije in nadgradnje pošiljajo sporočila strežniku sistemskega dnevnika. Sporočilo je mogoče generirati na začetku oddaljene zahteve za datoteko (nalaganje konfiguracijskega profila ali vdelane programske opreme) in ob zaključku postopka (ali je bil uspešen ali neuspešen).

Sporočila, zabeležena v dnevniku, se konfigurirajo z naslednjimi parametri in z makri razširijo v dejanska sporočila sistemskega dnevnika:

- Log_Request_Msg

- Log_Success_Msg
- Log_Failure_Msg



POGLAVJE 4

Primeri omogočanja uporabe

Pregled primerov omogočanja uporabe

V tem poglavju so primeri postopkov za prenos konfiguracijskih profilov med telefonom in strežnikom za omogočanje uporabe.

Informacije o ustvarjanju konfiguracijskih profilov so na voljo v razdelku Skripti za omogočanje uporabe, na strani 13.

Osnovna resinhronizacija

V tem razdelku so predstavljane osnovne funkcije resinhronizacije telefonov.

Resinhronizacija TFTP

Telefon podpira več omrežnih protokolov za pridobivanje konfiguracijskih profilov. Najosnovnejši protokol za prenos profilov je TFTP (RFC1350). TFTP je zelo razširjen za omogočanje uporabe omrežnih naprav v zasebnih krajevnih omrežjih. Čeprav ga ne priporočamo za uvajanje oddaljenih končnih točk po internetu, je lahko TFTP priročen za uvajanje v malih organizacijah, za interno predomogočanje uporabe ter za razvijanje in preskušanje. Za več informacij o internem predomogočanju uporabe si oglejte razdelek Interno predomogočanje uporabe naprav, na strani 39. V naslednjem postopku se profil spremeni po prenosu datoteke iz strežnika TFTP.

Postopek

Korak 1 V okolju krajevnega omrežja priključite računalnik in telefon na zvezdišče, stikalo ali majhen usmerjevalnik.

Korak 2 V računalniku namestite in aktivirajte strežnik TFTP.

Korak 3 Z urejevalnikom besedila ustvarite konfiguracijski profil, ki vrednost za GPP_A nastavi na 12345678, kot je prikazano v primeru.

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

Korak 4 Profil shranite z imenom `basic.txt` v korenskem imeniku strežnika TFTP.

Pravilno konfiguracijo strežnika TFTP lahko preverite tako, da z uporabo nekega drugega odjemalca TFTP poleg telefona zahtevate datoteko `basic.txt`. Po možnosti uporabite odjemalca TFTP, ki se izvaja v ločenem gostitelju od strežnika za omogočanje uporabe.

Korak 5 Brskalnik v računalniku odprite na strani za skrbniško/napredno konfiguracijo. Če je naslov IP telefona na primer 192.168.1.100:

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

Korak 6 Izberite zavihek **Glas** > **Omogočanje uporabe** in preglejte vrednosti parametrov splošnega namena od GPP_A do GPP_P. Morali bi biti prazni.

Korak 7 Telefon resinhronizirajte s konfiguracijskim profilom `basic.txt` tako, da v oknu brskalnika odprete URL za resinhronizacijo.

Če je naslov IP strežnika TFTP 192.168.1.200, bi moral biti ukaz podoben temu primeru:

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

Ko telefon prejme ta ukaz, naprava na naslovu 192.168.1.100 zahteva datoteko `basic.txt` od strežnika TFTP na naslovu IP 192.168.1.200. Telefon nato razčleni preneseno datoteko in parameter GPP_A posodobi z vrednostjo 12345678.

Korak 8 Preverite, ali je bil parameter pravilno posodobljen: v brskalniku računalnika osvežite konfiguracijsko stran in izberite zavihek **Glas** > **Omogočanje uporabe**.

Parameter GPP_A mora zdaj vsebovati vrednost 12345678.

Uporaba sistemskega dnevnika za beleženje sporočil

Telefon pošlje izbranemu strežniku sistemskega dnevnika sporočilo sistemskega dnevnika, ko je naprava tik pred tem, da se resinhronizira, in potem še po končani ali neuspešni resinhronizaciji. Za prepoznavanje tega strežnika lahko odprete stran za skrbništvo telefona (glejte Dostop do spletne strani telefona, na strani 7), izberete **Glas** > **Sistem** in strežnik določite v parametru **Strežnik sistemskega dnevnika** v razdelku **Izbirna konfiguracija omrežja**. Konfigurirajte naslov IP strežnika sistemskega dnevnika v napravo in opazujte sporočila, ki so generirana v preostalih postopkih.

Postopek

Korak 1 Namestitev in aktiviranje strežnika sistemskega dnevnika v lokalnem računalniku.

Korak 2 Naslov IP lokalnega računalnika programirajte v parameter Syslog_Server v profilu in pošljite spremembo:

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

Korak 3 Kliknite zavihek **System (Sistem)** in v parameter Syslog_Server vnesite vrednost lokalnega strežnika sistemskega dnevnika.

Korak 4 Ponovite postopek resinhronizacije, kot je opisano v razdelku Resinhronizacija TFTP, na strani 47.

Naprava med resinhronizacijo generira dve sporočili sistemskega dnevnika. Prvo sporočilo kaže, da poteka zahteva. Drugo sporočilo sporoča, ali je bila resinhronizacija uspešna ali ne.

Korak 5 Preverite, ali je strežnik sistemskega dnevnika prejel sporočila, podobna naslednjim:

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

Podrobna sporočila so na voljo, če parameter Debug_Server (namesto parametra Syslog_Server) programirate z naslovom IP strežnika sistemskega dnevnika, in tako, da Debug_Level nastavite na vrednost med 0 in 3 (3 je največ podrobnosti):

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

Vsebino sporočil je mogoče konfigurirati z uporabo teh parametrov:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Če je kateri koli od teh parametrov počiščen, se ustrezno sporočilo sistemskega dnevnika ne generira.

Samodejno resinhroniziranje naprave

Naprava se lahko redno resinhronizira s strežnikom za omogočanje uporabe, da se zagotovi razširjanje morebitnih sprememb profila v strežniku v naprave končnih točk (v nasprotju s pošiljanjem izrecne zahteve za resinhronizacijo končni točki).

Če želite, da se telefon redno resinhronizira s strežnikom, je treba s parametrom Profile_Rule opredeliti URL konfiguracijskega profila, s parametrom Resync_Periodic pa obdobje resinhronizacije.

Preden začnete

Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Postopek

Korak 1 Izberite **Glas** > **Omogočanje uporabe**.

Korak 2 Določite parameter Profile_Rule. V tem primeru je naslov IP strežnika TFTP 192.168.1.200.

Korak 3 V polje **Resync Periodic** vnesite nizko vrednost za preskušanje, na primer **30** sekund.

Korak 4 Kliknite **Pošlji vse spremembe**.

Z novimi nastavitvami parametra se telefon dvakrat na minuto resinhronizira s konfiguracijsko datoteko, določeno z URL-jem.

Korak 5 Sporočila, ki so generirana, opazujte v sledi sistemskega dnevnika (kot je opisano v razdelku Uporaba sistemskega dnevnika za beleženje sporočil, na strani 48).

Korak 6 Poskrbite, da bo polje **Resync On Reset** nastavljeno na **Yes**.

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

Korak 7 Izklopite in znova vklopite telefon, da vsilite resinhronizacijo s strežnikom za omogočanje uporabe.

Če postopek resinhronizacije iz kakršnega koli razloga ne uspe (na primer, če se strežnik ne odziva), enota počaka (za obdobje, določeno v sekundah v možnosti **Resync Error Retry Delay**), preden znova poskuša resinhronizirati. Če je **Resync_Error_Retry_Delay** nastavljen na 0, telefon po neuspešnem poskusu resinhronizacije ne poskuša resinhronizirati.

Korak 8 (Izbirno) Vrednost polja **Resync Error Retry Delay** nastavite na majhno število, na primer **30**.

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

Korak 9 Onemogočite strežnik TFTP in opazujte rezultate v izhodu sistemskega dnevnika.

Edinstveni profili, razširitev makrov in HTTP

V uvedbi, kjer je treba vsak telefon konfigurirati z drugačnimi nastavitvami za nekatere parametre, kot je User_ID ali Display_Name, lahko ponudnik storitev ustvari edinstven profil za vsako uvedeno napravo in te profile gosti v strežniku za omogočanje uporabe. Hkrati je treba vsak telefon konfigurirati tako, da se resinhronizira s svojim profilom skladno z vnaprej določenim načinom poimenovanja profilov.

Sintaksa URL-ja profila lahko vključuje identifikacijske podatke, ki so edinstveni za vsak telefon, kot je naslov MAC ali serijska številka, z uporabo razširitve makrov za vgrajene spremenljivke. Razširitev makrov odpravlja potrebo po določanju teh vrednosti na več mestih v vsakem profilu.

Za pravilo profila se razširitev makrov izvede pred uporabo pravila za telefon. Razširitev makrov nadzira več vrednosti, na primer:

- $MA se razširi v 12-mestni naslov MAC enote (z uporabo malih črk šestnajstiškega števila). Primer: 000e08abcdef.
- $SN se razširi v serijsko številko enote. Na primer: 88012BA01234.

Na ta način je mogoča razširitev makrov za druge vrednosti, vključno z vsemi parametri splošnega namena od GPP_A do GPP_P. Primer tega postopka si lahko ogledate v Resinhronizacija TFTP, na strani 47. Razširitev makrov ni omejena na ime datoteke URL-ja, vendar jo je mogoče uporabiti za poljuben del parametra pravila profila. Ti parametri so navedeni kot $A do $P. Za celoten seznam spremenljivk, ki so na voljo za razširitev makrov, glejte Spremenljivke za razširitev makrov, na strani 72.

V tej vaji se v strežniku TFTP določi profil, posebej za določen telefon.

Vaja: omogočanje uporabe določenega profila telefona IP v strežniku TFTP

Postopek

Korak 1 Na nalepki izdelka poiščite naslov MAC telefona. (Naslov MAC je številka, sestavljena iz šestnajstiških števk in malih črk, kot je 000e08aabbcc.

Korak 2 Konfiguracijsko datoteko `basic.txt` (opisano v razdelku Resinhronizacija TFTP, na strani 47) kopirajte v novo datoteko z imenom `CP-xxxx-3PCC macaddress.cfg` (`xxxx` zamenjajte s številko modela in `macaddress` z naslovom MAC telefona).

Korak 3 Novo datoteko premaknite v navidezni korenski imenik strežnika TFTP.

Korak 4 Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Korak 5 Izberite **Glas** > **Omogočanje uporabe**.

Korak 6 Vnesite `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` v polje **Pravilo za profil**.

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

Korak 7 Kliknite **Pošlji vse spremembe**. To sproži takojšnji vnovični zagon in sinhronizacijo.

Ko se izvede naslednja resinhronizacija, telefon prenese novo datoteko z razširjanjem makroizraza $MA v njegov naslov MAC.

Resinhronizacija HTTP GET

HTTP ponuja zanesljivejši mehanizem resinhronizacije kot TFTP, ker vzpostavi povezavo TCP, TFTP pa uporablja manj zanesljiv UDP. Poleg tega strežniki HTTP ponujajo izboljšane funkcije za filtriranje in beleženje dnevnikov kot strežniki TFTP.

Na odjemalski strani telefon ne potrebuje nobene posebne konfiguracijske nastavitve v strežniku, da bi se lahko resinhroniziral s HTTP-jem. Sintaksa parametra Profile_Rule za uporabo HTTP-ja z metodo GET je podobna sintaksi, ki se uporablja za TFTP. Če lahko standardni brskalnik prenese profil iz vašega strežnika HTTP, potem bi to moral biti zmožen storiti tudi telefon.

Vaja: resinhronizacija HTTP GET

Postopek

Korak 1 V lokalnem računalniku ali drugem dostopnem gostitelju namestite strežnik HTTP.

Odprtokodni strežnik Apache lahko prenesete iz interneta.

Korak 2 Konfiguracijski profil `basic.txt` (opisan v razdelku Resinhronizacija TFTP, na strani 47) kopirajte v navidezni korenski imenik nameščenega strežnika.

Korak 3 Preverite pravilno namestitev strežnika in dostop do datoteke `basic.txt` tako, da z brskalnikom dostopate do profila.

Korak 4 Profile_Rule preskusnega telefona spremenite tako, da bo namesto na strežnik TFTP kazal na strežnik HTTP in bo redno prenašal svoj profil.

Denimo, da je strežnik HTTP na naslovu 192.168.1.300 –vnesite to vrednost:

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

Korak 5 Kliknite **Pošlji vse spremembe**. To sproži takojšnji vnovični zagon in sinhronizacijo.

Korak 6 Opazujte sporočila sistemskega dnevnika, ki jih pošlje telefon. Redne resinhronizacije bi morale profil zdaj dobivati iz strežnika HTTP.

Korak 7 V dnevnikih strežnika HTTP opazujte, kako so podatki, ki določajo preskusni telefon, prikazani v dnevniku uporabnikovih posrednikov.

Ti podatki bi morali vključevati proizvajalca, ime izdelka, trenutno različico vdelane programske opreme in serijsko številko.

Omogočanje uporabe s Ciscovim XML-jem

Vsakega od telefonov, ki so tukaj označeni z xxxx, lahko omogočanje uporabe izvedete s Ciscovimi funkcijami XML.

Predmet XML lahko v telefon pošljete s paketom SIP Notify ali objavo HTTP v vmesnik CGI telefona: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC razširi Ciscovo funkcijo XML tako, da podpira omogočanje uporabe prek predmeta XML:

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

Ko telefon prejme predmet XML, prenese datoteko za omogočanje uporabe iz [profile-rule]. To pravilo uporablja makre za poenostavljanje razvoja aplikacije s storitvami XML.

Razreševanje URL-jev z razširitvijo makrov

Podimeniki z več profili v strežniku ponujajo priročen način upravljanja velikega števila uvedenih naprav. URL profila lahko vsebuje:

- ime strežnika za omogočanje uporabe ali ekspliciten naslov IP. Če je strežnik za omogočanje uporabe v profilu naveden poimensko, telefon izvede iskanje DNS, da razreši ime;
- nestandardna strežniška vrata, ki so v URL-ju navedena s standardno sintakso `:port` po imenu strežnika;
- podimenik navideznega korenskega imenika strežnika, kjer je shranjen profil, določen z uporabo standardnega zapisa URL-jev in upravljan z razširitvijo makrov.

Spodnji Profile_Rule na primer zahteva datoteko profila ($PN.cfg) v podimeniku strežnika `/cisco/config` iz strežnika TFTP, ki se izvaja v gostitelju prov.telco.com, ki čaka povezavo na vratih 6900:

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

```
</Profile_Rule>
```

Profil za vsak telefon je mogoče prepoznati po parametru splošnega namena, njegova vrednost v pravilu skupnega profila pa je navedena z uporabo razširitve makrov.

Kot primer denimo, da je GPP_B opredeljen kot `Dj6Lmp23Q`.

Profile_Rule ima vrednost:

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

Ko se naprava resinhronizira in se makri razširijo, telefon z naslovom MAC 000e08012345 zahteva profil z imenom, ki vsebuje naslov MAC naprave, na tem URL-ju:

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

Varna resinhronizacija HTTPS

V telefonu so na voljo ti mehanizmi za resinhronizacijo z uporabo varnega komunikacijskega postopka:

- Osnovna resinhronizacija HTTPS
- HTTPS s preverjanjem pristnosti z odjemalskim potrdilom
- Odjemalsko filtriranje HTTPS in dinamična vsebina

Osnovna resinhronizacija HTTPS

HTTPS doda HTTP-ju SSL za oddaljeno omogočanje uporabe, tako da lahko:

- telefon preverja pristnost strežnika za omogočanje uporabe;
- strežnik za omogočanje uporabe preverja pristnost telefona.
- Zaupnost podatkov, izmenjanih med telefonom in strežnikom za omogočanje uporabe, je zagotovljena.

SSL generira in izmenja skrivne (simetrične) ključe za vsako povezavo med telefonom in strežnikom z uporabo parov javnih/zasebnih ključev, ki so vnaprej nameščeni v telefonu in strežniku za omogočanje uporabe.

Na odjemalski strani telefon ne potrebuje nobene posebne konfiguracijske nastavitve v strežniku, da bi se lahko resinhroniziral s HTTPS-jem. Sintaksa parametra Profile_Rule za uporabo HTTPS-ja z metodo GET je podobna sintaksi, ki se uporablja za HTTP ali TFTP. Če lahko standardni brskalnik prenese profil iz vašega strežnika HTTPS, potem bi to moral biti zmožen storiti tudi telefon.

Poleg namestitev strežnika HTTPS je treba v strežniku za omogočanje uporabe namestiti tudi strežniško potrdilo SSL, ki ga podpiše Cisco. Naprave se ne morejo resinhronizirati s strežnikom, ki uporablja HTTPS, če ta ne zagotovi strežniškega potrdila, ki ga je podpisal Cisco. Navodila za ustvarjanje podpisanih potrdil SSL za glasovne izdelke so na voljo tukaj: https://supportforums.cisco.com/docs/DOC-9852.

Vaja: osnovna resinhronizacija HTTPS

Postopek

Korak 1 Strežnik HTTPS namestite v gostitelju, katerega naslov IP je omrežnemu strežniku DNS poznan prek običajnega prevajanja imen gostiteljev.

Odprtokodni strežnik Apache lahko konfigurirate, da deluje kot strežnik HTTPS, če je nameščen z odprtokodnim paketom mod_ssl.

Korak 2 Generirajte novo zahtevo za podpisovanje strežniškega potrdila za strežnik. Za ta korak boste morda morali namestiti odprtokodni paket OpenSSL ali enakovredno programsko opremo. Če uporabljate OpenSSL, je ukaz za generiranje osnovne datoteke CSR:

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

Ta ukaz generira javni/zasebni par ključev, ki je shranjen v datoteki `privkey.pem`.

Korak 3 Datoteko CSR (provserver.csr) pošljite v podpisi Ciscu.

Vrnjeno vam bo podpisano strežniško potrdilo (provserver.cert), skupaj z odjemalskim korenskim potrdilom Sipura CA, spacroot.cert.

Za več informacij si oglejte https://supportforums.cisco.com/docs/DOC-9852.

Korak 4 Podpisano strežniško potrdilo, datoteko s parom zasebnih ključev in odjemalsko korensko potrdilo shranite na ustreznih mestih v strežniku.

Če gre za namestitev strežnika Apache v Linuxu, so te lokacije običajno naslednje:

```
# 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
```

Korak 5 Znova zaženite strežnik.

Korak 6 Konfiguracijsko datoteko `basic.txt` (opisano v razdelku Resinhronizacija TFTP, na strani 47) kopirajte v navidezni korenski imenik strežnika HTTTPS.

Korak 7 Preverite, ali strežnik deluje pravilno, tako da s standardnim brskalnikom v lokalnem računalniku iz strežnika HTTPS prenesete datoteko `basic.txt`.

Korak 8 Preverite strežniško potrdilo, ki ga zagotovi strežnik.

Brskalnik potrdila verjetno ne bo prepoznal kot veljavnega, če ni vnaprej konfiguriran tako, da ga Cisco sprejme kot korenskega overitelja potrdil. Vendar pa telefoni pričakujejo, da je potrdilo podpisano na ta način.

Parameter Profile_Rule preskusne naprave spremenite tako, da bo vseboval sklic na strežnik HTTPS kot v tem primeru:

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

```
</Profile_Rule>
```

V tem primeru predpostavljamo, da je ime strežnika HTTPS **my.server.com**.

Korak 9 Kliknite **Pošlji vse spremembe**.

Korak 10 Opazujte sled sistemskega dnevnika, ki jo pošlje telefon.

V sporočilu sistemskega dnevnika mora biti navedeno, da je resinhronizacija pridobila profil iz strežnika HTTPS.

Korak 11 (izbirno) V podomrežju telefona se z uporabo analizatorja ethernetnega protokola prepričajte, da so paketi šifrirani.

V tej vaji ni bilo omogočeno preverjanje odjemalskega potrdila. Poveza med telefonom in omrežjem je šifrirana. Vendar pa prenos ni varen, ker se lahko s strežnikom poveže vsak odjemalec in zahteva datoteko, če pozna ime datoteke in ve, kje je imenik. Za varno resinhronizacijo mora strežnik preveriti tudi pristnost odjemalca, kot je prikazano v vaji, opisani v razdelku HTTPS s preverjanjem pristnosti z odjemalskim potrdilom, na strani 55.

HTTPS s preverjanjem pristnosti z odjemalskim potrdilom

V privzeti tovarniški konfiguraciji strežnik od odjemalca ne zahteva odjemalskega potrdila SSL. Prenos profila ni varen, ker se lahko s strežnikom poveže poljuben odjemalec in zahteva profil. To konfiguracijo lahko uredite tako, da omogočite preverjanje pristnosti odjemalca. Strežnik zahteva odjemalsko potrdilo za preverjanje pristnosti telefona, preden sprejme zahtevo za vzpostavitev povezave.

Postopka resinhronizacije zaradi te zahteve ni mogoče neodvisno preskusiti z uporabo brskalnika, ki nima ustreznih poverilnic. Izmenjavo ključa SSL v povezavi HTTPS med preskusnim telefonom in strežnikom je mogoče opazovati z orodjem ssldump. Sledenje z orodjem pokaže interakcijo med odjemalcem in strežnikom.

Vaja: HTTPS s preverjanjem pristnosti z odjemalskim potrdilom

Postopek

Korak 1 Omogočanje preverjanja pristnosti z odjemalskim potrdilom v strežniku HTTPS.

Korak 2 V strežniku Apache (v.2) nastavite naslednjo strežniško konfiguracijsko datoteko:

```
SSLVerifyClient  require
```

Poskrbite tudi, da je spacroot.cert shranjen, kot je prikazano v vaji Osnovna resinhronizacija HTTPS, na strani 53.

Korak 3 Znova zaženite strežnik HTTPS in opazujte sled sistemskega dnevnika iz telefona.

Vsaka resinhronizacija s strežnikom zdaj izvede simetrično preverjanje pristnosti, tako da se pred prenosom profila preverita tako strežniško kot tudi odjemalsko potrdilo.

Korak 4 Za zajem povezave resinhronizacije med telefonom in strežnikom HTTPS uporabite ssldump.

Če je preverjanje odjemalskega potrdila pravilno omogočeno v strežniku, sled orodja ssldump kaže simetrično izmenjavo potrdil (najprej iz strežnika v odjemalca in nato iz odjemalca v strežnik) pred šifriranimi paketi, ki vsebujejo profil.

Če je omogočeno preverjanje pristnosti odjemalca lahko profil iz strežnika za omogočanje uporabe zahteva samo telefon z naslovom MAC, ki se ujema z veljavnim odjemalskim potrdilom. Strežnik zavrne zahtevo iz navadnega brskalnika ali druge nepooblaščene naprave.

Odjemalsko filtriranje HTTPS in dinamična vsebina

Če je strežnik HTTPS konfiguriran tako, da zahteva odjemalsko potrdilo, podatki v potrdilu omogočajo prepoznavo telefona, ki se resinhronizira, in mu zagotovijo pravilne informacije o konfiguraciji.

Strežnik HTTPS da podatke o potrdilu na voljo skriptom CGI (ali prevedenim programom CGI), ki se sprožijo v okviru zahteve za omogočanje uporabe. Za namene te slike ta vaja uporablja odprtokodni skriptni jezik Perl in predpostavlja, da se v strežniku HTTPS uporablja Apache (v.2).

Postopek

Korak 1 Namestite Perl v gostitelju, v katerem se izvaja strežnik HTTPS.

Korak 2 Generirajte naslednji reflektorski skript v Perlu:

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

Korak 3 To datoteko shranite z imenom `reflect.pl` in z dovoljenji za izvajanje (chmod 755 v Linuxu) v imeniku s skripti CGI strežnika HTTPS.

Korak 4 Preverite dostopnost skriptov CGI v strežniku (torej `/cgi-bin/...`).

Korak 5 V preskusni napravi spremenite Profile_Rule tako, da se resinhronizira z reflektorskim skriptom, kot je prikazano v tem primeru:

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

Korak 6 Kliknite **Pošlji vse spremembe**.

Korak 7 Opazujte sled sistemskega dnevnika iz telefona, da se prepričate o uspešni resinhronizaciji.

Korak 8 Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Korak 9 Izberite **Glas** > **Omogočanje uporabe**.

Korak 10 Preverite, ali parameter GPP_D vsebuje podatke, ki jih je zajel skript.

Ti podatki vsebujejo ime izdelka, naslov MAC in serijsko številko, če ima preskusna naprava edinstveno potrdilo od proizvajalca. Podatki vsebujejo splošen niz, če je bila enota izdelana pred izdajo vdelane programske opreme 2.0.

Podoben skript lahko pridobi podatke o napravi, ki se resinhronizira, in ji nato zagotovi ustrezne vrednostni konfiguracijskih parametrov.

Potrdila HTTPS

Telefon ponuja zanesljivo in varno strategijo za omogočanje uporabe, ki temelji na zahtevah HTTPS iz naprav v strežnik za omogočanje uporabe. Za strežnikovo preverjanje pristnosti telefona in za telefonovo preverjanje pristnosti strežnika sta uporabljena tako strežniško kot tudi odjemalsko potrdilo.

Če želite s telefonom uporabljati HTTPS, morate generirati zahtevo za podpis potrdila (Certificate Signing Request oz. CSR) in ga poslati Ciscu. Telefon generira potrdilo za namestitev v strežnik za omogočanje uporabe. Telefon sprejme potrdilo, ko želi vzpostaviti povezavo HTTPS s strežnikom za omogočanje uporabe.

Metodologija HTTPS

HTTPS šifrira komunikacijo med odjemalcem in strežnikom ter vsebino sporočila tako zaščiti pred drugimi omrežnimi napravami. Način šifriranja za telo komunikacije med odjemalcem in strežnikom temelji na šifriranju s simetričnim ključem. Pri šifriranju s simetričnim ključem si odjemalec in strežnik delita en sam skrivni ključ prek varnega kanala, ki je zaščiten s šifriranjem z javnim/zasebnim ključem.

Sporočila, šifrirana s skrivnim ključem, je mogoče dešifrirati samo z uporabo istega ključa. HTTPS podpira mnoge algoritme za šifriranje s simetričnimi ključi. Telefon poleg 128-bitnega šifriranja RC4 uporablja do 256-bitno simetrično šifriranje z uporabo standarda AES (American Encryption Standard).

HTTPS omogoča tudi preverjanje pristnosti strežnika in odjemalca, ki izvajata varno transakcijo. Ta funkcija zagotavlja, da se druge naprave v omrežju ne morejo lažno predstavljati kot strežnik za omogočanje uporabe in posamezen odjemalec. Ta možnost je nujna za omogočanje uporabe oddaljenih končnih točk.

Preverjanje pristnosti strežnika in odjemalca se izvede z uporabo šifriranja z javnim/zasebnim ključem s potrdilom, ki vsebuje javni ključ. Besedilo, ki je šifrirano z javnim ključem, je mogoče dešifrirati samo z ustreznim zasebnim ključem (in obratno). Telefon podpira algoritem RSA (Rivest-Shamir-Adleman) za kriptografijo z javnim/zasebnim ključem.

Strežniško potrdilo SSL

Vsakemu varnemu strežniku za omogočanje uporabe se izda strežniško potrdilo SSL (secure sockets layer), ki ga Cisco neposredno podpiše. Vdelana programska oprema, ki se izvaja v telefonu, kot veljavno prepozna samo Ciscovo potrdilo. Ko se odjemalec poveže s strežnikom za uporabo protokola HTTPS, zavrne vsako strežniško potrdilo, ki ga ni podpisal Cisco.

Ta mehanizem ponudnika storitev zaščiti pred nedovoljenim dostopom do telefona ali morebitnim poskusom lažnega predstavljanja kot strežnik za omogočanje uporabe. Brez take zaščite bi lahko napadalec telefon na novo omogočil za uporabo, pridobil informacije o konfiguraciji ali uporabil drugo storitev VoIP. Brez zasebnega ključa, ki ustreza veljavnemu strežniškemu potrdilu, napadalec ne more vzpostaviti komunikacije s telefonom.

Pridobitev strežniškega potrdila

Postopek

Korak 1 Obrnite se na Ciscovo osebje za podporo, ki vam bo pomagalo pri postopku za potrdilo. Če ne sodelujete z določeno osebo za podporo, zahtevo po e-pošti pošljite na naslov ciscosb-certadmin@cisco.com.

Korak 2 Generirajte zasebni ključ, ki bo uporabljen v zahtevi za podpis potrdila (Certificate Signing Request oz. CSR). Ta ključ je zaseben in vam ga ni treba razkriti Ciscovi podpori. Za generiranje ključa uporabite odprtokodno orodje "openssl". Na primer:

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

Korak 3 Generirajte CSR, ki vsebuje polja, s katerimi je mogoče prepoznati vašo organizacijo in lokacijo. Na primer:

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

Imeti morate te podatke:

- Polje z zadevo – vnesite skupno ime (Common Name oz. CN), ki mora biti v sintaksi popolnoma določenega imena domene. Med predstavitvijo za preverjanje pristnosti SSL telefon preveri, ali je potrdilo, ki ga prejme, iz naprave, ki ga je poslala.
- Gostiteljsko ime strežnika – na primer provserv.domain.com.
- E-poštni naslov – vnesite e-poštni naslov, tako da se lahko podpora strankam po potrebi obrne na vas. Ta e-poštni naslov je viden v CSR-ju.

Korak 4 CSR po e-pošti pošljite (v obliki datoteke zip) Ciscovi osebi za podporo ali na naslov ciscosb-certadmin@cisco.com. Cisco podpiše potrdilo. Cisco vam pošlje potrdilo, da ga namestite v sistem.

Odjemalsko potrdilo

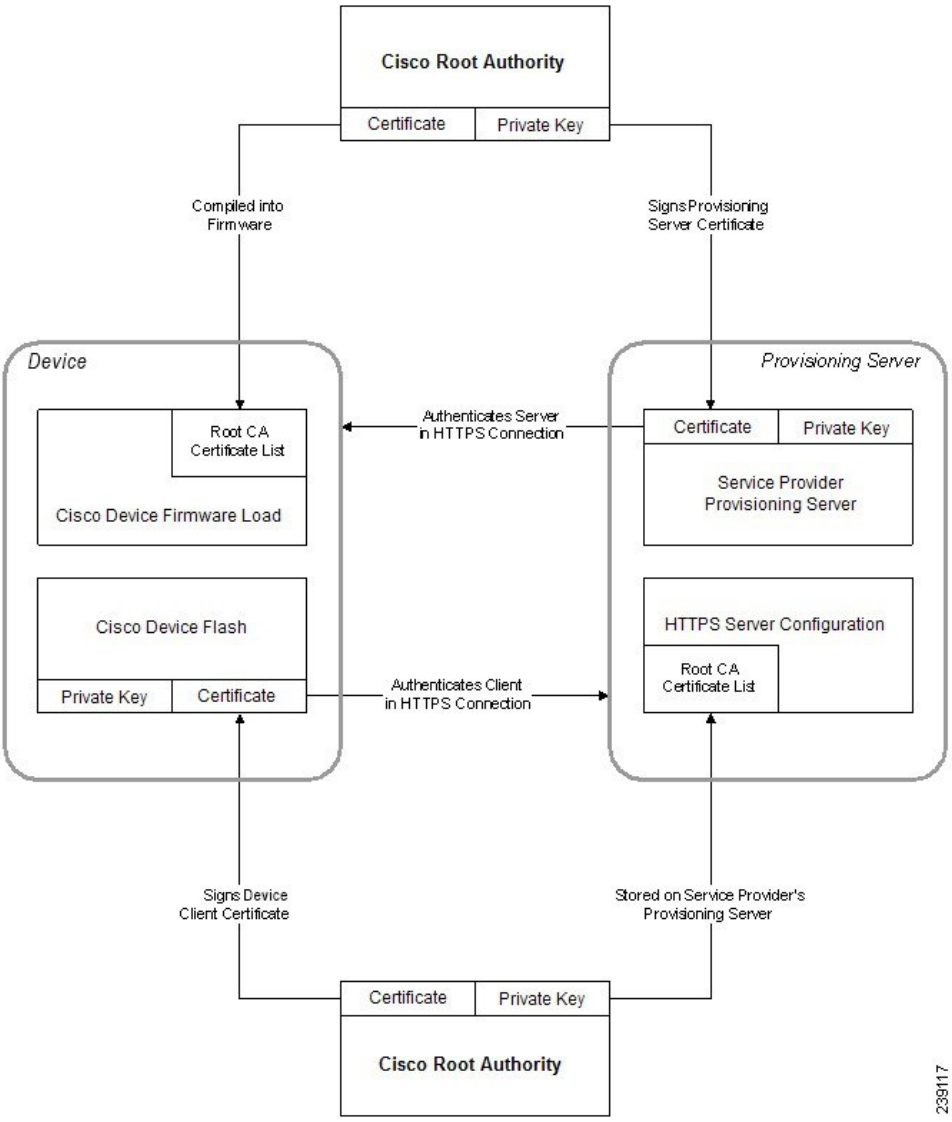
Poleg neposrednega napada na telefon lahko napadalec tudi poskuša vzpostaviti stik s strežnikom za omogočanje uporabe prek standardnega spletnega brskalnika ali drugega odjemalca HTTPS in dobiti konfiguracijski profil iz strežnika za omogočanje uporabe. Zaradi preprečevanja te vrste napada ima vsak telefon edinstveno odjemalsko potrdilo, ki ga podpiše Cisco in vključuje identifikacijske podatke o vsaki posamezni končni točki. Vsak ponudnik storitev dobi korensko potrdilo overitelja potrdil, ki ga je mogoče uporabiti za preverjanje pristnosti odjemalskega potrdila naprave. Ta pot preverjanja pristnosti omogoča strežniku za omogočanje uporabe zavrnitev nedovoljenih zahtev za konfiguracijske profile.

Struktura potrdil

Kombinacija strežniškega in odjemalskega potrdila zagotavlja varno komunikacijo med oddaljenim telefonom in strežnikom, ki ga omogoča za uporabo. Spodnja slika prikazuje odnos med potrdili, pari javnih/zasebnih ključev in podpisnimi korenskimi overitelji ter Ciscovim odjemalcem, strežnikom za omogočanje uporabe in overiteljem potrdil ter njihovo postavitev.

Zgornji del diagrama prikazuje korenskega overitelja strežnika za omogočanje uporabe, ki se uporablja za podpis posameznih potrdil strežnika za omogočanje uporabe. Ustrezno korensko potrdilo se prevede v vdelano programsko opremo, kar telefonu omogoča preverjanje pristnosti pooblaščenih strežnikov za omogočanje uporabe.

Slika 2: Potek overitelja potrdil



Konfiguriranje overitelja potrdil po meri

Digitalna potrdila je mogoče uporabiti za preverjanje pristnosti omrežnih naprav in uporabnikov v omrežju. Uporabiti jih je mogoče za pogajanja za seje IPSec med omrežnimi vozlišči.

Tretja oseba potrdilo overitelja potrdil uporablja za potrditev in preverjanje pristnosti dveh ali več vozlišč, ki poskušata komunicirati. Vsako vozlišče ima javni in zasebni ključ. Javni ključ šifrira podatke. Zasebni ključ dešifrira podatke. Ker so vozlišča potrdila pridobila iz istega vira, imajo zagotovila o svojih identitetah.

Naprava lahko za preverjanje pristnosti povezav IPSec uporabi digitalna potrdila zunanjega overitelja potrdil.

Telefoni podpirajo nabor vnaprej naloženih korenskih overiteljev potrdil, zabeleženih v vdelani programski opremi:

- Potrdilo Cisco Small Business CA

- Potrdilo CyberTrust CA
- Potrdilo Verisign CA
- Potrdilo korenskega overitelja potrdil Sipura
- Potrdilo korenskega overitelja potrdil Linksys

Preden začnete

Odprite spletno stran za skrbništvo telefona. Glejte Dostop do spletne strani telefona, na strani 7.

Postopek

Korak 1 Izberite **Informacije** > **Stanje**.

Korak 2 Pomaknite se na **Stanje overitelja potrdil po meri** in si oglejte naslednja polja:

- Stanje omogočanja uporabe overitelja potrdil po meri – kaže stanje omogočanja uporabe.
  - Zadnje omogočanje uporabe je uspelo dne mm/dd/llll HH:MM:SS; ali
  - Zadnje omogočanje uporabe ni uspelo dne mm/dd/llll HH:MM:SS
- Informacije o overitelju potrdil po meri – prikaže informacije o overitelju potrdil po meri.
  - Nameščeno – prikaže "Vrednost CN", pri čemer je "Vrednost CN" vrednost parametra CN za polje z zadevo v prvem potrdilu.
  - Ni nameščeno – prikazano, če overitelj potrdil po meri ni nameščen.

Upravljanje profilov

V tem razdelku predstavljamo oblikovanje konfiguracijskih profilov v okviru priprave na prenos. Pojasnilo te funkcionalnosti: kot način resinhronizacije se uporablja TFTP iz lokalnega strežnika, uporabiti pa je mogoče tudi HTTP ali HTTPS.

Stiskanje odprtega profila z orodjem Gzip

Konfiguracijski profil v obliki XML lahko postane precej velik, če profil določa vsak parameter posebej. Telefon za zmanjšanje obremenitve strežnika za omogočanje uporabe podpira stiskanje datoteke XML z uporabo oblike stiskanja "deflate", ki ga podpira orodje gzip (RFC 1951).

Opomba Stiskanje je treba izvesti pred šifriranjem, da bo telefon lahko prepoznal stisnjen in šifriran profil XML.

Za vključitev v zaledne strežniške rešitve po meri za omogočanje uporabe je za stiskanje profilov namesto orodja gzip mogoče uporabiti odprtokodno knjižnico za stiskanje zlib. Pri tem upoštevajte, da telefon pričakuje, da ima datoteka veljavno glavo gzip.

Postopek

Korak 1 Namestite gzip v lokalni računalnik.

Korak 2 Stisnite konfiguracijski profil `basic.txt` (opisan v razdelku Resinhronizacija TFTP, na strani 47) tako, da v ukazni vrstici sprožite gzip:

```
gzip basic.txt
```

S tem generirate stisnjeno datoteko `basic.txt.gz`.

Korak 3 Datoteko `basic.txt.gz` shranite v navideznem korenskem imeniku strežnika TFTP.

Korak 4 Profile_Rule v preskusni napravi spremenite tako, da se resinhronizacija namesto s prvotno datoteko XML izvede s stisnjeno datoteko, kot je prikazano v spodnjem primeru:

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

Korak 5 Kliknite **Pošlji vse spremembe.**

Korak 6 Opazujte sled sistemskega dnevnika iz telefona.

Ob resinhronizaciji telefon prenese novo datoteko in jo uporabi za posodobitev svojih parametrov.

Sorodne teme

Stiskanje odprtega profila, na strani 18

Šifriranje profila z OpenSSL-jem

Stisnjen ali nestisnjen profil je mogoče šifrirati (vendar mora biti datoteka pred šifriranjem stisnjena). Šifriranje je koristno, ko je zlasti pomembna zaupnost podatkov profila, na primer, ko se za komunikacijo med telefonom in strežnikom za omogočanje uporabe uporablja protokol TFTP ali HTTP.

Telefon podpira šifriranje s simetričnimi ključi z uporabo 256-bitnega algoritma AES. To šifriranje je mogoče izvesti z uporabo odprtokodnega paketa OpenSSL.

Postopek

Korak 1 V lokalnem računalniku namestite OpenSSL. Morda bo treba program OpenSSL znova prevesti, da omogočite AES.

Korak 2 Z uporabo konfiguracijske datoteke `basic.txt` (opisane v razdelku Resinhronizacija TFTP, na strani 47) s tem ukazom generirajte šifrirano datoteko:

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

Uporabite lahko tudi stisnjeno datoteko `basic.txt.gz`, ustvarjeno v razdelku Stiskanje odprtega profila z orodjem Gzip, na strani 60, ker je lahko profil XML stisnjen ali nestisnjen.

Korak 3 Šifrirano datoteko `basic.cfg` shranite v navideznem korenskem imeniku strežnika TFTP.

Korak 4 Pravilo Profile_Rule v preskusni napravi spremenite tako, da se resinhronizira s šifrirano datoteko namesto s prvotno datoteko XML. Telefon o šifrirnem ključu obvestite s to možnostjo URL-ja:

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

Korak 5 Kliknite **Pošlji vse spremembe**.

Korak 6 Opazujte sled sistemskega dnevnika iz telefona.

Ob resinhronizaciji telefon prenese novo datoteko in jo uporabi za posodobitev svojih parametrov.

Sorodne teme

Šifriranje AES-256-CBC, na strani 18

Ustvarjanje razdeljenih profilov

Telefon pri vsaki resinhronizaciji prenese več ločenih profilov. Ta postopek omogoča upravljanje različnih vrst podatkov profila v ločenih strežnikih in vzdrževanje vrednosti pogostih konfiguracijskih parametrov, ki so ločene od vrednosti, ki veljajo posebej za račun.

Postopek

Korak 1 Ustvarite nov profil XML, imenovan `basic2.txt`, ki določa vrednost parametra, zaradi česar je drugačen od prejšnjih vaj. Primer: profilu `basic.txt` dodajte naslednje:

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

Korak 2 Profil `basic2.txt` shranite v navideznem korenskem imeniku strežnika TFTP.

Korak 3 Prvo pravilo profila iz prejšnjih vaj pustite v mapi, drugega (Profile_Rule_B) pa konfigurirajte, da bo kazal na novo datoteko:

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

Korak 4 Kliknite **Pošlji vse spremembe**.

Telefon se zdaj resinhronizira tako s prvim kot tudi z drugim profilom (v tem zaporedju), vsakič ko je treba izvesti postopek resinhronizacije.

Korak 5 Opazujte sled sistemskega dnevnika, da se prepričate o pričakovanem delovanju.

Nastavitev glave za zasebnost v telefonu

Glava za zasebnost uporabnika v sporočilu SIP določi potrebe za zasebnost uporabnika iz zaupanja vrednega omrežja.

Vrednost glave za zasebnost uporabnika lahko za vsako interno linijo določite z uporabo oznake XML v datoteki `config.xml`.

Možnosti glave za zasebnost:

- Onemogočeno (privzeto)
- Brez – uporabnik zahteva, da storitev za zasebnost za to sporočilo SIP ne uporablja funkcij za zasebnost.
- Glava – uporabnik potrebuje storitev za zasebnost, da prikrije glave, v katerih ni mogoče odstraniti prepoznavnih informacij.
- Seja – uporabnik zahteva, da storitev za zasebnost zagotovi anonimnost sej.
- Uporabnik – uporabnik zahteva raven zasebnosti samo za posrednike.
- ID – uporabnik zahteva, da sistem vstavi nadomestni ID, ki ne razkrije naslova IP ali imena gostitelja.

Postopek

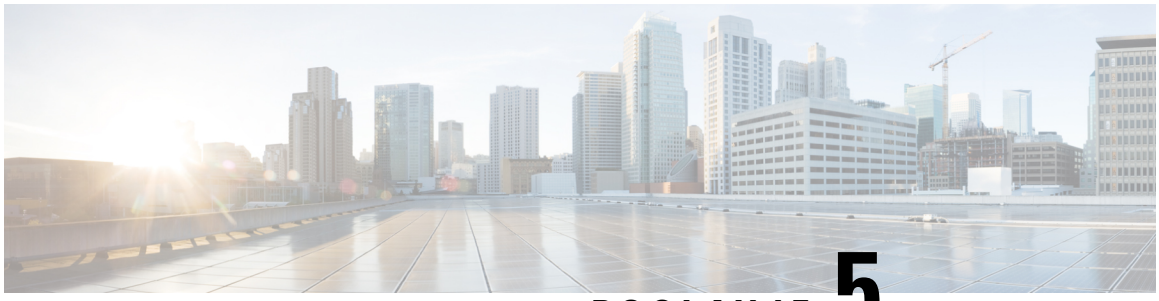
Korak 1 Uredite datoteko `config.xml` za telefon v urejevalniku besedila ali zapisov XML.

Korak 2 Vstavite oznako **<Privacy_Header_N_ ua="na">*Value*</Privacy_Header_N_>**, pri čemer je N številka interne linije (1–10), in uporabite eno od naslednjih vrednosti.

- Privzeta vrednost: **Onemogočeno**
- **brez**
- **glava**
- **seja**
- **uporabnik**
- **ID**

Korak 3 (izbirno) Dodatne interne številke zagotovite z uporabo iste oznake z zahtevano interno številko.

Korak 4 Spremembe shranite v datoteko `config.xml`.



POGLAVJE 5

Parametri za omogočanje uporabe

Pregled parametrov za omogočanje uporabe

V tem poglavju je opis parametrov za omogočanje uporabe, ki jih je mogoče uporabiti v skriptih konfiguracijskih profilov.

Parametri konfiguracijskega profila

V naslednji tabeli so opredeljene funkcije in uporaba posameznih parametrov v razdelku **Parametri konfiguracijskega profila** pod zavihkom **Omogočanje uporabe**.

Ime parametra	Opis in privzeta vrednost
Provision Enable (Omogoči omogočanje uporabe)	Nadzira vsa dejanja resinhronizacije neodvisno od dejanj nadgradnje vdelane programske opreme. Če želite omogočiti oddaljeno omogočanje uporabe, nastavite na **Yes** (Da). Privzeta vrednost je "Yes" (Da).
Resync On Reset (Resinhronizacija ob ponastavitvi)	Sproži resinhronizacijo po vsakem vnovičnem zagonu, razen ko vnovični zagon povzročijo posodobitve parametrov ali nadgradnje vdelane programske opreme. Privzeta vrednost je "Yes" (Da).

Ime parametra	Opis in privzeta vrednost
Resync Random Delay (Naključna zakasnitev resinhronizacije)	Naključna zakasnitev po zagonskem zaporedju, določena v sekundah, preden se izvede ponastavitev. V skupini naprav za telefonijo IP, ki so načrtovane za hkratni zagon, se s tem uvede paleta časov, ob katerih vsaka enota pošlje zahtevo za resinhronizacijo strežniku za omogočanje uporabe. Ta funkcija je lahko koristna v velikem stanovanjskem sistemu, če pride do območnega izpada napajanja. Vrednost za to polje mora biti celo število med 0 in 65535. Privzeta vrednost je 2.
Resync At (HHmm) (Resinh. ob (HHmmm))	Ura (HHmm), ko se naprava znova sinhronizira s strežnikom za omogočanje uporabe. Vrednost za to polje mora biti štirimestno število od 0000 do 2400, ki kaže čas v obliki zapisa HHmm. 0959 na primer označuje 09:59. Privzeto je ta možnost prazna. Če je vrednost neveljavna, se parameter prezre. Če je ta parameter nastavljen na veljavno vrednost, se parameter za resinhronizacijo ob rednih intervalih (Resync Periodic) prezre.
Resync At Random Delay (Resinhronizacija ob naključni zakasnitvi)	Preprečuje preobremenitev strežnika za omogočanje uporabe, ko se hkrati vklopi veliko število naprav. Za preprečitev preobremenitve strežnika z velikim številom zahtev za resinhronizacijo iz več telefonov se telefon resinhronizira v obsegu med urami in minutami ter urami in minutami plus naključno zakasnitvijo (hhmm, hhmm + naključna_zakasnitev). Če je naključna zakasnitev = (vnovična sinhronizacija z naključno zakasnitvijo + 30)/60 minut, je vhodna vrednost v sekundah pretvorjena v minute in zaokrožena navzgor na naslednjo minuto, da se izračuna končni interval random_delay. Obseg veljavnih vrednosti je med 0 in 65535. Če je ta parameter nastavljen na nič, je ta funkcija onemogočena. Privzeta vrednost je 600 sekund (10 minut).

Ime parametra	Opis in privzeta vrednost
Resync Periodic (Resinhronizacija ob rednih intervalih)	Časovni interval med resinhronizacijami s strežnikom za omogočanje uporabe ob rednih intervalih. Povezani časovnik za resinhronizacijo je aktiven samo po prvi uspešni sinhronizaciji s strežnikom. Veljavne oblike zapisa so: • Celo število Primer: vnos **`3000`** kaže, da se bo naslednja vnovična sinhronizacija izvedla čez 3000 sekund. • Več celih števil Primer: vnos **`600,1200,300`** kaže, da se prva vnovična sinhronizacija izvede čez 600 sekund, druga vnovična sinhronizacija čez 1200 sekund po prvi, tretja vnovična sinhronizacija pa 300 sekund po drugi. • Časovni razpon Vnos **`2400+30`** kaže, da se naslednja vnovična sinhronizacija izvede med 2400 in 2430 sekundami po uspešni vnovični sinhronizaciji. Če želite onemogočiti resinhronizacijo ob rednih intervalih, ta parameter nastavite na nič. Privzeta vrednost je 3600 sekund.

Ime parametra	Opis in privzeta vrednost
Resync Error Retry Delay (Zakasnitev vnovičnega poskusa ob napaki resinhronizacije)	Če postopek resinhronizacije ne uspe, ker naprava za telefonijo IP iz strežnika ni mogla dobiti profila, ker je prenesena datoteka poškodovana ali je prišlo do notranje napake, naprava po obdobju, določenem v sekundah, znova poskuša resinhronizirati. Veljavne oblike zapisa so: • Celo število Primer: vnos **300** kaže, da se bo naslednji poskus vnovične sinhronizacije izvedel čez 300 sekund. • Več celih števil Primer: vnos **600,1200,300** kaže, da se prvi vnovični poskus izvede 600 sekund po napaki, drugi vnovični poskus 1200 sekund po napaki pri prvem vnovičnem poskusu, tretji vnovični poskus pa 300 sekund po napaki pri drugem vnovičnem poskusu. • Časovni razpon Vnos **2400+30** kaže, da se naslednji vnovični poskus izvede med 2400 in 2430 sekundami po napaki pri vnovični sinhronizaciji. Če je zakasnitev nastavljena na 0, naprava po neuspešnem poskusu resinhronizacije ne poskuša resinhronizirati.
Forced Resync Delay (Vsiljena zakasnitev resinhronizacije)	Največja zakasnitev (v sekundah), ko telefon čaka pred izvedbo resinhronizacije. Naprava resinhronizacije ne izvede, medtem ko je aktivna ena od njenih telefonskih linij. Ker lahko resinhronizacija traja nekaj sekund, je pred resinhronizacijo dobro počakati, da je naprava dalj časa nedejavna. Tako lahko uporabnik izvede več zaporednih klicev brez prekinitev. Naprava ima časovnik, ki začne odštevati, ko so vse njene linije neaktivne. Ta parameter je začetna vrednost števca. Dogodki resinhronizacije so odloženi, dokler ta števec ne odšteje do ničle. Obseg veljavnih vrednosti je med 0 in 65535. Privzeta vrednost je 14.400 sekund.
Resync From SIP (Resinh. iz SIP)	Omogoča sprožanje resinhronizacije s sporočilom SIP NOTIFY. Privzeta vrednost je "Yes" (Da).

Ime parametra	Opis in privzeta vrednost
Resync After Upgrade Attempt (Resinhronizacija po poskusu nadgradnje)	Omogoči ali onemogoči postopek resinhronizacije po vsaki nadgradnji. Če je izbrana možnost "Yes" (Da), se sproži sinhronizacija. Privzeta vrednost je "Yes" (Da).
Resync Trigger 1, Resync Trigger 2 (Sprožilnik resinhronizacije 1, sprožilnik resinhronizacije 2)	Pogoji sprožanja resinhronizacije, ki jih je mogoče konfigurirati. Resinhronizacija se sproži, ko se logična enačba v teh parametrih razreši na vrednost TRUE. Privzeto je ta možnost prazna.
Resync Fails On FNF (Resinhronizacija ne uspe, ker datoteka ni najdena)	Obravnava se, da je resinhronizacija neuspešna, če iz strežnika ni prejet zahtevani profil. To je mogoče preglasiti s tem parametrom. Ko je nastavljen na **no**, naprava kot uspešno resinhronizacijo od strežnika sprejme odgovor `datoteka ni najdena`. Privzeta vrednost je "Yes" (Da).
Pravilo za profil Pravilo za profil B Pravilo za profil C Pravilo za profil D	Vsako pravilo profila telefon obvesti o viru, iz katerega naj pridobi profil (konfiguracijska datoteka). Telefon med vsakim postopkom resinhronizacije uporabi vse profile v zaporedju. Privzeto: **`/$PSN.xml`** Če za konfiguracijske datoteke uporabljate šifriranje AES-256-CBC, navedite šifrirni ključ s ključno besedo **`--key`**, kot je navedeno v nadaljevanju: **`[--key <šifrirni ključ>]`** Šifrirni ključ je lahko izbirno naveden v dvojnih narekovajih (").
DHCP Option To Use (Možnost DHCP, ki naj bo uporabljena)	Možnosti DHCP, ločene z vejicami, ki naj se uporabijo za pridobivanje vdelane programske opreme in profilov. Privzeta vrednost je 66,160,159,150,60,43,125.
Log Request Msg (Sporočilo dnevniške zahteve)	Ta parameter vsebuje sporočilo, ki se ob začetku poskusa resinhronizacije pošlje strežniku sistemskega dnevnika. Privzeta vrednost je `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`.
Log Success Msg (Dnevniško sporočilo o uspehu)	Sporočilo sistemskega dnevnika, izdano ob uspešnem poskusu resinhronizacije. Privzeta vrednost je `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.

Ime parametra	Opis in privzeta vrednost
Log Failure Msg (Dnevniško sporočilo o neuspehu)	Sporočilo sistemskega dnevnika, izdano ob neuspešnem poskusu resinhronizacije. Privzeta vrednost je `$PN $MAC -- Resync failed: $ERR`.
User Configurable Resync (Resinhronizacija, ki jo konfigurira uporabnik)	Uporabniku omogoča, da vnovično sinhronizacijo sproži z zaslona telefona IP. Privzeta vrednost je "Yes" (Da).

Parametri za nadgradnjo vdelane programske opreme

V naslednji tabeli so opredeljene funkcije in uporaba posameznih parametrov v razdelku **Nadgradnja vdelane programske opreme** na zavihku **Omogočanje uporabe**.

Ime parametra	Opis in privzeta vrednost
Upgrade Enable (Omogoči nadgradnjo)	Omogoči postopke nadgradnje vdelane programske opreme neodvisno od resinhronizacije. Privzeta vrednost je "Yes" (Da).
Upgrade Error Retry Delay (Zakasnitev za vnovični poskus ob napaki nadgradnje)	Interval čakanja pred vnovičnim poskusom nadgradnje (v sekundah) v primeru neuspešne nadgradnje. Naprava ima časovnik za napake pri nadgradnji vdelane programske opreme, ki se vklopi po neuspešnem poskusu nadgradnje vdelane programske opreme. Časovnik začne odštevati pri vrednosti, določeni s tem parametrom. Naslednji poskus nadgradnje vdelane programske opreme se začne, ko ta časovnik prešteje do vrednosti nič. Privzeta vrednost je 3600 sekund.

Ime parametra	Opis in privzeta vrednost
Pravilo za nadgradnjo	Skript za nadgradnjo vdelane programske opreme, ki določa pogoje za nadgradnjo in povezane URL-je vdelane programske opreme. Uporablja enako sintakso kot pravilo za profil. Za vnos pravila za nadgradnjo uporabite to sintakso: **<tftp|http|https>://<ip address>/image/<load name>** Na primer: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Če ni naveden protokol, se uporabi TFTP. Če ni navedeno ime strežnika, se uporabi ime gostitelja, ki zahteva URL. Če niso navedena vrata, se uporabijo privzeta vrata (69 za TFTP, 80 za HTTP ali 443 za HTTPS). Privzeto je ta možnost prazna.
Log Upgrade Request Msg (Dnevniško sporočilo o zahtevi za nadgradnjo)	Sporočilo sistemskega dnevnika, izdano na začetku poskusa nadgradnje vdelane programske opreme. Privzeto: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg (Dnevniško sporočilo o uspešni nadgradnji)	Sporočilo sistemskega dnevnika, izdano po uspešnem poskusu nadgradnje vdelane programske opreme. Privzeta vrednost je `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg (Dnevniško sporočilo o neuspešni nadgradnji)	Sporočilo sistemskega dnevnika, izdano po neuspešnem poskusu nadgradnje vdelane programske opreme. Privzeta vrednost je `$PN $MAC -- Upgrade failed: $ERR`
Skupna raba vdelane programske opreme med enakovrednimi	Omogoči ali onemogoči funkcijo PFS (Peer Firmware Sharing). Izberite **Da** ali **Ne**, da omogočite ali onemogočite funkcijo. Privzeto: Da
Dnevniški strežnik za PFS (Peer Firmware Sharing)	Označuje naslov IP in vrata, na katera se pošlje sporočilo UDP. Na primer: 10.98.76.123:514, kjer je 10.98.76.123 naslov IP, 514 pa številka vrat.

Parametri splošnega namena

V naslednji tabeli so opredeljene funkcije in uporaba posameznih parametrov v razdelku **Parametri splošnega namena** zavihka **Omogočanje uporabe**.

Ime parametra	Opis in privzeta vrednost
GPP A–GPP P	Parametri splošnega namena GPP_* se uporabljajo kot prosti registri za nize pri konfiguriranju telefonov za interakcijo z določeno strežniško rešitvijo za omogočanje uporabe. Konfigurirati jih je mogoče z raznolikimi vrednostmi, vključno z naslednjimi: • šifrirni ključi, • URL-ji, • podatki o stanju večstopenjskega omogočanja uporabe, • predloge za objavo zahtev, • preslikave vzdevkov imen parametrov, • delne vrednosti nizov, ki so sčasoma kombinirane v celotne vrednosti parametrov. Privzeto je ta možnost prazna.

Spremenljivke za razširitev makrov

Nekatere spremenljivke makrov so prepoznane z naslednjimi parametri za omogočanje uporabe:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (pod določenimi pogoji)

V okviru teh parametrov so prepoznane in razširjene vrste sintakse, kot je $NAME ali $(NAME).

Podnize spremenljivk makrov je mogoče navesti z zapisom $(NAME:p) in $(NAME:p:q), pri čemer sta p in q nenegativni celi števili (na voljo v različici 2.0.11 in novejših). Posledična razširitev makra je podniz, ki se začne pri odmiku znaka p in ima dolžino q (če q ni naveden, pa do konca niza). Če na primer GPP_A vsebuje ABCDEF, se $(A:2) razširi v CDEF in $(A:2:3) v CDE.

Neprepoznana imena se ne prevedejo in oblika $NAME ali $(NAME) po razširitvi ostane nespremenjena v vrednosti parametra.

Ime parametra	Opis in privzeta vrednost
$	Oblika $$ se razširi v posamezen znak $.
A do P	Zamenjajo se z vsebino parametrov splošnega namena od GPP_A do GPP_P.
SA do SD	Zamenjajo se s parametri za posebne namene od GPP_SA do GPP_SD. Ti parametri vsebujejo ključe ali gesla, uporabljene pri omogočanju uporabe. **Opomba** $SA do $SD so prepoznani kot argumenti za izbirni kvalifikator resinhronizacijskega URL-ja: --key.
MA	Naslov MAC, sestavljen iz malih črk šestnajstiškega števila – primer: 000e08aabbcc
MAU	Naslov MAC, sestavljen iz velikih črk šestnajstiškega števila – primer: 000E08AABBCC
MAC	Naslov MAC, sestavljen iz malih črk šestnajstiškega števila in podpičij, ki ločujejo pare števk – primer: 00:0e:08:aa:bb:cc
PN	Ime izdelka – primer: CP-6841-3PCC
PSN	Številka serije izdelka – primer: 6841-3PCC
SN	Niz s serijsko številko – primer: 88012BA01234
CCERT	Stanje odjemalskega potrdila SSL: nameščeno ali nenameščeno
IP	Naslov IP telefona v lokalnem podomrežju – primer: 192.168.1.100
EXTIP	Zunanji IP telefona, kot je viden iz interneta – primer: 66.43.16.52
SWVER	Niz različice programske opreme – primer: sip68xx.11-0-1MPP
HWVER	Niz različice strojne opreme – primer: 2.0.1
PRVST	Stanje omogočanja uporabe (številski niz): -1 = izrecna zahteva za resinhronizacijo 0 = resinhronizacija ob zagonu 1 = redna resinhronizacija 2 = resinhronizacija ni uspela, vnovični poskus

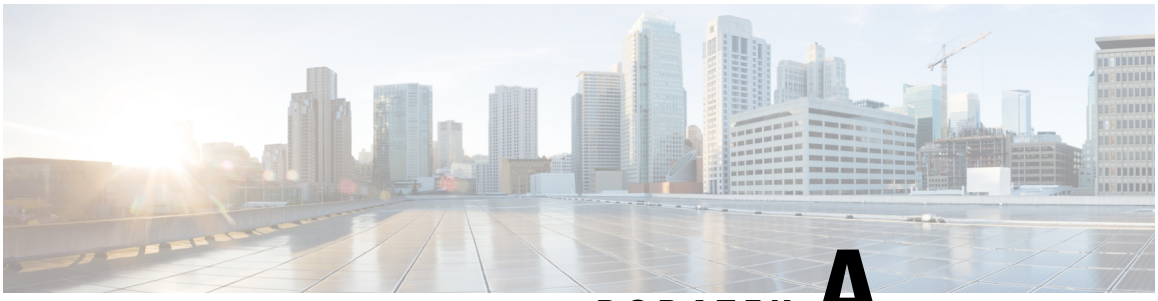
Ime parametra	Opis in privzeta vrednost
UPGST	Stanje nadgradnje (številski niz): 1 = prvi poskus nadgradnje 2 = nadgradnja ni uspela, vnovični poskus
UPGERR	Sporočilo z rezultatom (ERR) prejšnjega poskusa nadgradnje; primer: http_get failed
PRVTMR	Št. sekund od zadnjega poskusa resinhronizacije
UPGTMR	Št. sekund od zadnjega poskusa nadgradnje
REGTMR1	Št. sekund, odkar je linija 1 izgubila registracijo s strežnikom SIP
REGTMR2	Št. sekund, odkar je linija 2 izgubila registracijo s strežnikom SIP
UPGCOND	Ime podedovanega makra
SCHEME	Shema za dostop do datotek – TFTP, HTTP ali HTTPS, pridobljena z razčlenitvijo URL-ja za resinhronizacijo ali nadgradnjo
SERV	Gostiteljsko ime ciljnega strežnika zahteve, pridobljeno z razčlenitvijo URL-ja za resinhronizacijo ali nadgradnjo
SERVIP	Naslov IP ciljnega strežnika zahteve, pridobljen z razčlenitvijo URL-ja za resinhronizacijo ali nadgradnjo, po možnosti po iskanju DNS
PORT	Vrata UDP/TCP ciljnega strežnika zahteve, pridobljeno z razčlenitvijo URL-ja za resinhronizacijo ali nadgradnjo
PATH	Datotečna pot ciljnega strežnika zahteve, pridobljena z razčlenitvijo URL-ja za resinhronizacijo ali nadgradnjo
ERR	Sporočilo z rezultatom poskusa resinhronizacije ali nadgradnje Uporabno samo za generiranje sporočil sistemskega dnevnika z rezultatom. Vrednost je ohranjena v spremenljivki UPGERR v primeru poskusov nadgradnje.
UIDn	Vsebina konfiguracijskega parametra UserID za linijo n.
EMS	Stanje funkcije Extension Mobility
MUID	Uporabniški ID za funkcijo Extension Mobility

Ime parametra	Opis in privzeta vrednost
MPWD	Geslo za funkcijo Extension Mobility

Kode notranjih napak

Telefon ima določenih več kod notranjih napak (X00–X99), ki omogočajo konfiguriranje s tem, ker zagotavljajo natančnejši nadzor nad načinom delovanja enote v različnih pogojih, ko pride do napake.

Ime parametra	Opis in privzeta vrednost
X00	Napaka transportnega sloja (ali ICMP) pri pošiljanju zahteve SIP.
X20	Časovna omejitev zahteve SIP poteče med čakanjem na odziv.
X40	Splošna napaka protokola SIP (npr. nesprejemljiv kodek v SDP v sporočilih 200 in ACK ali potek časovne omejitve med čakanjem na ACK).
X60	Klicana številka je neveljavna v skladu z danim načrtom klicanja.



DODATEK A

Vzorčni konfiguracijski profili

Vzorec odprte oblike zapisa XML

```
<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>
```

Vzorčni konfiguracijski profili

```
<!--  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>
```

Vzorčni konfiguracijski profili

```
<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>
```

Vzorčni konfiguracijski profili

```
<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:
en-US|en-CA|en-AU|en-GB|fr-FR|fr-CA|es-ES|it-IT|de-DE|nn-NO|pt-PT|nl-NL|sv-SE|pt-BZ|es-MX|en-NZ|da-DK|ru-RU|pl-PL|tr-TR|cs-CZ|hu-HU|fi-FI|sk-SK|bg-BG|hr-HR|ja-JP|ko-KR|zh-CN|zh-HK

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

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

Vzorčni konfiguracijski profili

```
<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
```

Vzorčni konfiguracijski profili

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

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

Vzorčni konfiguracijski profili

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

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

Vzorčni konfiguracijski profili

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

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

Vzorčni konfiguracijski profili

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

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

Vzorčni konfiguracijski profili

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

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

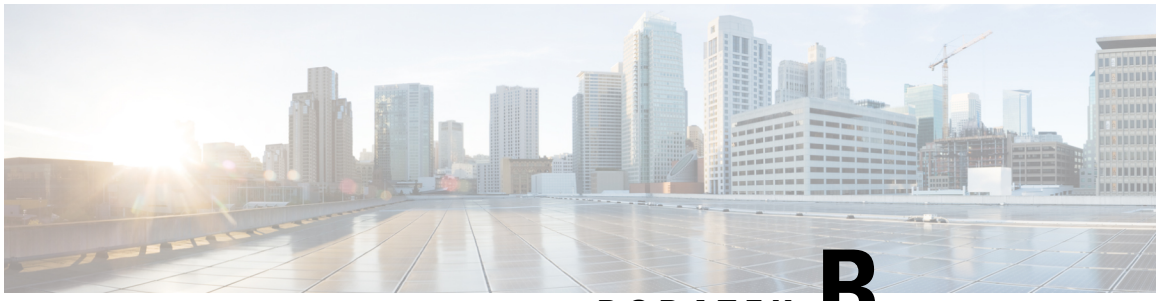
Vzorčni konfiguracijski profili

```
<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"/>
```

Vzorčni konfiguracijski profili

```
 <!--  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>
```



DODATEK B

Kratice

Kratice

AC	Izmenični tok
ACS	Strežnik za nadzor dostopa
A/D	Analogno digitalni pretvornik
AES	Advanced Encryption Standard
ANC	Anonimni klic
DT	Dostopna točka
ASCII	American Standard Code for Information Interchange
B2BUA	Zaporedni uporabnikov posrednik
BLF	Polje z lučko za zasedeno linijo
Bool	Logične vrednosti. V profilu navedeno kot "da" in "ne" oziroma 1 in 0
BootP	Protokol Bootstrap
CA	Urad za potrdila
CAS	Opozorilni signal CPE
CDP	Cisco Discovery Protocol
CDR	Zapis s podrobnostmi o klicu
CGI	Computer-Generated Imagery
CID	ID klicatelja
CIDCW	ID klicatelja za klic na čakanju

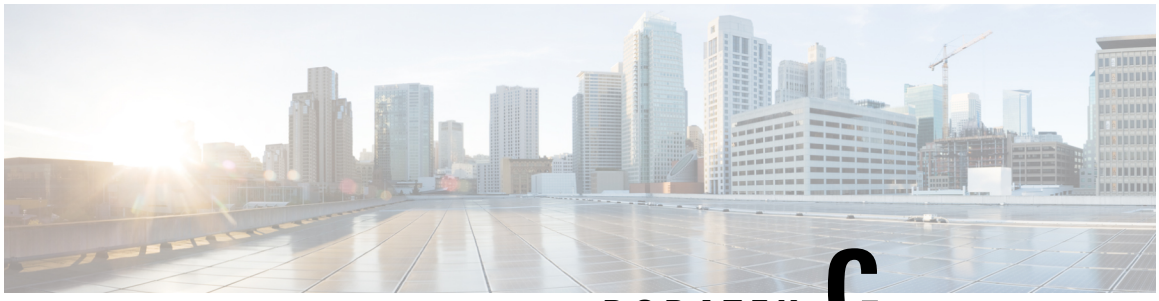
CNG	Generiranje odzadnega zvoka
CPC	Nadzor kličočega
CPE	Oprema v prostorih stranke
CSV	Z vejicami razmejena vrednost
CWCID	ID klicatelja za klic na čakanju
CWT	Ton za klic na čakanju
D/A	Digitalno analogni pretvornik
dB	decibel
dBm	dB glede na 1 mW
DHCP	Protokol za dinamično konfiguracijo gostitelja
Ne moti	Ne moti
DNS	Sistem DNS
DoS	Zavrnitev storitve
DRAM	Pomnilnik DRAM
DSL	Digitalna naročniška zanka
DSP	Digitalni signalni procesor
DST	Poletni/zimski čas
DTAS	Signal DTAS (enako kot CAS)
DTMF	Dvotonska večfrekvenčna signalizacija
FQDN	Popolnoma določeno ime domene
FSK	Modulacija s frekvenčnim pomikom
FW	Vdelana programska oprema
FXS	Foreign eXchange Station
GMT	Greenwiški srednji čas
GW	Prehod
HTML	Označevalni jezik za hiperbesedilo
HTTP	Protokol za prenos hiperbesedila
HTTPS	HTTP prek SSL
ICMP	Internet Control Message Protocol

IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internetni protokol
IPv4	Internetni protokol različice 4
IPv6	Internetni protokol različice 6
ISP	Ponudnik internetnih storitev
ITSP	Ponudnik storitev internetne telefonije
ITU	Mednarodna telekomunikacijska zveza
IVR	Interaktivni glasovni odgovor
LAN	Krajevno omrežje
LBR	Nizka bitna hitrost
LBRC	Kodek nizke bitne hitrosti
LCD	Zaslon iz tekočih kristalov; imenovan tudi zaslon
LDAP	Lightweight Directory Access Protocol
LED	Svetleča dioda
Naslov MAC	Naslov Media Access Control
MC	Minipotrdilo
MGCP	Protokol za nadzor predstavnostnega prehoda
MOH	Music On Hold
MOS	Povprečna ocena mnenja (1–5, višja je boljša)
MPP	Telefoni za več platform
ms	Milisekunda
MSA	Vmesnik za glasbeni vir
MWI	Indikator za čakajoče sporočilo
NAT	Prevajanje omrežnih naslovov
NPS	Običajni strežnik za omogočanje uporabe
NTP	Protokol omrežnega časa
OOB	Zunaj pasu
OSI	Odprt preklopni interval

PBX	Hišna centrala
PCB	Tiskano vezje
PoE	Napajanje prek etherneta (PoE)
PR	Zamenjava polarnosti
PS	Strežnik za omogočanje uporabe
PSQM	Merilo zaznane kakovosti govora (1–5, manjše je boljše)
PSTN	Javno komutirano telefonsko omrežje
QoS	Kakovost storitve
RC	Odstrani prilagajanje
REQT	(SIP) sporočilo z zahtevo
RESP	(SIP) odzivno sporočilo
RSC	(SIP) koda stanja odziva, kot je 404, 302, 600
RTP	Protokol realnega časa
RTT	Obhodni čas
SAS	Strežnik za pretočni zvok
SDP	Protokol SDP
SDRAM	Sinhroni DRAM
s	sekunde
SIP	Protokol SIP
SLA	Prikaz skupne linije
SLIC	Vmesniški krogotok naročniškega voda
SP	Ponudnik storitev
SSL	Sloj SSL
STUN	UDP seje prečkanja za NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTL	Življenjska doba
ToS	Vrsta storitve

UA	Uporabnikov posrednik
uC	Mikrokrmilnik
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Usklajeni univerzalni čas
VAR	Prodajalec z dodano vrednostjo
VLAN	Glasovni LAN
VM	Glasovna pošta
VMWI	Vizualni indikator za čakajoče sporočilo
VoIP	Prenos govora po omrežju IP
VQ	Kakovost zvoka
WAN	Prostrano omrežje
XML	Jezik Extensible Markup Language

Kratice



DODATEK C

Sorodna dokumentacija

Sorodna dokumentacija

Za pridobivanje povezanih informacij uporabite naslednje razdelke.

Dokumentacija za Cisco IP Phone 6800 Series

Oglejte si dokumentacijo posebej za svoj jezik, model telefona in izdajo vdelane programske opreme za več platform. Pojdite na ta spletni naslov (URL):

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

Pravilnik o podpori za vdelano programsko opremo telefonov Cisco IP Phone

Za informacije o pravilniku o podpori za telefone obiščite https://cisco.com/go/phonefirmwaresupport.