Příručka zřizování pro víceplatformové telefony řady Cisco IP Phone 6800

První vydání: 2017-11-22

Poslední změna: 2019-01-30

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

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

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

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

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

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

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

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

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

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

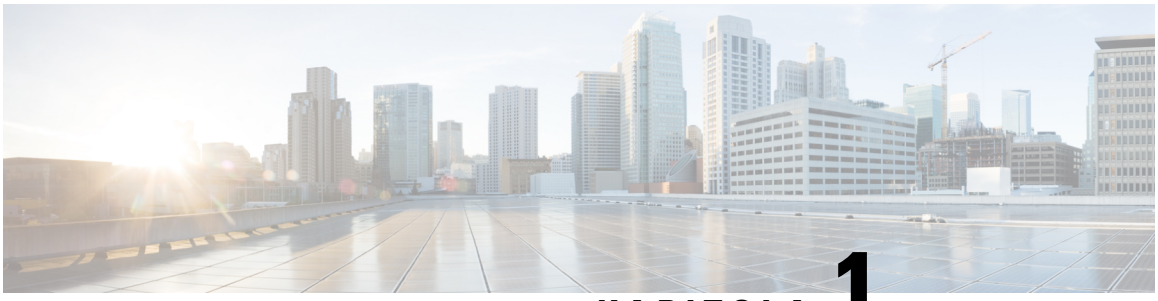
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

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

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

OBSAH



KAPITOLA 1

Nasazení a zřizování

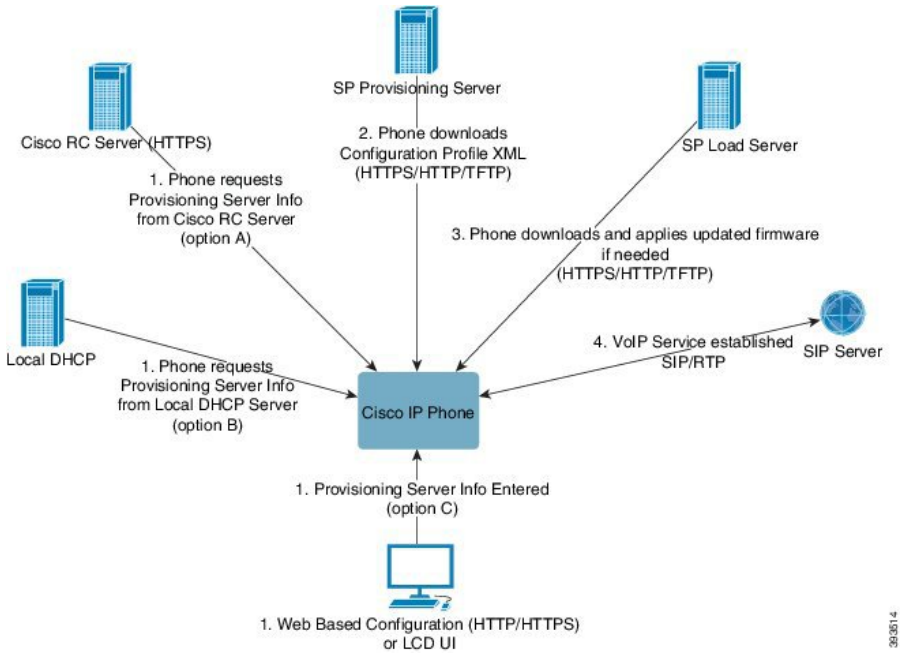
Přehled zřizování

Telefony Cisco IP Phones jsou určeny do velkoobjemových nasazení poskytovateli služeb Voice-over-IP (VoIP) pro zákazníky v domácím, firemním a podnikovém prostředí. Zřizování telefonu pomocí vzdálené správy a konfigurace tak zajišťuje správné fungování telefonu v lokalitě zákazníka.

Společnost Cisco podporuje přizpůsobenou a neustálou konfiguraci telefonu pomocí těchto funkcí:

- Spolehlivé vzdálené ovládání telefonu.
- Šifrování komunikace, která telefon ovládá.
- Zjednodušené spojování účtu telefonu.

Telefony lze zřídit tak, aby stahovaly profily konfigurace a aktualizovaný firmware ze vzdáleného serveru. Ke stažení může docházet při připojení telefonu k síti, při spuštění a v zadaných intervalech. Zřizování je obvykle součástí vysokoobjemových nasazení VoIP běžných poskytovatelů služeb. Konfigurační profily nebo aktualizovaný software jsou do telefonu přeneseny pomocí protokolu TFTP, HTTP nebo HTTPS.



Na vyšší úrovni probíhá proces zřizování telefonu takto:

1. Pokud telefon není nakonfigurován, údaje zřizovacího serveru jsou na telefon použity pomocí jedné z těchto možností:
   - **A –** Stažením ze serveru vzdáleného přizpůsobení systému Cisco EDOS (Enablement Data Orchestration System) pomocí protokolu HTTPS.
   - **B –** Získáním z místního serveru DHCP.
   - **C –** Ručním zadáním pomocí webového konfiguračního nástroje telefonu Cisco nebo přes uživatelské rozhraní telefonu.
2. Telefon údaje zřizovacího serveru stáhne a použije konfigurační soubor XML pomocí protokolu HTTPS, HTTP nebo TFTP.
3. Telefon v případě potřeby pomocí protokolu HTTPS, HTTP nebo TFTP stáhne a použije aktualizovaný firmware.
4. Služba VoIP je zavedena pomocí zadané konfigurace a firmwaru.

Poskytovatelé služeb VoIP mají v úmyslu nasadit mnoho telefonů k zákazníkům z domácností a malých firem. Ve firemním a podnikovém prostředí mohou telefony fungovat jako koncové uzly. Poskytovatelé distribuují po celém internetu tato zařízení, která jsou připojena pomocí směrovačů a firewallů v místě zákazníka.

Telefon se dá použít jako vzdálené rozšíření back-endového vybavení poskytovatele služeb. Vzdálená správa a konfigurace zajišťují správné fungování telefonu v lokalitě zákazníka.

Zřizování TR69

Telefon Cisco IP Phone pomáhá správci konfigurovat parametry TR69 pomocí webového uživatelského rozhraní. Informace týkající se parametrů, včetně porovnání parametrů XML a TR69, naleznete v příručce pro správu příslušné řady telefonu.

Telefony podporují zjišťování serveru automatické konfigurace (ACS) z možnosti DHCP 43, 60 a 125.

- Možnost 43 – Údaje týkající se konkrétního výrobce pro adresu URL ACS.
- Možnost 60 – Identifikátor třídy výrobce, aby se telefon pro ACS identifikoval se souborem `dslforum.org`.
- Možnost 125 – Údaje týkající se konkrétního výrobce pro přiřazení brány.

Metody RPC

Podporované metody RPC

Telefony podporují pouze omezenou sadu metod vzdáleného volání procedury (RCP), a to tyto:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: Stáhnout metodu RPC, podporované typy souborů jsou:
    - Obraz upgradu firmwaru
    - Konfigurační soubor výrobce
    - Soubor vlastní certifikační autority (CA)
- Přenos dokončen

Podporované typy událostí

Telefony podporují typy událostí na základě podporovaných funkcí a metod. Podporovány jsou pouze následující typy událostí:

- Samozavedení
- Spuštění
- Změna hodnoty
- Požadavek na připojení
- Pravidelné
- Přenos dokončen
- Stažení M
- Restart M

Chování telefonu v době silného síťového provozu

- Administrativní činnosti, jako je skenování vnitřních portů nebo skenování zabezpečení.
- Útoky na síť, jako je útok typu DoS (odepření služby).

Nasazení

Telefony Cisco IP Phone mají praktické mechanismy zřizování na základě těchto modelů nasazení:

- Hromadná distribuce – Poskytovatel služeb zakoupí telefony Cisco IP Phones hromadně a předem je zřídí na pracovišti nebo si od společnosti Cisco zakoupí jednotky vzdáleného přizpůsobení (RC). Zařízení jsou poté vydávána zákazníkům jako součást servisní smlouvy VoIP.
- Maloobchodní distribuce – Zákazník si zakoupí telefon Cisco IP Phone od maloobchodního prodejce a vyžádá si od poskytovatele služeb službu VoIP. Poskytovatel služeb musí poté podporovat zabezpečenou vzdálenou konfiguraci zařízení.

Velkoobjemová distribuce

V tomto modelu poskytovatel služeb vydává zákazníkům telefony jako součást servisní smlouvy VoIP. Zařízení jsou buď jednotky RC, nebo předem zřízené na pracovišti.

Společnost Cisco provádí předběžné zřizování jednotek k resynchronizaci se serverem Cisco, který stahuje profil zařízení a aktualizace firmwaru.

Poskytovatel služeb může provést předběžné zřizování telefonů požadovanými parametry, včetně parametrů, které řídí resynchronizaci, různě:

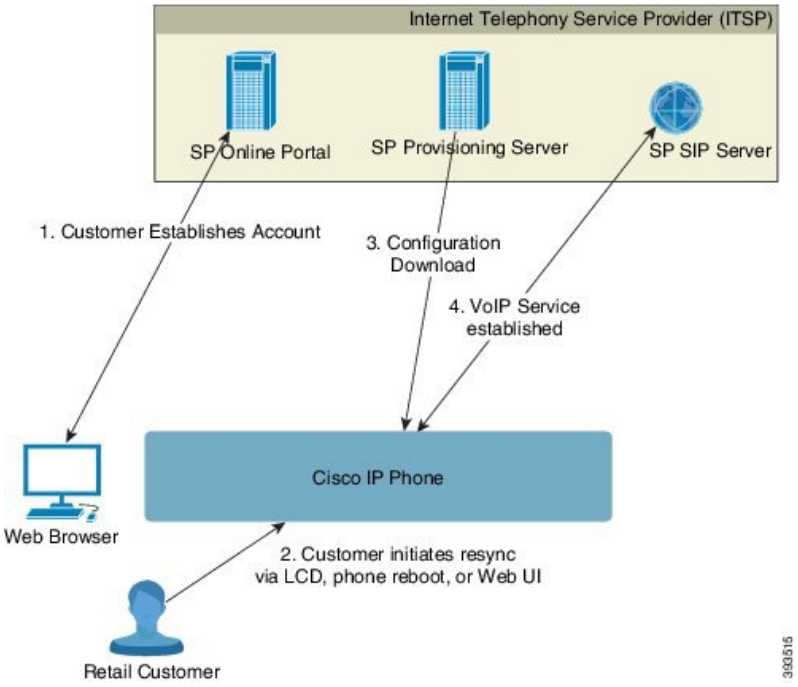
- Na pracovišti pomocí protokolu DHCP a TFTP

- Vzdáleně pomocí protokolu TFTP, HTTP nebo HTTPS
- Kombinací zřizování na pracovišti a vzdáleného zřizování

Maloobchodní distribuce

V modelu maloobchodní distribuce zákazník zakoupí telefon a přihlásí se k určité službě. Poskytovatel služeb internetové telefonie (ITSP) nastavuje a udržuje zřizovací server a provádí předběžné zřízení telefonu pro resynchronizaci se serverem poskytovatele služeb.

Obrázek 1: Maloobchodní distribuce



Telefon obsahuje webový konfigurační nástroj, který zobrazuje interní konfiguraci a do kterého je možné zadat nové hodnoty parametrů konfigurace. Server také přijímá syntax zvláštních příkazů adresy URL k provádění operací vzdálené resynchronizace profilu a upgradu firmwaru.

Zákazník se do služby přihlásí, zřídí si účet VoIP, například prostřednictvím online portálu, a zařízení propojí s přiřazeným servisním účtem. Nezřízenému telefonu je zadán příkaz k resynchronizaci s konkrétním zřizovacím serverem prostřednictvím příkazu adresy URL. Příkaz adresy URL obvykle za účelem přiřazení zařízení k novému účtu obsahuje číslo ID zákazníka nebo alfanumerický kód.

V následujícím příkladu je zařízení na adrese IP 192.168.1.102 přidělené serverem DHCP dán příkaz se zřídit na službu SuperVoIP:

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

V následujícím příkladu je číslo ID zákazníka nového účtu 1234abcd. Vzdálený zřizovací server na základě adresy URL a zadaného ID zákazníka přiřadí telefon, který provádí resynchronizaci, k novému účtu.

Prostřednictvím této operace úvodní resynchronizace je telefon jedním krokem nakonfigurován. Telefon je poté pro resynchronizaci automaticky směrován na trvalou adresu URL na serveru. Příklad:

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

K úvodnímu i trvalém přístupu zřizovací server využívá při ověření klientský certifikát telefonu. Zřizovací server dodá správné hodnoty parametrů konfigurace na základě přiřazeného účtu služby.

Když je zařízení zapnuto nebo když uběhne zadaná doba, telefon se resynchronizuje a stáhne si nejnovější parametry. Tyto parametry se mohou týkat cílů, jako je nastavení skupiny sdružených linek, nastavení čísel rychlé volby nebo omezení funkcí, které může upravovat uživatel.

Související témata

Předběžné zřizování zařízení na pracovišti, na straně 39

Proces resynchronizace

Firmware každého telefonu obsahuje webový server pro správu, do kterého je možné zadat nové hodnoty parametrů konfigurace. Telefonu může být prostřednictvím příkazu adresy URL resynchronizace v profilu zařízení zadán příkaz na resynchronizaci konfigurace se zadaným zřizovacím serverem po každém restartování nebo v plánovaných intervalech.

Ve výchozím nastavení je webový server povolen. Pokud chcete webový server zakázat nebo povolit, použijte příkaz adresy URL resynchronizace.

V případě potřeby je možné vyžádat okamžitou resynchronizaci prostřednictvím adresy URL akce „resynchronizace“. Příkaz adresy URL resynchronizace může za účelem jedinečného přiřazení zařízení k uživatelskému účtu obsahovat číslo ID zákazníka nebo alfanumerický kód.

Příklad

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

V tomto příkladu je zařízení na adrese IP 192.168.1.102, přidělené serverem DHCP, dán příkaz se zřídit na službu SuperVoIP na adrese prov.supervoip.com. Číslo ID zákazníka u nového účtu je 1234abcd. Vzdálený zřizovací server na základě adresy URL a ID zákazníka přiřadí telefon, který provádí resynchronizaci, k účtu.

Prostřednictvím této operace úvodní resynchronizace je telefon jedním krokem nakonfigurován. Telefon je poté pro resynchronizaci automaticky směrován na trvalou adresu URL na serveru.

K úvodnímu i trvalému přístupu zřizovací server využívá při ověření klientský certifikát. Server dodává hodnoty parametrů konfigurace na základě přiřazeného účtu služby.

Poskytování

Telefon lze nakonfigurovat, aby pravidelně a při spuštění resynchronizoval svůj vnitřní stav konfigurace tak, aby odpovídal vzdálenému profilu. Telefon kontaktuje normální zřizovací server (NPS) nebo server řízení přístupu (ACS).

Ve výchozím nastavení se resynchronizace profilu provádí pouze tehdy, když je telefon nečinný. Tento postup zabraňuje tomu, aby proběhl upgrade, který vynutí restart telefonu a přeruší hovor. Pokud je k dosažení aktuálního stavu upgradu ze starší vydané verze potřeba provést další upgrady, logika upgradování dokáže provést vícefázové upgrady automaticky.

Normální zřizovací server

Normální zřizovací server (NPS) může být server TFTP, HTTP nebo HTTPS. Vzdálený upgrade firmwaru se provádí protokolem TFTP, HTTP nebo HTTPS, protože firmware neobsahuje citlivé údaje.

Ačkoliv se doporučuje použít protokol HTTPS, komunikace s NPS nevyžaduje použití zabezpečeného protokolu, protože aktualizovaný profil lze zašifrovat pomocí sdíleného tajného klíče. Další informace o využití protokolu HTTPS naleznete v tématu Šifrování komunikace, na straně 8. Zabezpečené první zřízení je zajišťování mechanismem, který využívá funkce SSL. Nezřízený telefon dokáže přijmout profil zašifrovaný 256bitovým symetrickým klíčem, který je mu určen.

Řízení přístupu ke konfiguraci

Firmware telefonu poskytuje mechanismy k omezení přístupu koncových uživatelů k některým parametrům. Firmware poskytuje konkrétní oprávnění k přihlášení k účtu **Správce** a účtu **Uživatel**. Obě je možné nezávisle na sobě chránit heslem.

- Účet správce – umožňuje poskytovateli služeb plný přístup ke všem parametrům webového serveru pro správu.
- Účet uživatele – umožňuje uživateli konfigurovat podmnožinu parametrů webového serveru pro správu.

Poskytovatel služeb může uživatelský účet omezit ve zřizovacím profilu následovně:

- Při vytváření konfigurace určit, které parametry konfigurace jsou dostupné pro uživatelský účet.
- Zakázat uživateli přístup k webovému serveru pro správu.
- Zakázat uživateli přístup k uživatelskému rozhraní LCD.
- Obejít obrazovku **Nastavit heslo** pro uživatele.
- Omezit zařízení přístup k internetovým doménám pro resynchronizaci, aktualizace nebo registraci SIP pro linku 1.

Související témata

Vlastnosti značek prvků, na straně 14
Řízení přístupu, na straně 16

Otevření webové stránky telefonu

Webovou stránku telefonu otevřete z webového prohlížeče na telefonu, který se k telefonu dostane v jedné podsíti.

Pokud váš poskytovatel služeb zakázal přístup ke konfiguračnímu nástroji, než budete pokračovat, kontaktujte ho.

Procedura

Krok 1 Zkontrolujte, zda počítač s telefonem může komunikovat. Nepoužívá se žádné připojení VPN.

Krok 2 Spusťte webový prohlížeč.

Krok 3 Do adresního řádku webového prohlížeče zadejte adresu IP telefonu.

- Přístup pro uživatele: **http://<adresa ip>/user**
- Přístup pro správce: **http://<adresa ip>/admin/advanced**
- Přístup pro správce: **http://<adresa ip>**, klikněte na možnost **Přihlášení správce** a klikněte na možnost **pokročilé**

Například `http://10.64.84.147/admin`

Povolení webového přístupu pro telefon Cisco IP Phone

K zobrazení parametrů telefonu povolte profil konfigurace. Pokud chcete některý parametr změnit, musíte mít možnost změnit profil konfigurace. Váš správce systému mohl zakázat telefonu zobrazovat webové uživatelské rozhraní a provádět v něm změny.

Další informace získáte v *Příručce zřizování pro víceplatformové telefony řady Cisco IP Phone 6800*.

Než začnete

Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Procedura

Krok 1 Klikněte na možnost **Hlas** > **Systém**.

Krok 2 V části **Konfigurace systému** nastavte možnost **Povolit webový server** na **Ano**.

Krok 3 Po úpravě polí ve webovém uživatelském rozhraní telefonu klikněte na možnost **Odeslat všechny změny**, čímž aktualizujete uživatelské rozhraní.

Telefon se restartuje a změny se použijí.

Krok 4 Pokud chcete zrušit všechny změny, které jste během aktuální relace (nebo po posledním kliknutí na možnost **Odeslat všechny změny**) provedli, klikněte na možnost **Vrátit zpět všechny změny**. Hodnoty se vrátí k předchozímu nastavení.

Šifrování komunikace

Parametry konfigurace, které jsou odesílány zařízení, mohou obsahovat kódy autorizace nebo další údaje, které chrání systém před neoprávněným přístupem. Je v zájmu poskytovatele služeb předcházet neautorizované činnosti zákazníka. Je v zájmu zákazníka služeb předcházet neautorizovanému použití účtu. Poskytovatel služeb může šifrovat komunikaci profilu konfigurace mezi zřizovacím serverem a zařízením a také omezovat přístup k webovému serveru pro správu.

Postupy zřizování telefonu

Telefon Cisco IP Phone je obvykle nakonfigurován tak, aby provedl zřizování při prvním připojení k síti. Telefon je také zřizován v plánovaných intervalech, které jsou nastaveny, když poskytovatel služeb nebo prodejce telefon předem zřídí (nakonfiguruje). Poskytovatelé služeb mohou prodejcům nebo pokročilým

uživatelům povolit ruční zřizování telefonu pomocí klávesnice telefonu. Zřizování můžete nakonfigurovat také pomocí webového uživatelského rozhraní telefonu.

Podívejte se do nabídky **Stav** > **Stav telefonu** > **Zřizování** v uživatelském rozhraní na obrazovce telefonu nebo na stav zřizování na kartě **Stav** webového konfiguračního nástroje.

Související témata

Ruční zřízení telefonu z klávesnice, na straně 9

Ruční zřízení telefonu z klávesnice

Procedura

Krok 1 Stiskněte tlačítko **Aplikace**  .

Krok 2 Vyberte možnosti **Správa zařízení** > **Pravidlo profilu**.

Krok 3 Zadejte pravidlo profilu v následujícím formátu:

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

Příklad:

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

Pokud není zadán žádný protokol, předpokládá se TFTP. Pokud není zadán žádný název serveru, jako název serveru se použije hostitel, který o adresu URL žádá. Pokud není zadán žádný port, používá se výchozí port (69 pro TFTP, 80 pro HTTP a 443 pro HTTPS).

Krok 4 Stiskněte tlačítko **Znovu synchronizovat**.

Související témata

Postupy zřizování telefonu, na straně 8

Sdílení firmwaru s druh. stranou

Sdílení firmwaru s druhou stranou (metoda PFS) je model distribuce firmwaru, který umožňuje, aby IP telefony Cisco vyhledaly jiné telefony stejného modelu nebo řady v podsíti a sdílely aktualizovaný firmware, když potřebujete současně aktualizovat více telefonů. Metoda PFS používá protokol CPPDP (Cisco Peer-to-Peer-Distribution Protocol), což je proprietární protokol společnosti Cisco. Při použití protokolu CPPDP tvoří všechna zařízení v podsíti hierarchii typu peer-to-peer, kde se kopíruje firmware nebo jiné soubory z rovnocenných zařízení do blízkých zařízení. Kořenový telefon stáhne bitovou kopii firmwaru ze zaváděcího serveru a potom firmware odešle do ostatních telefonů v podsíti za použití připojení TCP, čímž je zajištěna optimalizace aktualizací firmwaru.

Sdílení firmwaru s druhou stranou:

- Omezuje zahlcení u přenosů TFTP směrem na centralizované servery pro odstranění zavedených dat.
- Aktualizace firmwaru není třeba řídit ručně.
- Zkracuje odstávku telefonů během aktualizací v situacích, kdy je resetován velký počet telefonů současně.

Poznámka

- Sdílení firmwaru s druhou stranou funguje, jen když je více telefonů nastaveno pro souběžnou aktualizaci. Když je parametr NOTIFY odeslán s parametrem Event:resync, v telefonu se zahájí resynchronizace. Příklad kódu XML, které mohou obsahovat konfigurace k zahájení aktualizace:

  „**Event:resync;profile=**“http://10.77.10.141/profile.xml
- Když nastavíte pro server protokolování sdílení firmwaru s druhou stranou nějakou IP adresu a port, na tento server jsou odesílány protokoly metody PFS ve formě zpráv UDP. Toto nastavení je třeba provést ve všech telefonech. Tyto zprávy protokolu potom můžete použít při řešení potíží souvisejících s metodou PFS.

Parametr Peer_Firmware_Sharing_Log_Server uvádí název hostitele a port vzdáleného serveru syslog UDP. Ve výchozím nastavení se používá port syslog 514.

Příklad:

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

Chcete-li tuto funkci použít, povolte v telefonech metodu PFS.

Obejití obrazovky pro nastavení hesla

V závislosti na následujících akcích zřizování můžete obejít obrazovku telefonu **Nastavit heslo**, která se zobrazuje při prvním spuštění nebo po zavedení továrního nastavení:

- konfigurace DHCP,
- konfigurace EDOS,
- konfigurace hesla uživatele pomocí konfiguračního souboru XML pro telefon.

Tabulka 1: Akce zřizování, které určují zobrazení obrazovky Nastavit telefon

Byla provedena konfigurace DHCP	Byla provedena konfigurace EDOS	Bylo nakonfigurováno heslo uživatele	Obejít obrazovku Nastavit heslo
Ano	Není k dispozici	Ano	Ano
Ano	Není k dispozici	Ne	**Ne**
Ne	Ano	Ano	Ano
Ne	Ano	Ne	**Ne**
Ne	Ne	Není k dispozici	**Ne**

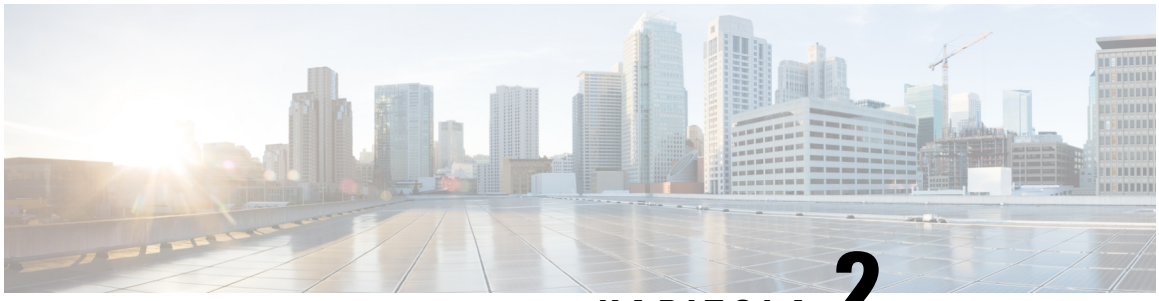
Procedura

Krok 1 Upravte soubor telefonu `config.xml` v textovém nebo XML editoru.

Krok 2 Vložte značku **<User_Password>** pomocí jedné z těchto možností.

- **Žádné heslo (počáteční a koncová značka)–<User_Password></User_Password>**
- **Hodnota hesla (4 až 127 znaků)–<User_Password ua="rw">abc123</User_Password>**
- **Žádné heslo (jen počáteční značka)–<User_Password />**

Krok 3 Uložte změny souboru `config.xml`.



KAPITOLA 2

Zřizovací skripty

Zřizovací skripty

Telefon přijímá konfiguraci ve formátu XML.

Podrobné informace o telefonu naleznete v příručce pro správu vašeho konkrétního zařízení. V každé příručce jsou popsány parametry, které lze pomocí webového serveru pro správu konfigurovat.

Formáty profilů konfigurace

Konfigurační profil definuje hodnoty parametrů telefonu.

Formát XML konfiguračního parametru ke kompilaci parametrů a hodnot využívá standardní nástroje vytváření obsahu XML.

Poznámka Je podporována pouze znaková sada UTF-8. Když upravujete profil v editoru, neměňte formát kódování. Jinak telefon soubor nerozpozná.

Každý telefon má jinou sadu funkcí, a tedy i jinou sadu parametrů.

Profil formátu XML (XML)

Profil otevřeného formátu je textový soubor se syntaxí podobou XML, hierarchií elementů a atributy a hodnotami elementů. Tento formát k vytváření konfiguračního souboru umožňuje použití standardních nástrojů. Konfigurační soubor v tomto formátu může být během operace resynchronizace odeslán ze zřizovacího serveru na telefon. Soubor může být odeslán bez kompilace jako binární objekt.

Telefon dokáže přijímat formáty konfigurace, které standardní nástroje generují. Tato funkce usnadňuje vývoj back-endového softwaru zřizovacích serverů, který generuje profily konfigurace z existujících databází.

Na ochranu důvěrných údajů v profilu konfigurace zřizovací server poskytuje telefonu tento typ souborů prostřednictvím kanálu zabezpečeného protokolem TLS. Soubor lze volitelně komprimovat pomocí algoritmu gzip (RFC1951).

Soubor můžete zašifrovat pomocí jedné z těchto metod šifrování:

- Šifrování AES-256-CBC
- Šifrování AES-128-GCM obsahu pro protokol HTTP pomocí metody RFC 8188

Například: Otevřený 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>
```

Telefon rozpoznává elementy se správnými názvy parametrů, které jsou součástí speciálního elementu <flat-profile>.

Související témata

Komprese a šifrování otevřeného profilu (XML), na straně 17

Komponenty konfiguračního souboru

Konfigurační soubor může obsahovat tyto komponenty:

- Značky elementů
- Atributy
- Parametry
- Formátovací prvky
- Komentáře XML

Vlastnosti značek prvků

- Formát zřizování XML a webové uživatelské rozhraní umožňují konfiguraci stejného nastavení. Název značky XML a názvy polí ve webovém uživatelském rozhraní jsou podobné, ale kvůli omezením na název elementu XML se liší. Například se používají podtržítka (_) místo „ “.
- Telefon rozpoznává elementy se správnými názvy parametrů, které jsou součástí speciálního elementu <flat-profile>.
- Názvy elementů se uzavírají do špičatých závorek.
- Většina názvů elementů je podobná názvům polí na webových stránkách správy zařízení s následujícími odlišnostmi:

- Názvy elementů nesmějí obsahovat mezery ani speciální znaky. Při odvozování názvu elementu z názvu pole webu správy nahraďte všechny mezery a speciální znaky `[`, `]`, `(`, `)` a `/` podtržítky.

  Příklad: Element <Resync_On_Reset> odpovídá poli **Resync On Reset**.

- Každý název elementu musí být jedinečný. Na webových stránkách správy se stejná pole mohou objevovat na různých webových stránkách, například Linka, Uživatel a Rozšíření. K názvu prvku připojte `[n]`, což značí číslo, které se zobrazuje na kartě stránky.

  Příklad: Element <Dial_Plan_1_> odpovídá poli **Dial Plan** při linku 1.

- Každá otevírací značka elementu musí mít odpovídající koncovou značku elementu. Příklad:

```
<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>
```

- U značek elementů záleží na velikosti písmen.
- Prázdné značky elementů jsou povolené a interpretují se tak, že hodnota je nakonfigurována jako prázdná. Zadejte otevírací značku elementu bez odpovídající značky elementu a před koncovou špičatou závodu (>) vložte mezeru a lomítko. V tomto příkladu je hodnota Profile Rule B prázdná:

```
<Profile_Rule_B />
```

- Prázdnou značku elementu lze využít k zabránění přepsání uživatelem zadaných hodnot během operace resynchronizace. V následujícím příkladu zůstávají uživatelská nastavení rychlé volby beze změny:

```
<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>
```

- Pokud chcete příslušný parametr nastavit na prázdný řetězec, použijte prázdnou hodnotu. Zadejte otevírací a koncový element a mezi ně nezadávejte žádnou hodnotu. V následujícím příkladu je parametr GPP_A nastaven jako prázdný řetězec.

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

- Nerozpoznané názvy elementů jsou ignorovány.

Související témata

Řízení přístupu ke konfiguraci, na straně 7

Atribut uživatelského přístupu

Ovládací prvky atributu uživatelského přístupu (**ua**) lze použít ke změně přístupu uživatelským účtem. Pokud není atribut **ua** zadán, zůstává stávající nastavení uživatelského přístupu. Tento atribut neovlivňuje přístup účtem správce.

Pokud je atribut **ua** přítomen, musí mít jednu z následujících hodnot:

- na – žádný přístup
- ro – pouze ke čtení
- rw – čtení a zápis

V následujícím příkladu je ukázka atributu **ua**.

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

Hodnota možnosti **ua** musí být uzavřena do dvojitých uvozovek.

Řízení přístupu

Pokud je povolen parametr <Phone-UI-User-Mode>, grafické uživatelské rozhraní telefonu respektuje atribut uživatelského přístupu příslušných parametrů, když se v grafickém uživatelském rozhraní zobrazí položka nabídky.

Položky nabídky, které jsou přiřazeny k jednomu parametru konfigurace:

- Když se parametr zřídí s atributem „ua=na“ („ua“ znamená „uživatelský přístup“), položka se nezobrazuje.
- Když se parametr zřídí s atributem „ua=ro“ („ua“ znamená „uživatelský přístup“), položka je jen ke čtení a nedá se upravovat.

Položky nabídky, které jsou přiřazeny k více parametrům konfigurace:

- Když se všechny dotčené parametry zřídí s atributem „ua=na“ („ua“ znamená „uživatelský přístup“), položky se nezobrazují.

Související témata

Řízení přístupu ke konfiguraci, na straně 7

Vlastnosti parametru

Parametry mají následující vlastnosti:

- Všechny parametry, které nejsou zadány v profilu, zůstávají v telefonu beze změny.
- Nerozpoznané parametry jsou ignorovány.
- Pokud profil otevřeného formátu obsahuje více výskytů stejné značky parametru, poslední takový výskyt má přednost před předcházejícími. Abyste předešli nechtěnému přepsání hodnot konfigurace parametru, doporučujeme, aby byla v každém profilu zadána maximálně jedna instance parametru.

- Poslední zpracovaný profil má přednost. Pokud má více profilů stejný parametr konfigurace, hodnota toho pozdějšího má přednost.

Formáty řetězců

Při formátování řetězců platí tyto vlastnosti:

- Komentáře je možné přidávat pomocí standardní syntaxe XML.

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

- Bílé znaky na začátku a na konci jsou kvůli čitelnosti povoleny, ale z hodnoty parametru jsou odstraněny.
- Nové řádky v rámci hodnoty jsou převedeny na mezery.
- Záhlaví XML ve tvaru `<? ?>` je povoleno, ale telefon je ignoruje.
- Pokud chcete zadat speciální znaky, použijte základní kódy znaků XML, jak jsou uvedeny v následující tabulce.

Zvláštní znak	Kód znaku XML
& (ampersand)	+
< (menší než)	<
> (větší než)	>
’ (apostrof)	'
” (dvojité uvozovky)	“

V následujícím příkladu jsou zadány kódy znaků reprezentující symboly větší než a menší než, které jsou vyžadovány pravidlem plánu číslování. V tomto příkladu je definován plán číslování informační linky, který nastavuje parametr <Dial_Plan_1_> (**Přihlášení správce** > **pokročilé** > **Hlas** > **Klap. (č.)**) na (S0 <:18005551212>).

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

- Kódy s číselnými znaky v desítkových nebo šestnáctkových hodnotách (např. `(` a `.`) jsou přeloženy
- Firmware telefonu podporuje pouze znaky ASCII.

Komprese a šifrování otevřeného profilu (XML)

Za účelem snížení síťové zátěže na zřizovací server můžete otevřený konfigurační profil komprimovat. Profil je možné také na ochranu důvěrných údajů zašifrovat. Komprese není vyžadována, ale musí být provedena před zašifrováním.

Související témata

Formáty profilů konfigurace, na straně 13

Komprese otevřeného profilu

Podporovaná metoda komprese je kompresní algoritmus gzip (RFC1951). Nástroj gzip a komprimační knihovna, která implementuje stejný algoritmus (zlib), jsou k dispozici na internetu.

Pro rozpoznání komprese telefon očekává, že komprimovaný soubor bude obsahovat hlavičku kompatibilní s nástrojem gzip. Hlavička je vygenerována zavoláním nástroje gzip na původní otevřený profil. Telefon se podívá do hlavičky staženého souboru, aby určil jeho formát.

Pokud je například `profile.xml` platný profil, soubor `profile.xml.gz` je také přijat. Tento profil mohou vygenerovat oba následující příkazy:

- `>gzip profile.xml`

  Nahradí původní soubor komprimovaným souborem.

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

  Nechá původní soubor na místě a vytvoří nový komprimovaný soubor.

Průvodce komprimací je k dispozici v části Zkomprimovat otevřený profil metodou Gzip, na straně 60.

Související témata

Zkomprimovat otevřený profil metodou Gzip, na straně 60

Šifrování otevřeného profilu

Bez ohledu na to, zda je soubor komprimovaný, lze šifrování symetrickým klíčem použít k šifrování otevřeného profilu konfigurace. Když používáte kompresi, je nutno ji provést před šifrováním.

Zřizovací server využívá k provedení počátečního zřízení telefonu po nasazení protokol HTTPS. Předběžné zašifrování profilů konfigurace offline umožňuje k následné resynchronizaci profilů použít protokol HTTP. Tím se snižuje zátěž serveru HTTPS v rozsáhlých nasazeních.

Telefon podporuje dvě metoddy šifrování konfiguračních souborů.

- Šifrování AES-256-CBC
- Šifrování AES-128-GCM obsahu pro protokol HTTP pomocí metody RFC 8188

Je třeba pro jednotku předem zřídit klíč nebo data IKM (Input Keying Material). Samozavedení tajného klíče lze zabezpečeně provést pomocí protokolu HTTPS.

Název konfiguračního souboru nemusí mít konkrétní formát, ale název souboru, který končí příponou `.cfg`, obvykle označuje profil konfigurace.

Šifrování AES-256-CBC

Telefon podporuje šifrování AES-256-CBC pro konfigurační soubory.

Šifrování může provést nástroj pro šifrování OpenSSL, který je k dispozici na různých webech na internetu. Podpora 256bitového šifrování AES může k povolení kódu AES vyžadovat překompilování nástroje. Firmware byl otestován s verzí openssl-0.9.7c.

Šifrování profilu pomocí OpenSSL, na straně 61 poskytuje průvodce šifrováním.

U zašifrovaného souboru profil očekává, že soubor bude mít stejný formát jako při vygenerování následujícím příkazem:

```
# 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 -k následované tajným klíčem, což může být libovolný textový výraz, který se používá k vygenerování náhodného 64bitového řetězce. Z tajného řetězce definovaného v argumentu -k šifrovací nástroj odvodí náhodný 128bitový úvodní vektor a nakonec 256bitový šifrovací klíč.

Když se tato podoba šifrování použije na profil konfigurace, telefon musí být pro dešifrovaní souboru informován o hodnotě tajného klíče. Tato hodnota je zadána jako modifikátor adresy URL profilu. Syntaxe je za použití explicitní adresy URL tato:

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

Toto je hodnota je naprogramována pomocí jednoho z parametrů Profile_Rule.

Související témata

Šifrování profilu pomocí OpenSSL, na straně 61

Rozšíření makra

Několik parametrů zřizování prochází před vyhodnocením rozšířením makra. Tento krok předběžného vyhodnocení poskytuje větší flexibilitu při řízení činností resynchronizace telefonu a upgradu.

Rozšířením makra před vyhodnocením procházejí tyto parametry:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

Za určitých okolností rozšíření makra podléhají také obecné parametry (GPP_*), jak je explicitně uvedeno v části Volitelné argumenty resynchronizace, na straně 22.

Při rozšíření makra se obsah pojmenovaných proměnných nahradí výrazy v podobě $JMENO a $(JMENO). Mezi tyto proměnné patří obecné parametry, několik identifikátorů produktů, některé časovače událostí a hodnoty stavu zřizování. Úplný seznam naleznete zde: Proměnné rozšíření makra, na straně 72.

V následujícím příkladu se výraz $(MAU) používá k zadání adresy MAC 000E08012345.

Správce zadá: **`$(MAU)config.cfg`**

Výsledné rozšíření makra pro zařízení s adresou MAC 000E08012345 je: `000E08012345config.cfg`

Pokud název makra není rozpoznán, zůstává nerozšířený. Například název STRANGE není rozpoznán jako platný název makra a název MAU je rozpoznán jako platný název makra.

Správce zadá: **`$STRANGE$MAU.cfg`**

Výsledné rozšíření makra pro zařízení s adresou MAC 000E08012345 je: `$STRANGE000E08012345.cfg`

Rozšíření makra se neprovádí rekurzivně. Například „$$MAU" se rozšíří na „$MAU" ($$ se rozšíří) a výsledkem není adresa MAC.

Obsah parametrů pro zvláštní účel, GPP_SA až GPP_SD, je mapován na výrazy makra $SA až $SD. Tyto výrazy jsou jako makro rozšíření pouze jako argument možností **--key**, **--uid** a **--pwd** v adrese URL resynchronizace.

Podmíněné výrazy

Podmíněné výrazy mohou spouštět událost resynchronizace s volit mezi alternativními adresami URL při operaci resynchronizace a upgradu.

Podmíněné výrazy se skládají ze seznamu srovnání oddělených operátorem **a**. Aby byla podmínka platná, musí být všechna srovnání pravdivá.

Každé srovnání se může týkat jednoho z těchto typů hodnot:

- Celočíselné hodnoty
- Čísla verzí softwaru a hardwaru
- Řetězce v dvojitých uvozovkách

Čísla verzí

Verze softwaru formální vydané verze víceplatformových telefonů (MPP) mají tento formát, kde BN = číslo sestavení:

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

Řetězec ve srovnání musí mít stejný formát. Jinak dojde k chybě analýzy formátu.

Ve verzi softwaru v1-v2-v3-v4 může obsahovat různé číslice a znaky, ale musí začínat číslicí. Při srovnávání verze softwaru je v1-v2-v3-v4 srovnáváno postupně a nejlevější číslice mají přednost před těmi více vpravo.

Pokud v[x] obsahuje pouze číslice, dojde k jejich srovnání. Pokud v[x] obsahuje číslice + písmena, nejprve jsou srovnány číslice a poté jsou srovnána písmena v abecedním pořadí.

Příklad platného čísla verze

sipyyyy.11-0-0MPP-BN

Naopak 11.0.0 není platný formát.

Srovnání

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

U řetězců v uvozovkách je možné srovnávat rovnost a nerovnost. Celá čísla a čísla verzí lze také srovnávat aritmeticky. Operátory srovnání lze vyjádřit jako symboly nebo zkratky. Zkratky jsou praktický způsob vyjádření podmínky v profilu otevřeného formátu.

Operátor	Alternativní syntax	Popis	Použitelné na operandy celého čísla a verze	Použitelné na operandy řetězců v uvozovkách
=	eq	rovná se	Ano	Ano
!=	ne	nerovná se	Ano	Ano
<	lt	menší než	Ano	Ne
<=	le	menší nebo rovno	Ano	Ne
>	gt	větší než	Ano	Ne
>=	ge	větší nebo rovno	Ano	Ne
A		a	Ano	Ano

Tam, kde je očekávána hodnota řetězce, je důležité proměnné makra uzavírat do dvojitých uvozovek. To nedělejte tam, kde je očekáváno číslo nebo číslo verze.

Při použití v kontextu parametrů Profile_Rule* a Upgrade_Rule musí být podmíněné výrazy uzavřeny v syntaxi "(vyraz)?" jako v tomto příkladu pravidla upgradu. Nezapomeňte, že BN znamená číslo sestavení.

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

Uvedenou syntax se závorkami nepoužívejte ke konfiguraci parametrů Resync_Trigger*.

Syntax URL

K zadání způsobu načítání konfiguračních souborů a firmwaru do parametrů Profile_Rule* a Upgrade_Rule používejte standardní syntax adresy URL. Syntaxe je tato:

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

Kde **`protokol`** je jedna z těchto hodnot:

- tftp
- http
- https

Při vynechání hodnoty **`protokol`** se předpokládá tftp. Server může být název hostitele rozpoznávaný serverem DNS nebo číselná adresa IP. Port je číslo cílového portu UDP nebo TCP. Cestaksouboru musí začínat kořenovým adresářem (/) a musí se jednat o absolutní cestu.

Pokud chybí hodnota **`server`**, používá se server tftp určený prostřednictvím DHCP (možnost 66).

Poznámka U pravidel upgradu musí být server zadán.

Pokud chybí hodnota **port**, používá se standardní port pro zadaný protokol. Protokol TFTP využívá port UDP 69, protokol HTTP využívá port TCP 80, protokol HTTPS využívá port TCP 443.

Cestaksouboru nesmí chybět. Není třeba nutně odkazovat na statický soubor, ale je možné zadat dynamický obsah získaný prostřednictvím skriptu CGI.

V rámci adres URL platí rozšíření maker. Toto jsou příklady platných adres 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
```

Při použití možnosti DHCP 66 není u pravidel upgradu v současné době podporována prázdná syntax. Platí pouze pro pravidlo profilu*.

Šifrování obsahu pro protokol HTTP pomocí metody RFC 8188

Telefon podporuje šifrování obsahu konfiguračních souborů pro protokol HTTP pomocí metody RFC 8188. Pomocí této metody šifrování může jakákoli entita číst záhlaví zpráv HTTP. Datovou část však mohou číst jen entity, které mají k dispozici data IKM (Input Keying Material). Když jsou pro telefon zřízena data IKM, mezi telefonem a zřizovacím serverem lze bezpečně přenášet konfigurační soubory a současně je možné, aby síťové prvky třetí strany používaly záhlaví zpráv pro účely analýz a monitrování.

Parametr konfigurace XML **IKM_HTTP_Encrypt_Content** v telefonu obsahuje data IKM. Z důvodů zabezpečení není tento parametr přístupný na webové stránce správy telefonu. Ani se nezobrazuje v konfiguračním souboru telefonu, ke kterému máte přístup z adresy IP telefonu nebo ze sestav konfigurace telefonu odeslaných na zřizovací server.

Pokud chcete používat šifrování podle metody RFC 8188, je třeba splnit následující podmínky:

- Zřiďte pro telefon data IKM zadáním IKM s parametrem XML **IKM_HTTP_Encrypt_Content** do konfiguračního souboru, který je do telefonu odesílán ze zřizovacího serveru.
- Pokud toto šifrování chcete použít na konfigurační soubory odesílané ze zřizovacího serveru do telefonu, záhlaví HTTP *Content-Encoding* v konfiguračním souboru musí obsahovat hodnotu “aes128gcm”.

  Pokud toto záhlaví bude chybět, přednost bude dána metodě AES-256-CBC. Telefon použije šifrování AES-256-CBC, jestliže je v pravidle profilu klíč AES-256-CBC (bez ohledu na data IKM).
- Pokud chcete, aby telefon použil toto šifrování na sestavy konfigurace odesílané na zřizovací server, v pravidle sestav nesmí být žádný klíč AES-256-CBC.

Volitelné argumenty resynchronizace

Volitelné argumenty, **key**, **uid** a **pwd**, mohou být uvedeny společně uzavřené do hranatých závorek před adresami URL zadanými v parametrech Profile_Rule*.

key

Možnost **--key** informuje telefon, že pro konfigurační soubor přijatý ze zřizovacího serveru je použito šifrování AES-256-CBC, pokud není v záhlaví *Content-Encoding* v souboru uvedeno šifrování "aes128gcm". Vlastní klíč je zadán za výrazem **--key** ve formě řetězce. Klíč může být volitelně ve dvojitých uvozovkách ("). Telefon použije tento klíč k dešifrování konfiguračního souboru.

Příklady použití

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

Volitelné argumenty v závorkách podléhají rozšíření makra. Parametry pro zvláštní účel, GPP_SA až GPP_SD, se rozšiřují makrem na hodnoty makra $SA až $SD, jen když se používají jako argumenty možnosti key. Viz tyto příklady:

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

V profilech otevřeného formátu musí být argument parametru **--key** stejný jako argument možnosti **-k**, která je předána příkazu **openssl**.

uid a pwd

Možnosti **uid** a **pwd** lze použít k zadání ID uživatele a hesla pro ověření u zadané adresy URL. Volitelné argumenty v závorkách podléhají rozšíření makra. Parametry pro zvláštní účel, GPP_SA až GPP_SD, se rozšiřují makrem na hodnoty makra $SA až $SD, jen když se používají jako argumenty možnosti key. Viz tyto příklady:

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

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

se rozšíří na:

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

Použití profilu na zařízení IP telefonie

Po vytvoření skriptu konfigurace XML je třeba ho předat telefonu, aby ho bylo možné použít. Pokud chcete konfiguraci použít, můžete stáhnout konfigurační soubor do telefonu ze serveru TFTP, HTTP nebo HTTPS pomocí webového prohlížeče nebo pomocí nástroj příkazové řádky cURL.

Stažení konfiguračního souboru do telefonu ze serveru TFTP

Ke stažení konfiguračního souboru do aplikace serveru TFTP v počítači proveďte následující postup.

Procedura

Krok 1 Připojte počítač k síti LAN telefonu.

Krok 2 Na počítači spusťte aplikaci serveru TFTP a zkontrolujte, že konfigurační soubor je dostupný v kořenovém adresáři TFTP.

Krok 3 Ve webovém prohlížeči zadejte adresu IP telefonu v síti LAN, adresu IP počítače, název souboru a přihlašovací údaje. Použijte tento formát:

`http://<Adresa_IP_WAN>/admin/resync?tftp://<Adresa_IP_počítače>/<název_souboru>&xuser=admin&xpassword=<heslo>`

Příklad:

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

Stažení konfiguračního souboru do telefonu pomocí příkazu cURL

Ke stažení konfigurace do telefonu pomocí příkazu cURL proveďte následující postup. Tento nástroj pro příkazové řádky se používá k přenosu dat pomocí syntaxe adresy URL. Nástroj cURL si můžete stáhnout na adrese:

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

Poznámka Doporučujeme, abyste příkaz cURL nepoužívali k odesílání konfigurace do telefonu, protože uživatelské jméno a heslo mohou být při použití protokolu cURL zachyceny.

Procedura

Krok 1 Připojte počítač k portu LAN telefonu.

Krok 2 Pomocí následujícího příkazu cURL do telefonu stáhněte konfigurační soubor:

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

Parametry zřizování

V této části jsou popsány parametry zřizování zhruba roztříděné podle funkce:

Existují tyto typy parametrů zřizování:

- Klasická
- Povolující
- Spouštěče

- Konfigurovatelné plány
- Pravidla profilu
- Pravidlo upgradu

Obecné parametry

Obecné parametry GPP_* (**Přihlášení správce** > **pokročilé** > **Hlas** > **Zřizování**) se při konfiguraci telefonu na komunikaci s konkrétním řešením zřizovacího serveru používají jako volné registry řetězců. Parametry GPP_* jsou ve výchozím nastavení prázdné. Je možné je nakonfigurovat tak, aby obsahovaly různé hodnoty, například tyto:

- Šifrovací klíče
- Adresy URL
- Informace o stavu vícefázového zřizování
- Šablony požadavku Post
- Mapy aliasů názvů proměnných
- Částečné hodnoty řetězců, které se ve výsledku zkombinují do úplných hodnot parametrů.

Parametry GPP_* jsou k dispozic k rozšíření makrem v rámci ostatních parametrů zřizování. Pro tento účel se k identifikaci obsahu proměnných GPP_A až GPP_P používají názvy maker obsahují jedno velké písmeno (A až P). Kromě toho dvoupísmenné názvy maker SA až SD určují parametry GPP_SA až GPP_SD jako speciální případy při použití v následujících možnostech adresy URL:

key, **uid** a **pwd**

Tyto parametry lze v pravidlech zřizování a upgradu použít jako proměnné. Odkazuje se na ně tím, že se před název proměnné přidá znak „$“, např. $GPP_A.

Použití obecných parametrů

Pokud například GPP_A obsahuje řetězec ABC a GPP_B obsahuje 123, makro AB se rozšíří na ABC123.

Než začnete

Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Procedura

Krok 1 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 2 Přejděte na část **Obecné parametry**.

Krok 3 Do políček GPP A až GPP P zadejte platné hodnoty.

Krok 4 Klikněte na tlačítko **Odeslat všechny změny**.

Povolující

Parametry Provision_Enable a Upgrade_Enable řídí všechny operace resynchronizace profilu a upgradu firmwaru. Tyto parametry řídí resynchronizace a upgrady nezávisle na sobě. Tyto parametry také řídí příkazy adresy URL resynchronizace a upgradu, které jsou zadávány prostřednictvím webového serveru pro správu. Oba tyto parametry jsou ve výchozím nastavení **Ano**.

Parametr Resync_From_SIP řídí požadavky na operace resynchronizace. Událost SIP NOTIFY je odeslána ze serveru proxy poskytovatele služeb do telefonu. Pokud je tato možnost zapnutá, server proxy může vyžádat resynchronizaci. Proto server proxy zařízení odešle zprávu SIP NOTIFY, která obsahuje hlavičku Event: resync.

Zařízení zareaguje na požadavek odpovědí 401 (ověření bylo použité přihlašovací údaje zamítlo). Zařízení očekává ověřený následný požadavek, než požadavek na resynchronizaci od serveru proxy splní. Hlavičky Event: reboot_now a Event: restart_now provádějí studený a teplý restart, který může zařízení také napadnout.

Zbývající dva povolující parametry jsou Resync_On_Reset a Resync_After_Upgrade_Attempt. Tyto parametry určují, zda zařízení provede operaci resynchronizaci po softwarových restartech a po každém pokusu o upgrade.

Když je možnost Resync_On_Reset zapnutá, zařízení zavede náhodnou prodlevu po spouštění, než je proveden restart. Prodleva je náhodná doba až do hodnoty zadané v parametru Resync_Random_Delay (v sekundách). Ve fondu telefonů, které se spouští současně, tato prodleva u jednotlivých jednotek zavádí rozptyl času zahájení požadavků resynchronizace. Tato funkce se může hodit ve velkém nasazení do domácností v případě místního výpadku dodávky energie.

Spouštěče

Telefon umožňuje provádět resynchronizaci v určených intervalech nebo v konkrétní čas.

Resynchronizace v zadaných intervalech

Telefon je navržen tak, aby se pravidelně resynchronizoval se zřizovacím serverem. Interval resynchronizace je konfigurován parametrem Resync_Periodic (v sekundách). Pokud je tato hodnota prázdná, zařízení se pravidelně neresynchronizuje.

K resynchronizaci obvykle dochází, když jsou hlasové linky nečinné. Pokud je ve chvíli naplánované resynchronizace aktivní hlasová linka, telefon resynchronizaci odloží do doby, než je linka opět nečinná. Resynchronizace může způsobit změnu hodnot parametrů konfigurace.

Resynchronizace může selhat, protože telefon nedokáže načíst ze serveru profil, stažený soubor je poškozený nebo došlo k interní chybě. Zařízení se pokusí znovu resynchronizovat po době, která je určena parametrem Resync_Error_Retry_Delay (v sekundách). Pokud je parametr Resync_Error_Retry_Delay nastaven na 0, zařízení se po neúspěšném pokusu o resynchronizaci nepokusí ji provést znovu.

Pokud se nezdaří upgrade, je opakovaný pokus proveden po sekundách nastavených v parametru Upgrade_Error_Retry_Delay.

K podmíněnému spuštění resynchronizace jsou k dispozici dva konfigurovatelné parametry: Resync_Trigger_1 a Resync_Trigger_2. Každý parametr lze naprogramovat pomocí podmíněného výrazu, který podléhá rozšíření makra. Když interval resynchronizace vyprší (čas na další resynchronizaci), spouštěče, pokud jsou nastavené, zabrání resynchronizaci, pokud není alespoň jeden z nich vyhodnocen jako pravdivý.

V následujícím příkladu je resynchronizace spuštěna podmíněně. V tomto příkladu poslední pokus o upgrade telefonu vypršel před více než 5 minutami (300 sekund) a od posledního pokusu o resynchronizaci uplynulo alespoň 10 minut (600 sekund).

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

Resynchronizace v zadaných časech

Parametr Resync_At umožňuje telefonu provádět resynchronizaci v určených intervalech nebo v konkrétní čas. Tento parametr využívá k zadání času 24hodinový formát (hhmm).

Parametr Resync_At_Random_Delay umožňuje telefonu provádět resynchronizaci po neurčité časové prodlevě. Tento parametr využívá k zadání času formát kladného celého čísla.

Je třeba předcházet zaplavení serveru požadavky na resynchronizaci od více telefonů, které jsou nastaveny na resynchronizaci ve stejný čas. Proto telefon spustí resynchronizaci až 10 minut po zadaném čase.

Pokud je například čas resynchronizace nastaven na 1000 (10.00), telefon spustí resynchronizaci kdykoliv mezi 10.00 a 10.10.

Ve výchozím nastavení je tato možnost vypnutá. Pokud je parametr Resync_At zřízen, je ignorován parametr Resync_Periodic.

Konfigurovatelné plány

Můžete nakonfigurovat plány pravidelných resynchronizací a zadat intervaly opakování při selhání resynchronizace a upgradu pomocí následujících parametrů:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Do každého parametru je možné zadat jednu hodnotu prodlevy (v sekundách). Nová rozšířená syntax umožňuje využít seznam po sobě jdoucích prvků prodlevy oddělených čárkami. Poslední prvek v řadě se automaticky opakuje donekonečna.

Nebo můžete použít znaménko plus a zadat jinou číselnou hodnotu, která znamená náhodnou prodlevu navíc.

Příklad 1

V tomto příkladu se telefon pravidelně resynchronizuje každé 2 hodiny. Pokud dojde k selhání resynchronizace, zařízení pokus opakuje v těchto intervalech: 30 minut, 1 hodina, 2 hodiny, 4 hodiny. Zařízení pokusy opakuje ve 4hodinových intervalech, dokud se resynchronizace nepodaří.

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

Příklad 2

V tomto příkladu se zařízení pravidelně resynchronizuje každou hodinu (plus až 10minutová náhodná prodleva navíc). V případě selhání resynchronizace zařízení pokus opakuje v těchto intervalech: 30 minut (plus až

5 minut). 1 hodina (plus až 10 minut), 2 hodiny (plus až 15 minut). Zařízení pokusy opakuje ve 2hodinových (plus až 15 minut) intervalech, dokud se resynchronizace nepodaří.

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

Příklad 3

Pokud se v tomto příkladu nepodaří provést upgrade, zařízení se pokusí ho provést za 30 minut, poté znovu po jedné hodině a poté po dvou hodinách. Pokud se provedení upgradu nepodaří ani tehdy, zařízení pokusy opakuje každé čtyři až pět hodin, dokud se upgrade nepodaří.

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

Pravidla profilu

Telefon má více parametrů profilu vzdálené konfigurace (Profile_Rule*). Při každé operaci resynchronizace je tak možné načíst více souborů, které spravují různé servery.

V nejjednodušším scénáři se zařízení pravidelně resynchronizuje s jedním profilem na centrálním serveru, který aktualizuje všechny důležité interní parametry. Nebo lze profil rozdělit na dva různé soubory. Jeden soubor je společný pro všechny telefony v nasazení. Každý účet má zvláštní, jedinečný soubor. Šifrovací klíče a údaje certifikátu může dodávat ještě jiný profil uložený na zvláštním serveru.

Vždy, když má dojít k operaci resynchronizace, telefon čtyři parametry Profile_Rule* vyhodnotí v následujícím pořadí:

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

Každé vyhodnocení může vést k načtení profilu ze vzdáleného zřizovacího serveru s možnou aktualizací několika interních parametrů. Pokud se vyhodnocení nezdaří, je resynchronizace přerušena a opakována od začátku po prodlevě určené v parametru Resync_Error_Retry_Delay (v sekundách). Pokud se vyhodnocení podaří, zařízení počká tolik sekund, kolik je uvedeno v parametru Resync_Periodic, a poté zahájí další resynchronizaci.

Obsah jednotlivých parametrů Profile_Rule* sestává ze sady alternativ. Alternativy se oddělují znakem |. Jednotlivé alternativy sestávají z podmíněného výrazu, výrazu přiřazení, adresy URL profilu a všech přiřazených možností adresy URL. Všechny tyto komponenty jsou u všech alternativ volitelné. Toto jsou platné kombinace a pořadí, ve kterém musí být případně uvedeny:

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

Ve všech parametrech Profile_Rule* musí všechny alternativy kromě poslední obsahovat podmíněný výraz. Tento výraz je vyhodnocen a zpracován následovně:

1. Podmínky jsou vyhodnocovány zleva doprava, dokud se nenarazí na takovou, která se vyhodnotí jako pravda (nebo dokud se nenajde alternativa, která podmíněný výraz nemá).
2. V případě zadání jsou vyhodnoceny všechny doprovodné výrazy přiřazení.
3. Pokud je jako součást dané alternativy zadána adresa URL, je proveden pokus o stažení profilu, který je na zadané adrese URL umístěn. Systém se pokusí příslušně aktualizovat interní parametry.

Pokud mají všechny alternativy podmíněný výraz a ani jeden není vyhodnocen jako pravda (nebo pokud je celé pravidlo profilu prázdné), je celý parametr Profile_Rule* přeskočen. Je vyhodnocen následující parametr pravidla profilu v pořadí.

Příklad 1

V tomto příkladu je provedena bezpodmínečná resynchronizace s profilem na zadané adrese URL a je odeslán požadavek HTTP GET na vzdálený zřizovací server:

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

Příklad 2

V tomto příkladu se zařízení resynchronizuje na dvě různé adresy URL v závislosti na stavu registrace linky 1. V případě ztráty registrace zařízení provede operaci HTTP POST na skript CGI. Zařízení odešle obsah proměnné GPP_A rozšířené makrem, která může poskytnout další informace o stavu zařízení:

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

Příklad 3

V tomto příkladu se zařízení resynchronizuje na stejný server. V případě, že v jednotce není nainstalovaný certifikát, zařízení poskytne další informace (u starších jednotek před verzí 2.0).

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

Příklad 4

V tomto příkladu je linka 1 zakázána, dokud proměnná GPP_A není první adresou URL nastavena na Zřízeno. Poté se resynchronizuje s druhou adresou URL:

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

Příklad 5

V tomto příkladu se předpokládá, že profil, který server vrátí, obsahuje značky elementu XML. Tyto značky musí pomocí aliasů uložených v proměnné GPP_B být přemapovány na odpovídající názvy parametrů:

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

Resynchronizace se obvykle považuje za neúspěšnou, pokud není ze serveru vyžádaný profil přijat. Pomocí parametru Resync_Fails_On_FNF je možné toto výchozí chování změnit. Když je parametr If Resync_Fails_On_FNF nastaven na Ne, zařízení přijme odpověď od serveru „file-not-found“ jako úspěšnou resynchronizaci. Výchozí hodnota parametru Resync_Fails_On_FNF je Ano.

Pravidlo upgradu

Pravidlo upgradu slouží jako pokyn zařízení, aby aktivovalo načtení a v případě potřeby informace, kde načtení získat. Pokud načtení v zařízení již je, zařízení se ho nepokusí získat. Když je požadované načtení v neaktivním oddílu, na platnosti umístění načtení tedy nezáleží.

Upgrade_Rule určuje načtení firmwaru, které bude staženo a použito, pokud se liší od aktuálního načtení a pokud není omezeno podmíněným výrazem nebo nastavením proměnné Upgrade_Enable na **Ne**.

Telefon poskytuje jeden konfigurovatelný parametr vzdáleného upgradu, Upgrade_Rule. Tento parametr má syntax obdobnou jako parametry pravidla profilu. Možnosti URL nejsou u upgradů podporovány, ale podmíněné výrazy a výrazy přiřazení použít lze. Pokud jsou používány podmíněné výrazy, je parametr možné naplnit více možnostmi, které se oddělují znakem |. Syntaxe pro jednotlivé alternativy je následující:

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

Stejně jako u parametrů Profile_Rule* i u parametrů Upgrade_Rule se vyhodnocují jednotlivé varianty, dokud není splněn podmíněný výraz nebo nějaká alternativa žádný podmíněný výraz nemá. V případě zadání je vyhodnocen doprovodný výraz přiřazení. Poté je proveden pokus o upgrade na zadané adrese URL.

Pokud proměnná Upgrade_Rule obsahuje adresu URL bez podmíněného výrazu, zařízení se upgraduje na obraz firmwaru na zadané adrese URL. Po rozšíření makra a vyhodnocení pravidla se zařízení znovu nepokusí o upgrade, dokud není pravidlo upraveno nebo není změněna skutečná kombinace protokol + server + port + cestaksouboru.

Při pokusu o upgrade firmwaru zařízení na začátku procesu vypne zvuk a na konci se restartuje. Zařízení automaticky zahájí upgrade, který je řízený obsahem proměnné Upgrade_Rule, jen v případě, kdy jsou všechny hlasové linky aktuálně neaktivní.

Příklad:

- U zařízení Cisco IP řady 6800:

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

  where BN==Build Number
  ```

V tomto příkladu Upgrade_Rule aktualizuje firmware na obraz, který je uložený na zadané adrese URL.

Zde je uveden další příklad k zařízení Cisco IP Phone řady 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
```

V tomto příkladu je zařízení dán příkaz načíst jeden ze dvou obrazů podle obsahu obecného parametru GPP_F.

Zařízení může vynutit limit downgradu podle čísla verze firmwaru, což může být praktická možnost přizpůsobení. Pokud je v parametru Downgrade_Rev_Limit nakonfigurováno platné číslo verze firmwaru, zařízení odmítne pokus o upgrade na verze firmwaru starší, než je zadaný limit.

Typy dat

V parametrech profilu konfigurace se používají tyto datové typy:

- {a,b,c,…} – Volba mezi a, b, c, …
- Bool – Logická hodnota „ano“, nebo „ne“.
- CadScript – Miniskript, který definuje parametry kadence signálu. Až 127 znaků.

  Syntax: $S_1[;S_2]$, kde:

  - $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ a označuje se jako část.
  - $on_{i,j}$ a $off_{i,j}$ jsou doby trvání vypnutí a zapnutí *segmentu*. i = 1 nebo 2 a j = 1 až 6.
  - D_i je celková doba trvání části v sekundách.

  Všechny doby trvání mohou mít až tři desetinná místa, aby se dalo dosáhnout přesnosti 1 ms. Zástupný znak „*“ znamená nekonečně dlouhé trvání. Segmenty v části se přehrávají v daném pořadí a opakují se, dokud není dosaženo celkové doby přehrávání.

  Příklad 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
  ```

  Příklad 2 – Rozpoznatelné zvonění (krátký, krátký, krátký, dlouhý):

  ```
  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 – Skriptovací syntaxe, která se používá u zadání plánů číslování linky 1 a linky 2.

- Float<n> – Hodnota s plovoucí desetinnou čárkou a až n desetinnými místy.
- FQDN – Plně kvalifikovaný název domény. Může obsahovat až 63 znaků. Toto jsou příklady:
  - sip.Cisco.com:5060 nebo 109.12.14.12:12345
  - sip.Cisco.com nebo 109.12.14.12
- FreqScript – Miniskript, který určuje parametry frekvence a hlasitosti tónu. Obsahuje až 127 znaků.

  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 jsou frekvence v Hz (pouze celá čísla bez znaménka).
  - L_1–L_6 jsou odpovídající hlasitosti v dBm (až s jedním desetinným místem).

  Bílé znaky před čárkou a po ní jsou povoleny, ale nejsou doporučovány.

  Příklad 1– Tón čekajícího hovoru:

```
440@-10

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

  Příklad 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 podobě x.x.x.x, kde x je mezi 0 a 255. Příklad: 10.1.2.100.
- UserID – ID uživatele, jak se uvádí v adrese URL; až 63 znaků.
- Telefon – Řetězec telefonního čísla, například 14081234567, *69, *72, 345678, nebo obecná adresa URL, například 1234@10.10.10.100:5068 nebo jsmith@Cisco.com. Řetězec může obsahovat až 39 znaků.
- PhTmplt – Šablona telefonního čísla. Každá šablona může obsahovat jeden nebo více vzorů oddělených čárkami (,). Bílý znaky na začátku jednotlivých vzorů jsou ignorovány. „?“ a „*“ představují zástupné znaky. Pokud chcete uvést přímo je, použijte %xx. Například %2a představuje *. Šablona může obsahovat až 39 znaků. Příklady: „1408*, 1510*“, „1408123????, 555?1.“.
- Port – Číslo portu TCP/UDP (0–65535). Zadání je možné v desítkovém nebo šestnáctkovém formátu.
- ProvisioningRuleSyntax – Syntaxe skriptování, která se používá k definici pravidel resynchronizace konfigurace a upgradu firmwaru.
- PwrLevel – Úroveň hlasitosti vyjádřená v dBm s jedním desetinným místem, např. −13,5 nebo 1,5 (dBm).
- RscTmplt – šablona stavového kódu odpovědi SIP, např. „404, 5*“, „61?“, „407, 408, 487, 481“. Může obsahovat až 39 znaků.
- Sig<n> – N-bitová hodnota se znaménkem. Zadání je možné v desítkovém nebo šestnáctkovém formátu. Před zápornými hodnotami musí být znak „-“. Znak + před kladnými hodnotami je volitelný.

- Kódy s hvězdičkami – Aktivační kód doplňkové služby, např. *69. Kód může obsahovat až 7 znaků.
- Str<n> – Obecný řetězec až s n nevyhrazenými znaky.
- Time<n> – Doba trvání v sekundách, až n desetinných míst. Další zadaná desetinná místa jsou ignorována.
- ToneScript – Miniskript, který určuje parametry frekvence, hlasitost a kadence tónu probíhajícího hovoru. Skript může obsahovat až 127 znaků.

  Syntax: FreqScript;Z_1[;Z_2].

  Oddíl Z_1 je podobný jako oddíl S_1 v části CadScript s tou výjimkou, že po každém segmentu zapnuto/vypnuto následuje parametr komponentu frekvence: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}[,on_{i,3}/off_{i,3}/f_{i,3}[,on_{i,4}/off_{i,4}/f_{i,4}[,on_{i,5}/off_{i,5}/f_{i,5}[,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$, kde:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ určuje komponenty frekvence v části FreqScript, které se v daném segmentu používají.

  Pokud se v segmentu používá více než jeden komponent frekvence, komponenty se sečtou.

  Příklad 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
```

  Příklad 2 – Tón čekání:

```
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 znaménka, kde n = 8, 16 nebo 32. Je možné ji zadat v desítkovém nebo šestnáctkovém formátu, např. 12 nebo 0x18. Hodnota se však musí vejít do n bitů.

Poznámka Mějte na paměti toto:

- <Nazev parametru> představuje název parametru konfigurace. Odpovídající značka v profilu je vytvořena záměnou mezery za podtržítko „_“, např. **Nazev_parametru**.
- Prázdné pole výchozí hodnoty představuje prázdný řetězec < “” >.
- Telefon u značek, které nejsou přítomny v daném profilu, poslední nakonfigurované hodnoty.
- Šablony se srovnávají v zadaném pořadí. Je vybrána první shoda, *ne ta nejlepší*. Název parametru musí odpovídat přesně.
- Pokud je v profilu zadána více než jedna definice parametru, v telefonu začne platit poslední taková definice v souboru.
- Zadání parametru na prázdnou hodnotu vrátí parametr na výchozí hodnotu. Pokud chcete místo toho zadat prázdný řetězec, použijte jako hodnotu parametru prázdný řetězec "".

Aktualizace profilu a upgrady firmwaru

Telefon podporuje zabezpečené vzdálené zřizování (konfiguraci) a upgrady firmwaru. Nezřízený telefon dokáže přijmout zašifrovaný profil, který je pro něj určen. Telefon kvůli mechanismu prvního zřizování, který využívá funkci SSL, nevyžaduje klíč explicitně.

Není vyžadován zásah uživatele na začátku ani při dokončení aktualizace profilu, upgradu firmwaru ani v případě, že jsou vyžadovány upgrady, aby se dal provést další upgrade ze starší verze. Pokus o resynchronizaci profilu se provádí pouze tehdy, když je telefon nečinný, protože resynchronizace může spustit restartování telefonu a odpojit hovor.

Proces zřizování řídí obecné parametry. Každý telefon lze nakonfigurovat, aby pravidelně kontaktoval normální zřizovací server (NPS). Komunikace s NPS nevyžaduje použití zabezpečeného protokolu, protože aktualizovaný profil lze zašifrovat pomocí sdíleného tajného klíče. NPS může být standardní server TFTP, HTTP nebo HTTPS s klientskými certifikáty.

Správce může upgradovat, restartovat nebo resynchronizovat telefony pomocí webového uživatelského rozhraní telefonu. Správce může tyto úlohy provádět také pomocí zprávy oznámení SIP.

Profily konfigurace jsou generovány pomocí běžných svobodných nástrojů, které se integrují se systémy zřizování poskytovatele služeb.

Související témata

Povolení a konfigurace aktualizací profilu, na straně 34

Povolení a konfigurace aktualizací profilu

Aktualizace profilu lze povolit v zadaných intervalech. Aktualizované profily jsou do telefonu odeslány ze serveru pomocí protokolu TFTP, HTTP nebo HTTPS.

Než začnete

Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Procedura

Krok 1 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 2 V části **Konfigurační profil** vyberte z rozevíracího seznamu**Povolit zřizování** možnost **Ano**.

Krok 3 Zadejte parametry.

Krok 4 Klikněte na tlačítko **Odeslat všechny změny**.

Související témata

Aktualizace profilu a upgrady firmwaru, na straně 34

Povolení a konfigurace upgradů firmwaru

Aktualizace firmwaru lze povolit v zadaných intervalech. Aktualizovaný firmware je do telefonu odeslán ze serveru pomocí protokolu TFTP nebo HTTP. Při upgradu firmwaru není zabezpečení takový problém, protože firmware neobsahuje osobní údaje.

Než začnete

Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Procedura

Krok 1 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 2 V části **Upgrade firmwaru** vyberte z rozevíracího seznamu **Povolit upgrade** možnost **Ano**.

Krok 3 Zadejte parametry.

Krok 4 Klikněte na tlačítko **Odeslat všechny změny**.

Upgrade firmwaru přes TFTP, HTTP nebo HTTPS

Telefon podporuje jeden upgrade obrazu přes protokol TFTP, HTTP nebo HTTPS.

Poznámka Downgrady na starší verze nemusí být dostupné pro všechna zařízení. Další informace naleznete v poznámkách k verzi telefonu a firmwaru.

Než začnete

Soubor načtení firmwaru musí být stažen na dostupný server.

Procedura

Krok 1 Obraz přejmenujte takto:

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

kde

x8xx je řada telefonu, například 6841.

aa-b-c je číslo vydané verze, např. 10-4-1

Krok 2 K rozbalení balíčku tar použijte příkaz **tar -xzvf**.

Krok 3 Zkopírujte složku do adresáře pro stažení přes protokol TFTP, HTTP nebo HTTPS.

Krok 4 Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Krok 5 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 6 Vyhledejte název souboru načtení, který končí **.loads** a připojte ho k platné adrese URL.

Krok 7 Klikněte na tlačítko **Odeslat všechny změny**.

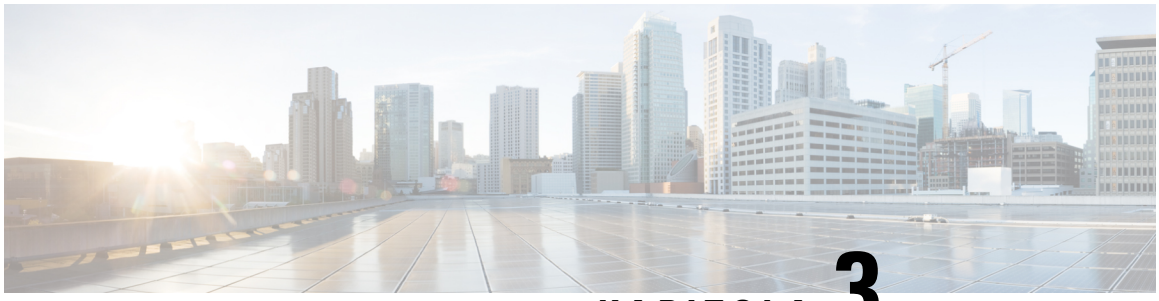
Upgrade firmwaru pomocí příkazu prohlížeče

K upgradu firmwaru na telefonu je možné použít příkaz k upgradu zadaný do adresního řádku prohlížeče. Telefon se upgraduje pouze tehdy, pokud je nečinný. Aktualizace se po dokončení hovoru automaticky spustí.

Procedura

Pokud chcete telefon upgradovat pomocí adresy URL ve webovém prohlížeči, použijte tento příkaz:

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



KAPITOLA 3

Servery předběžného zřizování a zřizování na pracovišti

Servery předběžného zřizování a zřizování na pracovišti

Poskytovatel služeb předem u telefonů, kromě jednotek RC, zřizuje profil. Profil předběžného zřizování se může skládat z omezené sady parametrů, které se s telefonem resynchronizují. Profil se může skládat také z úplné sady parametrů, které vzdálený server dodává. Ve výchozím nastavení se telefon resynchronizuje po spuštění a po intervalech nakonfigurovaných v profilu. Když uživatel připojí telefon na pracovišti zákazníka, zařízení stáhne aktualizovaný profil a všechny aktualizace firmwaru.

Tento proces předběžného zřizování, nasazování a vzdáleného zřizování lze provést mnoha způsoby.

Příprava serveru a softwarové nástroje

Příklady v této kapitole vyžadují dostupnost alespoň jednoho nebo více serverů. Tyto servery mohou být nainstalovány a spuštěny na místním počítači:

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

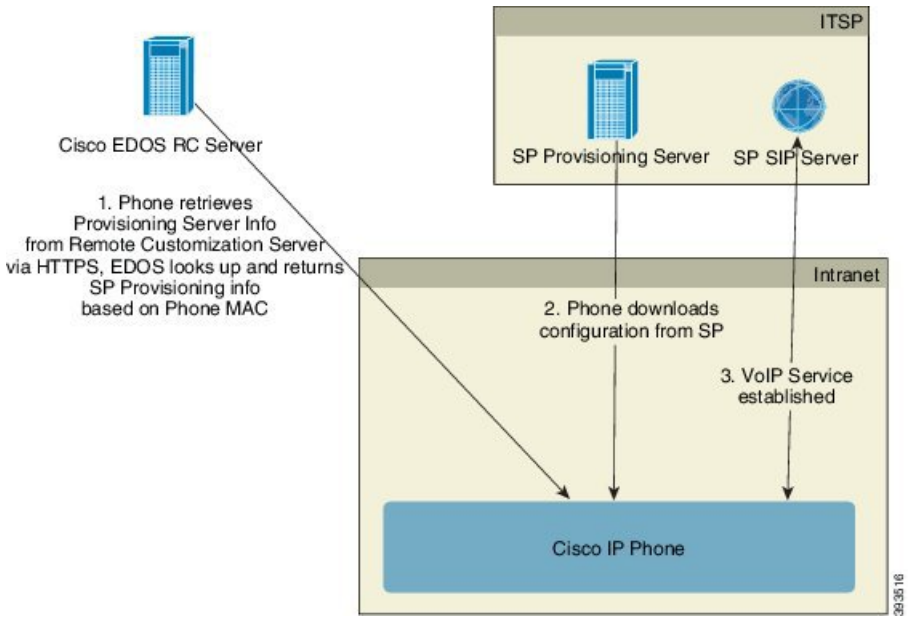
Při řešení potíží s konfigurací serveru pomáhá nainstalovat klienty pro jednotlivé typy serveru na zvláštní serverové počítače. Díky tomuto postupu se zavede správné fungování serveru nezávisle na komunikaci s telefony.

Doporučujeme, abyste si nainstalovali také tyto softwarové nástroje:

- Pro generování konfiguračních profilů si nainstalujte svobodný kompresní nástroj gzip.

- Na šifrování profilu a provoz HTTPS si nainstalujte svobodný softwarový balíček OpenSSL.
- K testování dynamického generování profilu a vzdáleného zřizování jedním krokem za použití HTTPS doporučujeme skriptovací jazyk s podporou skriptů CGI. Příkladem takového skriptovacího jazyka jsou svobodné nástroje jazyka Perl.
- K ověřování zabezpečené komunikace mezi zřizovacími servery a telefony si nainstalujte vyhledávač ethernetových paketů (jako je například volně stažitelný nástroj Ethereal/Wireshark). Zachyťte stopu ethernetového balíčku komunikace mezi telefonem a zřizovacím serverem. To uděláte tak, že spustíte vyhledávač paketů na počítači, který je připojen k přepínači se zapnutým zrcadlením portů. U transakcí HTTPS můžete používat nástroj ssldump.

Distribuce vzdáleného přizpůsobení (RC)



Do úvodního zřízení všechny telefony kontaktují server Cisco EDOS RC.

V distribučním modelu RC zákazník zakoupí telefon, který je na serveru Cisco EDOS RC již přiřazen ke konkrétnímu poskytovateli služeb. Poskytovatel služeb internetové telefonie (ITSP) nastavuje a udržuje zřizovací server a zaznamenává údaje o svém zřizovacím serveru na server Cisco EDOS RC.

Když je telefon spuštěn s připojením k internetu, stav přizpůsobení nezřízeného telefonu je **otevřený**. Telefon se na údaje o zřizovacím serveru nejprve dotáže místního serveru DHCP a nastaví si stav přizpůsobení. Pokud dotaz DHCP proběhl úspěšně, stav přizpůsobení se nastaví na **zrušeno** a RC se dále nezkouší, protože server DHCP poskytl potřebné údaje o zřizovacím serveru.

Když se připojí telefon poprvé do sítě nebo je v něm zavedeno tovární nastavení a nejsou nastaveny žádné možnosti DHCP, spojí se se serverem pro aktivaci zařízení, který zajistí bezobslužné zřízení. Nové telefony používají pro zřízení adresu “activate.cisco.com” namísto “webapps.cisco.com”. Telefony s firmwarem verze starší než 11.2(1) i nadále používají adresu webapps.cisco.com. Společnost Cisco doporučuje povolit oba názvy domén prostřednictvím firewallu.

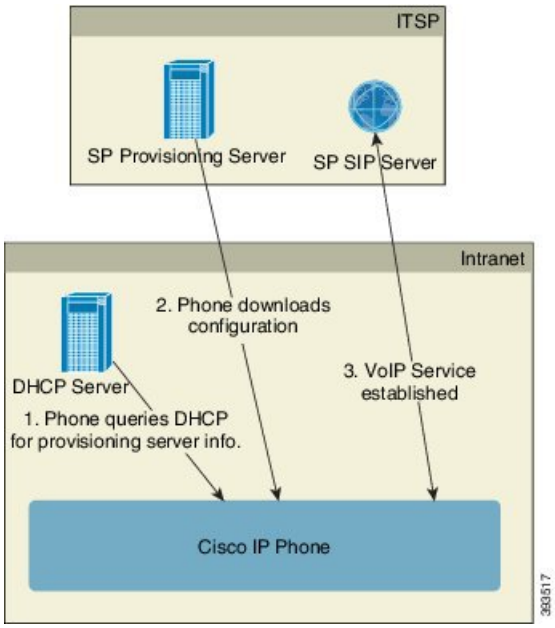
Pokud server DHCP neposkytne údaje o zřizovacím serveru, telefon se dotáže serveru Cisco EDOS RC a udá svou adresu MAC a model a stav přizpůsobení se nastaví na **Čeká na zpracování**. Server Cisco EDOS odpoví údaji o zřizovacím serveru přiřazeného poskytovatele služeb, mezi které patří adresa URL zřizovacího serveru, a stav přizpůsobení se nastaví na **Vlastní – čeká na zpracování**. Telefon poté provede příkaz adresy URL resynchronizace, načte konfiguraci poskytovatele služeb a v případě úspěchu se stav přizpůsobení nastaví na **Získáno**.

Pokud server Cisco EDOS RC nemá k telefonu přiřazeného poskytovatele služeb, stav přizpůsobení telefonu se nastaví na **Nedostupný**. Telefon lze nakonfigurovat ručně nebo lze na server Cisco EDOS přidat přiřazení k poskytovateli služeb telefonu.

Pokud je telefon zřízen prostřednictvím displeje nebo nástroje webové konfigurace předtím, než se stav přizpůsobení změní na **Získáno**, stav přizpůsobení se změní na **Přerušeno** a na server Cisco EDOS nebude poslán dotaz, dokud nedojde k obnovení továrního nastavení telefonu.

Po zřízení telefonu se server Cisco EDOS RC nepoužívá, pokud nedojde k obnovení továrního nastavení.

Předběžné zřizování zařízení na pracovišti



Ve výchozím továrním nastavení Cisco se telefon automaticky pokusí resynchronizovat s profilem na serveru TFTP. Spravovaný server DHCP na síti LAN zařízení poskytne informace o profilu a serveru TFTP, který je nakonfigurován na předběžné zřizování. Poskytovatel služeb připojí jednotlivé nové telefony do sítě LAN. Telefon se automaticky resynchronizuje s místním serverem TFTP a inicializuje svůj interní stav jako přípravu na nasazení. Tento profil předběžného zařizování obvykle obsahuje adresu URL vzdáleného zřizovacího serveru. Zřizovací server udržuje zařízení po nasazení a připojení do sítě zákazníka aktualizované.

Před odesláním zařízení zákazníkovi je možné naskenovat čárový kód předem zřízeného zařízení, a zaznamenat tak adresu MAC nebo sériové číslo. Tyto údaje lze použít k vytvoření profilu, se kterým se telefon resynchronizuje.

Po přijetí telefonu ho zákazník připojí k širokopásmovému připojení. Telefon po spuštění pomocí adresy URL nakonfigurované v rámci předběžného zřizování kontaktuje zřizovací server. Telefon se tak může resynchronizovat a podle potřeby aktualizovat profil a firmware.

Související témata

Maloobchodní distribuce, na straně 5
Zřizování TFTP, na straně 40

Nastavení zřizovacího serveru

V této části jsou popsány požadavky nastavení při zřizování telefonu za použití různých serverů a scénářů. Pro účely tohoto dokumentu a testování jsou zřizovací servery nainstalovány a spuštěny na místním počítači. Ke zřizování telefonů se hodí také obecně dostupné softwarové nástroje.

Zřizování TFTP

Telefony podporují protokol TFTP při resynchronizaci zřizování i upgradování firmwaru. Když jsou zařízení nasazena vzdáleně, doporučuje se protokol HTTPS, ale je možné použít protokol HTTP i TFTP. Pak je nutné pro větší zabezpečení provést šifrování zřizovacího souboru, protože nabízí větší spolehlivost vzhledem k ochranným mechanismům NAT a směrovače. Protokol TFTP se hodí pro předběžné zřizování na pracovišti většího množství nezřízených zařízení.

Telefon může získat adresu IP serveru TFTP přímo ze serveru DHCP prostřednictvím možnosti DHCP 66. Pokud je v parametru Profile_Rule nakonfigurována cesta k souboru daného serveru TFTP, zařízení z tohoto serveru TFTP stáhne svůj profil. Ke stažení dojde při připojení zařízení k síti LAN a spuštění.

Parametr Profile_Rule dodaný ve výchozí tovární konfiguraci je *&PN*.cfg, kde *&PN* představuje název modelu zařízení.

Například u modelu CP-6841-3PCC je název souboru CP-6841-3PCC.cfg.

Zařízení s profilem z továrního nastavení se při spuštění resynchronizuje s tímto souborem na místním serveru TFTP, který udává možnost 66 serveru DHCP. Cesta k souboru je relativní vzhledem k virtuálnímu kořenovému adresáři serveru TFTP.

Související témata

Předběžné zřizování zařízení na pracovišti, na straně 39

Řízení a NAT vzdáleného koncového bodu

Telefon je pro přístup k internetu prostřednictvím směrovače kompatibilní s překladem síťové adresy (NAT). K zajištění lepšího zabezpečení se směrovač může pokoušet blokovat neověřené příchozí pakety pomocí implementace symetrického NAT, což je strategie filtrování, která výrazně omezuje, které pakety mají přístup do chráněné sítě z internetu. Z tohoto důvodu není vzdálené zřizování použitím TFTP doporučováno.

Síť VoIP může s NAT fungovat jen tehdy, když je poskytována nějaká podoba obcházení NAT. Nakonfigurujte jednoduché obcházení UDP přes NAT (STUN). U této možnosti musí uživatel mít:

- Dynamickou externí (veřejnou) adresu IP od poskytovatele služeb
- Počítač se spuštěným softwarem serveru STUN
- Vstupní zařízení s mechanismem asymetrického NAT

Zřizování HTTP

Telefon se chová jako prohlížeč, který žádá o webové stránky ze vzdáleného webu na internetu. To poskytuje spolehlivý způsob, jak se dostat ke zřizovacímu serveru, i když směrovač zákazníka implementuje symetrické NAT nebo jiné ochranné mechanismy. Protokoly HTTP a HTTPS jsou ve vzdálených nasazeních spolehlivější než TFTP, zejména když jsou nasazené jednotky připojeny za firewally v domácnosti nebo směrovači s NAT. Protokoly HTTP a HTTPS jsou v následujících popisech typů požadavků zaměnitelné.

Základní zřizování na základě HTTP využívá k načtení konfiguračních profilů metodu HTTP GET. Obvykle je pro každý nasazený telefon vytvořen konfigurační soubor a tyto soubory jsou uloženy v adresáři serveru HTTP. Když server přijme požadavek GET, jednoduše vrátí soubor, který je zadaný v hlavičce požadavku GET.

Místo statického profilu je možné konfigurační profil možné generovat dynamicky dotázáním databáze zákazníka a vytvořením profilu za běhu.

Když telefon požádá o resynchronizaci, může k žádosti o data konfigurace resynchronizace použít metodu HTTP POST. Zařízení lze nakonfigurovat, aby na server v těle požadavku HTTP POST přeneslo určitý stav a identifikační údaje. Server využívá tyto údaje ke generování požadovaného konfiguračního profilu odpovědi nebo k uložení údajů o stavu pro pozdější analýzu a sledování.

Jako součást požadavku GET i POST telefon automaticky přikládá do pole User-Agent hlavičky požadavku identifikační údaje. Součástí těchto údajů je výrobce, název produktu, aktuální verze firmwaru a produktové sériové číslo zařízení.

Toto je příklad pole požadavku User-Agent od zařízení CP-6841-3PCC:

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

Když je telefon nakonfigurován na resynchronizaci s konfiguračním profilem pomocí protokolu HTTP, doporučujeme použití protokolu HTTPS nebo zašifrování protokolu, aby se chránily důvěrné údaje. Zašifrované profily, které telefon stáhne pomocí protokolu HTTP, brání vystavení důvěrných údajů, které jsou součástí konfiguračního profilu. Tento režim ve srovnání s protokolem HTTPS resynchronizace představuje nižší výpočetní zátěž na zřizovací server.

Telefon umožňuje dešifrování zašifrovaných profilů pomocí jedné z těchto metod:

- Šifrování AES-256-CBC
- Šifrování AES-128-GCM dat pomocí metody RFC 8188

Poznámka Telefony podporují protokol HTTP verze 1.0, HTTP verze 1.1 a dávkové kódování při použití přenosového protokolu HTTP verze 1.1.

Zacházení se stavovým kódem HTTP při resynchronizaci a upgradu

Telefon podporuje odpověď HTTP pro vzdálené zřizování (resynchronizaci). Aktuální chování telefonu lze rozdělit do tří kategorií:

- A – Úspěch, hodnoty „Pravidelná resynchronizace“ a „Náhodná prodleva resynchronizace“ určují následné požadavky.

- B – Neúspěch, soubor nebyl nalezen nebo je profil poškozený. Hodnota „Prodleva opakování po chybě resynchronizace“ určuje následné požadavky.
- C – Jiná chyba, nesprávná adresa URL nebo IP způsobuje chybu připojení. Hodnota „Prodleva opakování po chybě resynchronizace“ určuje následné požadavky.

Tabulka 2: Chování telefonu podle odpovědí HTTP

Stavový kód HTTP	Popis	Chování telefonu
301 Moved Permanently	Tento i další požadavky budou směřovány na nové umístění.	Okamžité opakování požadavku na novém umístění.
302 Found	Označuje se jako „dočasně přesunuto“.	Okamžité opakování požadavku na novém umístění.
3xx	Další odpovědi 3xx nejsou zpracovány.	C
400 Bad Request	Požadavek nelze naplnit kvůli špatné syntaxi.	C
401 Unauthorized	Žádost o ověření základního nebo výběrového přístupu.	Okamžité opakování požadavku s přihlašovacími údaji. Maximálně 2 opakování. Po chybě je chování telefonu C.
403 Forbidden	Server odmítá odpovídat.	C
404 Not Found	Požadovaný prostředek nebyl nalezen. Další požadavky klientem jsou přípustné.	B
407 Proxy Authentication Required	Žádost o ověření základního nebo výběrového přístupu.	Okamžité opakování požadavku s přihlašovacími údaji. Maximálně dvě opakování. Po chybě je chování telefonu C.
4xx	Další stavové kódy chyby klienty nejsou zpracovávány.	C
500 Internal Server Error	Obecná chybová zpráva.	Chování telefonu je C.
501 Not Implemented	Server nerozpoznává metodu požadavku nebo nedokáže požadavek splnit.	Chování telefonu je C.
502 Bad Gateway	Server funguje jako brána nebo proxy a od serveru za sebou obdržel neplatnou odpověď.	Chování telefonu je C.
503 Service Unavailable	Server momentálně není k dispozici (je přetížen nebo má odstávku kvůli údržbě). Jedná se o dočasný stav.	Chování telefonu je C.
504 Gateway Timeout	Server funguje jako brána nebo proxy a od serveru za sebou neobdržel včas odpověď.	C

Stavový kód HTTP	Popis	Chování telefonu
5xx	Další chyby serveru	C

Zřizování HTTPS

Telefon podporuje pro zřizování protokol HTTPS, což zvyšuje zabezpečení při správě vzdáleně nasazených jednotek. Každý telefon v sobě má jedinečný klientský certifikát SSL (a přiřazený privátní klíč) a navíc kořenový certifikát serveru Sipura CA. Ten telefonu umožňuje rozpoznávat autorizované zřizovací servery a odmítat neautorizované servery. Klientský certifikát na druhé straně umožňuje zřizovacímu serveru identifikovat konkrétní zařízení, které požadavek vydalo.

Aby poskytovatel služeb mohl spravovat nasazení pomocí protokolu HTTPS, pro každý zřizovací server, se kterým se telefon resynchronizuje pomocí protokolu HTTPS, musí být vygenerován serverový certifikát. Tento certifikát serveru musí být podepsán kořenovým klíčem Cisco Server CA, jehož certifikát je na všech nasazených jednotkách. K získání podepsaného certifikátu serveru musí poskytovatel služeb předat požadavek na podpis certifikátu společnosti Cisco, která certifikát serveru podepíše a vrátí k instalaci na zřizovací server.

Certifikát zřizovacího serveru musí v předmětu obsahovat pole pro obecný název (CN) a FQDN hostitele, na kterém je server spuštěn. Volitelně může obsahovat údaje následující FQDN hostitele, které se oddělují znakem lomítka (/). Následují příklady záznamů CN, které jsou telefonem přijímány jako platné:

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

Kromě ověření certifikátu serveru telefon kontroluje adresu IP serveru vyhledáním názvu serveru, který je v certifikátu serveru uvedený, v DNS.

Získání podepsaného certifikátu serveru

Nástroj OpenSSL dokáže vygenerovat požadavek na podpis certifikátu. V následujícím příkladu je uveden příkaz **openssl**, který vytvoří pár veřejný/privátní klíč 1024bitového RSA a požadavek na podepsání certifikátu:

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

Tento příkaz vygeneruje privátní klíč serveru do souboru **privkey.pem** a odpovídající požadavek na podepsání certifikátu do souboru **provserver.csr**. Poskytovatel služeb si nechá soubor **privkey.pem** v tajnosti a soubor **provserver.csr** odešle společnosti Cisco k podepsání. Po přijetí souboru **provserver.csr** společnost Cisco vygeneruje soubor **provserver.crt**, podepsaný certifikát serveru.

Procedura

Krok 1 Přejděte na stránku https://software.cisco.com/software/edos/home a přihlaste se pomocí přihlašovacích údajů CCO.

Poznámka Když se připojí telefon poprvé do sítě nebo je v něm zavedeno tovární nastavení a nejsou nastaveny žádné možnosti DHCP, spojí se se serverem pro aktivaci zařízení, který zajistí bezobslužné zřízení. Nové telefony používají pro zřízení adresu "activate.cisco.com" namísto "webapps.cisco.com". Telefony s firmwarem verze starší než 11.2(1) i nadále používají adresu "webapps.cisco.com". Doporučujeme povolit prostřednictvím firewallu oba názvy domén.

Krok 2 Vyberte možnost **Správa certifikátů**.

Na kartě **Podepsat CSR** se CSR z předchozího kroku nahraje k podepsání.

Krok 3 Z pole rozevíracího seznamu **Vybrat produkt** vyberte možnost **SPA1xx firmware 1.3.3 nebo novější / SPA232D firmware 1.3.3 nebo novější / SPA5xx firmware 7.5.6 nebo novější / CP-78xx-3PCC / CP-88xx-3PCC**.

Poznámka Tento produkt zahrnuje víceplatformové telefony řady Cisco IP Phone 6800.

Krok 4 V poli **Název souboru (soubor CSR)** klikněte na tlačítko **Procházet** a vyberte soubor CSR k podepsání.

Krok 5 Vyberte metodu šifrování:

- MD5
- SHA1
- SHA256

Společnost Cisco doporučuje zvolit šifrování SHA256.

Krok 6 V poli rozevíracího seznamu **Doba přihlášení** vyberte vhodnou délku trvání (například 1 rok).

Krok 7 Klikněte na možnost **Požadavek na podpis certifikátu**.

Krok 8 Pro příjem podepsaného certifikátu vyberte jednu z následujících možností:

- **Zadat e-mailovou adresu příjemce**: Pokud chcete certifikát dostat e-mailem, do tohoto pole zadejte svou e-mailovou adresu.
- **Stáhnout**: Pokud chcete podepsaný certifikát stáhnout, vyberte tuto možnost.

Krok 9 Klepněte na příkaz **Odeslat**.

Podepsaný certifikát serveru je odeslán e-mailem na zadanou e-mailovou adresu nebo stažen.

Klientský kořenový certifikát Sipura CA pro víceplatformové telefony

Společnost Cisco poskytuje poskytovatelům služeb také klientský kořenový certifikát pro víceplatformové telefony. Tento kořenový certifikát dosvědčuje pravost klientského certifikátu, který v telefonech je. Víceplatformové telefony podporují také certifikáty podepsané třetí stranou, například Verisign, Cybertrust atd.

Jedinečný klientský certifikát, který každé zařízení během relace HTTPS nabízí, obsahuje identifikační údaje, které jsou součástí pole předmět. Tyto údaje může server HTTPS zpřístupnit skriptu CGI spuštěnému, aby reagoval na zabezpečené požadavky. Předmět certifikátu obsahuje především název produktu jednotky (element OU), adresu MAC (element S) a sériové číslo (element L).

V následujícími příkladu víceplatformových telefonů Cisco IP Phone 6841 jsou v poli předmět klientského certifikátu tyto elementy:

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

K určení toho, zda je v telefonu individualizovaný certifikát, použijte proměnnou makra zřizování $CCERT. Hodnota proměnné se podle toho, zda je přítomen jedinečný klientský certifikát, rozšíří na „Nainstalovaný“ nebo „Nenainstalovaný“. V případě obecného certifikátu je možné z pole User-Agent hlavičky požadavku HTTP získat sériové číslo jednotky.

Servery HTTPS je možné nakonfigurovat tak, aby od připojujících se klientů vyžadovaly certifikáty SSL. Pokud je tato možnost zapnuta, může server k ověření klientského certifikátu použít klientský kořenový certifikát víceplatformového telefonu, který dodává společnost Cisco. Server může poté pro další zpracování poskytnout údaje o certifikátu skriptu CGI.

Umístění, kde je certifikát uložen, se může lišit. Například v instalaci Apache jsou cesty k místu, kde je uložen certifikát podepsaný zřizovacím serverem, jeho přiřazený privátní klíč a klientský certifikát víceplatformového telefonu CA, následující:

```
# 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
```

Konkrétní údaje naleznete v dokumentaci k serveru HTTPS.

Autorita kořene klientského certifikátu podepíše jednotlivé jedinečné certifikáty. Odpovídající kořenový certifikát je pro účely ověření klienta zpřístupněn poskytovatelům služeb.

Redundantní zřizovací servery

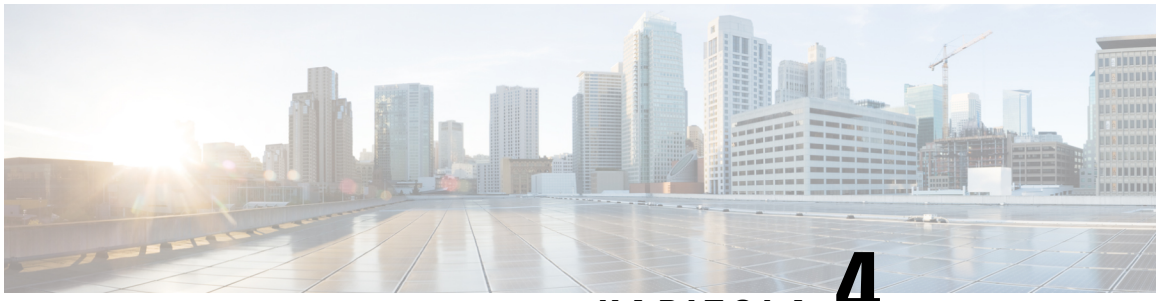
Zřizovací server lze zadat jako adresu IP nebo jako plně kvalifikovaný název domény (FQDN). Použití FQDN umožňuje nasazení redundantních zřizovacích serverů. Když je zřizovací server určen prostřednictvím FQDN, telefon se pokusí přiřadit FQDN k adrese IP prostřednictvím serveru DNS. Při zřizování jsou podporovány pouze záznamy DNS A. Zjišťování adresy DNS SRV není při zřizování k dispozici. Telefon pokračuje ve zpracovávání záznamů A, dokud nějaký server neodpoví. Pokud žádný server, který je přiřazený k záznamům A neodpoví, telefon na server syslog zaprotokoluje chybu.

Server syslog

Pokud je na telefonu pomocí parametrů <Syslog Server> nakonfigurován server syslog, operace resynchronizace a upgradu odesílají zprávy na server syslog. Na začátku požadavku na vzdálený server (profil konfigurace nebo načtení firmwaru) a na konci operace (oznámení úspěchu, nebo selhání) lze vygenerovat zprávu.

Zaprotokolované zprávy lze konfigurovat v následujících parametrech a rozšířit makrem do celých zpráv syslog:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



KAPITOLA 4

Příklady zřizování

Přehled příkladů zřizování

V této kapitole jsou uvedeny příklady postupů přenosu konfiguračních profilů mezi telefonem a zřizovacím serverem.

Informace o vytváření konfiguračních profilů naleznete v části Zřizovací skripty, na straně 13.

Základní resynchronizace

V této části je ukázka základní funkce resynchronizace telefonů.

Resynchronizace TFTP

Telefon podporuje více síťových protokolů k načítání konfiguračních profilů. Nejzákladnější protokol pro přenos profilu je TFTP (RFC1350). Protokol TFTP je široce využíván ke zřizování síťových zařízení v rámci privátních sítí LAN. Ačkoliv se protokol TFTP nedoporučuje pro nasazování vzdálených koncových bodů přes internet, může jít o praktickou možnost při nasazování v malé organizace pro předběžné zřizování na pracovišti a při vývoji a testování. Další informace o předběžném zřizování na pracovišti naleznete v části Předběžné zřizování zařízení na pracovišti, na straně 39. V následujícím postupu je upraven profil po stažení souboru ze serveru TFTP.

Procedura

Krok 1 V prostředí LAN připojte počítač a telefon k rozbočovači, přepínači nebo malému směrovači.

Krok 2 V počítači nainstalujte a aktivujte server TFTP.

Krok 3 Pomocí textového editoru vytvořte profil konfigurace, ve kterém je hodnota GPP_A nastavena na 12345678, jak je uvedeno v příkladu.

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

Krok 4 Profil uložte do kořenového adresáře serveru pod názvem `basic.txt`.

Že je server TFTP správně nakonfigurován, můžete ověřit takto: vyžádejte si soubor `basic.txt` pomocí jiného klienta TFTP, než je telefon. Ideálně použijte klienta TFTP, který je spuštěn na jiném hostiteli než zřizovací server.

Krok 5 Otevřete webový prohlížeč v počítači na stránce konfigurace správce/pokročilé. Pokud je například adresa IP telefonu 192.168.1.100:

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

Krok 6 Vyberte kartu **Hlas** > **Zřizování** a podívejte se na hodnoty obecných parametrů GPP_A až GPP_P. Měly by být prázdné.

Krok 7 Otevřením adresy URL resynchronizace v okně webového prohlížeče resynchronizujte testovací telefon s profilem konfigurace `basic.txt`.

Pokud je adresa IP serveru TFTP 192.168.1.200, příkaz by měl vypadat nějak takto:

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

Když telefon tento příkaz obdrží, zařízení na adrese 192.168.1.100 požádá server TFTP na adrese 192.168.1.200 o soubor `basic.txt`. Telefon poté analyzuje stažený soubor a aktualizuje parametr GPP_A na hodnotu 12345678.

Krok 8 Ověřte, že byl parametr správně aktualizován: Obnovte stránku konfigurace ve webovém prohlížeči na telefonu a vyberte kartu **Hlas** > **Zřizování**.

Parametr GPP_A by nyní měl obsahovat hodnotu 12345678.

Používání serveru Syslog k protokolování zpráv

Telefon na určený server syslog odešle zprávu syslog, když se zařízení chystá resynchronizovat na zřizovací server a když je resynchronizace dokončena nebo se nezdařila. Tento server můžete určit na webové stránce pro správu telefonu (viz Otevření webové stránky telefonu, na straně 7), kde vyberete možnost **Hlas** > **Systém** a zadáte server do parametru **Server Syslog** v části **Volitelná konfigurace sítě**. Nakonfigurujte adresu IP serveru syslog do zařízení a sledujte zprávy, které jsou během zbývajících postupů vygenerovány.

Procedura

Krok 1 Na místním počítači nainstalujte a aktivujte server syslog.

Krok 2 Naprogramujte adresu IP počítače do parametru Syslog_Server profilu a změnu potvrďte:

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

Krok 3 Klikněte na kartu **Systém** a do parametru Syslog_Server zadejte hodnotu místního serveru syslog.

Krok 4 Opakujte operaci resynchronizace, jak je popsána v části Resynchronizace TFTP, na straně 47.

Zařízení během resynchronizace vygeneruje dvě zprávy syslog. První zpráva znamená, že požadavek probíhá. Druhá zpráva označuje úspěšné nebo neúspěšné provedení resynchronizace.

Krok 5 Zkontrolujte, zda váš server syslog obdržel zprávy podobné těmto:

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

Podrobné zprávy jsou k dispozici po naprogramování parametru Debug_Server (místo parametru Syslog_Server) na adresu IP serveru syslog a nastavení parametru Debug_Level na hodnotu mezi 0 a 3 (3 znamená nejpodrobnější informace):

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

Obsah těchto zpráv je možné nakonfigurovat pomocí následujících parametrů:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Pokud je některý z těchto parametrů vymazán, příslušná zpráva syslog se negeneruje.

Automatická resynchronizace zařízení

Zařízení se může se zřizovacím serverem pravidelně resynchronizovat, aby se zajistilo, že se všechny změny profilu provedené na serveru dostanou do koncového zařízení (místo odeslání explicitního požadavku na resynchronizaci koncovému bodu).

Aby se telefon pravidelně resynchronizoval se serverem, pomocí parametru Profile_Rule je definována adresa URL konfiguračního profilu a pomocí parametru Resync_Periodic je definován interval resynchronizace.

Než začnete

Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Procedura

Krok 1 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 2 Definujte parametr Profile_Rule. V tomto příkladu se předpokládá, že adresa IP serveru TFTP je 192.168.1.200.

Krok 3 Do pole **Pravidelná resynchronizace** zadejte na testování malou hodnotu, např. **30** sekund.

Krok 4 Klikněte na tlačítko **Odeslat všechny změny**.

S novým nastavením parametru se telefon s konfiguračním souborem určeným adresou URL resynchronizuje dvakrát za minutu.

Krok 5 Sledujte výsledné zprávy ve sledování syslog (jak je popsáno v části Používání serveru Syslog k protokolování zpráv, na straně 48).

Krok 6 Pole **Resynchronizace při restartování** musí být nastaveno na **Ano**.

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

Krok 7 Telefon restartujte, a vynuťte tak resynchronizaci se zřizovacím serverem.

Pokud se resynchronizace z nějakého důvodu nezdaří, například když server neodpovídá, jednotka počká (počet sekund nakonfigurovaný v parametru **Prodleva opakování po chybě resynchronizace**)a poté se znovu pokusí o resynchronizaci. Pokud je parametr **Prodleva opakování po chybě resynchronizace** nastaven na nulu, telefon se po neúspěšném pokusu o resynchronizaci nepokusí ji provést znovu.

Krok 8 (Volitelně) Nastavte hodnotu pole **Prodleva opakování po chybě resynchronizace** na malé číslo, například **30**.

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

Krok 9 Deaktivujte server TFTP a sledujte výsledky na výstupu syslog.

Jedinečné profily, rozšíření makra a HTTP

V nasazeních, kde musí být každý telefon nakonfigurován s jedinečnými hodnotami u některých parametrů, jako jsou např. User_ID nebo Display_Name, může poskytovatel služeb vytvořit jedinečný profil pro každé nasazené zařízení a hostovat tyto profily na zřizovacím serveru. Každý telefon potom musí být nakonfigurovaný, aby se resynchronizoval na vlastní profil v souladu s předem určenými pravidly pojmenování profilů.

Syntaxe URL profilu může pomocí rozšíření makra integrovaných proměnných obsahovat identifikující údaje, které jsou pro každý telefon jedinečné, jako je adresa MAC nebo sériové číslo. Rozšíření makra eliminuje potřebu zadávat tyto hodnoty na různých místech v rámci jednoho profilu.

Pravidlo profilu prodělá rozšíření makra před použitím pravidla v telefonu. Rozšíření makra řídí počet hodnot, například:

- $MA se rozšíří na 12číselnou adresu MAC (s malými šestnáctkovými znaky). Například 000e08abcdef.
- $SN se rozšíří na sériové číslo jednotky. Například 88012BA01234.

Tímto způsobem mohou být makrem rozšířeny další hodnoty, včetně všech obecných parametrů, GPP_A až GPP_P. Příklad tohoto procesu si můžete prohlédnout v části Resynchronizace TFTP, na straně 47. Rozšíření makra není omezeno na název souboru URL, ale lze ho použít také na libovolnou část parametru pravidla profilu. Tyto parametry se označují jako $A až $P. Úplný seznam proměnných, které jsou k dispozici k rozšíření makrem, naleznete v části Proměnné rozšíření makra, na straně 72.

V tomto cvičení profil k telefonu zřizuje server TFTP.

Cvičení: Zřídit profil konkrétního IP telefonu na serveru TFTP

Procedura

Krok 1 Zjistěte z produktového štítku adresu MAC telefonu. (Adresa MAC je číslo z číslic a malých šestnáctkových čísel, například, 000e08aabbcc.

Krok 2 Zkopírujte konfigurační soubor `basic.txt` (popsaný v části Resynchronizace TFTP, na straně 47) do nového souboru s názvem `CP-xxxx-3PCC macaddress.cfg` (kde nahradíte `xxxx` číslem modelu a `macaddress` adresou MAC telefonu).

Krok 3 Nový soubor přesuňte do virtuálního kořenového adresáře serveru TFTP.

Krok 4 Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Krok 5 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 6 Do pole **Pravidlo profilu** zadejte `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 Klikněte na tlačítko **Odeslat všechny změny**. To způsobí okamžité restartování a resynchronizaci.

Když dojde k další resynchronizaci, telefon načte nový soubor rozšířením výrazu makra $MA na adresu MAC telefonu.

Resynchronizace HTTP GET

Protokol HTTP poskytujte spolehlivější mechanismus resynchronizace než TFTP, protože v rámci protokolu HTTP je vytvořené připojení TCP a protokol TFTP využívá méně spolehlivé připojení UDP. Servery HTTP navíc ve srovnání se servery TFTP nabízejí vylepšené funkce filtrování a protokolování.

Pokud jde o stranu klienta, telefon nevyžaduje na serveru žádné zvláštní nastavení konfigurace, aby mohl provést resynchronizaci pomocí protokolu HTTP. Syntaxe parametru Profile_Rule pro použití protokolu HTTP s metodou GET je obdobná jako syntax, která se používá u protokolů TFTP. Pokud standardní webový prohlížeč dokáže načíst profil ze serveru HTTP, telefon by to měl dokázat také.

Cvičení: Resynchronizace HTTP GET

Procedura

Krok 1 Nainstalujte server HTTP na místní počítač nebo jiného přístupného hostitele.

Z internetu je možné stáhnout svobodný server Apache.

Krok 2 Profil konfigurace `basic.txt` (popsaný v části Resynchronizace TFTP, na straně 47) zkopírujte do virtuálního kořenového adresáře nainstalovaného serveru.

Krok 3 Abyste ověřili správnou instalaci serveru a přístup k souboru `basic.txt`, otevřete profil ve webovém prohlížeči.

Krok 4 Upravte pravidlo Profile_Rule testovacího telefonu tak, aby místo serveru TFTP mířilo na server HTTP, aby se profil stahoval pravidelně.

Pokud je server HTTP například 192.168.1.300, zadejte následující hodnotu:

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

Krok 5 Klikněte na tlačítko **Odeslat všechny změny**. To způsobí okamžité restartování a resynchronizaci.

Krok 6 Podívejte se na zprávy syslog, které telefon odesílá. Při pravidelných resynchronizacích by nyní mělo docházet k získávání profilu ze serveru HTTP.

Krok 7 V protokolech serveru HTTP sledujte, že se v protokolu uživatelských agentů objevují údaje identifikující testovací telefon.

Součástí tohoto údaje by měl být výrobce, název produktu, aktuální verze firmwaru a sériové číslo.

Zřizování pomocí souboru Cisco XML

U každého telefonu, který je zde označen jako xxxx, můžete provést zřizování pomocí funkcí Cisco XML.

Do telefonu můžete prostřednictvím paketů oznámení SIP nebo metodou HTTP Post na rozhraní CGI telefonu poslat objekt XML: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC rozšiřuje funkci Cisco XML k podpoře zřizování prostřednictvím objektu XML:

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

Poté co telefon obdrží objekt XML, stáhne zřizovací soubor z [profile-rule]. Toto pravidlo využívá ke zjednodušení vývoje aplikace služeb XML makra.

Analýza URL s rozšířením makra

Podsložky s více profily na serveru představují praktickou metodu správy velkého počtu nasazených zařízení. Adresa URL profilu může obsahovat:

- název zřizovacího serveru nebo přímo adresu IP. Pokud profil identifikuje zřizovací server podle názvu, telefon k analýze názvu provede vyhledávání v serveru DNS.
- Nestandardní port serveru, který je zadaný v adrese URL pomocí standardní syntaxe `:port` za názvem serveru.
- Podadresář virtuálního kořenového adresáře serveru, kde je profil uložen, zadaný pomocí standardní notace adresy URL a spravovaný rozšířením makra.

Například následující Profile_Rule si vyžádá soubor profilu ($PN.cfg) v podsložce serveru `/cisco/config` ze serveru TFTP, který je spuštěn na hostiteli prov.telco.com a očekává připojení na portu 6900:

```
<Profile_Rule>
```

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

Profil lze u jednotlivých telefonů identifikovat pomocí obecného parametru, na jehož hodnotu se odkáže v obecném pravidle profilu pomocí rozšíření makra.

Dejme tomu, že je GPP_B definováno jako `Dj6Lmp23Q`.

Profile_Rule má hodnotu:

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

Když se zařízení resynchronizuje a makra jsou rozšířena, telefon s adresou 000e08012345 si vyžádá profil s názvem, který obsahuje adresu MAC zařízení na následující adrese URL:

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

Zabezpečená resynchronizace HTTP

Na telefonu jsou pro resynchronizaci pomocí zabezpečeného procesu komunikace k dispozici tyto mechanismy:

- Základní resynchronizace HTTP
- Ověření HTTP s klientským certifikátem
- Filtrování klienta HTTPS a dynamický obsah

Základní resynchronizace HTTP

Protokol HTTPS má pro vzdálené zřizování oproti protokolu HTTP navíc SSL, takže:

- Telefon může ověřovat zřizovací server.
- Zřizovací server může ověřovat telefon.
- Je zajištěna důvěrnost dat vyměňovaných mezi telefonem a zřizovacím serverem.

SSL u každého připojení mezi telefonem a serverem pomocí párů veřejný/privátní klíč, které jsou předinstalovány v telefonu a na zřizovacím serveru, vygeneruje a navzájem vymění privátní (symetrické) klíče.

Pokud jde o stranu klienta, telefon nevyžaduje na serveru žádné zvláštní nastavení konfigurace, aby mohl provést resynchronizaci pomocí protokolu HTTPS. Syntaxe parametru Profile_Rule pro použití protokolu HTTPS s metodou GET je obdobná jako syntax, která se používá u protokolů HTTP a TFTP. Pokud standardní webový prohlížeč dokáže načíst profil ze serveru HTTPS, telefon by to měl dokázat také.

Kromě instalace serveru HTTPS musí být na zřizovacím serveru nainstalován certifikát serveru SSL podepsaný společností Cisco. Zařízení se nemohou resynchronizovat se serverem, který využívá protokol HTTPS, pokud server nedodá certifikát serveru podepsaný společností Cisco. Pokyny k vytvoření podepsaných certifikátů SSL pro hlasové produkty lze najít na adrese https://supportforums.cisco.com/docs/DOC-9852.

Cvičení: Základní resynchronizace HTTP

Procedura

Krok 1 Nainstalujte server HTTPS na hostitele, jehož adresa IP je serveru DNS sítě známá prostřednictvím normálního překladu názvu hostitele.

Svobodný server Apache lze v instalaci se svobodným balíčkem mod_ssl nakonfigurovat tak, aby fungoval jako server HTTPS.

Krok 2 Pro server vygenerujte požadavek na podepsání certifikátu serveru. Na tento krok možná budete muset nainstalovat svobodný balíček OpenSSL nebo podobný software. Pokud používáte OpenSSL, příkaz k vygenerování základního souboru CSR je následující:

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

Tento příkaz vygeneruje pár veřejný/privátní klíč, který se uloží do souboru `privkey.pem`.

Krok 3 Odešlete soubor CSR (provserver.csr) společnosti Cisco k podepsání.

Vrátí se podepsaný certifikát serveru (provserver.cert) spolu s klientským kořenovým certifikátem Sipura CA, spacroot.cert.

Další informace naleznete v tématu https://supportforums.cisco.com/docs/DOC-9852.

Krok 4 Uložte podepsaný certifikát serveru, soubor s párem privátního klíče a klientský kořenový certifikát do příslušných umístění na serveru.

V případě instalace Apache v systému Linux jsou tato umístěný typicky následující:

```
# 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 Restartujte server.

Krok 6 Soubor konfigurace `basic.txt` (popsaný v části Resynchronizace TFTP, na straně 47) zkopírujte do virtuálního kořenového adresáře nainstalovaného serveru HTTPS.

Krok 7 Ověřte správné fungování serveru stažením souboru `basic.txt` ze serveru HTTPS v běžném prohlížeči na místním počítači.

Krok 8 Zkontrolujte certifikát serveru, který server dodá.

Prohlížeč pravděpodobně nerozpozná certifikát jako platný, pokud nebyl předem nakonfigurován, aby přijal společnost Cisco jako kořenovou CA. Telefony však očekávají, že certifikát bude podepsán tímto způsobem.

Upravte hodnotu Profile_Rule na testovacím zařízení, aby obsahovala odkaz na server HTTP, například:

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

```
</Profile_Rule>
```

V tomto příkladu se předpokládá, že název serveru HTTPS je **my.server.com**.

Krok 9 Klikněte na tlačítko **Odeslat všechny změny**.

Krok 10 Podívejte se na sledování syslog, které telefon odesílá.

Ze zpráv syslog by mělo vyplývat, že při resynchronizaci byl profil získán ze serveru HTTPS.

Krok 11 (Nepovinné) K ověření toho, že jsou pakety zašifrovány, použijte analyzátor ethernetového protokolu na podsíti telefonu.

V tomto cvičení není ověření klientského certifikátu povoleno. Připojení mezi telefonem a serverem je zašifrováno. Přenos však není zabezpečený, protože se k serveru může připojit libovolný klient a soubor si vyžádat, pokud zná jeho název a umístění v adresáři. Aby byla resynchronizace zabezpečená, server musí ověřit také klient, jak je demonstrováno v cvičení popsaném v části Ověření HTTP s klientským certifikátem, na straně 55.

Ověření HTTP s klientským certifikátem

Ve výchozím továrním nastavení server nepožaduje klientský certifikát SSL od klienta. Přenos profilu není zabezpečený, protože se k serveru může připojit libovolný klient a profil si vyžádat. Konfiguraci můžete upravit tak, aby bylo povoleno ověření klienta. Server k ověření telefonu před přijetím požadavku na připojení vyžaduje klientský certifikát.

Kvůli tomuto požadavku nelze operaci resynchronizace nezávisle otestovat pomocí prohlížeče bez správných přihlašovacích údajů. Výměnu klíče v rámci připojení HTTPS mezi testovacím telefonem a serverem lze sledovat pomocí nástroje ssldump. Stopa nástroje ukazuje komunikace mezi klientem a serverem.

Cvičení: Ověření HTTP s klientským certifikátem

Procedura

Krok 1 Zapněte na serveru HTTPS ověření klientského certifikátu.

Krok 2 Na serveru Apache (v. 2) nastavte následující konfigurační soubor serveru:

```
SSLVerifyClient  require
```

Zajistěte také, aby byl soubor spacroot.cert uložen jako ve cvičení Základní resynchronizace HTTP, na straně 53.

Krok 3 Server HTTPS restartujte a v telefonu se podívejte na sledování syslog.

Při každé resynchronizaci serveru se nyní provádí symetrické ověření, takže před přenosem profilu je ověřen certifikát serveru i klientský certifikát.

Krok 4 Pomocí příkazu ssldump zachyťte resynchronizační připojení mezi telefonem a serverem HTTPS.

Pokud je ověření klientského certifikátu na serveru správně zapnuto, je ve stopě ssldump vidět symetrická výměna certifikátů (nejprve server-klient a poté klient-server) a následně zašifrované pakety, které obsahují profil.

Když je zapnuté ověření klienta, může si profil ze zřizovacího serveru vyžádat pouze telefon s adresou MAC, která odpovídá platnému certifikátu. Server zamítne požadavek od běžného prohlížeče nebo jiného neautorizovaného zařízení.

Filtrování klienta HTTPS a dynamický obsah

Pokud je server HTTPS nakonfigurován tak, aby vyžadoval klientský certifikát, resynchronizovaný telefon identifikují údaje v certifikátu, které také obsahují správné konfigurační údaje.

Server HTTPS údaje certifikátu zpřístupní skriptům CGI (nebo zkompilovaným programům CGI), které jsou v rámci požadavku na resynchronizaci spuštěny. Pro demonstrační účely je v tomto cvičení využívat svobodný skriptovací jazyk Perl a předpokládá se, že jako server HTTPS je využíván server Apache (v. 2).

Procedura

Krok 1 Nainstalujte jazyk Perl na hostitele, na kterém je server HTTPS spuštěný.

Krok 2 Vygenerujte následující reflexní skript Perl:

```
#!/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 soubor pod názvem `reflect.pl` do adresáře se skripty CGI serveru HTTPS s oprávněním ke spouštění (chmod 755 v systému Linux).

Krok 4 Ověřte dostupnost skriptů CGI na serveru (to znamená `/cgi-bin/…`).

Krok 5 Upravte hodnotu Profile_Rule na testovacím zařízení, a proveďte tak resynchronizaci reflexního skriptu. Níže je uveden příklad:

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

Krok 6 Klikněte na tlačítko **Odeslat všechny změny**.

Krok 7 Podívejte se na sledování syslog a ověřte tak, že resynchronizace proběhla úspěšně.

Krok 8 Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Krok 9 Vyberte možnosti **Hlas** > **Zřizování**.

Krok 10 Ověřte, že parametr GPP_C obsahuje údaje, které skript zachytil.

Součástí těchto údajů je název produktu, adresa MAC a sériové číslo, pokud testovací zařízení má unikátní certifikát od výrobce. Pokud byla jednotka vyrobena před vydanou verzí firmwaru 2.0, obsahují údaje obecný řetězec.

Podobný skript dokáže určit údaje o resynchronizačním zařízení a poté mu poskytnout vhodné hodnoty parametrů konfigurace.

Certifikáty HTTPS

Telefon poskytuje spolehlivou a bezpečnou strategii zřizování, která je založena na požadavcích HTTPS od zařízení zřizovacímu serveru. K ověření telefonu u serveru a serveru u telefonu se používá certifikát serveru i klientský certifikát.

Pokud chcete s telefonem použít protokol HTTPS, musíte vygenerovat požadavek na podepsání certifikátu (CSR) a odeslat ho společnosti Cisco. Telefon vygeneruje certifikát k instalaci na zřizovací server. Telefon certifikát přijme, když se pokouší ke zřizovacímu serveru vytvořit připojení HTTPS.

Metodologie HTTPS

Protokol HTTPS šifruje komunikaci mezi klientem a serverem, čímž chrání obsah zpráv od ostatních síťových zařízení. Metoda šifrování pro tělo komunikace mezi klientem a serverem je založena na šifrování symetrickým klíčem. Díky šifrování symetrickým klíčem klient a server sdílejí jeden tajný klíč přes zabezpečený kanál, který je chráněn šifrováním s veřejným/privátním klíčem.

Zprávy zašifrované tajným klíčem je možné rozšifrovat pouze pomocí stejného klíče. Protokol HTTPS podporuje širokou řadu algoritmů symetrického šifrování. V telefonu je kromě 128bitového šifrování RC4 implementováno 256bitové symetrické šifrování za použití standardu AES (American Encryption Standard).

Protokol HTTPS umožňuje také ověření serveru a klienta zapojených do zabezpečené transakce. Tato funkce zajišťuje, že zřizovací server a jednotliví klienti se nedají podvrhnout jinými zařízeními v síti. Tato funkce je v kontextu vzdáleného zřizování koncového bodu klíčová.

Ověření serveru a klienta se provádí pomocí šifrování s veřejným/privátním klíčem s certifikátem, který obsahuje veřejný klíč. Text, který je zašifrován veřejným klíčem, může být rozšifrován pouze pomocí příslušného privátního klíče (a naopak). Telefon podporuje pro šifrování s veřejným/privátním klíčem algoritmus Rivest-Shamir-Adleman (RSA).

Certifikát serveru SSL

Každý zabezpečený zřizovací server má vydaný certifikát serveru SSL, který společnost Cisco přímo podepisuje. Firmware, který je v telefonu, jako platný rozpoznává pouze certifikát Cisco. Když se klient připojí k serveru pomocí protokolu HTTPS, odmítne jakýkoliv certifikát serveru, který není podepsaný společností Cisco.

Tento mechanismus chrání poskytovatele služeb před neoprávněným přístupem k telefonu a všemi pokusy podvrhnutí falešného zřizovacího serveru. Bez takové ochrany by mohl útočník dokázat změnit zřízení telefonu, aby získal konfigurační údaje nebo použil jinou službu VoIP. Bez privátního klíče, který odpovídá platnému certifikátu serveru, nedokáže útočník zahájit komunikaci s telefonem.

Získat certifikát serveru

Procedura

Krok 1 Kontaktujte pracovníka podpory Cisco, který vás procesem certifikace provede. Pokud nespolupracujete s konkrétním pracovníkem podpory, odešlete e-mail se svým požadavkem na adresu ciscosb-certadmin@cisco.com.

Krok 2 Vygenerujte si soukromý klíč, který se bude používat v CSR (požadavek na podpis certifikátu). Tento klíč je privátní a nemusíte ho uvádět podpoře Cisco. K vygenerování klíče použijte svobodný nástroj „openssl“. Příklad:

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

Krok 3 Vygenerujte CSR, který obsahuje políčka, která identifikují vaši organizaci a umístění. Příklad:

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

Musíte použít tyto údaje:

- Pole Předmět – zadejte obecný název (CN), který musí mít syntaxi FQDN (plně kvalifikovaný název domény). Během handshaku ověření SSL telefon ověří, že certifikát, který obdrží, je od zařízení, které ho odeslalo.
- Název hostitele serveru – například, provserv.domain.com.
- E-mailová adresa – zadejte e-mailovou adresu, aby vás v případě potřeby mohla kontaktovat zákaznická podpora. Tato e-mailová adresa je v CSR viditelná.

Krok 4 Odešlete CSR e-mailem (v souboru ZIP) pracovníkovi podpory Cisco nebo na adresu ciscosb-certadmin@cisco.com. Certifikát je podepsán společností Cisco. Společnost Cisco vám certifikát pošle, abyste si ho mohli nainstalovat do systému.

Klientský certifikát

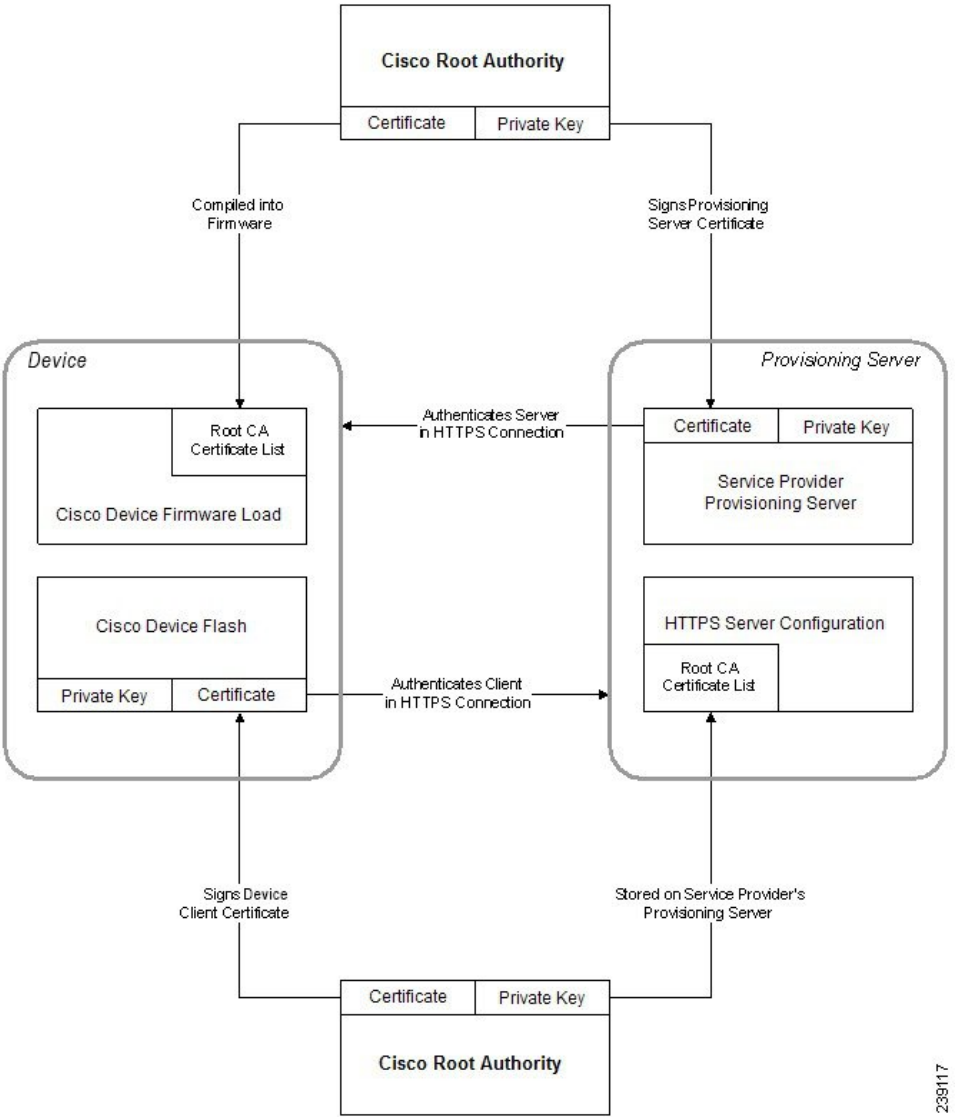
Vedle přímého útoku na telefon se útočník může pokusit kontaktovat zřizovací server prostřednictvím standardního webového prohlížeče nebo jiného klienta HTTPS a profil konfigurace ze zřizovacího serveru získat. Aby se zabránilo tomuto druhu útoku, každý telefon má v sobě také jedinečný klientský certifikát podepsaný společností Cisco, který obsahuje identifikující údaje o všech jednotlivých koncových bodech. Každý poskytovatel služeb má kořenový certifikát certifikační autority, který dokáže ověřit klientský certifikát zařízení. Tato cesta ověření umožňuje zřizovacímu serveru odmítat neověřené požadavky na profily konfigurace.

Struktura certifikátu

Kombinace serverového certifikátu a klientského certifikátu zaručuje zabezpečenou komunikace mezi vzdáleným telefonem a zřizovacím serverem. Na obrázku je ilustrován vztah a umístění certifikátů, párů veřejný/privátní klíč a podepisujících kořenových autorit mezi klientem Cisco, zřizovacím serverem a certifikační autoritou.

V horní části schématu je uvedena kořenová autorita zřizovacího serveru, která je využívána k podpisu jednotlivých certifikátů zřizovacího serveru. Odpovídající kořenový certifikát je zkompilován ve firmwaru, což umožňuje telefonu ověřit oprávněné zřizovací servery.

Obrázek 2: Diagram certifikační autority



Konfigurace vlastní certifikační autority

K ověření digitálních certifikátů a uživatelů v síti lze použít digitální certifikáty. Lze je používat k domlouvání relací IPSec mezi uzly sítě.

K validaci a ověření dvou nebo více uzlů, které se pokoušejí komunikovat, využívá třetí strana certifikát certifikační autority. Každý uzel má veřejný a privátní klíč. Veřejný klíč se používá k zašifrování dat. Privátní klíč se používá k rozšifrování dat. Protože uzly získaly své certifikáty ze stejného zdroje, jsou si o identitě druhého uzlu jisté.

Zařízení může k ověření připojení IPSec používat digitální certifikáty poskytnuté certifikační autoritou (CA) třetí strany.

Telefony podporují sadu předem nahraných autorit kořenových certifikátů integrovaných ve firmwaru:

- Certifikát Cisco Small Business CA
- Certifikát CyberTrust CA
- Certifikát Verisign CA
- Kořenový certifikát Sipura CA
- Kořenový certifikát CA Linksys

Než začnete

Přejděte na webovou stránku správy telefonu. Viz Otevření webové stránky telefonu, na straně 7.

Procedura

Krok 1 Vyberte možnosti **Infomace** > **Stav**.

Krok 2 Přejděte na možnost **Stav vlastního CA** a podívejte se na tato políčka:

- Stav vlastního zřizování CA – ukazuje stav zřizování.
  - Poslední zřizování bylo úspěšně provedeno mm/dd/rrrr v HH:MM:SS nebo
  - Poslední zřizování mm/dd/rrrr v HH:MM:SS neproběhlo úspěšně
- Informace o vlastní CA – zobrazuje údaje o vlastní CA.
  - Nainstalováno – Zobrazuje položku „Hodnota CN“, kde „Hodnota CN“ je hodnota parametru CN pole Předmět v prvním certifikátu.
  - Nenainstalováno – Zobrazuje se, když není nainstalován žádný certifikát CA.

Správa profilu

V této části je demonstrováno vytvoření profilů konfigurace jako přípravy ke stažení. K vysvětlení funkce je jako metoda resynchronizace použit protokol TFTP z místního počítače. Lze však použít i protokol HTTP a HTTPS.

Zkomprimovat otevřený profil metodou Gzip

Konfigurační profil ve formátu XML může být poměrně velký, pokud jsou v profilu specifikovány všechny parametry jednotlivě. Ke snížení zátěže na zřizovací server telefon podporuje kompresi souboru XML pomocí formátu komprese, který podporuje nástroj gzip (RFC 1951).

Poznámka Aby telefon dokázal rozpoznat komprimovaný a zašifrovaný profil XML, musí komprese předcházet před šifrováním.

Pro integraci do upravených back-endových řešení zřizovaní serverů lze k provedení komprese profilu použít místo samostatného nástroje gzip svobodnou komprimační knihovnu zlib. Telefon však očekává, že soubor bude obsahovat platnou hlavičku gzip.

Procedura

Krok 1 Do místního počítače nainstalujte nástroj gizp.

Krok 2 Zkomprimujte konfigurační profil `basic.txt` (popsaný v částiResynchronizace TFTP, na straně 47) zavoláním příkazu gzip z příkazového řádku:

```
gzip basic.txt
```

Tak se vygeneruje zabalený soubor `basic.txt.gz`.

Krok 3 Uložte soubor `basic.txt.gz` do virtuálního kořenového adresáře serveru TFTP.

Krok 4 Upravte hodnotu Profile_Rule na testovacím zařízení, a proveďte tak resynchronizaci zabaleného souboru místo původního souboru XML. Níže je uveden příklad:

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

Krok 5 Klikněte na tlačítko **Odeslat všechny změny**.

Krok 6 V telefonu se podívejte na sledování syslog.

Po resynchronizaci telefon nový soubor stáhne a použije ho k aktualizaci svých parametrů.

Související témata

Komprese otevřeného profilu, na straně 18

Šifrování profilu pomocí OpenSSL

Zašifrovat je možné komprimovaný i nekomprimovaný profil (soubor však musí být zkomprimován před zašifrováním). Šifrování se hodí, když je důvěrnost údajů profilu důležitá, například když se ke komunikaci mezi telefonem a zřizovacím serverem používá protokol TFTP nebo HTTP.

Telefon podporuje šifrování se symetrickým klíčem pomocí 256bitového algoritmu AES. Toto šifrování lze provést pomocí svobodného balíčku OpenSSL.

Procedura

Krok 1 Do místního počítače nainstalujte nástroj OpenSSL. Aby bylo možné povolit AES, možná bude nutné překompilovat aplikaci OpenSSL.

Krok 2 Pomocí konfiguračního souboru `basic.txt` (který je popsán v části Resynchronizace TFTP, na straně 47) vygenerujte následujícím příkazem šifrovaný soubor:

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

Lze také použít zašifrovaný soubor `basic.txt.gz`, který byl vytvořen v části Zkomprimovat otevřený profil metodou Gzip, na straně 60, protože profil XML může být zkomprimovaný i zašifrovaný.

Krok 3 Uložte zašifrovaný soubor `basic.cfg` do virtuálního kořenového adresáře serveru TFTP.

Krok 4 Upravte hodnotu Profile_Rule na testovacím zařízení, čímž provedete resynchronizaci zašifrovaného souboru místo původního souboru XML. Šifrovací klíč je telefonu oznámen následující možností adresy URL:

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

Krok 5 Klikněte na tlačítko **Odeslat všechny změny**.

Krok 6 V telefonu se podívejte na sledování syslog.

Po resynchronizaci telefon nový soubor stáhne a použije ho k aktualizaci svých parametrů.

Související témata

Šifrování AES-256-CBC, na straně 18

Vytvoření rozdělených profilů

Telefon během každé resynchronizace stáhne několik oddělených profilů. Díky tomuto postupu je možné spravovat různé druhy údajů profilů na různých serverech a udržovat hodnoty společných parametrů konfigurace, které se liší od hodnot u konkrétního účtu.

Procedura

Krok 1 Vytvořte nový profil XML, `basic2.txt`, jehož součástí je hodnota parametru, díky které se liší od předchozích cvičení. Například do profilu `basic.txt` můžete přidat toto:

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

Krok 2 Uložte soubor profilu `basic2.txt` do virtuálního kořenového adresáře serveru TFTP.

Krok 3 Nechte ve složce první pravidlo profilu ze staršího cvičení, ale nakonfigurujte druhé pravidlo profilu (Profile_Rule_B) tak, aby mířilo na nový soubor:

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

Krok 4 Klikněte na tlačítko **Odeslat všechny změny**.

Telefon nyní při každé naplánované resynchronizaci provede resynchronizaci prvního a druhého profilu v tomto pořadí.

Krok 5 Podívejte se na sledování syslog a ověřte, že dochází k očekávanému chování.

Nastavení záhlaví pro konfiguraci soukromí telefonu

Záhlaví pro nastavení soukromí uživatele ve zprávách SIP nastavuje požadované soukromí uživatele v důvěryhodné síti.

Pomocí značky XML v souboru `config.xml` můžete nastavit hodnotu záhlaví soukromí uživatele pro každou linku.

Dostupné možnosti záhlaví pro nastavení soukromí:

- Disabled (Zakázáno) – výchozí
- none (žádné) – uživatel požaduje, aby služba ochrany soukromí nepoužila na danou zprávu SIP žádné funkce ochrany soukromí.
- header (záhlaví) – uživatel požaduje, aby služba ochrany soukromí skryla záhlaví, ze kterých nelze odstranit identifikující údaje.
- session (relace) – uživatel požaduje, aby služba ochrany soukromí zajistila anonymitu v rámci relací.
- user (uživatel) – uživatel požaduje určitou úroveň ochrany soukromí pouze v případě zprostředkujících stran.
- id – uživatel požaduje, aby systém použil jiný identifikátor, který neobsahuje informace o adrese IP nebo názvu hostitele.

Procedura

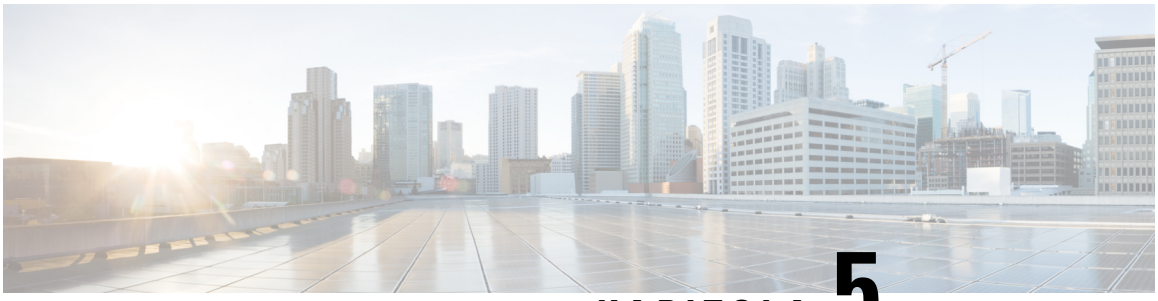
Krok 1 Upravte soubor telefonu `config.xml` v textovém nebo XML editoru.

Krok 2 Vložte značku **<Privacy_Header_N_ ua="na">*Hodnota*</Privacy_Header_N_>**, kde N je číslo linky (1–10), a použijte jednu z následujících hodnot.

- Výchozí hodnota: **Disabled** (Zakázáno)
- **žádné**
- **header**
- **relace**
- **user**
- **id**

Krok 3 (Nepovinné) Zřiďte veškeré další linky pomocí stejné značky s požadovaným číslem linky.

Krok 4 Uložte změny souboru `config.xml`.



KAPITOLA 5

Parametry zřizování

Přehled parametrů zřizování

V této kapitole jsou popsány parametry zřizování, které lze použít ve skriptech profilu konfigurace.

Parametry profilu konfigurace

V následující tabulce je definována funkce a použití jednotlivých parametrů v části **Parametry profilu konfigurace** karty **Zřizování**.

Název parametru	Popis a výchozí hodnota
Povolit zřizování	Řídí všechny činnosti resynchronizace nezávisle na činnostech upgradu firmwaru. Pokud chcete povolit vzdálené zřizování, nastavte hodnotu **Ano**. Výchozí hodnota je Ano.
Resynchronizace při restartování	Resynchronizace se spustí po každém restartování kromě restartování způsobených aktualizacemi parametru a upgrady firmwaru. Výchozí hodnota je Ano.

Název parametru	Popis a výchozí hodnota
Náhodná prodleva resynchronizace	Náhodná prodleva následující po spouštěcí sekvenci před provedením resetování udaná v sekundách. Ve fondu zařízení IP telefonie, u kterých je naplánováno současné spuštění, se tímto zavádí rozptyl v časech, kdy jednotlivé jednotky zřizovacímu serveru odešlou požadavek na resynchronizaci. Tato funkce se může hodit ve velkém nasazení do domácností v případě místního výpadku dodávky energie. Hodnota tohoto pole musí být celé číslo v rozmezí 0 až 65 535. Výchozí hodnota je 2.
Resynchronizace v (HHmm)	Čas (HHmm), kdy se zařízení se zřizovacím serverem resynchronizuje. Hodnota tohoto pole musí být čtyřmístné číslo v rozmezí 0000 až 2 400 pro indikaci času ve formátu HHmm. Například 0959 znamená 09:59. Výchozí hodnota je prázdná. Pokud je hodnota neplatná, parametr se ignoruje. Pokud je tento parametr nastaven na platnou hodnotu, je parametr Pravidelná resynchronizace ignorován.
Resynchronizace po náhodné prodlevě	Brání přetížení zřizovacího serveru, když se najednou spustí velký počet zařízení. Aby se zabránilo zaplavení serveru požadavky na resynchronizaci z více telefonů, telefon se resynchronizuje v rozsahu hodin a minut a hodin a minut plus náhodná prodleva (hhmm, hhmm + náhodná_prodleva). Pokud je například náhodná prodleva = (resynchronizace po náhodné prodlevě + 30)/60 minut, pro výpočet konečného intervalu náhodné_prodlevy je vstupní hodnota v sekundách převedena na minuty a je zaokrouhlena na následující minutu. Rozmezí platných hodnot 0 až 65 535. Tato funkce je zakázána, když je tento parametr nastaven na nulu. Výchozí hodnota je 600 sekund (10 minut).

Název parametru	Popis a výchozí hodnota
Pravidelná resynchronizace	Časový interval mezi pravidelnými resynchronizacemi se zřizovacím serverem. Přiřazený časovač resynchronizace je aktivní až po první úspěšné resynchronizaci se serverem. Platné formáty: • Celé číslo Příklad: Vstup `3000` značí, že další resynchronizace proběhne za 3 000 sekund. • Více celých čísel Příklad: Vstup `600,1200,300` znamená, že první resynchronizace nastane za 600 sekund, druhá resynchronizace za 1 200 sekund po první a třetí resynchronizace za 300 sekund po druhé. • Časový rozsah Příklad: Vstup `2400+30` znamená, že další resynchronizace nastane za 2 400 až 2 430 sekund po úspěšné resynchronizaci. Pokud chcete pravidelnou resynchronizaci zakázat, nastavte tento parametr na nulu. Výchozí hodnota je 3600 sekund.

Název parametru	Popis a výchozí hodnota
Prodleva opakování po chybě resynchronizace	Pokud se resynchronizace nezdaří, protože zařízení IP telefonie nedokázalo ze serveru načíst profil, stažený soubor je poškozený nebo došlo k interní chybě, zařízení se po době v sekundách pokusí provést resynchronizaci znovu. Platné formáty: • Celé číslo Příklad: Vstup `300` značí, že další pokus o resynchronizaci proběhne za 300 sekund. • Více celých čísel Příklad: Vstup `600,1200,300` znamená, že první pokus o resynchronizaci proběhne za 600 sekund po selhání, druhý pokus za 1 200 sekund po selhání prvního pokusu a třetí pokus za 300 po selhání druhého pokusu. • Časový rozsah Příklad: Vstup `2400+30` znamená, že další pokus proběhne za 2 400 až 2 430 sekund po neúspěšném pokusu o resynchronizaci. Pokud je prodleva nastavena na 0, zařízení se po neúspěšném pokusu o resynchronizaci nepokusí ji provést znovu.
Prodleva nucené resynchronizace	Maximální prodleva (v sekundách), po kterou telefon čeká, než provede resynchronizaci. Zařízení neprovede resynchronizaci, když je některá telefonní linka aktivní. Protože resynchronizace může trvat několik sekund, je před resynchronizací žádoucí počkat, než je zařízení po určitou dobu nečinné. Díky tomu může uživatel bez přerušení provádět více hovorů po sobě. Zařízení má časovač, který začíná odpočet od chvíle, kdy jsou všechny linky nečinné. Tento parametr je výchozí hodnota čítače. Události resynchronizace jsou odloženy, dokud tento čítač neklesne na nulu. Rozmezí platných hodnot 0 až 65 535. Výchozí hodnota je 14 400 sekund.
Resynchronizace ze SIP	Umožňuje spuštění resynchronizace prostřednictvím zprávy SIP NOTIFY. Výchozí hodnota je Ano.

Název parametru	Popis a výchozí hodnota
Resynchronizace po pokusu o upgrade	Zapíná a vypíná operaci resynchronizace po provedení upgradu. Pokud je zvolena možnost Ano, synchronizace se provede. Výchozí hodnota je Ano.
Spouštěč resynchronizace 1, Spouštěč resynchronizace 2	Konfigurovatelné podmínky spuštění resynchronizace. Když je logická rovnice v těchto parametrech vyhodnocena jako PRAVDA, spustí se resynchronizace. Výchozí hodnota je prázdná.
Resynchronizace se nezdaří při FNF	Resynchronizace se považuje za neúspěšnou, pokud není ze serveru přijat vyžádaný profil. To lze změnit pomocí tohoto parametru. Když je parametr nastaven na **ne**, zařízení bere odpověď `file-not-found` od serveru jako úspěšnou resynchronizaci. Výchozí hodnota je Ano.
Pravidlo profilu Pravidlo profilu B Pravidlo profilu C Pravidlo profilu D	Každé pravidlo profilu informuje telefon o zdroji, ze kterého lze získat profil (konfigurační soubor). Během každé resynchronizaci telefon postupně použije všechny profily. Výchozí nastavení: **`/$PSN.xml`** Pokud používáte na konfigurační soubory šifrování AES-256-CBC, zadejte následujícím způsobem šifrovací klíč s klíčovým slovem **`--key`**: **`[--key <šifrovací klíč>]`** Šifrovací klíč může být volitelně ve dvojitých uvozovkách (").
Použití možnost DHCP	Možnosti DHCP oddělené čárkami používané k načtení firmwaru a profilů. Výchozí hodnota je 66,160,159,150,60,43,125.
Zpráva protokolu při požadavku	Tento parametr obsahuje zprávu, která se odešle na server syslog na začátku pokusu o resynchronizaci. Výchozí hodnota je `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`
Zpráva protokolu při úspěchu	Zpráva syslog vydaná po úspěšném dokončení resynchronizace. Výchozí hodnota je `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`

Název parametru	Popis a výchozí hodnota
Zpráva protokolu při selhání	Zpráva syslog vydaná po neúspěšném dokončení resynchronizace. Výchozí hodnota je `$PN $MAC -- Resync failed: $ERR`.
Uživatelsky konfigurovatelná resynchronizace	Umožňuje uživateli resynchronizovat telefon z obrazovky IP telefonu. Výchozí hodnota je Ano.

Parametry upgradu firmwaru

V následující tabulce je definována funkce a použití jednotlivých parametrů v části **Upgrade firmwaru** karty **Zřizování**.

Název parametru	Popis a výchozí hodnota
Povolit upgrade	Povoluje operace upgradu firmwaru nezávisle na činnostech resynchronizace. Výchozí hodnota je Ano.
Prodleva opakování při chybě upgradu	Interval opakování upgradu (v sekundách) použitý v případě selhání upgradu. Zařízení má časovač chyby upgradu firmwaru, který se aktivuje po neúspěšném pokusu o upgrade firmwaru. Časovač se inicializuje na hodnotu v tomto parametru. Další pokus o upgrade firmwaru proběhne, když čítač dojde na nulu. Výchozí hodnota je 3 600 sekund.
Pravidlo upgradu	Skript upgradu firmwaru, který definuje podmínky upgradu a přiřazené adresy URL firmwaru. Využívá se v něm stejná syntax jako v pravidle profilu. K zadání pravidla profilu použijte tento formátů **<tftp|http|https>://<adresa ip>/image/<název načtení>** Příklad: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Pokud není zadán žádný protokol, předpokládá se TFTP. Pokud není zadán žádný název serveru, jako název serveru se použije hostitel, který o adresu URL žádá. Pokud není zadán žádný port, používá se výchozí port (69 pro TFTP, 80 pro HTTP a 443 pro HTTPS). Výchozí hodnota je prázdná.

Název parametru	Popis a výchozí hodnota
Zpráva do protokolu při požadavku na upgrade	Zpráva syslog vydaná na začátku pokusu o upgrade firmwaru. Výchozí hodnota: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Zpráva do protokolu při úspěšném upgradu	Zpráva syslog vydaná po úspěšném dokončení upgradu firmwaru. Výchozí hodnota je `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Zpráva do protokolu při neúspěšném upgradu	Zpráva syslog vydaná po neúspěšném dokončení upgradu firmwaru. Výchozí hodnota je `$PN $MAC -- Upgrade failed: $ERR`
Sdílení firmwaru s druh. stranou	Povolí nebo zakáže funkci Sdílení firmwaru s druhou stranou. Funkci povolte nebo zakažte zvolením možnosti **Ano** nebo **Ne**. Výchozí hodnota: Ano
Server protokolování sdílení firmwaru s druhou stranou	Uvádí adresu IP a port, na které je odeslána zpráva UDP. Příklad: 10.98.76.123:514, kde 10.98.76.123 je adresa IP a 514 číslo portu.

Obecné parametry

V následující tabulce je definována funkce a použití jednotlivých parametrů v části **Obecné parametry** karty **Zřizování**.

Název parametru	Popis a výchozí hodnota
GPP A – GPP P	Obecné parametry GPP_* se při konfiguraci telefonu na komunikaci s konkrétním řešením zřizovacího serveru používají jako volné registry řetězců. Je možné je nakonfigurovat tak, aby obsahovaly různé hodnoty, například tyto: • Šifrovací klíče. • Adresy URL. • Informace o stavu vícefázového zřizování. • Šablony požadavku Post. • Mapy aliasů názvů proměnných. • Částečné hodnoty řetězců, které se ve výsledku zkombinují do úplných hodnot parametrů. Výchozí hodnota je prázdná.

Proměnné rozšíření makra

Některé proměnné makra jsou rozpoznávány v rámci těchto parametrů zřizování:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (za určitých podmínek)

V rámci těchto parametrů jsou rozpoznávány a rozšiřovány typy syntaxe $JMENO nebo $(JMENO).

Podřetězce proměnné makra lze zadat pomocí notace $(JMENO:p) a $(JMENO:p:q), kde p a q jsou nezáporná celá čísla (dostupné od verze 2.0.11). Výsledné rozšíření makra je podřetězec začínající p-tým znakem s délkou q (nebo do konce řetězce, pokud hodnota q není zadána). Pokud například GPP_A obsahuje ABCDEF, pak se $(A:2) rozšíří na CDEF a $(A:2:3) se rozšíří na CDE.

Nerozpoznaný název se nepřekládá a podoba $JMENO nebo $(JMENO) zůstává v hodnotě parametru po rozšíření beze změny.

Název parametru	Popis a výchozí hodnota
$	Zápis $$ se rozšíří na jeden znak $.
A až P	Nahrazuje se obsahem obecných parametrů GPP_A až GPP_P.

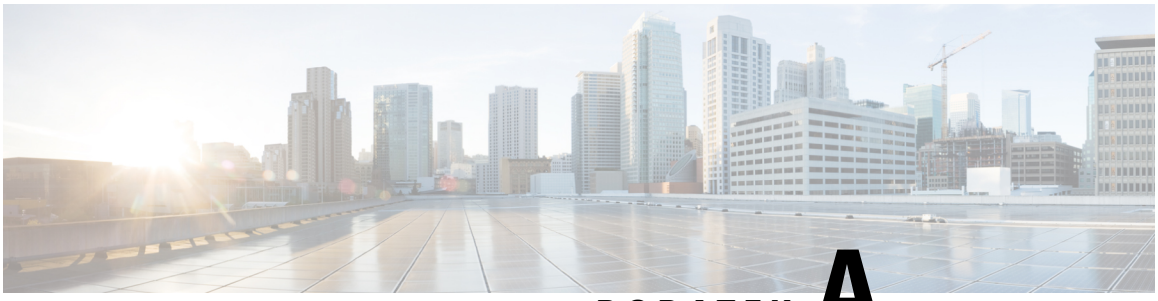
Název parametru	Popis a výchozí hodnota
SA až SD	Nahrazuje se obsahem parametrů pro zvláštní účel GPP_SA až GPP_SD. V těchto parametrech jsou uloženy klíče a hesla používaná při zřizování. **Poznámka** $SA až $SD se považují za argumenty volitelného kvalifikátoru adresy URL resynchronizace, --key
MA	Adresa MAC v malých šestnáctkových číslech, například 000e08aabbcc.
MAU	Adresa MAC ve velkých šestnáctkových číslech, například 000E08AABBCC.
MAC	Adresa MAC v malých šestnáctkových číslech a se středníky oddělujícími páry šestnáctkových číslic. Například 00:0e:08:aa:bb:cc.
PN	Název produktu. Například CP-6841-3PCC.
PSN	Číslo řady produktu. Například 6841-3PCC.
SN	Řetězec sériového čísla. Například 88012BA01234.
CCERT	Stav klientského certifikátu SSL: nainstalovaný, nebo nenainstalovaný.
IP	Adresa IP telefonu v místní podsíti. Například 192.168.1.100.
EXTIP	Externí adresa IP telefonu, jak je vidět z internetu. Například 66.43.16.52.
SWVER	Řetězec verze softwaru. Například sip68xx.11-0-1MPP.
HWVER	Řetězec verze hardwaru. Například 2.0.1
PRVST	Stav zřizování (číselný řetězec): -1 = explicitní požadavek na resynchronizaci 0 = resynchronizace při spuštění 1 = pravidelná resynchronizace 2 = resynchronizace se nezdařila, opakování pokusu
UPGST	Stav upgradu (číselný řetězec): 1 = první pokus o upgrade 2 = upgrade se nezdařil, opakování pokusu

Název parametru	Popis a výchozí hodnota
UPGERR	Zpráva výsledku (ERR) předchozího pokusu o upgrade, například „nezdařilo se provést http_get“.
PRVTMR	Počet sekund od posledního pokusu o resynchronizaci.
UPGTMR	Počet sekund od posledního pokusu o upgrade.
REGTMR1	Počet sekund od registrace ztráty linky 1 se serverem SIP.
REGTMR2	Počet sekund od registrace ztráty linky 2 se serverem SIP.
UPGCOND	Starší název makra.
SCHEME	Protokol pro přístup k souboru, TFTP, HTTP nebo HTTPS, zjištěný po analýze adresy URL resynchronizace nebo upgradu.
SERV	Název hostitele serveru cíle požadavku zjištěný po analýze adresy URL resynchronizace nebo upgradu.
SERVIP	Adresa IP serveru cíle požadavku zjištěná po analýze adresy URL resynchronizace nebo upgradu, možná po zjištění na serveru DNS.
PORT	Port UDP/TCP cíle požadavku zjištěný po analýze adresy URL resynchronizace nebo upgradu.
PATH	Cesta k souboru cíle požadavku zjištěný po analýze adresy URL resynchronizace nebo upgradu.
ERR	Zpráva výsledku pokusu o resynchronizaci nebo upgrade. Hodí se pouze při generování zpráv syslog výsledku. Hodnota se v případě pokusů o upgrade uchovává v proměnné UPGERR.
UIDn	Obsah parametru konfigurace UserID linky n.
EMS	Stav Extension Mobility
MUID	ID uživatele Extension Mobility
MPWD	Heslo Extension Mobility

Kódy interních chyb

Telefon k umožnění konfigurace definuje několik kódů interních chyb (X00–X99), čímž poskytuje lepší kontrolu nad chováním jednotky za určitých chybových stavů.

Název parametru	Popis a výchozí hodnota
X00	Chyba přenosové vrstvy nebo (ICMP) při odesílání požadavku SIP.
X20	Požadavek SIP při čekání na odpověď vypršel.
X40	Obecná chyba protokolu SIP (například nepřijatelný kodek v SDP ve zprávách 200 a ACK nebo vypršení platnosti při čekání na ACK).
X60	Vytočené číslo není podle daného plánu číslování platné.



DODATEK A

Vzorové profily konfigurace

Příklad otevřeného 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>
```

Vzorové profily konfigurace

```
<!--  available options: Disabled|Enabled  -->
<Auto_Config ua="rw">Enabled</Auto_Config>
<!--  available options: Disabled|Enabled  -->
 <!--  802.1X Authentication  -->
<Enable_802.1X_Authentication ua="rw">No</Enable_802.1X_Authentication>
 <!--  Optional Network Configuration  -->
<Host_Name ua="rw"/>
<Domain ua="rw"/>
<DNS_Server_Order ua="na">Manual,DHCP</DNS_Server_Order>
<!--  available options: Manual|Manual,DHCP|DHCP,Manual  -->
<DNS_Query_Mode ua="na">Parallel</DNS_Query_Mode>
<!--  available options: Parallel|Sequential  -->
<DNS_Caching_Enable ua="na">Yes</DNS_Caching_Enable>
<Switch_Port_Config ua="na">AUTO</Switch_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_Port_Config ua="na">AUTO</PC_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_PORT_Enable ua="na">Yes</PC_PORT_Enable>
<Enable_PC_Port_Mirror ua="na">No</Enable_PC_Port_Mirror>
<Syslog_Server ua="na"/>
<Syslog_Identifier ua="na">None</Syslog_Identifier>
<!--  available options: None|$MA|$MAU|$MAC|$SN  -->
<Debug_Level ua="na">NOTICE</Debug_Level>
<!--
 available options: EMERGENCY|ALERT|CRITICAL|ERROR|WARNING|NOTICE|INFO|DEBUG
-->
<Primary_NTP_Server ua="rw"/>
<Secondary_NTP_Server ua="rw"/>
<Enable_SSLv3 ua="na">No</Enable_SSLv3>
<Use_Config_TOS ua="na">No</Use_Config_TOS>
 <!--  VLAN Settings  -->
<Enable_VLAN ua="rw">No</Enable_VLAN>
<VLAN_ID ua="rw">1</VLAN_ID>
<PC_Port_VLAN_ID ua="na">1</PC_Port_VLAN_ID>
<Enable_CDP ua="na">Yes</Enable_CDP>
<Enable_LLDP-MED ua="na">Yes</Enable_LLDP-MED>
<Network_Startup_Delay ua="na">3</Network_Startup_Delay>
<DHCP_VLAN_Option ua="na"/>
 <!--  Wi-Fi Settings  -->
 <!--  Wi-Fi Profile 1  -->
 <!--  Wi-Fi Profile 2  -->
 <!--  Wi-Fi Profile 3  -->
 <!--  Wi-Fi Profile 4  -->
 <!--  Inventory Settings  -->
<Asset_ID ua="na"/>
 <!--  SIP Parameters  -->
<Max_Forward ua="na">70</Max_Forward>
<Max_Redirection ua="na">5</Max_Redirection>
<Max_Auth ua="na">2</Max_Auth>
<SIP_User_Agent_Name ua="na">$VERSION</SIP_User_Agent_Name>
<SIP_Server_Name ua="na">$VERSION</SIP_Server_Name>
<SIP_Reg_User_Agent_Name ua="na"/>
<SIP_Accept_Language ua="na"/>
<DTMF_Relay_MIME_Type ua="na">application/dtmf-relay</DTMF_Relay_MIME_Type>
<Hook_Flash_MIME_Type ua="na">application/hook-flash</Hook_Flash_MIME_Type>
<Remove_Last_Reg ua="na">No</Remove_Last_Reg>
<Use_Compact_Header ua="na">No</Use_Compact_Header>
<Escape_Display_Name ua="na">No</Escape_Display_Name>
<Talk_Package ua="na">No</Talk_Package>
<Hold_Package ua="na">No</Hold_Package>
```

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

Vzorové profily konfigurace

```
<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>
```

Vzorové profily konfigurace

```
<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>
```

Vzorové profily konfigurace

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

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

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

Vzorové profily konfigurace

```
<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
```

Vzorové profily konfigurace

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

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

Vzorové profily konfigurace

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

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

Vzorové profily konfigurace

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

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

Vzorové profily konfigurace

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

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

Vzorové profily konfigurace

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

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

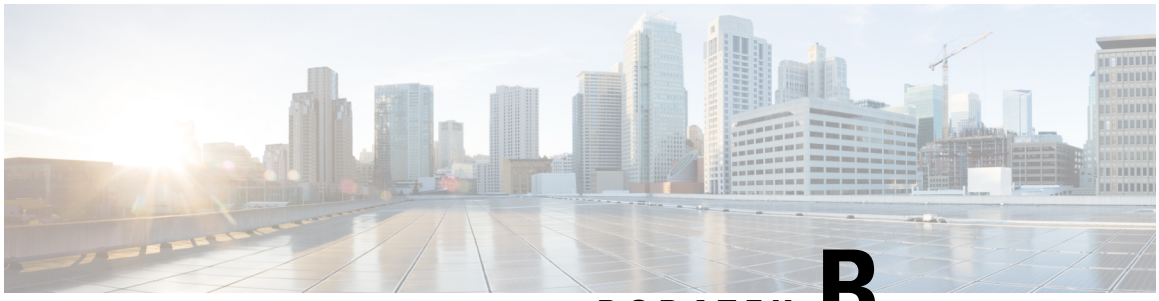
Vzorové profily konfigurace

```
<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"/>
```

Vzorové profily konfigurace

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



DODATEK B

Zkratky

Zkratky

AC	Střídavý proud
ACS	Access Control Server (server řízení přístupu)
A/D	Konvertor analogového signálu na digitální
AES	Advanced Encryption Standard (standard pokročilého šifrování)
ANC	Anonymní hovor
AP	Přístupový bod
ASCII	American Standard Code for Information Interchange (americký standardní kód pro výměnu informací)
B2BUA	Uživatelský agent back-to-back
BLF	Funkce BLF (Busy Lamp Field)
Bool	Logické hodnoty. V profilu uvedené jako ano a ne, nebo 1 a 0
BootP	Protokol Bootstrap Protocol
CA	Certifikační úřad
CAS	Signál upozornění CPE
CDP	protokol CDP (Cisco Discovery Protocol)
záznamy s podrobnostmi o hovoru	Záznam s podrobnostmi o hovoru
CGI	Computer-Generated Imagery (počítačem vytvářená grafika)

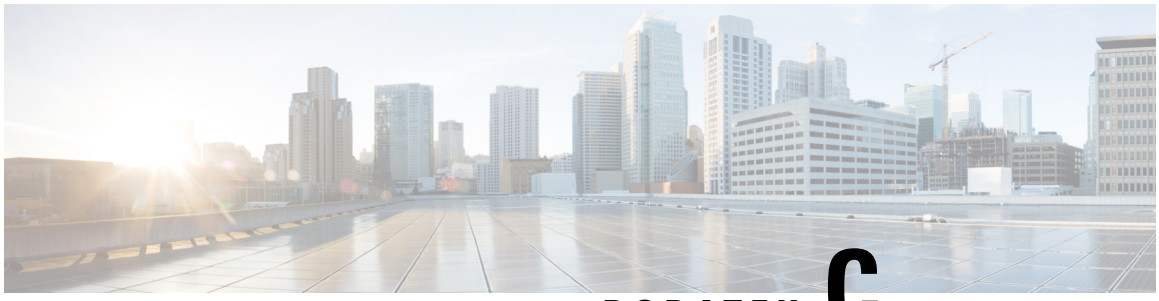
CID	zobrazení ID volajícího,
CIDCW	ID volajícího čekajícího hovoru
CNG	Generování příjemného hluku
CPC	Řízení volající strany
CPE	Zařízení na pracovišti zákazníka
CSV	Hodnota oddělená čárkami
CWCID	ID volajícího čekajícího hovoru
CWT	Tón čekajícího hovoru
D/A	Konvertor digitálního signálu na analogový
dB	decibel
dBm	dB nad 1 miliwattem
DHCP	Dynamic Host Configuration Protocol
Nerušit	Nerušit
DNS	Služba DNS (Domain Name System)
□DoS	Útok typu odmítnutí služby
DRAM	Dynamická paměť s náhodným přístupem
DSL	Smyčka digitálního odběratele
DSP	Procesor digitálního signálu
xDST	Letní čas
DTAS	Signál upozornění datového terminálu (stejný jako CAS)
DTMF	Tónová volba
Úplný doménový název (FQDN)	Plně kvalifikovaný název domény
FSK	Klíčování frekvenčním posunem
FW	Firmware
FXS	Foreign eXchange Station
GMT	Střední čas
GW	Brána

HTML	Hypertextový značkovací jazyk
HTTP	Hypertextový přenosový protokol
HTTPS	HTTP přes SSL
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ILEC	Povinný místní operátor
IP	Protokol IP (Internet Protocol)
IPv4	Protokol IP (Internet Protocol) verze 4
IPv6	Protokol IP (Internet Protocol) verze 6
ISP	Poskytovatel služeb internetu
ITSP	Poskytovatel služeb internetové telefonie
ITU	Mezinárodní telekomunikační unie
IVR	Interactive Voice Response
LAN	Místní síť
LBR	Nízká rychlost přenosu
LBRC	Kodek nízké rychlosti přenosu
LCD	Displej z tekutých krystalů, označovaný také jako obrazovka
protokol LDAP	LDAP
□LED	Světelná dioda
Adresa MAC	Adresu MAC pro řízení přístupu k médiím
MC	Minicertifikát
MGCP	Media Gateway Control Protocol
MOH	Music On Hold
MOS	Průměrné skóre hodnocení (1–5, čím vyšší, tím lepší)
MPP	Víceplatformové telefony
ms	Milisekunda
MSA	Adaptér zdroje hudby

Indikace čekající zprávy	Indikátor čekající zprávy
NAT	Překlad síťové adresy
NPS	Normální zřizovací server
NTP	Protokol NTP (Network Time Protocol)
OOB	Mimo pásmo
OSI	Interval otevřeného směrování
PBX	Pobočková ústředna
PCB	Deska plošných spojů
PoE	Power over Ethernet (napájení přes ethernet)
PR	Otočení polarity
PS	Zřizovací server
PSQM	Trvalé měření kvality hlasu (1–5, čím nižší, tím lepší)
PSTN	Veřejná telefonní síť
QoS	Kvalita služby (Quality of Service)
RC	Odebrat přizpůsobení
REQT	Zpráva požadavku (SIP)
RESP	Zpráva s odpovědí (SIP)
RSC	Kód stavu odpovědi (SIP), např. 404, 302, 600
RTP	Protokol v reálném čase
RTT	Čas doby odezvy
SAS	Server streamování zvuku
SDP	Session Description Protocol
SDRAM	Synchronní DRAM
s	sekundy
SIP	Protokol SIP (Session Initiation Protocol)
SLA	Sdílená linka
SLIC	Obvod rozhraní linky odběratele

SP	Poskytovatel služeb
SSL	Secure Socket Layer
STUN	Session Traversal UDP for NAT – sada pomocných internetových standardů
TCP	Transmission Control Protocol
TFTP	Jednoduchý protokol na přenos souborů
TLS	Transport Layer Security (zabezpečení přenášených dat)
TTL	Time to Live – doba platnosti dat nebo počet průchodů paketů
ToS	Type of Service – klasifikace typ služby
UA	Uživatelský agent
uC	Jednočipový počítač
UDP	User Datagram Protocol
URI	Uniform Resource Identifier – jednodný indentifikátor zdroje
Adresa URL	Jednotná adresa zdroje
UTC	Coordinated Universal Time – koordinovaný světový čas
VAR	Prodejce s přidanou hodnotou
síť VLAN	Hlasová síť LAN
VM	Hlasová schránka
VMWI	Vizuální indikátor čekající zprávy
VoIP	Protokol Voice over Internet Protocol pro přenos hlasu prostřednictvím paketů
VQ	Kvalita zvuku
WAN	Rozsáhlá síť
XML	Rozšiřitelný značkovací jazyk

Zkratky



DODATEK C

Související dokumentace

Související dokumentace

K získání souvisejících informací využijte následující části.

Dokumentace k telefonům Cisco IP Phone 6800 Series

Podívejte se do publikací, které jsou ve vašem jazyce a pro váš model telefonu a verzi víceplatformového firmwaru. Přejděte z této adresy URL:

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

Zásady podpory firmwaru Cisco IP Phone

Informace o zásadách podpory pro telefony najdete na adrese https://cisco.com/go/phonefirmwaresupport.