Ръководство за обезпечаване на многоплатформени телефони Cisco IP Phone 6800

Първо издание: 2017-11-22

Последна промяна: 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.

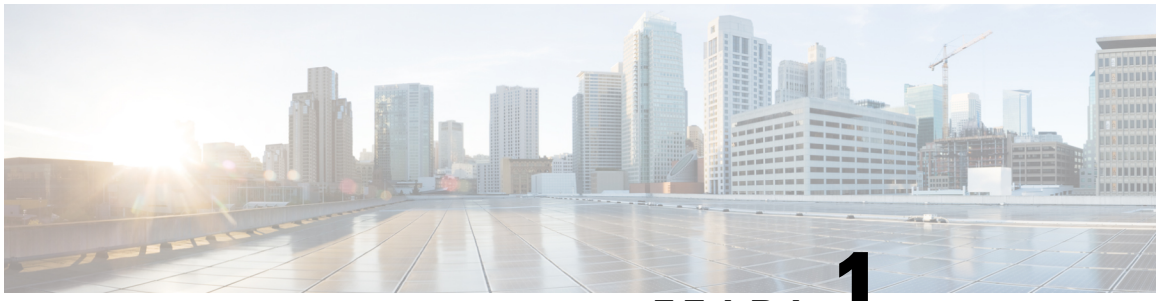
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

СЪДЪРЖАНИЕ



ГЛАВА 1

Разгръщане и обезпечаване

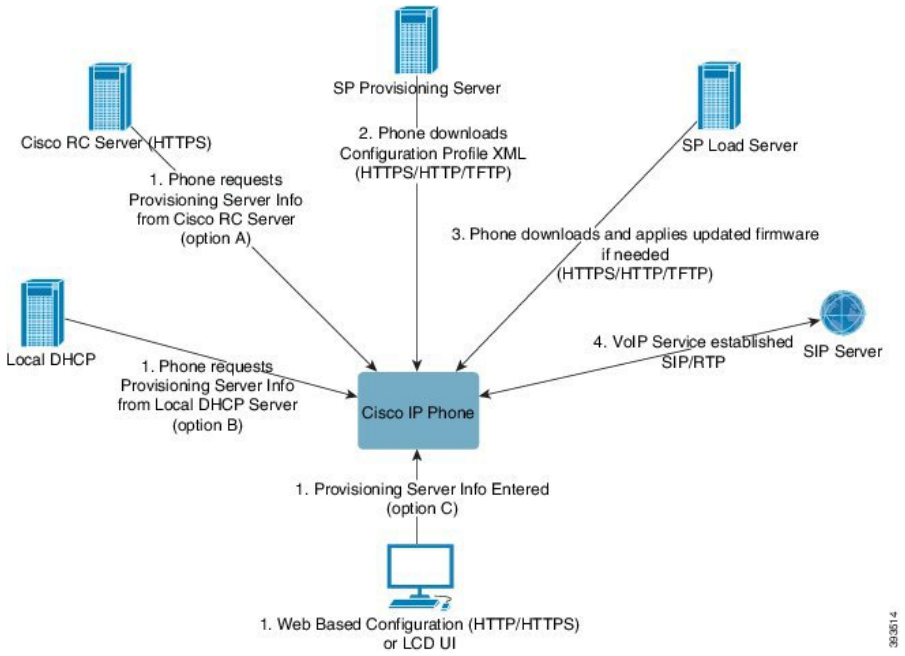
Преглед на обезпечаването

Cisco IP Phones са предназначени за големи внедрявания от доставчици на услуги за Voice-over-IP (VoIP) на клиенти в домове, фирми или в корпоративни среди. Следователно обезпечаването на телефона при използване на дистанционно управление и конфигуриране осигурява правилната работа на телефона на обекта на клиента.

Cisco поддържат персонализирано, непрекъснато конфигуриране на функциите на телефона чрез използване на:

- Надеждно дистанционно управление на телефона
- Шифроване на комуникацията, която управлява телефона.
- Опростено сдвояване на телефонни акаунти.

Телефоните могат да бъдат обезпечени да изтеглят профили за конфигуриране или да актуализират сървър от дистанционен сървър. Изтеглянето може да се случи, когато телефоните са свързани към мрежа, когато са включени и на зададени интервали. Обезпечаването е типична част от високообемните разгръщания с VoIP, предлагани от повечето доставчици на услуги. Профилите за конфигуриране или актуализиране на фърмуера се прехвърлят към устройството при използване на TFTP, HTTP или HTTPS.



На високо ниво процесът на обезпечаване на телефона е както следва:

1. Ако телефонът не е конфигуриран, информацията на сървъра за обезпечаване се прилага към телефона при използване на една от следните опции:
   - **A**–Изтегляне от Системата за активиране на аранжиране на данните на Cisco(EDOS), сървър за дистанционно персонализиране (RC) при използване на HTTPS.
   - **B**–Със заявка от местен DHCP сървър.
   - **C**–Ръчно въвеждане при използване на уеб базираната помощна програма за конфигуриране на телефони Cisco или потребителския интерфейс на телефона.
2. Телефонът изтегля информация за сървъра за обезпечаване и прилага конфигурационния XML при използване на HTTPS, HTTP или TFTP протокол.
3. Телефонът изтегля и прилага актуализирания фърмуер, ако е необходимо, при използване на HTTPS, HTTP или TFTP.
4. Услугата VoIP се установява при използване на посочена конфигурация и фърмуер.

VoIP услугата осигурява възможност за разгръщане на много телефони в жилищни сгради и при малки бизнес клиенти. В бизнес и корпоративни среди телефоните могат да служат като терминални възли. Доставчиците широко разпространяват тези устройства през интернет, свързвайки ги през маршрутизатори и защитни стени в помещенията на потребителите.

Телефонът може да се използва като дистанционна вътрешна линия на крайното оборудване на доставчика на услуги. Дистанционното управление и конфигуриране осигуряват правилна работа на телефона в помещенията на клиента.

Обезпечаване на TR69

Cisco IP Phone помага на администратора да конфигурира параметрите TR69 при използване на мрежов потребителски интерфейс. За информация относно параметрите, включително сравнение между тези в XML и TR69, вижте ръководството за администриране на съответната серия телефони.

Телефоните поддържат откриване на сървъри за автоматично конфигуриране (ACS) от DHCP, опция 43, 60 и 125.

- Опция 43–Специфична информация за оператора за ACS URL.
- Опция 60–Идентификатор на класа на доставчика за телефони, които се идентифицират с `dslforum.org` пред ACS.
- Опция 125– Специфична информация за оператора за асоцииране на шлюз.

Методи за RPC

Поддържани методи за RPC

Телефонът поддържа само ограничен набор от методи за повикване по дистанционна процедура (PRC), както следва:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Изтегляне: Изтегляне на PRC метод. Поддържаните типове файлове са:
  - Образ за фърмуерно надграждане
  - Конфигурационен файл на доставчика
  - Файл на Custom Certificate Authority (CA)
- Завършване на прехвърляне

Поддържани типове събития

Телефонът поддържа типове събития въз основа на поддържани характеристики и методи. Поддържат се само следните типове събития:

- Bootstrap
- Boot
- промяна на стойността
- заявка за свързване
- Periodic
- Завършване на прехвърляне
- M Download
- M Reboot

Поведение на телефона по време на задръстване на мрежата

- Административни задачи, като сканиране на вътрешни портове и защитно сканиране
- Атаки, които могат да възникнат в мрежата, като атака от тип отказ на услуга

Разгръщане

Cisco IP Phones осигурява удобни механизми за обезпечаване въз основа на моделите за разгръщане:

- Масово разпространение —Доставчикът на услуги придобива Cisco IP Phones на едро и или ги обезпечава на място, или закупува модули за дистанционно персонализиране (RC) от Cisco. Устройствата след това се издават на клиентите като част от договора за VoIP услуги.
- Разпространение на дребно—Клиентът закупува Cisco IP Phone от магазин и изисква VoIP услуга от доставчик на услуги. Доставчикът на услуги трябва да поддържа защитена дистанционна конфигурация на устройството.

Масови разпространения

В този модел доставчикът на услуги издава телефони на клиентите си като част от договора за VoIP услуги. Устройствата са или RC модули или предварително обезпечени домашни устройства.

Cisco обезпечава предварително RC модулите за повторно синхронизиране със Cisco сървър, който изтегля профила на устройството и актуализациите на фърмуера.

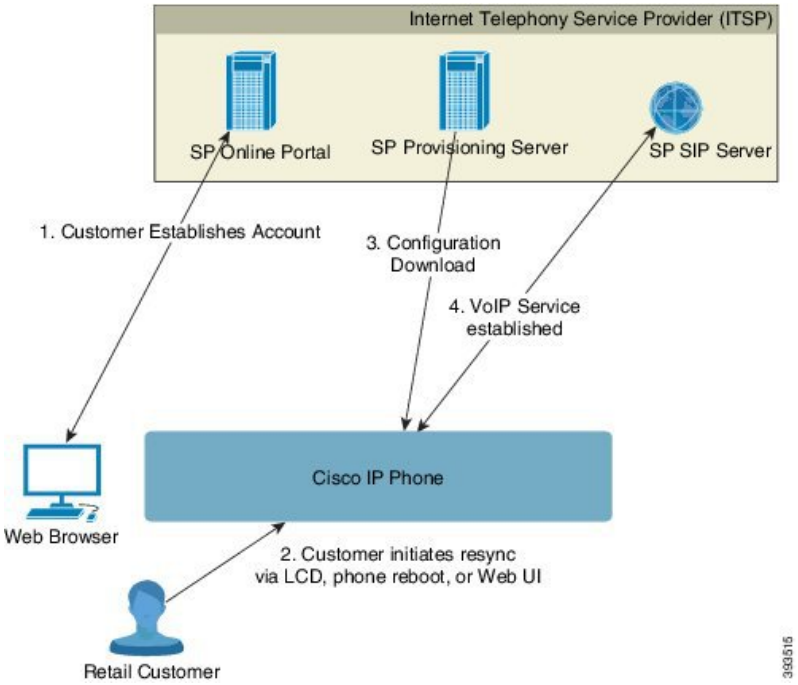
Доставчикът на услуги може да обезпечи предварително телефоните с желаните параметри, включително параметри, които управляват повторното синхронизиране с помощта на различни методи.

- На място при използване на DHCP и TFTP
- Дистанционно чрез използване на TFTP, HTTP или HTTPS
- Комбинация от обезпечаване на дистанционно и местно обезпечаване

Разпространение на дребно

В модела за разпространение на дребно клиентът закупува телефон и се абонира за определена услуга. Доставчикът на интернет услуги (ITSP) настройва и поддържа сървъра за обезпечаване и предварително обезпечава телефините за повторно синхронизиране със сървъра на доставчика на услуги.

Фигура *1:* Разпространение на дребно



Телефонът включва уеб базирана помощна програма за конфигуриране, която показва вътрешната конфигуриация и приема нови стойности на параметъра за конфигуриране. Сървърът освен това приема специален команден синтаксис за URL за изпълнение на повторно синхронизиране на дистанционния профил и операции по надграждане на фърмуера.

Клиентът се вписва на сървъра и създава VoIP акаунт най-често чрез онлайн портал и свързва устройството към асоциирания акаунт за услуги. Необезпеченият телефон получава инструкции да се синхронизира отново с посочен сървър за обезпечаване с помощта на URL команда за

повторно синхронизиране. URL командата обикновено включва номер на акаунт за клиентски ИД или буквеноцифров код за асоцииране на устройството с новия акаунт.

В следващия пример устройство на назначен с DHCP IP адрес 192.168.1.102 получава инструкции да се обезпечи към услугата SuperVoIP:

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

В този пример, 1234abcd представлява клиентския ИД номер на новия акаунт. Сървърът за дистанционно обезпечаване асоциира телефона, който изпълнява заявка за повторно синхронизиране, с новия акаунт въз основа на URL и доставения ИД на клиент. Чрез операцията за първоначално синхронизиране телефонът се конфигурира в една стъпка. Телефонът след това автоматично се насочва към повторно синхронизиране от постоянен URL на сървъра. Например:

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

За първоначален и постоянен достъп сървърът за обезпечаване разчита на удостоверяване на сертификата за клиент на телефона. Сървърът за обезпечаване подава правилни стойности на параметъра за конфигуриране въз основа на асоциирания акаунт за услуга.

При включване на устройството или при изтичане на посоченото време телефонът се синхронизира отново и изтегля последните параметри. Тези параметри могат да адресират цели, като задаване на група за претърсване, номера за бързо набиране и ограничаване на функциите, които могат да бъдат променени от потребителя.

Сродни теми

Устройство за обезпечаване на място, на стр.44

Процес на повторно синхронизиране

Фърмуерът за всеки от телефоните включва административен уеб сървър, който приема новите стойности на параметъра за конфигуриране. Телефонът може да бъде инструктиран да синхронизира отново конфигурацията след презареждане или на планирани интервали с посочен сървър за обезпечаване чрез URL команда за повторно синхронизиране в профила на устройството.

Уеб сървърът е активиран по подразбиране. За да деактивирате или активирате уеб сървъра, използвайте URL команда за повторно синхронизиране.

Ако е необходимо, можете да заявите незабавно повторно синхронизиране чрез “resync" на URL на действие. URL командата за повторно синхронизиране може да включва ИД номер на акаунт на клиент или буквено-цифров код за уникално асоцииране на устройството с акаунта на потребителя.

Пример

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

В този пример устройство с DHCP-зададен IP адрес 192.168.1.102 получава инструкции да обезпечи себе си за услугата SuperVoIP на prov.supervoip.com. Потребителският ИД номер за новия акаунт е 1234abcd. Сървърът за дистанционно обезпечаване асоциира телефона, който извършва заявката за повторно синхронизиране, с акаунта въз основа на URL и ИД на клиент.

Чрез операцията за първоначално синхронизиране телефонът се конфигурира в една стъпка. Телефонът след това автоматично се насочва към повторно синхронизиране от постоянен URL на сървъра.

За първоначалния и постоянен достъп сървърът за обезпечаване разчита на сертификат за удостоверяване на клиента. Сървърът подава стойностите на параметъра за конфигуриране въз основа на асоциирания акаунт за услуга.

Осигуряване

Телефонът може да се конфигурира да синхрозира повторно състоянието на вътрешно конфигуриране така, че да съответства на дистанционния профил периодично и при включване. Телефонът се свързва със сървър за обикновено обезпечаване (NPS) или сървър за контрол на достъпа (ACS).

По подразбиране се прави опит за повторно синхронизиране на профила, когато телефонът е свободен. Тази практика предотвратява надграждане, което би стартирало повторно зареждане на софтуера и прекъсване на повикване. Ако са необходими междинни надграждания за достигане на настоящото състояние на надграждане от по-стара версия, логиката за надграждане може да автоматизира надграждане на много етапи.

Обикновен сървър за обезпечаване

Обикновеният сървър за обезпечаване (NPS) може да бъде TFTP, HTTP или HTTPS сървър. Дистанционното надграждане на сървъра се постига при използване на TFTP или HTTP, или HTTPS, тъй като фърмуерът не съдържа чувствителна информация.

Въпреки че се препоръчва HTTPS, комуникацията с NPS не изисква използване на защитен протокол, тъй като надграденият профил може да се шифрова чрез споделяне на защитен ключ. За повече информация относно използването на HTTPS вижте Шифроване на комуникацията, на стр.9. Защитеното първоначално обезпечаване се осигурява чрез механизъм, който използва SSL функции. Необезпеченият телефон може да получава профил, шифрован с 256-битов симетричен ключ, който е специално предназначен за това устройство.

Управление на достъпа до конфигурирането

фърмуерът на телефона осигурява механизми за ограничаване на достъпа на крайния потребител до някои параметри. Фърмуерът осигурява определени привилегии за вписване в акаунта **Администратор** на акаунта **Потребител**. Всеки може да бъде независимо защитен от парола.

- Администраторски акаунт – Позволява на доставчика на услуги пълен достъп до всички параметри на уеб сървъра за администриране.
- Потребителски акаунт – Позволява на потребителя да конфигурира подмножество от параметри на уеб сървъра за администриране.

Доставчикътна услуги може да ограничи потребителския акаунт в профила за обезпечаване по следните начини:

- Да посочи кои параметри за конфигуриране са достъпни в потребителския акаунт при създаването на конфигурацията.
- Деактивирайте достъпа на потребителя до административния уеб сървър.
- Деактивирайте достъпа на потребителя до потребителския интерфейс на LCD.
- Пропускане на екрана **Задаване на парола** за потребителя.
- Ограничаване на домейните в интернет, до които устройството осъществява достъп за повторно синхронизиране, надграждане или SIP регистрация за линия 1.

Сродни теми

Свойства на тагове на елемент, на стр.14
Управление на достъпа, на стр.16

Достъп до уеб страницата на телефона

Осъществете достъп до уеб страницата на телефона от уеб браузър на компютър, който може да достигне до телефона в подмрежата.

Ако доставчикът на услуги е деактивирал достъпа до помощната програма за конфигуриране, се свържете с него преди да продължите.

Процедура

Стъпка 1 Уверете се, че компютърът може да комуникира с телефона. Не се използва VPN.

Стъпка 2 Стартирайте уеб браузъра.

Стъпка 3 Въведете IP адреса на телефона в адресното поле на уеб браузъра.

- Потребителски достъп: **`http://<ip address>/user`**
- Достъп за администратори: **`http://<ip address>/admin/advanced`**
- Достъп за администратори: **`http://<ip address>`**, щракнете върху **Влизане на администратор** и натиснете **разширени**

Например `http://10.64.84.147/admin`

Позволява уеб достъп до Cisco IP Phone

За да прегледате параметрите на телефона, активирайте профила за конфигуриране. За да направите промени в някои от параметрите, трябва да можете да промените профила за конфигуриране. Системният администратор може да е деактивирал опция на телефона, за да направи потребителският уеб интерфейс на телефона достъпен за преглед или запис.

За повече информация вижте Ръководство за обезпечаване на многоплатформени телефони серия *Cisco IP Phone 6800*.

Преди да започнете

Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Процедура

Стъпка 1 Щракнете върху **Гласови** > **Система**.

Стъпка 2 В раздела **Конфигурация на системата** задайте **Активиране на уеб сървър** на **Да**.

Стъпка 3 За да актуализирате профила за конфигуриране, натиснете **Изпрати всички промени** след като промените полетата в потребителския уеб интерфейс на телефона.

Телефонът се зарежда отново и промените се прилагат.

Стъпка 4 За да изтриете всички направени промени по време на текущата сесия (или след последното щракване върху**Изпращане на всички промени**), щракнете върху **Отмяна на всички промени**. Стойностите се връщат към предишните си настройки.

Шифроване на комуникацията

Параметрите за конфигуриране, които се съобщават на устройството, могат да съдържат кодове за удостоверяване или друга информация, която защитава системата от неупълномощен достъп. В интерес на доставчика на услуги е да предотврати неупълномощена дейност на клиентите. В интерес на клиентите е да предотвратят неупълномощено използване на акаунта. Доставчикът на услуги може да шифрова комуникацията за профила за конфигуриране между сървъра за обезпечаване и устройството в допълнение към ограничаването на достъпа до уеб сървъра на администратора.

Практики за обезпечаване на телефона

Обикновено Cisco IP Phone се конфигурира за обезпечаване, когато се свърже с мрежата за първи път. Телефонът освен това се обезпечава на планирани интервали, които се задават от доставчика на услуги или от предварителното обезпечаване VAR (конфигуриране) на телефона. Доставчиците на услуги могат да упълномощят VAR или напреднали потребители за ръчно обезпечаване на телефона при използване на клавиатурата му. Освен това можете да конфигуирате обезпечаване при използване на уеб потребителския интерфейс на телефона.

Проверете **Състояние** > **Състояние на телефона** > **Обезпечаване** от потребителския интерфейс на LCD на телефона или състоянието на обезпечаване в раздела **Състояние** на уеб базираната помощна програма за конфигуриране.

Сродни теми

Ръчно обезпечаване на телефона от клавиатурата, на стр.10

Ръчно обезпечаване на телефона от клавиатурата

Процедура

Стъпка 1 Натиснете **Приложения** .

Стъпка 2 Изберете **Администриране на устройството** > **Правило за профил**.

Стъпка 3 Въведете правилото за профил, като използвате следния формат:

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

Например:

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

Ако не е посочен протокол, се разбира TFTP. Ако не е посочено име на сървър, хостът, който заявява URL се използва като име на сървър. Ако не е посочен порт, се използва портът по подразбиране (69 за TFTP или 443 за HTTPS).

Стъпка 4 Натиснете **Повторно синхронизиране**.

Сродни теми

Практики за обезпечаване на телефона, на стр.9

Равноправно споделяне на фърмуер

Равноправното споделяне на фърмуер (PFS) представлява модел за разпространение на фърмуера, който позволява на Cisco IP Phone да намира други телефони от същия модел или серия в подмрежата и да споделя файлове с актуализирания фърмуер, когато е необходимо надграждане на много телефони едновременно. PFS използва собствения протокол Cisco Peer-to-Peer-Distribution Protocol (CPPDP). Със CPPDP всички устройства в подмрежата образуват равноправна йерархия, след което фърмуерът или други файлове се копират от равноправните устройства към съседните. За да оптимизира надграждането на фърмуер, основният телефон изтегля образ на фърмуера от сървъра за зареждане и след това го прехвърля на другите телефони в подмрежата, като използва TCP връзки.

Равноправно споделяне на фърмуер

- Ограничава претоварването при TFTP прехвърляния към централизирани отдалечени сървъри за зареждане.
- Елиминира необходимостта за ръчно управление на надграждането на фърмуера.
- Намалява времето за престой на телефона при надграждане, когато едновременно се нулират голям брой телефони.

Забележка

- Равноправното споделяне на фърмуер не функционира, освен ако не е настроено едновременно надграждане на няколко телефона. Когато с Event:resync се изпрати NOTIFY, това стартира повторно синхронизиране на телефона. Пример за xml, който може да съдържа конфигурации за стартиране на надграждане:

  "Събитие: resync; профил ="http://10.77.10.141/profile.xml
- Когато посочите IP адрес и порт за сървъра с регистрационни файлове за равноправното споделяне на фърмуер (PFS), данните за PFS се изпращат до този сървър като UDP съобщения. Тази настройка трябва да се извърши на всеки телефон. След това можете да използвате съобщенията в регистрационния файл при отстраняването на проблеми, свързани с PFS.

Peer_Firmware_Sharing_Log_Server посочва името на хоста и порта за отдалечения syslog сървър, работещ с UDP. Портът по подразбиране е стандартният за syslog – 514.

Например:

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

За да използвате тази функция, активирайте PFS на телефоните.

Пропускане на екрана за задаване на парола

Можете да пропуснете екрана **Задаване на парола** при първото стартиране или след възстановяване на фабричните настройки в зависимост от следните действия при обезпечаването:

- DHCP конфигурация
- EDOS конфигурация
- Конфигурация на потребителската парола чрез XML файла за конфигуриране на телефона.

Таблица *1:* Действия при обезпечаването, които определят дали да се показва екранът за задаване на парола

Конфигуриран през DHCP	Конфигуриран през EDOS	Конфигурирана потребителска парола	Пропускане на екрана за задаване на парола
Да	неприложимо	Да	Да
Да	неприложимо	Не	**Не**
Не	Да	Да	Да
Не	Да	Не	**Не**
Не	Не	неприложимо	**Не**

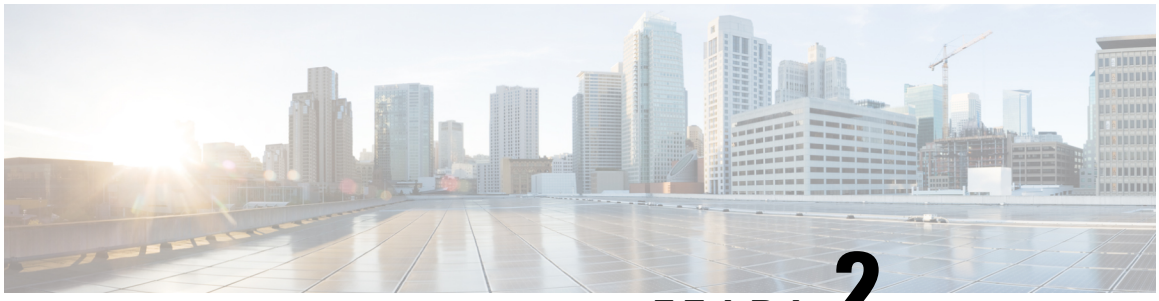
Процедура

Стъпка 1 Редактирайте файла `config.xml` на телефона с текстов или XML редактор.

Стъпка 2 Вмъкнете маркера **<User_Password>**, като използвате някоя от следните опции.

- **Без парола (начален и краен маркер)** – **<User_Password></User_Password>**
- **Стойност на паролата (от 4 до 127 знака)** – **<User_Password ua="rw">abc123</User_Password>**
- **Без парола (само начален маркер)** – **<User_Password />**

Стъпка 3 Запазете промените във файла `config.xml`.



ГЛАВА 2

Обезпечаващи скриптове

Обезпечаващи скриптове

Телефонът получава конфигурацията в XML формат.

За подробна информация относно телефона вижте ръководството за администриране за конкретното устройство. Всяко ръководство описва параметрите, които могат да се конфигурират чрез уеб сървър за конфигуриране.

Формати на конфигурационни профили

Профилът за конфигуриране дефинира стойностите на параметъра за телефона.

XML форматът на профила за конфигуриране използва стандартни инструменти за упълномощаване на XML за попълване на параметрите и стойностите.

Забележка Поддържа се само кодова таблица UTF-8. Ако промените профила в редактор, не променяйте формата на кодиране; в противен случай телефонът не може да разпознае файла.

За всеки телефон са зададени различни функции и следователно има различен набор от параметри.

Профил в XML формат (XML)

Профилът в отворен формат представлява текстов файл с подобен на XML синтаксис в йерархията на елементите, с атрибути на елементи и стойности. Този формат позволява да

използвате стандартни инструменти за създаване на конфигурационен файл. Конфигурационният файл в този формат може да се изпрати от сървъра за обезпечаване към телефона по време на операция за повторно синхронизиране. Файлът може да се изпрати без компилиране като двоичен обект.

Телефонът може да приема формати за конфигуриране, генерирани от стандартните инструменти. Тази функция улеснява разгръщането на софтуера на крайния сървър за обезпечаване, който генерира профили за конфигуриране от съществуващи бази с данни.

За да защити поверителната информация в профила за конфигуриране, сървърът за обезпечаване предава този тип файл към телефона през защитен от TLS канал. Като опция файлът може да се компресира при използване на алгоритъм за намаляване на gzip (RFC1951).

Файлът може да бъде шифрован с един от следните методи за шифроване:

- AES-256-CBC шифроване
- Шифроване на HTTP въз основа на RFC-8188 с AES-128-GCM шифроване

Пример: Профил с отворен формат

```
<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>
```

Тагът на елемента <flat-profile> затваря всички елементи на параметъра, които се разпознават от телефона.

Сродни теми

Компресиране и шифроване на профил Open (XML), на стр.18

Компоненти на конфигурационни профили

Конфигурационният файл може да включва следните компоненти:

- Маркери за елементи
- Атрибути
- Параметри
- Функции за форматиране
- XML коментари

Свойства на тагове на елемент

- Форматът за XML обезпечаване и уеб потребителският интерфейс позволяват конфигуриране на същите настройки. Името на XML маркера и имената на полетата в уеб потребителския интерфейс са подобни, но варират поради ограниченията за имена на XML елементи. Например долна черта (_) вместо " ".

- Телефонът разпознава елементи с правилни имена на параметри, които са капсулирани в специален елемент <flat-profile>.
- Имената на елементите са затворени в ъглови скоби.
- Повечето имена на елементи са подобни на имената на полетата в уеб страниците за администриране на устройството при следните изменения:
  - Имената на елементите не могат да включват интервали или специални знаци. За да се породят имената на елементите от името на полето в интерфейса за уеб администриране, заменете с долна черта всеки интервал или специален знак `[`, `]`, `(`, `)` или `/`.

    Например: елементът <Resync_On_Reset> представя полето **Повторно синхронизиране при нулиране**.
  - Всяко име на елемент трябва да бъде уникално. На уеб страниците за администриране едни и същи полета могат да се показват на много страници, като страниците за ред, потребител и разширение. Долепете `[n]` към името на елемента, за да посочите, че номерът е показан на раздела на страницата.

    Пример: Елементът <Dial_Plan_1_> представя **План за набиране** за Линия 1.
- Всеки отварящ таг на елемент трябва да има съответстващ затварящ таг. Например:

```
<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>
```

- Таговете на елементите различават малки и големи букви.
- Позволяват се празни тагове на елементи и ще бъдат интерпретирани като конфигуриране на празна стойност. Въведете отварящия таг на елемент без съответен таг на елемент и вмъкнете интервал и наклонена напред черта преди да затворите ъгловата скоба (>). В този пример Profile Rule B е празен:

```
<Profile_Rule_B />
```

- Празният таг на елемент може да се използва за предотвратяване на презапис на поставена от потребителя стойност по време на повторно синхронизиране. В следващия пример настройките за бързо набиране от потребителя не са променени.

```
<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>
```

- Използвайте празна стойност, за да зададете съответния параметър на празен низ. Въведете отварящ и затварящ елемент без стойност помежду им. В следващия пример параметърът GPP_A е настроен на празен низ.

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

- Неразпознатите имена на елементи се игнорират.

Сродни теми

Управление на достъпа до конфигурирането, на стр.7

Атрибут за потребителски достъп

Атрибутът за потребителски достъп (**ua**) може да се използва за промяна на достъпа от потребителския акаунт. Ако атрибутът **ua** не се посочи, съществуващата настройка за потребителски достъп се запазва. Този атрибут не оказва влияние върху достъпа от администраторски акаунт.

Атрибутът **ua**, ако присъства, трябва да има една от следните стойности:

- na—Няма достъп
- ro—Само за четене
- rw—Четене и запис

Следващият пример илюстрира атрибута **ua**:

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

Опцията **ua** трябва да бъде оградена от двойни кавички.

Управление на достъпа

Ако е активиран параметър <Phone-UI-User-Mode>, трафичният потребителски интерфейс на телефона уважава атрибута за достъп на потребителя за съответните параметри, когато интерфейсът представя елемент на меню.

За въвежданията в менюто, които се свързват с един конфигурационен параметър:

- Обезпечаването на параметъра с атрибута „ua=na" („ua" означава потребителски достъп) води до изчезване на полето за въвеждане.
- Обезпечаването на параметъра с атрибута ua=ro" прави полето за въвеждане само за четене и не позволява редактиране.

За елементи на менюто, които са асоциирани с много параметри за конфигуриране:

- Обезпечаването на всички съответни параметри с атрибута „ua=na” води до изчезване на съответните елементи.

Сродни теми

Управление на достъпа до конфигурирането, на стр.7

Свойства на параметри

Към параметрите се прилагат следните свойства:

- Параметрите, които не са посочени от профила, остават непроменени в телефона.
- Неразпознатите параметри се игнорират.
- Ако профилът във формат Open съдържа много екземпляри от един и същи таг на параметър, последният екземпляр има предимство пред по-ранните. За да избегнете нежелано припокриване на стойностите на конфигурацията за параметър, препоръчваме всеки профил да посочва само по един екземпляр от параметър.
- Последният обработен профил има предимство. Ако много профили посочват един и същи параметър за конфигуриране, има предимство стойността на по-новите профили.

формати на низове

Тези свойства се отнасят за форматирането на низовете.

- Коментарите се разрешават чрез стандартен XML синтаксис.

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

- Позволяват се водещи и крайни интервали за подобряване на четенето, но се отстраняват от стойността на параметъра.
- Новите редове в стойността се преобразуват в интервали.
- Допуска се XML заглавка във формата <? ?>, но телефонът я пренебрегва.
- За да въведете специални знаци, използвайте основните XML знаци, които са показани в следващата таблица.

Специален знак	XML ескейп последователност
& (амперсанд)	&amp;
< (по-малко от)	&lt;
> (по-голямо от)	&gt;
’ (апостроф)	&apos;
” (двойни кавички)	&quot;

В следващия пример ескейп знакът се въвежда, за да представи символите за по-голямо и по-малко, които се изискват от правилото на плана за набиране. Примерът дефинира план за набиране на гореща линия за информация, която задава параметъра

<Dial_Plan_1_>(**Влизане на администратор** > **разширени** > **Гласови** > **Вн. (n)**) равно на (S0 <:18005551212>).

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

- Ескейп символи на цифрови знаци, които използват десетични и шестнадесетични стойности (напр. `&#40;` и `&#x2e;`), се преобразуват.
- Фърмуерът на телефона поддържа само ASCII знаци.

Компресиране и шифроване на профил Open (XML)

Профилът на конфигурацията Open може да се компресира, за да се намали мрежовото натоварване на сървъра за обезпечаване. Профилът може също да се шифрова, за да се защити поверителната информация. Не се изисква компресиране, но то трябва да предшества шифроването.

Сродни теми

Формати на конфигурационни профили, на стр.13

Компресирарне на профил Open

Поддържаният метод на компресиране е алгоритъм с gzip намаляване (RFC1951). Помощната програма gzip и библиотеката за компресиране, която прилага същия алгоритъм (zlib), са достъпни от интернет сайтове.

За да разпознае компресирането, телефонът очаква компресираният файл да съдържа съвместима с gzip заглавна част. Извикването на помощната програма gzip на оригиналния профил за Open генерира заглавната част. Телефонът проверява заглавието на изтегления файл, за да определи файловия формат.

Например, ако `profile.xml` е валиден профил, файлът `profile.xml.gz` също ще бъде приет. Всяка от следните команди може да генерира този тип профил:

- `>gzip profile.xml`

  Заменя оригиналния файл с компресирания.

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

  Оставя на място оригиналния файл и създава нов компресиран файл.

Обучение за компресирането можете да намерите в раздела Компресиране на профил Open с Gzip, на стр.68.

Сродни теми

Компресиране на профил Open с Gzip, на стр.68

Шифроване на отворен профил

Симетричното шифроване с ключ може да се използва за шифроване на профил на отворена конфигурация, независимо дали файлът е компресиран или не. Компресиране, ако се прилага, трябва да се прилагат преди шифроване.

Сървърът за обезпечаване използва HTTPS за обработване на първоначалното обезпечаване на телефона след разгръщането. Предварително шифрованите офлайн профили на конфигурацията позволяват използване на HTTP за последващо повторно синхронизиране на профилите. Това намалява натоварването на HTTPS сървъра при широкомащабни разгръщания.

Телефонът поддържа два метода на шифроване на конфигурационни файлове:

- AES-256-CBC шифроване
- Основаващо се на RFC 8188-шифромване на HTTP съдържание с шифър AES-128 Лепкавост използваме

Ключът трябва да бъде обезпечен в модула по-рано. Зареждащата лента на секретния ключ може да бъде извършена защитено при използване на HTTPS.

Името на конфигурационният файл не изисква специален формат, но името на файл, който завършва с разширение `.cfg` обикновено показва профил за конфигуриране.

AES-256-CBC шифроване

Телефонът поддържа AES-256 ТГС шифроване за конфигурационни файлове.

Инструментът за шифроване на OpenSSL, който можете да изтеглите от различни сайтове в интернет, може да извърши шифроването. Поддръжката на 256-битово AES шифроване може да изисква повторно компилиране на инструмента, за да се активира AES кода. Фърмуерът е тестван според версия openssl-0.9.7c.

Шифроване на профил с OpenSSL, на стр.69 осигурява обучение по шифроване.

Профилът очаква шифрован файл, който има същия формат, който е генериран от следната команда:

```
# 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
```

Малки букви -k предшества защитния ключ, който може да бъде обикновена текстова фраза и който се използва за генериране на произволен 64-битов солт. С посочена от -k аргумента тайна, инструментът за шифроване подава произволен 128-битов начален вектор и реален 256-битов ключ за шифроване.

Когато тази форма на шифроване се използва на конфигурационен профил, телефонът трябва да бъде информиран за стойността на секретния ключ, за да дешифрира файла. Тази стойност

се посочва като квалификатор в URL на профила. Синтаксисът е както следва при използване на изричен URL:

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

Тази стойност е програмирана чрез използване на параметри за правило на профила.

Сродни теми

Шифроване на профил с OpenSSL, на стр.69

Макро разширяване

Няколко параметъра за обезпечаване преминават вътрешно през макро разширение преди да бъда оценени. Стъпката на предварителна оценка осигурява по-голяма гъвкавост при управлението на повторното дейностите за повторно синхронизиране и надграждане на телефона.

Следните групи параметри преминават през макро разширение преди да бъдат оценени:

- Resync_Trigger_*
- Profile_Rule_*
- Log_xxx_Msg
- Upgrade_Rule

При определени условия някои параметри с общо предназначение (GPP_*) също преминават през макро разширение, както е посочено изрично в Незадължителни аргументи за повторно синхронизиране, на стр.24.

По време на макро разширението съдържанието на променливите с имена заменя изразите под формата на $NAME и $(NAME). Тези променливи включват параметри с общо предназначение, няколко идентификатора на продукти, определени таймери на събития и стойности за състояние на обезпечаване. Пълният списък можете да видите на Променливи за макро разширение, на стр.82.

В следния пример изразът $(MAU) се използва за вмъкване на MAC адрес 000E08012345.

Администраторът въвежда: **`$(MAU)config.cfg`**

Полученото макро разширение за устройство с MAC адрес 000E08012345 е:
`000E08012345config.cfg`

Ако макро името не бъде разпознато, остава неразширено. Например името STRANGE не се разпознава като валидно макро име, а MAU се разпознава като валидно макро име.

Администраторът въвежда: **`$STRANGE$MAU.cfg`**

Полученото макро разширение за устройство с MAC адрес 000E08012345 е:
`$STRANGE000E08012345.cfg`

Макро разширяването не се прилага рекурсивно. Например $$MAU" се разширява в $MAU" (разширява се $$) и не води до получаване на MAC адрес.

Съдържанието на параметрите със специална цел GPP_SA до GPP_SD се назначава за макро изрази $SA до $SD. Тези параметри получават макро разширение само като аргументи на опциите **--key** , **--uid** и **--pwd** в URL за повторно синхронизиране.

Условни изрази

Условните изрази могат да превключат събития за повторно синхронизиране и да избират от алтернативни URL за операции на повторно синхронизиране и надграждане.

Условните изрази се състоят от списък от сравнения, разделени от оператора **и**. Всички сравнения трябва да бъдат удовлетворени, за да бъде условието истина.

Всяко сравнение може да бъде свързано с един от следните типове групи от литерали:

- Цели стойности
- Номера на софтуерни или хардуерни версии
- Низове в двойни кавички

Номера на версии

Официалните софтуерни версии на многоплатформените телефони (MPP) използват следния формат, където BN==Номер на варианта:

- Серия Cisco IP Phone 6800—`sip68xx.v1-v2-v3MPP-BN`

Низът за сравнение трябва да използва същия формат. В противен случай се получава грешка във формата на синтактичния анализ.

В софтуерна версия v1-v2-v3-v4 може да се посочат различни цифри и знаци, но първо трябва да има число. При сравняване на софтуерна версия v1-v2-v3-v4 се сравняват последователно, а най-левия знак има преимущество пред останалите.

Ако v[x] включва само цифри, се сравняват цифрите; ако v[x] включва само номера + алфа знаци, първо се сравняват цифрите, а след това знаците се сравняват в азбучен ред.

Пример за валиден номер на версията

sipyyyy.11-0-0MPP-BN

По контраст: 11.0.0 е невалиден формат.

Сравнение

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

Низовете в кавички могат да се сравнят за еднаквост или различие. Целите числа и номерата на версии също могат да се сравняват аритметично. Операторите за сравнение могат да се изразят като символи или акроними. Акронимите са удобни при изразяване на условие в профил с отворен формат.

На оператора	Алтернативен синтаксис	Описание	Приложим за цели числа и операнди на версия	Приложим за операнди на низове в кавички
=	eq	равен на	Да	Да
!=	ne	не равен на	Да	Да
<	lt	по-малко от	Да	Не
<=	le	по-малко или равно на	Да	Не
>	gt	по-голямо от	Да	Не
>=	ge	по-голямо или равно на	Да	Не
AND		и	Да	Да

Важно е да се оградят макро променливите в двойни кавички, когато се очаква низ от литерали. Не правете това, когато се очаква число или номер на версия.

Когато се използват в контекста на параметрите Profile_Rule* и Upgrade_Rule, условните изрази трябва да бъдат със синтаксис „(израз)?“, както в следния пример за правило на надграждане. Помнете, че BN означава номер на варианта.

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

Не използвайте предходния синтаксис със скоби, за да конфигурирате параметрите Resync_Trigger_*.

Синтаксис на URL

Използвайте стандартен синтаксис за URL, за да посочите как да се извлекат конфигурационните файлове и зарежданията на фърмуера съответно в параметрите Profile_Rule* и Upgrade_Rule Синтаксисът е както следва:

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

Където **`scheme`** е една от следните стойности:

- tftp
- http
- HTTPS

Ако **`scheme`** се пропусне, се подразбира tftp. Сървърът може да бъде разпознаван с DNS име на хост или цифров IP адрес. Портът е дестинационния UDP или номер на TCP порт. Пътят на файла трябва да започва с главната директория (/); трябва да бъде абсолютен път.

Ако **`server`** липсва, се използва tftp сървъра, посочен чрез DHCP (опция 66).

Забележка Сървърът трябва да бъде посочен в правилата за надграждане.

Ако **port** липсва, се използва tftp сървъра, посочен чрез DHCP (опция 66). Tftp използва UDP порт 69, http използва TCP порт 80, https използва TCP порт 443.

Трябва да има път до файл. Не е необходимо позоваване на статичен файл, но може да посочи динамично съдържание, получено чрез CGI.

Макро изразът е приложим в URL. Следват примери от валидни 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
```

При използване на DHCP опция 66 правилата за надграждане не поддържат празен синтаксис. Прилага се само за правилото на профила *.

Основаващо се на RFC 8188 шифроване на HTTP съдържанието

Телефонът пддържа основаващо се RFC 8188 шифроване на HTTP с шифър AES-128-GCM за конфигурационни файлове. С този метод за шифроване всички въвеждания елементи могат да четат заглавията на HTTPS съобщенията. Въпреки това само елементите, които знаят входния ключов материал (IKM) могат да четат пакета.. Когато телефонът е обезпечен с IKM, телефонът и сървърът за обезпечаване могат да обменят конфигурационни файлове защитено, докато позволяват на мрежови елементи на трети страни да използват заглавията на съобщенията за целите на наблюдение и анализ.

Параметърът на XML конфигурацията **IKM_HTTP_Encrypt_Content** съдържа IKM на телефона. Поради съображения за безопасност този параметър не е достъпен на уеб страницата за администриране на телефона. Освен това не е видим в конфигурационния файл на телефона, който е достъпен от IP адреса на телефона или от отчетите за конфигурацията на телефона, изпратени към сървъра за обезпечаване.

Ако искате да използвате основаващо се на RFC 8188 шифроване, гарантирайте следното:

- Осигурете телефона с IKM като посочите IKM с XML параметър **IKM_HTTP_Encrypt_Content**във конфигурационния фал, който се изпраща от сървъра за обезпечаване към телефона.
- Ако това шифроване се приложи към конфигуационни файлове, изпратени от сървър за обезпечаване към телефона, се уверете, че заглавието на HTTP шифровано съдържание в онфигурационния файл е “aes128gcm”.

  При липса на това заглавие методът AES-256 ТГС има предимство. Телефонът прилага дешифриране AES-256 CBC, ако в правилото на профила присъства бутона AES-256 CBC, независимо от IKM.
- Ако искате телефонът да прилага това шифроване към отчетите на конфигурацията, кито изпраща към сървъра за обезпечаване, се уверете че няма бутон AES-256 ТГС в правилото на отчета.

Незадължителни аргументи за повторно синхронизиране

Незадължителните аргументи **key**, **uid** и **pwd** могат да предшестват URL, въведени в параметрите Profile_Rule*, като бъдат оградени от квадратни скоби.

key

Опцията **--key** указва на телефона, че конфигурационният файл, който получава от сървъра за обезпечаване е шифрован с AES-256-CBC , освен ако заглавието Шифрован на съдържанието във файла не показва "aes128gcm" шифроване. Самият ключ е посочен като низ след термина **--key**. Ключът може да бъде затворен в двойни кавички ("), като опция Телефонът използва ключа за дешифриране на конфигурационния файл.

Примери за използване

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

Посочените в скоби аргументи-опция са макроразширени. Параметрите за специални цели GPP_SA до GPP_SD са макроразширени в макро променливи, $SA до $SD, само когато се използват като аргументи на ключова опция. Вижте следните примери:

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

При профилите във формат Open аргументът към **--key** трябва да бъде същия, както аргументът към опцията **-k**, която се дава за **openssl**.

uid и pwd

Опциите **uid** и **pwd** могат да се използват за посочване на удостоверяването на потребителски ИД и парола за посочения URL. Посочените в скоби аргументи-опция са макроразширени. Параметрите за специални цели GPP_SA до GPP_SD са макроразширени в макро променливи, $SA до $SD, само когато се използват като аргументи на ключова опция. Вижте следните примери:

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

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

при това се разширяват в:

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

Прилагане на профил към устройство за IP телефония

След като създадете XML конфигурационен скрипт, той трябва да бъде предаден към телефона за прилагане. За да приложите конфигурацията, можете или да изтеглите конфигурационния файл на телефона от TFTP, HTTP или HTTPS сървър с помощта на уеб браузър, или като използвате командата cURL на помощната програма на командния ред.

Изтеглете конфигурационния файл на телефона от TFTP сървър

Изпълнете тези стъпки, за да изтеглите конфигурационния файл на приложението за TFTP на компютъра.

Процедура

Стъпка 1 Свържете компютъра към LAN на телефона.

Стъпка 2 Изпълнете прприложението за TFTP сървър на компютъра и се уверете, че конфигурационният файл е достъпен в главната директория на TFTP.

Стъпка 3 В уеб браузъра въведете IP адреса на LAN на телефона, IP адреса на компютъра, името на файла и данните за вход. Използвайте следния формат:

http://<WAN_IP_Address>/admin/resync?tftp://<PC_IP_Address>/<file_name>&xuser=admin&xpassword=<password>

Пример:

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

Изтеглете конфигурационния файл на телефона с помощта на cURL

Извършете следните стъпки, за да изтеглилте конфигурацията на телефона като използвате cURL. Този инструмент на командния ред се използва за прехвърляне на данни със синтаксис на URL. За да изтеглите cURL, вижте:

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

Забележка Препоръчваме да не използвате cURL за публикуване на конфигурацията на телефона, тъй като потребителското име и паролата могат да се прихванат при използване на cURL

Процедура

Стъпка 1 Свържете компютъра с LAN порта на телефона.

Стъпка 2 Изтеглете конфигурационния файл на телефона, като въведете следната команда на cURL:

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

Параметри за обезпечаване

Този раздел описва параметрите за обезпечаване, които се организират в съответствие с функциите:

Съществуват следните типове параметри за обезпечаване:

- Обща цел
- Активирания
- Превключватели
- Подлежащи на конфигуриране графици
- Правила за профил
- Правило за надграждане

Параметри с общо предназначение

Параметрите с общо предназначение GPP_* (**Вход на администратор** > **разширени** > **Гласови** > **Обезпечаване**) се използват като безплатни регистратори на низове при конфигуриране на телефона за взаимодействие с определено решение за сървър за обезпечаване. Параметрите GPP_* са празни по подразбиране. Те могат да се конфигурират така, че да съдържат различни стойности, включително следните:

- Ключове за шифроване
- URL
- Информация за многото етапи на обезпечаване
- Шаблони за публикуване на заявка
- Карти на псевдонимите на името на параметъра
- Частични стойности на низове, евентуално комбинирани в пълни параметрични стойности.

Параметрите GPP_* са достъпни за макро разширяване в други параметри за обезпечаване. За тази цел се използват макро имена със суфикс от една главна буква (A до P) за разпознаване на съдържанието на GPP_A до GPP_P. Освен това макро имената с две главни букви, от SA до

SD, посочват GPP_SA through GPP_SD като специален случай при използване на аргументи на следните URL опции:

key, **uid** и **pwd**

Тези параметри могат да се използват като променливи при правилата за обезпечаване и надграждане. Посочват се чрез поставяне пред името на променливата на знака'$'. Например $GPP_A.

Използване на параметри с общо предназначение

Например, ако GPP_A съдържа низ ABC, а GPP_B съдържа 123, макросът на израза AB се разширява до ABC123.

Преди да започнете

Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Процедура

Стъпка 1 Изберете **Глас** > **Обезпечаване**.

Стъпка 2 Превъртете до раздела **Параметри с общо предназначение**.

Стъпка 3 Въведете валидни стойности в полетата GPP A до GPP P.

Стъпка 4 Кликнете върху **Изпращане на всички промени**.

Активирания

Параметрите Provision_Enable и Upgrade_Enable управляват всички операции по повторно синхронизиране на профили и надграждане. Тези параметри управляват повторното синхронизиране на профилите и надграждането независимо един от друг. Тези параметри освен това управляват командите за повторно синхронизиране и надграждане на URL, които се издават през уеб сървъра за администриране. И двата параметъра се установяват на **Да** по подразбиране.

Параметърът Resync_From_SIP управлява заявките за операции за повторно синхронизиране. Събитието SIP NOTIFY се изпраща от прокси сървъра на доставчика на услуги към телефона. Ако е активиран, прокси сървърът може да изиска повторно синхронизиране. За да направи това прокси сървърът изпраща съобщение SIP NOTIFY, което съдържа събитието: повторно синхронизиране на заглавието към устройството

Устройството отговаря на заявката с отговор 401 (отказано удостоверяване за използвани данни за вход). Устройството очаква удостоверена последваща заявка преди да уважи заявката за повторно синхронизиране от прокси сървъра. Заглавията на събитието: reboot_now и събитието: restart_now изпълняват съответно студено и горещо рестартиране, които се подлагат на проверка.

Двете останали разрешения са Resync_On_Reset и Resync_After_Upgrade_Attempt. Тези параметри определят дали устройството изпълнява операция по повторно синхронизиране след включване, презареждане на софтуера и след всеки опит за надграждане.

При активиране на Resync_On_Reset устройството въвежда произволно закъснение, което следва последователността за зареждане преди изпълнение на заявката. Закъснението представлява произволно време до стойността, която е посочена в Resync_Random_Delay (в секунди). В набор от телефони, които се включват едновременно, това закъснение отделя времето на стартиране на заявките за повторно синхронизиране на всяко отделно устройство. Тази функция може да бъде полезна при големи разгръщания в жилищни сгради и в случаи на регионално спиране на захранването.

Превключватели

Телефонът позволява повторно синхронизиране на определени интервали или в посочено време.

Повторно синхронизиране на определени интервали

Телефонът е създаден за периодично повторно синхронизиране със сървър за обезпечаване. Интервалът за повторно синхронизиране се конфигурира в Resync_Periodic (секунди). Ако тази стойност остане празна, устройството не извършва периодично повторно синхронизиране.

Повторното синхронизиране обикновено се извършва, когато гласовите линии са свободни. Ако гласовата линия е активна, когато е насрочено повторно синхронизиране, телефонът забавя процедурата за повторно синхронизиране докато линията отново остане свободна. Повторното синхронизиране може да причини промени в стойностите на параметъра за конфигуриране.

Операцията за повторно синхронизира е неуспешна, тъй като телефонът не може да извлече профила от сървъра, изтегленият файл е повреден или е възникнала вътрешна грешка. Устройството прави опити за повторно синхронизиране след време, което е посочено в Resync_Error_Retry_Delay (секунди). Ако Resync_Error_Retry_Delay се установи на 0, устройството не прави отново опит за повторно синхронизиране след неуспешен опит за повторно синхронизиране.

Ако надграждането е неуспешно се прави повторен опит след посочените в Upgrade_Error_Retry_Delay секунди.

Достъпни са два подлежащи на конфигуриране параметъра за условно превключване на повторно синхронизиране: Resync_Trigger_1 и Resync_Trigger_2.: Всеки от параметрите може да се програмира с условен израз, който преминава макро разширение. Когато интервалът за повторно синхронизиране изтече (време за следващо повторно синхронизиране), параметрите за превключване, ако са зададени, ще предотвратят повторно синхронизиране, освен ако една или повече от тези стойности са установени на истина.

Условието в следващия пример включва повторно синхронизиране. В примера от последния опит за надграждане на телефона са изминали 5 минути (300 секунди) и поне 10 минути (600 секунди) са изминали от последния опит за повторно синхронизиране.

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

Повторно синхронизиране в определено време

Параметърът Resync_At позволява на телефона повторно синхронизиране на определено време. Този параметър използва 24-часов формат (ччмм), за да посочи времето.

Параметърът Resync_At_Random_Delay позволява на телефона да се синхронизира отново при непосочено закъснение във времето. Този параметър използва формат с положително цяло число, за да посочи времето.

Заливането на сървъра със заявки за повторно синхронизиране от много телефони, които са установени да се синхронизират повторно в едно и също време, трябва да бъде избягвано. За тази цел телефонът включва повторното синхронизиране до 10 минути след посоченото време.

Например ако зададете времето за повторно синхронизиране на 1000 (10 сутринта.), телефонът включва повторното синхронизиране в диапазона 10:00 сутринта до 10:10 сутринта.

Тази функция е деактивирана по подразбиране. Ако е обезпечен параметър Resync_At, параметърът Resync_Periodic се игнорира.

Подлежащи на конфигуриране графици

Можете да конфигурирате графици за периодично повторно синхронизиране и да посочите интервалите за повторен опит за повторно синхронизиране и неуспешните надграждания чрез използване на следните параметри за обезпечаване.

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Всеки параметър приема една стойност за закъснение (секунди). Новият разширен синтаксис позволява използване на разделени от запетая списъци на последователните елементи на закъснението. Последният елемент в последователността изрично се повтаря безкрайно.

Като опция можете да използвате знака плюс, за да посочите друга цифрова стойност, която се долепва до произволно допълнително закъснение.

Пример 1

В този пример телефонът се синхронизира повторно периодично на всеки 2 часа. При неуспех на повторното синхронизиране устройството прави повторен опит при следните интервали: 30 минути, 1 час, 2 часа, 4 часа. Устройството продължава да опитва на интервали от 4 часа докато повторното синхронизиране е успешно.

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

Пример 2

В този пример устройството се синхронизира повторно на всеки час (плюс допълнително произволно закъснение от до 10 минути). В случая на неуспешно повторно синхронизиране,

устройството прави повторни опити на следните интервали: 30 минути (плюс до 5 минути). 1 час (плюс до 10 минути), 2 час (плюс до 15 минути). Устройството продължава да опитва на интервали от 2 часа (плюс до 15 минути) до успешно повторно синхронизиране.

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

Пример 3

В този пример при неуспех на опита за дистанционно надграждане устройството прави повторен опит за надграждане след 30 минути, а след това отново след още един час, а след това - след два часа. Ако надграждането все още е неуспешно, устройството прави повторен опит всеки четири до пет часа до успешното надграждане.

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

Правила за профил

Телефонът осигурява множество параметри за дистанционния профил на конфигуриране (Profile_Rule*). Следователно, всяка операция за повторно синхронизиране може да извлече много файлове, които се управляват от различни сървъри.

В най-простите сценарии устройството се синхронизира повторно периодично за един профил на централния сървър, който актуализира съответните вътрешни параметри. Другият начин е профилът да бъде разделен между различни файлове. Един файл е общ за всички параметри в разгръщането. За всеки акаунт се осигурява отделен, уникален файл. Ключовете за шифроване и информация за сертификатите могат да бъдат подадени от друг профил, който се съхранява на отделен сървър.

Когато е необходима операция по повторно синхронизиране, телефонът оценява последователно четирите параметъра в правилото за профил*.

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

Всяка оценка може да доведе до извличане на профил от сървър за дистанционно обезпечаване с възможно актуализиране на известен брой вътрешни параметри. При неуспех на оценяването последователността за повторно синхронизиране се прекъсва и се прави повторен опит от начало, посочен от закъснението за повторен опит при грешка от повторно синхронизиране* (секунди). При успех на всички оценки, устройството изчаква броя секунди, посочени от параметъра Resync_Periodic, и изпълнява друго повторно синхронизиране.

Съдържанието на всеки от параметрите на правилото на профила се състои от набор от алтернативи. Алтернативите са разделени от знака | (права черта). Всяка алтернатива се състои от условен израз, израз за задаване, URL на профил и всички свързани с URL опции. Всички тези компоненти са опция във всяка от алтернативите. Следващите представляват валидни комбинации и редът, в който трябва да се показват, ако присъстват:

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

Във всеки параметър Profile_Rule* всички алтернативи, освен последната, трябва да имат условен израз. Този израз се оценява и се обработва както следва:

1. Условията се оценяват отляво надясно, докато се намери някое вярно (или докато се намери алтернатива без условен израз).
2. Оценяват се всички придружаващи изрази за назначаване, ако присъстват.
3. Ако е посочен URL като част от тази алтернатива, се прави опит за изтегляне на профила, който се намира на посочения URL. Системата прави опити съответно за надграждане на вътрешните параметри.

Ако всички алтернативи имат условни изрази и нито един не се оценява като верен (или ако цялото правило за профила е празно), се пропуска целия параметър Profile_Rule*. Оценява се следващия параметър за правило за профил в последователността.

Пример 1

Този пример извършва безусловно повторно синхронизиране на профила на посочения URL и извършва заявка за HTTP GET към сървъра за дистанционно обезпечаване.

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

Пример 2

В този пример устройството се синхронизира повторно с два различни URL в зависимост от състоянието на регистриране на Линия 1. В случай на изгубена регистрация, устройството изпълнява HTTP POST за CGI скрипт. Устройството изпраща съдържанието на макро разширения GPP_A, което може да осигури допълнителна информация относно състоянието му.

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

Пример 3

В този пример устройството се синхронизира отново със същия сървър. Устройството осигурява допълнителна информация, ако в модула няма инсталиран сертификат (за стари устройства преди версия 2.0):

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

Пример 4

В този пример Линия 1 е деактивирана докато GPP_A се установи на „Обезпечена“ от първия URL. След това се синхронизира отново с втория URL:

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

Пример 5

В този пример се приема, че профилът, който връща първия сървър, съдържа тагове на XML елемент. Тези тагове трябва да бъдат назначени отново с правилни имена на параметри от картата на псевдонимите, съхранена в GPP_B.

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

Повторното синхронизиране обикновено се счита за неуспешно, ако исканият профил не се получи от този сървър. Параметърът Resync_Fails_On_FNF може да препокрие това подразбиращо се поведение. Ако Resync_Fails_On_FNF се установи на „Не“, устройството приема отговор за ненамерен файл от сървъра като успешно повторно синхронизиране. Стойността по подразбиране за Resync_Fails_On_FNF е „Да“.

Правило за надграждане

Правилото за надграждане е да се укаже на устройството да активира ново зареждане и откъде да извлече зареждането, ако е необходимо. Ако зареждането е вече на устройството, то няма да направи опит да извлече зареждане. Така че валидността на местоположението за зареждане няма значение, когато желаното зареждане е в неактивен дял.

Upgrade_Rule посочва фърмуерното зареждане, което, ако се различава от текущото зареждане, ще бъде изтеглено и приложено, освен ако не бъде ограничено от условен израз или Upgrade_Enable е установена на **Не**.

Телефонът осигурява един подлежащ на конфигуриране параметър за дистанционно надграждане, Upgrade_Rule. Този параметър приема синтаксис, подобен на параметрите за правило на профила. За актуализации не се поддържат URL опции, но могат да се използват условни изрази и изрази за задаване. Ако се използват условни изрази, параметърът може да се популяризира по много начини, разделени от знака |. Синтаксисът за всяка от алтернативите е както следва:

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

Както в случая с параметрите за правило на профила*, параметърът Upgrade_Rule оценява всяка от алтернативите до удовлетворяване на условния израз или ако алтернативата няма условен израз. Ако е посочен, се оценява придружаващия израз за задаване. След това се прави надграждане на посочения URL.

Ако правилото за надграждане съдържа URL без условен израз, устройството надгражда до образа на фърмуера, посочен от URL. След макро израз и оценка на правилото, устройството не прави повторен опит за надграждане докато правилото се промени или се промени ефективната комбинация от схема + сървър + порт + път до файл.

За да направи опит за надграждане на фърмуера, устройството деактивира аудиото при стартиране на процедурата и го зарежда отново в нейния край. Устройството започва

автоматично надграждане, което се управлява от съдържанието на Upgrade_Rule, само ако всички гласови линии са неактивни.

Например

- За серията Cisco IP 6800:

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

where BN==Build Number
```

В този пример Upgrade_Rule надгражда фърмеура до образа, който се съхранява на посочения URL.

Ето още един пример за серията Cisco IP Phone 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
```

Този пример насочва модула за зарежда един от два образа въз основа на съдържанието на параметър с общо предназначение, GPP_F.

Устройството може да стартира принудително ограничение за обратно понижаване по отношение на номера на версията на фърмуера, което може да бъде полезна опция за персонализиране. Ако в параметъра Downgrade_Rev_Limit е конфигуриран валиден номер на фърумерната версия, устройството отказва опити за надграждане за фърмуерни версии, които са по-ниски от посоченото ограничение.

Типове данни

Тези типове данни се използват с параметри за конфигуриране на профила:

- {a,b,c,…}—Избор между a, b, c, …
- Bool—Булева стойност „да“ или „не“
- CadScript—Минискрипт, който посочва параметрите за каданс на сигнала. До 127 знака.

  Синтаксис: $S_1[;S_2]$, където:

  - $S_i=D_i$(вкл.$_{i,1}$/изкл.$_{i,1}$[,вкл.$_{i,2}$/изкл.$_{i,2}$[,вкл.$_{i,3}$/изкл$_{i,3}$[вкл.$_{i,4}$/изкл$_{i,4}$[,вкл.$_{i,5}$/изкл$_{i,5}$[,вкл.$_{i,6}$/изкл$_{i,6}$]]]]]) и е известно като секция.
  - вкл. $_{i,j}$ и изкл. $_{i,j}$ представляват продължителността на включване/изключване в секунди на сегвент. i = 1 или 2, и j = 1 до 6.
  - D_i е общата продължителност на секцията в секунди.

  Всички продължителности могат да имат три десетични места за осигуряване на резолюция от 1 ms. Знакът на символа "*" означава безкрайна продължителност. Сегментите в секцията се изпълняват по ред и се повтарят до постигане на цялата продължителност.

  Пример 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
```

Пример 2—Определен пръстен (short,short,short,long):

```
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—Синтаксис за скриптиране, който се използва за посочване на плановете за набиране на Линия 1 и Линия 2.
- Float<n>—Стойност на плаваща запетая с до десет десетични места.
- FQDN—Напълно квалифицирано име на домейн. Може да съдържа до 63 знака. Примерите са както следва:
  - sip.Cisco.com:5060 или 109.12.14.12:12345
  - sip.Cisco.com или 109.12.14.12
- FreqScript—Минискрипт, който посочва параметрите за честота и ниво на тона. Съдържа до 127 знака.

  Синтаксис: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, където:
  - F_1–F_6 са честотите в Hz (само цели числа без знак).
  - L_1–L_6 са съответните нива в dBm (с до едно десетично място).

  Интервалите преди и след запетаята са позволени, но не се препоръчват.

  Пример 1—Тон за изчакване на повикване:

```
440@-10

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

  Пример 2—Тон за набиране:

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

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

- IP— Валиден IPv4 адрес във формат x.x.x.x, където x е между 0 и 255. Пример: 10.1.2.100.
- UserID—Потребителския ИД, както се показва на URL: до 63 знака.
- Phone—Низ за телефонен номер, като 14081234567, *69, *72, 345678; или генеричен URL, като 1234@10.10.10.100:5068 или jsmith@Cisco.com. Низът може да съдържа до 39 знака.
- PhTmplt—Шаблон за телефонен номер. Всеки шаблон може да съдржа един или повече модела, разделени от запетая (,). Интервалите в началото на всеки от моделите се игнорират. “?” и “*” представляват знаци на символи. За да представите литерал, използвайте %xx. Например %2a представя *. Шаблонът може да съдържа до 39 знака. Примери: „1408*, 1510*“, „1408123????, 555?1.“.
- Port—Номер на порт за TCP/UDP (0-65535). Може да бъде в десетичен или шестнадесетичен формат.
- ProvisioningRuleSyntax—Синтаксис за скриптиране, който се използва за дефиниране на повторно синхронизиране на конфигурацията и правила за надграждане на фърмуера.
- PwrLevel—Ниво на мощност, изразено в dBm с едно десетично място, като –13,5 или 1,5 (dBm).
- RscTmplt – Шаблон за код на състоянието в SIP отговорите, като „404, 5*“, „61?“, „407, 408, 487, 481“. Може да съдържа до 39 знака.
- Sig<n>—Записана стойност в n-бита. Може да бъде в десетичен или шестнадесетичен формат. Знакът “-” трябва да предшества отрицателните стойности. Знакът „+“ пред положителните стойности е опция.
- Кодове със звезда—Код за активиране на допълнителна услуга, като *69. Кодът може да съдържа до 7 знака.
- Str<n>—Генеричен низ с до n нерезервирани знака.
- Time<n>—Времева продължителност в секунди с до n десетични места. Допълнително посочените десетични места се пренебрегват.
- ToneScript—Минискрипт, който посочва параметрите за честота, ниво и каданс на тона за ход на повикване. Скриптът може да съдържа до 127 знака.

  Syntax: FreqScript;Z_1[;Z_2].

  Раздел Z_1 е подобен на раздел S_1 в CadScript, с изключение на това, че всеки сегмент за вкл./изкл. се следва от параметър за компоненти на честота: Z_1 = D_1(вкл.$_{i,1}$/изкл.$_{i,1}$/$f_{i,1}$[,вкл.$_{i,2}$/изкл.$_{i,2}$/$f_{i,2}$ [,вкл.$_{i,3}$/изкл.$_{i,3}$/$f_{i,3}$ [,вкл.$_{i,4}$/изкл.$_{i,4}$/$f_{i,4}$ [,вкл.$_{i,5}$/изкл.$_{i,5}$/$f_{i,5}$ [,вкл.$_{i,6}$/изкл.$_{i,6}$/$f_{i,6}$]]]]]) където:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ посочва компонентите за честота във FreqScript, които се използват в този сегмент.

Ако в даден сегмент се използва повече от един компонент за честота, компонентите се сумират.

Пример 1—Тон за набиране:

```
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
```

Пример 2—Прекъсващ сигнал:

```
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>—Незаписана n-битова стойност, където n = 8, 16 или 32. Може да се посочи в десетичен или шестнадесетичен формат, като 12 или 0x18, ако стойността може да бъде записана в n бита.

Забележка Имайте това предвид.

- <Par Name> представя името на параметъра на конфгурацията. В профила съответният таг се формира чрез замяна на интервал с долна черта "_", като **Par_Name**.
- Празното поле на стойност по подразбиране показва празен низ < "" >.
- Телефонът продължава да използва последните конфигурирани стойности за тагове, които са представени в дадения профил.
- Шаблоните се сравняват по реда на представянето им. Избира се първото, не най-близко съвпадение. Името на параметъра трябва да съвпада точно.
- Ако е дадена повече от една дефиниция на профил, последната дефиниция във файла е тази, която се прилага към телефона.
- Спецификация на параметър с празна параметрична стойност привежда параметъра обратно към стойността по подразбиране. За да посочите празен низ вместо това, използвайте празен низ "", като стойност на параметър.

Актуализиране на профили и надграждане на фърмуер

Телефонът поддържа защитено дистанционно обезпечаване (конфигуриране) и надграждане на фърмуера. Необезпеченият телефон може да получава шифрован профил, предназначен за това устройство. Телефонът не изисква изричен ключ поради защитения механизъм на първоначално обезпечаване, който използва SSL функции.

Не се изисква намеса на потребителя за стартиране или завършване на актуализирането на профила или надграждане на фърмуера или ако се изисква междинно надграждане за достигане на бъдещо състояние на надграждане от по-стара версия. Прави се опит за повторно синхронизиране на профила, когато телефонът е свободен, тъй като повторното синхронизиране може да стартира повторно зареждане на софтуера и да изключи повикване.

Параметрите с общо предназначение управляват процеса на обезпечаване. Всеки телефон може да се конфигурира периодично да се свързва с обикновен сървър за обезпечаване (NPS). Комуникацията с NPS не изисква използване на защитен протокол, тъй като актуализираният профил е шифрован от споделен секретен ключ. NPS може да бъде стандартен TFTP, HTTP или HTTPS сървър със сертификати за клиент.

Администраторът може да надгради, зареди повторно, рестартира или синхронизира повторно телефоните, като използва потребителския уеб интерфейс на телефона. Администраторът също може да извършва тези задания като използва съобщение за уведомяване SIP.

Профилите за конфигуриране се генерират чрез използване на обикновени инструменти с отворен код, които се интегрират със системите за обезпечаване на доставчика на услуги.

Сродни теми

Разрешаване и конфигуриране на актуализации на профил, на стр.37

Разрешаване и конфигуриране на актуализации на профил

Актуализации на профила могат да се разрешават на определени интервали. Актуализираните профили се изпращат от сървъра към телефона при използване на TFTP, HTTP или HTTPS.

Преди да започнете

Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Процедура

Стъпка 1 Изберете **Глас** > **Обезпечаване**.

Стъпка 2 В раздела **Профил на конфигурацията** изберете **Да** от полето на падащия списък **Активиране на обезпечаване**.

Стъпка 3 Въведете параметрите.

Стъпка 4 Кликнете върху **Изпращане на всички промени**.

Сродни теми

Актуализиране на профили и надграждане на фърмуер, на стр.37

Разрешаване и конфигуриране на надграждания на фърмуер

Актуализациите на фърмуера могат да бъдат разрешени на посочените интервали. Актуализираният фърмуер се изпраща от сървъра към телефона при използване на TFTP или HTTP. При надграждането на фърмуера защитата не е проблем, тъй като фърмуърът не съдържа лична информация.

Преди да започнете

Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Процедура

Стъпка 1 Изберете **Глас** > **Обезпечаване**.

Стъпка 2 В раздела **Надграждане на фърмуера** изберете **Да** от падащия списък **Активиране на надграждане**.

Стъпка 3 Въведете параметрите.

Стъпка 4 Кликнете върху **Изпращане на всички промени**.

Надграждане на фърмуер чрез TFTP, HTTP или HTTPS

Телефонът поддържа еднократно надграждане с един образ по TFTP, HTTP или HTTPS.

Забележка Понижаванията до по-ранни версии е възможно да не са достъпни за всички устройства. За повече информация вижте забележките за версията на вашия телефон и версията на фърмуера.

Преди да започнете

Файлът за зареждане на фърмуера трябва да се изтегли на достъпен сървър.

Процедура

Стъпка 1 Преименувайте образа както следва:

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

където:

x8xx е серията на телефона, като 6841.

aa-b-c е номера на версията, като 10-4-1

Стъпка 2 Използвайте командата **tar -xzvf** за отмяна на tar на tar ball.

Стъпка 3 Копирайте папката в директория за изтегляне TFTP, HTTP или HTTPS.

Стъпка 4 Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Стъпка 5 Изберете **Глас** > **Обезпечаване**.

Стъпка 6 Намерете името на файла за зареждане, което завършва на **.loads** и го долепете до валиден URL.

Стъпка 7 Кликнете върху **Изпращане на всички промени**.

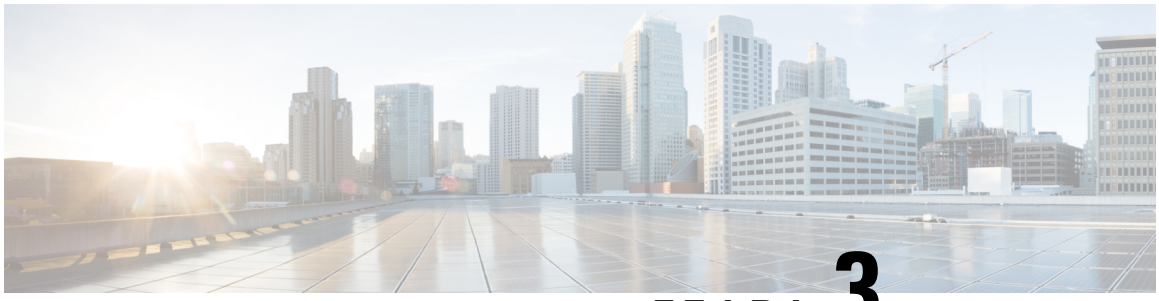
Надграждане на фърмуера с команда на браузъра

Въведената в адресното поле на браузъра команда за надграждане може да се използва за надграждане на фърмуера на телефона. Телефонът се актуализира само когато е свободен. Надграждането се предприема автоматично след завършване на повикването.

Процедура

За да се надгради телефона с URL в уеб браузър, въведете следната команда:

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



ГЛАВА 3

Обезпечаване на място и сървъри за обезпечаване

Обезпечаване на място и сървъри за обезпечаване

Предварително обезпечени с профил от доставчика на услуги телефони, които се различават от RC модули. Профилът за предварително обезпечаване може да се състои от ограничен набор от параметри, които извършват повторно синхронизиране на телефона. Профилът може освен това да се състои от пълен набор параметри, подавани от дистанционния сървър. По подразбиране телефонът се синхронизира отново при включване на захранването и на определени интервали, конфигурирани в профила. Когато потребителят свърже телефона на обекта на клиента, устройството изтегля актуализирания профил и всички актуализации на фърмуера.

Този процес на разгръщане с предварително обезпечаване и дистанционно обезпечаване може да бъде извършен по много начини.

Подготовка на сървъра и софтуерни инструменти

Примерът в тази глава изисква наличие на един или повече сървъра. Тези сървъри могат да бъдат инсталирани и да работят на местен компютър:

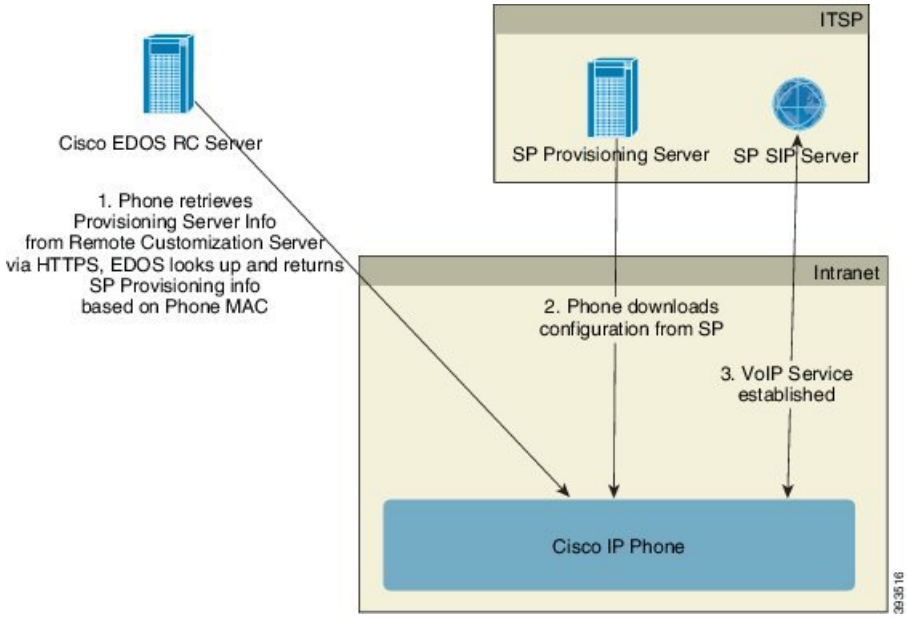
- TFTP (UDP порт 69)
- syslog (UDP порт 514)
- HTTP (TCP порт 80)
- HTTPS (TCP порт 443).

За отстраняване на неизправности в конфигурацията на сървъра е полезно да се инсталират клиенти за всеки от типовете сървъри на отделна машина за сървър. Тази практика гарантира правилна работа на сървъра, независима от взаимодействието с телефоните.

Освен това препоръчваме да инсталирате следните софтуерни инструменти:

- За да генерирате профили на конфигурацията, инсталирайте помощната програма за компресиране с отворен код gzip.
- За шифроване на профила и операциите на HTTPS инсталирайте софтуерния пакет с отворен код OpenSSL.
- За да тествате в динамика работата на профила и едностъпково дистанционно обезпечаване при използване на HTTPS, препоръчваме език за скриптиране с поддръжка за CGI скриптиране. Езиковият инструмент с отворен код Perl е пример на подобен език за скриптиране.
- За да проверите защитения обмен между сървърите за обезпечаване и телефоните, инсталирайте анализатор в Ethernet пакет (например свободно достъпния за изтегляне Ethereal/Wireshark). Прихванете трасировката на Ethernet пакета от взаимодействието между телефона и сървъра за обезпечаване. За да направите това, изпълнете пакетния анализатор на компютър, който е свързан към превключвател с активирано огледално изобразяване на портове. За HTTPS транзакции можете да използвате помощната програма ssldump.

Разпределение на дистанционното персонализиране (RC)



Всички телефони се свързват със сървър Cisco EDOS RC до първоначалното си обезпечаване.

При модела за RC разпределение клиентът закупува телефон, който вече е свързан с определен доставчик на услуги на сървъра Cisco EDOS RC. Доставчикът на услуги за интернет телефония

(ITSP) задава и поддържа сървър за обезпечаване и регистрира информацията от сървъра за обезпечаване в сървър Cisco EDOS RC.

Когато телефонът се включи в интернет връзка, състоянието на персонализиране за необезпечения телефон е **Отворен**. Телефонът първо прави запитване към местния DHCP сървър за информация относно сървъра за обезпечаване и задава състоянието на персонализация на телефона. Ако DHCP заявката е успешна, състоянието на персонализиране се установява на **Прекъснат** и няма обръщение към RC поради това, че DHCP осигурява необходимата информация за сървъра за обезпечаване.

Когато даден телефон се свърже към мрежата за първи път или след възстановяване на фабричните настройки, ако има не са настроени DHCP опции, той се свързва със сървър за активиране на устройства с цел автоматично обезпечаване. Новите телефони ще използват за обезпечаване "activate.cisco.com" вместо "webapps.cisco.com". Телефоните с версия на фърмуера под 11.2(1) ще продължат да използват webapps.cisco.com. Cisco препоръчва да позволите достъп и до двата домейна през защитната стена.

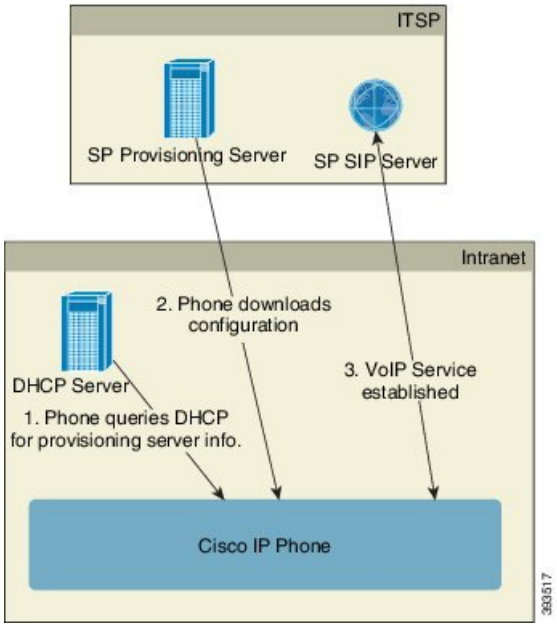
Ако DHCP сървърът не осигури информация за сървъра за обезпечаване, телефонът прави запитване към сървъра Cisco EDOS RC и осигурява неговия MAC адрес и модел, а състоянието на персонализиране се установява на **Изчакване**. Сървърът Cisco EDOS отговаря с информация за сървъра за обезпечаване на асоциирания доставчик на услуги, включително URL на сървъра за обезпечаване, а състоянието на персонализиране на телефона се установява на **Потребителско изчакване**. След това телефонът изпълнява команда за повторно синхронизиране с URL за извличане на конфигурацията на доставчика на услуги. При успех състоянието на персонализиране се установява на **Придобит**.

Ако сървърът Cisco EDOS RC няма асоцииран с телефона доставчик на услуги, състоянието на персонализиране на телефона се установява на **Недостъпен**. Телефонът може да се конфигурира ръчно или да се добави асоциация за доставчик на услуги на телефона на сървъра Cisco EDOS.

Ако телефонът е обезпечен чрез LDC или помощна програма за уеб конфигуриране преди състоянието на персонализиране да стане **Придобит**, то се установява на **Прекъснат** и сървърът Cisco EDOS няма да получава заявки, освен ако телефонът не се нулира до фабричните настройки.

След като телефонът бъде обезпечен, сървърът Cisco EDOS RC не се използва, освен ако телефонът не се нулира до фабричните настройки.

Устройство за обезпечаване на място



Със подразбиращата се фабрична конфигурация на Cisco телефонът автоматично прави опити да извърши повторно синхронизиране с профил на сървър TFTP. Управляваният DHCP сървър на LAN подава информацията относно профила и TFTP сървъра, която е конфигурирана за обезпечаване на устройството. Доставчикът на услуги свързва всеки нов профил с LAN. Телефонът се синхронизира повторно автоматично с местния TFTP сървър и инициализира вътрешното си състояние в подготовка на разгръщането. Този профил за обезпечаване обикновено включва URL на дистанционния сървър за обезпечаване. Сървърът за обезпечаване поддържа устройството актуализирано след разгръщането му и свързването към мрежата на клиента.

Баркодът на предварително обезпеченото устройство може да се сканира, за да запише неговия MAC адрес или сериен номер, преди телефонът да се достави на клиента. Тази информация може да се използва за създаване на профил, към който да се синхронизира повторно телефона.

При получаване на телефона клиентът го свързва към широколентовата връзка. При включване телефонът осъществява контакт със сървъра за обезпечаване през URL, който е конфигуриран чрез обезпечаване. При това телефонът се синхронизира повторно и актуализира профила и фърмуера, ако е необходимо.

Сродни теми

Разпространение на дребно, на стр.5
Обезпечаване на TFTP, на стр.45

Първоначална настройка на сървъра за обезпечаване

Този раздел описва изискванията за първоначална настройка за обезпечаване на телефон при използване на различни сървъри и различни сценарии. За целите на този документи и на тестването се инсталират сървъри за обезпечаване и се изпълняват на местен компютър. Освен това общодостъпните софтуерни инструменти също са полезни за обезпечаване на телефони.

Обезпечаване на TFTP

Телефоните поддържат TFTP за операции по обезпечаване при повторно синхронизиране и надграждане на фърмуера. При дистанционно разгръщане на устройството се препоръчва използване на HTTPS, но също могат да се използват HTTPS и TFTP. При това се изисква шифроване на файла за обезпечаване за добавяне на защита, тъй като този начин предлага по-голяма надеждност, механизми за NAT и защита на маршрутизатора. TFTP е полезен при обезпечаване на място на голям брой необезпечени устройства.

Телефонът може да получи IP адрес на TFTP сървър директно от DHCP сървър чрез опция 66 на DHCP. Ако правилото на профила е конфигурирано с път на файл на TFTP сървър, устройството изтегля неговия профил от TFTP сървъра. Изтеглянето се извършва, когато устройството се свърже към LAN и се захрани.

Profile_Rule с фабричната конфигурация по подразбиране е *&PN*.cfg, където *&PN* представлява името на модела на телефона.

Например за CP-6841-3PCC, името на файла е CP-6841-3PCC.cfg.

За устройство с фабричен профил по подразбиране, при включване устройството се синхронизира повторно с този файл на местен TFTP сървър, който се посочва от DHCP опцията 66. Пътят на файла е по отношение на виртуалната корнева директория до TFTP сървъра.

Сродни теми

Устройство за обезпечаване на място, на стр.44

Дистанционно управление на крайна точка и NAT

Телефонът е съвместим с превод на мрежов адрес (NAT) за достъп до интернет през маршрутизатор. За подобряване на защитата маршрутизаторът може да направи опит да блокира неупълномощените постъпващи пакети чрез прилагане на симетричен NAT, стратегия за филтриране на пакети, която значително ограничава пакетите, които са позволени за влизане от интернет в защитената мрежа. Поради тази причина не се препоръчва дистанционно обезпечаване при използване на TFTP.

VoIP може да съществува съвместно с NAT само при осигуряване на някои форми на ограничаване на NAT. Конфигурирайте просто ограничаване на UDP през NAT (STUN). Тази опция изисква потребителят да има:

- Динамичен външен (общодостъпен) IP адрес от вашата услуга
- Компютър, който работи със софтуер за сървър STUN

- Крайно устройство с асиметричен механизъм на NAT

Обезпечаване на HTTP

Телефонът се държи като браузър, който заявява уеб страници от дистанционен интернет сайт. Това осигурява надеждни средства за достигане на сървъра за позициониране, дори когато маршрутизаторът на клиента прилага симетричен NAT или други защитни механизми. HTTP и HTTPS работят по-надеждно от TFTP при дистанционно разгръщане, особено когато разгърнатите модули се свързват зад защитни стени или маршрутизатори с възможност за NAT. HTTP и HTTPs се използват взаимозаменяемо в описанията на следните типове заявки.

Основното обезпечаване, основаващо се на HTTP, разчита на метода HTTP GET за извличане на конфигурационни профили. За всеки разгърнат телефон обикновено се създава конфигурационен файл и тези файлове се съхраняват в директорията на HTTP сървър. Когато сървърът получи заявка GET, просто връща файла, който е посочен в заглавието на заявката GET.

Вместо статично, конфигурационният профил може да се генерира динамично чрез запитване в базата с данни на клиента и създаване на профил в движение.

Когато телефонът заяви повторно синхронизиране, може да използва метода HTTP POST, за да заяви данни за повторно конфигуриране при повторно синхронизиране. Устройството може да се конфигурира да предава определено състояние и идентификационна информация към сървъра в тялото на заявката за HTTP POST. Сървърът използва тази информация за генериране на желания конфигурационен профил за отговор или да съхрани информацията за състоянието за по-късен анализ и проследяване.

Като част от заявките GET и POST, телефонът автоматично включва основна идентификационна информация в полето User-Agent на заглавието на заявката. Тази информация предава име на производителя, име на продукта, текуща версия на фърмуера и сериен номер на продукта на устройството.

Следващият пример е полето за заявка User-Agentот CP-6841-3PCC:

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

Когато телефонът се конфигурира за повторно синхронизиране към конфигурационен профил при използване на HTTP, се препоръчва да се използва HTTPS или профилът да бъде шифрован, за да се защити поверителността на информацията. Шифрованите профили, които изтегля телефона при използване на HTTP, избягват опасността от излагане на поверителната информация, която се съдържа в профила за конфигуриране. Този режим на повторно синхронизира създава по-ниско изчислително натоварване в сървъра за позициониране при използване на HTTPS.

Телефонът може да дешифрира профили, шифровани с един от следните методи на шифроване:

- AES-256-CBC шифроване
- RFC-8188 базирано ширование с AES-128-GCM шифър

Забележка Телефонът поддържа HTTP версия 1.0, HTTP версия 1.1, и Chunk кодиране, когато HTTP версия 1.1 е договорения транспортен протокол.

Работа с код за състояние на HTTP при повторно синхронизиране и надграждане

Телефонът поддържа HTTP отговор за дистанционно обезпечаване (Повторно синхронизиране). Настоящото поведение на телефона се категоризира по три начина:

- A—Успех, при което стойностите на „Периодично повторно синхронизиране“ и „Закъснение при произволно повторно синхронизиране“ определят последващите заявки.
- B—Неуспех, когато файлът не е намерен или профилът е повреден. Стойността „Закъснение при повторен опит при грешка при повторно синхронизиране“ определя последващите заявки.
- C—Други неизправности, когато лош URL или IP причинява грешки при свързване. Стойността „Закъснение при повторен опит при грешка при повторно синхронизиране“ определя последващите заявки.

Таблица *2:* Поведение на телефона при *HTTP* отговори

Код за състояние на HTTP	Описание	Поведение на телефона
301 Moved Permanently	Тази и бъдещите заявки трябва да се насочват към ново местоположение.	Незабавна заявка за повторен опит с ново местоположение.
302 Found	Известна като временно преместен.	Незабавна заявка за повторен опит с ново местоположение.
3xx	Останалите отговори 3xx не се обработват.	C
400 Bad Request	Заявката не може да се изпълни поради лош синтаксис.	C
401 Unauthorized	Трудност при основно или съставно удостоверяване за достъп.	Незабавен повторен опит на заявката с данни за вход за удостоверяване. Максимум 2 повторни опита. При неуспех поведението на телефона е C.
403 Forbidden	Сървърът отказва да отговори.	C
404 Not Found	Заявеният ресурс не е намерен. Разрешени са последващи заявки от клиента.	B

Код за състояние на HTTP	Описание	Поведение на телефона
407 Proxy Authentication Required	Трудност при основно или съставно удостоверяване за достъп.	Незабавен повторен опит на заявката с данни за вход за удостоверяване. Максимум два повторни опита. При неуспех поведението на телефона е C.
4xx	Кодовете за състояние на грешка за другия клиент не се обработват.	C
500 Internal Server Error	Генерично съобщение за грешка.	Поведението на телефона е C.
501 Not Implemented	Сървърът не разпознава метода за заявка или липсва възможност за изпълнение на заявката.	Поведението на телефона е C.
502 Bad Gateway	Сървърът работи кат шлюз или прокси сървъра получава невалиден отговор от следващия сървър.	Поведението на телефона е C.
503 Service Unavailable	В момента сървърът е недостъпен (претоварен или спрян за поддръжка). Това е временно състояние.	Поведението на телефона е C.
504 Gateway Timeout	Сървърът се държи като шлюз или прокси и не получава навременен отговор от следващия сървър.	C
5xx	Друга грешка на сървъра	C

Обезпечаване на HTTPS

Телефонът поддържа HTTPS за обезпечаване за увеличена защита при управление на дистанционно разгърнати модули. Всеки телефон носи уникален SLL сертификат за клиент (и свързан с него частен ключ) в допълнение към сертификата за корневи сървър Sipura CA. Последният позволява на телефона да разпознава упълномощени сървъри за обезпечаване и да отказва неупълномощените. От друга страна сетификатът на клиента позволява на сървъра за обезпечаване да разпознава отделните устройства, които издават заявката.

За да може доставчикът на услуги да управлява разгръщането при използване на HTTPS, е необходимо да се генерира сертификат на сървър за всеки от сървърите за обезпечаване, към който телефонът се синхронизира повторно при използване на HTTPS. Сертификатът на сървъра трябва да бъде подписан корневи ключ за CA сървър на Cisco, чийто сертификат се носи от всички модули в разгръщането. За да получите подписан сертификат за сървър, доставчикът на услуги трябва да препрати заявката за подписване на сертификата към Cisco, който го подписва и връща сертификата на сървъра за инсталиране на сървъра за обезпечаване.

Сертификатът на сървъра за обезпечаване трябва да съдържа поле за общо име (CN) и FQDN на хоста, на който работи сървъра в темата Като опция може да съдържа информация, която следва FQDN на хоста, разделена от знака наклонена черта (/). Следват примери на CN въвеждания, които се приемат за валидни от телефона:

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

В допълнение към потвърждаването на сертификата на сървъра, телефонът тества IP адреса на сървъра спрямо DNS търсене на името на сървъра, посочено от сертификата на сървъра.

Получаване на подписан сертификат на сървър

Помощната програма OpenSSL може да генерира заявки за подписване на сертификат. Следващият пример показва командата **openssl**, която създава двойка от публичен/частен ключ 1024-бита RSA и заявка за подписване на сертификат:

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

Тази команда генерира частен ключ за сървъра в **privkey.pem** и съответстваща заявка за подписване на сертификат в **provserver.csr**. Доставчикът на услуги запазва секретния **privkey.pem** и подава **provserver.csr** към Cisco за подписване. При получаване на файла **provserver.csr** Cisco генерира **provserver.crt**, подписаният сертификат за сървър.

Процедура

Стъпка 1 Придвижете се до https://software.cisco.com/software/edos/home и влезте със своите данни за CCO.

Забележка Когато телефонът се свърже с мрежата за първи път или след нулиране до фабричните настройки и няма настроена опция за DHCP, той се свързва към сървъра за активиране на устройството за обезпечаване с нулево докосване. Новите телефони използват за обезпечаване “activate.cisco.com” вместо “webapps.cisco.com”. Телефоните с версия на фърмуера, по-ранна о 11.2(1) продължават да използват “webapps.cisco.com”. Препоръчваме да позволите и двете имена на домейни през защитната стена.

Стъпка 2 Изберете **Управление на сертификат**.

В раздела **Подписване на CSR** се зарежда CSR от предишната стъпка за подписване.

Стъпка 3 От падащия списък **Избор на продукт** изберете **SPA1xx фърмуер 1.3.3 и нов/SPA232D фърмуер 1.3.3 и нов/SPA5xx фърмуер 7.5.6 и нов/CP-78xx-3PCC/CP-88xx-3PCC**.

Забележка Продуктът включва многоплатформените телефони от серия Cisco IP Phone 6800

Стъпка 4 В полето **CSR файл** щракнете върху **Търсене** и изберете CSR за подписване.

Стъпка 5 Изберете метод на шифроване:

- MD5
- SHA1

- SHA256

Cisco препоръчва да изберете шифроването SHA256.

Стъпка 6 От падащия списък **Продължителност на подписване** изберете приложимата продължителност (например 1 година).

Стъпка 7 Щракнете върху **Заявка за подписване на сертификат**.

Стъпка 8 Изберете една от следните опции, за да получите подписания сертификат:

- **Въведете имейл адреса на получателя** – Ако искате да получите сертификата по имейл, въведете имейл адреса си в това поле.
- **Изтегляне** – Ако искате да изтеглите подписания сертификат, изберете тази опция.

Стъпка 9 Щракнете върху **Подаване**.

Подписаният сертификат на сървъра се изтегля или се изпраща по имейл до посочения имейл адрес.

Корневи сертификат на клиент за многоплатформен телефон CA

Cisco освен това предлага корневи сертификат за клиент на многоплатформен телефон на доставчика на услуги. Този корневи сертификат сертифицира удостоверяването на сертификата за клиент, който носи всеки от телефоните. Многоплатформените телефони освен това поддържат подписани от трети страни сертификати, като предлаганите от Verisign, Cybertrust и др.

Уникалният сертификат за клиент, който се предлага от всяко устройство по време на HTTPS сесия, носи идентификационна информация, вградена в неговото поле за тема. Тази информация може да се направи достъпна чрез HTTPS сървър към CGI скрипт, извикан да обработи защитените заявки. В частност темата на сертификата посочва името на продукта на модула (OU елемент), MAC адреса (S елемент) и серийния номер (L елемент).

Следващият пример от полето за тема на сертификата за клиент на многоплатформени телефони Cisco IP Phone 6841 показва тези елементи:

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

За да определите дали телефонът има индивидуализиран сертификат, използвайте макро променливата за обезпечаване $CCERT. Стойността на променливата се разширява до „инсталиран“ или „неинсталиран“ в съответствие с наличието или отсъствието на уникален сертификат на клиент. В случай на генеричен сертификат е възможно да получите серийния номер на модула от заглавието на заявката към HTTP в полето User-Agent.

HTTPS сървърите могат да бъдат конфигурирани да заявяват SSL сертификати от свързващите се клиенти. При активиране сървърът може да използва корневи сертификат за клиент на многоплатформен телефон, предлаган от Cisco, за да потвърди сертификата на клиента. При това сървърът може да осигури информация за сертификат към GGI за по-нататъшно обработване.

Местоположението за съхранение на сертификата може да варира. Например при Apache инсталация пътят до файловете на подписан сертификат на сървър за обезпечаване,

свързаният с него частен ключ и корневият сертификат на клиента на многоплатформения телефон CA, са както следва:

```
# 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
```

За конкретна информация вижте документацията на HTTPS сървъра.

Органът за корневи сертификати на клиент на Cisco подписва всеки отделен сертификат. Съответният корневи сертификат става достъпен за доставчиците на услуги с цел удостоверяване на клиент.

Допълнителни сървъри за обезпечаване

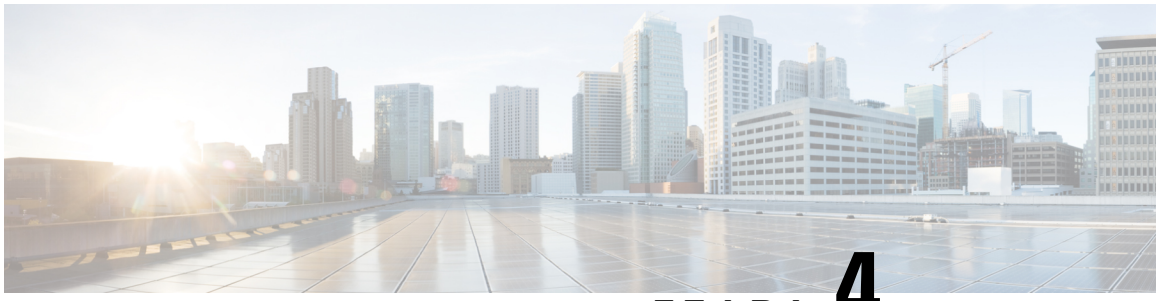
Сървърът за обезпечаване може да се посочи като IP адрес или като напълно квалифицирано име на домейн (FQDN). Използването на FQDN подпомага разгръщането на допълнителни сървъри за обезпечаване. При идентифициране на сървъра за обезпечаване чрез FQDN, телефонът прави опити да разреши FQDN като IP адрес чрез DNS. Поддържат се само записи DNS A за обезпечаване: Разрешаването на адреси DNS_SRV не е достъпно за обезпечаване. Телефонът продължава да обработва а записите докато сървърът отговори. Ако не отговори сървър, който е свързан с А записи, телефонът записва грешка на сървъра syslog.

Сървър Syslog

Ако на телефона е конфигуриран syslog сървър чрез използване на параметрите <Syslog Server>, операциите за повторно синхронизиране и надграждане изпращат съобщение до сървъра syslog. Съобщението може да се генерира в началото на заявката за дистанционен файл (конфигурационен профил или фърмурно зареждане) и в заключението на операцията (включително успех или неуспех).

Заредените съобщения се конфигурират в следните параметри и макроразширяват в реалните съобщения на syslog:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



ГЛАВА 4

Примери за обезпечаване

Преглед на примерите за обезпечаване

Тази глава осигурява примерни процедури за прехвърляне на конфигурационни профили между телефона и сървъра за обезпечаване.

За информация относно създаването на конфигурационни профили вижте Обезпечаващи скриптове, на стр.13.

Основно повторно синхронизиране

Този раздел показва функциите за основно повторно синхронизиране на телефона.

Повторно синхронизиране с TFTP

Телефонът поддържа много мрежови протоколи за извличане на профили за конфигуриране. най-основният протокол за прехвърляне на профили е TFTP RFC1350). TFTP се използва широко за обезпечаване на мрежови устройства в частни LAN мрежи. Въпреки че не се препоръчва за разгръщане на дистанционни крайни точки в интернет, TFTP може да бъде удобен за разгръщане в малки организации, за домашно обезпечаване и за разработване и тестване. Вижте Устройство за обезпечаване на място, на стр.44 за повече информация относно домашното обезпечаване. В следната процедура профилът се променя след изтегляне на файл от TFTP сървър.

Процедура

Стъпка 1 В LAN среда свържете компютър и телефон към концентратор, суич или малък маршрутизатор.

Стъпка 2 На компютъра инсталирайте и активирайте TFTP сървър.

Стъпка 3 Използвайте текстов редактор за създаване на профил за конфигуриране, който установява стойността за GPP_A на 12345678, както е показано в примера.

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

Стъпка 4 Запишете профила с името `basic.txt` в корневата директория на FTP сървъра.

Можете да посочите дали TFTP сървъра е правилно конфигуриран: заявете файла `basic.txt` като използвате TFTP клиент, който се различава от телефона. За предпочитане използвайте TFTP клиент, който работи на отделен хост от сървъра за обезпечаване.

Стъпка 5 Отворете уеб браузъра на компютъра на страницата за конфигуриране на администриране/разширени. Например, ако IP адресът на телефона е 192.168.1.100:

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

Стъпка 6 Изберете раздела **Гласови** > **Обезпечаване** и проверете стойността на параметрите за общо предназначение GPP_A до GPP_P Те трябва да бъдат празни.

Стъпка 7 Синхронизирайте отново телефона с профила за конфигуриране `basic.txt` , като отворите URL за повторно синхронизиране в прозореца на уеб браузър.

Ако IP адресът на TFTP сървъра е 192.168.1.200, командата трябва да бъде подобна на следния пример:

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

Когато телефонът получи команда, устройството на адрес 192.168.1.100 заявява файла `basic.txt` от TFTP сървъра на IP адрес 192.168.1.200. При това телефонът извършва синтактичен анализ на изтегления файл и актуализира параметъра GPP_A със стойността 12345678.

Стъпка 8 Проверете дали параметърът е правилно актуализиран: Опреснете страницата за конфигуриране на уеб браузъра на компютъра и изберете раздела **Гласови** > **Обезпечаване**.

Параметърът GPP_A сега трябва да съдържа стойност 12345678.

Използване на Syslog за регистриране на съобщения

Телефонът изпраща съобщение syslog към съответния сървър syslog, когато устройството се готви да се синхронизира отново със сървъра за обезпечаване и след завършване или неуспех на повторното синхронизиране. За да разпознаете този сървър, можете да отидете на уеб страницата за администриране на телефона (вижте Достъп до уеб страницата на телефона, на стр.8), да изберете **Гласови** > **Система** и да посочите сървъра в параметъра **Syslog сървър** на раздела **Мрежова конфигурация-опция**. Конфигурирайте IP адреса на сървъра

syslog в устройството и наблюдавайте съобщението, което се генерира по време на останалите процедури.

Процедура

Стъпка 1 Инсталиране и активиране на сървър syslog на местен компютър.

Стъпка 2 Програмирайте IP адреса на компютъра в параметъра Syslog_Server на профила и подайте промяната:

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

Стъпка 3 Щракнете върху раздела **Система** и въведете стойността на местния сървър syslog в параметъра Syslog_Server.

Стъпка 4 Повторете операцията за повторно синхронизиране, както е описано в Повторно синхронизиране с TFTP, на стр.53.

Устройството генерира две съобщения syslog по време на повторното синхронизиране. Първото съобщение показва, че има заявка в ход. Второто съобщение обозначава успех или неуспех на повторното синхронизиране.

Стъпка 5 Проверете дали сървърът syslog получава съобщение, подобно на следното:

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

Подробни съобщения могат да се програмират с параметъра Debug_Server (вместо с параметъра Syslog_Server) с IP адреса на сървъра syslog и задаване на Debug_Level със стойност между 0 и 3 (3 е най-подробното ниво):

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

Съдържанието на тези съобщения може да се конфигурира чрез използване на следните параметри:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Ако някой от тези параметър се изтрие, не се генерира съответното съобщение на syslog.

Автоматично повторно синхронизиране на устройството

Устройството може периодично да се синхронизира повторно със сървъра за обезпечаване, за да гарантира, че промените в профила, направени на сървъра, се разпространяват в крайните устройства (за разлика от изпращане на изрична заявка за повторно синхронизиране към крайната точка).

За да се предизвика периодично повторно синхронизиране на телефона, URL на профила за конфигуриране се дефинира чрез използване на параметър за правило на профил, а периодът на повторно синхронизиране се дефинира чрез използване на параметъра Resync_Periodic.

Преди да започнете

Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Процедура

Стъпка 1 Изберете **Глас** > **Обезпечаване**.

Стъпка 2 Дефинирайте параметъра Profile_Rule. Този пример приема, че IP адресът на TFTP сървъра е 192.168.1.200.

Стъпка 3 В полето **Периодично повторно синхронизиране** въведете малка стойност за тестване, като **30** секунди.

Стъпка 4 Щракнете върху **Изпращане на всички промени**.

С новите настройки на параметъра телефонът се синхронизира повторно два тъпи в минута с конфигурационния файл, посочен от URL.

Стъпка 5 Наблюдавайте получените съобщения в трасировката syslog (както се описват в раздела Използване на Syslog за регистриране на съобщения, на стр.54).

Стъпка 6 Уверете се, че полето **Повторно синхронизиране при нулиране** е установено на **Да**.

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

Стъпка 7 Включете телефона, за да го принудите да се синхронизира повторно със сървъра за обезпечаване.

Ако операцията за повторно синхронизиране не успее поради някаква причина, като липса на отговор от сървъра, модулът изчаква (за броя секунди, конфигурирани в **Закъснение при повторен опит поради грешка в повторното синхронизиране**) преди да направи нов опит за синхронизиране. Ако **Закъснение преди повторен опит поради грешка в повторното синхронизиране** е нула, телефонът не прави опит за повторно синхронизиране след неуспешно повторно синхронизиране.

Стъпка 8 (Опция) Установете стойността на полето **Закъснение преди повторен опит поради грешка в повторното синхронизиране** на малка стойност, като **30**.

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

Стъпка 9 Деактивирайте TFTP сървъра и наблюдавайте резултатите в изхода на syslog.

Уникални профили, макро изрази и HTTP

При разгръщането, когато всеки от телефоните трябва да бъде конфигуриран с определени стойности за някои параметри, като потребителски ИД или име на дисплея, доставчикът на услуги може да създаде уникален профил за всяко разгърнато устройство и да хоства тези профили на сървър за обезпечаване. Всеки телефон на свой ред трябва да бъде конфигуриран да се синхронизира отново със собствения си профил в съответствие с предварително определена конвенция за именуване.

Синтаксисът на URL на профила може да включва идентифицираща информация, която е специфична за всеки от телефоните, като MAC адрес или сериен номер при използване на макро израз от вградени променливи. Макро изразът елиминира нуждата да се посочват тези стойности на много места във всеки от профилите.

Правилото за профил преминава през макро израз преди да се приложи към телефона. Макро изразът управлява броя на променливите. Например:

- $MA разширява 12-цифрения MAC адрес (при използване на шестнадесетични числа, изписани с малки букви). Например 000e08abcdef.
- $SN се разширява до серийния номер на устройството. Например 88012BA01234.

Другите стойности могат да бъдат макро разширени по същия начин, като се включат всички параметри с общо предназначение, GPP_A до GPP_P. Пример от този процес можете да видите в Повторно синхронизиране с TFTP, на стр.53. Макро разширяването не се ограничава до името на файла на URL, а също може да се приложи към всяка част от параметъра за правило на профила. Тези параметри се обозначават като $A до $P. Пълният списък на достъпните за макро разширяване параметри можете да видите в Променливи за макро разширение, на стр.82.

В това упражнение се обезпечава специфичен за даден телефон профил на TFTP сървър.

Упражнение: Обезпечаване на специфичен профил за IP телефон на TFTP сървър

Процедура

Стъпка 1 Вземете MAC адреса на телефона от етикета на продукта. (MAC адресът представлява номер, който използва цифри и шестнадесетични числа с малка буква, като 000e08aabbcc.

Стъпка 2 Копирайте конфигурационния файл `basic.txt` (описан в Повторно синхронизиране с TFTP, на стр.53) в нов файл с име `CP-xxxx-3PCC macaddress.cfg` (заменяйки `xxxx` с номера на модела и `macaddress` с MAC адреса на телефона.

Стъпка 3 Преместете новия файл във виртуалната корнева директория на сървъра TFTP.

Стъпка 4 Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Стъпка 5 Изберете **Глас** > **Обезпечаване**.

Стъпка 6 Въведете `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` в полето **Правило на профила** .

```
<Profile_Rule>
```

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

Стъпка 7 Кликнете върху **Изпращане на всички промени**. Това ще доведе до незабавно повторно зареждане и повторно синхронизиране.

При следващото повторно синхронизиране телефонът извлича новия файл чрез разширяване на макро израза $MA в неговия MAC адрес.

Повторно синхронизиране с HTTP GET

HTTP осигурява по-надежден механизъм за повторно синхронизиране от TFTP, тъй като HTTP установява TCP връзка, а TFTP използва по-малко надежден UDP. В допълнение HTTP сървърите предлагат подобрени функции за филтриране и регистриране в сравнение с TFTP сървърите.

От страната на клиента телефонът не изисква специална настройка за конфигуриране на сървъра, за да може да се синхронизира повторно при използване на HTTP. Синтаксисът на параметъра Profile_Rule за използване на HTTP с метод GET е подобен на синтаксиса, който се използва за TFTP. Ако профилът може да бъде извлечен от HTTP сървъра със стандартен уеб браузър, телефонът също трябва да може да го прави.

Упражнение*:* Повторно синхронизиране с *HTTP GET*

Процедура

Стъпка 1 Инсталирайте HTTP сървър на местен компютър или друг достъпен хост.

Сървърът с отворен код Apache може да се изтегли от интернет.

Стъпка 2 Копирайте профила за конфигуриране `basic.txt` (описан в Повторно синхронизиране с TFTP, на стр.53) във виртуалната главна директория на инсталирания сървър.

Стъпка 3 За да потвърдите правилното инсталиране на сървъра и достъпа до файловете в `basic.txt`, осъществете достъп до профила с уеб браузър.

Стъпка 4 Променете правилото на профила на тестовия телефон така, че да сочи към HTTP сървъра вместо към TFTP сървър, така че да изтегля профила си периодично.

Например, ако приемем, че HTTP сървърът има адрес 192.168.1.300, въведете следната стойност:

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

Стъпка 5 Кликнете върху **Изпращане на всички промени**. Това ще доведе до незабавно повторно зареждане и повторно синхронизиране.

Стъпка 6 Наблюдавайте съобщенията syslog, които се изпращат от телефона. Периодичното повторно синхронизиране сега трябва да получава профила от HTTP сървър.

Стъпка 7 В регистрационните файлове на HTTP сървъра наблюдавайте как информацията , която разпознава тестовия профил, се показва в регистрационния файл на потребителските агенти.

Тази информация трябва да включва производителя, името на продукта, текущата версия на фърмуера и серийния номер.

Обезпечаване чрез Cisco XML

Всеки от обозначените тук с xxxx телефони можете да обезпечите чрез XML функциите на Cisco.

Можете да изпратите XML обект към телефона чрез уведомителен пакет SIP или публикуване на HTTP на CGI интерфейса на телефона: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC разширява XML функцията на Cisco да поддържа обезпечаване чрез XML обект:

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

След като телефонът получи XML обекта, той изтегля файла за обезпечаване от [profile-rule]. Това правило използва макроси за опростяване на разгръщането на приложението на XML услугите.

Разрешаване на URL с макро израз

Поддиректориите с много профили на сървъра осигуряват удобен метод за управление на голям брой разгърнати устройства. URL на профила може да съдържа:

- Името на обезпечаващия сървър или изричен IP адрес. Ако профилът разпознава сървъра за обезпечаване по име, телефонът изпълнява DNS търсене, за да разреши името.
- Нестандартният сървърен порт, който е посочен в URL чрез използване на стандартен синтаксис `:порт`, последван от името на сървъра.
- Поддиректорията на виртуалната главна директория на сървъра, в която се съхранява профила, посочен чрез използване на стандартна URL нотация и управляван от макро разширение.

Например следното правило за профил изисква файлът на профила ($PN.cfg), в поддиректорията на сървъра `/cisco/config`, от TFTP сървър, който работи на хост prov.telco.com да очаква свързване на порт 6900:

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

Профилът за всеки от телефоните може да се разпознае чрез параметър с общо предназначение, чиято стойност е спомената в общо правило за профил при използване на макро израз.

Например нека приемем, че GPP_B е дефиниран като `Dj6Lmp23Q`.

Правилото на профила съдържа стойността:

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

При повторно синхронизиране на устройството и разширяване на макросите, телефонът с MAC адрес 000e08012345 изисква профил с име, което съдържа MAC адреса на устройството на следния URL:

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

Защитено повторно синхронизиране с HTTPS

Тези механизми са достъпни на телефона за повторно синхронизиране при използване на процес за защитена комуникация:

- Основно повторно синхронизиране с HTTPS
- HTTPS с удостоверяване на сертификата на клиента
- HTTPS филтриране на клиент и динамично съдържание

Основно повторно синхронизиране с HTTPS

HTTPS добавя SSL към HTTP при дистанционно обезпечаване, така че:

- Телефонът да може да удостовери сървъра за обезпечаване.
- Сървърът за обезпечаване може да удостовери телефона.
- Поверителността на обменената информация между телефона и сървъра за обезпечаване е гарантирана.

SSL генерира и обменя тайни (симетрични) ключове за всяка връзка между телефона и сървъра, като използва части с общодостъпен/частен ключ, които са предварително инсталирани на телефона и сървъра за обезпечаване.

От страната на клиента телефонът не изисква специална настройка за конфигуриране на сървъра, за да бъде повторно синхронизиран при използване на HTTPS. Синтаксисът на параметъра за правило на профила за използване на HTTPS с метод GET е подобен на синтаксиса, който се използва за HTTPS или TFTP. Ако профилът може да бъде извлечен от HTTPS сървър със стандартен уеб браузър, телефонът би трябвало също да може да го направи.

В допълнение към инсталирането на HTTPS сървър, сертификатът от SSL сървър, който се подписва от Cisco, трябва да бъде инсталиран на сървъра за обезпечаване. Устройствата не могат да се синхронизират повторно със сървър, който използва HTTPS, освен ако сървърът не подава подписан от Cisco сертификат. Инструкции за създаването на подписани SSL сетификати за гласови продукти можете да намерите на https://supportforums.cisco.com/docs/DOC-9852.

Упражнение: Основно повторно синхронизиране с HTTPS

Процедура

Стъпка 1 инсталирайте сървъра HTTPS на хост, чийто IP адрес е известен на мрежовия DNS сървър чрез нормално превеждане на име на хост.

Сървърът с отворен код Apache може да се конфигурира да раоти като HTTPS сървър при инсталирането с пакет mod_ssl с отворен код.

Стъпка 2 Генерирайте сървърна заявка за подписване на сертификат за сървъра. За тази стъпка може да се наложи да инсталирате пакет OpenSSL с отворен код или друг еквивалентен софтуер. Ако използвате OpenSSL, командата за генериране на основен CSR файл е както следва:

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

Тази команда генерира публична/частна двойка ключове, която се записва във файла `privkey.pem`.

Стъпка 3 Изпратете CSR файла (provserver.csr) на Cisco за подписване.

Подписаният сървърен сертификат се връща (provserver.cert) заедно със корневия сертификат за клиент Sipura CA, spacroot.cert.

За повече информация вижте https://supportforums.cisco.com/docs/DOC-9852.

Стъпка 4 Съхранете подписания сървърен сертификат, файла с двойката частни ключове и корневия сертификат за клиент на съответните места на сървъра.

В случай на инсталация Apache на Linux тези местоположения обикновено са както следва:

```
# 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
```

Стъпка 5 Рестартирайте сървъра.

Стъпка 6 Копирайте конфигурационния файл `basic.txt` (описан в Повторно синхронизиране с TFTP, на стр.53) във виртуалната корнева директория на HTTPS сървъра.

Стъпка 7 Проверете правилната работа на сървъра, като изтеглите `basic.txt` от HTTPS сървъра при използване на стандартен браузър от местния компютър.

Стъпка 8 Проверете сертификата на сървъра, който се подава от сървъра.

Най-вероятно браузърът няма да разпознае сертификата като валиден, освен ако не е предварително конфигуриран да приема Cisco като корневи CA. Въпреки това телефонът очаква сертификатът да бъде подписан по този начин.

Променете правилото на профила на тестовото устройство така, че да съдържа препратка към HTTPS сървър. Например:

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

Този пример приема, че името на HTTPS сървъра е **my.server.com**.

Стъпка 9 Кликнете върху **Изпращане на всички промени**.

Стъпка 10 Наблюдавайте трасировката на syslog, която се изпраща от телефона.

Съобщението на syslog трябва да посочва, че повторното синхронизиране е получило профила от HTTPS сървър.

Стъпка 11 (по избор) Използвайте анализатора на Ethernet протокол в подмрежата на телефона, за да потвърдите, че пакетите са шифровани.

В това упражнение не е активирано потвърждение на сертификата на клиент. Връзката между телефона и сървъра е шифрована. Въпреки това прехвърлянето не е защитено, тъй като клиентът може да се свърже със сървъра и да заяви файла, при положение че му е известно името на файла и местоположението на директорията. За защитено повторно синхронизиране сървърът трябва да удостовери клиента, както е показано в упражнението, описано в HTTPS с удостоверяване на сертификата на клиента, на стр.62.

HTTPS с удостоверяване на сертификата на клиента

Във фабричната конфигурация по подразбиране сървърът не изисква SSL сертификат на клиент от клиента. Прехвърлянето на профила не е защитено, тъй като всеки клиент може да се свърже със сървъра и да изиска профил. Можете да редактирате конфигурацията, за да разрешите удостоверяване на клиента: сървърът изисква сертификат на клиент, за да удостовери телефона преди да получи заявка за свързване.

Поради това искане операцията за повторно синхронизиране не може да се тества независимо при използване на браузър, който няма правилни данни за вход. Обменът на SSL ключове в HTTPS връзката между тествания телефон и сървъра може да се наблюдава с помощната програма ssldump. Трасирането на помощната програма показва взаимодействието между клиента и сървъра.

Упражнение: HTTPS с удостоверяване на сертификата на клиента

Процедура

Стъпка 1 Активирайте удостоверяването на сертификата за клиента на HTTPS сървъра.

Стъпка 2 При Apache (v.2) задайте следното в конфигурационния файл на сървъра:

```
SSLVerifyClient  require
```

Освен това се уверете, че spacroot.cert е съхранен, както е показано в упражнението Основно повторно синхронизиране с HTTPS, на стр.60.

Стъпка 3 Рестартирайте HTTPS сървъра и наблюдавайте трасирането на syslog от телефона.

Всяко повторно синхронизиране със сървъра сега изпълнява симетрично удостоверяване, така че сертификатът на сървъра и сертификатът на клиента да се проверяват преди прехвърлянето на профила.

Стъпка 4 Използвайте ssldump, за да прихванете връзка за повторно синхронизиране между телефона и HTTPS сървъра.

Ако на сървъра е правилно разрешено потвърждаването на сертификата на клиента, трасирането на ssldump показва симетричен обмен на сертификати (първо сървър към клиент, а след това клиент към сървър) преди шифрованите пакети, които съдържат профила.

При активирано удостоверяване на клиент, само телефони с MAC адрес, който съвпада с валиден сертификат на клиент могат да заявяват профил от сървъра за обезпечаване. Сървърът отхвърля заявка от обикновен браузър или друго неупълномощено устройство.

HTTPS филтриране на клиент и динамично съдържание

Ако HTTPS сървърът е конфигуриран да изисква сертификат за клиент, информацията в сертификата посочва телефона за повторно синхронизиране и му подава правилна информация за конфигуриране.

HTTPS сървърът прави достъпна информацията за сертификат за CGI скриптовете (или компилираните CGI програми), които се извикват като част от заявката за повторно синхронизиране. С цел илюстриране това упражнение използва езика за скриптиране с отворен код Perl и приема, че като HTTPS сървър се използва Apache (v.2).

Процедура

Стъпка 1 Инсталирайте Perl на хоста, на който работи HTTPS сървъра.

Стъпка 2 Генерирайте следния рефлекторен скрипт на 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>”;
```

Стъпка 3 Запазете файла с име `reflect.pl` с разрешение за изпълнение (chmod 755 при Linux) в директорията за CGI скриптове на HTTPS сървъра.

Стъпка 4 Потвърдете достъпността на CGI скриптовете на сървъра (т.е. `/cgi-bin/…`).

Стъпка 5 Променете правилото за профил на текстовото устройство за повторно синхронизиране с рефлекторен скрипт, както е посочено в следващия пример:

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

Стъпка 6 Кликнете върху **Изпращане на всички промени**.

Стъпка 7 Наблюдавайте трасирането на syslog, за да гарантирате успешно повторно синхронизиране.

Стъпка 8 Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Стъпка 9 Изберете **Глас** > **Обезпечаване**.

Стъпка 10 Проверете дали параметърът GPP_D съдържа информацията, която е прихваната от скрипта.

Тази информация съдържа името на продукта, MAC адреса и серийния номер, ако текстовото устройство има уникален сертификат от производителя. Информацията съдържа генерични низове, ако устройството е произведено преди фърмуерна версия 2.0.

Подобен скрипт може да определи информацията за повторно синхронизиращо се устройство и след това да осигури на устройството подходящи стойности на параметъра за конфигуриране.

HTTPS сертификати

Телефонът осигурява надеждна и защитена стратегия за обезпечаване, която се основава на HTTPS заявки от устройството към сървъра за обезпечаване. Сертификатът на сървъра и сертификатът на клиента се използват за удостоверяване на телефона пред сървъра и сървъра пред телефона.

За да използвате HTTPS с телефона, трябва да генерирате заявка за подписване на сертификат (CSR) и да я изпратите на Cisco. Телефонът генерира сертификат за инсталиране на сървъра за обезпечаване. Телефонът приема сертификата, когато търси да установи HTTPS връзка със сървъра за обезпечаване.

HTTPS методология

HTTPS шифрова комуникацията между клиента и сървъра, защитавайки съдържанието на съобщението от други мрежови устройства. Методът за шифроване в тялото на комуникацията между клиента и сървъра се основава на шифроване със симетричен ключ. При шифроване със симетричен ключ клиентът и сървърът споделят един секретен ключ през защитен канал, който се защитава от шифроване с публичен/частен ключ.

Шифрованите със секретен ключ съобщения могат да се дешифрират само при използване на същия ключ. HTTPS поддържа широка гама от алгоритми за симетрично шифроване. Телефонът прилага до 256-битово симетрично шифроване при използване на Американски стандарт за шифроване (AES) в допълнение към 128-битов RC4.

HTTPS освен това предлага удостоверяване на сървър и клиент, ангажирани в защитена транзакция. Тази функция гарантира, че сървърът за обезпечаване и отделния клиент не могат да бъдат измамени от други устройства в мрежата. тази възможност е особено важна в контекста на дистанционното обезпечаване на крайни точки.

Удостоверяването на сървъра и клиента се извършва чрез използване на шифроване с публичен/частен ключ със сертификат, който съдържа публичен ключ. Текстът, който се шифрова с публичен ключ, може да бъде дешифриран само от съответния частен ключ (и

обратно). Телефонът поддържа алгоритъм Rivest-Shamir-Adleman (RSA) за шифроване с публичен/частен ключ.

Сертификат на SSL сървър

Всеки от защитените сървъри за обезпечаване издава SSL сертификат, който Cisco подписва директно. Работещият на телефона фърмуер разпознава като валидни само сертификати на Cisco. Когато клиентът се свързва към сървър с помощта на HTTPS, той отказва сертификат на сървър, който не е подписан от Cisco.

Този механизъм защитава доставчика на услуги от неупълномощен достъп до телефона или други опити за измама на обезпечаващия сървър. Без такава защита атакуващият може да обезпечи отново телефона, за да получи достъп до информацията за конфигуриране или да използва различна VoIP услуга. Без частен ключ, който съответства на валиден сертификат на сървър, атакуващият не може да установи комуникация с телефона.

Получаване на сертификат на сървър

Процедура

Стъпка 1 Свържете се с лице от поддръжката на Cisco, което да работи с вас при обработката на сертификата. Ако не работите с определено лице по поддръжката, изпратете по имейл заявката си на ciscosb-certadmin@cisco.com.

Стъпка 2 Генерирайте частен ключ, който да се използва в CSR (Заявка за подписване на сертификат). Ключът е частен и не е необходимо да го подавате на поддръжката на Cisco. Използвайте "openssl" с отворен код, за да генерирате ключа. Например:

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

Стъпка 3 Генерира CSR, който съдържа полета, идентифициращи вашата организация и местоположение. Например:

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

Трябва да разполагате със следната информация:

- Поле на темата—Въведете общото име (CN), което трябва да има синтаксис на FQDN (Напълно квалифицирано име на домейн). По време на опознавателната процедура за SSL удостоверяване телефонът потвърждава, че сертификатът, който е получил, е от машината, която го е представила.
- Име на хоста на сървъра—Например provserv.domain.com.
- Имейл адрес—Въведете имейл адрес, така че от отдела за поддръжка на клиенти да се свържат с вас при необходимост. Този имейл адрес е видим в CSR.

Стъпка 4 Изпратете по имейл CSR (в zip формат) на лице от екипа за поддръжка на Cisco или на адрес ciscosb-certadmin@cisco.com. Сертификатът се подписва от Cisco. Cisco ви връща сертификата, за да го инсталирате на системата си.

Сертификат на клиент

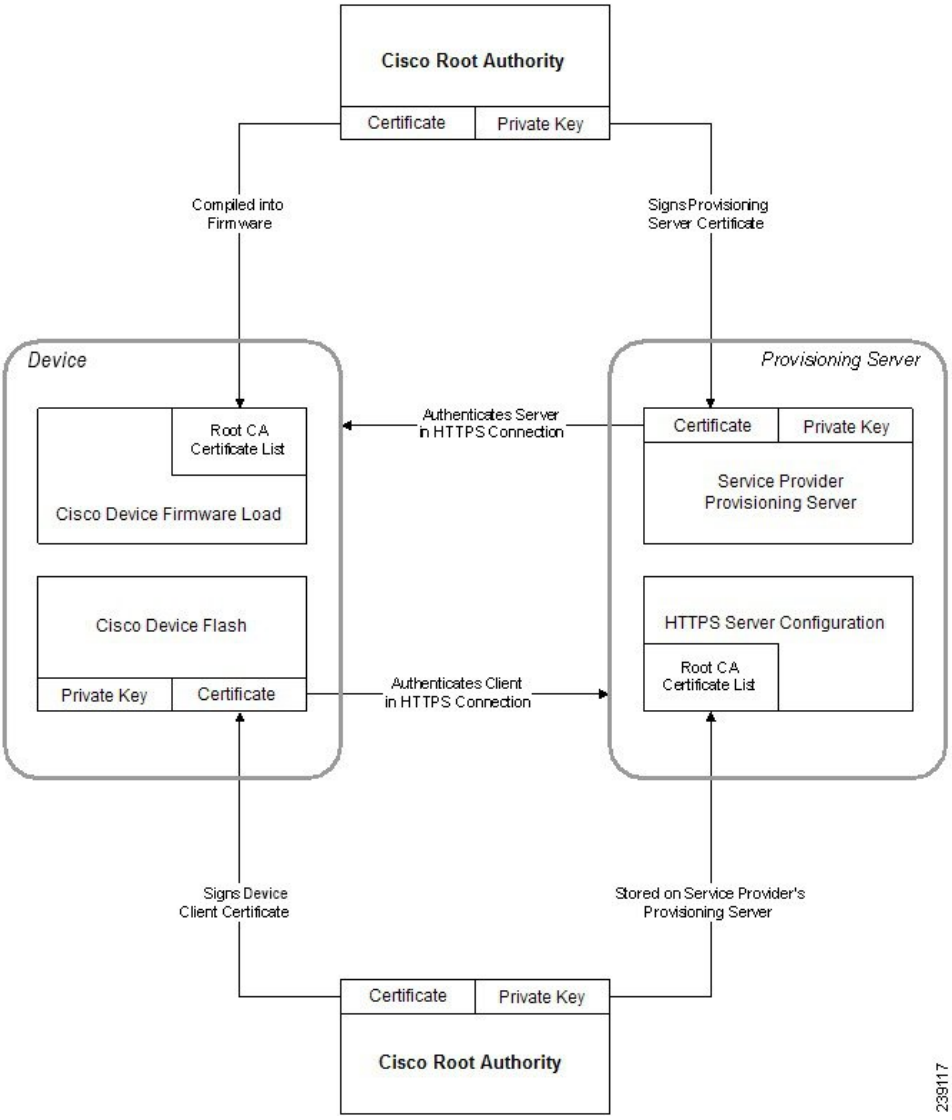
В допълнение към директната атака на телефона, атакуващият може да предприеме опит за контакт със сървъра за обезпечаване чрез стандартен уеб браузър или друг HTTPS клиент за получаване на профил за конфигуриране от сървъра за обезпечаване. За да се предотврати този тип атаки, всеки телефон освен това носи уникален сертификат на клиент, подписан от Cisco, който включва идентифициращa информация относно всяка отделна крайна точка. Всеки доставчик на услуги получава сертификат корневи сертификат от сертификационния орган за удостоверяване на сертификата на клиент на устройството. Този път за сертифициране позволява на сървъра за обезпечаване да откаже неупълномощени заявки за профили за конфигуриране.

Структура на сертификат

Комбинацията от сертификат на сървъра и сертификат на клиента гарантира защитена комуникация между дистанционния телефон и сървъра за обезпечаване. Следващата фигура показва връзката и разполагането на сертификатите, двойката публичен/частен ключ и корневите органи за подписване, сред клиентите Cisco, сървъра за обезпечаване и органа за сертифициране.

Горната половина на схемата показва корневия орган на сървъра за обезпечаване, който се използва за подписване на индивидуалния сертификат на сървъра за обезпечаване. Съответният корневи сертификат се компилира във фърмуера, което позволява на телефона да удостовери упълномощените сървъри за обезпечаване.

Фигура *2:* Поток на органа за сертифициране



Конфигуриране на потребителска Certificate Authority

Цифровите сертификати могат да използват устройства за удостоверяване на мрежа и потребители в мрежата. Те могат да се използват за сесии за преговори IPSec между мрежовите възли.

Трети страни използват сертификат на Cerificate Authority за потвърждаване и удостоверяване на два или повече възела, които правят опит за комуникация. Всеки възел има публичен и частен ключ. Публичният ключ шифрова данни. Частният ключ дешифрира данни. Тъй като възлите са получили сертификата си от един и същи източник, те гарантират за съответните самоличности.

Устройството може да използва цифрови сертификати, осигурявани от Certificate Authority (CA) на трети страни, за да удостовери връзките IPSec.

Телефоните поддържат набор от предварително заредени Root Certificate Authority, вградени във фърмуера:

- Сертификат Cisco Small Business CA
- Сертификат CyberTrust CA
- Сертификат CyberTrust CA
- Сертификат Sipura Root CA
- Сертификат Linksys Root CA

Преди да започнете

Преминете към уеб страницата за администриане на телефона. Виж Достъп до уеб страницата на телефона, на стр.8.

Процедура

Стъпка 1 Изберете **Информация** > **Състояние**.

Стъпка 2 Превъртете до **Състояние на потребителски CA** и вижте следните полета:

- Състояние на обезпечаване на потребителски CA—Показва състоянието на обезпечаване.
  - Последното обезпечаване е извършено на мм/дд/гггг ЧЧ:ММ:СС; или
  - Последното обезпечаване е извършено на мм/дд/гггг ЧЧ:ММ:СС
- Информация за потребителски CA —Показва информация за потребителски CA.
  - Инсталирани—Показва „CN стойност,” където „CN стойност” е стойността на CN параметъра за полето на темата в първия сертификат.
  - Неинсталиран—Показва се, ако няма инсталиран CA сертификат.

Управление на профилите

Този раздел показва формирането на профилите за конфигуриране, които се подготвят за изтегляне. За да се обяснят функциите, като метод за повторно синхронизиране се използва TFTP от местен компютър, въпреки че могат да се използват още HTTP или HTTPS.

Компресиране на профил Open с Gzip

Конфигурационните профили в XmL формат могат да бъдат доста големи, ако профилът посочва всички параметри по отделно. За да се намали натоварването на обезпечаващия сървър, телефонът поддържа компресиране на XML файлове чрез използване на понижаващ формат за компресиране, поддържан от помощната програма gzip (RFC 1951).

Забележка Компресирането трябва да се предшества от шифроване за телефона, за да разпознае компресирания и шифрован XML профил.

За интегриране в персонализирани решения на крайни обезпечаващи сървъри, библиотеката за компресиране с отворен код на zlib може да се използва вместо самостоятелна помощна програма zlib за извършване на компресирането на профила. Въпреки това телефонът очаква файлът да съдържа валидно заглавие на gzip.

Процедура

Стъпка 1 Инсталиране на gzip на локален компютър.

Стъпка 2 Компресирайте конфигурационния профил `basic.txt` (описан в Повторно синхронизиране с TFTP, на стр.53) като извикате gzip от командния ред:

```
gzip basic.txt
```

Това води до генериране на по-малкия файл `basic.txt.gz`.

Стъпка 3 Запишете файла `basic.txt.gz` във виртуалната главна директория на сървъра TFTP.

Стъпка 4 Променете правилото за профила на текстово устройство, за да синхронизирате отново компресирания файл на мястото на оригиналния XML файл, както е показано в следващия пример:

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

Стъпка 5 Кликнете върху **Изпращане на всички промени**.

Стъпка 6 Наблюдавайте трасирането на syslog от телефона.

При повторно синхронизиране телефонът изтегля новия файл и го използва за актуализиране на параметрите му.

Сродни теми

Компресирарне на профил Open, на стр.18

Шифроване на профил с OpenSSL

Компресирания или некомпресиран профил може да бъде шифрован (файлът обаче трябва да бъде компресиран преди да се шифрова). Шифроването се използва, когато поверителността на информацията за телефона е от особена важност. Например, когато TFTP или HTTP се използва за комуникация между телефона и сървъра за обезпечаване.

Телефонът поддържа симетрично шифроване с ключ при използване на 256-битов AES алгоритъм. Това шифроване може да се извърши при използване на пакет на OpenSSL с отворен код.

Процедура

Стъпка 1 Инсталирайте OpenSSL на локален компютър. Това може да наложи приложението OpenSSL да бъде повторно компилирано, за да се активира AES.

Стъпка 2 С помощта на конфигурационния файл `basic.txt` (описан в Повторно синхронизиране с TFTP, на стр.53) генерирайте шифрован файл със следната команда:

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

Компресираният файл `basic.txt.gz`, създаден в Компресиране на профил Open с Gzip, на стр.68, също може да се използва, тъй като файлът на XML профила може да бъде едновременно компресиран и шифрован.

Стъпка 3 Съхранете шифрования файл `basic.cfg` във виртуалната корнева директория на TFTP сървъра.

Стъпка 4 Променете правилото на профила на тестовото устройство така, че да се синхронизира отново с шифрования файл вместо с оригиналния XML файл. Ключът за шифроване става известен на телефона със следната опция за URL:

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

Стъпка 5 Кликнете върху **Изпращане на всички промени**.

Стъпка 6 Наблюдавайте трасирането на syslog от телефона.

При повторно синхронизиране телефонът изтегля новия файл и го използва за актуализиране на параметрите му.

Сродни теми

AES-256-CBC шифроване, на стр.19

Създаване на профили с дялове

Телефонът изтегля много отделни профили по време на всяко повторно синхронизиране. Тази практика позволява управление на различни видове информация за профила на отделни сървъри и поддръжка на общи стойности на параметъра за конфигуриране, отделно от специфичните стойности за акаунта.

Процедура

Стъпка 1 Създайте нов XML профил, `basic2.txt`, посочващ стойност за параметъра, който го отличава от предишен опит. Например добавете следното към профила `basic.txt`:

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

Стъпка 2 Съхранете профила `basic2.txt` във виртуалната главна директория на TFTP сървъра.

Стъпка 3 Оставете първото правило от по-ранните упражнения в папката, но конфигурирайте второто правило на профила (Правило на профила B) да посочва към нов файл.

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

Стъпка 4 Кликнете върху **Изпращане на всички промени**.

При това телефонът се синхронизира повторно с първия и втория профил в този ред, когато е необходима операция по повторно синхронизиране.

Стъпка 5 Наблюдавайте трасировката на syslog, за да потвърдите очакваното поведение.

Задаване на заглавката за поверителност за телефона

Заглавката за поверителност на потребителя в SIP съобщението задава нуждите на потребителя от поверителност от доверената мрежа.

Можете да зададете стойност за тази заглавка за всеки вътрешен номер на линия, като използвате XML маркер във файла `config.xml`.

Опциите за заглавката за поверителност са следните:

- Disabled (по подразбиране)
- none – Потребителят иска от услугата за поверителност да не прилага функции за поверителност към това SIP съобщение.
- header – Потребителят иска от услугата за поверителност да прикрие заглавките, от които не може да се премахне идентифициращата информация.
- session – Потребителят иска от услугата за поверителност да обезпечи анонимност на сесиите.
- user – Потребителят иска ниво на поверителност само през посредниците.
- id – Потребителят иска от системата да използва идентификатор, който не разкрива IP адреса или името на хоста.

Процедура

Стъпка 1 Редактирайте файла `config.xml` на телефона с текстов или XML редактор.

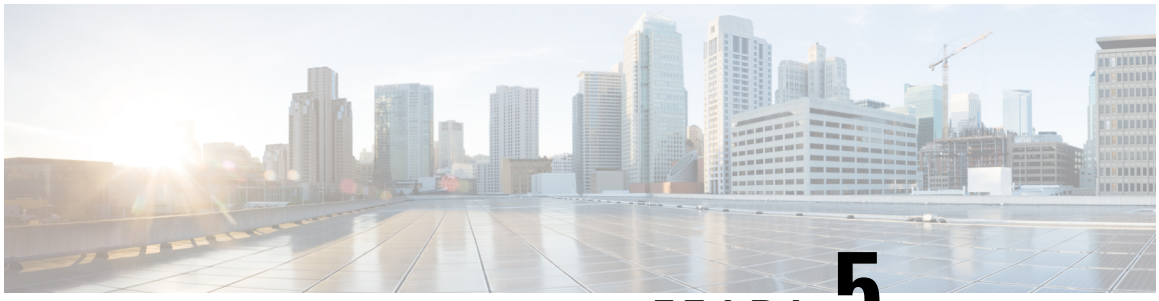
Стъпка 2 Вмъкнете маркера **<Privacy_Header_N_ ua="na">*Value*</Privacy_Header_N_>**, където N е вътрешният номер на линията (1 – 10), и използвайте една от следните стойности.

- Стойност по подразбиране: **Disabled**

- **none**
- **header**
- **session**
- **потребител**
- **id**

Стъпка 3 (по избор) Обезпечете другите номера на линии със същия маркер, като използвате подходящия вътрешен номер на линия.

Стъпка 4 Запазете промените във файла `config.xml`.



ГЛАВА 5

Параметри за обезпечаване

Преглед на параметрите за обезпечаване

Тази глава описва параметрите за обезпечаване, които могат да се използват в скриптове на профила за конфигуриране.

Параметри на профила за конфигуриране

Следващата таблица дефинира функциите и употребата на всеки от параметрите в секцията **Параметри на профила за конфигуриране** в раздела **Обезпечаване**.

Име на параметъра	Описание на стойността по подразбиране
Provision Enable	Управлява всички действия при повторно синхронизиране независимо от действията за надграждане на фърмуера. Задайте на **Да**, за да активирате дистанционно обезпечаване. Стойността по подразбиране е „Да“.
Resync On Reset	Включва повторно синхронизиране след всяко презареждане, освен при презареждане причинено от актуализиране на параметър или фърмуерни надграждания. Стойността по подразбиране е „Да“.

Име на параметъра	Описание на стойността по подразбиране
Resync Random Delay	Произволно закъснение, следващо последователност за зареждане преди извършване на нулиране, посочено в секунди. В набор от устройства за IP телефония, които са планирани за едновременно включване, въвежда разпространени във времената, в които всеки от модулите изпраща заявка за повтоно синхронизиране към сървъра за обезпечаване. Тази функция може да бъде полезна при големи разгръщания в жилищни сгради и в случаи на регионално спиране на захранването. Стойността на първото поле трябва да бъде цяло число между 0 и 65535. Стойността по подразбиране е 2.
Resync At (HHmm)	Часът и минутите (ЧЧмм), които устройството синхронизира отново със сървъра за обезпечаване. Стойността на това поле трябва да включва четирицифрено число в диапазона от 0000 до 2400, за да покаже времето във формат ЧЧм. Например 0959 показва 09:59. Стойността по подразбиране е празно поле. Ако стойността е невалидна, параметърът се игнорира. Ако този параметър е зададен с валидна стойност,параметрите за периодично повторно синхронизиране се игнорират.

Име на параметъра	Описание на стойността по подразбиране
Resync At Random Delay	Предотвратява презареждането на сървъра за обезпечаване при едновременно включване на голям брой устройства. За да се избегнат твърде много заявки за повторно синхронизиране към сървъра от много телефони, телефонът се синхронизира повторно в диапазона между часовете и минутите и часовете и минутите плюс произволно закъснение (ччмм, ччмм+ произволно закъснение). Например при произволно закъснение = (Повторно синхронизиране при произволно закъснение + 30)/60 минути входната стойност във секунди се преобразува в минути със закръгление до следващата минута, за да изчисли окончателния интервал random_delay. Валиден стойност варира от 0 до 65535. Тази функция се деактивира, когато параметърът е установен на нула. Стойността по подразбиране е 600 секунди (10 минути).

Име на параметъра	Описание на стойността по подразбиране
Resync Periodic	Времевият интервал между периодичното повторно синхронизиране със сървъра за обезпечаване. Асоцииранията таймер за повторно синхронизиране е активен само след първото успешно синхронизиране със сървъра. Валидни са следните формати: • Цяло число Пример: Въвеждането на **3000** означава, че следващото повторно синхронизиране ще се извърши след 3000 секунди. • Няколко цели числа Пример: Въвеждането на **600,1200,300** показва, че първото повторно синхронизиране ще се извърши след 600 секунди, второто повторно синхронизиране ще се извърши 1200 секунди след първото, а третото повторно синхронизиране ще се извърши 300 секунди след второто. • Времеви диапазон Например въвеждането на **2400 + 30**показва, че следващото повторно синхронизиране ще се извърши между 2400 и 2430 секунди след успешно повторно синхронизиране. Задайте параметъра на нула, за да деактивирате периодичното повторно синхронизиране. Стойността по подразбиране е 3600 секунди.

Име на параметъра	Описание на стойността по подразбиране
Resync Error Retry Delay	Ако операцията по повторно синхронизиране е неуспешна поради невъзможност на устройството за IP телефония да извлече профила от сървъра или изтегленият файл е повреден, или при възникване на вътрешна грешка, устройството прави опити за повторно синхронизиране отново след посоченото време в секунди. Валидни са следните формати: • Цяло число Пример: Въвеждането на **300** показва, че следващия опит за повторно синхронизиране ще се извърши след 300 секунди. • Няколко цели числа Пример: Въвеждането на **600,1200,300** показва, че първият повторен опит се извършва след 600 секунди след неуспеха, вторият повторен опит се извършва 1200 секунди след неуспеха на първия повторен опит и третият повторен опит се извършва след 300 секунди след неуспеха на втория повторен опит. • Времеви диапазон Например въвеждането на **2400+30** показва, че следващият повторен опит се извършва между 2400 и 2430 секунди след неуспеха на повторното синхронизиране. Ако закъснението се установи на 0, устройството не прави отново опит за повторно синхронизиране след неуспешен опит за повторно синхронизиране.

Име на параметъра	Описание на стойността по подразбиране
Forced Resync Delay	Максималното закъснение (в секунди), през което телефонът чака преди да извърши повторно синхронизиране. Устройството не извършва повторно синхронизиране, когато някоя от линиите му е активна. Тъй като повторното синхронизиране може да отнеме няколко секунди, е желателно да изчакате устройството да бъде свободно за продължителен период преди повторно синхронизиране. Това позволява на потребителя да прави повиквания без прекъсване. Устройството има таймер, който започва обратно броене, когато всички линии са свободни. Този параметър е първоначалната стойност на брояча. Събитията на повторно синхронизиране се забавят докато броячът стигне нула. Валиден стойност варира от 0 до 65535. Стойността по подразбиране е 14 400 секунди.
Resync From SIP	Активира стартиране на повторно синхронизиране от съобщението SIP NOTIFY. Стойността по подразбиране е „Да“.
Resync After Upgrade Attempt	Активира или деактивира операция по повторно синхронизиране след надграждане. Ако се избере „Да“, се стартира синхронизиране. Стойността по подразбиране е „Да“.
Resync Trigger 1, Resync Trigger 2	Подлежащи на конфигуриране превключватели на повторно синхронизиране Повторното синхронизиране се стартира, когато уравнението на логиката в тези параметри получи стойност ИСТИНА. Стойността по подразбиране е (празно поле).

Име на параметъра	Описание на стойността по подразбиране
Resync Fails On FNF	Повторното синхронизиране се счита за неуспешно, ако заявеният профил не се получи от сървъра. Този параметър може да има предимство пред това. Когато е установено на **не**, устройството приема отговор `file-not-found` от сървъра като успешно повторно синхронизиране. Стойността по подразбиране е „Да“.
Правило на профила Profile Rule B Profile Rule C Profile Rule D	Всяко от правилата за профил информира телефона за източника, от който да получи профил (кнфигурационен файл). По време на всяка операция resync телефонът прилага последователно всички политики.. По подразбиране: **`/$PSN.xml`** Ако прилагате AES-256 ТГС шифроване към конфигурационните файлове, посочете ключа за шифроване с ключовата дума **`--key`** както следва: **`--key <encryption key>]`** Можете да приложите ключ за шифроване в двойни кавички ("), като опция.
Опции за използване на DHCP	Опции за DHCP, разделени от запетаи, използвани за извличане на фърмуер и профили. Стойността по подразбиране е 66,160,159,150,60,43,125.
Log Request Msg	Този параметър съдържа съобщение, което се изпраща на сървъра syslog при стартирането на опит за повторно синхронизиране. Стойността по подразбиране е `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`.
Log Success Msg	Съобщение на syslog, което се издава при успешно завършване на опит за повторно синхронизиране. Стойността по подразбиране е `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.

Име на параметъра	Описание на стойността по подразбиране
Log Failure Msg	Съобщение на syslog, което се издава след неуспешен опит за повторно синхронизиране. Стойността по подразбиране е `$PN $MAC -- Resync failed: $ERR`.
User Configurable Resync	Позволява на потребителя да синхронизира отново от екрана на IP телефона. Стойността по подразбиране е „Да“.

Параметри за надграждане на фърмуера

Следващата таблица дефинира функциите и употребата на всеки от параметрите в секцията **Надграждане на фърмуера** на раздела **Обезпечаване**.

Име на параметъра	Описание на стойността по подразбиране
Upgrade Enable	Активира операции по надграждане на фърмуера независимо от действията за повторно синхронизиране. Стойността по подразбиране е „Да“.
Upgrade_Error_Retry_Delay	Интервалът за повторен опит за надграждане (в секунди), който се прилага в случай на неуспешно надграждане. Устройството има таймер за грешка при надграждане на фърмуера, който се активира след неуспешен опит за фърмуерно надграждане. Таймерът е инициализиран със стойността на този параметър. Следващият опит за надграждане на фърмуера е когато таймерът отброи нула. Стойността по подразбиране е 3600 секунди.

Име на параметъра	Описание на стойността по подразбиране
Upgrade Rule	Скрипт за надграждане на фърмуера, който дефинира условия за надграждане и асоциирани URL за фърмуера. Използва същия синтаксис както правилото за профил. Използвайте следния формат, за да въведете правилото за надграждане: **<tftp|http|https>://<ip address>/image/<load name>** Например: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Ако не е посочен протокол, се разбира TFTP. Ако не е посочено име на сървър, хостът, който заявява URL се използва като име на сървър. Ако не е посочен порт, се използва порт по подразбиране (69 за TFTP, 80 за HTTP или 443 за HTTPS). Стойността по подразбиране е празно поле.
Log Upgrade Request Msg	Издадено при стартирането на опита за надграждане на фърмуера съобщение на Syslog. По подразбиране: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Издадено след успешното завършване на опита за надгарждане на фърмуера съобщение на Syslog. Стойността по подразбиране е `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg	Издадено след неуспешен опит за надграждане на фърмуера съощение на Syslog. Стойността по подразбиране е `$PN $MAC -- Upgrade failed: $ERR`
Равноправно споделяне на фърмуер	Активира или деактивира функцията за равноправно споделяне на фърмуер. Изберете **Да** или **Не**, за да активирате или деактивирате функцията. По подразбиране: Да

Име на параметъра	Описание на стойността по подразбиране
Сървър за регистрационни файлове за равноправното споделяне на фърмуер	Посочва IP адреса и порта, където да се изпращат UDP съобщенията. Например: 10.98.76.123:514, където 10.98.76.123 е IP адресът, а 514 е номерът на порта.

Параметри с общо предназначение

Следващата таблица дефинира функцията и използването на всеки от параметрите в секцията **Параметри с общо предназначение** на раздела **Обезпечаване**.

Име на параметъра	Описание на стойността по подразбиране
GPP A - GPP P	Параметрите с общо предназначение GPP_* се използват като свободни регистри на низове при конфигуриране на телефона да взаимодейства с конкретно решение на сървър за обезпечаване. Те могат да се конфигурират така, че да съдържат различни стойности, включително следните: • Ключове за шифроване: • URL. • Информация за състоянието при обезпечаване с много стъпки. • Шаблони за последваща заявка. • Карти на псевдонимите на име на параметър. • Частични стойности на низове, евентуално комбинирани в пълни параметрични стойности. Стойността по подразбиране е празно поле.

Променливи за макро разширение

В следните параметри за обезпечаване се различават определени макро променливи:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*

- Upgrade_Rule
- Log_*
- GPP_* (при специфични условия)

В тези параметри типовете синтаксис, като $NAME или $(NAME), се разпознават и разширяват.

Низовете на променливите на макросите могат да се посочат с нотацията $(NAME:p) и $(NAME:p:q), където p и q са неотрицателни цели числа (предлага се във версия 2.0.11 и следващи). Полученият макро израз е подниз, започващ с отместване от буквата p, с дължина q (или до края на низа, ако q не е посочено). Например, ако GPP_A съдържа ABCDEF, то $(A:2) се разширява до CDEF, а $(A:2:3) се разширява до CDE.

Неразпознатото име не се превежда, а формата $NAME или $(NAME) остава непроменена в стойностите на параметрите след израза.

Име на параметъра	Описание на стойността по подразбиране
$	формата $$ се разширява до един знак $.
A до P	Заменя се от съдържанието на параметрите с общо предназначение GPP_A до GPP_P.
SA до SD	Заменя се от параметрите за специална цел GPP_SA до GPP_SD. Тези параметри носят ключове или пароли, използвани в обезпечаването. **Забележка** $SA до $SD се разпознават като аргументи на предлагания като опция URL квалификатор за повторно синхронизиране, --key.
MA	MAC адрес при използване на шестнадесетични цифри с малки букви. Например 000e08aabbcc.
MAU	MAC адрес при използване на големи шестнадесетични цифри. Например 000E08AABBCC.
MAC	MAC адрес при използване на малки шестнадесетични цифри и двуеточия за разделяне на цифровите двойки. Например 00:0e:08:aa:bb:cc.
PN	Име на продукт. Например CP-6841-3PCC.
PSN	Сериен номер на продукта. Например 6841-3PCC.
SN	Низ на серийния номер. Например 88012BA01234.

Име на параметъра	Описание на стойността по подразбиране
CCERT	Състояние на сертификата на SSL клиент: Инсталиран или не инсталиран.
IP	IP адрес на телефона в местната подмрежа. Например 192.168.1.100.
EXTIP	Външен IP на телефона, както се вижда от интернет. Например 66.43.16.52.
SWVER	Низ на софтуерната версия. Например sip68xx.11-0-1MPP.
HWVER	Низ на хардуерната версия. Например 2.0.1
PRVST	Състояние на обезпечаване (цифров низ): -1 = изрична заявка за повторно синхронизиране 0 = повторно синхронизиране при включване на захранването 1 = периодично повторно синхронизиране 2 = неуспешно повторно синхронизиране, повторен опит
UPGST	Състояние на надграждане (цифров низ): 1 = първи опит за надграждане 2 = неуспешно надграждане, повторен опит
UPGERR	Съобщение с резултат (ERR) от предишен опит за надграждане; например неуспех на http_get.
PRVTMR	Секунди след последния опит за повторно синхронизиране.
UPGTMR	Секунди след последния опит за надграждане.
REGTMR1	Секунди след загуба на регистрацията на SIP сървъра на линия 1.
REGTMR2	Секунди след загуба на регистрацията на SIP сървъра на линия 2.
UPGCOND	Старо име на макрос.
SCHEME	Схема за достъп до файл, един от TFTP, HTTP или HTTPS, както е получен след повторно синхронизиране за синтактичен анализ или надграждане на URL.

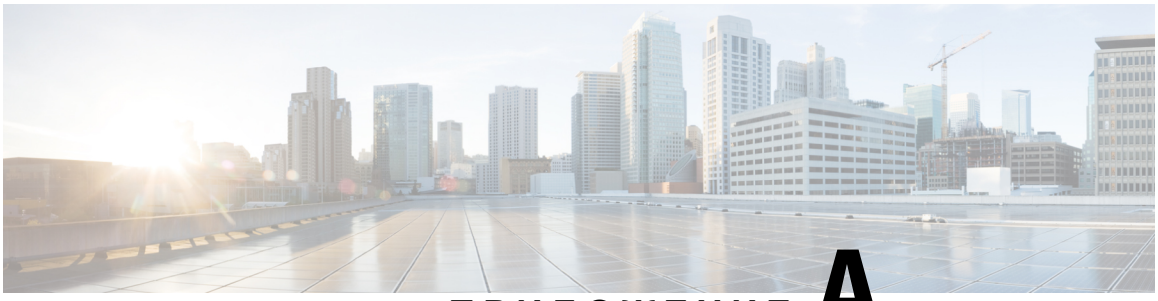
Име на параметъра	Описание на стойността по подразбиране
SERV	Изискайте името на хоста на целевия сървър, както е получен след повторното синхронизиране за синтактичен анализ или надграждането на URL.
SERVIP	Изискайте IP адреса на целевия сървър, както се получава след повторното синхронизиране за синтактичен анализ или надграждане на URL, като следвате търсенето на DNS.
PORT	Изискайте порта UDP/TCP, както е получен след повторното синхронизиране за синтактичен анализ или надграждането на URL.
PATH	Изискайте пътя на целевия файл, както е получен след повторното синхронизиране за синтактичен анализ или надграждането на URL.
ERR	Съобщение за резултата от повторно синхронизиране или опит за надграждане. Полезно е само при генериране на съобщения с резултат от syslog. Стойността се запазва в променливата UPGERR в случай на опити за надграждане.
UIDn	Съдържанието на реда n в конфигурационния параметър UserID.
EMS	Състояние на разширена мобилност
MUID	Потребителски ИД за разширена мобилност
MPWD	Парола за разширена мобилност

Вътрешни кодове за грешка

Телефонът дефинира редица кодове за вътрешна грешка (X00–X99), за да подпомогне конфигурирането при осигуряване на по добър контрол на поведението на модула при определени условия на грешка.

Име на параметъра	Описание на стойността по подразбиране
X00	Грешка в транспортния слой (или ICMP) при изпращане на заявка за SIP.
X20	Времето за изчакване на заявката за SIP изтича при изкачване на отговор.

Име на параметъра	Описание на стойността по подразбиране
X40	Обща грешка в SIP протокола (например недостъпен код в SDP в 200 и съобщенията ACK или изтичане на времето за изчакване при изчакване на ACK).
X60	Набраният номер е невалиден в съответствие с дадения план за избиране.



ПРИЛОЖЕНИЕ A

Примерни профили за конфигуриране

Пример с XML във формат Open

```
<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>
```

Примерни профили за конфигуриране

```
<!--  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>
```

Примерни профили за конфигуриране

```
<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>
```

Примерни профили за конфигуриране

```
<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>
```

Примерни профили за конфигуриране

```
<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>
```

Примерни профили за конфигуриране

```
<!--
 available options:
[illegible]

-->
<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  -->
```

Примерни профили за конфигуриране

```
<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>
```

Примерни профили за конфигуриране

```
<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
```

Примерни профили за конфигуриране

```
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  -->
```

Примерни профили за конфигуриране

```
<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_>
```

Примерни профили за конфигуриране

```
<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_>
```

Примерни профили за конфигуриране

```
<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_>
```

Примерни профили за конфигуриране

```
<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"/>
```

Примерни профили за конфигуриране

```
 <!--  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_>
```

Примерни профили за конфигуриране

```
<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
```

Примерни профили за конфигуриране

```
-->
<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
-->
```

Примерни профили за конфигуриране

```
<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"/>
```

Примерни профили за конфигуриране

```
 <!--  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"/>
```

Примерни профили за конфигуриране

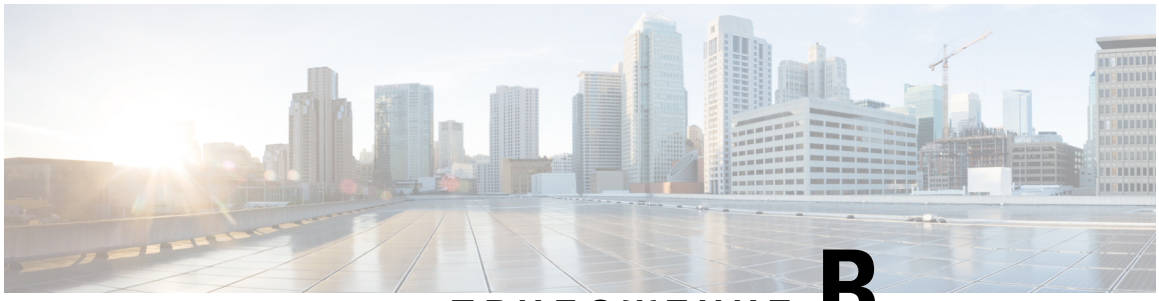
```
<Cfwd_No_Ans_Dest ua="rw"/>
<Cfwd_No_Ans_Delay ua="rw">20</Cfwd_No_Ans_Delay>
 <!--  Speed Dial  -->
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name 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  -->
```

Примерни профили за конфигуриране

```
<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"/>
```

Примерни профили за конфигуриране

```
 <!--  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>
```



ПРИЛОЖЕНИЕ B

Акроними

Акроними

AC	Променлив ток
ACS	Сървър за управление на достъпа
A/D	Аналогово-цифров преобразовател
AES	Разширен стандарт за шифроване
ANC	Анонимно повикване
AP	Точка за достъп
ASCII	Американски стандартен код за обмен на информация
B2BUA	Потребителски агент от край до край
състояние на линията	Поле с лампа за заето повикване
Bool	Булева стойност Показва се като да или не или като 1 и 0 в профила
BootP	Протокол за първоначално зареждане
CA	Орган за издаване на сертиф
CAS	Сигнал за предупреждение CPE
CDP	Cisco Discovery Protocol
CDR	Запис за подробности относно повикването
CGI	Генериран от компютър Mmagery
CID	ИД на търсеща страна

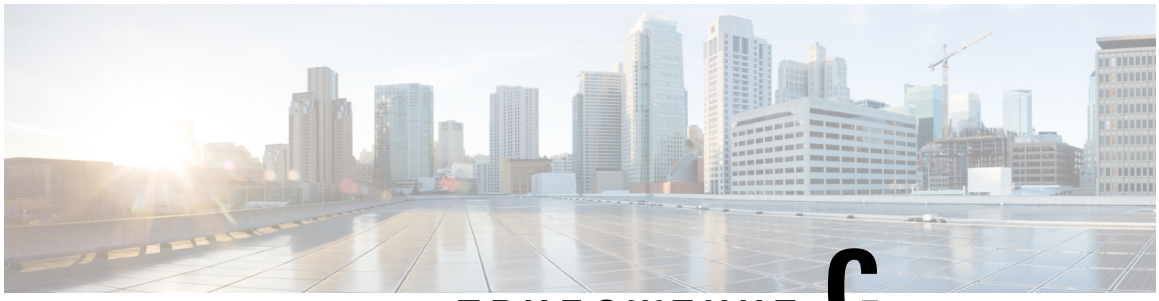
CIDCW	ИД на повикващ при изчакване на повикване
CNG	Генериране на комфортен шум
CPC	Управление на повикващата страна
CPE	Оборудване в помещението на клиента
CSV	Стойности, разделени от запетаи
CWCID	ИД на повикващ при изчакване на повикване
CWT	Тон за изчакване на повикване
D/A	Цифрово-аналогов преобразовател
dB	децибел
dBm	dB по отношение на 1 миливат
DHCP	Протокол за динамично конфигуриране на хост
Не ме безпокойте	НеМеБезпокой
DNS	Система от имена на домейни
DoS	Отказ на услуга
DRAM	Динамична памет за произволен достъп
DSL	Цикъл на цифром абонат
DSP	Процесор на цифрови сигнали
DST	Лятно часово време
DTAS	Предупредителен сигнал на терминал за данни (също като CAS)
DTMF	Множествена честота на двоен тон
FQDN	Напълно квалифицирано име на домейн
FSK	Манипулация по повдигане на честотата
FW	Фърмуер
FXS	Станция на Foreign eXchange
GMT	Гринуич
GW	Шлюз
HTML	Език за маркиране на хипертекст
HTTP	Протокол за прехвърляне на хипертекст

HTTPS	HTTP през SSL
ICMP	Протокл за контролни съобщения в интернет
IGMP	Протокол за управление на групи в интернет
ILEC	Изпълнителен оператор на местен обмен
IP	Интернет протокол
IPv4	Internet Protocol версия 4
IPv6	Internet Protocol версия 6
ISP	Доставчик на интернет
ITSP	Доставчик на интернет телефония
ITU	Международен съюз по телекомуникации
IVR	Интерактивен гласов отговор
LAN	Локална мрежа
LBR	Ниска битова скорост
LBRC	Кодек с ниска битова скорост
LCD	Дисплей с течни кристали, известен още като екран
LDAP	Lightweight Directory Access Protocol
СВЕТЛИННИ ИНДИКАТОРИ	Светодиод
MAC адрес	Адрес за управление на достъпа до медии
MC	Мини сертификат
MGCP	Контролен протокол за медиен шлюз
MOH	Музика при задържане
MOS	Резултат от средно мнение (1-5, колкото по-висок, толкова по-добре)
MPP	Многоплатформени телефони
мс	Милисекунда
MSA	Адаптер на музикален източник
MWI	Индикация за изчакване на съобщение
NAT	Превеждане на мрежов адрес
NPS	Обикновен сървър за обезпечаване

NTP	Мрежов протокол за време
OOB	Извън лентата
OSI	Интервал на отворено превключване
PBX	Обмен на частен клон
PCB	Печатна платка
PoE	Захранване по Ethernet
PR	Обръщане на полярността
PS	Сървър за обезпечаване
PSQM	Перцептуално управление на качеството на речта (1-5, колкото по-ниска, толкова по-добре)
PSTN	Обществено превключвана телефонна мрежа
QoS	Качество на услугата
RC	Отстраняване на персонализирането
REQT	(SIP) Съобщение за заявка
RESP	(SIP) Съобщение-отговор
RSC	(SIP) Код за състояние на отговора, като 404, 302, 600
RTP	Протокол в реално време
RTT	Време за преминаване през сегмента
SAS	Сървър за поточно предаване на звук
SDP	Протокол за описание на сесия
SDRAM	Синхронен DRAM
sec	секунди
SIP	Протокол за стартиране на сесия
SLA	Изглед на споделена линия
SLIC	Интерфейсна верига на линията на абоната
SP	Доставчик на услуги
SSL	Secure Socket Layer
STUN	Сесия Traversal UDP за NAT
TCP	Протокол за управление на предаването

TFTP сървър	Елементарен протокол за предаване на файлове
TLS	Защита на транспортния слой
TTL	Време за активност
ToS	Вид на услугата
UA	Потребителски агент
uC	Микроконтролер
UDP	Протокол за дейтаграма на потребителя
URI	Идентификатор на еднакви ресурси
URL адрес	Унифициран локатор на ресурси
UTC	Коокридинано унидерсално време
РАЗЛИЧНИ	Търговец с добавена стойност
VLAN	Гласов LAN
VM	Гласова поща
VMWI	Индикация/индикатор за изчакване на визуално съобщение
VoIP	Глес през Internet Protocol
VQ	Качество на гласа
WAN	Регионална мрежа
XML	Разширяем език за маркиране

Акроними



ПРИЛОЖЕНИЕ C

Сродни документи

Сродни документи

Използвайте следващите раздели, за да получите съответна информация.

Документация на серията Cisco IP Phone 6800

Вижте публикациите на вашия език, модела на телефона и изданието на многоплатформения фърмуер. Придвижете се от следния локатор за унифицирани ресурси (URL):

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

Политика за поддръжка на фърмуер за Cisco IP Phone

За информация относно политиката за поддръжка на телефони вижте https://cisco.com/go/phonefirmwaresupport.