



## **Príručka o poskytovaní pre multiplatformové telefóny Cisco IP Phone radu 6800**

**Prvé vydanie:** 2017-11-22

**Posledná zmena:** 2019-01-30

### **Americas Headquarters**

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

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

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

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

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://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](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. Všetky práva vyhradené.



## OBSAH

---

### KAPITOLA 1

#### Nasadzovanie a poskytovanie 1

Prehľad poskytovania 1

Poskytovanie TR69 2

Metódy RPC 3

Podporované metódy RPC 3

Podporované typy udalostí 3

Správanie telefónu pri zhutnení sieťových prenosov 4

Nasadenie 4

Hromadná distribúcia 4

Maloobchodná distribúcia 5

Proces opätovnej synchronizácie 6

Poskytovanie 6

Normálny poskytovací server 7

Spravovanie prístupu ku konfigurácii 7

Prístup na webovú stránku telefónu 7

Povolenie webového prístupu k telefónu Cisco IP Phone 8

Šifrovanie komunikácie 8

Praktiky poskytovania telefónov 8

Manuálne poskytovanie telefónu z klávesnice 9

Zdieľanie verzie SW v skupine 9

Obídienie obrazovky nastavenia hesla 10

---

### KAPITOLA 2

#### Poskytovacie skripty 13

Poskytovacie skripty 13

Formáty konfiguračných profilov 13

Komponenty konfiguračných súborov 14

Vlastnosti značiek prvkov	14
Atribút prístupu používateľa	16
Správa prístupu	16
Vlastnosti parametrov	16
Formáty reťazcov	17
Kompresia a šifrovanie otvoreného profilu (XML)	17
Skomprimovanie otvoreného profilu	18
Šifrovanie otvoreného profilu	18
Šifrovanie AES-256-CBC	18
Šifrovanie obsahu HTTP podľa normy RFC 8188	22
Voliteľné argumenty opätovnej synchronizácie	23
key	23
uid a pwd	23
Aplikácia profilu na telefonické IP zariadenie	23
Stiahnutie konfiguračného súboru na telefón zo servera TFTP	24
Stiahnutie konfiguračného súboru na telefón s použitím cURL	24
Parametre poskytovania	24
Parametre na všeobecné účely	25
Použitie parametrov na všeobecné účely	25
Povoľovacie	26
Spúšťače	26
Opätovná synchronizácia v určených intervaloch	26
Opätovná synchronizácia v určenom čase	27
Konfigurovateľné plány	27
Pravidlá profilu	28
Pravidlo aktualizácie	30
Typy údajov	31
Aktualizácie profilu a firmvéru	34
Povolenie a konfigurácia aktualizácií profilu	35
Povolenie a konfigurácia aktualizácií firmvéru	35
Aktualizácia firmvéru cez TFTP, HTTP alebo HTTPS	36
Aktualizácia firmvéru cez príkaz v prehliadači	36

Interná príprava na poskytovanie a poskytovacie servery	37
Príprava servera a softvérové nástroje	37
Distribúcia Vzdialeného prispôsobenia (Remote Customization – RC)	38
Interná príprava zariadení na poskytovanie	39
Nastavenie poskytovacieho servera	40
Poskytovanie TFTP	40
Ovládanie vzdialených koncových bodov a NAT	40
Poskytovanie HTTP	41
Riadenie kódu stavu HTTP pre opätovnú synchronizáciu a aktualizáciu	42
Poskytovanie HTTPS	43
Získanie podpísaného certifikátu servera	43
Hlavný certifikát klienta CA multiplatformových telefónov	44
Redundantné poskytovacie servery	45
Server systémového denníka	45

---

**KAPITOLA 4**
**Príklady poskytovania 47**

Prehľad príkladov poskytovania	47
Základná opätovná synchronizácia	47
Opätovná synchronizácia s TFTP	47
Požitie systémového denníku na zaznamenávanie správ	48
Automatická opätovná synchronizácia zariadenia	49
Jedinečné profily, rozvoj makier a HTTP	50
Príklad: Poskytnutie konkrétneho profilu telefónu IP Phone na serveri TFTP	51
Poskytovanie cez Cisco XML	52
Rozpoznanie URL pomocou rozvoja makier	52
Bezpečná opätovná synchronizácia s HTTPS	53
Základná opätovná synchronizácia s HTTPS	53
Príklad: Základná opätovná synchronizácia s HTTPS	54
HTTPS s overovaním pomocou certifikátu klienta	55
Príklad: HTTPS s overovaním pomocou certifikátu klienta	55
Filtrovanie klientov HTTPS a dynamický obsah	56
Certifikáty HTTPS	57
Metodológia HTTPS	57
Certifikát servera SSL	57

Získanie certifikátu servera	58
Certifikát klienta	58
Štruktúra certifikátu	58
Konfigurácia vlastnej certifikačnej autority (Certificate Authority – CA)	59
Správa profilu	60
Skomprimovanie otvoreného profilu pomocou aplikácie Gzip	60
Šifrovanie profilu pomocou OpenSSL	61
Vytváranie rozdelených profilov	62
Nastavenie hlavičky súkromia telefónu	63

---

**KAPITOLA 5****Parametre poskytovania 65**

Prehľad parametrov poskytovania	65
Parametre konfiguračného profilu	65
Parametre aktualizácie firmvéru	70
Parametre na všeobecné účely	72
Premenné rozvoja makier	72
Kódy interných chýb	75

---

**DODATOK A:****Príklady konfiguračných profilov 77**

Príklad otvoreného formátu XML	77
--------------------------------	----

---

**DODATOK B:****Skratky 99**

Skratky	99
---------	----

---

**DODATOK C:****Súvisiaca dokumentácia 105**

Súvisiaca dokumentácia	105
Dokumentácia k telefónu Cisco IP Phone radu 6800	105
Pravidlá podpory firmvéru pre IP telefóny Cisco IP Phone	105



## KAPITOLA 1

# Nasadzovanie a poskytovanie

---

- [Prehľad poskytovania, na strane 1](#)
- [Poskytovanie TR69, na strane 2](#)
- [Správanie telefónu pri zhutnení sieťových prenosov, na strane 4](#)
- [Nasadenie, na strane 4](#)
- [Poskytovanie, na strane 6](#)

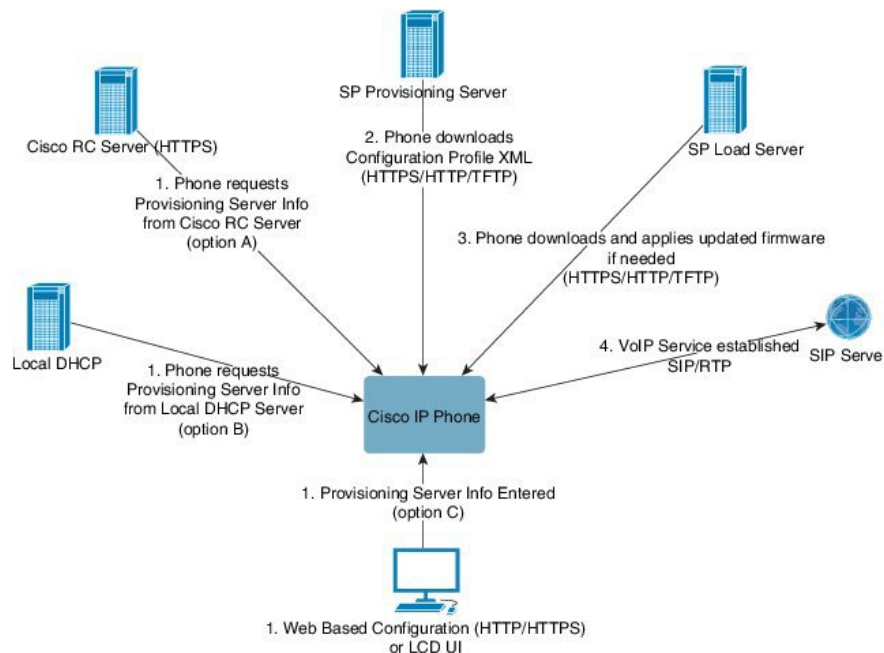
## Prehľad poskytovania

Telefóny Cisco IP phones sú určené na vysokoobjemové nasadenia poskytovateľmi služby VoIP (Voice-over-IP – prenos hlasu internetovým protokolom) zákazníkom v domácnostiach, firmám a podnikovému prostrediu. Preto poskytovanie telefónu prostredníctvom vzdialenej správy a konfigurácie zabezpečuje správne fungovanie telefónu na strane zákazníka.

Spoločnosť Cisco podporuje prispôsobenú a neustálu konfiguráciu funkcií telefónu vďaka:

- Spoľahlivému vzdialenému ovládaniu telefónu.
- Šifrovaniu komunikácie, ktorá ovláda telefón.
- Zjednodušenej väzbe konta telefónu.

Telefóny môžu byť nastavené tak, aby sťahovali konfiguračné profily alebo aktualizovaný firmvér zo vzdialeného servera. Sťahovanie sa môže uskutočniť, keď sú telefóny pripojené k sieti, po spustení alebo v určených intervaloch. Poskytovanie je zvyčajne súčasťou veľkoobjemových nasadení VoIP bežných u poskytovateľov služieb. Konfiguračné profily alebo aktualizovaný firmvér sa odosielaajú na zariadenie prostredníctvom TFTP, HTTP alebo HTTPS.



Vo všeobecnosti proces poskytovania telefónov prebieha nasledovne:

1. Ak telefón nie je nakonfigurovaný, aplikujú sa naň informácie poskytovajúceho servera pomocou jednej z nasledovných možností:
  - **A** – Stiahnuté pomocou HTTPS zo servera Vzdialeného prispôsobenia (RC) v systéme EDOS (Enablement Data Orchestration System) spoločnosti Cisco.
  - **B** – Vyhľadane na miestnom serveri DHCP.
  - **C** – Zadané manuálne pomocou webovej konfiguračnej pomôcky spoločnosti Cisco alebo UI telefónu.
2. Telefón stiahne informácie poskytovajúceho servera a aplikuje konfiguračné XML pomocou protokolu HTTPS, HTTP alebo TFTP.
3. Telefón v prípade potreby stiahne a aplikuje aktualizovaný firmvér pomocou HTTPS, HTTP alebo TFTP.
4. Služba VoIP je zriadená s použitím určenej konfigurácie a firmvéru.

Poskytovatelia služby VoIP chcú pre klientov v domácnostiach a malých firmách nasadiť veľa telefónov. Vo firmách alebo obchodným spoločnostiach môžu telefóny fungovať ako terminálové uzly. Poskytovatelia často cez internet rozširujú tieto zariadenia, ktoré sú u zákazníka pripojené cez smerovače a brány Firewall.

Telefón sa môže použiť ako vzdialené rozšírenie backendového vybavenia poskytovateľa služby. Vzdialená správa a konfigurácia telefónu zabezpečuje správne fungovanie telefónu na strane zákazníka.

## Poskytovanie TR69

Telefón Cisco IP Phone pomáha správcovi konfigurovať parametre TR69 pomocou webového UI. Informácie o parametroch vrátane porovnania parametrov XML a TR69 nájdete v Príručke na správu príslušného radu telefónov.



Telefóny podporujú zisťovanie servera automatickej konfigurácie (Auto Configuration Server – ACS) z možnosti DHCP 43, 60 a 125.

- Možnosť 43 – Informácie konkrétneho dodávateľa pre URL servera ACS.
- Možnosť 60 – Identifikátor triedy dodávateľa, aby sa telefón identifikoval s `dslforum.org` do ACS.
- Možnosť 125 – Informácie konkrétneho dodávateľa pre priradenie brány.

## Metódy RPC

### Podporované metódy RPC

Telefóny podporujú iba niektoré metódy RPC (Remote Procedure Call – Vzdialené volanie procedúr), ktoré sú uvedené nižšie:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: Metóda RPC na sťahovanie, podporované typy súborov sú:
  - Oblasť aktualizácie firmvéru
  - Konfiguračný súbor dodávateľa
  - Súbor vlastnej certifikačnej autority (Certificate Authority – CA)
- Prepojenie dokončené

### Podporované typy udalostí

Telefóny podporujú typy udalostí podľa podporovaných funkcií a metód. Sú podporované iba nasledovné typy udalostí:

- Bootstrap
- Boot

- zmena hodnoty
- Žiadosť o pripojenie
- Pravidelné
- Prepojenie dokončené
- M stiahnutie
- M reštart

## Správanie telefónu pri zhustení sieťových prenosov

- administratívne úkony, ako je skenovanie interných portov alebo bezpečnostné skenovanie,
- útoky, ku ktorým dochádza v sieti, napr. útok odmietnutia služby.

## Nasadenie

Telefóny Cisco IP Phones poskytujú praktické mechanizmy pre poskytovanie založené na týchto modeloch nasadenia:

- Hromadná distribúcia – Poskytovateľ služby nakúpi telefóny Cisco IP Phones vo veľkom počte a pripraví ich na poskytovanie na mieste alebo od spoločnosti Cisco zakúpi jednotky Vzdialeného prispôsobenia (Remote Customization - RC). Tieto zariadenia sú potom dodávané zákazníkovi v rámci servisnej zmluvy o VoIP.
- Maloobchodná distribúcia – Zákazník zakúpi telefón Cisco IP Phone v maloobchodnej predajni a požiadava poskytovateľa služby o službu VoIP. Poskytovateľ služby musí podporovať bezpečnú vzdialenú konfiguráciu zariadenia.

## Hromadná distribúcia

Pre tento model poskytovateľ služby vydáva telefóny svojim zákazníkom v rámci servisnej zmluvy VoIP. Zariadenia sú buď jednotky RC, alebo sú pripravované na poskytovanie na mieste.

Spoločnosť Cisco jednotky RC pripravuje na poskytovanie, aby sa opätovne synchronizovali so serverom Cisco, ktorý sťahuje profil zariadenia a aktualizácie firmvéru.

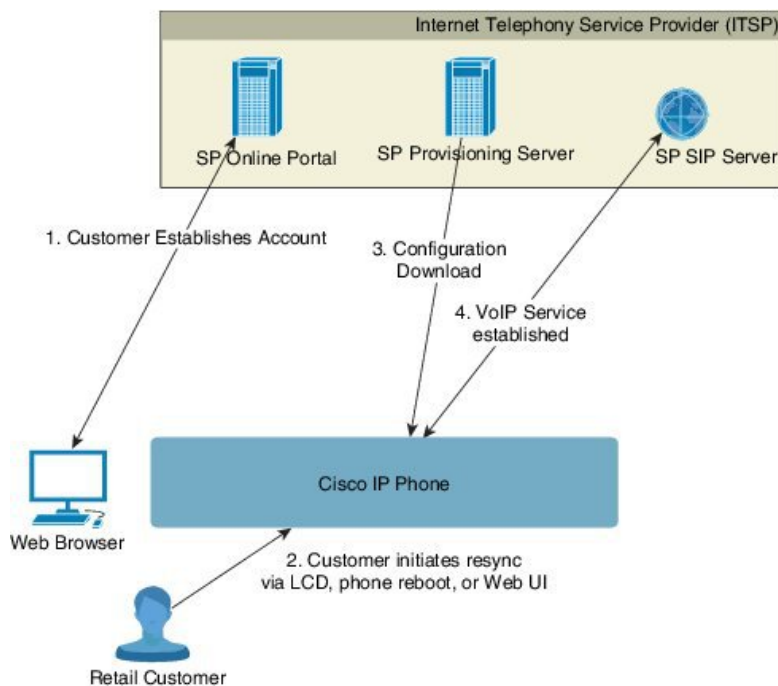
Poskytovateľ služby môže telefóny pripraviť na poskytovanie so želanými parametrami vrátane parametrov, ktoré spravujú opätovnú synchronizáciu, viacerými spôsobmi:

- Na mieste s použitím DHCP a TFTP
- Vzdialene s použitím TFTP, HTTP alebo HTTPS
- Kombináciou poskytovania na mieste a vzdialeného poskytovania

## Maloobchodná distribúcia

V modeli maloobchodnej distribúcie zákazník zakúpi telefón a predplatí si konkrétnu službu. Poskytovateľ internetových telefonických služieb (ITSP) nastaví a udržiava poskytovací server a pripraví telefón na opätovnú synchronizáciu so serverom poskytovateľa služby.

**Obrázok 1: Maloobchodná distribúcia**



Telefón obsahuje webovú konfiguračnú pomôcku, ktorá zobrazuje vnútornú konfiguráciu a prijíma nové hodnoty parametrov konfigurácie. Server tiež prijíma špeciálnu syntax príkazov URL na vykonávanie operácií vzdialenej opätovnej synchronizácie profilu a aktualizácie firmvéru.

Zákazník sa k službe prihlási a vytvorí si konto VoIP, potenciálne cez online portál, a prepojí zariadenie s pridruženým kontom služby. Nenastavený telefón dostane inštrukciu, aby sa opätovne synchronizoval s určeným poskytovacím serverom cez príkaz URL. Príkaz URL zvyčajne zahŕňa číslo ID zákazníka alebo alfanumerický kód, ktorý pridruží zariadenie k novému kontu.

V nasledovnom príklade má zariadenie na adrese IP 192.168.1.102 priradenej protokolom DHCP poskytovať samo seba službu SuperVoIP:

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

V tomto príklade je číslo ID zákazníka pre nový účet 1234abcd. Vzdialený poskytovateľ pridruží telefón, ktorý žiada o opätovnú synchronizáciu, k novému kontu na základe URL a dodaného ID zákazníka. Vďaka tejto operácii opätovnej synchronizácie na začiatku sa telefón nakonfiguroval v jednom kroku. Telefón je následne automaticky presmerovaný na opätovnú synchronizáciu s permanentným URL na serveri. Príklad:

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

Pri počiatočnom aj permanentnom prístupe poskytovací server využíva na overenie certifikát klienta telefónu. Poskytovací server poskytuje správne hodnoty parametrov konfigurácie na základe pridruženého konta služby.

Keď sa zariadenie zapne alebo prejde určená doba, telefón sa opätovne synchronizuje a stiahne najnovšie parametre. Tieto parametre sa môžu týkať napríklad vytvárania skupiny vyhľadávania, nastavenia čísel rýchlejšej voľby a obmedzenia funkcií, ktoré môže používateľ meniť.

#### Príbuzné témy

[Interná príprava zariadení na poskytovanie](#), na strane 39

## Proces opätovnej synchronizácie

Firmvér každého telefónu zahŕňa administratívny webový server, ktorý prijíma nové hodnoty parametrov konfigurácie. Telefón môže byť nastavený tak, aby opätovne synchronizoval konfiguráciu po reštarte alebo v určených intervaloch s určeným poskytovacím serverom prostredníctvom príkazu na opätovnú synchronizáciu URL v profile zariadenia.

Webový server je predvolene aktivovaný. Ak chcete povoliť alebo zakázať webový server, použite príkaz URL na opätovnú synchronizáciu.

V prípade potreby je možné požiadať o okamžitú opätovnú synchronizáciu pomocou adresy URL akcie „opätovná synchronizácia“. Príkaz URL na opätovnú synchronizáciu môže zahŕňať číslo ID zákazníka alebo alfanumerický kód, ktorý jedinečne pridruží zariadenie ku kontu používateľa.

#### Príklad

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

V tomto príklade má zariadenie na adrese IP 192.168.1.102 priradenej protokolom DHCP poskytovať samo seba službu SuperVoIP na prov.supervoip.com. Číslo ID zákazníka pre nový účet je 1234abcd. Vzdialený poskytujúci server pridruží telefón, ktorý žiada o opätovnú synchronizáciu, ku kontu na základe URL a ID zákazníka.

Vďaka tejto operácii opätovnej synchronizácie na začiatku sa telefón nakonfiguroval v jednom kroku. Telefón je následne automaticky presmerovaný na opätovnú synchronizáciu s permanentným URL na serveri.

Pri počiatočnom aj permanentnom prístupe poskytujúci server využíva na overenie certifikát klienta. Server poskytuje hodnoty parametrov konfigurácie na základe pridruženého konta služby.

## Poskytovanie

Telefón je možné nakonfigurovať tak, aby pravidelne a pri zapnutí opätovne synchronizoval svoj vnútorný stav konfigurácie so vzdialeným profilom. Telefón kontaktuje normálny poskytovací server (NPS) alebo server spravovania prístupu (ACS).

Predvolené nastavenie je, že telefón sa pokúsi o opätovnú synchronizáciu profilu, keď je nečinný. Pomáha to predchádzať aktualizácii, ktorá by spustila reštart softvéru a prerušila by hovor. Ak sa vyžaduje čiastočná aktualizácia kvôli súčasnému stavu aktualizácie zo staršieho vydania, logika aktualizácie môže automaticky spustiť aktualizáciu vo viacerých fázach.

## Normálny poskytovací server

Normálny poskytovací server (NPS) môže byť server TFTP, HTTP alebo HTTPS. Vzdialená aktualizácia firmvéru sa uskutočňuje pomocou TFTP, HTTP alebo HTTPS, pretože firmvér neobsahuje dôverné informácie.

Hoci sa odporúča HTTPS, komunikácia s NPS nevyžaduje používanie zabezpečeného protokolu, pretože aktualizovaný profil môže byť zašifrovaný zdieľaným tajným kľúčom. Ďalšie informácie o používaní HTTPS nájdete v časti [Šifrovanie komunikácie, na strane 8](#). Zabezpečené prvé poskytovanie sa uskutoční pomocou mechanizmu, ktorý využíva funkciu SSL. Nezapojený telefón môže prijať 256-bitový profil zašifrovaný symetrickým kľúčom, ktorý je určený pre konkrétne zariadenie.

## Spravovanie prístupu ku konfigurácii

Firmvér telefónu poskytuje mechanizmy na obmedzenie prístupu koncového používateľa k niektorým parametrom. Firmvér poskytuje určené povolenia, ktoré sa viažu k prihláseniu do konta **Správca** alebo **Používateľ**. Každé môže byť nezávisle chránené heslom.

- Konto správcu – Umožňuje poskytovateľovi služby plný prístup k všetkým parametrom administratívneho webového servera.
- Používateľské konto – Umožňuje používateľovi služby konfiguráciu podskupiny parametrov administratívneho webového servera.

Poskytovateľ služby môže obmedziť používateľské konto v poskytovacom profile nasledovným spôsobom:

- Pri vytváraní konfigurácie vyberte, ktoré parametre konfigurácie majú byť dostupné používateľskému kontu.
- Zakázať prístup používateľa k administratívne webovému serveru.
- Zakázať prístup používateľa k používateľskému rozhraniu LCD.
- Obísť obrazovku **Nastaviť heslo** pre používateľa.
- Obmedziť internetové domény, na ktoré pristupuje zariadenie kvôli opätovnej synchronizácii, aktualizácii a registrácii SIP pre Linku 1.

### Príbuzné témy

[Vlastnosti značiek prvkov](#), na strane 14

[Správa prístupu](#), na strane 16

## Prístup na webovú stránku telefónu

Prejdite na webovú stránku telefónu z webového prehliadača na počítači, ktorý dosiahne na telefón v podsieti.

Vás poskytovateľ služby zakázal prístup ku konfiguračnej pomôcke, pred pokračovaním kontaktujte svojho poskytovateľa služby.

### Procedúra

- 
- Krok 1** Ubezpečte sa, že počítač môže komunikovať s telefónom. Nepoužíva sa žiadne VPN.
- Krok 2** Otvorte webový prehliadač.

**Krok 3** Zadajte adresu IP telefónu do riadku adresy vo vašom webovom prehliadači.

- Prístup používateľa: **http://<adresa ip>/user**
- Prístup správcu: **http://<adresa ip>/správca/pokročilé**
- Prístup správcu: **http://<adresa ip>** kliknite na **Prihlásenie správy** a potom na **pokročilé**.

Napríklad `http://10.64.84.147/správca`

## Povolenie webového prístupu k telefónu Cisco IP Phone

Ak chcete zobraziť parametre telefónu, povoľte profil konfigurácie. Ak chcete meniť niektoré parametre, musíte byť schopní meniť konfiguračný profil. Je možné, že vás správca systému zakázal možnosť telefónu povoliť prístup alebo zápis do webového používateľského rozhrania telefónu.

Viac informácií nájdete v *Príručke o poskytovaní pre multiplatformové telefóny Cisco IP Phone radu 6800*.

### Skôr ako začnete

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).

### Procedúra

**Krok 1** Kliknite na možnosť **Hlas > Systém**.

**Krok 2** V sekcii **Konfigurácia systému** nastavte možnosť **Povoľiť webový server** na **Áno**.

**Krok 3** Ak chcete aktualizovať konfiguračný profil, po upravení polí vo webovom používateľskom rozhraní telefónu kliknite na tlačidlo **Odoslať všetky zmeny**.

Telefón sa reštartuje a zmeny sa aplikujú.

**Krok 4** Ak chcete vymazať všetky zmeny, ktoré ste spravili počas súčasnej relácie (alebo po poslednom kliknutí na **Odoslať všetky zmeny**), kliknite na tlačidlo **Zmazať všetky zmeny**. Hodnoty sa obnovia na predchádzajúce nastavenia.

## Šifrovanie komunikácie

Parametre komunikácie posielané zariadeniu môžu obsahovať kódy oprávnenia alebo iné informácie, ktoré chránia systém pred nepovoleným prístupom. Je v záujme poskytovateľa služby, aby zabránil nepovoleným aktivitám zákazníka. Je v záujme zákazníka aby zabránil nepovolenému používaniu konta. Poskytovateľ služby môže okrem obmedzenia prístupu k administráčnému webovému serveru tiež zašifrovať prenos konfiguračného profilu medzi poskytovacím serverom a zariadením.

## Praktiky poskytovania telefónov

Zvyčajne je telefón Cisco IP Phone nakonfigurovaný pre poskytovanie, keď sa prvýkrát pripojí k sieti. Telefón je tiež nastavovaný v pravidelných intervaloch určených vtedy, keď poskytovateľ služby alebo VAR pripravuje telefón na poskytovanie (nakonfiguruje). Poskytovatelia služieb môžu povoliť VAR alebo pokročilým

používateľom nastavovať telefón pomocou klávesnice telefónu. Poskytovanie môžete nakonfigurovať aj pomocou webového UI telefónu.


Skontrolujte možnosť **Stav > Stav telefónu > Poskytovanie** na UI LCD telefónu alebo Stav poskytovania v karte **Stav** vo webovej konfiguračnej pomôcke.

#### Príbuzné témy

[Manuálne poskytovanie telefónu z klávesnice](#), na strane 9

## Manuálne poskytovanie telefónu z klávesnice

### Procedúra

- Krok 1** Stlačte tlačidlo **Aplikácie** .
- Krok 2** Vyberte možnosť **Správa zariadenia > Pravidlo profilu**.
- Krok 3** Zadajte pravidlo profilu vo formáte:

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

Príklad:

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

Ak nie je určený žiadny protokol, predpokladá sa TFTP. Ak nie je určený žiadny názov servera, hostiteľ si vyžiada URL, ktoré sa použije ako názov servera. Ak nie je určený žiadny port, použije sa predvolený port (69 pre TFTP, 80 pre HTTP alebo 443 pre HTTPS).

- Krok 4** Stlačte tlačidlo **Znova synchronizovať**.

### Príbuzné témy

[Praktiky poskytovania telefónov](#), na strane 8

## Zdieľanie verzie SW v skupine

Zdieľanie verzie SW v skupine (PFS) je model distribúcie firmvéru, ktorý umožňuje telefónom Cisco IP Phone vyhľadať v podsieti iné telefóny s rovnakým modelom alebo z rovnakého radu a zdieľať s nimi aktualizované súbory firmvéru. Umožňuje tak súbežne inovovať viacero telefónov. Funkcia PFS používa protokol CPPDP (Cisco Peer-to-Peer-Distribution Protokol), čo je proprietárny protokol spoločnosti Cisco. Keď sa používa protokol CPPDP, všetky zariadenia v podsieti utvoria hierarchiu peer-to-peer a následne sa firmvér a všetky ďalšie súbory zo zariadení v skupine skopírujú na susedné zariadenia. V záujme optimalizácie inovácie firmvéru hlavný (koreňový) telefón stiahne obraz firmvéru zo servera na načítanie a potom odošle tento firmvér do ďalších telefónov v podsieti prostredníctvom pripojení TCP.

Zdieľanie verzie SW v skupine:

- Obmedzuje preťaženie prenosov cez TFTP do centralizovaných vzdialených serverov pre načítanie.
- Eliminuje potrebu manuálne riadiť inovácie firmvéru.
- Skracuje prestoje telefónov počas inovácie, keď dôjde k súbežnému resetovaniu veľkého množstva telefónov.

**Poznámka**

- Zdieľanie verzie SW v skupine nebude fungovať, pokiaľ viacero telefónov nie je nakonfigurovaných tak, aby sa súčasne inovovali. Keď sa odošle správa NOTIFY s Event:resync, spustí sa operácia resync na telefóne. Príklad súboru XML, ktorý môže obsahovať konfigurácie na spustenie inovácie:

"Event:resync;profile="http://10.77.10.141/profile.xml"

- Ak nastavíte adresu IP a port servera denníka funkcie zdieľania verzie SW v skupine, denníky súvisiace s funkciou PFS sa budú odosielať na tento server ako správy protokolu UDP. Toto nastavenie je potrebné vykonať na každom telefóne. Potom budete môcť na základe týchto správ v denníku riešiť problémy súvisiace s funkciou PFS.

Prvok Peer\_Firmware\_Sharing\_Log\_Server určuje názov hostiteľa a port vzdialeného servera systémového denníka komunikujúceho cez protokol UDP. Predvolený port servera systémového denníka je 514.

Príklad:

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

Ak chcete používať túto funkciu, zapnite funkciu PFS v telefónoch.

## Obídenie obrazovky nastavenia hesla

Obrazovku **Nastaviť heslo** telefónu môžete pri prvom spustení alebo po obnovení výrobných nastavení obísť, ak ste vykonali tieto akcie zriadenia:

- Konfigurácia DHCP
- Konfigurácia EDOS
- Konfigurácia hesla používateľa prostredníctvom konfiguračného súboru XML telefónu

**Tabuľka 1: Akcie zriadenia, ktoré určujú, či sa zobrazí obrazovka Nastaviť heslo**

Je nakonfigurované DHCP	Je nakonfigurované EDOS	Je nakonfigurované heslo používateľa	Obísť obrazovku Nastaviť heslo
Áno	nie je k dispozícii	Áno	Áno
Áno	nie je k dispozícii	Nie	Nie
Nie	Áno	Áno	Áno
Nie	Áno	Nie	Nie
Nie	Nie	nie je k dispozícii	Nie

### Procedúra

- Krok 1** Upravte súbor `config.xml` telefónu v textovom editore alebo editore XML.
- Krok 2** Vložte značku `<User_Password>` niektorým z nasledujúcich spôsobov.



- Žiadne heslo (začiatočná a koncová značka) – `<User_Password></User_Password>`
- Hodnota hesla (4 až 127 znakov) – `<User_Password ua="rw">abc123</User_Password>`
- Žiadne heslo (iba začiatočná značka) – `<User_Password />`

**Krok 3** Uložte zmeny do súboru `config.xml`.

---





## KAPITOLA 2

# Poskytovacie skripty

- [Poskytovacie skripty, na strane 13](#)
- [Formáty konfiguračných profilov, na strane 13](#)
- [Kompresia a šifrovanie otvoreného profilu \(XML\), na strane 17](#)
- [Aplikácia profilu na telefonické IP zariadenie, na strane 23](#)
- [Parametre poskytovania, na strane 24](#)
- [Typy údajov, na strane 31](#)
- [Aktualizácie profilu a firmvéru, na strane 34](#)

## Poskytovacie skripty

Telefón prijíma konfiguráciu vo formáte XML.

Podrobné informácie o telefóne nájdete v príručke na správu pre vaše konkrétne zariadenie. Každá príručka opisuje parametre, ktoré je možné konfigurovať prostredníctvom administratívneho webového servera.

## Formáty konfiguračných profilov

Konfiguračný profil definuje hodnoty parametrov pre telefón.

Formát konfiguračného profilu XML využíva na kompilovanie parametrov a hodnôt štandardné nástroje na tvorbu súborov XML.



### Poznámka

Je podporovaná iba znaková sada UTF-8. Ak profil upravíte v editore, nemeňte formát kódovania, inak telefón súbor nerozpozná.

Každý telefón má rôzne funkcie a preto aj rôzne parametre.

### Profil vo formáte XML (XML)

Profil v otvorenom formáte je textový súbor so syntaxou podobnou XML v hierarchii prvkov, ktorý obsahuje atribúty prvkov a hodnoty. Tento formát vám umožňuje na vytvorenie konfiguračného súboru použiť štandardné nástroje. Konfiguračný súbor v tomto formáte sa počas operácie opätovnej synchronizácie môže odoslať z poskytovacieho servera na telefón. Súbor môže byť poslaný bez kompilácie ako binárny objekt.

Telefón dokáže prijať konfiguračné formáty generované štandardnými nástrojmi. Táto funkcia zjednodušuje vývoj backendového softvéru poskytovacieho servera, ktorý generuje konfiguračné profily z existujúcich databáz.

Aby boli chránené dôverné informácie v konfiguračnom profile, poskytovací server odošle tento typ súboru na telefón cez kanál zabezpečený TLS. Súbor môže byť voliteľne skomprimovaný použitím algoritmu DEFLATE nástroja gzip (RFC1951).

Súbor môže byť zašifrovaný niektorou z nasledujúcich metód šifrovania:

- Šifrovanie AES-256-CBC
- Šifrovanie obsahu HTTP podľa normy RFC 8188 so šifrou AES-128-GCM

### Príklad: Otvorený formát profilu

```
<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>
```

Značka prvku <flat-profile>ohraničuje všetky prvky parametrov, ktoré telefón dokáže rozpoznať.

### Príbuzné témy

[Kompresia a šifrovanie otvoreného profilu \(XML\)](#), na strane 17

## Komponenty konfiguračných súborov

Konfiguračný súbor môže zahŕňať nasledovné komponenty:

- Značky prvkov
- Vlastnosti
- Parametre
- Funkcie formátovania
- Komentáre XML

### Vlastnosti značiek prvkov

- Formát poskytovania XML a webové UI umožňujú konfiguráciu rovnakých nastavení. Názov značky XML a poľa vo webovom UI sú podobné, ale môžu sa líšiť kvôli obmedzeniam názvu prvkov v XML. Napríklad podčiarknutie ( \_ ) namiesto " ".
- Telefón rozpozná prvky s vlastnými názvami parametra, ktoré sú uvedené v špeciálnom prvku typu <flat-profile>.
- Názvy prvkov sú uvedené v lomených zátvorkách.
- Názvy prvkov sú väčšinou rovnaké ako názvy polí na administratívnej webovej stránke zariadenia, vyskytujú sa len nasledovné rozdiely:

- Názvy prvkov nemôžu zahŕňať medzery ani špeciálne znaky. Ak chcete z názvu poľa na administratívnej webovej stránke vytvoriť názov prvku, nahraďte každú medzeru alebo špeciálny znak [ ], ( ), alebo / podčiarknutím.

**Príklad:** Prvok <Resync\_On\_Reset> zodpovedá poľu **Resync On Reset (Po reštarte opätovne synchronizovať)**.

- Každý názov prvku musí byť jedinečný. Na administratívnych webových stránkach sa rovnaké polia môžu zobrazovať na viacerých webových stránkach, napríklad na stránkach Linka, Používateľ a Klapka. Pripojením [n] na koniec názvu prvku určíte číslo, ktoré sa zobrazuje na karte stránky.

**Príklad:** Prvok <Dial\_Plan\_1\_> reprezentuje **Dial Plan (Plán vytáčania)** pre linku 1.

- Každá otváracia značka prvku musí mať priradenú zatváraciu značku. Príklad:

```
<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>
```

- Značky prvkov rozlišujú malé a veľké písmená.
- Prázdne značky prvkov sú povolené a interpretujú sa ako prázdna konfigurácia hodnoty. Zadáte otváraciu značku prvku bez zodpovedajúcej značky prvku, medzeru a lomku a potom zatváraciu lomenú zátvorku (>). V tomto prípade je pravidlo profilu B prázdne:

```
<Profile_Rule_B />
```

- Prázdna značka elementu sa môže využiť na to, aby sa zabránilo prepísaniu hodnôt poskytnutých používateľom počas operácie opätovnej synchronizácie. V nasledovnom prípade sa nastavenia rýchlej voľby používateľa nemenia:

```
<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>
```

- Použitím prázdnej hodnoty nastavíte prázdny reťazec ako zodpovedajúci parameter. Zadáte otváraciu a zatváraciu značku prvku, medzi ktorými nebude zadaná žiadna hodnota. V nasledovnom prípade je ako hodnota parametra GPP\_A nastavený prázdny reťazec.

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

- Nerozpoznané názvy prvkov sa ignorujú.

**Príbuzné témy**

[Spravovanie prístupu ku konfigurácii](#), na strane 7

**Atribút prístupu používateľa**

Ovládanie atribútu prístupu používateľa (**ua**) sa môže použiť na zmenu prístupu používateľského konta. Ak atribút **ua** nie je určený, súčasné nastavenie prístupu používateľa sa nezmení. Tento atribút neovplyvňuje prístup konta správcu.

Ak je atribút **ua** špecifikovaný, musí mať nasledovné hodnoty:

- na – Žiadny prístup
- ro – Iba na čítanie
- rw – Čítanie a zapisovanie

Príklad atribútu **ua**:

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

Okolo hodnoty možnosti **ua** musia byť dvojité úvodzovky.

**Správa prístupu**

Ak je povolený parameter <Phone-UI-User-Mode>, grafické používateľské rozhranie telefónu pri zobrazovaní vstupy ponuky dodržiava atribút prístupu používateľa relevantných parametrov.

Pre vstupy ponuky, ktoré sú pridružené s jedným parametrom konfigurácie:

- Po nastavení parametra na atribút „ua=na“ („ua“ znamená user access – prístup používateľa) vstup zmizne.
- Po nastavení parametra na atribút „ua=ro“ bude vstup iba na čítanie a nebude sa dať upravovať.

Pre vstupy ponuky, ktoré sú pridružené s viacerými parametrami konfigurácie:

- Po nastavení všetkých relevantných parametrov na atribút „ua=na“ vstupy zmiznú.

**Príbuzné témy**

[Spravovanie prístupu ku konfigurácii](#), na strane 7

**Vlastnosti parametrov**

Na parametre sa vzťahujú tieto vlastnosti:

- Všetky parametre, ktoré nie sú určené v profile, sa v telefóne nezmenia.
- Nerozpoznané parametre sa ignorujú.
- Ak profil v otvorenom formáte obsahuje viacero výskytov rovnakej značky parametru, posledný výskyt prepíše všetky predchádzajúce. Aby sa predišlo nechcenému prepísaniu konfiguračných hodnôt parametra, odporúčame, aby každý profil určil maximálne jeden výskyt parametru.

- Posledný spracovaný profil má prednosť. Ak viacero profilov určí rovnaký parameter konfigurácie, hodnota posledného profilu má prednosť.

## Formáty reťazcov

Na formátovanie reťazcov sa vzťahujú tieto vlastnosti:

- Komentáre v štandardnej syntaxi XML sú povolené.  

```
<!-- My comment is typed here -->
```
- Medzery na začiatku a na konci sú kvôli čitateľnosti povolené, ale z hodnoty parametra sa odstraňujú.
- Nové riadky v hodnote sa menia na medzery.
- Hlavička XML vo formáte `<? ?>`, ale telefón ju bude ignorovať.
- Na zadanie špeciálnych znakov použite základné ukončovacie znaky XML uvedené v tejto tabuľke:

Špeciálny znak	Ukončovacia sekvencia XML
& (ampersand)	&
< (menšie ako)	<
> (väčšie ako)	>
' (apostrof)	'
" (dvojité úvodzovky)	"

V nasledovnom príklade sú zadané ukončovacie znaky pre symboly „väčšie ako“ a „menšie ako“, ktoré sú vyžadované v pravidle plánu vytáčania. Tento príklad definuje plán vytáčania informačnej linky, ktorý nastavuje parameter `<Dial_Plan_1_>` (**Prihlásenie správy > pokročilé > Hlas > Linka (n)**) na hodnotu (`S0<:18005551212>`).

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

- Ukončovacie znaky pre číselné znaky s použitím desiatkových alebo šestnástkových hodnôt (napr. ( a .) sú preložené.
- Firmvér telefónu podporuje iba znaky ASCII.

## Kompresia a šifrovanie otvoreného profilu (XML)

Otvorený konfiguračný profil je možné skomprimovať, aby sa znížilo zaťaženie siete na poskytujúcom serveri. Profil je tiež možné zašifrovať, aby sa ochránili dôverné informácie. Kompresia sa nevyžaduje, ale musí sa uskutočniť pred šifrovaním.

### Príbuzné témy

[Formáty konfiguračných profilov](#), na strane 13

## Skomprimovanie otvoreného profilu

Podporovaná metóda kompresie je algoritmus DEFLATE pomôcky gzip (RFC1951). Pomôcka gzip a komprimačná knižnica, ktorá tento algoritmus vykonáva (zlib) sú dostupné na internete.

Aby telefón dokázal identifikovať kompresiu, očakáva, že skomprimovaný súbor bude obsahovať hlavičku kompatibilnú s pomôckou gzip. Hlavička sa vygeneruje vyvolaním pomôcky gzip na pôvodnom otvorenom profile. Telefón skontroluje hlavičku stiahnutého súboru a určí formát súboru.

Napríklad ak je `profile.xml` platný profil, súbor `profile.xml.gz` sa prijme tiež. Každým z nasledovných príkazov sa vygeneruje tento typ profilu:

- `>gzip profile.xml`

Nahradzuje pôvodný súbor skomprimovaným súborom.

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

Pôvodný súbor nechá na jeho mieste a vygeneruje nový skomprimovaný súbor.

Návod na komprimáciu nájdete v sekcii [Skomprimovanie otvoreného profilu pomocou aplikácie Gzip](#), na strane 60.

### Príbuzné témy

[Skomprimovanie otvoreného profilu pomocou aplikácie Gzip](#), na strane 60

## Šifrovanie otvoreného profilu

Šifrovanie symetrickým kľúčom sa môže použiť na šifrovanie otvoreného konfiguračného profilu, ktorý je alebo nie je komprimovaný. Kompresia, ak sa používa, sa musí použiť ešte pred šifrovaním.

Poskytovací server na riešenie počítačného poskytovania telefónu po nasadení používa HTTPS. Predbežné šifrovanie konfiguračných profilov offline umožní následnú opätovnú synchronizáciu profilov cez protokol HTTP. Tým sa znižuje záťaž servera HTTPS pri rozsiahlych nasadeniach.

Telefón podporuje dve metódy šifrovania konfiguračných súborov:

- Šifrovanie AES-256-CBC
- Šifrovanie obsahu HTTP podľa normy RFC 8188 so šifrou AES-128-GCM

Kľúč alebo šifrovacia technika vstupu (IKM) musia byť dopredu pripravené a vložené do jednotky. Bezpečné spustenie tajného kľúča dosiahnete použitím HTTPS.

Názov konfiguračného súboru nemusí mať špecifický formát, ale názov súboru končiacu príponou `.cfg` obvykle značí názov konfiguračného profilu.

## Šifrovanie AES-256-CBC

Telefón podporuje šifrovanie AES-256-CBC pre konfiguračné súbory.



Šifrovanie môže vykonať šifrovací nástroj OpenSSL, ktorý môžete stiahnuť z rôznych internetových stránok. Podpora 256-bitového šifrovania AES môže vyžadovať rekompiláciu nástroja, aby bol povolený kód AES. Firmvér bol testovaný na verzii openssl-0.9.7c.

[Šifrovanie profilu pomocou OpenSSL, na strane 61](#) vám poskytne návod na šifrovanie.

Profil očakáva, že šifrovaný súbor bude mať rovnaký formát, ako ten vygenerovaný nasledujúcim príkazom:

```
# 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
```

Malé písmeno -k pred tajným kľúčom, ktorý môže byť akýkoľvek obyčajný text, a ktorý sa používa na generovanie 64-bitovej soli. Keď je tajný kľúč určený argumentom -k, šifrovací nástroj vytvorí náhodný 128-bitový počiatkový vektor a 256-bitový šifrovací kľúč.

Keď je tento druh šifrovania použitý na konfiguračnom profile, telefón musí poznať hodnotu tajného kľúča, aby dokázal súbor rozšifrovať. Táto hodnota je určená ako kvalifikátor v URL profilu. Syntax s použitím explicitnej URL je nasledovná:

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

Táto hodnota je naprogramovaná použitím jedného z parametrov Profile\_Rule.

### Príbuzné témy

[Šifrovanie profilu pomocou OpenSSL, na strane 61](#)

## Rozvoj makier

Viacero poskytovacích parametrov pred vyhodnotením prejde interným rozvojom makier. Tento krok pred vyhodnotením poskytuje väčšiu pružnosť pri spravovaní aktivít opätovnej synchronizácie a aktualizácie telefónu.

Nasledovné skupiny parametrov pred vyhodnotením prechádzajú rozvojom makier:

- Resync\_Trigger\_\*
- Profile\_Rule\*
- Log\_xxx\_Msg
- Upgrade\_Rule

V niektorých podmienkach môžu rozvoj makier podstupovať aj niektoré parametre pre všeobecné účely (GPP\_\*), ako je to explicitne uvedené v časti [Volitelné argumenty opätovnej synchronizácie, na strane 23](#).

Počas rozvoja makier obsah menovaných premenných nahrádza výrazy v tvare \$NAME a \$(NAME). Tieto premenné zahŕňajú parametre so všeobecným použitím, rôzne identifikátory produktu, niektoré časovače udalostí a hodnoty stavu poskytovania. Úplný zoznam nájdete v časti [Premenné rozvoja makier, na strane 72](#).

V nasledovnom príklade sa výraz \$(MAU) využíva na vloženie adresy MAC 000E08012345.

Správca zadá: `$ (MAU) config.cfg`

Výsledný rozvoj makra pre zariadenie s adresou MAC 000E08012345 je: `000E08012345config.cfg`

Ak názov makra nie je rozpoznáný, zostane nerozvinuté. Napríklad názov STRANGE sa nerozpozna ako platný názov makra, ale názov MAU sa rozpozná ako platný názov makra.

Správca zadá: `$STRANGE$MAU.cfg`

Výsledný rozvoj makra pre zariadenie s adresou MAC 000E08012345 je: `$STRANGE000E08012345.cfg`

Rozvoj makra sa neaplikuje rekurzívne. Napríklad `$$MAU` sa rozvinie na `$MAU` (`$$` sa rozvinie) a výsledkom nie je adresa MAC.

Obsah parametrov na špeciálne účely GPP\_SA až GPP\_SD je namapovaný na makro výrazy `$SA` až `$SD`. Tieto parametre podstupujú rozvoj makier iba ako argument možností `--kľúč`, `--uid` a `pwd` v URL opätovnej synchronizácie.

## Podmienené výrazy

Podmienené výrazy môžu spustiť udalosti opätovnej synchronizácie a vybrať z alternatívnych URL pre udalosti opätovnej synchronizácie a aktualizácie.

Podmienené výrazy pozostávajú zo zoznamu porovnaní oddelených operátormi `a`. Aby bola podmienka splnená, všetky porovnania sa musia splniť.

Každé porovnanie sa môže týkať jednej z týchto troch explicitných hodnôt:

- Celočíselné hodnoty
- Čísla verzii hardvéru alebo softvéru
- Reťazce s dvojitémi úvodzovkami

### Čísla verzii

Formálne vydanie verzie softvéru pre multiplatformové telefóny (MPP) používa tento formát, v ktorom BN == číslo zostavy:

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

Porovnávací reťazec musí používať rovnaký formát. V opačnom prípade sa stane chyba analýzy formátu.

Vo verzii softvéru `v1-v2-v3-v4` môžu byť určené rôzne cifry a znaky, ale musia začínať číselnou cifrou. Pri porovnávaní verzie softvéru sa `v1-v2-v3-v4` porovnávajú postupne a cifry, ktoré sú vľavo majú prednosť pred tými, ktoré sú na konci.

Ak `v[x]` zahŕňa obe cifry, cifry sa porovnávajú. Ak zahŕňa cifry aj písmená, najprv sa porovnávajú cifry a potom sa porovnávajú písmená v abecednom poradí.

### Príklad platného čísla verzie

`sipyyyy.11-0-0MPP-BN`

Naopak, `11.0.0` je neplatný formát.

## Porovnanie

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

Reťazce s úvodzovkami možno porovnávať ako rovnaké alebo rozdielne. Celé čísla a čísla verzií je tiež možné aritmeticky porovnať. Porovnávacie operátory môžu byť vyjadrené ako symboly alebo ako skratky. Skratky sú užitočné na vyjadrovanie podmienky v profile v otvorenom formáte.

Operátor	Alternatívna syntax	Popis	Aplikovateľná na operandy celé číslo a verzia	Aplikovateľná na operandy reťazec s úvodzovkami
=	eq	rovná sa	Áno	Áno
!=	ne	nerovná sa	Áno	Áno
<	lt	menšie ako	Áno	Nie
<=	le	menšie alebo rovné	Áno	Nie
>	gt	väčšie ako	Áno	Nie
>=	ge	väčšie alebo rovné	Áno	Nie
A		a	Áno	Áno

Je dôležité uviesť makro v dvojité úvodzovkách, ak sa očakáva literál reťazca. Ak sa očakáva číslo alebo číslo verzie, dvojité úvodzovky nepoužívajte.

Keď sa podmienené výrazy používajú v kontexte parametrov Profile\_Rule\* a Upgrade\_Rule, musia byť vo formáte "(expr)?", ako v tomto príklade pravidla aktualizácie. Nezabúdajte, že BN znamená číslo zostavy.

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

Uvedenú syntax so zátvorkami nepoužívajte na konfiguráciu parametrov Resync\_Trigger\_\*.

## Syntax URL

Na určenie toho, ako načítať konfiguračné súbory a načítania firmvéru v parametroch Profile\_Rule\* a Upgrade\_Rule (v tomto poradí), používajte štandardnú syntax URL. Syntax je nasledovná:

```
[ schéma:// ] [ server [:port]] cesta súboru
```

Kde **schéma** má jednu z nasledujúcich hodnôt:

- tftp
- http
- https

Ak je hodnota **schéma** vynechaná, predpokladá sa použitie tftp. Server môže byť názov hostiteľa rozpoznávaný DNS alebo číselná adresa IP. Port je číslo cieľového portu UDP alebo TCP. Cesta súboru musí začínať hlavným adresárom (/), musí to byť absolútna cesta.

Ak nie je vyplnené pole **server**, použije sa tftp server určený cez DHCP (možnosť 66).



#### Poznámka

Pre pravidlá aktualizácie musí byť server určený.

Ak nie je vyplnené pole **port**, použije sa štandardný port určenej schémy. TFTP používa port UDP 69, http používa port TCP 80, https používa port TCP 443.

Cesta súboru musí byť špecifikovaná. Nemusí odkazovať na statický súbor, ale môže indikovať dynamický obsah získaný prostredníctvom CGI.

V URL sa uskutočňuje rozvoj makier. Príklady platných URL:

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

Pri použití DHCP možnosti 66 pravidlá aktualizácie momentálne nepodporujú prázdnu syntax. Toto sa vzťahuje iba na parameter Profile\_Rule\*.

## Šifrovanie obsahu HTTP podľa normy RFC 8188

Telefón podporuje šifrovanie obsahu HTTP podľa normy RFC 8188 so šifrou AES-128-GCM pre konfiguračné súbory. Pri tejto metóde šifrovania môže hlavičky správ HTTP prečítať akýkoľvek subjekt. Obsah správy však môžu prečítať iba subjekty, ktoré poznajú šifrovaciu techniku vstupu (IKM). Keď sa telefónu poskytne IKM, telefón a poskytujúci server si môžu bezpečne vymieňať konfiguračné súbory, kým iné prvky siete môžu zároveň vykonávať analytické a monitorovacie úlohy na základe hlavičiek správ.

Konfiguračný parameter XML **IKM\_HTTP\_Encrypt\_Content** obsahuje IKM v telefóne. Z bezpečnostných dôvodov tento parameter nie je prístupný na webovej stránke správy telefónu. Nie je ani viditeľný v konfiguračnom súbore telefónu, ktorý môžete otvoriť zadaním adresy IP telefónu alebo zo správ konfigurácie telefónu, ktoré sa posielajú na poskytovací server.

Ak chcete používať šifrovanie podľa normy RFC 8188, musia byť splnené nasledujúce podmienky:

- Poskytnite IKM pre telefón nastavením IKM prostredníctvom parametra XML **IKM\_HTTP\_Encrypt\_Content** v konfiguračnom súbore, ktorý sa posiela z poskytovacieho servera do telefónu.
- Ak sa šifrujú konfiguračné súbory, ktoré sa odosielajú z poskytovacieho servera do telefónu, skontrolujte, či hlavička HTTP *Content-Encoding* konfiguračného súboru obsahuje hodnotu "aes128gcm".  
Ak táto hlavička neexistuje, uprednostní sa metóda AES-256-CBC. Ak pravidlo profilu obsahuje kľúč AES-256-CBC, telefón použije dešifrovanie AES-256-CBC, bez ohľadu na IKM.
- Ak chcete, aby telefón používal toto šifrovanie pre konfiguračné správy, ktoré odosiela na poskytovací server, uistite sa, že pravidlo správy neurčuje kľúč AES-256-CBC.

## Voliteľné argumenty opätovnej synchronizácie

Pred adresami URL zadanými v parametroch pravidla profilu sa môžu objaviť voliteľné argumenty **key**, **uid** a **pwd**, ktoré budú spolu v jednej hranatej zátvorke.

### key

Voľba **--key** informuje telefón o tom, že konfiguračný súbor prijatý z poskytovacieho servera je zašifrovaný šifrou AES-256-CBC, pokiaľ v hlavičke *Content-Encoding* súboru nie je určené šifrovanie "aes128gcm". Samotný kľúč sa zadáva ako reťazec za pojmom **--key**. Ak chcete, šifrovací kľúč môžete uzavrieť do úvodzoviek ("). Telefón použije tento kľúč na dešifrovanie konfiguračného súboru.

#### Príklady použitia:

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

Voliteľné argumenty v zátvorkách prejdú rozvojom makier. Parametre na špeciálne účely GPP\_SA až GPP\_SD sú rozvinuté na makro premenné \$SA až \$SD iba v prípade, ak sú použité ako argumenty možnosti kľúča. Príklady:

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

V profiloch s otvoreným formátom musí byť argument pre **--kľúč** rovnaký ako argument pre možnosť **-k**, ktorý sa poskytuje **openssl**.

### uid a pwd

Možnosti **uid** a **pwd** sa môžu použiť na určenie overenia pomocou ID používateľa a hesla pre konkrétne URL. Voliteľné argumenty v zátvorkách prejdú rozvojom makier. Parametre na špeciálne účely GPP\_SA až GPP\_SD sú rozvinuté na makro premenné \$SA až \$SD iba v prípade, ak sú použité ako argumenty možnosti kľúča. Príklady:

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

```
[--uid $SA -pwd $SB] https://URL_poskytovacieho_servera/cesta_ku_konfig_súboru/konfig_súbor.xml
```

sa rozvinie na:

```
[--uid MyUserID -pwdMySecretPassword]
https://URL_poskytovacieho_servera/cesta_ku_konfig_súboru/konfig_súbor.xml
```

## Aplikácia profilu na telefonické IP zariadenie

Po vytvorení konfiguračného skriptu v XML ho musíte poslať do telefónu, aby sa aplikoval. Aby sa konfigurácia aplikovala, môžete buď stiahnuť konfiguračný súbor na telefón zo servera TFTP, HTTP alebo HTTPS pomocou webového prehliadača alebo použiť pomôcku pre príkazový riadok cURL.

## Stiahnutie konfiguračného súboru na telefón zo servera TFTP

Pomocou týchto krokov stiahnete konfiguračný súbor na aplikáciu TFTP servera na vašom PC.

### Procedúra

- 
- Krok 1** Pripojte svoj PC k sieti LAN telefónu.
  - Krok 2** Spustíte aplikáciu servera TFTP na PC a uistíte sa, že konfiguračný súbor je dostupný v hlavnom adresári TFTP.
  - Krok 3** Vo webovom prehliadači zadajte adresu IP LAN telefónu, adresu IP počítača, názov súboru a prihlasovacie údaje. Použijete tento formát:

`http://<IP_adresa_WAN>/správca/resync?tftp://<IP_adresa_EC>/<názov_súboru>&užívateľ=správca&heslo=<heslo>`

Príklad:

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

---

## Stiahnutie konfiguračného súboru na telefón s použitím cURL

Ak chcete stiahnuť konfiguráciu na telefón pomocou cURL, riadte sa týmto postupom. Tento nástroj pre príkazový riadok sa používa na prenos údajov so syntaxou URL. Nástroj cURL môžete stiahnuť na adrese:

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



### Poznámka

Odporúčame, aby ste nástroj cURL nepoužívali na odosielanie konfigurácie na telefón, pretože počas používania cURL by mohlo byť zachytené meno používateľa a heslo.

---

### Procedúra

- 
- Krok 1** Pripojte svoj PC k portu LAN na telefóne.
  - Krok 2** Stiahnite konfiguračný súbor na telefón zadaním nasledovného príkazu cURL:

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

---

## Parametre poskytovania

Táto sekcia opisuje parametre poskytovania všeobecne zoskupené podľa funkcií:

Existujú tieto typy parametrov poskytovania:

- Na všeobecné účely

- Povoľovacie
- Spúšťače
- Konfigurovateľné plány
- Pravidlá profilu
- Pravidlo aktualizácie

## Parametre na všeobecné účely

Parametre na všeobecné účely GPP\_\* (**Prihlásenie správy** > **pokročilé** > **Hlas** > **Poskytovanie**) sa používajú ako register voľných reťazcov pri konfigurácii telefónu pre interakciu s konkrétnym riešením poskytovacieho servera. Parametre GPP\_\* sú predvolene prázdne. Môžu byť nakonfigurované, aby obsahovali rôzne hodnoty, napríklad:

- Šifrovacie kľúče
- Adresy URL
- Informácie o stave viacstupňového poskytovania
- Šablóny požiadavky post
- Mapy aliasov názvov parametrov
- Čiastočné hodnoty reťazcov, ktoré sa nakoniec spoja a vytvoria kompletne hodnoty parametrov.

Parametre GPP\_\* môžu prejsť rozvojom makier v rámci iných parametrov poskytovania. Na tento účel postačujú na zistenie obsahu parametrov GPP\_A až GPP\_P názvy makier s jedným veľkým písmenom (A až P). Názvy makier s dvomi veľkými písmenami (SA až AD) identifikujú parametre GPP\_SA až GPP\_SD ako špeciálny prípad, ak sú použité ako argument v nasledovných možnostiach URL.

### klíč, UID a PWD

Tieto parametre môžu byť použité ako premenné v pravidlách poskytovania a aktualizácie. Odkazuje sa na ne uvedením znaku „\$” pred názvom premennej, napríklad \$GPP\_A.

## Použitie parametrov na všeobecné účely

Napríklad parameter GPP\_A obsahuje reťazec ABC a parameter GPP\_B obsahuje reťazec 123, takže výraz makra \$A\$B sa rozvinie na ABC123.

### Skôr ako začnete

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).

### Procedúra

- 
- Krok 1** Vyberte možnosť **Hlas** > **Poskytovanie**.
  - Krok 2** Posuňte sa na sekciu **Parametre na všeobecné účely**.
  - Krok 3** Zadajte platné hodnoty do polí GPP A až GPP P.

**Krok 4** Kliknite na možnosť **Odoslať všetky zmeny**.

---

## Povoľovacie

Parametre Provision\_Enable a Upgrade\_Enable spravujú všetky operácie opätovnej synchronizácie profilu a aktualizácie firmvéru. Tieto parametre spravujú opätovnú synchronizáciu a aktualizáciu nezávisle od seba. Tiež spravujú príkazy URL pre opätovnú synchronizáciu a aktualizáciu zaslané administračným webovým serverom. Oba tieto parametre sú predvolene nastavené na možnosť **Áno**.

Parameter Resync\_From\_SIP spravuje žiadosti pre operácie opätovnej synchronizácie. Udalosť SIP NOTIFY je poslaná zo servera proxy poskytovateľa služby na telefón. Ak to je povolené, proxy môže požiadať o opätovnú synchronizáciu. Aby to uskutočnil, proxy pošle zariadeniu správu SIP NOTIFY, ktorá obsahuje hlavičku Event: resync.

Zariadenie na overenie použije odpoveď 401 (overenie pre použité prihlasovacie údaje odmietnuté). Zariadenie následne očakáva overenú žiadosť a potom schváli žiadosť o opätovnú synchronizáciu z proxy. Hlavička Event: reboot\_now spúšťa studený reštart a hlavička Event: restart\_now spúšťa teplý reštart, obe sú taktiež overené.

Posledné dva povoľovacie parametre sú Resync\_On\_Reset a Resync\_After\_Upgrade\_Attempt. Tieto parametre určujú, či zariadenie uskutoční operáciu opätovnej synchronizácie po spustení systému a po každom pokuse o aktualizáciu.

Keď je možnosť Resync\_On\_Reset povolená, zariadenie pridá po spustení zariadenia náhodné oneskorenie pred tým, ako sa uskutoční reset. Oneskorenie je náhodný počet sekúnd, najdlhšie trvanie určuje parameter Resync\_Random\_Delay (v sekundách). V skupine telefónov, ktoré sa zapínajú naraz, toto oneskorenie rovnomerne rozloží počiatkový čas žiadostí všetkých jednotiek o opätovnú synchronizáciu. Táto funkcia môže byť užitočná vo veľkom obytnom nasadení v prípade výpadku energie v regióne.

## Spúšťáče

Telefón vám umožňuje uskutočniť opätovnú synchronizáciu v určených intervaloch alebo v konkrétnom čase.

### Opätovná synchronizácia v určených intervaloch

Telefón je navrhnutý tak, aby sa v pravidelných intervaloch opätovne synchronizoval s poskytovacím serverom. Interval opätovnej synchronizácie je nakonfigurovaný v parametri Resync\_Periodic (sekundy). Ak je táto hodnota prázdna, zariadenie sa nebude pravidelne opätovne synchronizovať.

Opätovná synchronizácia zvyčajne prebieha, keď sú hlasové linky nečinné. Ak sa vyžaduje opätovná synchronizácia, keď je hlasová linka aktívna, telefón odloží proces opätovnej synchronizácie na dobu, keď bude linka znovu nečinná. Opätovná synchronizácia môže spôsobiť zmenu hodnôt parametra konfigurácie.

Operácia opätovnej synchronizácie môže zlyhať, ak telefón nie je schopný načítať profil zo servera, stiahnutý súbor je poškodený alebo ak nastala interná chyba. Zariadenie sa po čase určenom v parametri Resync\_Error\_Retry\_Delay (v sekundách) znova pokúsi o opätovnú synchronizáciu. Ak je parameter Resync\_Error\_Retry\_Delay nastavený na 0, zariadenie sa po prvom neúspešnom pokuse o opätovnú synchronizáciu nebude pokúšať znova.



Ak aktualizácia zlyhá, po dobe špecifikovanej v parametri `Upgrade_Error_Retry_Delay` v sekundách sa pokus uskutočni znovu.

Na podmienené spustenie opätovnej synchronizácie sú dostupné dva konfigurovateľné parametre: `Resync_Trigger_1` a `Resync_Trigger_2`. Každý parameter môže byť naprogramovaný pomocou podmieneného výrazu, ktorý prejde rozvojom makier. Po uplynutí intervalu na opätovnú synchronizáciu (času pre ďalšiu opätovnú synchronizáciu) spúšťače, ak sú nastavené, zabránia opätovnej synchronizácii, pokiaľ aspoň jeden spúšťač nebude vyhodnotený ako pravdivý.

Nasledovný príklad podmienky spustí opätovnú synchronizáciu. V tomto príklade prebehol posledný pokus o aktualizáciu telefónu pred viac ako 5 minútami (300 sekúnd) a posledný pokus o opätovnú synchronizáciu prebehol pred viac ako 10 minútami (600 sekúnd).

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

## Opätovná synchronizácia v určenom čase

Parameter `Resync_At` umožňuje telefónu opätovne sa synchronizovať v presne určenom čase. Tento parameter na špecifikovanie času používa 24-hodinový formát (hhmm).

Parameter `Resync_At_Random_Delay` umožňuje telefónu opätovne sa synchronizovať v po neurčenej dobe oneskorenia. Tento parameter na špecifikovanie času používa kladné celé číslo.

Je potrebné vyhnúť sa preťaženiu servera veľkým množstvom žiadostí o opätovnú synchronizáciu od telefónov ktoré sú nastavené tak, aby sa synchronizovali naraz. Aby sa tomu zabránilo, telefón spustí opätovnú synchronizáciu s oneskorením do 10 minút po určenom čase.

Napríklad, ak nastavíte čas opätovnej synchronizácie na 1000 (10:00), telefón spustí opätovnú synchronizáciu kedykoľvek medzi 10:00 a 10:10.

Táto možnosť je predvolene deaktivovaná. Ak je poskytovaný parameter `Resync_At`, parameter `Resync_Periodic` sa ignoruje.

## Konfigurovateľné plány

Pomocou týchto poskytovacích parametrov môžete konfigurovať plány pravidelných opätovných synchronizácií a určiť, aké dlhé majú byť intervaly medzi pokusmi o opätovnú synchronizáciu a zlyhanie aktualizácií:

- `Resync_Periodic`
- `Resync_Error_Retry_Delay`
- `Upgrade_Error_Retry_Delay`

Každý parameter akceptuje jedinú hodnotu oneskorenia (v sekundách). Nová rozšírená syntax umožňuje používanie čiarkami oddeleného zoznamu za sebou nasledujúcich elementov oneskorenia. Posledný element v tomto zozname sa implicitne opakuje donekonečna.

Voliteľne môžete použiť znamienko plus na určenie ďalšej číselnej hodnoty, ktoré náhodne pridáva ďalšie oneskorenie.

### Príklad 1

V tomto príklade sa telefón pravidelne opätovne synchronizuje každé 2 hodiny. Ak sa opätovná synchronizácia zlyhá, zariadenie sa o ňu pokúsi znova v týchto intervaloch: 30 minút, 1 hodina, 2 hodiny, 4 hodiny. Zariadenie pokračuje v pokuse o opätovnú synchronizáciu každé 4 hodiny, až kým neprebehne správne.

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

### Príklad 2

V tomto príklade sa zariadenie opätovne synchronizuje každú hodinu (plus pridané náhodné oneskorenie do 10 minút). V prípade zlyhania opätovnej synchronizácie sa o ňu zariadenie pokúsi znova v týchto intervaloch: 30 minút (plus až 5 minút), 1 hodiny (plus až do 10 minút), 2 hodiny (plus až do 15 minút). Zariadenie pokračuje v pokuse o opätovnú synchronizáciu každé 2 hodiny (plus až 15 minút), až kým neprebehne správne.

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

### Príklad 3

V tomto príklade sa zariadenie v prípade zlyhania vzdialenej aktualizácie pokúsi o ďalšiu aktualizáciu o 30 minút, potom o hodinu, potom o dve hodiny. Ak aktualizácia naďalej zlyhá, zariadenie sa o ňu pokúša každých 4 – 5 hodín, až kým neprebehne úspešne.

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

## Pravidlá profilu

Telefón poskytuje viacero konfigurovateľných vzdialených parametrov profilu (Profile\_Rule\*). Preto každá operácia opätovnej synchronizácie môže načítať viaceré súbory, ktoré môžu byť riadené rôznymi servermi.

V najjednoduchšom prípade sa zariadenie pravidelne opätovne synchronizuje s jedným profilom na centrálnom serveri, ktorý aktualizuje všetky relevantné vnútorné parametre. Je tiež možné profil rozdeliť medzi viacero súborov. Jeden súbor je spoločný pre všetky telefóny v jednom nasadení. Pre každý účet je poskytnutý individuálny, jedinečný súbor. Šifrovacie kľúče a informácie o certifikáte môžu byť dodávané ďalším profilom uloženom na individuálnom serveri.

Telefón vždy, keď sa vyžaduje opätovná synchronizácia, vyhodnotí všetky štyri parametre Profile\_Rule\* v poradí:

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

Každé vyhodnotenie môže vyvolať načítanie profilu zo vzdialeného poskytovacieho servera a prípadne aj aktualizáciu niektorých vnútorných parametrov. Ak vyhodnotenie zlyhá, sekvencia opätovnej synchronizácie

sa preruší a od začiatku prebehne nový pokus určený parametrom `Resync_Error_Retry_Delay` (v sekundách). Ak sú všetky vyhodnotenia úspešné, zariadenie počká dobu určenú parametrom `Resync_Periodic` a potom znova uskutoční opätovnú synchronizáciu.

Obsah každého parametra `Profile_Rule*` pozostáva zo skupiny alternatív. Alternatívy sú oddelené znakom zvislej čiary (`()`). Každá alternatíva obsahuje podmienený výraz, priradovací výraz, URL profilu a prípadne pridružených možností URL. Všetky tieto súčasti sú v rámci každej alternatívy voliteľné. Nasledujú príklady platných kombinácií a poradia, v ktorom sa musia uvádzať:

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

V každom parametre `Profile_Rule*` musia všetky alternatívy okrem poslednej poskytovať podmienený výraz. Tento výraz sa vyhodnotí a spracuje nasledovne:

1. Podmienky sa vyhodnocujú zľava doprava, až kým sa jedna nevyhodnotí ako pravdivá (alebo kým sa nenájde alternatíva bez podmieneného výrazu).
2. Ak je uvedený sprievodný priradovací výraz, je tiež vyhodnotený.
3. Ak je URL určená ako súčasť tejto alternatívy, vykoná sa pokus o stiahnutie profilu umiestneného na špecifikovanej URL. Systém s pokúsi o zodpovedajúcu aktualizáciu vnútorných parametrov.

Ak všetky alternatívy obsahujú podmienené výrazy a žiaden z nich sa nevyhodnotí ako pravdivý (alebo ak je celé pravidlo profilu prázdne), celý parameter `Profile_Rule*` sa preskočí. Vyhodnotí sa ďalší parameter pravidla profilu v poradí.

### Príklad 1

V tomto príklade prebieha opätovná synchronizácia bez podmienky s profilom na určenej URL a uskutoční sa požiadavka HTTP GET na vzdialený poskytovací server.

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

### Príklad 2

V tomto príklade sa zariadenie opätovne synchronizuje s dvomi rôznymi URL podľa stavu registrácie Linky 1. V prípade stratenej registrácie zariadenie uskutoční HTTP POST na CGI skript. Zariadenie odošle obsah parametra `GPP_A` po rozvoji makier, ktorý môže poskytnúť ďalšie informácie o stave zariadenia:

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

### Príklad 3

V tomto príklade sa zariadenie opätovne synchronizuje s rovnakým serverom. Zariadenie poskytuje ďalšie informácie, ak v jednotke nie je nainštalovaný certifikát (pre staršie jednotky pred verziou 2.0)

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

**Príklad 4**

V tomto príklade je Linka 1 zakázaná, až kým sa GPP\_A nenastaví na hodnotu Poskytnutý prostredníctvom prvého URL. Potom prebehne synchronizácia s druhou URL:

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

**Príklad 5**

V tomto príklade sa očakáva, že profil vrátený serverom obsahuje značky prvkov XML. Tieto značky sa musia premapovať na správne názvy parametrov pomocou mapy aliasov uloženej v GPP\_B:

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

Opätovná synchronizácia sa typicky považuje za neúspešnú, ak požadovaný profil nebol prijatý zo servera. Parameter Resync\_Fails\_On\_FNF môže toto predvolené správanie prepísať. Ak je parameter Resync\_Fails\_On\_FNF nastavený na Nie, zariadenie prijme odpoveď servera file-not-found (súbor nebol nájdený) ako úspešnú opätovnú synchronizáciu. Predvolená hodnota pre Resync\_Fails\_On\_FNF je Áno.

## Pravidlo aktualizácie

Pravidlo aktualizácie prikazuje zariadeniu aktivovať nové načítanie a v prípade potreby aj určuje, kde ho získať. Ak je načítanie už v zariadení stiahnuté, nebude sa o stiahnutie snažiť znova. Preto platnosť umiestnenia načítania nie je dôležitá, ak je želané načítanie už v neaktívnej oblasti.

Upgrade\_Rule určuje načítanie firmvéru, ktoré, ak sa líši od súčasného načítania, bude stiahnuté a aplikované, pokiaľ podmienený výraz alebo Upgrade\_Enable nie je nastavený na **Nie**.

Telefón poskytuje jeden konfigurovateľný parameter vzdialenej aktualizácie: Upgrade\_Rule. Tento parameter akceptuje syntax podobnú parametrom pravidiel profilu. Možnosti URL nie sú pre aktualizácie podporované, môžete však použiť podmienené a priraďovacie výrazy. Ak sa použijú podmienené výrazy parameter sa môže zaplniť viacerými alternatívami oddelenými znakom |. Syntax každej alternatívy je nasledovná:

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

Rovnako, ako parametre Profile\_Rule\*, aj parameter Upgrade\_Rule vyhodnocuje každú alternatívu, až kým sa nespĺní podmienka podmieneného výrazu alebo alternatíva nemá žiadny podmienený výraz. Ak je určený sprievodný priraďovací výraz, je tiež vyhodnotený. Potom sa uskutoční pokus o aktualizáciu z určenej URL.

Ak parameter Upgrade\_Rule obsahuje URL bez podmieneného výrazu, zariadenie sa aktualizuje na obraz firmvéru, ktorý určí URL. Po rozvoji makier a vyhodnotení pravidla sa zariadenie nepokúsi o opätovnú synchronizáciu, až kým sa pravidlo neupraví alebo kým sa nezmení efektívna kombinácia schéma + server + port + cesta súboru.

Pri pokuse o aktualizáciu firmvéru zariadenie na začiatku procesu vypne audio a na konci sa rešartuje. Zariadenie automaticky spustí aktualizáciu, ktorá sa riadi obsahom parametra Upgrade\_Rule, iba v prípade, ak sú všetky hlasové linky momentálne neaktívne.

Napríklad

- Pre telefóny Cisco IP radu 6800:

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

V tomto príklade parameter Upgrade\_Rule aktualizuje firmvér na obraz, ktorý je uložený na určenom URL.

Ďalší príklad pre telefón Cisco IP Phone radu 6800:

```
("$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
```

Tento príklad prikáže jednotke načítať jeden alebo dva obrazy na základe obsahu parametru pre všeobecné účely GPP\_F.

Zariadenie môže vynútiť limit zníženia čísla verzie firmvéru, čo môže byť užitočná možnosť prispôsobenia. Ak je v parametri Downgrade\_Rev\_Limit nakonfigurované platné číslo verzie firmvéru, zariadenie odmietne pokusy o aktualizáciu na firmvérové verzie, ktoré sú staršie, ako určený limit.

## Typy údajov

S parametrami konfiguračného profilu sa používajú tieto typy údajov:

- {a,b,c,...} – Výber z a, b, c,...
- Bool – Hodnota Boolean, „áno“ alebo „nie“.
- CadScript – Miniskript, ktorý určuje parametre kadencie signálu. Až do 127 znakov.

Syntax: S<sub>1</sub>[;S<sub>2</sub>], kde:

- S<sub>i</sub>=D<sub>i</sub>(zap<sub>·i,1</sub>/off<sub>·i,1</sub>[,zap<sub>·i,2</sub>/vyp<sub>·i,2</sub>[,zap<sub>·i,3</sub>/vyp<sub>·i,3</sub>[,zap<sub>·i,4</sub>/vyp<sub>·i,4</sub>[,zap<sub>·i,5</sub>/vyp<sub>·i,5</sub>[,zap<sub>·i,6</sub>/vyp<sub>·i,6</sub>]]]])) a je známy ako sekcia.
- zap<sub>·i,j</sub> a vyp<sub>·i,j</sub> sú sekundy trvania zapnutia a vypnutia *segmentu*. i = 1 alebo 2 a j = 1 až 6.
- D<sub>i</sub> je celkové trvanie sekcie v sekundách.

Všetky trvania môžu mať až tri desatinné miesta, aby poskytli rozlíšenie na 1 ms. Zástupný znak „\*“ znamená nekonečné trvanie. Segmenty v sekcii sa prehrávajú v poradí a opakujú sa, až kým sa neprehrá celé trvanie.

Príklad 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
```

Príklad 2 – Odlíšujúce zvonenie (krátke, krátke, krátke, dlhé):

```
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 – Skriptovacia syntax používaná na určenie plánov vytáčania linky 1 a 2.
- Float<n> – Pohyblivá hodnota bodu, ktorá môže mať až n desatinných čísel.
- FQDN – Úplný názov domény. Môže obsahovať až 63 znakov. Príklady:
  - sip.Cisco.com:5060 alebo 109.12.14.12:12345
  - sip.Cisco.com alebo 109.12.14.12
- FreqScript – Miniskript, ktorý určuje parametre frekvencie a úrovňové parametre tónu. Môže obsahovať až 127 znakov.

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

- $F_1$ – $F_6$  sú frekvencie v Hz (iba celé čísla bez znamienok).
- $L_1$ – $L_6$  sú zodpovedajúce úrovne v dBm (najviac jedno desatinné miesto).

Prázdne znaky pred a po čiarky sú povolené, ale neodporúčajú sa.

Príklad 1 – Tón čakajúceho hovoru:

```
440@-10

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

Príklad 2 – Oznamovací tón:

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

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

- IP – Platná adresa IPv4 v tvare x.x.x.x, kde x je číslo medzi 0 a 255. Príklad: 10.1.2.100.
- UserID – ID používateľa, ako je uvedené v URL, najviac 63 znakov.
- Telefón – Reťazec telefónneho čísla, napríklad 14081234567, \*69, \*72, 345678, alebo všeobecná URL, napríklad 1234@10.10.10.100:5068 alebo jsmith@Cisco.com. Reťazec môže obsahovať až 39 znakov.
- PhTmpl – Šablóna telefónneho čísla. Každá šablóna môže obsahovať jeden alebo viacero vzorov oddelených čiarkami (.). Prázdne znaky na začiatku každého vzoru sa ignorujú. „?“ a „\*“ sú zástupné

znaky. Na doslovné zastúpenie použite %xx. Napríklad %2a zastupuje znak \*. Šablóna môže obsahovať až 39 znakov. Príklady: "1408\*", "1510\*", "1408123????", "555?1".

- Port – Číslo portu TCP/UDP (0 – 65535). Môže byť určené v desiatkovom alebo šestnástkovom formáte.
- ProvisioningRuleSyntax – Skriptovacia syntax použitá pre definovanie pravidiel opätovnej synchronizácie konfigurácie alebo aktualizácie firmvéru.
- PwrLevel – Úroveň intenzity vyjadrená v dBm s jedným desatinným miestom, napríklad -13,5 alebo 1,5 (dBm).
- RscTmpl – Šablóna kódu stavu odpovede SIP, napríklad „404, 5\*“, „61?“, "407, 408, 487, 481". Môže obsahovať až 39 znakov.
- Sig<n> – N-bitová hodnota so znamienkom. Môže byť určené v desiatkovom alebo šestnástkovom formáte. Pred zápornými hodnotami musí byť znamienko „-“. Znamienko „+“ pred kladnými hodnotami je voliteľné.
- Kódy s hviezdičkou – Aktivačný kód dodatkového služby, napríklad \*69. Kód môže obsahovať až 7 znakov.
- Str<n> – Všeobecný reťazec, môže mať až n nerezervovaných znakov.
- Time <n> – Trvanie v sekundách, môže mať až n desatinných miest. Ďalšie určené desatinné miesta sa ignorujú.
- ToneScript – Miniskript, ktorý určuje parametre frekvencie, úrovne a kadencie tónu prebiehajúceho hovoru. Skript môže obsahovať až 127 znakov.

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

Sekcia Z<sub>1</sub> je podobná sekcii S<sub>1</sub> v CadScript s rozdielom, že za každým segmentom zap./vyp. nasleduje parameter komponentov frekvencie: Z<sub>1</sub> = D<sub>1</sub>(zap.<sub>i,1</sub>/vyp.<sub>i,1</sub>/f<sub>i,1</sub>[,zap.<sub>i,2</sub>/vyp.<sub>i,2</sub>/f<sub>i,2</sub> [,zap.<sub>i,3</sub>/vyp.<sub>i,3</sub>/f<sub>i,3</sub> [,zap.<sub>i,4</sub>/vyp.<sub>i,4</sub>/f<sub>i,4</sub> [,zap.<sub>i,5</sub>/vyp.<sub>i,5</sub>/f<sub>i,5</sub> [,zap.<sub>i,6</sub>/vyp.<sub>i,6</sub>/f<sub>i,6</sub>]]]]]) kde:

- $f_{i,j} = n_1[+n_2][+n_3][+n_4][+n_5][+n_6]$
- $1 < n_k < 6$  určuje komponenty frekvencie v skripte FreqScript, ktoré sa v konkrétnom segmente používajú.

Ak je v segmente použitý viac, ako jeden komponent frekvencie, komponenty sa sčítajú.

Príklad 1 – Oznamovací tón:

```
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
```

Príklad 2 – Prerušovaný tón:

```
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-bitová hodnota bez znamienka, kde  $n = 8, 16$  alebo  $32$ . Môže byť určená v desiatkovom alebo šestnástkovom formáte, napríklad  $12$  alebo  $0x18$ , ale musí sa zmestiť do  $n$  bitov.



#### Poznámka Majte na pamäti, že:

- `<Par Name>` je názov parametra konfigurácie. V profile sa zodpovedajúca značka vytvorí nahradením medzery za podčiarknutie „\_“, napríklad **Par\_Name**.
- Prázdne pole predvolenej hodnoty znamená prázdny reťazec `<"">`.
- Telefón pokračuje v používaní naposledy nakonfigurovaných hodnôt značiek, ktoré sa v aktuálnom profile nenachádzajú.
- Šablóny sa porovnávajú v danom poradí. Vyberie sa prvá, *nie najbližšia* zhoda. Názov parametra sa musí presne zhodovať.
- Ak je v profile určená viac, ako jedna definícia parametra, v telefóne sa využije posledná definícia v súbore.
- Určenie parametra prázdnu hodnotou parametra zmení parameter späť na predvolenú hodnotu. Ak chcete namiesto toho určiť prázdny reťazec, použite ako hodnotu parametra prázdny reťazec `""`.

## Aktualizácie profilu a firmvéru

Telefón podporuje bezpečné vzdialené poskytovanie (konfiguráciu) a aktualizácie firmvéru. Nezapojený telefón môže prijať zašifrovaný profil, ktorý je určený pre konkrétne zariadenie. Telefón nevyžaduje explicitný kľúč, pretože mechanizmus bezpečného prvého nastavenia využíva funkciu SSL.

Na spustenie alebo dokončenie aktualizácie profilu alebo firmvéru, ani v prípade, ak sa vyžaduje čiastočná aktualizácia kvôli plánovaným stavom aktualizácií zo staršieho vydania, nie je potrebný zásah používateľa. Opätovná synchronizácia profilu sa spustí len ak je telefón nečinný, pretože môže spôsobiť reštart a odpojiť hovor.

Parametre na všeobecné účely spravujú proces poskytovania. Každý telefón môže byť nakonfigurovaný tak, aby pravidelne kontaktoval normálny poskytovací server (NPS). Komunikácia s NPS nevyžaduje používanie zabezpečeného protokolu, pretože aktualizovaný profil je zašifrovaný zdieľaným tajným kľúčom. NPS môže byť bežný server TFTP, HTTP alebo HTTPS s certifikátom klienta.

Správca môže aktualizovať, rebootovať, reštartovať alebo opätovne synchronizovať telefóny pomocou používateľského webového rozhrania telefónu. Správca môže tieto úlohy vykonať aj prostredníctvom správy SIP NOTIFY.



Konfiguračné profily sa generujú pomocou bežných nástrojov s otvoreným kódom, ktoré sa dajú integrovať s poskytovacími systémami poskytovateľov služieb.

#### Príbuzné témy

[Povolenie a konfigurácia aktualizácií profilu](#), na strane 35

## Povolenie a konfigurácia aktualizácií profilu

Aktualizácie profilu môžu byť povolené v určených intervaloch. Aktualizované profily sa posielajú zo serveru na telefón prostredníctvom TFTP, HTTP alebo HTTPS.

#### Skôr ako začnete

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu](#), na strane 7.

#### Procedúra

- 
- Krok 1** Vyberte možnosť **Hlas > Poskytovanie**.
  - Krok 2** V sekcii **Konfiguračný profil** vyberte možnosť **Áno** z rozbaľovacieho zoznamu **Povoliť poskytovanie**.
  - Krok 3** Zadajte parametre.
  - Krok 4** Kliknite na možnosť **Odoslať všetky zmeny**.

#### Príbuzné témy

[Aktualizácie profilu a firmvéru](#), na strane 34

## Povolenie a konfigurácia aktualizácií firmvéru

Aktualizácie firmvéru môžu byť povolené v určených intervaloch. Aktualizovaný firmvér sa odosiela zo serveru na telefón prostredníctvom TFTP alebo HTTP. Zabezpečenie nemá pri aktualizácii firmvéru veľkú dôležitosť, pretože firmvér neobsahuje žiadne osobné informácie.

#### Skôr ako začnete

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu](#), na strane 7.

#### Procedúra

- 
- Krok 1** Vyberte možnosť **Hlas > Poskytovanie**.
  - Krok 2** V sekcii **Aktualizácia firmvéru** vyberte možnosť **Áno** z rozbaľovacieho zoznamu **Povoliť aktualizáciu**.
  - Krok 3** Zadajte parametre.
  - Krok 4** Kliknite na možnosť **Odoslať všetky zmeny**.
-

## Aktualizácia firmvéru cez TFTP, HTTP alebo HTTPS

Telefón podporuje aktualizáciu pomocou jedného obrazu cez TFTP, HTTP alebo HTTPS.



### Poznámka

Zníženie na nižšie vydanie nemusí byť dostupné pre všetky zariadenia. Viac informácií nájdete v poznámkach k vydaniu pre váš telefón a firmvérovú verziu.

### Skôr ako začnete

Súbor načítania firmvéru sa musí stiahnuť na dostupný server.

### Procedúra

#### Krok 1

Obraz premenujte nasledovným spôsobom:

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

kde:

`x8xx` je séria telefónu, napríklad 6841.

`aa-b-c` je číslo vydania, napríklad 10-4-1

#### Krok 2

Pomocou príkazu `tar -xzvf` rozbaľte súbor typu `.tar`.

#### Krok 3

Skopírujte priečinok do sťahovacieho adresára TFTP, HTTP alebo HTTPS.

#### Krok 4

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).

#### Krok 5

Vyberte možnosť **Hlas > Poskytovanie**.

#### Krok 6

Nájdite názov načítacieho súboru, ktorý končí príponou `.loads` a pripojte ho k platnému URL.

#### Krok 7

Kliknite na možnosť **Odoslať všetky zmeny**.

## Aktualizácia firmvéru cez príkaz v prehliadači

Na aktualizáciu firmvéru telefónu môžete zadať príkaz na aktualizáciu zadaný do riadku adresy v prehliadači. Telefón sa aktualizuje iba vtedy, keď je nečinný. Pokus o aktualizáciu sa automaticky spustí po dokončení hovoru.

### Procedúra

Ak chcete aktualizovať telefón pomocou URL vo webovom prehliadači, zadajte tento príkaz:

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



## KAPITOLA 3

# Interná príprava na poskytovanie a poskytovacie servery

---

- [Interná príprava na poskytovanie a poskytovacie servery, na strane 37](#)
- [Príprava servera a softvérové nástroje, na strane 37](#)
- [Interná príprava zariadení na poskytovanie, na strane 39](#)
- [Nastavenie poskytovacieho servera, na strane 40](#)

## Interná príprava na poskytovanie a poskytovacie servery

Poskytovateľ služby pripraví telefóny, okrem jednotiek RC, na poskytovanie tak, že im nastaví profil. Profil prípravy na poskytovanie môže obsahovať limitovanú skupinu parametrov, ktorá opätovne synchronizuje telefón. Profil tiež môže obsahovať všetky parametre, ktoré odosiela vzdialený server. Predvolené nastavenie je, že telefón sa opätovne synchronizuje pri spustení a v intervaloch, ktoré sú nastavené v profile. Keď používateľ pripojí telefón u používateľa, zariadenie stiahne aktualizovaný profil a všetky aktualizácie firmvéru.

Tento proces prípravy na poskytovanie, nasadenia a vzdialené poskytovanie môže byť dosiahnutý rôznymi spôsobmi.

## Príprava servera a softvérové nástroje

Príklady v tejto kapitole vyžadujú, aby bol dostupný jeden alebo viac serverov. Tieto servery môžu byť nainštalované na miestnom PC a bežať na ňom:

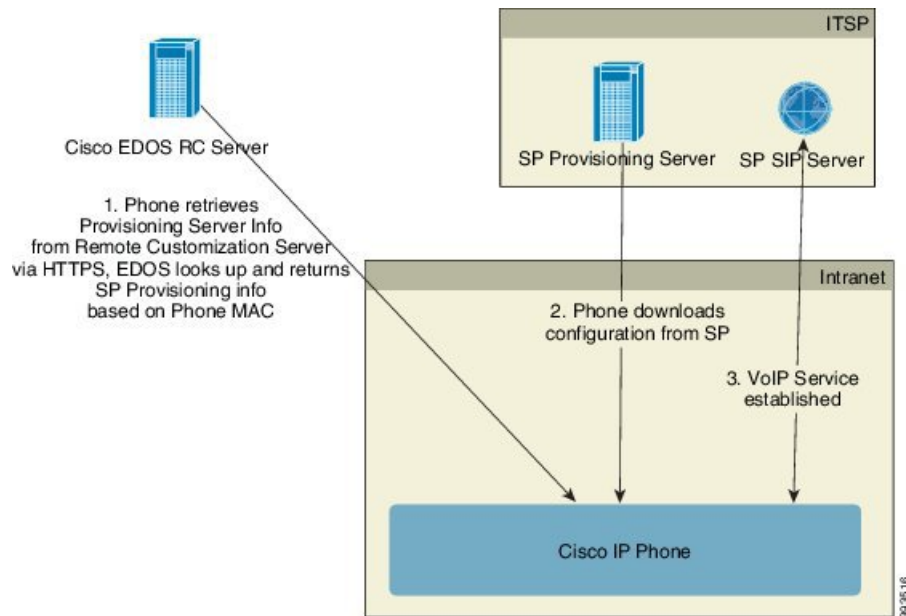
- TFTP (port UDP 69),
- systémový denník (port UDP 514),
- HTTP (port TCP 80),
- HTTPS (port TCP 443).

Ak chcete riešiť problémy s konfiguráciou servera, je užitočné inštalovať klientov pre každý typ servera na samostatný server. Vďaka tomu vytvoríte správne fungovanie serverov, ktoré bude nezávislé na interakcii s telefónmi.

Odporúčame si tiež nainštalovať nasledovné softvérové nástroje:

- Na generovanie konfiguračných profilov si nainštalujte kompresnú pomôcku gzip s otvoreným zdrojovým kódom.
- Na šifrovanie profilov a operácií HTTPS si nainštalujte softvérový balík OpenSSL s otvoreným zdrojovým kódom.
- Na testovanie dynamického generovania profilov a vzdialeného poskytovania v jednom kroku s použitím HTTPS odporúčame skriptovací jazyk s podporou skriptov CGI. Príkladom takéhoto skriptovacieho jazyka sú nástroje jazyka Perl s otvoreným zdrojovým kódom.
- Na kontrolu výmen medzi poskytujúcimi servermi a telefónmi nainštalujte inšpektor ethernetových paketov (napríklad voľne stiahnuteľné programy Ethereal/Wireshark). Zachyťte stopu ethernetového paketu interakcie medzi telefónom a poskytujúcim serverom. Podarí sa vám to vďaka inšpektorovi paketov na PC, ktorý je pripojený k prepínaču, na ktorom je povolené zrkadlenie portov. Pre transakcie HTTPS môžete využiť pomôcku ssldump.

## Distribúcia Vzdialeného prispôsobenia (Remote Customization – RC)



Všetky telefóny kontaktujú server EDOS RC spoločnosti Cisco, kým nie sú prvýkrát nastavené.

V distribučnom modeli RC zákazník zakúpi telefón, ktorý už bol pridružený k určenému poskytovateľovi služby na serveri EDOS RC spoločnosti Cisco. Poskytovateľ internetových telefonických služieb (ITSP) nastaví a udržiava poskytovací server a registruje informácie o svojom poskytovacom serveri na serveri EDOS RC spoločnosti Cisco.

Keď je telefón zapnutý a pripojený k internetu, stav prispôsobenia nenastaveného telefónu je **Otvorený**. Telefón najprv kontaktuje miestny server DHCP a získa informácie o poskytovacom serveri a potom nastaví stav prispôsobenia telefónu. Ak je požiadavka na DHCP úspešná, stav prispôsobenia sa zmení na **Prerušené** a neprebehne pokus o RC, pretože DHCP už poskytol potrebné informácie o poskytovacom serveri.

Keď sa telefón pripojí k sieti po prvý raz alebo po obnovení výrobných nastavení a nie sú nastavené žiadne možnosti servera DHCP, telefón kontaktuje server na aktiváciu zariadenia. Týmto možno dosiahnuť plne

automatizované nastavenie. Nové telefóny použijú na nastavenie adresu “activate.cisco.com”, nie “webapps.cisco.com”. Telefóny s firmvérom starším ako 11.2(1) budú naďalej používať adresu webapps.cisco.com. Spoločnosť Cisco odporúča, aby ste povolili obe tieto názvy domén cez bránu firewall.

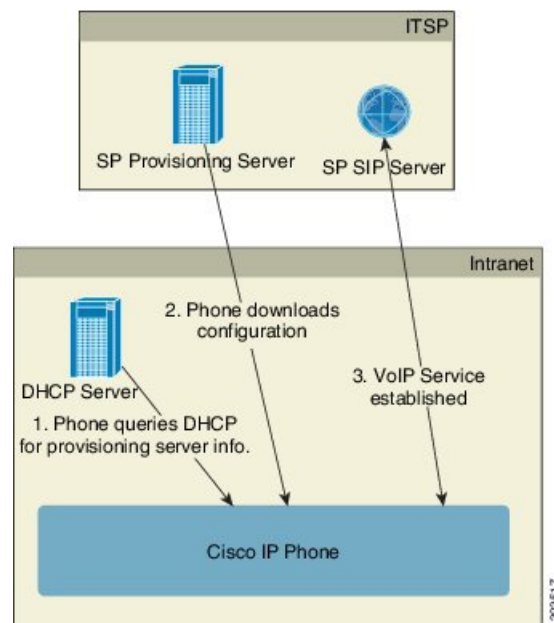
Ak server DHCP neposkytne informácie o poskytovacom serveri, telefón kontaktuje server Cisco EDOS RC a poskytne svoju adresu MAC a model a nastaví svoj stav prispôsobenia na **Čakanie** Server Cisco EDOS poskytne informácie o pridruženom poskytovacom serveri poskytovateľa služieb vrátane URL poskytovacieho servera a stav prispôsobenia telefónu sa zmení na **Prispôsobené čakanie**. Telefón potom spustí príkaz na opätovnú synchronizáciu URL, aby načítal konfiguráciu poskytovateľa služby a ak sa príkaz úspešne uskutoční, stav prispôsobenia sa nastaví na **Získané**.

Ak server Cisco EDOS RC nemá k telefónu pridruženého poskytovateľa služieb, stav prispôsobenia telefónu sa nastaví na **Nedostupný**. Telefón môže byť manuálne nakonfigurovaný, alebo môže byť pridaná asociácia poskytovateľa služieb k serveru Cisco EDOS.

Ak sa telefón nastavuje pomocou LCD alebo webovej konfiguračnej pomôcky pred tým, ako sa stav prispôsobenia nastaví na **Získané**, sa stav prispôsobenia najprv zmení na **Prerušené** a server Cisco EDOS sa nebude kontaktovať, až kým telefón nebude obnovený na nastavenia výrobcu.

Po nastavení telefónu sa server Cisco EDOS RC nebude používať, až kým telefón nebude obnovený na nastavenia výrobcu.

## Interná príprava zariadení na poskytovanie



S továrenskou predvolenou konfiguráciou spoločnosti Cisco sa telefón automaticky snaží o opätovnú synchronizáciu s profilom na serveri TFTP. Spravovaný server DHCP na sieti LAN poskytuje informácie o profile a server TFTP, ktorý je nakonfigurovaný na prípravu zariadenia na poskytovanie. Poskytovateľ služby pripojí každý nový telefón k sieti LAN. Telefón sa automaticky opätovne synchronizuje s miestnym serverom TFTP a v rámci prípravy na nasadenie inicializuje svoj vnútorný stav. Tento profil prípravy na poskytovanie štandardne zahŕňa adresu URL vzdialeného poskytovacieho servera. Poskytovací server aktualizuje zariadenie po jeho nasadení a pripojení k sieti zákazníka.

Oskenovaním čiarového kódu zariadenia pripravovaného na poskytovanie môžete zaznamenať jeho adresu MAC alebo sériové číslo pred tým, ako bude telefón odoslaný zákazníkovi. Tieto informácie sa môžu použiť na vytvorenie profilu, s ktorým sa telefón bude opätovne synchronizovať.

Po prijatí telefónu ho zákazník pripojí k širokopásmovému prepojeniu. Pri zapnutí telefón skontaktuje poskytovací server prostredníctvom URL, ktoré bolo nakonfigurované v rámci prípravy na poskytovanie. Telefón sa tak môže opätovne synchronizovať a podľa potreby aktualizovať profil a firmvér.

#### Príbuzné témy

[Maloobchodná distribúcia](#), na strane 5

[Poskytovanie TFTP](#), na strane 40

## Nastavenie poskytovacieho servera

Táto sekcia opisuje požiadavky na nastavenie poskytovaniu telefónom s použitím rôznych serverov a rôznych možností. Pre účely tohto dokumentu a testovania sú poskytovacie servery nainštalované a spúšťané na miestnom PC. Na nastavovanie telefónov sa používajú všeobecne dostupné softvérové nástroje.

## Poskytovanie TFTP

Telefóny podporujú TFTP pre poskytovanie operácií opätovnej synchronizácie aj aktualizácie. Keď sú zariadenia nasadzované vzdialene, odporúča sa používanie HTTPS, ale môžu sa používať aj HTTP a TFTP. Pri nich sa však vyžaduje šifrovanie poskytovacieho súboru, kvôli zvýšeniu zabezpečenia a zlepšeniu spoľahlivosti s ohľadom na NAT a ochranné mechanizmy smerovača. Protokol TFTP je užitočný pri príprave veľkého množstva zariadení na poskytovanie, ktorá prebieha na mieste.

Telefón by mal prijať adresu IP servera TFTP priamo od servera DHCP cez možnosť DHCP 66. Ak je v parametri Profile\_Rule nakonfigurovaná cesta súboru servera TFTP, zariadenie stiahne svoj profil zo servera TFTP. Stiahnutie sa uskutoční, keď bude zariadenie pripojené k sieti LAN a zapnuté.

Parameter Profile\_Rule je nastavený na predvolenú hodnotu `&PN.cfg`, kde `&PN` je názov modelu telefónu.

Napríklad pre CP-6841-3PCC je názov súboru CP-6841-3PCC.cfg.

Pri spustení sa zariadenie s predvoleným profilom výrobcu opätovne synchronizuje s týmto súborom na miestnom serveri TFTP, ktorý je špecifikovaný v možnosti DHCP 66. Cesta súboru je relatívna k hlavnému virtuálnemu adresáru servera TFTP.

#### Príbuzné témy

[Interná príprava zariadení na poskytovanie](#), na strane 39

## Ovládanie vzdialených koncových bodov a NAT

Telefón je kompatibilný s prekladom sieťových adries (network address translation – NAT), aby mal prístup k internetu prostredníctvom smerovača. Smerovač sa môže kvôli posilneniu zabezpečenia pokúsiť zablokovať nepovolené prichádzajúce pakety tak, že vykoná symetrický NAT, stratégiu filtrovania paketov, ktorá prísne vymedzuje, ktoré pakety môžu z internetu vstúpiť do chránenej siete. Preto sa neodporúča vzdialené poskytovanie prostredníctvom TFTP.

VoIP môže fungovať zároveň s NAT len v prípade, že je poskytnutý nejaký druh prechodu cez NAT. Konfigurácia jednoduchého prechodu UDP cez NAT (STUN). Táto možnosť vyžaduje, aby používateľ mal:

- Dynamickú externú (verejnú) adresu IP vašej služby

- Počítač, na ktorom beží softvér servera STUN
- Okrajové zariadenie s asymetrickým mechanizmom NAT

## Poskytovanie HTTP

Telefón sa správa ako prehliadač, ktorý vyžaduje webové stránky zo vzdialenej internetovej stránky. Je to spoľahlivý spôsob, ako kontaktovať poskytovací server, a to aj v prípade, že smerovač zákazníka vykonáva symetrický NAT alebo iné ochranné mechanizmy. Protokoly HTTP a HTTPS sú pri vzdialenom nasadzovaní spoľahlivejšie ako TFTP, najmä ak sú nasadzované jednotky pripojené za rezidenčnými bránami Firewall alebo smerovačmi s povoleným NAT. V nasledovných opisoch typov požiadaviek sú HTTP a HTTPS zameniteľné.

Základné poskytovanie založené na HTTP na načítanie konfiguračných profilov používa metódu HTTP GET. Zvyčajne sa vytvorí konfiguračný súbor pre každý nasadený telefón a tieto súbory sa potom uložia v adresári servera HTTP. Keď server prijme požiadavku GET, jednoducho vráti súbor určený v hlavičke požiadavky GET.

Konfiguračný profil nie je statický, naopak, môže byť generovaný dynamicky dopytovaním databázy klienta a priebežným vytvorením profilu.

Keď telefón požiadava o opätovnú synchronizáciu, na získanie konfiguračných údajov opätovnej synchronizácie môže použiť metódu HTTP POST. Zariadenie môže byť nakonfigurované tak, aby serveru v tele požiadavky HTTP POST poskytlo určité informácie o stave a identifikácii. Server tieto informácie použije na vygenerovanie vyžadovaného návratového konfiguračného profilu alebo na uloženie informácií o stave na neskoršiu analýzu a sledovanie.

V rámci požiadaviek GET aj POST telefón automaticky do poľa Používateľ-Agent v hlavičke žiadosti zahrnie základné identifikačné informácie. Tieto informácie obsahujú výrobcu, názov produktu, súčasnú firmvérovú verziu a produktové sériové číslo zariadenia.

Nasledujúci príklad je pole Používateľ-Agent požiadavky z CP-6841-3PCC:

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

Keď je telefón nakonfigurovaný tak, aby opätovne synchronizoval profil pomocou HTTP, odporúča sa používať HTTPS alebo zašifrovať profil, aby boli chránené dôverné informácie. Zašifrované profily, ktoré telefón stiahne pomocou HTTP, sa vyhnú riziku odhalenia dôverných informácií konfiguračného profilu. Tento režim opätovnej synchronizácie v porovnaní s HTTPS produkuje nižšiu výpočtovú záťaž pre poskytovací server.

Telefón dokáže dešifrovať profily zašifrované niektorou z nasledujúcich metód šifrovania:

- Šifrovanie AES-256-CBC
- Šifrovanie podľa normy RFC 8188 so šifrou AES-128-GCM



### Poznámka

Telefóny podporujú verziu HTTP 1.0, verziu HTTP 1.1 a Chunk Encoding (kódovanie po skupinách), ak je HTTP verzia 1.1 vyjednaný prenosový protokol.

## Riadenie kódu stavu HTTP pre opätovnú synchronizáciu a aktualizáciu

Telefón podporuje odpoveď HTTP pre vzdialené poskytovanie (opätovnú synchronizáciu). Súčasné správanie telefónu sa charakterizuje tromi spôsobmi:

- A – Úspech, keď hodnoty „Pravidelná opätovná synchronizácia“ a „Náhodné oneskorenie opätovnej synchronizácie“ určujú ďalšie požiadavky.
- B – Chyba, keď sa vyskytne chyba Súbor nebol nájdený alebo ak je profil poškodený. Hodnota „Oneskorenie ďalšieho pokusu po chybe opätovnej synchronizácie“ určuje ďalšie požiadavky.
- C – Iná chyba, ak kvôli neprávnomu URL alebo adrese IP vznikne chyba pripojenia. Hodnota „Oneskorenie ďalšieho pokusu po chybe opätovnej synchronizácie“ určuje ďalšie požiadavky.

Tabuľka 2: Správanie telefónu pre odpovede HTTP

Kód stavu HTTP	Popis	Správanie telefónu
<b>301 Trvalé presmerovanie</b>	Táto a všetky požiadavky v budúcnosti budú presmerované na inú lokalitu.	Skúste poslať požiadavku znova na novú lokalitu.
<b>302 Nájdený</b>	Známy aj ako dočasné presmerovaný.	Skúste poslať požiadavku znova na novú lokalitu.
<b>3xx</b>	Ostatné odpovede 3xx nie sú spracovávané.	C
<b>400 Nesprávna požiadavka</b>	Požiadavka nemôže byť spracovaná kvôli nesprávnej syntaxi.	C
<b>401 Neautorizovaný prístup</b>	Výzva jednoduchého alebo skráteného overenia prístupu.	Okamžite znova odošlite žiadosť s overovacími údajmi. Maximálne dva ďalšie pokusy. Po zlyhaní bude správanie telefónu C.
<b>403 Prístup zakázaný</b>	Server odmieta odpovedať.	C
<b>404 Stránka nenájdená</b>	Požadovaný zdroj sa nenašiel. Ďalšie požiadavky klienta sú povolené.	B
<b>407 Požadované overenie proxy</b>	Výzva jednoduchého alebo skráteného overenia prístupu.	Okamžite znova odošlite žiadosť s overovacími údajmi. Maximálne dva ďalšie pokusy. Po zlyhaní bude správanie telefónu C.
<b>4xx</b>	Ostatné stavy chyby klienta sa nespracúvajú.	C
<b>500 Vnútrošná chyba servera</b>	Všeobecné chybové hlásenie	Správanie telefónu je C.
<b>501 Nevykonané</b>	Server nerozpoznal metódu požiadavky alebo nedokáže požiadavku splniť.	Správanie telefónu je C.
<b>502 Chybná brána</b>	Server funguje ako brána alebo proxy a prijal neplatnú odpoveď z nadradeného servera.	Správanie telefónu je C.



Kód stavu HTTP	Popis	Správanie telefónu
<b>503 Služba nie je k dispozícii</b>	Server je dočasne nedostupný (je preťažený alebo prebieha údržba). Je to dočasný stav.	Správanie telefónu je C.
<b>504 Bráne vypršal časový limit</b>	Server sa správa ako brána alebo proxy a neprijal včas odpoveď z nadradeného servera.	C
<b>5xx</b>	Iná chyba servera	C

## Poskytovanie HTTPS

Telefón podporuje používanie HTTPS na poskytovanie kvôli zvýšenému zabezpečeniu spravovania vzdialene nasadzovaných jednotiek. Každý telefón má unikátny certifikát klienta SSL (a pridružený súkromný kľúč) a certifikát hlavného priečinku servera Sipura CA. Druhý uvedený certifikát umožňuje telefónu rozpoznať poskytovacie servery a odmietnuť neoverené servery. Na druhej strane certifikát klienta umožňuje poskytovaciemu serveru identifikovať jednotlivé zariadenie, ktoré vyslalo požiadavku.

Aby poskytovateľ služby mohol spravovať nasadenie pomocou HTTPS, musí byť vygenerovaný certifikát pre každý poskytovací server, s ktorým sa telefón opätovne synchronizuje pomocou HTTPS. Certifikát servera musí byť podpísaný hlavným kľúčom Cisco Server CA Root Key, ktorého certifikát majú všetky nasadené jednotky. Aby poskytovateľ služby získal podpísaný certifikát servera, musí preposlať žiadosť o podpis certifikátu spoločnosti Cisco, ktorá ho podpíše a vráti, aby mohol byť potom nainštalovaný na poskytovacom serveri.

Certifikát poskytovacieho servera musí obsahovať pole Bežný názov (Common Name - CN) a FQDN hostiteľa, na ktorom beží server v predmete. Voliteľne môže obsahovať informácie nasledujúce FQDN hostiteľa oddelené znakom lomky (/). Nasledujú vstupy CN, ktoré telefón prijme ako platné:

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

Okrem overenia certifikátu servera telefón tiež testuje adresu IP servera a vyhľadávanie DNS názvu servera, ktorý je určený v certifikáte servera.

## Získanie podpísaného certifikátu servera

Pomôcka OpenSSL môže vygenerovať žiadosť o podpis certifikátu. Nasledovné príklady ilustrujú príkaz `openssl`, ktorý vytvorí 1024-bitový pár verejného/súkromného kľúča RSA a žiadosť o podpis certifikátu.

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

Tento príkaz vygeneruje súkromný kľúč servera v súbore `privkey.pem` a zodpovedajúcu žiadosť o podpis certifikátu v súbore `provserver.csr`. Poskytovateľ služby uchová súbor `privkey.pem` v tajnosti a súbor `provserver.csr` pošle spoločnosti Cisco na podpis. Po prijatí súboru `provserver.csr` spoločnosť Cisco vygeneruje súbor `provserver.crt` – podpísaný certifikát servera.

## Procedúra

---

- Krok 1** Prejdite na <https://software.cisco.com/software/edos/home> a prihláste sa so svojimi prihlasovacími údajmi CCO.
- Poznámka** Keď sa telefón pripojí k sieti po prvý raz alebo po obnovení výrobných nastavení a nie sú nastavené žiadne možnosti servera DHCP, telefón kontaktuje server na aktiváciu zariadenia. Týmto možno dosiahnuť plne automatizované nastavenie. Nové telefóny použijú na nastavenie adresu “activate.cisco.com”, nie “webapps.cisco.com”. Telefóny s firmvérom starším ako 11.2(1) budú naďalej používať adresu “webapps.cisco.com”. Odporúčame, aby ste povolili obe tieto názvy domén cez bránu firewall.
- Krok 2** Vyberte možnosť **Certificate Management**.  
Na karte **Podpísať CSR** je nahraný CSR z predchádzajúceho kroku na podpis.
- Krok 3** Z rozbaľovacieho zoznamu **Vybrať produkt** vyberte možnosť **SPA1xx firmvér 1.3.3 a novší/SPA232D firmvér 1.3.3 a novší/SPA5xx firmvér 7.5.6 a novší/CP-78xx-3PCC/CP-88xx-3PCC**.
- Poznámka** Tento produkt zahŕňa multiplatformové telefóny Cisco IP Phone radu 6800.
- Krok 4** V poli **Súbor CSR** kliknite na položku **Prehľadávať** a vyberte súbor CSR na podpis.
- Krok 5** Vyberte metódu šifrovania:
- MD5
  - SHA1
  - SHA256
- Spoločnosť Cisco odporúča, aby ste vybrali šifrovanie SHA256.
- Krok 6** V rozbaľovacom zozname **Trvanie prihlásenia** vyberte aplikovateľné trvanie (napríklad 1 rok).
- Krok 7** Kliknite na možnosť **Podpísať žiadosť o certifikát**.
- Krok 8** Vyberte jednu z nasledovných možností, ako prijať podpísaný certifikát.
- **Zadať e-mailovú adresu prijímateľa** – do tohto poľa zadajte svoju e-mailovú adresu, ak chcete certifikát prijať cez e-mail.
  - **Stiahnuť** – vyberte túto možnosť, ak chcete podpísaný certifikát stiahnuť.
- Krok 9** Kliknite na tlačidlo **Odoslať**.  
Podpísaný certifikát servera sa potom buď odošle na uvedenú emailovú adresu, alebo sa stiahne.
- 

## Hlavný certifikát klienta CA multiplatformových telefónov

Spoločnosť Cisco tiež poskytovateľovi služieb poskytuje hlavný certifikát klienta multiplatformových telefónov. Tento hlavný certifikát potvrdzuje autenticitu certifikátu klienta, ktorý má každý telefón. Multiplatformové telefóny tiež podporujú podpísané certifikáty od tretej strany poskytované napríklad spoločnosťami Verisign, Cybertrust a pod.

Jedinečný certifikát klienta, ktorý poskytuje každé zariadenie počas relácie HTTPS, obsahuje identifikačné informácie, ktoré sú vložené v poli predmetu. Tieto informácie môže server HTTPS poskytnúť skriptu CGI,

ktorý je vyvolaný, aby pracoval so zabezpečenými požiadavkami. Konkrétne tento predmet certifikátu indikuje názov produktu jednotky (OU element), adresu MAC (S element) a sériové číslo (L element).

Nasledovný príklad z poľa predmetu certifikátu klienta multiplatformových telefónov Cisco IP Phone 6841 obsahuje tieto elementy:

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

Na zistenie toho, či telefón obsahuje individualizovaný certifikát, použite premennú poskytovacieho makra \$CCERT. Hodnota premennej sa rozvinie na Nainštalované alebo Nenainštalované podľa toho, či jedinečný certifikát klienta je alebo nie je prítomný. V prípade všeobecného certifikátu je možné získať sériové číslo jednotky z hlavičky požiadavky HTTP v poli Používateľ-Agent.

Servery HTTPS môžu byť nakonfigurované, aby od pripájajúcich sa klientov vyžadovali certifikáty SSL. Ak je to povolené, server môže používať hlavný certifikát klienta multiplatformových telefónov poskytnutý spoločnosťou Cisco na overenie certifikátu klienta. Server môže potom poskytnúť informácie o certifikáte CGI na ďalšie spracovanie.

Umiestenie certifikátu sa môže meniť. Napríklad v inštalácii Apache sú cesty súborov pre certifikát podpísaný poskytovacím serverom, jeho pridružený súkromný kľúč a hlavný certifikát klienta CA multiplatformových telefónov nasledovné:

```
# 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
```

Určené informácie nájdete v dokumentácii pre server HTTPS.

Autorita pre hlavný certifikát klienta spoločnosti Cisco podpíše každý jedinečný certifikát. Zodpovedajúci hlavný certifikát sa zverejní pre poskytovateľov služby na účely overenia klienta.

## Redundantné poskytovacie servery

Poskytovací server môže byť určený ako adresa IP alebo ako úplný názov domény (FQDN). Použitie FQDN zjednodušuje nasadenie redundantných poskytovacích serverov. Keď je poskytovací server identifikovaný cez FQDN, telefón sa pokúsi o rozpoznanie FQDN na adresu IP cez DNS. Pre poskytovanie sú podporované iba záznamy DNS typu A; rozlišovanie adresy DNS SRV nie je pre poskytovanie dostupné. Telefón pokračuje v spracovávaní záznamov typu A, až kým server neodpovie. Ak neodpovie žiadny server pridružený k záznamom typu A, telefón na server zapisovania do denníka systému zaznamená chybu.

## Server systémového denníka

Ak je server systémového denníka nakonfigurovaný na telefóne použitím parametrov <Syslog Server>, operácie opätovnej synchronizácie a aktualizácie naň posielajú správy. Správa sa môže vygenerovať pri začiatku vzdialenej požiadavky o súbor (konfiguračný profil alebo načítanie firmvéru) a po dokončení operácie (ukážu úspech alebo zlyhanie operácie).

Správy zapísané do denníka sú konfigurované nasledovnými parametrami a v správach systémového denníka sú rozvinuté pomocou makier:

- Log\_Request\_Msg
- Log\_Success\_Msg
- Log\_Failure\_Msg



## KAPITOLA 4

# Príklady poskytovania

- [Prehľad príkladov poskytovania, na strane 47](#)
- [Základná opätovná synchronizácia, na strane 47](#)
- [Bezpečná opätovná synchronizácia s HTTPS, na strane 53](#)
- [Správa profilu, na strane 60](#)
- [Nastavenie hlavičky súkromia telefónu, na strane 63](#)

## Prehľad príkladov poskytovania

Táto kapitola poskytuje príklady postupov prepojenia konfiguračných profilov medzi telefónom a poskytovacím serverom.

Informácie o vytváraní konfiguračných profilov nájdete v časti [Poskytovacie skripty, na strane 13](#).

## Základná opätovná synchronizácia

Táto sekcia predstavuje funkciu základnej opätovnej synchronizácie telefónu.

## Opätovná synchronizácia s TFTP

Telefón podporuje na získavanie konfiguračných profilov viacero sieťových protokolov. Základný protokol prenosu profilu je TFTP (RFC1350). TFTP sa často používa na poskytovanie údajov sieťovým zariadeniam v rámci súkromných sietí LAN. Hoci sa TFTP neodporúča na nasadzovanie vzdialených koncových bodov cez internet, môže byť užitočný pri nasadzovaní v menších organizáciách, príprave na poskytovanie na mieste a na vývoj a testovanie. Viac informácií o príprave na poskytovanie na mieste nájdete v časti [Interná príprava zariadení na poskytovanie, na strane 39](#). V nasledovnom procese sa profil po stiahnutí súboru zo servera TFTP upraví.

### Procedúra

- Krok 1** V prostredí siete LAN pripojte PC a telefón k rozbočovaču, prepínaču alebo malému smerovaču.
- Krok 2** Na PC nainštalujte a aktivujte server TFTP.

- Krok 3** Pomocou textového editora vytvorte konfiguračný profil, ktorý nastavuje hodnotu parametra GPP\_A na 12345678 tak, ako je to uvedené v príklade.

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

- Krok 4** Profil uložte ako `basic.txt` v hlavnom virtuálnom adresári servera TFTP. Môžete overiť, či je server TFTP správne nakonfigurovaný: vyžiadajte súbor `basic.txt` pomocou iného klienta TFTP, ako je váš telefón. Najvhodnejšie bude, ak použijete klienta TFTP, ktorý beží na inom hostiteľovi ako poskytovací server.

- Krok 5** Vo webovom prehliadači PC otvorte stránku konfigurácie správca/pokročilý. Napríklad, ak je IP adresa telefónu 192.168.1.100:

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

- Krok 6** Vyberte kartu **Hlas > Poskytovanie** a prezrite si hodnoty parametrov pre všeobecné účely GPP\_A až GPP\_P. Mali by byť prázdne.

- Krok 7** Opätovne synchronizujte telefón so súborom `basic.txt` tak, že otvoríte URL opätovnej synchronizácie v okne webového prehliadača.

Ak je adresa IP servera TFTP 192.168.1.200, príkaz by mal byť podobný tomuto príkladu:

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

Keď telefón prijme tento príkaz, zariadenie na adrese 192.168.1.100 si vyžiada súbor `basic.txt` zo serveru TFTP na adrese IP 192.168.1.200. Telefón potom zanalyzuje stiahnutý súbor a aktualizuje parameter GPP\_A na hodnotu 12345678.

- Krok 8** Skontrolujte, že parameter bol správne aktualizovaný: Obnovte konfiguračnú stránku na webovom prehliadači počítača a vyberte kartu **Hlas > Poskytovanie**.

Parameter GPP\_A by teraz mal obsahovať hodnotu 12345678.

## Požitie systémového denníku na zaznamenávanie správ

Tesne pred začiatkom opätovnej synchronizácie telefónu s poskytovacím serverom a po tom, ako sa opätovná synchronizácia dokončila alebo zlyhala, telefón pošle serveru systémového denníka správu systémového denníka. Ak chcete nájsť tento server, prejdite na webovú stránku správy telefónu (pozrite časť [Prístup na webovú stránku telefónu, na strane 7](#)), vyberte možnosť **Hlas > Systém** a nájdite server v parametri **Syslog Server** v sekcii **Voliteľná sieťová konfigurácia**. Nakonfigurujte zariadeniu adresu IP servera systémového denníka a pozorujte správy vygenerované počas zostávajúcich procesov.

### Procedúra

- Krok 1** Nainštalujte a aktivujte server systémového denníka na miestnom PC.

**Krok 2** Naprogramujte IP adresu PC do parametra profilu Syslog\_Server a odošlite zmenu:

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

**Krok 3** Kliknite na kartu **Systém** a zadajte hodnotu vášho miestneho servera systémového denníka do parametra Syslog\_Server.

**Krok 4** Zopakujte operáciu opätovnej synchronizácie tak, ako je uvedené v časti [Opätovná synchronizácia s TFTP, na strane 47](#).

Zariadenie počas opätovnej synchronizácie vygeneruje dve správy systémového denníka. Prvá správa oznamuje, že požiadavka prebieha. Druhá správa oznamuje úspech alebo zlyhanie opätovnej synchronizácie.

**Krok 5** Overte, že váš server systémového denníka prijal správy podobné týmto:

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

Detailné správy môžete zobrazíť, keď parametru Debug\_Server (namiesto parametra Syslog\_Server) nastavíte adresu IP servera systémového denníka a hodnotu Debug\_Level nastavíte na 0 až 3 (3 obsahuje najviac podrobností):

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

Obsah týchto správ môže byť nakonfigurovaný pomocou nasledovných parametrov:

- Log\_Request\_Msg
- Log\_Success\_Msg
- Log\_Failure\_Msg

Ak je niektorý z týchto parametrov vymazaný, zodpovedajúca správa systémového denníka sa nevygeneruje.

---

## Automatická opätovná synchronizácia zariadenia

Zariadenie sa môže pravidelne opätovne synchronizovať so serverom, aby sa zabezpečilo, že každá zmena profilu na serveri sa dostane na koncové zariadenie (takže nebude potrebné posilať koncovému bodu explicitné žiadosti o opätovnú synchronizáciu).

Aby sa telefón pravidelne opätovne synchronizoval so serverom, URL konfiguračného profilu sa nadefinuje pomocou parametra Profile\_Rule a v parametri Resync\_Periodic sa definuje interval opätovnej synchronizácie.

### Skôr ako začnete

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).

### Procedúra

---

**Krok 1** Vyberte možnosť **Hlas > Poskytovanie**.

- Krok 2** Nastavte parameter Profile\_Rule. V tomto príklade sa predpokladá, že adresa IP servera TFTP je 192.168.1.200.
- Krok 3** V poli **Pravidelná opätovná synchronizácia** zadajte malú hodnotu na účely testovania, napríklad **30** sekúnd.
- Krok 4** Kliknite na možnosť **Odoslať všetky zmeny**.
- Vďaka novému nastaveniu parametra sa telefón dvakrát sa minútu opätovne synchronizuje s konfiguračným súborom špecifikovanom v URL.
- Krok 5** Prezrite si výsledné správy v systémovom denníku (ako je to popísané v sekcii [Požitie systémového denníku na zaznamenávanie správ, na strane 48](#)).
- Krok 6** Uistite sa, že pole **Po reštarte opätovne synchronizovať** je nastavené na hodnotu **Áno**.

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

- Krok 7** Telefón vypnite a zapnite, aby sa opätovne synchronizoval s poskytovacím serverom.
- Ak z nejakého dôvodu opätovná synchronizácia zlyhá (napríklad ak server neodpovedá), jednotka počká (počet sekúnd je nakonfigurovaný v poli **Oneskorenie ďalšieho pokusu po chybe opätovnej synchronizácie**) a potom sa o opätovnú synchronizáciu pokúsi znova. Ak je hodnota **Oneskorenie ďalšieho pokusu po chybe opätovnej synchronizácie** nastavená na 0, telefón sa po prvom neúspešnom pokuse o opätovnú synchronizáciu nebude pokúšať znova.
- Krok 8** (Voliteľné) Nastavte hodnotu poľa **Oneskorenie ďalšieho pokusu po chybe opätovnej synchronizácie** na malé číslo, napríklad **30**.

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

- Krok 9** Vypnite server TFTP a prezrite si výsledky v systémovom denníku.

## Jedinečné profily, rozvoj makier a HTTP

Počas nasadzovania musí byť každý telefón nakonfigurovaný pre niektoré parametre (napríklad User\_ID alebo Display\_Name) na rôzne hodnoty. Poskytovateľ služby môže pre každé nasadené zariadenie vytvoriť jedinečný profil a potom tieto profily uložiť na poskytujúci server. Každý telefón potom musí byť nakonfigurovaný tak, aby znova zosynchronizoval svoj profil podľa preddefinovaných pomenovacích konvencií profilu.

URL syntax profilu môže zahŕňať identifikačné informácie, ktoré sa líšia pre každý telefón, napríklad adresu MAC alebo sériové číslo, s použitím rozvoja makier zabudovaných premenných. Vďaka rozvoju makier nebude potrebné určiť tieto hodnoty na viacerých miestach v každom profile.

V pravidle profilu sa rozvoj makier uskutoční pred tým, ako sa pravidlo aplikuje na telefón. Rozvoj makier riadi rôzne hodnoty, napríklad:

- \$MA sa rozvinie na dvanásťcifernú adresu MAC (s použitím čífer v šesťnástkovej sústave s malým písmenom) Napríklad 000e08abcdef.
- \$SN sa rozvinie na sériové číslo jednotky. Napríklad 88012BA01234.

Takto rozvinuté môžu byť aj iné hodnoty vrátane parametrov na všeobecné účely od GPP\_A do GPP\_P. Príklad tohto procesu je znázornený v časti [Opätovná synchronizácia s TFTP, na strane 47](#). Rozvoj makier



nie je obmedzený na názov súboru URL, môže sa aplikovať na akúkoľvek časť parametra pravidla profilu. Tieto parametre sú označované ako \$A až \$P. Úplný zoznam premenných, pre ktoré je možný rozvoj makier, nájdete v časti [Premenné rozvoja makier, na strane 72](#).

V tomto cvičení je profil konkrétneho telefónu poskytovaný na serveri TFTP.

## Príklad: Poskytnutie konkrétneho profilu telefónu IP Phone na serveri TFTP

### Procedúra

- 
- Krok 1** Získajte adresu MAC telefónu z jeho produktového označenia. (Adresa MAC je číslo, ktoré obsahuje cifry a číslice šestnástkovej sústavy a malé písmená, napríklad 000e08aabbcc.
  - Krok 2** Skopírujte konfiguračný súbor `basic.txt` (opísaný v časti [Opätovná synchronizácia s TFTP, na strane 47](#)) do nového súboru nazvaného `CP-xxxx-3PCC macaddress.cfg` (xxxx nahraďte číslom modelu a `macaddress` nahraďte adresou MAC telefónu).
  - Krok 3** Nový súbor presuňte do hlavného virtuálneho adresára servera TFTP.
  - Krok 4** Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).
  - Krok 5** Vyberte možnosť **Hlas > Poskytovanie**.
  - Krok 6** Do poľa `Pravidlo profilu` zadajte `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg`.

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

- Krok 7** Kliknite na možnosť **Odoslať všetky zmeny**. Tým sa spustí okamžitý reštart a opätovná synchronizácia. Pri ďalšej opätovnej synchronizácii načíta telefón nový súbor rozvojom výrazu makra \$MA na svoju adresu MAC.

### Opätovná synchronizácia s HTTP GET

HTTP poskytuje spoľahlivejší mechanizmus opätovnej synchronizácie ako TFTP, pretože vytvára spojenie TCP, kým TFTP používa menej spoľahlivé spojenie UDP. Servery HTTP tiež umožňujú pokročilejšie funkcie filtrovania a záznamu ako servery TFTP.

Aby sa telefón mohol opätovne synchronizovať pomocou HTTP, na strane klienta sa nevyžaduje žiadne špecifické nastavenie konfigurácie na serveri. Syntax parametra `Profile_Rule` pre používanie HTTP s metódou HTTP je podobná syntaxi používanej pre TFTP. Ak bežný webový prehliadač dokáže načítať profil z vášho servera HTTP, telefón by to mal dokázať tiež.

*Príklad: Opätovná synchronizácia s HTTP GET*

### Procedúra

- 
- Krok 1** Na miestny PC alebo iného prístupného hostiteľa nainštalujte HTTP server.

Server Apache s otvoreným kódom môžete stiahnuť z internetu.

- Krok 2** Skopírujte konfiguračný profil `basic.txt` (opísaný v časti [Opätovná synchronizácia s TFTP, na strane 47](#)) do hlavného virtuálneho adresára nainštalovaného servera.
- Krok 3** Aby ste overili správnu inštaláciu servera a prístup k súboru `basic.txt`, pristúpte k profilu prostredníctvom webového prehliadača.
- Krok 4** Upravte pravidlo profilu testovaného telefónu tak, aby namiesto servera TFTP smeroval na server HTTP, aby sa profil sťahoval pravidelne.

Napríklad ak je server HTTP na adrese 192.168.1.300, zadajte nasledovnú hodnotu:

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

- Krok 5** Kliknite na možnosť **Odoslať všetky zmeny**. Tým sa spustí okamžitý reštart a opätovná synchronizácia.
- Krok 6** Pozorujte syslog správy, ktoré posiela telefón. Pravidelná opätovná synchronizácia teraz bude získavať profil zo servera HTTP.
- Krok 7** V denníkoch servera HTTP si všimnite, ako sa informácie, ktoré identifikujú telefón, zobrazia v denníku používateľov-agentov.

Tieto informácie by mali zahŕňať výrobcu, názov produktu, súčasnú firmvérovú verziu a sériové číslo.

## Poskytovanie cez Cisco XML

Každý telefón, tu označený ako `xxxx`, môžete nastaviť pomocou funkcií Cisco XML.

Môžete na telefón poslať objekt XML cez balíček SIP NOTIFY alebo HTTP príkazom POST na rozhranie CGI telefónu: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC rozširuje funkciu Cisco XML, aby podporovala poskytovanie prostredníctvom objektu XML:

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

Po prijatí objektu XML telefón stiahne nastavovací súbor z lokality `[profile-rule]`. Toto pravidlo používa makrá na zjednodušenie aplikácie služieb XML.

## Rozpoznanie URL pomocou rozvoja makier

Podadresáre s viacerými profilmi na serveri sú vhodnou metódou na spravovanie veľkého počtu nasadených zariadení. URL profilu môže obsahovať:

- Názov poskytujúceho servera alebo explicitnú adresu IP. Ak profil identifikuje poskytujúci server podľa mena, telefón vyhledá DNS a rozpozna názov.
- Neštandardný port servera, ktorý je určený v URL pomocou štandardnej syntaxe `:port` nasledujúci za názvom serveru.
- Podadresár hlavného virtuálneho adresára na serveri, kde je uložený profil, určený štandardným zápisom URL a spravovaný rozvojom makra.

Napríklad nasledovné pravidlo profilu požaduje súbor profilu (\$PN.cfg) v podadresári na serveri /cisco/config zo servera TFTP, ktorý beží na hostiteľovi prov.telco.com a načúva na porte 6900:

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

Profil každého telefónu je možné identifikovať parametrom na všeobecné účely, na ktorého hodnotu odkazuje spoločné pravidlo profilu, pomocou rozvoja makier.

Napríklad predpokladajme, že GPP\_B je definovaný ako Dj6Lmp23Q.

Nové pravidlo telefónu Profile\_Rule má hodnotu:

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

Keď sa zariadenie opätovne zosynchronizuje a makrá sa rozvinú, telefón s adresou MAC 000e08012345 si vyžiada profil s názvom, ktorý obsahuje MAC adresu zariadenia, na nasledovnej adrese URL:

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

## Bezpečná opätovná synchronizácia s HTTPS

Tieto mechanizmy sú dostupné na telefóne a umožňujú opätovnú synchronizáciu pomocou bezpečného komunikačného procesu:

- Základná opätovná synchronizácia s HTTPS
- HTTPS s overovaním pomocou certifikátu klienta
- Filtrovanie klientov HTTPS a dynamický obsah

## Základná opätovná synchronizácia s HTTPS

HTTPS pridáva do HTTP pre vzdialené poskytovanie SSL, aby:

- Telefón mohol overiť poskytovací server.
- Poskytovací server mohol overiť telefón.
- Bola zabezpečená dôvernosť informácií, ktorá sa odošlú medzi telefónom a poskytovacím serverom.

SSL generuje a vymieňa tajné (symetrické) kľúče pre každé pripojenie medzi telefónom a serverom pomocou párov verejných/súkromných kľúčov, ktoré sú vopred nainštalované v telefóne a na poskytovacom serveri.

Aby sa telefón mohol opätovne synchronizovať pomocou HTTPS na strane klienta nevyžaduje žiadne špeciálne nastavenie konfigurácie na serveri. Syntax parametra Profile\_Rule pre používanie HTTPS s metódou GET je podobná syntaxi používanej pre HTTP alebo TFTP. Ak bežný webový prehliadač dokáže načítať profil z vášho servera HTTPS, telefón by to mal dokázať tiež.

Okrem inštalácie servera HTTPS musí byť na poskytujúcom serveri nainštalovaný aj certifikát SSL servera Cisco podpísaný spoločnosťou Cisco. Zariadenia sa nemôžu opätovne zosynchronizovať so serverom, ktorý

používa HTTPS, pokiaľ server neposkytuje certifikát servera podpísaný spoločnosťou Cisco. Inštrukcie na vytvorenie podpísaného certifikátu SSL pre hlasové produkty nájdete na <https://supportforums.cisco.com/docs/DOC-9852>.

## Príklad: Základná opätovná synchronizácia s HTTPS

### Procedúra

- Krok 1** Nainštalujte server HTTPS na hostiteľa, ktorého adresa IP je známa serveru siete DNS pomocou normálneho prekladu názvu hostiteľa.
- Server Apache s otvoreným zdrojovým kódom môže byť nakonfigurovaný tak, aby fungoval ako server HTTPS, ak je nainštalovaný s balíčkom `mod_ssl` s otvoreným zdrojovým kódom.
- Krok 2** Vygenerujte žiadosť o podpis certifikátu servera pre server. Na tento krok budete možno musieť nainštalovať balíček OpenSSL s otvoreným zdrojovým kódom alebo podobný softvér. Ak používate OpenSSL, príkaz na vygenerovanie základného súboru CSR je nasledovný:
- ```
openssl req -new -out provserver.csr
```
- Tento príkaz generuje pár verejného/súkromného kľúča, ktorý sa uloží v súbore `privkey.pem`.
- Krok 3** Pošlite súbor CSR (`provserver.csr`) na podpis spoločnosti Cisco.
- Podpísaný certifikát servera sa vráti (`provserver.cert`) spolu s hlavným certifikátom klienta Sipura CA, `spacroot.cert`.
- Viac informácií nájdete v časti <https://supportforums.cisco.com/docs/DOC-9852>.
- Krok 4** Uložte podpísaný certifikát servera, súbor s párom súkromných kľúčov a hlavný certifikát klienta na príslušných miestach na serveri.
- V prípade inštalácie Apache na Linuxe sú tieto miesta nasledovné:
- ```
# 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
```
- Krok 5** Reštartujte server.
- Krok 6** Skopírujte konfiguračný súbor `basic.txt` (opísaný v časti [Opätovná synchronizácia s TFTP, na strane 47](#)) do hlavného virtuálneho adresára servera HTTPS.
- Krok 7** Overte správne fungovanie servera stiahnutím súboru `basic.txt` zo servera HTTPS pomocou štandardného prehliadača z lokálneho PC.
- Krok 8** Skontrolujte certifikát servera, ktorý server poslal.
- Prehliadač pravdepodobne nerozpozna certifikát ako platný, pokiaľ nebol predkonfigurovaný, aby prijímal Cisco ako hlavnú CA. Telefón však očakáva, že certifikát bude podpísaný týmto spôsobom.
- Upravte parameter `Profile_Rule` testovaného zariadenia, aby obsahoval odkaz na server HTTPS, napríklad:

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

V tomto príklade sa predpokladá, že názov servera HTTPS je **my.server.com**.

**Krok 9** Kliknite na možnosť **Odoslať všetky zmeny**.

**Krok 10** Pozorujte denníkové správy systému, ktoré posiela telefón.

V denníkovej správe systému by malo byť uvedené, že opätovná synchronizácia získala profil zo servera HTTPS.

**Krok 11** (voliteľné) Použite analyzátor ethernetového protokolu v podsieti telefónu, aby ste overili, či sú balíčky zašifrované.

V tomto cvičení nebolo overovanie pomocou certifikátu klienta povolené. Prepojenie medzi telefónom a serverom je šifrované. Prenos ale nie je bezpečný, pretože akýkoľvek klient sa môže pripojiť k serveru a vyžiadať si súbor, pokiaľ pozná názov súboru a umiestnenie adresára. Pre bezpečnú opätovnú synchronizáciu sa vyžaduje, aby server overil aj klienta tak, ako je to ukázané v časti [HTTPS s overovaním pomocou certifikátu klienta, na strane 55](#).

## HTTPS s overovaním pomocou certifikátu klienta

V konfigurácii na predvolené nastavenia výrobcu server nevyžaduje od klienta certifikát klienta SSL. Prenos profilu nie je bezpečný, pretože akýkoľvek klient sa môže pripojiť k serveru a profil si vyžiadať. Môžete upraviť konfiguráciu a povoliť overenie klienta. Server potom bude vyžadovať certifikát klienta na overenie telefónu pred tým, ako prijme požiadavku na pripojenie.

Kvôli tejto požiadavke nemôže byť operácia opätovnej synchronizácie testovaná nezávisle s použitím prehliadača, ktorý nemá potrebné poverenia. Výmenu kľúčov SSL v rámci HTTPS spojenia medzi testovacím telefónom a serverom je možné sledovať prostredníctvom pomôcky ssldump. V zázname tejto pomôcky sa zobrazí interakcia medzi klientom a serverom.

### Príklad: HTTPS s overovaním pomocou certifikátu klienta

#### Procedúra

**Krok 1** Povoľte overovanie pomocou certifikátu klienta na serveri HTTPS.

**Krok 2** Konfiguračný súbor servera nastavte v službe Apache (v.2) nasledovne:

```
SSLVerifyClient require
```

Uistite sa tiež, že súbor spacroot.cert bol uložený tak, ako je zobrazené v cvičení [Základná opätovná synchronizácia s HTTPS, na strane 53](#).

**Krok 3** Reštartujte server HTTPS a pozorujte správy systémového denníka z telefónu.

S každou nasledujúcou opätovnou synchronizáciou sa teraz spustí symetrické overenie, aby sa pred prenosom profilu overil certifikát servera aj certifikát klienta.

**Krok 4** Pomocou nástroja `ssldump` zachyťte pripojenie opätovnej synchronizácie telefónu a servera HTTPS.

Ak je overovanie pomocou klientského certifikátu na serveri správne povolené, záznam `ssldump` zobrazí symetrickú výmenu certifikátov (najprv od servera ku klientovi a potom naopak) pred šifrovanými paketmi, ktoré obsahujú profil.

Keď je overovanie pomocou certifikátu klienta povolené, profil z poskytujúceho serveru si môže vyžiadať iba telefón s adresou MAC, ktorá zodpovedá platnému certifikátu klienta. Požiadavky z bežného prehliadača alebo iného nepovoleného zariadenia server odmieta.

## Filtrovanie klientov HTTPS a dynamický obsah

Ak je HTTPS server nakonfigurovaný tak, aby vyžadoval certifikát klienta, podľa informácií na certifikáte sa identifikuje opätovne synchronizovaný telefón a poskytnú sa mu správne konfiguračné informácie.

Server HTTPS sprístupní informácie o certifikáte skriptom CGI (alebo skompilovaným programom CGI), ktoré sa vyvolajú v rámci žiadosti o opätovnú synchronizáciu. Pre ilustračné účely sa v tomto príklade používa skriptovací jazyk Perl s otvoreným kódom a predpokladá, že ako HTTPS server sa používa Apache (v.2).

### Procedúra

**Krok 1** Nainštalujte Perl na hostiteľa, na ktorom beží server HTTPS.

**Krok 2** Vygenerujte nasledovný reflečný skript v Perle:

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

**Krok 3** Uložte tento súbor pod názvom `reflect.pl` s povolením na spustenie (na Linuxe `chmod 755`) v adresári skriptov CGI na serveri HTTPS.

**Krok 4** Overte dostupnosť skriptov CGI na serveri (teda `/cgi-bin/...`).

**Krok 5** Upravte `Profile_Rule` na testovacom zariadení, aby sa reflečný skript znova synchronizoval tak, ako je to znázornené v nasledujúcom príklade:

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

**Krok 6** Kliknite na možnosť **Odoslať všetky zmeny**.

**Krok 7** Skontrolujte v zázname systémového denníka, či opätovná synchronizácia prebehla úspešne.

**Krok 8** Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).

**Krok 9** Vyberte možnosť **Hlas > Poskytovanie**.

**Krok 10** Skontrolujte, že parameter GPP\_D obsahuje informácie, ktoré zachytil skript.

Tieto informácie obsahujú názov produktu, adresu MAC a sériové číslo, ak má testovacie zariadenie jedinečný certifikát od výrobcu. Ak bola jednotka vyrobená pred vydaním firmvéru verzie 2.0, informácie obsahujú generické reťazce.

Podobný skript dokáže zistiť informácie o zariadení, ktoré sa opätovne synchronizuje, a potom zariadeniu poskytnúť príslušné hodnoty parametrov konfigurácie.

## Certifikáty HTTPS

Telefón poskytuje spoľahlivú a bezpečnú stratégiu poskytovania založenú na požiadavkách HTTPS posielaných zo zariadenia na poskytovací server. Na overenie telefónu serverom a naopak sa používa certifikát servera aj certifikát klienta.

Aby bolo možné na telefóne používať HTTPS, musíte najprv vygenerovať žiadosť o podpis certifikátu (Certificate Signing Request – CSR) a poslať ju spoločnosti Cisco. Telefón vygeneruje certifikát, ktorý sa nainštaluje na poskytovací server. Telefón prijme certifikát, keď sa bude snažiť vytvoriť spojenie s poskytovacím serverom prostredníctvom HTTPS.

## Metodológia HTTPS

HTTPS šifruje komunikáciu medzi klientom a serverom, čím chráni obsah správy pred ostatnými sieťovými zariadeniami. Šifrovacia metóda pre obsah komunikácie medzi klientom a serverom je založená na symetrickej kryptografii. Vďaka symetrickej kryptografii klient aj server zdieľajú jeden tajný kľúč na zabezpečenom kanáli, ktorý je chránený šifrovaním verejným/súkromným kľúčom.

Správy zašifrované tajným kľúčom je možné dešifrovať iba s použitím rovnakého kľúča. HTTPS podporuje rôzne algoritmy symetrickeho šifrovania. Telefón okrem 256-bitového šifrovania RC4 vykonáva až 256-bitové šifrovanie so štandardom AES (American Encryption Standard).

HTTP tiež umožňuje overenie servera a klienta zapojeného do zabezpečenej transakcie. Vďaka tejto funkcii žiadne iné zariadenie v sieti nemôže imitovať poskytovací server ani klienta. To je mimoriadne dôležité v kontexte poskytovania pre vzdialené koncové body.

Overenie servera a klienta sa uskutočňuje prostredníctvom šifrovania s verejným/súkromným kľúčom s certifikátom obsahujúcim verejný kľúč. Text zašifrovaný verejným kľúčom môže byť dešifrovaný iba zodpovedajúcim súkromným kľúčom (a naopak). Telefón podporuje algoritmus Rivest-Shamir-Adleman (RSA) pre kryptografiu s verejným/súkromným kľúčom.

## Certifikát servera SSL

Pre každý zabezpečený poskytovací server je vydaný certifikát servera SSL (secure sockets layer – vrstva bezpečných soketov) podpísaný priamo spoločnosťou Cisco. Firmvér bežiaci na telefóne rozpozná ako platný iba certifikát od spoločnosti Cisco. Keď sa klient pripojí k serveru pomocou HTTPS, server odmietne všetky certifikáty, ktoré nie sú podpísané spoločnosťou Cisco.

Tento mechanizmus chráni poskytovateľa služby pred nepovoleným prístupom k telefónu alebo pokusom o imitáciu poskytovacieho servera. Bez takejto ochrany by útočník mohol mať možnosť znova nastaviť telefón

a získať tak konfiguračné informácie alebo použiť inú službu VoIP. Bez súkromného kľúča zodpovedajúceho platnému certifikátu servera útočník nemôže nadviazať komunikáciu s telefónom.

## Získanie certifikátu servera

### Procedúra

- 
- Krok 1** Kontaktuje pracovníka podpory Cisco, ktorý vám pomôže s procesom získavania certifikátu. Ak nie ste v kontakte so žiadaným pracovníkom podpory, napíšte svoju žiadosť na adresu `ciscosb-certadmin@cisco.com`.
- Krok 2** Vygenerujte súkromný kľúč, ktorý sa použije v žiadosti o podpis certifikátu (Certificate Signing Request – CSR). Tento kľúč je súkromný a nemusíte ho poskytnúť podpore Cisco. Pomocou služby „openssl“ s otvoreným zdrojom vygenerujte kľúč. Príklad:
- ```
openssl genrsa -out <file.key> 1024
```
- Krok 3** Vygenerujte CSR, ktorá bude obsahovať polia s vašou organizáciou a lokalitou. Príklad:
- ```
openssl req -new -key <file.key> -out <file.csr>
```
- Musíte zadať nasledujúce informácie:
- Pole Predmet – Zadajte bežný názov (Common Name – CN), ktorý musí byť v syntaxi FQDN (Fully Qualified Domain Name – úplný názov domény). Počas podania rúk overovania SSL telefón overí, či certifikát, ktorý prijíma, pochádza zo zariadenia, ktoré ho vytvorilo.
  - Názov hostiteľa servera – Napríklad `provserv.domain.com`.
  - Emailová adresa – Zadajte emailovú adresu, aby vás v prípade potreby mohol kontaktovať pracovník zákazníckej podpory. Táto emailová adresa bude viditeľná v CSR.
- Krok 4** E-mailom pošlite CSR (vo formáte súboru ZIP) zástupcovi oddelenia podpory spoločnosti Cisco alebo na adresu `ciscosb-certadmin@cisco.com`. Spoločnosť Cisco podpíše tento certifikát. Spoločnosť Cisco vám podpísaný certifikát pošle, aby ste ho mohli nainštalovať do svojho systému.
- 

## Certifikát klienta

Okrem priameho útoku na telefón sa útočník môže pokúsiť aj o kontaktovanie poskytovacieho servera cez bežný webový prehliadač alebo iný klient HTTPS s cieľom získať konfiguračný profil z poskytovacieho servera. Aby sa zabránilo tomuto druhu útoku, každý telefón obsahuje jedinečný certifikát klienta podpísaný spoločnosťou Cisco, v ktorom sú uvedené identifikačné informácie o každom koncovom bode. Každému poskytovateľovi služby je poskytnutý hlavný certifikát Certificate Authority, pomocou ktorého je možné overiť certifikát klienta zariadenia. Tento spôsob overenia umožňuje poskytovaciemu serveru odmietnuť neoverené požiadavky na konfiguračné profily.

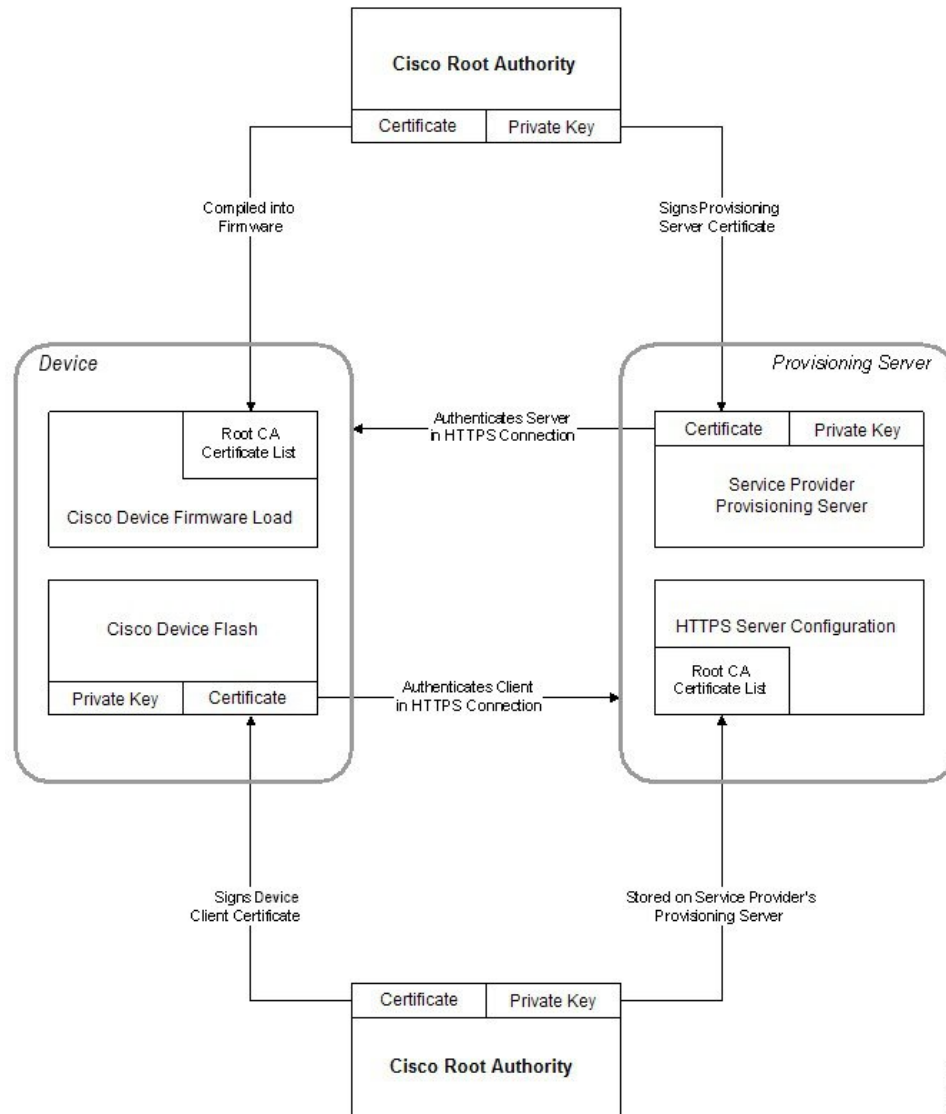
## Štruktúra certifikátu

Kombinácia certifikátu servera a certifikátu klienta umožňuje bezpečnosť komunikácie medzi vzdialeným telefónom a jeho poskytovacím serverom. Nižšie uvedený obrázok ilustruje vzťah a umiestnenie certifikátov, verejných/súkromných kľúčov a hlavných podpisových autorít na klientovi Cisco, poskytovacom serveri a certifikačnej autorite.



V hornej časti diagramu je zobrazená hlavná autorita poskytovacieho servera, ktorá sa používa na podpis konkrétneho certifikátu poskytovacieho servera. Zodpovedajúci hlavný certifikát zabudovaný do firmvéru, vďaka čomu telefón môže overiť schválené poskytovacie servery.

**Obrázok 2: Spracovanie certifikačnej autority (Certificate Authority)**



239117

## Konfigurácia vlastnej certifikačnej autority (Certificate Authority – CA)

Digitálne certifikáty sa môžu používať na overovanie sieťových zariadení a používateľov v sieti. Môžu sa používať na riešenie relácií IPsec medzi uzlami siete.

Tretia strana používa certifikát Certificate Authority na overenie dvoch alebo viacerých uzlov, ktoré sa snažia o komunikáciu. Každý uzol má verejný a súkromný kľúč. Verejný kľúč šifruje údaje. Súkromný kľúč dešifruje údaje. Keďže uzly získali certifikáty z rovnakého zdroja, poznajú svoje vzájomné identity.

Zariadenie môže používať digitálne certifikáty poskytnuté certifikačnou autoritou Certificate Authority (CA) tretej strany na overovanie pripojení IPsec.

Telefóny podporujú súbor prednahranych hlavných certifikačných autorít (Root Certificate Authority) zabudovaných vo firmvéri:

- Cisco Small Business CA Certificate
- CyberTrust CA Certificate
- Verisign CA certificate
- Sipura Root CA Certificate
- Linksys Root CA Certificate

### Skôr ako začnete

Prejdite na webovú stránku správy telefónu. Pozrite [Prístup na webovú stránku telefónu, na strane 7](#).

### Procedúra

---

**Krok 1** Vyberte možnosť **Info** > **Stav**.

**Krok 2** Posuňte sa na **Stav vlastného CA** a prezrite si nasledovné polia:

- Stav poskytovania vlastného CA – Zobrazuje stav poskytovania.
    - Posledné úspešné poskytnutie dňa mm/dd/yyyy HH:MM:SS alebo
    - Posledné neúspešné poskytnutie dňa mm/dd/yyyy HH:MM:SS
  - Informácie o vlastnom CA – Zobrazuje informácie o vlastnom CA.
    - Nainštalované – Zobrazí hodnotu „CN Value”, ktorá je hodnotou CN parametra pre pole Predmet na prvom certifikáte.
    - Nainštalovaný – Zobrazuje sa, ak nie je nainštalovaný žiadny vlastný certifikát CA.
- 

## Správa profilu

Táto sekcia opisuje vytváranie konfiguračných profilov v rámci prípravy na sťahovanie. Funkcionalita funguje tak, že TFTP z lokálneho PC sa používa ako metóda opätovnej synchronizácie, použiť sa však môže aj HTTP alebo HTTPS.

## Skomprimovanie otvoreného profilu pomocou aplikácie Gzip

Konfiguračný profil vo formáte XML sa môže stať dosť veľkým v prípade, že sa v profile jednotlivu určia všetky parametre. Aby sa znížilo zaťaženie poskytujúceho servera, telefón podporuje komprimovanie súborov XML pomocou kompresného formátu DEFLATE podporovanom pomôckou gzip (RFC 1951).



**Poznámka** Aby telefón dokázal rozpoznať skomprimovaný a zašifrovaný profil XML, kompresia sa musí uskutočniť pred šifrovaním.

Kvôli integrácii prispôbených backendových riešení pre poskytovací server sa na komprimovanie profilu namiesto samostatnej pomôcky `gzip` môže používať komprimačná knižnica `zlib` s otvoreným zdrojovým kódom. Telefón však očakáva, že súbor bude obsahovať platnú hlavičku pomôcky `gzip`.

### Procedúra

**Krok 1** Nainštalujte pomôcku `gzip` na miestny PC.

**Krok 2** Skomprimujte konfiguračný profil `basic.txt` (opísaný v [Opätovná synchronizácia s TFTP, na strane 47](#)) tak, že z príkazového riadku spustíte `gzip`:

```
gzip basic.txt
```

Tým vygenerujete súbor `basic.txt.gz` skomprimovaný pomocou algoritmu DEFLATE.

**Krok 3** Súbor `basic.txt.gz` uložte v hlavnom virtuálnom adresári servera TFTP.

**Krok 4** Upravte `Profile_Rule` na testovacom zariadení, aby sa skomprimovaný súbor opätovne synchronizoval na miesto pôvodného súboru XML tak, ako je to znázornené na nasledujúcom príklade:

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

**Krok 5** Kliknite na možnosť **Odoslať všetky zmeny**.

**Krok 6** Pozorujte `syslog` správy z telefónu.

Po opätovnej synchronizácii telefón stiahne nový súbor a použije ho na aktualizáciu svojich parametrov.

### Príbuzné témy

[Skomprimovanie otvoreného profilu](#), na strane 18

## Šifrovanie profilu pomocou OpenSSL

Skomprimovaný alebo neskomprimovaný profil je možné zašifrovať (kompresia súboru však musí prebehnúť pred šifrovaním). Šifrovanie je užitočné v prípade, že sa dbá na dôvernosť informácií v profile, napríklad pri využívaní HTTP alebo TFTP na komunikáciu medzi telefónom a poskytovacím serverom.

Telefón podporuje šifrovanie symetrickým kľúčom pomocou 256-bitového algoritmu AES. Toto šifrovanie sa môže uskutočniť s použitím balíka OpenSSL s otvoreným kódom.

### Procedúra

**Krok 1** Nainštalujte OpenSSL na miestny PC. Môže sa vyžadovať rekompilácia aplikácie OpenSSL, aby podporovala AES.

- Krok 2** Pomocou konfiguračného súboru `basic.txt` (opísaného v časti [Opätovná synchronizácia s TFTP, na strane 47](#)) vygenerujte zašifrovaný súbor pomocou nasledovného príkazu:

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

Tiež je možné použiť skomprimovaný súbor `basic.txt.gz` vytvorený v [Skomprimovanie otvoreného profilu pomocou aplikácie Gzip, na strane 60](#), pretože profil XML môže byť skomprimovaný a zároveň zašifrovaný.

- Krok 3** Uložte zašifrovaný súbor `basic.cfg` v hlavnom virtuálnom adresári servera TFTP.
- Krok 4** Upravte `Profile_Rule` na testovacom zariadení, aby sa zašifrovaný súbor znova synchronizoval na miesto pôvodného súboru XML. Šifrovací kľúč sa prístupní telefónu pomocou tejto možnosti URL:

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

- Krok 5** Kliknite na možnosť **Odoslať všetky zmeny**.

- Krok 6** Pozorujte syslog správy z telefónu.

Po opätovnej synchronizácii telefón stiahne nový súbor a použije ho na aktualizáciu svojich parametrov.

---

#### Príbuzné témy

[Šifrovanie AES-256-CBC](#), na strane 18

## Vytváranie rozdelených profilov

Telefón sťahuje počas každej opätovnej synchronizácie viacero jednotlivých profilov. Vďaka tomu je možné spravovať rôzne druhy profilových informácií na jednotlivých serveroch a udržiavať spoločné hodnoty parametrov konfigurácie, ktoré sú oddelené od hodnôt pre konkrétne kontá.

#### Procedúra

---

- Krok 1** Vytvorte nový profil XML `basic2.txt`, ktorý určuje hodnotu parametra, ktorý ho odlišuje od minulých cvičení. Napríklad k profilu `basic.txt` pridajte:

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

- Krok 2** Profil `basic2.txt` uložte v hlavnom virtuálnom adresári servera TFTP.

- Krok 3** Prvé pravidlo profilu z minulých cvičení nechajte v priečinku, ale konfigurujte druhé pravidlo profilu (`Profile_Rule_B`) tak, aby odkazovalo na nový súbor:

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

- Krok 4** Kliknite na možnosť **Odoslať všetky zmeny**.

Telefón sa teraz vždy pri opätovnej synchronizácii bude opätovne synchronizovať s prvým aj druhým profilom (v tomto poradí).

**Krok 5** Skontrolujte v správe systémového denníka, či prebehlo očakávané správanie.

---

## Nastavenie hlavičky súkromia telefónu

Hlavička súkromia používateľa v správe SIP určuje požiadavky v oblasti ochrany súkromia používateľa kladené na dôveryhodnú sieť.

Hodnotu hlavičky súkromia používateľa pre každú linku môžete nastaviť prostredníctvom značky XML v súbore `config.xml`.

Možnosti hlavičky súkromia sú:

- Disabled (predvolená hodnota)
- none – používateľ požaduje, aby služba ochrany súkromia neaplikovala žiadne funkcie ochrany súkromia na túto správu SIP.
- header – používateľ požaduje, aby služba ochrany súkromia zamaskovala hlavičky, z ktorých nemožno úplne odstrániť identifikačné informácie.
- session – používateľ požaduje, aby služba ochrany súkromia zabezpečila anonymitu relácií.
- user – používateľ požaduje úroveň ochrany súkromia iba podľa sprostredkovateľov.
- ID – používateľ požaduje, aby systém poskytol ID, na základe ktorého nemožno zistiť jeho adresu IP alebo názov hostiteľa.

### Procedúra

---

**Krok 1** Upravte súbor `config.xml` telefónu v textovom editore alebo editore XML.

**Krok 2** Vložte hlavičku `<Privacy_Header_N_ua="na">hodnota</Privacy_Header_N_>`, kde N predstavuje číslo linky (1 až 10), a uveďte niektorú z nasledujúcich hodnôt.

- Predvolená hodnota: **Disabled**
- **none**
- **header**
- **session**
- **user**
- **id**

**Krok 3** (voliteľné) Ďalšie linky môžete pridať použitím rovnakej značky s požadovaným číslom linky.

**Krok 4** Uložte zmeny do súboru `config.xml`.

---





## KAPITOLA 5

# Parametre poskytovania

- [Prehľad parametrov poskytovania, na strane 65](#)
- [Parametre konfiguračného profilu, na strane 65](#)
- [Parametre aktualizácie firmvéru, na strane 70](#)
- [Parametre na všeobecné účely, na strane 72](#)
- [Premenné rozvoja makier, na strane 72](#)
- [Kódy interných chýb, na strane 75](#)

## Prehľad parametrov poskytovania

Každá príručka opisuje parametre poskytovania, ktoré je možné použiť v skriptoch konfiguračného profilu.

## Parametre konfiguračného profilu

Nasledovná tabuľka definuje funkcie a použitie každého parametra v sekcii **Parametre konfiguračného profilu** na karte **Poskytovanie**.

Názov parametra	Opis a predvolená hodnota
Povoliť poskytovanie	Spravuje všetky aktivity opätovnej synchronizácie nezávisle od aktivít aktualizácie firmvéru. Ak chcete povoliť vzdialené poskytovanie, nastavte ho na <b>Áno</b> . Predvolená hodnota je <b>Áno</b> .
Po reštarte opätovne synchronizovať	Po každom reštarte s výnimkou reštartov spôsobených aktualizáciou parametrov a firmvéru spustí opätovnú synchronizáciu. Predvolená hodnota je <b>Áno</b> .

Názov parametra	Opis a predvolená hodnota
Náhodné oneskorenie opätovnej synchronizácie	<p>Náhodné oneskorenie po spustení pred reštartovaním, určené v sekundách. V skupine telefonických IP zariadení, ktoré sa majú zapínať naraz, vytvára rozostup v požiadavkách o opätovnú synchronizáciu, ktoré jednotky posielajú na poskytovací server. Táto funkcia môže byť užitočná vo veľkom obytnom nasadení v prípade výpadku energie v regióne.</p> <p>Hodnota v tomto poli musí byť celé číslo v rozsahu od 0 do 65535.</p> <p>Predvolená hodnota je 2.</p>
Opätovná synchronizácia o (HHmm)	<p>Čas (HHmm), kedy sa zariadenie opätovne synchronizuje s poskytujúcim serverom.</p> <p>Hodnota v tomto poli musí byť štvorciferné číslo v rozsahu od 0000 do 2400 predstavujúca čas vo formáte HHmm. Napríklad hodnota 0959 značí čas 09:59.</p> <p>Predvolená hodnota je prázdna. Ak hodnota nie je platná, parameter sa ignoruje. Ak má tento parameter nastavenú platnú hodnotu, parameter Pravidelná opätovná synchronizácia sa ignoruje.</p>
Opätovná synchronizácia s náhodným oneskorením	<p>Zabraňuje preťaženiu poskytovacieho servera pri súčasnom zapnutí veľkého množstva zariadení.</p> <p>Aby sa predišlo veľkému množstvu žiadostí o opätovnú synchronizáciu z rôznych telefónov na server, telefón sa opätovne synchronizuje v rozsahu hodín a minút a hodín a minút plus náhodné oneskorenie (hhmm, hhmm + náhodné oneskorenie). Napríklad ak náhodné oneskorenie = (Opätovná synchronizácia s náhodným oneskorením + 30)/60 minút, zadaná hodnota v sekundách sa prepočíta na minúty a zaokrúhli sa nahor pre výpočet výsledného intervalu oneskorenia.</p> <p>Platné hodnoty sú v rozsahu od 0 do 65535.</p> <p>Keď je parameter nastavený na nulu, táto funkcia je vypnutá. Predvolená hodnota je 600 sekúnd (10 minút).</p>



Názov parametra	Opis a predvolená hodnota
Pravidelná opätovná synchronizácia	<p>Časový interval pravidelných opätovných synchronizácií s poskytovacím serverom. Pridružený časovač opätovnej synchronizácie je aktívny iba po prvej úspešnej synchronizácii so serverom.</p> <p>Platné formáty:</p> <ul style="list-style-type: none"> <li>• Celé číslo <p>Príklad: zadaná hodnota <b>3000</b> značí, že ďalšia opätovná synchronizácia sa vykoná o 3000 sekúnd.</p> </li> <li>• Viacero celých čísel <p>Príklad: zadaná hodnota <b>600 , 1200 , 300</b> značí, že prvá opätovná synchronizácia sa vykoná o 600 sekúnd, druhá opätovná synchronizácia 1200 sekúnd po prvej a tretia opätovná synchronizácia sa vykoná 300 sekúnd po druhej.</p> </li> <li>• Časový rozsah <p>Príklad: zadaná hodnota <b>2400+30</b> značí, že ďalšia opätovná synchronizácia sa vykoná v čase 2400 až 2430 sekúnd po úspešnej opätovnej synchronizácii.</p> </li> </ul> <p>Nastavením parametra na nulu pravidelnú opätovnú synchronizáciu vypnete.</p> <p>Predvolená hodnota je 3600 sekúnd.</p>

Názov parametra	Opis a predvolená hodnota
Oneskorenie ďalšieho pokusu po chybe opätovnej synchronizácie	<p>Ak operácia opätovnej synchronizácie zlyhala, pretože telefonické IP zariadenie nebolo schopné načítať profil zo servera, ak je stiahnutý súbor poškodený alebo ak sa stane interná chyba, zariadenie sa po časovom intervale (určenom v sekundách) znova pokúsi o opätovnú synchronizáciu.</p> <p>Platné formáty:</p> <ul style="list-style-type: none"> <li>• Celé číslo <p>Príklad: zadaná hodnota <b>300</b> značí, že ďalší pokus o opätovnú synchronizáciu sa vykoná o 300 sekúnd.</p> </li> <li>• Viacero celých čísel <p>Príklad: zadaná hodnota <b>600 , 1200 , 300</b> značí, že prvý opakovaný pokus sa vykoná o 600 sekúnd, druhý opakovaný pokus 1200 sekúnd po zlyhaní prvého a tretí opakovaný pokus sa vykoná 300 sekúnd po zlyhaní druhého.</p> </li> <li>• Časový rozsah <p>Príklad: zadaná hodnota <b>2400+30</b> značí, že ďalší opakovaný pokus sa vykoná v čase 2400 až 2430 sekúnd po zlyhaní opätovnej synchronizácie.</p> </li> </ul> <p>Ak je oneskorenie nastavené na 0, zariadenie sa po prvom neúspešnom pokuse o opätovnú synchronizáciu nebude pokúšať znova.</p>
Vynútené oneskorenie opätovnej synchronizácie	<p>Maximálne oneskorenie (v sekundách) pred uskutočnením opätovnej synchronizácie.</p> <p>Kým je telefónna linka aktívna, zariadenie sa nesynchronizuje. Keďže opätovná synchronizácia môže trvať niekoľko sekúnd, je vhodné pred ňou zabezpečiť, aby bolo zariadenie dlhšiu dobu nečinné. Vďaka tomu bude používateľ môcť uskutočňovať hovory bez prerušenia.</p> <p>Zariadenie má časovač, ktorý spustí odpočítavanie, keď sú všetky jeho linky nečinné. Tento parameter je počiatočnou hodnotou časovača. Udalosti opätovnej synchronizácie sú odložené, až kým sa odpočítavanie dostane na nulu.</p> <p>Platné hodnoty sú v rozsahu od 0 do 65535.</p> <p>Predvolená hodnota je 14,400 sekúnd.</p>

Názov parametra	Opis a predvolená hodnota
Opätovná synchronizácia z protokolu SIP	Umožňuje, aby opätovnú synchronizáciu spustila správa NOTIFY z protokolu SIP. Predvolená hodnota je <b>Áno</b> .
Opätovná synchronizácia po pokuse o aktualizáciu	Povoľuje alebo zakazuje operáciu opätovnej synchronizácie po uskutočnení akejkoľvek aktualizácie. Ak je vybraná možnosť <b>Áno</b> , spustí sa synchronizácia. Predvolená hodnota je <b>Áno</b> .
Spúšťač opätovnej synchronizácie 1, spúšťač opätovnej synchronizácie 2	Konfigurovateľné podmienky spúšťača opätovnej synchronizácie. Opätovná synchronizácia sa spustí, keď sa logická rovnica týchto parametrov bude rovnať hodnote <b>TRUE</b> . Predvolená hodnota je (prázdne).
Zlyhanie opätovnej synchronizácie – FNF	Ak požadovaný profil nebol prijatý od servera, opätovná synchronizácia sa považuje za neúspešnú. Toto nastavenie môže byť prepísané týmto parametrom. Ak je vybraná možnosť <b>Nie</b> , zariadenie prijme odpoveď servera <i>file-not-found</i> (súbor nebol nájdený) ako úspešnú opätovnú synchronizáciu. Predvolená hodnota je <b>Áno</b> .
Pravidlo profilu Pravidlo profilu B Pravidlo profilu C Pravidlo profilu D	Každé pravidlo profilu informuje telefón o zdroji, z ktorého má získať profil (konfiguračný súbor). Pri každej operácii opätovnej synchronizácie telefón aplikuje všetky profily v poradí. Predvolené: <b>/\$PSN.xml</b> Ak chcete aplikovať šifrovanie AES-256-CBC na konfiguračné súbory, zadajte šifrovací kľúč s voľbou <b>--key</b> nasledovne: <b>[--key &lt;šifrovací kľúč&gt;]</b> Ak chcete, šifrovací kľúč môžete uzavrieť do úvodzoviek (").
Použitie možnosti DHCP	Možnosti DHCP oddelené čiarkami používané na načítanie firmvéru a profilov. Predvolená hodnota je 66,160,159,150,60,43,125.

Názov parametra	Opis a predvolená hodnota
Denníková správa o žiadosti	Tento parameter obsahuje správu, ktorá je zaslaná serveru systémového denníka na začiatku pokusu o opätovnú synchronizáciu. Predvolená hodnota je <code>\$PN \$MAC -Requesting % \$SCHEME://\$SERVIP:\$PORT\$PATH</code> .
Denníková správa o úspechu	Správa systémového denníka vyslaná po úspešnom dokončení pokusu o opätovnú synchronizáciu. Predvolená hodnota je <code>\$PN \$MAC -Successful Resync % \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR</code> .
Denníková správa o zlyhaní	Správa systémového denníka vyslaná po neúspešnom dokončení pokusu o opätovnú synchronizáciu. Predvolená hodnota je <code>\$PN \$MAC -- Resync failed: \$ERR</code> .
Opätovná synchronizácia konfigurovateľná používateľom	Umožňuje používateľovi opätovne synchronizovať telefón z obrazovky IP telefónu. Predvolená hodnota je <code>Áno</code> .

## Parametre aktualizácie firmvéru

Nasledovná tabuľka definuje funkcie a použitie každého parametra v sekcii **Aktualizácia firmvéru** na karte **Poskytovanie**.

Názov parametra	Opis a predvolená hodnota
Povoliť aktualizáciu	Povolí všetky operácie aktualizácie firmvéru bez ohľadu na akcie opätovnej synchronizácie. Predvolená hodnota je <code>Áno</code> .
Oneskorenie ďalšieho pokusu po chybe	Interval uskutočnenia ďalšieho pokusu (v sekundách) v prípade zlyhania aktualizácie. Zariadenie má časovač aktualizácie firmvéru, ktorý sa spustí po zlyhaní pokusu o aktualizáciu firmvéru. Časovač sa začne odpočítavať na hodnote uvedenej v tomto parametri. Keď sa odpočítavanie dostane na nulu, uskutoční sa ďalší pokus o aktualizáciu firmvéru. Predvolená hodnota je <code>3600</code> sekúnd.

Názov parametra	Opis a predvolená hodnota
Pravidlo aktualizácie	<p>Skript aktualizácie firmvéru, ktorý definuje podmienky aktualizácie a pridružené URL firmvéru. Používa rovnakú syntax ako pravidlo profilu.</p> <p>Na zadanie pravidla aktualizácie používajte nasledovný formát:</p> <pre>&lt;tftp http https&gt;://&lt;adresa ip&gt;/obraz/&lt;názov načítania&gt;</pre> <p>Príklad:</p> <pre>tftp://192.168.1.5/obraz/sip68x.11-0-IMP-EN.loads</pre> <p>Ak nie je určený žiadny protokol, predpokladá sa TFTP. Ak nie je určený žiadny názov servera, hostiteľ si vyžiada URL, ktoré sa použije ako názov servera. Ak nie je určený žiadny port, použije sa predvolený port (69 pre TFTP, 80 pre HTTP alebo 443 pre HTTPS).</p> <p>Predvolená hodnota je prázdna.</p>
Denníková správa o žiadosti o aktualizáciu	<p>Správa denníka systému vyslaná na začiatku pokusu o aktualizáciu firmvéru.</p> <p>Predvolená hodnota: \$PN \$MAC -- Requesting upgrade \$SCHEME://\$SERVIP:\$PORT\$PATH.</p>
Denníková správa o úspechu aktualizácie	<p>Správa denníka systému po úspešnom dokončení aktualizácie firmvéru.</p> <p>Predvolená hodnota je \$PN \$MAC -- Successful upgrade \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR.</p>
Denníková správa o zlyhaní aktualizácie	<p>Správa denníka systému po neúspešnom dokončení aktualizácie firmvéru.</p> <p>Predvolená hodnota je \$PN \$MAC -- Upgrade failed: \$ERR.</p>
Zdieľanie verzie SW v skupine	<p>Zapne alebo vypne funkciu Zdieľanie verzie SW v skupine. Výberom možnosti <b>Áno</b> alebo <b>Nie</b> zapnete, respektíve vypnete túto funkciu.</p> <p>Predvolená hodnota: Áno</p>
Server zapisovania do denníka funkcie Zdieľanie verzie SW v skupine	<p>Určuje adresu IP a port, kam sa má poslať správa UDP.</p> <p>Napríklad: 10.98.76.123:514, kde 10.98.76.123 je adresa IP a 514 je číslo portu.</p>

## Parametre na všeobecné účely

Nasledovná tabuľka definuje funkcie a použitie každého parametra v sekcii **Parametre na všeobecné účely** na karte **Poskytovanie**.

Názov parametra	Opis a predvolená hodnota
GPP A – GPP P	<p>Parametre na všeobecné účely GPP_* sa používajú ako register voľných reťazcov pri konfigurácii telefónov pre interakciu s konkrétnym riešením poskytovacieho servera. Môžu byť nakonfigurované, aby obsahovali rôzne hodnoty, napríklad:</p> <ul style="list-style-type: none"> <li>• Šifrovacie kľúče.</li> <li>• Adresy URL.</li> <li>• Informácie o stave viacstupňového poskytovania.</li> <li>• Šablóny požiadavky post.</li> <li>• Mapy aliasov názvov parametrov.</li> <li>• Čiastočné hodnoty reťazcov, ktoré sa nakoniec spoja a vytvoria kompletne hodnoty parametrov.</li> </ul> <p>Predvolená hodnota je prázdna.</p>

## Premenné rozvoja makier

Niektoré premenné makier sú rozpoznávané v nasledovných poskytovacích parametroch:

- Profile\_Rule
- Profile\_Rule\_\*
- Resync\_Trigger\_\*
- Upgrade\_Rule
- Log\_\*
- GPP\_\* (v určených podmienkach)

V týchto parametroch sa rozpoznávajú a rozvíjajú typy syntaxe ako napríklad \$NAME alebo \$(NAME).

Podreťazce premennej makra môžu byť určené v zápise \$(NAME:p) a \$(NAME:p:q), kde p a q sú nezáporné celé čísla (dostupné vo verzii 2.0.11 a vyššej). Výsledný rozvoj makra je podreťazec, ktorý začína na umiestnení určenom znakom p s dĺžkou q (alebo s dĺžkou do konca reťazca ak q nie je určené). Napríklad GPP\_A obsahuje ABCDEF, takže \$(A:2) sa rozvinie na CDEF a \$(A:2:3) sa rozvinie na CDE.

Nerozpoznaný názov sa nepreloží a tvar \$(NAME) alebo \$(NAME) sa v hodnote parametra po rozvoji nezmení.

Názov parametra	Opis a predvolená hodnota
\$	Tvar \$\$ sa rozvinie na jediný znak \$.
A až P	Nahradené obsahom parametrov pre všeobecné účely GPP_A až GPP_P.
SA až SD	Nahradené obsahom parametrov pre špeciálne účely GPP_SA až GPP_SD. Tieto parametre obsahujú kľúče alebo heslá používané počas poskytovania.  <b>Poznámka</b> \$SA až \$SD sa považujú za argumenty voliteľného kvalifikátora URL opätovnej synchronizácie – kľúča.
MA	Adresa MAC s použitím cifier v šestnástkovej sústave s malými písmenami, napríklad 000e08aabbcc.
MAU	Adresa MAC s použitím cifier v šestnástkovej sústave s veľkými písmenami, napríklad 000E08AABBCC.
MAC	Adresa MAC s použitím cifier v šestnástkovej sústave s malými písmenami (a dvojbodkami na oddelenie párov cifier v šestnástkovej sústave). Napríklad 00:0e:08:aa:bb:cc.
PN	Názov produktu. Napríklad CP-6841-3PCC.
PSN	Číslo série produktu. Napríklad 6841-3PCC.
SN	Reťazec sériového čísla, napríklad 88012BA01234.
CCERT	Stav certifikátu klienta SSL: Nainštalovaný alebo nenainštalovaný.
IP	Adresa IP telefónu v rámci jeho miestnej podsiete. Napríklad 192.168.1.100.
EXTIP	Externá adresa IP telefónu, ktorá je uvedená na internete. Napríklad 66.43.16.52.
SWVER	Reťazec verzie softvéru. Napríklad sip68xx.11-0-1MPP.
HWVER	Reťazec verzie hardvéru. Napríklad 2.0.1.
PRVST	Stav poskytovania (číselný reťazec): -1 = explicitná žiadosť o opätovnú synchronizáciu 0 = opätovná synchronizácia pri spustení 1 = pravidelná opätovná synchronizácia 2 = opätovná synchronizácia zlyhala, skúsiť znova

Názov parametra	Opis a predvolená hodnota
UPGST	Stav aktualizácie (číselný reťazec): 1 = prvý pokus o aktualizáciu 2 = aktualizácia zlyhala, skúsiť znova
UPGERR	Výsledná správa (ERR) posledného pokusu o aktualizáciu, napríklad http_get zlyhalo.
PRVTMR	Počet sekúnd od posledného pokusu o opätovnú synchronizáciu.
UPGTMR	Počet sekúnd od posledného pokusu o aktualizáciu.
REGTMR1	Počet sekúnd, odkedy Linka 1 stratila registráciu na serveri SIP.
REGTMR2	Počet sekúnd, odkedy Linka 2 stratila registráciu na serveri SIP.
UPGCOND	Pôvodný názov makra.
SCHEME	Schéma prístupu k súboru (TFTP, HTTP alebo HTTPS), ktorá bola získaná pri analýze opätovnej synchronizácie alebo URL aktualizácie.
SERV	Názov hostiteľa servera, ktorý bol cieľom požiadavky, získaný pri analýze opätovnej synchronizácie alebo URL aktualizácie.
SERVIP	Názov adresy IP servera, ktorá bola cieľom požiadavky, získaný pri analýze opätovnej synchronizácie alebo URL aktualizácie, prípadne po vyhľadávaní DNS
PORT	Názov portu UDP/TCP, ktorý bol cieľom požiadavky, získaný pri analýze opätovnej synchronizácie alebo URL aktualizácie.
PATH	Názov cesty súboru, ktorý bol cieľom požiadavky, získaný pri analýze opätovnej synchronizácie alebo URL aktualizácie.
ERR	Výsledná správa o opätovnej synchronizácii alebo pokuse o aktualizáciu. Užitočná len pre generovaní výsledných správ systémového denníka. Hodnota je uložená v premennej UPGERR pre prípad pokusov o aktualizáciu.
UIDn	Obsah parametra konfigurácie ID používateľa Linky n.
EMS	Stav služby Extension mobility



Názov parametra	Opis a predvolená hodnota
MUID	ID používateľa služby Extension Mobility
MPWD	Heslo služby Extension Mobility

## Kódy interných chýb

Telefón definuje niekoľko kódov interných chýb (X00 – X99), aby sa uľahčila konfigurácia poskytovania podrobného riadenia správania jednotky v určitých chybových podmienkach.

Názov parametra	Opis a predvolená hodnota
X00	Chyba transportnej vrstvy (alebo ICMP) pri odosielaní žiadosti SIP.
X20	Žiadosť SIP vyprší pri čakaní na odpoveď.
X40	Všeobecná chyba protokolu SIP (napríklad neprijateľný codec v SDP v správach 200 a ACK alebo vypršanie pri čakaní na ACK).
X60	Vytočené číslo je podľa plánu vytáčania neplatné.





## DODATOK **A**

# Príklady konfiguračných profilov

- [Príklad otvoreného formátu XML, na strane 77](#)

## Príklad otvoreného formátu 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>
```

```

<!-- 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_SSIPv3 ua="na">No</Enable_SSIPv3>
<Use_Config_TOS ua="na">No</Use_Config_TOS>
<!-- VLAN Settings -->
<Enable_VLAN ua="rw">No</Enable_VLAN>
<VLAN_ID ua="rw">1</VLAN_ID>
<PC_Port_VLAN_ID ua="na">1</PC_Port_VLAN_ID>
<Enable_CDP ua="na">Yes</Enable_CDP>
<Enable_LLDP-MED ua="na">Yes</Enable_LLDP-MED>
<Network_Startup_Delay ua="na">3</Network_Startup_Delay>
<DHCP_VLAN_Option ua="na"/>
<!-- Wi-Fi Settings -->
<!-- Wi-Fi Profile 1 -->
<!-- Wi-Fi Profile 2 -->
<!-- Wi-Fi Profile 3 -->
<!-- Wi-Fi Profile 4 -->
<!-- Inventory Settings -->
<Asset_ID ua="na"/>
<!-- SIP Parameters -->
<Max_Forward ua="na">70</Max_Forward>
<Max_Redirection ua="na">5</Max_Redirection>
<Max_Auth ua="na">2</Max_Auth>
<SIP_User_Agent_Name ua="na">$VERSION</SIP_User_Agent_Name>
<SIP_Server_Name ua="na">$VERSION</SIP_Server_Name>
<SIP_Reg_User_Agent_Name ua="na"/>
<SIP_Accept_Language ua="na"/>
<DTMF_Relay_MIME_Type ua="na">application/dtmf-relay</DTMF_Relay_MIME_Type>
<Hook_Flash_MIME_Type ua="na">application/hook-flash</Hook_Flash_MIME_Type>
<Remove_Last_Reg ua="na">No</Remove_Last_Reg>
<Use_Compact_Header ua="na">No</Use_Compact_Header>
<Escape_Display_Name ua="na">No</Escape_Display_Name>
<Talk_Package ua="na">No</Talk_Package>
<Hold_Package ua="na">No</Hold_Package>

```

```

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

```

```

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

```

```

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

```

```

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

```



```

<!--
  available options:
  -----
-->
<Time_Offset_HH_mm_ua="na">-00/08</Time_Offset_HH_mm_>
<Ignore_DHCP_Time_Offset_ua="na">Yes</Ignore_DHCP_Time_Offset>
<Daylight_Saving_Time_Rule
ua="na">start=3/-1/7/2;end=10/-1/7/2;save=1</Daylight_Saving_Time_Rule>
<Daylight_Saving_Time_Enable_ua="na">Yes</Daylight_Saving_Time_Enable>
  <!-- Language -->
<Dictionary_Server_Script_ua="na"/>
<Language_Selection_ua="na">English-US</Language_Selection>
<Locale_ua="na">en-US</Locale>
<!--
  available options:
  -----
-->
  <!-- General -->
<Station_Name_ua="na">arupiSSomSok</Station_Name>
<Station_Display_Name_ua="na">RCDN Time</Station_Display_Name>
<Voice_Mail_Number_ua="na"/>
<WideBand_Handset_Enable_ua="na">No</WideBand_Handset_Enable>
  <!-- Video Configuration -->
  <!-- Handsfree -->
<Bluetooth_Mode_ua="na">Phone</Bluetooth_Mode>
<!-- available options: Phone|Handsfree|Both -->
<Line_ua="na">5</Line>
<!--
  available options: 1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|Disabled
-->
<Extension_1_ua="na">1</Extension_1_>
<!-- available options: 1|2|3|4|Disabled -->
<Short_Name_1_ua="na">$USER hot</Short_Name_1_>
<Share_Call_Appearance_1_ua="na">private</Share_Call_Appearance_1_>
<!-- available options: private|shared -->
<Extended_Function_1_ua="na"/>
<Extension_2_ua="na">2</Extension_2_>
<!-- available options: 1|2|3|4|Disabled -->
<Short_Name_2_ua="na">$USER</Short_Name_2_>
<Share_Call_Appearance_2_ua="na">private</Share_Call_Appearance_2_>
<!-- available options: private|shared -->
<Extended_Function_2_ua="na"/>
<Extension_3_ua="na">3</Extension_3_>
<!-- available options: 1|2|3|4|Disabled -->
<Short_Name_3_ua="na">$USER</Short_Name_3_>
<Share_Call_Appearance_3_ua="na">private</Share_Call_Appearance_3_>
<!-- available options: private|shared -->
<Extended_Function_3_ua="na"/>
<Extension_4_ua="na">4</Extension_4_>
<!-- available options: 1|2|3|4|Disabled -->
<Short_Name_4_ua="na">$USER</Short_Name_4_>
<Share_Call_Appearance_4_ua="na">private</Share_Call_Appearance_4_>
<!-- available options: private|shared -->
<Extended_Function_4_ua="na"/>
  <!-- Miscellaneous Line Key Settings -->
<Line_ID_Mapping_ua="na">Vertical First</Line_ID_Mapping>
<!-- available options: Horizontal First|Vertical First -->
<SCA_Barge-In-Enable_ua="na">No</SCA_Barge-In-Enable>
<SCA_Sticky_Auto_Line_Seize_ua="na">No</SCA_Sticky_Auto_Line_Seize>
<Call_Appearances_Per_Line_ua="na">2</Call_Appearances_Per_Line>
<!-- available options: 2|3|4|5|6|7|8|9|10 -->
  <!-- Supplementary Services -->

```

```

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

```

```

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

```

```

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

```

```

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

```

```

<CFWD_Enable_1_ua="na">No</CFWD_Enable_1_>
<!-- Audio Configuration -->
<Preferred_Codec_1_ua="na">G711u</Preferred_Codec_1_>
<!--
available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_1_ua="na">No</Use_Pref_Codec_Only_1_>
<Second_Preferred_Codec_1_ua="na">Unspecified</Second_Preferred_Codec_1_>
<!--
available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_1_ua="na">Unspecified</Third_Preferred_Codec_1_>
<!--
available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_1_ua="na">Yes</G711u_Enable_1_>
<G711a_Enable_1_ua="na">Yes</G711a_Enable_1_>
<G729a_Enable_1_ua="na">Yes</G729a_Enable_1_>
<G722_Enable_1_ua="na">Yes</G722_Enable_1_>
<G722.2_Enable_1_ua="na">Yes</G722.2_Enable_1_>
<iLBC_Enable_1_ua="na">Yes</iLBC_Enable_1_>
<OPUS_Enable_1_ua="na">Yes</OPUS_Enable_1_>
<Silence_Supp_Enable_1_ua="na">No</Silence_Supp_Enable_1_>
<DTMF_Tx_Method_1_ua="na">Auto</DTMF_Tx_Method_1_>
<!--
available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_1_ua="na">Default</Codec_Negotiation_1_>
<!-- available options: Default|List All -->
<Encryption_Method_1_ua="na">AES 128</Encryption_Method_1_>
<!-- available options: AES 128|AES 256 GCM -->
<!-- Video Configuration -->
<!-- Dial Plan -->
<Dial_Plan_1_ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|lxxx[2-9]xxxxxxS0|xxxxxxxxxxxxx.)
</Dial_Plan_1_>
<Caller_ID_Map_1_ua="na"/>
<Enable_URI_Dialing_1_ua="na">No</Enable_URI_Dialing_1_>
<Emergency_Number_1_ua="na"/>
<!-- E911 Geolocation Configuration -->
<Company_UUID_1_ua="na"/>
<Primary_Request_URL_1_ua="na"/>
<Secondary_Request_URL_1_ua="na"/>
<!-- General -->
<Line_Enable_2_ua="na">Yes</Line_Enable_2_>
<!-- Share Line Appearance -->
<Share_Ext_2_ua="na">No</Share_Ext_2_>
<Shared_User_ID_2_ua="na"/>
<Subscription_Expires_2_ua="na">3600</Subscription_Expires_2_>
<Restrict_MWI_2_ua="na">No</Restrict_MWI_2_>
<!-- NAT Settings -->
<NAT_Mapping_Enable_2_ua="na">No</NAT_Mapping_Enable_2_>
<NAT_Keep_Alive_Enable_2_ua="na">No</NAT_Keep_Alive_Enable_2_>
<NAT_Keep_Alive_Msg_2_ua="na">$NOTIFY</NAT_Keep_Alive_Msg_2_>
<NAT_Keep_Alive_Dest_2_ua="na">$PROXY</NAT_Keep_Alive_Dest_2_>
<!-- Network Settings -->
<SIP_TOS_DiffServ_Value_2_ua="na">0x68</SIP_TOS_DiffServ_Value_2_>
<RTP_TOS_DiffServ_Value_2_ua="na">0xb8</RTP_TOS_DiffServ_Value_2_>
<!-- SIP Settings -->
<SIP_Transport_2_ua="na">UDP</SIP_Transport_2_>
<!-- available options: UDP|TCP|TLS|AUTO -->
<SIP_Port_2_ua="na">5061</SIP_Port_2_>
<SIP_100REL_Enable_2_ua="na">No</SIP_100REL_Enable_2_>
<EXT_SIP_Port_2_ua="na">0</EXT_SIP_Port_2_>

```

```

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

```

```

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

```



```

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

```

```

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

```

```

-->
<G711u_Enable_3_ ua="na">Yes</G711u_Enable_3_>
<G711a_Enable_3_ ua="na">Yes</G711a_Enable_3_>
<G729a_Enable_3_ ua="na">Yes</G729a_Enable_3_>
<G722_Enable_3_ ua="na">Yes</G722_Enable_3_>
<G722.2_Enable_3_ ua="na">Yes</G722.2_Enable_3_>
<iLBC_Enable_3_ ua="na">Yes</iLBC_Enable_3_>
<OPUS_Enable_3_ ua="na">Yes</OPUS_Enable_3_>
<Silence_Supp_Enable_3_ ua="na">No</Silence_Supp_Enable_3_>
<DTMF_Tx_Method_3_ ua="na">Auto</DTMF_Tx_Method_3_>
<!--
  available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_3_ ua="na">Default</Codec_Negotiation_3_>
<!-- available options: Default|List All -->
<Encryption_Method_3_ ua="na">AES 128</Encryption_Method_3_>
<!-- available options: AES 128|AES 256 GCM -->
  <!-- Video Configuration -->
  <!-- Dial Plan -->
  <Dial_Plan_3_ ua="na">
  (*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxS0|xxxxxxxxxxxxx.)
  </Dial_Plan_3_>
  <Caller_ID_Map_3_ ua="na"/>
  <Enable_URI_Dialing_3_ ua="na">No</Enable_URI_Dialing_3_>
  <Emergency_Number_3_ ua="na"/>
  <!-- E911 Geolocation Configuration -->
  <Company_UUID_3_ ua="na"/>
  <Primary_Request_URL_3_ ua="na"/>
  <Secondary_Request_URL_3_ ua="na"/>
  <!-- General -->
  <Line_Enable_4_ ua="na">Yes</Line_Enable_4_>
  <!-- Share Line Appearance -->
  <Share_Ext_4_ ua="na">No</Share_Ext_4_>
  <Shared_User_ID_4_ ua="na"/>
  <Subscription_Expires_4_ ua="na">3600</Subscription_Expires_4_>
  <Restrict_MWI_4_ ua="na">No</Restrict_MWI_4_>
  <!-- NAT Settings -->
  <NAT_Mapping_Enable_4_ ua="na">No</NAT_Mapping_Enable_4_>
  <NAT_Keep_Alive_Enable_4_ ua="na">No</NAT_Keep_Alive_Enable_4_>
  <NAT_Keep_Alive_Msg_4_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_4_>
  <NAT_Keep_Alive_Dest_4_ ua="na">$PROXY</NAT_Keep_Alive_Dest_4_>
  <!-- Network Settings -->
  <SIP_TOS_DiffServ_Value_4_ ua="na">0x68</SIP_TOS_DiffServ_Value_4_>
  <RTP_TOS_DiffServ_Value_4_ ua="na">0xb8</RTP_TOS_DiffServ_Value_4_>
  <!-- SIP Settings -->
  <SIP_Transport_4_ ua="na">UDP</SIP_Transport_4_>
  <!-- available options: UDP|TCP|TLS|AUTO -->
  <SIP_Port_4_ ua="na">5063</SIP_Port_4_>
  <SIP_100REL_Enable_4_ ua="na">No</SIP_100REL_Enable_4_>
  <EXT_SIP_Port_4_ ua="na">0</EXT_SIP_Port_4_>
  <Auth_Resync-Reboot_4_ ua="na">Yes</Auth_Resync-Reboot_4_>
  <SIP_Proxy-Require_4_ ua="na"/>
  <SIP_Remote-Party-ID_4_ ua="na">No</SIP_Remote-Party-ID_4_>
  <Referor_Bye_Delay_4_ ua="na">4</Referor_Bye_Delay_4_>
  <Refer-To_Target_Contact_4_ ua="na">No</Refer-To_Target_Contact_4_>
  <Referee_Bye_Delay_4_ ua="na">0</Referee_Bye_Delay_4_>
  <Refer_Target_Bye_Delay_4_ ua="na">0</Refer_Target_Bye_Delay_4_>
  <Sticky_183_4_ ua="na">No</Sticky_183_4_>
  <Auth_INVITE_4_ ua="na">No</Auth_INVITE_4_>
  <Ntfy_Refer_On_lxx-To-Inv_4_ ua="na">Yes</Ntfy_Refer_On_lxx-To-Inv_4_>
  <Set_G729_annexb_4_ ua="na">yes</Set_G729_annexb_4_>
  <!--
  available options: none|no|yes|follow silence supp setting
-->

```

```

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

```

```

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

```

```

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

```

```

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

```

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





## DODATOK **B**

### Skratky

---

- [Skratky, na strane 99](#)

### Skratky

AC	Striedavý prúd
ACS	Access Control Server
A/D	Konvertor z analógu na digitál
AES	Advanced Encryption Standard
ANC	Anonymný hovor
AP	Prístupový bod
ASCII	American Standard Code for Information Interchange
B2BUA	Používateľ-Agent typu back-to-back
BLF	Pole obsadenia linky
Bool	Hodnoty typu Boolean. Určené v profile ako áno a nie alebo 1 a 0.
BootP	Bootstrap Protocol
CA	Certifikačný úrad
CAS	Signál výstrahy CPE
CDP	Cisco Discovery Protocol
CDR	Záznam s podrobnosťami o hovore
CGI	Computer-Generated Imagery (počítačom generované obrazy)
CID	ID volajúceho
CIDCW	ID volajúceho pre čakajúci hovor

CNG	Generovanie príjemného zvuku
CPC	Riadenie volajúceho účastníka
CPE	Vybavenie u zákazníka
CSV	Hodnoty oddelené čiarkou
CWCID	ID volajúceho pre čakajúci hovor
CWT	Tón čakajúceho hovoru
D/A	Konvertor z digitálu na analóg
dB	decibel
dBm	dB s ohľadom na 1 miliwatt
DHCP	Protokol dynamickej konfigurácie hostiteľa
DND	Nevyrušovať
DNS	Systém názvov domén
DoS	Odmietnutie služby
DRAM	Dynamická pamäť s priamym prístupom
DSL	Slučka digitálneho predplatiteľa
DSP	Digitálny signálový procesor
DST	Letný čas
DTAS	Výstražný signál dátového terminálu (rovnako ako CAS)
DTMF	Tónová voľba
FQDN	Úplný názov domény
FSK	Kľúčovanie frekvenčným posunom
FW	Firmvér
FXS	Stanica vzdialenej výmeny
GMT	Greenwichský čas
GW	Brána
HTML	Hypertextový značkovací jazyk
HTTP	Hypertextový prenosový protokol
HTTPS	HTTP cez SSL

ICMP	Protokol Internet Control Message Protocol
IGMP	Protokol Internet Group Management Protocol
ILEC	Výkonná miestna ústredňa
IP	Internetový protokol
IPv4	Internetový protokol verzie 4
IPv6	Internetový protokol verzie 6
ISP	Poskytovateľ internetových služieb
ITSP	Poskytovateľ telefonických internetových služieb
ITU	Medzinárodná telekomunikačná únia
IVR	Interaktívna hlasová odozva
LAN	Miestna počítačová sieť
LBR	Nízka bitová rýchlosť
LBRC	Codec s nízkou bitovou rýchlosťou
LCD	Displej z tekutých kryštálov; nazývaný aj obrazovka
LDAP	Lightweight Directory Access Protocol
LED	Svetelná dióda
MAC	Adresa Media Access Control
MC	Mini certifikát
MGCP	Protokol Media Gateway Control Protocol
MOH	Music On Hold
MOS	Priemerná známka hodnotenia (1 – 5, čím vyššia, tým lepšie hodnotenie)
MPP	Multiplatformové telefóny
ms	Milisekunda
MSA	Adaptér hudobného zdroja
MWI	Indikátor čakajúcich správ
NAT	Preklad sieťovej adresy
NPS	Normálny poskytovací server
NTP	Protokol Network Time Protocol
OOB	Mimo pásma

OSI	Interval otvoreného prepínania
PBX	Pobočková ústredňa
PCB	Doska plošných spojov
PoE	Napájanie cez Ethernet
PR	Prepólovanie
PS	Poskytovací server
PSQM	Meranie kvality vnímanej reči (1 – 5, čím nižšie, tým lepšie)
PSTN	Verejná telefónna sieť
QoS	Kvalita služby
RC	Odstránenie prispôsobenia
REQT	(SIP) Správa požiadavky
RESP	(SIP) Správa odpovede
RSC	(SIP) Kód stavu odpovede, napríklad 404, 302, 600
RTP	Protokol komunikácie v skutočnom čase
RTT	Obojsmerné oneskorenie
SAS	Streamovací audio server
SDP	Protokol opisu relácie
SDRAM	Synchrónna DRAM
sec	sekundy
SIP	Protokol SIP
SLA	Vzhľad zdieľanej linky
SLIC	Obvod rozhrania linky predplatiteľa
SP	Poskytovateľ služieb
SSL	Vrstva bezpečných soketov
STUN	UDP prechodu relácie pre NAT
TCP	Protokol Transmission Control Protocol
TFTP	Protokol Trivial File Transfer Protocol
TLS	Protokol Transport Layer Security

TTL	Životnosť
ToS	Typ služby
UA	Používateľ – Agent
uC	Mikroradič
UDP	Protokol User Datagram Protocol
URI	Uniform Resource Identifier
URL	Jednotná adresa zdroja
UTC	Koordinovaný svetový čas
VAR	Predajca s pridanou hodnotou
VLAN	Hlasová sieť LAN
VM	Hlasová pošta
VMWI	Vizuálny indikátor čakajúcich správ
VoIP	Voice over Internet Protocol
VQ	Hlasová kvalita
WAN	Rozsiahla sieť
XML	Rozšíriteľný značkovací jazyk





## DODATOK **C**

# Súvisiaca dokumentácia

---

- Súvisiaca dokumentácia, na strane 105
- Pravidlá podpory firmvéru pre IP telefóny Cisco IP Phone, na strane 105

## Súvisiaca dokumentácia

Súvisiace informácie nájdete v nasledovných sekciách.

### Dokumentácia k telefónu Cisco IP Phone radu 6800

Pracujte s publikáciami, ktoré sú špecifické pre váš jazyk, model telefónu a vydanie multiplatformového firmvéru. Začnite na nasledovnej jednotnej adrese zdroja (URL):

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

### Pravidlá podpory firmvéru pre IP telefóny Cisco IP Phone

Viac informácií o politike podpory pre telefóny nájdete v časti <https://cisco.com/go/phonefirmwaresupport>.

