# Przewodnik obsługi administracyjnej wieloplatformowych telefonów Cisco IP Phone z serii 6800

**Pierwsza publikacja:** 2017-11-22

**Ostatnia modyfikacja:** 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.

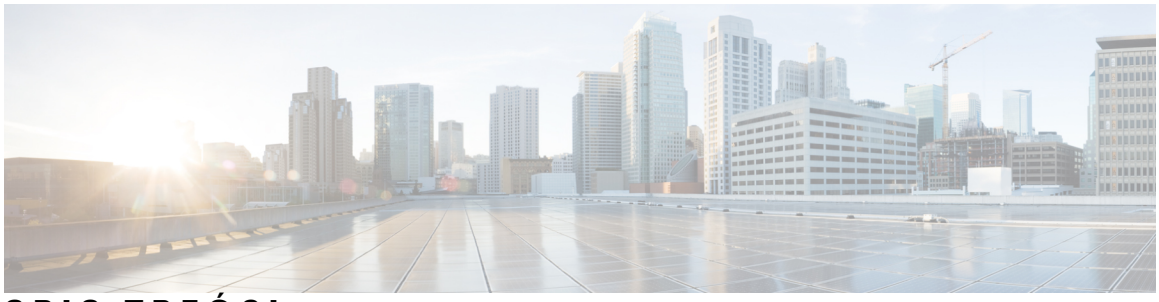
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

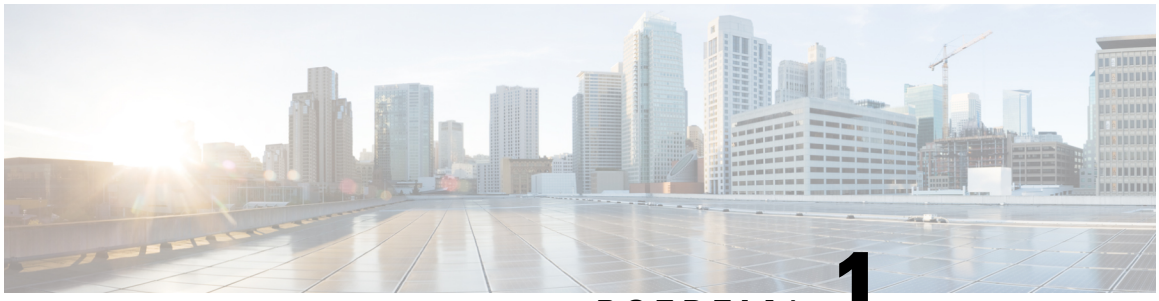
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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)



# SPIS TREŚCI



ROZDZIAŁ 1

# Wdrażanie i obsługa administracyjna



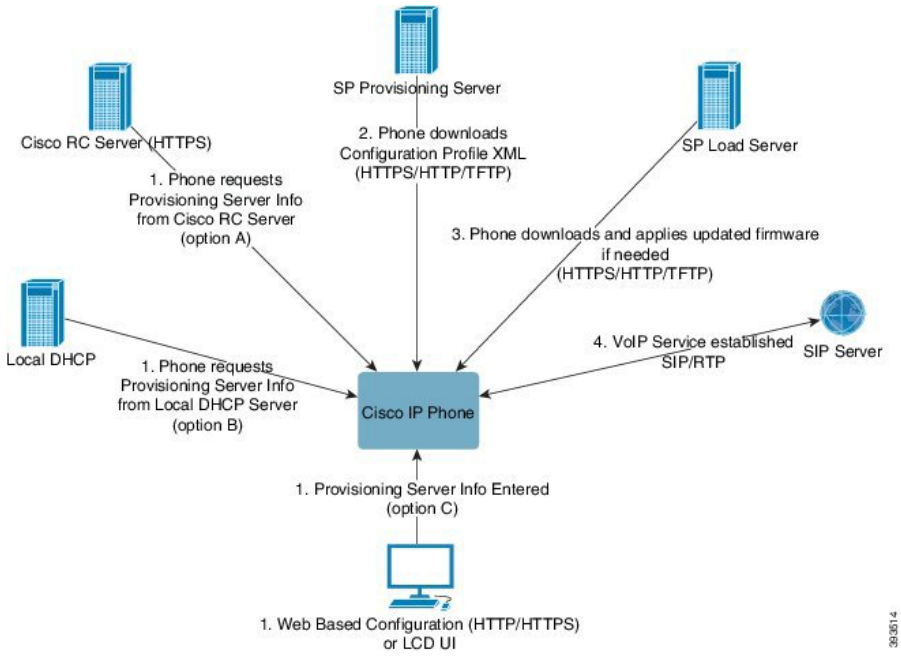
## Obsługa administracyjna — omówienie

Telefony Cisco IP Phone są przeznaczone do masowego wdrażania przez dostawców usług Voice over IP (VoIP) u klientów w domach, organizacjach i przedsiębiorstwach. W związku z tym obsługa administracyjna przy użyciu funkcji zdalnego zarządzania i konfigurowania zwiększa szanse na prawidłowe działanie telefonów w obiektach klientów.

Cisco wspiera ustawiczne niestandardowe konfigurowanie funkcji telefonu za pomocą następujących mechanizmów:

- Niezawodne zdalne sterowanie telefonem.
- Szyfrowanie komunikatów sterujących telefonem.
- Zoptymalizowane łączenie z kontem telefonu.

W ramach obsługi administracyjnej na telefonach można ustawić pobieranie profili konfiguracji lub zaktualizowanego oprogramowania sprzętowego ze zdalnego serwera. Pobieranie może następować po podłączeniu telefonów do sieci, ich włączeniu i w ustalonych odstępach czasu. Zazwyczaj obsługa administracyjna jest elementem masowych wdrożeń rozwiązań VoIP powszechnie realizowanych przez dostawców usług. Profile konfiguracji lub zaktualizowane oprogramowanie sprzętowe jest przesyłane do urządzeń przy użyciu protokołu TFTP, HTTP lub HTTPS.




Na poziomie ogólnym proces obsługi administracyjnej telefonu przebiega następująco:

1. Jeśli telefon nie jest skonfigurowany, informacje z serwera obsługi administracyjnej są wprowadzane do telefonu przy użyciu jednej z następujących opcji:
   - **A —** pobranie z serwera zdalnego dostosowywania (RC) Cisco Enablement Data Orchestration System (EDOS) za pośrednictwem protokołu HTTPS.
   - **B —** wysłanie zapytania do lokalnego serwera DHCP.
   - **C —** ręczne wprowadzenie przy użyciu internetowego narzędzia konfiguracji telefonów Cisco lub interfejsu użytkownika telefonu.
2. Telefon pobiera informacje z serwera obsługi administracyjnej i stosuje kod źródłowy XML konfiguracji przy użyciu protokołu HTTPS, HTTP lub TFTP.
3. W razie potrzeby telefon pobiera i wdraża zaktualizowane oprogramowanie sprzętowe za pośrednictwem protokołu HTTPS, HTTP lub TFTP.
4. Usługa VoIP jest ustanawiana przy użyciu podanej konfiguracji i oprogramowania sprzętowego.

Dostawcy usług VoIP wdrażają wiele telefonów u klientów indywidualnych i w małych firmach. W firmach i przedsiębiorstwach telefony mogą pełnić rolę węzłów końcowych. Usługodawcy rozprowadzają te urządzenia przez Internet, a klienci podłączają je u siebie przez routery i zapory.

Telefon może funkcjonować jako zdalne rozszerzenie systemów zaplecza dostawcy usług. Zdalne zarządzanie i konfigurowanie zwiększa szanse na prawidłowe działanie telefonów w siedzibach klientów.

# Obsługa administracyjna przy użyciu protokołu TR69

Telefon Cisco IP Phone umożliwia administratorowi konfigurowanie parametrów protokołu TR69 za pomocą internetowego interfejsu użytkownika. Informacje związane z parametrami, w tym porównanie parametrów języka XML i specyfikacji TR69, można znaleźć w Podręczniku administratora odpowiedniej serii telefonów.

Telefony obsługują wykrywanie danych serwera automatycznej konfiguracji (ACS) przy użyciu opcji DHCP 43, 60 i 125.

- Opcja 43 — Informacje o adresie URL serwera ACS specyficzne dla dostawcy.
- Opcja 60 — Identyfikator klasy dostawcy umożliwiający telefonowi identyfikowanie się na stronie `dslforum.org` wobec serwera ACS.
- Opcja 125 — Informacje o skojarzeniu bramy specyficzne dla dostawcy.

## Metody RPC

### Obsługiwane metody RPC

Telefony obsługują tylko ograniczony zestaw metod zdalnego wywoływania procedur (RPC):

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: obsługiwane są następujące typy plików:
  - Obraz uaktualnienia oprogramowania sprzętowego
  - Plik konfiguracyjny dostawcy
  - Plik niestandardowego urzędu certyfikacji (CA)
- Transfer Complete

## Obsługiwane typy zdarzeń

Typy zdarzeń obsługiwanych w telefonach zależą od używanych funkcji i metod. Obecnie są obsługiwane są następujące typy zdarzeń:

- Ładowanie początkowe
- Rozruch
- Zmiana wartości
- Żądanie połączenia
- Okresowe
- Przesyłanie zakończone
- M Pobieranie
- M Ponowne uruchomienie

# Działanie telefonu w okresach dużego obciążenia sieci

- zadania administracyjne, np. skanowanie portów wewnętrznych czy skanowanie zabezpieczeń,
- ataki na sieć, np. ataki typu „odmowa usługi".

# Wdrożenie

Telefony Cisco IP Phone udostępniają wygodny mechanizm obsługi administracyjnej oparty na następujących modelach wdrożenia:

- Dystrybucja zbiorcza — dostawca usług kupuje dużą liczbę telefonów Cisco IP Phone, a następnie dokonuje ich wstępnej obsługi administracyjnej wewnętrznie albo kupuje od Cisco jednostki zdalnego dostosowania (RC). Następnie urządzenia są wydawane klientom w ramach umowy na usługę VoIP.
- Dystrybucja detaliczna — klient kupuje telefon Cisco IP Phone w sklepie detalicznym i zamawia usługę VoIP u dostawcy usług. Wtedy dostawca usług musi zapewnić bezpieczne zdalne skonfigurowanie urządzenia.

## Dystrybucja zbiorcza

W tym modelu dostawca usług przekazuje klientom telefony w ramach umowy o świadczenie usługi VoIP. Urządzenia są zdalnie sterowane lub wstępna obsługa administracyjna jest przeprowadzana lokalnie (w sieci wewnętrznej).

Cisco zapewnia wstępną obsługę administracyjną zdalnych urządzeń w celu zapewnienia ich synchronizacji z serwerem Cisco, który będzie pobierał profile urządzeń i aktualizacje ich oprogramowania sprzętowego.

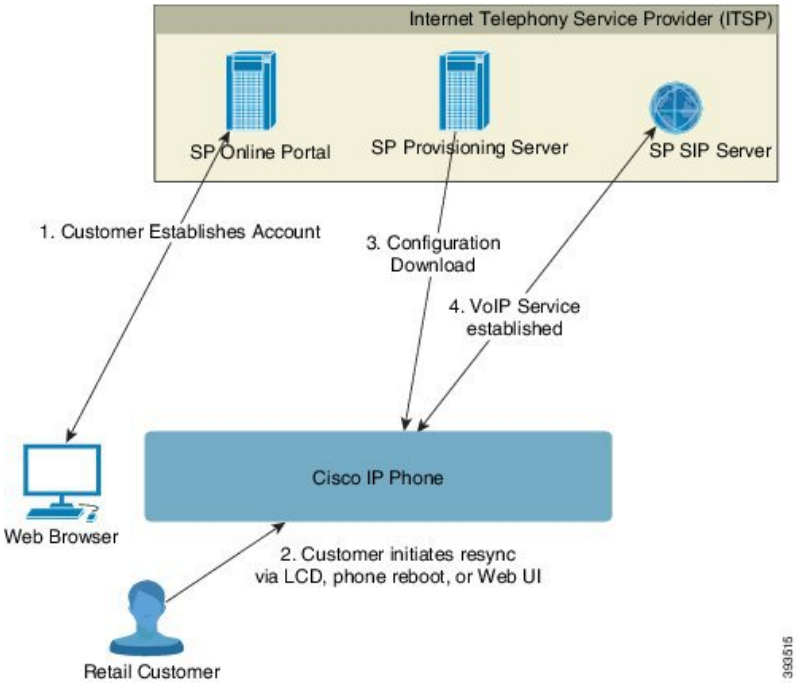
Dostawca usług może wstępnie skonfigurować w telefonach żądane parametry, w tym parametry sterujące ponowną synchronizacją, przy użyciu różnych metod:

- W sieci wewnętrznej przy użyciu protokołów DHCP i TFTP
- Zdalnie przy użyciu protokołu TFTP, HTTP lub HTTPS
- Połączenie lokalnej i zdalnej obsługi administracyjnej

# Dystrybucja detaliczna

W modelu dystrybucji detalicznej klient kupuje telefon i subskrybuje określoną usługę. Dostawca usług telefonii internetowej (ITSP) konfiguruje i utrzymuje serwer obsługi administracyjnej oraz dokonuje wstępnej obsługi administracyjnej telefonu, tak aby synchronizował się z serwerem u dostawcy usług.

***Rysunek 1: Dystrybucja detaliczna***




Telefon zawiera internetowe narzędzie konfiguracyjne, które pokazuje wewnętrzną konfigurację i przyjmuje nowe wartości parametrów konfiguracyjnych. Ponadto serwer akceptuje specjalną składnię poleceń z adresami URL, które służą do ponownej synchronizacji zdalnego profilu i uaktualniania oprogramowania sprzętowego.

Klient loguje się w usłudze i tworzy konto VoIP, często przez portal internetowy, a następnie wiąże urządzenie z przypisanym kontem usługi. Telefon bez obsługi administracyjnej otrzymuje instrukcję ponownej synchronizacji z konkretnym serwerem obsługi administracyjnej przy użyciu polecenia z adresem URL ponownej synchronizacji. Polecenie z adresem URL zwykle zawiera numer identyfikacyjny lub kod alfanumeryczny klienta, który kojarzy urządzenie z nowym kontem.

W przykładzie poniżej do urządzenia o adresie IP 192.168.1.102, który został przypisany przez serwer DHCP, jest wysyłana instrukcja włączenia obsługi administracyjnej usługi SuperVoIP:

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

W tym przykładzie numerem identyfikacyjnym klienta na nowym koncie jest 1234abcd. Zdalny serwer obsługi administracyjnej kojarzy telefon wykonujący żądanie ponownej synchronizacji z nowym kontem na podstawie adresu URL i podanego identyfikatora klienta. Dzięki tej początkowej operacji ponownej synchronizacji telefon został skonfigurowany w jednym kroku. Odtąd telefon będzie automatycznie kierowany do ponownej synchronizacji ze stałym adresem URL na serwerze. Na przykład:

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

Zarówno przy dostępie początkowym, jak i trwałym serwer wykonuje uwierzytelnianie za pomocą certyfikatu klienta zainstalowanego w telefonie. Serwer obsługi administracyjnej przekazuje odpowiednie wartości parametrów konfiguracyjnych na podstawie skojarzonego konta usługi.

Podczas włączania lub po upływie określonego czasu telefon synchronizuje się ponownie i pobiera najnowsze parametry. Te parametry mogą służyć celom takim jak skonfigurowanie grupy poszukiwania, ustawienie numerów szybkiego wybierania czy ograniczenie użytkownikowi możliwości edytowania funkcji.

**Tematy pokrewne**

Wstępna obsługa administracyjna w sieci wewnętrznej, na stronie 42

## Proces ponownej synchronizacji

Oprogramowanie sprzętowe każdego telefonu zawiera administracyjny serwer WWW, który akceptuje nowe wartości parametrów konfiguracyjnych. Polecenie z adresem URL ponownej synchronizacji zawarte w profilu urządzenia może wymuszać ponowne synchronizowanie konfiguracji z konkretnym serwerem obsługi administracyjnej po restarcie telefonu lub w zaplanowanych odstępach czasu.

Domyślnie serwer WWW jest włączony. Aby wyłączyć lub włączyć serwer WWW, użyj polecenia z adresem URL ponownej synchronizacji.

W razie potrzeby adres URL z operacją „resync” może służyć do natychmiastowego żądania ponownej synchronizacji. Polecenie z adresem URL ponownej synchronizacji może zawierać numer identyfikacyjny lub kod alfanumeryczny klienta, który jednoznacznie kojarzy urządzenie z kontem użytkownika.

**Przykład.**

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

W tym przykładzie do urządzenia o adresie IP 192.168.1.102, który został przypisany przez serwer DHCP, jest wysyłana instrukcja włączenia obsługi administracyjnej usługi SuperVoIP działającej na serwerze prov.supervoip.com. Numerem identyfikacyjnym klienta na nowym koncie jest 1234abcd. Zdalny serwer obsługi administracyjnej kojarzy telefon wykonujący żądanie ponownej synchronizacji z kontem na podstawie adresu URL i identyfikatora klienta.

Dzięki tej początkowej operacji ponownej synchronizacji telefon został skonfigurowany w jednym kroku. Odtąd telefon będzie automatycznie kierowany do ponownej synchronizacji ze stałym adresem URL na serwerze.

Zarówno przy dostępie początkowym, jak i trwałym serwer wykonuje uwierzytelnianie za pomocą certyfikatu klienta. Serwer przekazuje wartości parametrów konfiguracyjnych na podstawie skojarzonego konta usługi.

# Dostarczanie

W telefonie można skonfigurować ponowne synchronizowanie wewnętrznego stanu konfiguracji ze zdalnym profilem okresowo oraz podczas włączania zasilania. Telefon kontaktuje się ze standardowym serwerem obsługi administracyjnej (NPS) z lub serwerem kontroli dostępu (ACS).

Domyślnie ponowna synchronizacja profilu następuje tylko w czasie, gdy telefon jest bezczynny. Takie rozwiązanie zapobiega uaktualnianiu, które mogłoby spowodować ponowne uruchomienie programowe i rozłączenie połączenia. Jeśli są konieczne pośrednie uaktualnienia w celu osiągnięcia przyszłego stanu uaktualnienia ze starszej wersji, mechanizm uaktualniania może zautomatyzować takie uaktualnianie wielostopniowe.

## Standardowy serwer obsługi administracyjnej

Standardowym serwerem obsługi administracyjnej (Normal Provisioning Server, NPS) może być serwer TFTP, HTTP lub HTTPS. Zdalne uaktualnianie oprogramowania sprzętowego może być wykonywane przy użyciu protokołu TFTP, HTTP lub HTTPS, ponieważ oprogramowanie sprzętowe nie zawiera wrażliwych informacji.

Zalecany jest protokół HTTPS, jednak komunikacja z serwerem NPS nie wymaga używania bezpiecznego protokołu, ponieważ zaktualizowany profil może być szyfrowany kluczem współdzielonym. Aby uzyskać więcej informacji na temat używania protokołu HTTPS, zobacz Szyfrowanie komunikacji, na stronie 9. Obsługa administracyjna jest bezpiecznie inicjowana za pomocą mechanizmu wykorzystującego funkcje protokołu SSL. Telefon bez obsługi administracyjnej może odebrać profil szyfrowany 256-bitowym kluczem symetrycznym przeznaczony dla tego konkretnego urządzenia.

## Kontrola dostępu do konfiguracji

Oprogramowanie sprzętowe telefonu zawiera mechanizmy ograniczające użytkownikom końcowym dostęp do niektórych parametrów. Konta **Admin** i **Użytkownik** mają różne uprawnienia. Każde konto może być niezależnie chronione hasłem.

- Konto Admin — umożliwia dostawcy usług pełny dostęp do wszystkich parametrów administracyjnego serwera WWW.
- Konto Użytkownik — ma uprawnienia do konfigurowania wybranych parametrów administracyjnego serwera WWW.

Dostawca usług może w profilu obsługi administracyjnej ograniczyć funkcjonalność konta użytkownika w następujący sposób:

- Wskazać, które parametry konfiguracyjne są dostępne na koncie użytkownika podczas tworzenia konfiguracji.
- Wyłączyć użytkownikowi dostęp do administracyjnego serwera WWW.
- Wyłączyć użytkownikowi dostęp do interfejsu użytkownika na wyświetlaczu LCD.
- Pominąć wyświetlanie użytkownikowi ekranu **Ustawianie hasła**.

- Ograniczyć zbiór domen internetowych dostępnych z urządzenia na potrzeby ponownej synchronizacji, uaktualniania lub rejestracji SIP na linii 1.

### Tematy pokrewne

Właściwości znaczników elementów, na stronie 14
Kontrola dostępu, na stronie 16

## Otwieranie strony WWW telefonu

Przejdź do strony WWW telefonu z przeglądarki internetowej na komputerze, który ma dostęp do telefonu w podsieci.

Jeśli dostawca usług wyłączył dostęp do narzędzia konfiguracji, poproś go o zmianę ustawień.

### Procedura

**Krok 1** Upewnij się, że komputer ma połączenie z telefonem. Nie używaj sieci VPN.

**Krok 2** Uruchom przeglądarkę WWW.

**Krok 3** Wpisz adres IP telefonu na pasku adresu w przeglądarce.

- Dostęp użytkownika: **`http://<adres ip>/user`**
- Dostęp administratora: **`http://<adres ip>/admin/advanced`**
- Dostęp administratora: **`http://<adres ip>`**, kliknij opcję **Logowanie się administratora**, a następnie opcję **Zaawansowane** (Advanced).

Na przykład: `http://10.64.84.147/admin`

## Umożliwianie dostępu do telefonu Cisco IP Phone przez Internet

Aby wyświetlić parametry telefonu, należy włączyć profil konfiguracji. Wprowadzanie jakichkolwiek modyfikacji parametrów wymaga zmiany konfiguracji profilu. Być może administrator systemu wyłączył w telefonie opcję umożliwiającą użytkownikom wyświetlanie interfejsu WWW telefonu i zapisywanie w nim.

Aby uzyskać więcej informacji, zobacz *Przewodnik obsługi administracyjnej wieloplatformowych telefonów Cisco IP Phone 6800 Series*.

### Zanim rozpoczniesz

Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

### Procedura

**Krok 1** Kliknij kolejno opcje **Głos (Voice)** > **System**.

**Krok 2** W części **Konfiguracja systemu** (System Configuration) w parametrze **Włącz serwer WWW** (Enable Web Server) ustaw wartość **Tak** (Yes).

**Krok 3** Aby zaktualizować profil konfiguracji, zmodyfikuj pola w interfejsie WWW telefonu, a następnie kliknij przycisk **Prześlij wszystkie zmiany** (Submit All Changes).

Telefon zostanie ponownie uruchomiony, a zmiany — zastosowane.

**Krok 4** Aby wyczyścić wszystkie zmiany wprowadzone w trakcie bieżącej sesji (lub po ostatnim kliknięciu przycisku **Prześlij wszystkie zmiany**), kliknij przycisk **Cofnij wszystkie zmiany** (Undo All Changes). Spowoduje to przywrócenie poprzednich wartości ustawień.

# Szyfrowanie komunikacji

Parametry konfiguracyjne przekazywane do urządzenia mogą zawierać kody uwierzytelnienia i inne informacje, które chronią system przed nieautoryzowanym dostępem. W interesie dostawcy usług leży zapobieganie niedozwolonym działaniom użytkowników. Z kolei w interesie użytkownika leży zapobieganie nieuprawnionemu korzystaniu z jego konta. Dostawca usług może szyfrować przesyłanie danych profilu konfiguracji między serwerem obsługi administracyjnej a urządzeniem oraz ograniczyć dostęp do administracyjnego serwera WWW.

# Zasady obsługi administracyjnej telefonu

Zazwyczaj telefon Cisco IP Phone otrzymuje obsługę administracyjną, gdy po raz pierwszy nawiązuje połączenie z siecią. Ponadto obsługa jest inicjowana w zaplanowanych odstępach czasu ustawionych przez dostawcę usług albo dostawca VAR dokonuje wstępnej obsługi administracyjnej (skonfigurowania) telefonu. Dostawcy usług mogą upoważnić dostawców VAR lub zaawansowanych użytkowników do wykonywania ręcznej obsługi administracyjnej za pomocą klawiatury telefonu. Wreszcie obsługi administracyjnej można dokonywać w internetowym interfejsie użytkownika telefonu.

Obejrzyj wartość pola **Stan** > **Stan telefonu (Phone Status)** > **Obsługa administracyjna (Provisioning)** w interfejsie użytkownika na wyświetlaczu LCD telefonu lub pola Stan obsługi administracyjnej (Provisioning Status) na karcie **Stan** w internetowym narzędziu konfiguracyjnym.

### Tematy pokrewne

Ręczna obsługa administracyjna telefonu przy użyciu klawiatury, na stronie 9

# Ręczna obsługa administracyjna telefonu przy użyciu klawiatury

### Procedura

**Krok 1** Naciśnij przycisk **Aplikacje** .

**Krok 2** Wybierz kolejno opcje **Administrowanie urządzeniem (Device administration)** > **Reguła profilu (Profile Rule)**.

**Krok 3** Wprowadź regułę profilu w następującym formacie:

```
protokół://serwer[:port]/ścieżka_pliku_profilu
```

Na przykład:

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

Jeśli protokół nie zostanie podany, domyślnie będzie używany protokół TFTP. Jeśli nazwa serwera nie zostanie podana, jego rolę będzie pełnił host żądający adresu URL. Jeśli port nie zostanie podany, będzie używany port domyślny (69 w protokole TFTP, 80 w protokole HTTP lub 443 w protokole HTTPS).

**Krok 4** Naciśnij przycisk **Ponów synch.**

**Tematy pokrewne**

Zasady obsługi administracyjnej telefonu, na stronie 9

# Równy dostęp do firmware

Równy dostęp do oprogramowania sprzętowego (PFS) to model dystrybucji oprogramowania sprzętowego, który umożliwia telefonowi Cisco IP Phone znalezienie w podsieci innych telefonów o tym samym modelu lub serii oraz udostępnienie zaktualizowanych plików oprogramowania sprzętowego; w ten sposób można odświeżyć wiele telefonów równocześnie. Model PFS używa autorskiego protokołu Cisco o nazwie Cisco Peer-to-Peer-Distribution Protocol (CPPDP). Dzięki protokołowi CPPDP wszystkie urządzenia w podsieci tworzą hierarchię równorzędną, a następnie kopiują między sobą oprogramowanie sprzętowe lub inne pliki. Aby zoptymalizować proces aktualizacji oprogramowania sprzętowego, telefon główny pobiera obraz tego oprogramowania z serwera pobierania, a następnie przesyła je do innych telefonów w podsieci przez połączenia TCP.

Równy dostęp do firmware:

- Ogranicza przeciążenie przy transferach TFTP ze scentralizowanych zdalnych serwerów pobierania.
- Likwiduje konieczność ręcznego sterowania uaktualnieniami oprogramowania firmware.
- Skraca niedostępność telefonów spowodowaną jednoczesnym zresetowaniem wielu telefonów.

**Uwaga**

- Model Równy dostęp do oprogramowania sprzętowego działa tylko wtedy, gdy uaktualnianie zostanie skonfigurowane na więcej niż jednym telefonie w tym samym czasie. Wysłanie żądania NOTIFY z atrybutem Event:resync inicjuje ponowną synchronizację w telefonie. Oto przykładowy plik XML, który może zawierać konfigurację inicjowania uaktualnienia:

  "**Event:resync;profile="**http://10.77.10.141/profile.xml
- Gdy ustawisz adres IP i port serwera dziennika mechanizmu równego dostępu do oprogramowania sprzętowego, dzienniki zdarzeń funkcji PFS będą wysyłane do tego serwera jako wiadomości UDP. To ustawienie należy skonfigurować na każdym telefonie. Komunikatów dziennika można następnie używać podczas rozwiązywania problemów z modelem PFS.

Parametr Peer_Firmware_Sharing_Log_Server określa nazwę hosta i port zdalnego serwera dziennika systemu używającego protokołu UDP. Domyślnie jest to port 514.

Na przykład:

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

Aby używać funkcji PFS, należy ją włączyć w telefonach.

# Pomijanie ekranu Ustawianie hasła

Istnieje możliwość pomijania ekranu **Ustawianie hasła** w telefonie podczas pierwszego rozruchu lub po przywróceniu do ustawień fabrycznych, muszą być jednak wykonane następujące czynności konfiguracyjne:

- Konfiguracja usługi DHCP
- Konfiguracja systemu EDOS
- Konfiguracja hasła użytkownika za pomocą pliku konfiguracyjnego XML telefonu

***Tabela 1: Czynności konfiguracyjne decydujące o wyświetlaniu ekranu Ustawianie hasła***

| Skonfigurowana usługa DHCP | Skonfigurowany system EDOS | Skonfigurowane hasło użytkownika | Pomijanie ekranu Ustawianie hasła |
|---|---|---|---|
| Tak | n/d | Tak | Tak |
| Tak | n/d | Nie | **Nie** |
| Nie | Tak | Tak | Tak |
| Nie | Tak | Nie | **Nie** |
| Nie | Nie | n/d | **Nie** |

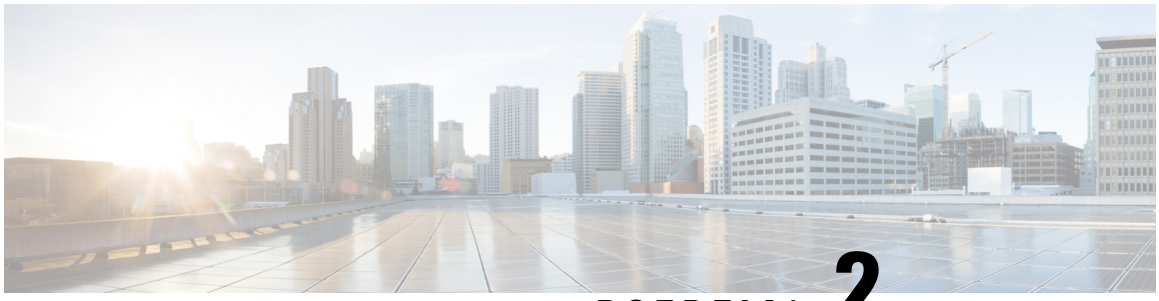
### Procedura

**Krok 1** Otwórz plik `config.xml` telefonu do edycji w edytorze tekstu lub kodu źródłowego XML.

**Krok 2** Wstaw tag **<User_Password>**, używając jednej z poniższych opcji.

- **Brak hasła (tagi początkowy i końcowy)–<User_Password></User_Password>**
- **Wartość hasła (od 4 do 127 znaków)–<User_Password ua="rw">abc123</User_Password>**
- **Brak hasła (tylko tag początkowy)–<User_Password />**

**Krok 3** Zapisz zmiany dokonane w pliku `config.xml`.



ROZDZIAŁ 2

# Skrypty obsługi administracyjnej



## Skrypty obsługi administracyjnej

Telefon akceptuje konfigurację w formacie XML.

Szczegółowe informacje o telefonie można znaleźć w podręczniku administrowania konkretnego urządzenia. W każdym przewodniku opisano parametry, które można konfigurować za pomocą administracyjnego serwera WWW.

## Formaty profilu konfiguracji

Profil konfiguracji definiuje wartości parametrów telefonu.

Format XML profilu konfiguracji wykorzystuje standardowe narzędzia tworzenia XML do kompilowania parametrów i wartości.

**Uwaga** Obsługiwany jest tylko zestaw znaków UTF-8. Podczas modyfikowania profilu w edytorze nie należy zmieniać formatu kodowania. W przeciwnym razie telefon nie rozpozna pliku.

Każdy telefon ma inny zestaw funkcji i w efekcie inny zbiór parametrów.

### Profil w formacie XML

Profil w formacie otwartym to plik tekstowy o składni przypominającej XML pod względem hierarchii elementów, z atrybutami i wartościami elementów. Ten format pozwala używać standardowych narzędzi do tworzenia pliku konfiguracyjnego. Plik konfiguracyjny w tym formacie może być wysyłany z serwera obsługi

administracyjnej do telefonu podczas operacji ponownej synchronizacji. Plik może zostać wysłany bez kompilowania, jako obiekt binarny.

Telefon akceptuje formaty konfiguracji generowane przez standardowe narzędzia. Ta funkcjonalność ułatwia tworzenie oprogramowania serwera obsługi administracyjnej przeznaczonego do działania na zapleczu, które generuje profile konfiguracji na podstawie istniejących baz danych.

W celu ochrony poufnych informacji zawartych w profilu konfiguracji serwer obsługi administracyjnej przekazuje tego typu plik do telefonu przez kanał zabezpieczony protokołem TLS. Opcjonalnie plik można skompresować przy użyciu algorytmu Deflate stosowanego w narzędziu gzip (RFC1951).

Plik można szyfrować za pomocą jednej z następujących metod szyfrowania:

- Szyfrowanie AES-256-CBC
- Szyfrowanie zawartości HTTP zgodne z dokumentem RFC-8188 przy użyciu szyfru AES-128-GCM

#### Przykład: Format profilu otwartego

```
<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>
```

Znacznik elementu <flat-profile> ujmuje wszystkie elementy parametrów rozpoznawane przez telefon.

#### Tematy pokrewne

Szyfrowanie i kompresja otwartego profilu (XML), na stronie 18

# Składniki pliku konfiguracyjnego

Plik konfiguracyjny może zawierać następujące elementy:

- Znaczniki elementów
- Atrybuty
- Parametry
- Funkcje formatowania
- Komentarze XML

## Właściwości znaczników elementów

- Format obsługi administracyjnej przy użyciu kodu źródłowego XML i internetowy interfejs użytkownika umożliwiają konfigurowanie tych samych ustawień. Nazwy znaczników XML i nazw pól w internetowym interfejsie użytkownika są podobne, ale różnią się z powodu ograniczeń w nazwach elementów XML. Na przykład zamiast spacji („ ”) zawierają znaki podkreślenia (_).

- Telefon rozpoznaje elementy o prawidłowych nazwach parametrów, które są ujęte w specjalny element <flat-profile>.
- Nazwy elementów są otoczone nawiasami ostrymi.
- Większość nazw elementów jest podobna do nazw pól na stronach WWW administrowania urządzeniem, z następującymi modyfikacjami:
  - Nazwy elementów nie mogą zawierać spacji ani znaków specjalnych. Aby utworzyć nazwę elementu na podstawie nazwy pola w interfejsie WWW administrowania, zastąp podkreśleniami wszystkie spacje i znaki specjalne `[`, `]`, `(`, `)` lub `/`.

    **Przykład:** Element <Resync_On_Reset> reprezentuje pole **Ponowna synchronizacja po zresetowaniu** (Resync On Reset).
  - Nazwa każdego elementu musi być unikatowa. W interfejsie WWW administrowania te same pola mogą się pojawiać na różnych stronach, takich jak Linia, Użytkownika i Numer wewnętrzny. Dołącz ciąg `[n]` do nazwy elementu, aby pokazywać numer wyświetlany na karcie strony.

    **Przykład:** Element <Dial_Plan_1_> reprezentuje obiekt **Plan wybierania numerów** dla linii 1.
- Każdy znacznik elementu otwierającego musi mieć odpowiadający mu znacznik elementu zamykającego. Na przykład:

```
<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>
```

- W znacznikach elementów jest uwzględniana wielkość liter.
- Puste znaczniki elementów są dozwolone i będą interpretowana jako ustawiające puste wartości. Wprowadź znacznik elementu otwierającego bez odpowiadającego mu znacznika elementu, a następnie dodaj spację i ukośnik przed zamykającym nawiasem ostrym (>). W tym przykładzie parametr Profile Rule B jest pusty:

```
<Profile_Rule_B />
```

- Pusty znacznik elementu może służyć do zapobiegania nadpisaniu wartości wprowadzonych przez użytkownika podczas operacji ponownej synchronizacji. W poniższym przykładzie nie zmieniły się ustawienia szybkiego wybierania zdefiniowane przez użytkownika:

```
<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>
```

- Za pomocą pustej wartości ustaw pusty ciąg w odnośnym parametrze. Wprowadź elementy otwierający i zamykający bez wartości między nimi. W poniższym przykładzie w parametrze GPP_A jest ustawiany pusty ciąg.

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

- Nierozpoznane nazwy elementów są ignorowane.

### Tematy pokrewne

Kontrola dostępu do konfiguracji, na stronie 7

## Atrybut dostępu użytkownika

Formanty atrybutu dostępu użytkownika (**ua**) mogą służyć do zmiany praw dostępu przyznawanych kontom użytkowników. Jeśli atrybut **ua** nie zostanie zdefiniowany, istniejące ustawienie dostępu użytkownika nie zmieni się. Atrybut nie wpływa na prawa dostępu z konta administratora.

Jeżeli atrybut **ua** zostanie podany, musi mieć jedną z następujących wartości:

- na — brak dostępu
- ro — tylko do odczytu
- rw — odczyt i zapis

Poniższy przykład ilustruje działanie atrybutu **ua**:

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

Wartość opcji **ua** musi być ujęta w podwójny cudzysłów.

## Kontrola dostępu

Jeśli parametr <Phone-UI-User-Mode> jest włączony, graficzny interfejs użytkownika (GUI) telefonu akceptuje atrybut dostępu użytkownika w odnośnych parametrach podczas wyświetlania elementów menu w tym interfejsie.

W przypadku elementów menu skojarzonych z jednym parametrem konfiguracyjnym:

- Włączenie obsługi administracyjnej parametru poprzez zadeklarowanie „ua=na” („ua” oznacza „dostęp użytkownika”) powoduje, że element menu znika.
- Włączenie obsługi administracyjnej parametru poprzez zadeklarowanie „ua=ro” powoduje, że element jest tylko do odczytu i nie można go edytować.

W przypadku elementów menu skojarzonych z wieloma parametrami konfiguracyjnymi:

- Włączenie obsługi administracyjnej wszystkich odnośnych parametrów poprzez zadeklarowanie „ua=na” powoduje, że elementy menu znikają.

### Tematy pokrewne

Kontrola dostępu do konfiguracji, na stronie 7

## Właściwości parametrów

Parametry mają następujące właściwości:

- Wszystkie parametry, które nie zostały określone w profilu, pozostają w telefonie niezmienione.
- Nierozpoznane parametry są ignorowane.
- Jeśli profil w formacie otwartym zawiera wiele wystąpień tego samego znacznika parametru, ostatnie wystąpienie zastępuje wszystkie poprzednie wystąpienia. W celu uniknięcia przypadkowego nadpisania wartości konfiguracji w parametrze zalecamy, aby w każdym profilu było maksymalnie jedno wystąpienie parametru.
- Ostatnio przetwarzany profil ma pierwszeństwo. Jeśli ten sam parametr konfiguracyjny jest zdefiniowany w kilku profilach, pierwszeństwo ma wartość z ostatniego profilu.

## Formaty ciągów

Podczas formatowania ciągów obowiązują poniższe zalecenia:

- Komentarze można dodawać za pomocą standardowej składni XML.

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

- Spacje początkowe i końcowe są dozwolone w celu poprawy czytelności, ale system usuwa je z wartości parametru.
- Nowe wiersze wewnątrz wartości są przekształcane na spacje.
- Nagłówek XML w postaci `<? ?>` jest dozwolony, ale telefon go ignoruje.
- Aby wprowadzać znaki specjalne, należy używać standardowych znaków modyfikacji XML, jak to pokazano w poniższej tabeli.

| Znak specjalny | Sekwencja specjalna XML |
|---|---|
| & (handlowe i) | &i |
| < (mniejsze niż) | < |
| > (większe niż) | > |
| ' (apostrof) | ' |
| " (podwójny cudzysłów) | " |

W przykładzie poniżej wprowadzono znaki modyfikacji (sekwencje specjalne) w celu reprezentowania symboli „większe niż" i „mniejsze niż", które są wymagane w regule planu wybierania. W tym przykładzie jest definiowany plan wybierania numeru infolinii informacyjnej, w którym parametr <Dial_Plan_1_> (**Logowanie się administratora** > **Zaawansowane (Advanced)** > **Głos (Voice)** > **Wewn.(n) (Ext (n))**) otrzymuje wartość (S0 <:18005551212>).

```
<flat-profile>
```

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

- Liczbowe znaki modyfikacji, zawierające wartości dziesiętne i szesnastkowe (np. ( i . ), są przekształcane.
- Oprogramowanie sprzętowe telefonu obsługuje tylko znaki ASCII.

# Szyfrowanie i kompresja otwartego profilu (XML)

Otwarty profil konfiguracji można skompresować w celu zmniejszenia ruchu sieciowego obsługiwanego przez serwer obsługi administracyjnej. Profil można również szyfrować w celu ochrony poufnych informacji. Kompresja nie jest wymagana, ale musi poprzedzać szyfrowanie.

**Tematy pokrewne**

Formaty profilu konfiguracji, na stronie 13

## Kompresja otwartego profilu

Obsługiwaną metodą kompresji jest algorytm Deflate stosowany w narzędziu gzip (RFC1951). Narzędzie gzip oraz biblioteka kompresji, która implementuje ten sam algorytm (zlib), są dostępne do pobrania w Internecie.

Na potrzeby identyfikowania parametrów kompresji skompresowany plik pobrany do telefonu powinien zawierać nagłówek zgodny z narzędziem gzip. Wywołanie narzędzia gzip w oryginalnym otwartym profilu powoduje wygenerowanie nagłówka. W telefonie następuje sprawdzenie nagłówka pobranego pliku w celu rozpoznania formatu pliku.

Na przykład jeśli `profile.xml` jest prawidłowym profilem, zostanie zaakceptowany plik `profile.xml.gz`. Ten typu profilu może zostać wygenerowany przez dowolne z poniższych poleceń:

- `>gzip profile.xml`

  Zastępuje oryginalny plik skompresowanym plikiem.

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

  Pozostawia oryginalny plik i tworzy nowy skompresowany plik.

Samouczek o kompresji znajduje się w rozdziale Kompresowanie otwartego profilu za pomocą narzędzia Gzip, na stronie 66.

**Tematy pokrewne**

Kompresowanie otwartego profilu za pomocą narzędzia Gzip, na stronie 66

## Szyfrowanie otwartego profilu

Szyfrowanie kluczem symetrycznym może służyć do szyfrowania otwartego profilu konfiguracji — bez względu na to, czy plik jest skompresowany, czy nie. Jeśli jest używana kompresja, należy ją zastosować przed szyfrowaniem.

Po wdrożeniu serwer obsługi administracyjnej zapewnia początkową obsługę administracyjną telefonu za pomocą protokołu HTTPS. Wstępne zaszyfrowanie profili konfiguracji w trybie offline umożliwia stosowanie protokołu HTTP do późniejszego ponownego synchronizowania profili. Takie rozwiązanie zmniejsza obciążenie serwera HTTPS w dużych wdrożeniach.

Telefon obsługuje dwie metody szyfrowania plików konfiguracyjnych:

- Szyfrowanie AES-256-CBC
- Szyfrowanie zawartości HTTP zgodne z dokumentem RFC-8188 przy użyciu szyfru AES-128-GCM

Wcześniej należy dodać w urządzeniu obsługę administracyjną klucza lub materiału wejściowego klucza (IKM). Tajny klucz można bezpiecznie załadować wstępnie przy użyciu protokołu HTTPS.

Nazwa pliku konfiguracyjnego nie musi mieć żadnego konkretnego formatu, ale nazwa kończąca się rozszerzeniem `.cfg` zwykle oznacza profil konfiguracji.

## Szyfrowanie AES-256-CBC

Telefon obsługuje szyfrowanie plików konfiguracyjnych metodą AES-256-CBC.

Szyfrowanie można wykonać za pomocą narzędzia szyfrującego OpenSSL, które jest dostępne do pobrania z różnych witryn internetowych. Aby umożliwić szyfrowanie 256-bitowymi kluczami AES, może być konieczne ponowne skompliowanie narzędzia w celu włączenia w nim obsługi kodu źródłowego algorytmu AES. Oprogramowanie sprzętowe przetestowano dla wersji openssl-0.9.7c.

Szyfrowanie profilu przy użyciu narzędzia OpenSSL, na stronie 66 zawiera samouczek o szyfrowaniu.

Zaszyfrowany plik profilu powinien mieć taki sam format, jak plik wygenerowany przez następujące polecenie:

```
# 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
```

Mała litera -k poprzedza tajny klucz, którym może być dowolne wyrażenie tekstowe i który służy do wygenerowania losowego 64-bitowego ciągu zaburzającego. Przy użyciu tajnego klucza określonego przez argument -k, narzędzie szyfrowania generuje pochodny losowy 128-bitowy wektor inicjujący i faktyczny 256-bitowy klucz szyfrujący.

Jeżeli ta metoda jest używana dla profilu konfiguracji, w telefonie musi być dostępna wartość klucza poufnego, tak aby można było odszyfrować plik. Wartość ta jest podana jako kwalifikator w adresie URL profilu. Obowiązuje następująca składnia z jawnym adresem URL:

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

Ta wartość jest programowana za pomocą jednego z parametrów Profile_Rule.

### Tematy pokrewne

Szyfrowanie profilu przy użyciu narzędzia OpenSSL, na stronie 66

## Rozwijanie w makro

Niektóre parametry obsługi administracyjnej są wewnętrznie rozwijane w makra przed oceną ich wartości. Ten krok wstępnej oceny zapewnia większą elastyczność sterowania procesami ponownej synchronizacji i uaktualniania telefonu.

Parametry z poniższych grup są rozwijane do makr przed fazą oceny:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

W pewnych warunkach również niektóre parametry ogólnego przeznaczenia (GPP_*) są rozwijane w makra, zgodnie z opisem w rozdziale Opcjonalne argumenty ponownej synchronizacji, na stronie 23.

Podczas rozwijania w makra zawartość nazwanych zmiennych zastępuje wyrażenia typu $NAZWA i $(NAZWA). Te zmienne to między innymi parametry ogólnego przeznaczenia, niektóre identyfikatory produktów, wybrane zegary zdarzeń oraz wartości stanów obsługi administracyjnej. Pełna lista znajduje się w punkcie Zmienne rozwijane w makra, na stronie 79.

W poniższym przykładzie wyrażenie $(MAU) służy do wstawiania adresu MAC 000E08012345.

Administrator wpisuje: **`$(MAU)config.cfg`**

Rozwinięcie w makro dla urządzenia o adresie MAC 000E08012345 daje następujące dane wyjściowe:
`000E08012345config.cfg`

Jeśli rozwinięcie w makro nie jest rozpoznawane, zmienna pozostaje nierozwinięta. Na przykład nazwa STRANGE nie jest rozpoznawana jako prawidłowa nazwa makra, w przeciwieństwie do nazwy MAU.

Administrator wpisuje: **`$STRANGE$MAU.cfg`**

Rozwinięcie w makro dla urządzenia o adresie MAC 000E08012345 daje następujące dane wyjściowe:
`$STRANGE000E08012345.cfg`

Rozwijanie w makra nie jest cykliczne. Na przykład zmienna $$MAU" jest rozwijana do wartości $MAU" (jest rozwijana część $$), a nie do adresu MAC.

Zawartość parametrów specjalnych od GPP_SA do GPP_SD jest mapowana na wyrażenia makr od $SA do $SD. Parametry te są rozwijane w makra tylko jako argumenty opcji **--key**, **--uid** i **--pwd** w adresie URL ponownej synchronizacji.

## Wyrażenia warunkowe

Wyrażenia warunkowe mogą inicjować zdarzenia ponownej synchronizacji oraz wybierać z dostępnej puli adresy URL do operacji ponownej synchronizacji i uaktualniania.

Wyrażenia warunkowe składają się z listy porównań rozdzielonych operatorem **I**. Aby warunek był spełniony, wszystkie porównania muszą mieć wartość prawda (true).

Każde porównanie może się odnosić do jednego z trzech następujących typów literałów:

- Wartości całkowite
- Numery wersji oprogramowania lub sprzętu

- Ciągi ujęte w podwójne cudzysłowy

### Numery wersji

W telefonach wieloplatformowych (MPP) formalne numery wersji oprogramowania mają następujący format, gdzie BN oznacza numer kompilacji:

- Telefon Cisco IP Phone z serii 6800 — `sip68xx.v1-v2-v3MPP-BN`

Porównywany ciąg musi mieć ten sam format. W przeciwnym razie zostanie zgłoszony błąd analizy formatu.

W oznaczeniu wersji oprogramowania wartościami elementów v1-v2-v3-v4 mogą być różne cyfry i znaki, ale na początku zawsze musi się znajdować cyfra. Podczas porównywania wersji oprogramowania elementy v1-v2-v3-v4 są porównywane kolejno, a cyfry po lewej stronie mają pierwszeństwo przed dalszymi cyframi.

Jeśli element v[x] zawiera tylko cyfry, są one porównywane. Jeśli element v[x] zawiera cyfry i znaki alfanumeryczne, najpierw są porównywane cyfry, a następnie znaki w kolejności alfabetycznej.

### Przykład prawidłowego numeru wersji

sipyyyy.11-0-0MPP-BN

Z kolei format 11.0.0 jest nieprawidłowy.

### Porównanie

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

Ciągi w cudzysłowach można porównywać, żeby sprawdzić, czy są takie same. Ponadto można arytmetycznie porównywać liczby całkowite i numery wersji. Operatory porównań mogą być wyrażone za pomocą symboli lub akronimów. Akronimy są wygodne do wyrażania warunków w profilu w formacie otwartym.

| Operator | Alternatywna składnia | Opis | Zastosowanie do argumentów w postaci liczb całkowitych i oznaczeń wersji | Zastosowanie do argumentów w postaci ciągów w cudzysłowach |
|---|---|---|---|---|
| = | eq | równa się | Tak | Tak |
| != | ne | nie równa się | Tak | Tak |
| < | lt | mniejsze niż | Tak | Nie |
| <= | le | mniejsze niż lub równe | Tak | Nie |
| > | gt | większe niż | Tak | Nie |
| >= | ge | większe niż lub równe | Tak | Nie |

| Operator | Alternatywna składnia | Opis | Zastosowanie do argumentów w postaci liczb całkowitych i oznaczeń wersji | Zastosowanie do argumentów w postaci ciągów w cudzysłowach |
|---|---|---|---|---|
| AND | | i | Tak | Tak |

Jeśli oczekiwaną wartością jest literał w postaci ciągu, należy pamiętać, aby zmienne makr ująć w cudzysłowy. Nie należy tego robić, jeśli oczekiwaną wartością jest liczba lub numer wersji.

Jeżeli wyrażenia warunkowe są używane w kontekście parametrów Profile_Rule* i Upgrade_Rule, muszą mieć składnię „(wyrażenie)?", tak jak w tym przykładzie reguły uaktualniania. Należy pamiętać, że element BN oznacza numer kompilacji.

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

Nie należy używać powyższej składni z nawiasami do konfigurowania parametrów Resync_Trigger_*.

## Składnia adresu URL

Do określenia, jak mają być pobierane pliki konfiguracyjne i oprogramowanie sprzętowe za pomocą parametrów odpowiednio Profile_Rule* i Upgrade_Rule, należy użyć standardowej składni adresu URL. Składnia jest następująca:

**[ schemat:// ] [ serwer [:port]] ścieżka_pliku**

Gdzie atrybut **schemat** przybiera jedną z następujących wartości:

- tftp
- http
- https

Atrybut **schemat** można pominąć i będzie wtedy używany serwer tftp. Serwer można określić za pomocą nazwy hosta rozpoznawanej przez serwer DNS lub liczbowego adresu IP. Port to numer docelowego portu UDP lub TCP. Ścieżka pliku musi się rozpoczynać od katalogu głównego (/) i być ścieżką bezwzględną.

Jeśli nie będzie atrybutu **serwer**, zostanie użyty serwer tftp określony w protokole DHCP (opcja 66).

**Uwaga** W regułach uaktualniania podanie serwera jest wymagane.

Jeśli nie będzie atrybutu **port**, zostanie użyty standardowy port wskazanego schematu. Protokół tftp używa portu UDP 69, http portu TCP 80, a https portu TCP 443.

Podanie ścieżki pliku jest wymagane. Nie musi się odwoływać do statycznego pliku — może to być dynamiczna zawartość pobierana za pośrednictwem skryptu CGI.

Rozwijanie w makra działa wewnątrz adresów URL. Poniżej przedstawiono przykłady prawidłowych adresów 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
```

Jeśli w protokole DHCP jest używana opcja 66, pusta składnia jest niedopuszczalna w regułach uaktualniania. Ma zastosowanie tylko do reguły profilu*.

## Szyfrowanie zawartości HTTP zgodne z dokumentem RFC 8188

Telefon obsługuje szyfrowanie plików konfiguracyjnych zgodne z dokumentem RFC-8188 szyfrowania zawartości HTTP przy użyciu szyfru AES-128-GCM. Dzięki tej metodzie szyfrowania wszystkie podmioty mogą odczytywać nagłówki komunikatów HTTP. Jednak właściwe dane mogą odczytywać tylko podmioty znające materiał wejściowy klucza (IKM). Gdy w telefonie jest włączona obsługa funkcjonalności IKM, telefon i serwer obsługi administracyjnej mogą bezpiecznie przesyłać między sobą pliki konfiguracyjne, zezwalając przy tym zewnętrznym elementom sieci na wykorzystywanie nagłówków komunikatów do celów analitycznych i monitorowania.

Parametr konfiguracyjny XML **IKM_HTTP_Encrypt_Content** przechowuje wartość IKM w telefonie. Ze względów bezpieczeństwa parametr ten nie jest dostępny na stronie WWW administrowania telefonem. Ponadto nie jest on widoczny w pliku konfiguracyjnym telefonu, który można obejrzeć po podaniu adresu IP telefonu lub w raportach o konfiguracji telefonu wysyłanych do serwera obsługi administracyjnej.

Aby można było używać szyfrowania zgodnego z dokumentem RFC-8188, muszą być spełnione następujące warunki:

- Należy włączyć w telefonie obsługę funkcji IKM, ustawiając dla niej parametr XML **IKM_HTTP_Encrypt_Content** w pliku konfiguracyjnym wysłanym z serwera obsługi administracyjnej do telefonu.
- Jeśli to szyfrowanie ma być stosowane do plików konfiguracyjnych wysyłanych z serwera obsługi administracyjnej do telefonu, należy się upewnić, że w pliku konfiguracyjnym nagłówek HTTP *Content-Encoding* ma wartość "aes128gcm".

  W razie braku tego nagłówka pierwszeństwo ma metoda AES-256-CBC. Jeśli w regule profilu zostanie określony klucz AES-256-CBC, w telefonie jest stosowane odszyfrowywanie metodą AES-256-CBC, niezależnie od IKM.
- Aby stosować to szyfrowanie w telefonie do raportów o konfiguracji wysyłanych do serwera obsługi administracyjnej, należy usunąć z reguły raportu klucz AES-256-CBC.

# Opcjonalne argumenty ponownej synchronizacji

Opcjonalne argumenty **key**, **uid** i **pwd**, wspólnie ujęte w nawiasy kwadratowe, mogą poprzedzać adresy URL wprowadzone w parametrach Profile_Rule*.

## key

Opcja **--key** informuje telefon, że plik konfiguracyjny otrzymany z serwera obsługi administracyjnej jest zaszyfrowany metodą AES-256-CBC, chyba że nagłówek *Content-Encoding* w tym pliku określa szyfrowanie "aes128gcm". Sam klucz jest definiowany jako ciąg następujący po słowie kluczowym **--key**. Opcjonalnie

klucz może być ujęty w podwójny cudzysłów ("). Klucz jest używany w telefonie do odszyfrowania pliku konfiguracyjnego.

#### Przykłady użycia

```
[--key VerySecretValue]
[--key “my secret phrase”]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

Opcjonalne argumenty w nawiasach kwadratowych są rozwijane w makra. Parametry specjalne od GPP_SA do GPP_SD są rozwijane w makra ze zmiennych makr od $SA do $SD tylko wtedy, gdy pełnią rolę argumentów opcji klucza. Zobacz poniższe przykłady:

```
[--key $SC]
[--key “$SD”]
```

W profilach typu Format otwarty argument opcji **--key** musi być taki sam, jak argument opcji **-k** podawany do polecenia **openssl**.

### uid i pwd

Opcje **uid** i **pwd** mogą służyć do określania identyfikatora użytkownika i hasła na potrzeby uwierzytelniania przy użyciu podanego adresu URL. Opcjonalne argumenty w nawiasach kwadratowych są rozwijane w makra. Parametry specjalne od GPP_SA do GPP_SD są rozwijane w makra ze zmiennych makr od $SA do $SD tylko wtedy, gdy pełnią rolę argumentów opcji klucza. Zobacz poniższe przykłady:

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

[--uid $SA -pwd $SB]
https://adres_url_serwera_obsługi_administracyjnej/ścieżka_do_konfiguracji/Twoja_konfiguracja.xml

rozwinie się do:

[--uid MojIdentyfikatorUzytkownika -pwd MojeTajneHaslo]
https://adres_url_serwera_obsługi_administracyjnej/ścieżka_do_konfiguracji/Twoja_konfiguracja.xml

# Stosowanie profilu do telefonu IP

Po utworzeniu skryptu konfiguracyjnego w formacie XML należy go przekazać do telefonu, w którym ma być zastosowany. W celu zastosowania konfiguracji można pobrać plik konfiguracyjny do telefonu z serwera TFTP, HTTP lub HTTPS za pomocą przeglądarki WWW albo przy użyciu narzędzia wiersza poleceń cURL.

## Pobieranie pliku konfiguracyjnego do telefonu z serwera TFTP

Poniżej opisano procedurę pobierania pliku konfiguracyjnego do aplikacji serwera TFTP na komputerze.

**Procedura**

**Krok 1** Podłącz komputer do sieci LAN, do której jest podłączony telefon.

**Krok 2** Uruchom aplikację serwera TFTP na komputerze, a następnie upewnij się, że plik konfiguracyjny jest dostępny w katalogu głównym serwera TFTP.

**Krok 3** W przeglądarce WWW wprowadź adres IP telefonu w sieci LAN, adres IP komputera, nazwę pliku i poświadczenia logowania. Użyj następującego formatu:

`http://<adres_IP_w_sieci_WAN>/admin/resync?tftp://<adres_IP_komputera>/<nazwa_pliku>&xuser=admin&xpassword=<hasło>`

Przykład:

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

# Pobieranie pliku konfiguracyjnego do telefonu IP za pomocą narzędzia cURL

Poniżej opisano procedurę pobierania konfiguracji do telefonu za pomocą narzędzia cURL. To narzędzie wiersza poleceń służy do przesyłania danych za pomocą opcji w składni adresu URL. Narzędzie cURL można pobrać z następującej strony:

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

**Uwaga** Zalecamy, aby nie używać narzędzia cURL do wysyłania konfiguracji do telefonu, ponieważ istnieje ryzyko przechwycenia nazwy użytkownika i hasła.

**Procedura**

**Krok 1** Podłącz komputer do portu sieci LAN w telefonie.

**Krok 2** Pobierz plik konfiguracyjny do telefonu, wpisując następujące polecenie w narzędziu cURL:

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

# Parametry obsługi administracyjnej

W tej części opisano parametry obsługi administracyjnej, ogólnie uporządkowane według funkcji:

Istnieją następujące typy parametrów obsługi administracyjnej:

- Przeznaczenie ogólne
- Włączniki
- Wyzwalacze

- Konfigurowalne harmonogramy
- Reguły dotyczące profili
- Reguła uaktualniania

# Parametry ogólnego przeznaczenia

Parametry ogólnego przeznaczenia GPP_* (**Logowanie się administratora** > **Zaawansowane (Advanced)** > **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**) pełnią rolę tekstowych pól używanych podczas konfigurowania współpracy telefonu z określonym serwerem obsługi administracyjnej. Parametry GPP_* są domyślnie puste. Można skonfigurować przechowywanie w nich różnych wartości, w tym następujących:

- Klucze szyfrowania
- Adresy URL
- Informacje o stanie wielostopniowej obsługi administracyjnej
- Szablony żądań POST
- Mapy aliasów nazw parametrów
- Częściowe wartości ciągów łączone w kompletne wartości parametrów

Parametry GPP_* mogą być rozwijane w makra wewnątrz innych parametrów obsługi administracyjnej. W tym kontekście do identyfikowania zawartości parametrów od GPP_A do GPP_P wystarczają nazwy makr w postaci pojedynczych wielkich liter (od A do P). Ponadto nazwy makr składające się z dwóch wielkich liter od SA do SD identyfikują parametry od GPP_SA do GPP_SD w szczególnych przypadkach, gdy są używane jako argumenty w następujących opcjach adresów URL:

**key**, **uid** i **pwd**

Te parametry mogą pełnić rolę zmiennych w regułach obsługi administracyjnej i uaktualniania. Odwołania do nich tworzy się przed dodanie prefiksu „$” do nazwy zmiennej, np. $GPP_A.

## Używanie parametrów ogólnego przeznaczenia

Na przykład jeśli parametr GPP_A zawiera ciąg ABC, a parametr GPP_B ciąg 123, wyrażenie $A$B zostanie rozwinięte w makro o danych wyjściowych ABC123.

### Zanim rozpoczniesz

Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

### Procedura

**Krok 1** Wybierz kolejno opcje **Głos** > **Obsługa administracyjna**.

**Krok 2** Przewiń do sekcji **Parametry ogólnego przeznaczenia** (General Purpose Parameters).

**Krok 3** Wprowadź prawidłowe wartości w polach od GPP_A do GPP_P.

**Krok 4** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

# Włączniki

Parametry Provision_Enable i Upgrade_Enable sterują wszystkimi operacjami ponownej synchronizacji profili i uaktualniania oprogramowania sprzętowego. Działają one niezależnie od siebie. Ponadto sterują poleceniami ponownej synchronizacji i uaktualniania adresów URL wysyłanymi za pośrednictwem administracyjnego serwera WWW. Oba parametry mają domyślnie ustawioną wartość **Tak** (Yes).

Parametr Resync_From_SIP steruje żądaniami ponownej synchronizacji. Zdarzenie SIP NOTIFY jest wysyłane z serwera proxy dostawcy usług do telefonu. Jeśli na serwerze proxy są włączone odpowiednie funkcje, może się pojawić żądanie ponownej synchronizacji. W tym celu do urządzenia jest wysyłany komunikat SIP NOTIFY zawierający nagłówek Event: resync.

Żądanie jest kwestionowane przez urządzenie za pomocą odpowiedzi 401 (odmowa autoryzacji użytych poświadczeń). Żądanie ponownej synchronizacji z serwera proxy zostanie zrealizowane w urządzeniu po otrzymaniu uwierzytelnionego następnego żądania. Nagłówki Event: reboot_now i Event: restart_now powodują odpowiednio ponowny rozruch sprzętowy i programowy; one również są kwestionowane.

Dwa pozostałe włączniki to Resync_On_Reset i Resync_After_Upgrade_Attempt. Parametry te decydują o tym, czy w urządzeniu jest wykonywana operacja ponownej synchronizacji po każdym ponownym uruchomieniu programowym i po każdej próbie uaktualnienia.

Jeżeli parametr Resync_On_Reset jest włączony, wówczas po sekwencji rozruchu, a przed wykonaniem resetu w urządzeniu jest dodawane losowe opóźnienie. Czas trwania opóźnienia jest losowy, jednak nie dłuższy niż wartość określona w parametrze Resync_Random_Delay (w sekundach). W puli telefonów włączanych jednocześnie to opóźnienie powoduje różnicowanie czasów rozpoczęcia wykonywania żądań ponownej synchronizacji z każdego urządzenia. Funkcja może być przydatna w dużych wdrożeniach na terenach mieszkalnych w razie awarii lokalnej sieci elektrycznej.

# Wyzwalacze

Telefon umożliwia ponowne synchronizowanie w określonych odstępach czasu lub określonych godzinach.

## Ponowna synchronizacja w określonych odstępach czasu

Telefon powinien się okresowo synchronizować z serwerem obsługi administracyjnej. Interwał ponownej synchronizacji jest ustawiany w parametrze Resync_Periodic (w sekundach). Jeśli ta wartość jest pusta, urządzenie nie synchronizuje się okresowo.

Zazwyczaj ponowna synchronizacja odbywa się w okresie bezczynności linii głosowych. Jeśli linia głosowa jest aktywna w momencie, gdy powinna zostać wykonana ponowna synchronizacja, telefon opóźnia procedurę synchronizacji do czasu, aż linia znów będzie bezczynna. Ponowna synchronizacja może spowodować zmianę wartości parametrów konfiguracyjnych.

Operacja ponownej synchronizacji może się nie udać, jeśli telefon nie jest w stanie pobrać profilu z serwera, pobrany plik jest uszkodzony lub wystąpił błąd wewnętrzny. Urządzenie ponowi próbę synchronizacji po czasie określonym w parametrze Resync_Error_Retry_Delay (w sekundach). Ustawienie w parametrze Resync_Error_Retry_Delay wartości 0 spowoduje, że urządzenie nie będzie próbować ponownej synchronizacji po jednej nieudanej próbie.

W przypadku nieudanego uaktualnienia system ponawia próbę po liczbie sekund ustawionej w parametrze Upgrade_Error_Retry_Delay.

Istnieją dwa konfigurowalne parametry umożliwiające warunkowe inicjowanie ponownej synchronizacji: Resync_Trigger_1 i Resync_Trigger_2. W każdym parametrze można zaprogramować wyrażenie warunkowe rozwijane do makra. Po upływie interwału ponownej synchronizacji (czasu do następnej synchronizacji) wyzwalacze (jeśli zostały ustawione) uniemożliwią ponowną synchronizację, jeżeli nie jest spełniony warunek co najmniej jednego z nich.

W przykładzie poniżej warunek powoduje zainicjowanie ponownej synchronizacji. Tutaj od ostatniej próby uaktualnienia telefonu upłynęło ponad 5 minut (300 sekund), a co najmniej 10 minut (600 sekund) upłynęło od ostatniej próby ponownej synchronizacji.

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

## Ponowna synchronizacja o określonej godzinie

Parametr Resync_At umożliwia synchronizowanie telefonu o konkretnie wybranej godzinie. Godzina jest ustalana na podstawie zegara w formacie 24-godzinnym (ggmm).

Parametr Resync_At_Random_Delay umożliwia synchronizowanie telefonu z nieokreślonym opóźnieniem czasowym. Do określania czasu wykorzystywana jest dodatnia liczba całkowita.

Należy unikać zalewania serwera żądaniami ponownej synchronizacji z wielu telefonów, dla których ustawiono synchronizowanie w tym samym czasie. Aby zapobiec temu zjawisku, ponowna synchronizacja telefonu może być inicjowana nawet 10 minut po wyznaczonej godzinie.

Jeśli na przykład ustawisz godzinę ponownej synchronizacji na 1000 (10 rano), synchronizacja rozpocznie się w dowolnym momencie między 10:00 a 10:10.

Domyślnie ta funkcja jest wyłączona. Włączenie parametru Resync_At powoduje ignorowanie parametru Resync_Periodic.

# Konfigurowalne harmonogramy

Za pomocą poniższych parametrów obsługi administracyjnej można skonfigurować harmonogramy okresowych ponownych synchronizacji oraz określić odstępy czasu między kolejnymi próbami po niepowodzeniach ponownej synchronizacji i uaktualniania:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Każdy parametr może zawierać jedną wartość opóźnienia (w sekundach). Nowa rozszerzona składnia umożliwia wprowadzenie listy kolejnych elementów opóźnienia oddzielonych przecinkami. Ostatni element sekwencji jest domyślnie powtarzany bezterminowo.

Opcjonalnie za pomocą znaku plusa można podać inną wartość liczbową, która dodaje losowe dodatkowe opóźnienie.

### Przykład 1

W tym przykładzie telefon synchronizuje się ponownie regularnie co 2 godziny. Jeśli w trakcie ponownej synchronizacji wystąpi błąd, urządzenie będzie ponawiać próby w następujących odstępach: 30 minut, 1 godzina, 2 godziny i 4 godziny. Potem urządzenie będzie nadal próbować co 4 godziny do czasu, aż ponowna synchronizacja się powiedzie.

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

### Przykład 2

W tym przykładzie urządzenie synchronizuje się ponownie co godzinę (plus dodatkowe losowe opóźnienie wynoszące maksymalnie 10 minut). W razie błędu ponownej synchronizacji urządzenie będzie ponawiać próby w następujących odstępach: 30 minut (plus maksymalnie 5 minut). 1 godzina (plus maksymalnie 10 minut), 2 godziny (plus maksymalnie 15 minut). Potem urządzenie będzie nadal próbować co 2 godziny (plus maksymalnie 15 minut) do czasu, aż ponowna synchronizacja się powiedzie.

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

### Przykład 3

W tym przykładzie w razie niepowodzenia próby zdalnego uaktualnienia urządzenie ponowi próbę po 30 minutach, następnie ponownie po 1 godzinie, a następnie po kolejnych 2 godzinach. Jeśli uaktualnienie nadal się nie uda, urządzenie będzie próbować co 4-5 godzin do momentu, aż uaktualnienie się powiedzie.

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

# Reguły dotyczące profili

Telefon zawiera wiele parametrów zdalnych profili konfiguracji (Profile_Rule*). W efekcie podczas każdej operacji ponownej synchronizacji może być pobieranych wiele plików zarządzanych przez różne serwery.

W najprostszym scenariuszu urządzenie jest ponownie synchronizowane co pewien czas za pomocą jednego profilu na centralnym serwerze, co powoduje aktualizuję wszystkich odpowiednich wewnętrznych parametrów. Alternatywnie profil może być podzielony między różne pliki. Jeden plik jest wspólny dla wszystkich telefonów we wdrożeniu. Dodatkowo dla każdego konta istnieje oddzielny, unikatowy plik. Klucze szyfrowania i dane certyfikatów mogą być dostarczane przez jeszcze inny profil, przechowywany na osobnym serwerze.

Za każdym razem, gdy zbliża się operacja ponownej synchronizacji, telefon ocenia cztery parametry Profile_Rule* w następującej kolejności:

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

Każda ocena może spowodować pobranie profilu ze zdalnego serwera obsługi administracyjnej, a następnie aktualizację niektórych parametrów wewnętrznych. Jeżeli wynik będzie negatywny, sekwencja ponownej synchronizacji zostanie przerwana i rozpocznie się od nowa po czasie określonym przez parametr Resync_Error_Retry_Delay (w sekundach). Jeśli wszystkie oceny będą pozytywne, urządzenie czeka przez liczbę sekund określoną parametrem Resync_Periodic, a następnie wykonuje kolejną synchronizację.

Każdy parametr Profile_Rule* zawiera zbiór wartości alternatywnych. Wartości alternatywne są oddzielone znakiem | (potoku). Każda wartość alternatywna składa się z wyrażenia warunkowego, wyrażenia przypisania, adresu URL profilu i powiązanych opcji w adresie URL. Wszystkie te składniki są opcjonalne w każdej wartości alternatywnej. Poniżej wymieniono prawidłowe kombinacje oraz kolejność, w jakiej muszą być uszeregowane, jeśli występują:

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

W każdym parametrze Profile_Rule* wszystkie wartości alternatywne (poza ostatnią) muszą zawierać wyrażenie warunkowe. To wyrażenie jest oceniane i przetwarzane w następujący sposób:

1. Warunki są oceniane w kolejności od lewej do prawej strony do czasu, aż zostanie znaleziony warunek dający rezultat Prawda (lub do momentu znalezienia wartości alternatywnej bez wyrażenia warunkowego).
2. Wtedy następuje ocena towarzyszącego wyrażenia przypisania, jeśli takie występuje.
3. Jeśli częścią wartości alternatywnej jest adres URL, następuje próba pobrania profilu znajdującego się pod tym adresem. Następnie system próbuje odpowiednio zaktualizować parametry wewnętrzne.

Jeśli wszystkie wartości alternatywne zawierają wyrażenia warunkowe, a żadna z nich po ocenie nie daje rezultatu Prawda (lub jeśli cała reguła profilu jest pusta), cały parametr Profile_Rule* jest pomijany. Wtedy rozpoczyna się ocena następnego w kolejności parametru reguły profilu.

### Przykład 1

W tym przykładzie następuje bezwarunkowa ponowna synchronizacja z profilem pod wskazanym adresem URL oraz wysłanie żądania HTTP GET do zdalnego serwera obsługi administracyjnej:

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

### Przykład 2

W tym przykładzie urządzenie synchronizuje się ponownie z dwoma różnymi adresami URL, zależnie od stanu rejestracji linii 1. W przypadku utraty rejestracji urządzenie wysyła żądanie HTTP POST do skryptu CGI. Urządzenie wysyła zawartość parametru GPP_A rozwiniętego w makro, która może obejmować dodatkowe informacje o stanie urządzenia:

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

### Przykład 3

W tym przykładzie urządzenie synchronizuje się z tym samym serwerem. Jeśli na urządzeniu (z wersją oprogramowania starszą niż 2.0) nie jest zainstalowany certyfikat, przekazuje ono dodatkowe informacje:

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

### Przykład 4

W tym przykładzie linia 1 jest wyłączona do momentu, aż parametr GPP_A zostanie ustawiony na obsługę administracyjną z pierwszego adresu URL. Później następuje ponowna synchronizacja z drugim adresem URL:

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

### Przykład 5

W tym przykładzie zakłada się, że profil zwracany przez serwer zawiera znaczniki elementów XML. Znaczniki należy przyporządkować odpowiednim nazwom parametrów zgodnie z mapą aliasów przechowywaną w parametrze GPP_B:

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

Ponowna synchronizacja jest zazwyczaj uznawana za nieudaną, jeśli urządzenie nie otrzyma żądanego profilu z serwera. To domyślne zachowanie można zastąpić parametrem Resync_Fails_On_FNF. Ustawienie wartości Nie (No) w parametrze Resync_Fails_On_FNF spowoduje, że urządzenie potraktuje odpowiedź „Nie znaleziono pliku" otrzymaną z serwera jako pomyślną ponowną synchronizację. Domyślna wartość parametru Resync_Fails_On_FNF to Tak (Yes).

# Reguła uaktualniania

Reguła uaktualniania określa, że urządzenie ma zostać uaktywnione przy użyciu nowego pakietu oprogramowania sprzętowego, oraz w razie potrzeby wskazuje, gdzie można uzyskać ten pakiet. Jeśli pakiet już znajduje się na urządzeniu, próba pobrania nie nastąpi. Oznacza to, że prawidłowość lokalizacji pakietu oprogramowania sprzętowego nie ma znaczenia, jeżeli pakiet znajduje się na nieaktywnej partycji.

Parametr Upgrade_Rule określa pakiet oprogramowania sprzętowego, który — jeśli różni się od bieżącego pakietu — zostanie pobrany i zastosowany, chyba że wyrażenie warunkowe nakłada pewne ograniczenia albo w parametrze Upgrade_Enable ustawiono wartość **No**.

Telefon udostępnia jeden konfigurowalny parametr zdalnego uaktualniania — Upgrade_Rule. Parametr akceptuje wartości o składni podobnej jak w parametrach reguł profilu. W uaktualnianiu w adresach URL nie można podawać opcji, natomiast można używać wyrażeń warunkowych i wyrażeń przypisania. W przypadku stosowania wyrażeń warunkowych parametr można wypełnić wieloma wartościami alternatywnymi, rozdzielając je znakiem |. Składnia każdej alternatywnej wartości wygląda następująco:

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

Podobnie jak w przypadku parametrów Profile_Rule*, parametr Upgrade_Rule ocenia każdą wartość alternatywną do momentu, aż zostanie spełnione wyrażenie warunkowe lub wartość alternatywna nie będzie mieć wyrażenia warunkowego. Wtedy następuje ocena towarzyszącego wyrażenia przypisania, jeśli jest ono określone. Następnie system próbuje wykonać uaktualnienie z podanego adresu URL.

Jeśli parametr Upgrade_Rule zawiera adres URL bez wyrażenia warunkowego, urządzenie uaktualni się do obrazu oprogramowania sprzętowego wskazanego przez adres URL. Po rozwinięciu do makra i ocenie reguły urządzenie nie ponawia prób uaktualnienia do momentu, aż reguła zostanie zmodyfikowana lub realnie zmieni się kombinacja schemat + serwer + port + ścieżka pliku.

Podczas próby uaktualnienia oprogramowania sprzętowego urządzenie wyłącza dźwięk na początku procedury i uruchomiania się ponownie po jej zakończeniu. Urządzenie automatycznie rozpoczyna uaktualnienie wymuszone zawartością parametru Upgrade_Rule tylko wtedy, gdy wszystkie linie głosowe są nieaktywne.

Na przykład:

- Dla telefonów Cisco IP z serii 6800:

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

where BN==Build Number
```

W tym przykładzie parametr Upgrade_Rule powoduje uaktualnienie oprogramowania sprzętowego do obrazu zapisanego w ścieżce wskazanej przez adres URL.

Oto inny przykład dla telefonu Cisco IP Phone z serii 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
```

W tym przykładzie urządzenie otrzymuje instrukcję wczytania jednego z dwóch obrazów na podstawie zawartości parametru ogólnego przeznaczenia GPP_F.

Urządzenie może wymuszać ograniczenie instalowania starszej wersji oprogramowania sprzętowego, co może się okazać przydatną opcją personalizacji. Jeśli w parametrze Downgrade_Rev_Limit zostanie podany prawidłowy numer wersji oprogramowania sprzętowego, urządzenie będzie odrzucało próby uaktualniania do wersji oprogramowania sprzętowego starszych niż podany limit.

# Typy danych

W parametrach profili konfiguracji są używane następujące typy danych:

- {a,b,c,...} — Wybór spośród wartości a, b, c...
- Bool — Wartość logiczna „tak” lub „nie”.
- CadScript — Miniskrypt określający parametry rytmu sygnału. Maksymalnie 127 znaków.

  Składnia: $S_1[;S_2]$, gdzie:

  - $S_i=D_i(wł._{i,1}/wył._{i,1}[,wł._{i,2}/wył._{i,2}[,wł._{i,3}/wył._{i,3}[,wł._{i,4}/wył._{i,4}[,wł._{i,5}/wył._{i,5}[,wł._{i,6}/wył._{i,6}]]]]])$; jest to „sekcja”.
  - $wł._{i,j}$ i $wył._{i,j}$ to podany w sekundach czas trwania włączenia/wyłączenia *segmentu*. i = 1 lub 2, a j = od 1 do 6.
  - $D_i$ to łączny czas trwania sekcji w sekundach.

Wszystkie wartości czasów trwania mogą zawierać do trzech miejsc po przecinku, co pozwala uzyskać rozdzielczość 1 ms. Symbol wieloznaczny „*” oznacza nieograniczony czas trwania. Segmenty w sekcji są odtwarzane kolejno i powtarzane aż do upływu łącznego czasu trwania.

Przykład 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
```

Przykład 2 — Charakterystyczny dzwonek (krótki, krótki, krótki, długi):

```
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 — Składnia skryptowa, która służy do określania planów wybierania na linii 1 i linii 2.
- Float<n> — Wartość zmiennoprzecinkowa zawierająca maksymalnie n miejsc dziesiętnych.
- FQDN — W pełni kwalifikowana nazwa domeny. Może zawierać do 63 znaków. Oto kilka przykładów:
  - sip.Cisco.com:5060 lub 109.12.14.12:12345
  - sip.Cisco.com lub 109.12.14.12
- FreqScript — Miniskrypt określający parametry częstotliwości i poziom sygnału dźwiękowego. Zawiera maksymalnie 127 znaków.

  Składnia: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, gdzie:
  - $F_1$–$F_6$ to częstotliwości w Hz (tylko liczby całkowite bez znaku).
  - $L_1$–$L_6$ to odnośne poziomy w dBm (z dokładnością do maksymalnie jednego miejsca po przecinku).

  Spacje przed i po przecinku są dozwolone, ale nie zaleca się ich stosowania.

  Przykład 1 — Sygnał połączenia oczekującego:

```
440@-10

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

Przykład 2 — Sygnał wybierania:

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

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

- IP — Prawidłowy adres IPv4 w postaci x.x.x.x, gdzie x to liczba od 0 do 255. Przykład: 10.1.2.100.
- UserID — Identyfikator użytkownika w postaci, w jakiej jest wyświetlany w adresie URL; maksymalnie 63 znaki.
- Phone — Ciąg określający numer telefonu, np. 14081234567, *69, *72, 345678; lub ogólny adres URL, taki jak 1234@10.10.10.100:5068 lub jsmith@Cisco.com. Ciąg może zawierać maksymalnie 39 znaków.
- PhTmplt — Szablon numeru telefonu. Każdy szablon może zawierać jeden lub kilka wzorców oddzielonych przecinkami (,). Spacja na początku każdego wzorca jest ignorowana. „?" i „*" to symbole wieloznaczne. Aby reprezentować te konkretne znaki, użyj składni „%xx". Na przykład wyrażenie „%2a" reprezentuje znak „*". Szablon może zawierać maksymalnie 39 znaków. Przykłady: „1408*, 1510*", „1408123????, 555?1.".
- Port — Numer portu TCP/UDP (0-65535). Można podać w formacie dziesiętnym lub szesnastkowym.
- ProvisioningRuleSyntax — Składnia skryptowa, która służy do definiowania reguł ponownej synchronizacji konfiguracji i uaktualniania oprogramowania sprzętowego.
- PwrLevel — Poziom mocy wyrażony w dBm z jednym miejscem po przecinku, np. –13,5 lub 1,5 (dBm).
- RscTmplt — Szablon kodu stanu odpowiedzi w protokole SIP, np. „404, 5*", „61?", „407, 408, 487, 481". Może zawierać do 39 znaków.
- Sig<n> — Wartość n-bitowa ze znakiem. Można podać w formacie dziesiętnym lub szesnastkowym. Wartości ujemne muszą być poprzedzone znakiem „-". Znak „+" przed wartościami dodatnimi jest opcjonalny.
- Kody z gwiazdką — Kod aktywacji usługi pomocniczej, np. *69. Kod może zawierać maksymalnie 7 znaków.
- Str<n> — Ogólny ciągu zawierający maksymalnie n niezastrzeżonych znaków.
- Time<n> — Czas trwania w sekundach, z dokładnością do maksymalnie n miejsc dziesiętnych. Dodatkowe liczby po przecinku są ignorowane.
- ToneScript — Miniskrypt określający parametry częstotliwości, poziomu i rytmu sygnału dźwiękowego postępu połączenia. Skrypt może zawierać do 127 znaków.

  Składnia: FreqScript;$Z_1$[;$Z_2$].

  Sekcja $Z_1$ przypomina sekcję $S_1$ w typie danych CadScript, z tą różnicą, że po każdym segmencie wł./wył. jest umieszczony parametr składowych częstotliwości: $Z_1 = D_1(\text{wł.}_{i,1}/\text{wył.}_{i,1}/f_{i,1}[,\text{wł.}_{i,2}/\text{wył.}_{i,2}/f_{i,2}[,\text{wł.}_{i,3}/\text{wył.}_{i,3}/f_{i,3}\ [,\text{wł.}_{i,4}/\text{wył.}_{i,4}/f_{i,4}\ [,\text{wł.}_{i,5}/\text{wył.}_{i,5}/f_{i,5}\ [,\text{wł.}_{i,6}/\text{wył.}_{i,6}/f_{i,6}]]]]])$, gdzie:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ określa składowe częstotliwości z typu danych FreqScript, które są używane w tym segmencie.

Jeżeli w segmencie jest używana więcej niż jedna składowa częstotliwości, wszystkie składowe są sumowane.

Przykład 1 — Sygnał wybierania:

```
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
```

Przykład 2 — Przerywany sygnał dźwiękowy:

```
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> — Wartość n-bitowa bez znaku, gdzie n = 8, 16 lub 32. Może być określona w formacie dziesiętnym lub szesnastkowym, np. 12 lub 0x18, o ile tylko długość wartości nie przekracza n bitów.

**Uwaga** Należy pamiętać o następujących kwestiach:

- <Par Name> reprezentuje nazwę parametru konfiguracji. W profilu odpowiedni znacznik tworzy się przez zastąpienie spacji znakiem podkreślenia „_”, co daje w efekcie **Par_Name**.
- Puste pole wartości domyślnej jest interpretowane jako pusty ciąg < „” >.
- Jeśli w wybranym profilu nie ma danego znacznika, w telefonie jest używana dotychczas używana wartość.
- Szablony są porównywane kolejno. System wybiera pierwszą, a *nie najlepiej pasującą* pozycję. Nazwa parametru musi być dokładnie taka sama.
- Jeśli profil zawiera więcej niż jedną definicję parametru, w telefonie zostanie użyta ostatnia definicja znajdująca się w profilu.
- Specyfikacja parametru z pustą wartością wymusza przywrócenie domyślnej wartości parametru. Aby zamiast tego określić pusty ciąg, podaj pusty ciąg „” jako wartość parametru.

# Aktualizacje profili i uaktualnienia oprogramowania sprzętowego

Telefon obsługuje bezpieczne zdalne włączanie obsługi administracyjnej (konfigurowanie) i uaktualnianie oprogramowania sprzętowego. Telefon bez obsługi administracyjnej może odebrać zaszyfrowany profil przeznaczony specjalnie dla niego. Ponieważ jest stosowany bezpieczny mechanizm inicjowania obsługi administracyjnej wykorzystujący funkcje protokołu SSL, telefon nie wymaga konkretnego klucza.

Interwencja użytkownika nie jest wymagana do rozpoczęcia ani zakończenia procesu aktualizacji profilu, uaktualnienia oprogramowania sprzętowego ani w sytuacjach, gdy są potrzebne pośrednie uaktualnienia w celu osiągnięcia przyszłego stanu uaktualnienia ze starszej wersji. Próba ponownej synchronizacji profilu następuje tylko wtedy, gdy telefon jest bezczynny, ponieważ operacja może spowodować ponowne uruchomienie programowe i rozłączenie połączenia.

Proces obsługi administracyjnej jest zarządzany przez parametry ogólnego przeznaczenia. Na każdym telefonie można skonfigurować okresowe kontaktowanie się ze standardowym serwerem obsługi administracyjnej (NPS). Komunikacja z serwerem NPS nie wymaga używania bezpiecznego protokołu, ponieważ zaktualizowany profil jest szyfrowany kluczem współdzielonym. Rolę serwera NPS może pełnić standardowy serwer TFTP, HTTP lub HTTPS z certyfikatami klienta.

Administrator może uaktualniać, ponownie uruchamiać, restartować i ponownie synchronizować telefony za pomocą interfejsu WWW użytkownika telefonu. Administrator może wykonywać te zadania również za pomocą komunikatu powiadamiania w protokole SIP.

Profile konfiguracji są generowane przy użyciu popularnych narzędzi open source, które współpracują z systemami obsługi administracyjnej u dostawców usług.

### Tematy pokrewne

Zezwalanie na aktualizacje profili i konfigurowanie aktualizacji, na stronie 36

# Zezwalanie na aktualizacje profili i konfigurowanie aktualizacji

Można zezwolić na aktualizowanie profili w określonych odstępach czasu. Zaktualizowane profile są wysyłane z serwera do telefonu przy użyciu protokołu TFTP, HTTP lub HTTPS.

### Zanim rozpoczniesz

Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

### Procedura

**Krok 1** Wybierz kolejno opcje **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**.

**Krok 2** W sekcji **Profil konfiguracji** (Configuration Profile) na liście rozwijanej **Włącz obsługę administracyjną** (Provision Enable) wybierz opcję **Tak** (Yes).

**Krok 3** Wprowadź parametry.

**Krok 4** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

**Tematy pokrewne**

Aktualizacje profili i uaktualnienia oprogramowania sprzętowego, na stronie 36

# Zezwalanie na uaktualnianie oprogramowania sprzętowego i konfigurowanie uaktualniania

Można zezwolić na aktualizowanie oprogramowania sprzętowego w określonych odstępach czasu. Zaktualizowane oprogramowanie sprzętowe jest wysyłane z serwera do telefonu przy użyciu protokołu TFTP lub HTTP. Podczas uaktualniania oprogramowania sprzętowego kwestie bezpieczeństwa są mniej istotne, ponieważ to oprogramowanie nie zawiera danych osobowych.

### Zanim rozpoczniesz

Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

### Procedura

**Krok 1** Wybierz kolejno opcje **Głos** > **Obsługa administracyjna**.

**Krok 2** W części **Uaktualnianie oprogramowania sprzętowego** (Firmware Upgrade) na liście rozwijanej **Włącz uaktualnianie** (Upgrade Enable) wybierz opcję **Tak** (Yes).

**Krok 3** Wprowadź parametry.

**Krok 4** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

# Uaktualnienie oprogramowania sprzętowego przy użyciu protokołu TFTP, HTTP lub HTTPS

Telefon obsługuje uaktualnianie przy użyciu jednego obrazu za pośrednictwem protokołu TFTP, HTTP lub HTTPS.

**Uwaga** Zmiana na starszą wersję może być możliwa tylko na wybranych urządzeniach. Więcej informacji można znaleźć w uwagach do wersji dla używanego telefonu i wersji oprogramowania sprzętowego.

### Zanim rozpoczniesz

Plik pakietu oprogramowania sprzętowego musi zostać pobrany na dostępny serwer.

### Procedura

**Krok 1** Zmień nazwę obrazu w następujący sposób:

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

gdzie:

**`x8xx`** to seria telefonu, np. 6841.

**`aa-b-c`** to numer wersji, np. 10-4-1.

**Krok 2** Do rozpakowania pliku tar użyj polecenia **`tar –xzvf`**.

**Krok 3** Skopiuj folder do katalogu pobierania na serwerze TFTP, HTTP lub HTTPS.

**Krok 4** Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

**Krok 5** Wybierz kolejno opcje **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**.

**Krok 6** Znajdź plik pakietu, którego nazwa kończy się rozszerzeniem **.loads**, i dołącz go do prawidłowego adresu URL.

**Krok 7** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

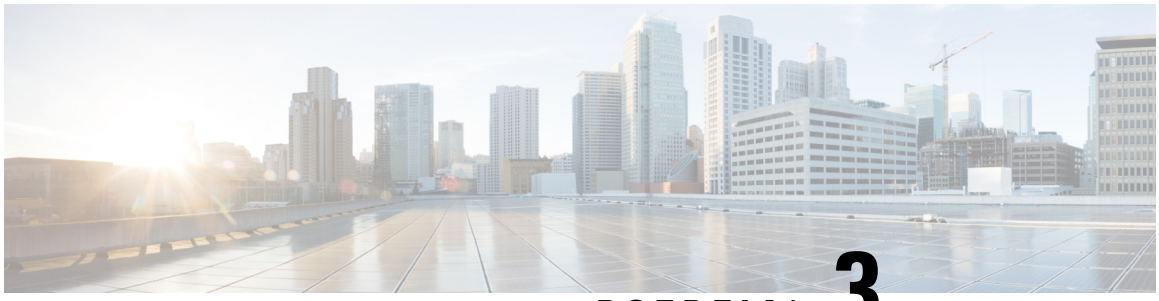
# Uaktualnianie oprogramowania sprzętowego za pomocą polecenia w przeglądarce

W celu uaktualnienia oprogramowania sprzętowego w telefonie można wpisać polecenie uaktualniania na pasku adresu w przeglądarce. Telefon zostanie zaktualizowany tylko wtedy, gdy jest wolny. System spróbuje automatycznie wykonać aktualizację po zakończeniu połączenia.

### Procedura

Aby uaktualnić telefon przy użyciu adresu URL w przeglądarce WWW, wprowadź następujące polecenie:

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



ROZDZIAŁ 3

# Wstępna obsługa administracyjna w sieci wewnętrznej i serwery obsługi administracyjnej



## Wstępna obsługa administracyjna w sieci wewnętrznej i serwery obsługi administracyjnej

Dostawca usług zapewnia wstępną obsługę administracyjną (z wyjątkiem urządzeń dostosowywanych zdalnie) za pomocą profilu. Profil wstępnej obsługi administracyjnej może zawierać ograniczony zbiór parametrów, które służą tylko do synchronizacji telefonu. Jednak w profilu mogą się również znajdować wszystkie parametry dostarczane ze zdalnego serwera. Domyślnie telefon synchronizuje się ponownie po włączeniu zasilania oraz w odstępach czasu skonfigurowanych w profilu. Gdy użytkownik podłączy telefon w swojej siedzibie, urządzenie pobierze zaktualizowany profil i wszelkie aktualizacje oprogramowania sprzętowego.

Ten proces wstępnej obsługi administracyjnej, wdrażania i zdalnej obsługi administracyjnej może być realizowany na wiele sposobów.

## Przygotowanie serwera i narzędzia programowe

Przykłady w tym rozdziale wymagają dostępności co najmniej jednego serwera. Serwery mogą być zainstalowane i uruchomione na lokalnym komputerze:

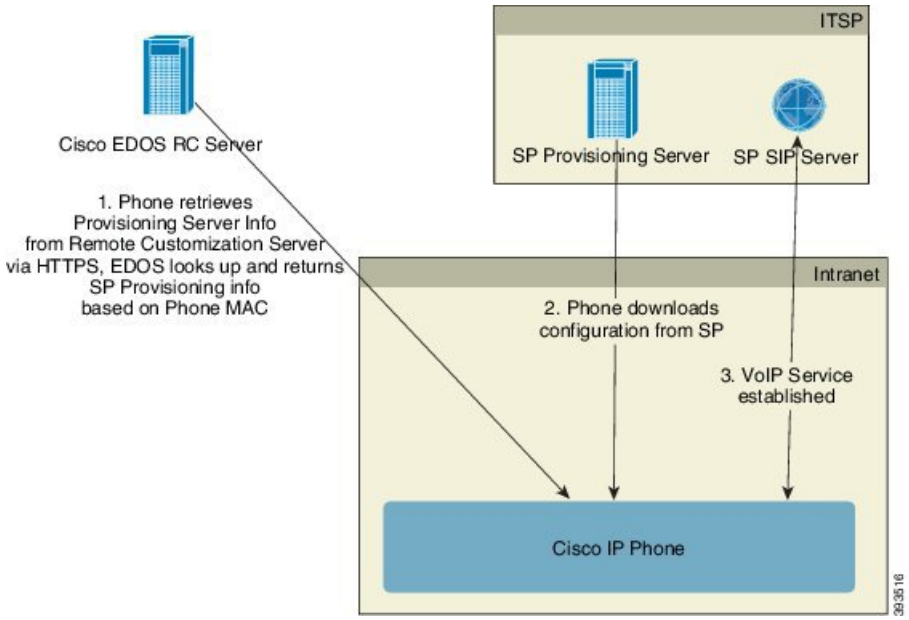
- TFTP (port UDP 69)
- Dziennik systemu (port UDP 514)
- HTTP (port TCP 80)
- HTTPS (port TCP 443)

Aby ułatwić rozwiązywanie ewentualnych problemów z konfiguracją serwerów, warto instalować klienty różnych typów serwerów na osobnych komputerach. Pomoże to zapewnić prawidłowe działanie serwerów, niezależne od interakcji z telefonami.

Zalecamy również zainstalowanie następujących narzędzi programowych:

- Do generowania profili konfiguracji zainstaluj narzędzie kompresujące open source gzip.
- Do szyfrowania profili i obsługi serwerów HTTPS zainstaluj pakiet oprogramowania open source OpenSSL.
- Do testowania funkcji dynamicznego tworzenia profili i jednoetapowego włączania zdalnej obsługi administracyjnej przy użyciu protokołu HTTPS zalecamy zainstalowanie kompilatora języka skryptowego z obsługą skryptów CGI. Przykładem takiego kompilatora są narzędzia open source języka Perl.
- Do sprawdzania bezpieczeństwa wymiany danych między serwerami obsługi administracyjnej a telefonami zainstaluj narzędzie do podsłuchiwania pakietów Ethernet (na przykład bezpłatne narzędzie Ethereal/Wireshark). Przechwyć informacje o pakietach Ethernet w interakcji między telefonem a serwerem obsługi administracyjnej. W tym celu uruchom narzędzie do podsłuchiwania pakietów na komputerze podłączonym do przełącznika z włączonym dublowaniem portów. Do operacji realizowanych za pośrednictwem protokołu HTTPS można używać narzędzia ssldump.

# Dystrybucja za pośrednictwem serwera zdalnego dostosowywania (RC)




Wszystkie telefony komunikują się z serwerem RC EDOS Cisco do momentu, aż otrzymają wstępną obsługę administracyjną.

W modelu dystrybucji z serwerem RC klient kupuje telefon, który został już skojarzony z określonym dostawcą usług na serwerze RC EDOS Cisco. Dostawca usług telefonii internetowej (ITSP) konfiguruje i utrzymuje serwer obsługi administracyjnej oraz rejestruje informacje z tego serwera na serwerze RC EDOS Cisco.

Gdy telefon bez obsługi administracyjnej, ale podłączony do Internetu, zostanie włączony, będzie miał stan dostosowania **Otwarte**. Telefon najpierw wysyła do lokalnego serwera DHCP zapytanie o dane serwera

obsługi administracyjnej i ustawia swój stan dostosowania. Jeśli zapytanie do serwera DHCP powiedzie się, stan dostosowania jest ustawiany na **Przerwano**, a system nie próbuje dokonać zdalnego dostosowania, ponieważ serwer DHCP przekazał niezbędne informacje z serwera obsługi administracyjnej.

Gdy telefon nawiązuje połączenie z siecią po raz pierwszy lub po przywróceniu do ustawień fabrycznych, to w razie nieskonfigurowania opcji usługi DHCP kontaktuje się z serwerem aktywacji urządzeń w scenariuszu automatycznego inicjowania obsługi administracyjnej (konfiguracji automatycznej). W nowych telefonach inicjowanie obsługi administracyjnej będzie się odbywało przez domenę "activate.cisco.com", a nie "webapps.cisco.com". Telefony z oprogramowaniem sprzętowym w wersji starszej niż 11.2(1) nadal będą używały domeny webapps.cisco.com. Cisco zaleca, aby w zaporze zezwolić na ruch z obu domen.

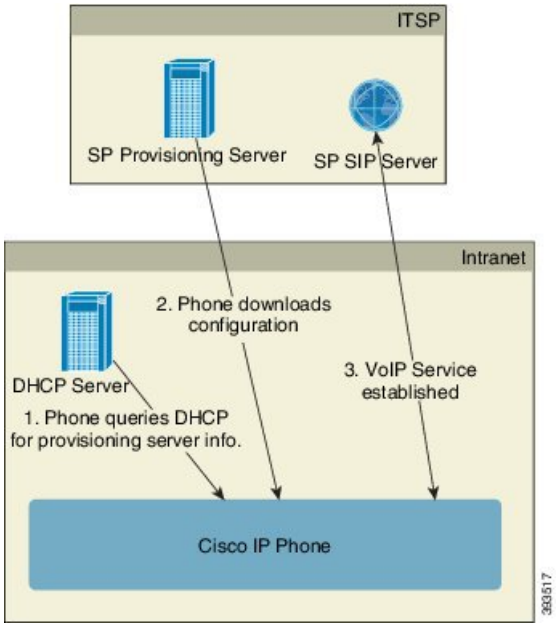
Jeśli serwer DHCP nie przekaże danych serwera obsługi administracyjnej, telefon wysyła zapytanie do serwera RC EDOS Cisco, przekazuje swój adres MAC i model, po czym ustawia stan dostosowania **Operacja oczekująca**. Serwer EDOS Cisco odpowiada informacjami z serwera obsługi administracyjnej skojarzonego z dostawcą usług, w tym przekazuje adres URL serwera obsługi administracyjnej, a stan dostosowania telefonu jest ustawiany na **Niestandardowe oczekujące**. Następnie telefon wykonuje polecenie z adresem URL ponownej synchronizacji w celu pobrania konfiguracji dostawcy usług. Jeżeli ta operacja się powiedzie, stan dostosowania jest ustawiany na **Pobrano**.

Jeśli na serwerze RC EDOS Cisco telefon nie jest skojarzony z żadnym dostawcą usług, stan dostosowania telefonu jest ustawiany na **Niedostępne**. Telefon można skonfigurować ręcznie lub na serwerze EDOS Cisco można dodać skojarzenie dostawcy usług z telefonem.

Jeśli obsługa administracyjna telefonu jest wykonywana z wyświetlacza LCD lub internetowego narzędzia konfiguracyjnego, przed ustawieniem stanu dostosowania **Pobrano** jest ustawiany stan **Przerwano**, a do serwera EDOS Cisco nie będzie wysyłane zapytanie, chyba że na telefonie zostaną przywrócone ustawienia fabryczne.

Po zainicjowaniu obsługi administracyjnej telefonu serwer RC EDOS Cisco przestaje być używany do czasu, aż nastąpi przywrócenie ustawień fabrycznych telefonu.

# Wstępna obsługa administracyjna w sieci wewnętrznej




Zgodnie z domyślną fabryczną konfiguracją Cisco telefon automatycznie próbuje się synchronizować z profilem przechowywanym na serwerze TFTP. Zarządzany serwer DHCP w sieci LAN dostarcza do urządzenia informacje o profilu i o skonfigurowanym serwerze TFTP wstępnej obsługi administracyjnej. Dostawca usług podłącza każdy nowy telefon do sieci LAN. Telefon automatycznie synchronizuje się ponownie z lokalnym serwerem TFTP i inicjuje swój wewnętrzny stan w celu przygotowania do wdrożenia. Zazwyczaj profil wstępnej obsługi administracyjnej zawiera adres URL zdalnego serwera obsługi administracyjnej. Po wdrożeniu urządzenia i podłączeniu go do sieci u klienta serwer obsługi administracyjnej na bieżąco aktualizuje urządzenia.

Zanim telefon ze wstępną obsługą administracyjną zostanie wysłany do klienta, można zeskanować jego kod kreskowy i zapisać adres MAC lub numer seryjny. Informację tę można wykorzystać do utworzenia profilu, z którym telefon będzie synchronizowany.

Po odebraniu telefonu klient podłącza go do sieci szerokopasmowej. Gdy telefon zostanie włączony, skontaktuje się z serwerem obsługi administracyjnej przy użyciu adresu URL skonfigurowanego w fazie wstępnej obsługi administracyjnej. W ten sposób telefon może się wielokrotnie synchronizować i zgodnie z potrzebami aktualizować swój profil oraz oprogramowanie sprzętowe.

### Tematy pokrewne

Dystrybucja detaliczna, na stronie 5
Obsługa administracyjna przy użyciu protokołu TFTP, na stronie 43

# Konfiguracja serwera obsługi administracyjnej

W tej części opisano wymagania konfiguracyjne w zakresie obsługi administracyjnej telefonu przy użyciu różnych serwerów i w różnych scenariuszach. Na potrzeby tego dokumentu i wykonywania testów serwery

obsługi administracyjnej zostały zainstalowane i uruchomione na lokalnym komputerze. Ponadto do zapewnienia obsługi administracyjnej telefonów przydadzą się ogólnie dostępnie narzędzia programowe.

# Obsługa administracyjna przy użyciu protokołu TFTP

Telefony mogą współpracować z serwerem TFTP podczas ponownych synchronizacji na potrzeby obsługi administracyjnej i uaktualniania oprogramowania sprzętowego. Podczas wdrażania urządzeń zdalnie zaleca się używanie serwera HTTPS, jednak można również używać serwerów HTTP i TFTP. Następnie w celu zwiększenia bezpieczeństwa należy włączyć obsługę administracyjną funkcji szyfrowania plików, ponieważ oferuje ona większą niezawodność dzięki wykorzystywaniu mechanizmów translacji adresów sieciowych i ochrony routerów. Serwer TFTP sprawdza się dobrze w wewnętrznej obsłudze administracyjnej dużej liczby urządzeń.

Telefon może pobierać adres IP serwera TFTP bezpośrednio z serwera DHCP przy użyciu jego opcji 66. Jeśli w parametrze Profile_Rule skonfigurowano ścieżkę do pliku na tym serwerze TFTP, profil zostanie pobrany na urządzenie z serwera TFTP. Pobieranie nastąpi po podłączeniu urządzenia do sieci LAN i włączeniu go.

Parametr Profile_Rule w domyślnej konfiguracji fabrycznej ma wartość *&PN*.cfg, gdzie *&PN* reprezentuje nazwę modelu telefonu.

Na przykład dla modelu CP-6841-3PCC plik nosi nazwę CP-6841-3PCC.cfg.

Na urządzeniu z domyślnym profilem fabrycznym po włączeniu zasilania następuje ponowna synchronizacja z tym plikiem umieszczonym na lokalnym serwerze TFTP określonym w opcji 66 serwera DHCP. Ścieżka do pliku jest względna wobec wirtualnego katalogu głównego serwera TFTP.

### Tematy pokrewne

Wstępna obsługa administracyjna w sieci wewnętrznej, na stronie 42

## Kontrola zdalnych punktów końcowych i mechanizm NAT

Telefon obsługuje mechanizm translacji adresów sieciowych (NAT) umożliwiający dostęp do Internetu za pośrednictwem routera. W celu zwiększenia bezpieczeństwa router może próbować zablokować nieautoryzowane pakiety przychodzące poprzez zaimplementowanie symetrycznego mechanizmu NAT — strategii filtrowania pakietów, która znacząco ogranicza grupę pakietów mających pozwolenie na wejście do chronionej sieci z Internetu. Z tego powodu nie zaleca się zdalnej obsługi administracyjnej za pośrednictwem protokołu TFTP.

Funkcjonalność VoIP może współistnieć z mechanizmem NAT tylko pod warunkiem zapewnienia możliwości przechodzenia ruchu przez zabezpieczenia NAT. Konfigurowanie prostego przechodzenia ruchu protokołu UDP przez zabezpieczenia NAT. Ta opcja wymaga, aby użytkownik miał:

- Dynamiczny zewnętrzny (publiczny) adres IP z usługi
- Komputer z zainstalowanym oprogramowaniem serwera STUN
- Urządzenie brzegowe z mechanizmem asymetrycznej translacji adresów sieciowych

# Obsługa administracyjna przy użyciu protokołu HTTP

Telefon zachowuje się podobnie do przeglądarki, która żąda stron WWW ze zdalnej witryny internetowej. Takie rozwiązanie pozwala niezawodnie dotrzeć do serwera obsługi administracyjnej, nawet jeśli na routerze

klienta zaimplementowano symetryczną translację adresów sieciowych (NAT) lub inne mechanizmy ochrony. W zdalnych wdrożeniach protokoły HTTP i HTTPS działają bardziej niezawodnie niż protokół TFTP, szczególnie jeśli połączone wdrożone urządzenia znajdują się za lokalnymi zaporami lub routerami z funkcją NAT. Protokoły HTTP i HTTPS są używane zamiennie w scenariuszach z poniższymi rodzajami żądań.

W podstawowej obsłudze administracyjnej opartej na protokole HTTP profile konfiguracji są pobierane za pomocą metody HTTP GET. Zazwyczaj plik konfiguracyjny jest tworzony dla każdego wdrożonego telefonu, a powstałe pliki są przechowywane w katalogu na serwerze HTTP. Gdy serwer odbierze żądanie GET, po prostu zwraca plik wskazany w nagłówku tego żądania.

Profil konfiguracji nie musi być statyczny, ale może być generowany dynamicznie poprzez wykonanie zapytania do bazy danych klientów. W oparciu o otrzymane informacje zostanie utworzony na bieżąco.

Gdy telefon żąda ponownej synchronizacji, może za pomocą metody HTTP POST wnioskować o odpowiednie dane konfiguracyjne. Na urządzeniu można skonfigurować przekazywanie pewnych informacji o stanie i identyfikacyjnych do serwera w treści żądania HTTP POST. Na podstawie tych informacji serwer wygeneruje żądany profil konfiguracji w celu przesłania go w odpowiedzi albo może zapisać informacje o stanie na potrzeby późniejszej analizy i monitorowania.

W ramach żądań GET i POST telefon automatycznie dołącza podstawowe informacje identyfikacyjne w polu User-Agent w nagłówku żądania. Informacje te obejmują producenta, nazwę produktu, obecną wersję oprogramowania sprzętowego i numer seryjny urządzenia.

Oto przykładowe pole User-Agent w żądaniu dla modelu CP-6841-3PCC:

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

Jeżeli na telefonie ustawiono ponowne synchronizowanie z profilem konfiguracji przy użyciu protokołu HTTP, zalecamy stosowanie protokołu HTTPS albo szyfrowane profilu, tak aby zapewnić ochronę poufnych informacji. Zaszyfrowane profile konfiguracji pobierane przez telefon za pośrednictwem protokołu HTTP nie są narażone na ryzyko ujawnienia zawartych w nich poufnych informacji. W porównaniu z używaniem protokołu HTTPS ten tryb ponownej synchronizacji w mniejszym stopniu obciąża serwer obsługi administracyjnej zadaniami obliczeniowymi.

Telefon potrafi odszyfrować profile zaszyfrowane za pomocą jednej z następujących metod:

- Szyfrowanie AES-256-CBC
- Szyfrowanie zgodne z dokumentem RFC-8188 przy użyciu szyfru AES-128-GCM

**Uwaga** Telefony obsługują protokół HTTP w wersjach 1.0 i 1.1, a jeśli wynegocjowanym protokołem transmisji jest HTTP 1.1, dodatkowo obsługą kodowanie fragmentów.

## Obsługa kodów stanu protokołu HTTP w operacjach ponownej synchronizacji i uaktualniania

Telefon obsługuje nadsyłanie odpowiedzi przez protokół HTTP podczas zdalnej obsługi administracyjnej (ponownej synchronizacji). Obecne zachowanie telefonu można podzielić na trzy kategorie:

- A — Powodzenie, gdzie wartości „Okresowa ponowna synchronizacja” i „Losowe opóźnienie ponownej synchronizacji” określają kolejne żądania.

- B — Niepowodzenie z powodu błędu Nie znaleziono pliku lub uszkodzenia profilu. Wartość „Opóźnienie kolejnych prób po błędzie synchronizacji" określa kolejne żądania.
- C — Inny problem, błąd połączenia powodowany przez błędny adres URL lub IP. Wartość „Opóźnienie kolejnych prób po błędzie synchronizacji" określa kolejne żądania.

***Tabela 2: Zachowanie telefonu w odpowiedziach HTTP***

| Kod stanu protokołu HTTP | Opis | Zachowanie telefonu |
|---|---|---|
| **301 Trwale przeniesiono** | To i przyszłe żądania powinny być kierowane do nowej lokalizacji. | Należy natychmiast spróbować wysłać żądanie do nowej lokalizacji. |
| **302 Znaleziono** | Zwane inaczej „Tymczasowo przeniesiono". | Należy natychmiast spróbować wysłać żądanie do nowej lokalizacji. |
| **3xx** | Inne odpowiedzi w formacie 3xx nie są przetwarzane. | C |
| **400 Nieprawidłowe żądanie** | Nie można zrealizować żądania z powodu niepoprawnej składni. | C |
| **401 Brak autoryzacji** | Monit o dostęp przy użyciu uwierzytelniania podstawowego lub szyfrowanego. | Należy natychmiast spróbować wysłać żądanie z poświadczeniami uwierzytelniania. Maksymalnie 2 próby. W razie niepowodzenia zachowanie telefonu odpowiada zachowaniu C. |
| **403 Zabronione** | Serwer odmawia odpowiedzi. | C |
| **404 Nie znaleziono** | Nie znaleziono żądanego zasobu. Klient może wysyłać kolejne żądania. | B |
| **407 Wymagane uwierzytelnianie serwera proxy.** | Monit o dostęp przy użyciu uwierzytelniania podstawowego lub szyfrowanego. | Należy natychmiast spróbować wysłać żądanie z poświadczeniami uwierzytelniania. Maksymalnie 2 próby. W razie niepowodzenia zachowanie telefonu odpowiada zachowaniu C. |
| **4xx** | Inne kody stanów błędów klientów nie są przetwarzane. | C |
| **500 Wewnętrzny błąd serwera** | Standardowy komunikat o błędzie. | Zachowanie telefonu odpowiada zachowaniu C. |
| **501 Nie zaimplementowano** | Serwer nie rozpoznaje metody żądania lub nie jest w stanie zrealizować żądania. | Zachowanie telefonu odpowiada zachowaniu C. |

| Kod stanu protokołu HTTP | Opis | Zachowanie telefonu |
|---|---|---|
| **502 Nieprawidłowa brama** | Serwer pełni rolę bramy lub serwera proxy i odebrał nieprawidłową odpowiedź z nadrzędnego serwera. | Zachowanie telefonu odpowiada zachowaniu C. |
| **503 Usługa niedostępna** | Serwer jest obecnie niedostępny (przeciążony lub wyłączony w związku z konserwacją). Jest to stan tymczasowy. | Zachowanie telefonu odpowiada zachowaniu C. |
| **504 Limit czasu bramy** | Serwer pełni rolę bramy lub serwera proxy i nie otrzymał w odpowiednim czasie odpowiedzi z nadrzędnego serwera. | C |
| **5xx** | Inny błąd serwera | C |

# Obsługa administracyjna przy użyciu protokołu HTTPS

Obsługa administracyjna telefonu jest możliwa przy użyciu protokołu HTTPS, co zapewnia większe bezpieczeństwo zarządzania zdalnie wdrożonymi urządzeniami. Do każdego telefonu jest przypisany unikatowy certyfikat klienta SSL (i skojarzony z nim klucz prywatny) oraz główny certyfikat serwera wystawiony przez urząd certyfikacji Sipura CA. Ten ostatni umożliwia telefonowi rozpoznawanie autoryzowanych serwerów obsługi administracyjnej i odrzucanie nieautoryzowanych. Z drugiej strony certyfikat klienta umożliwia serwerowi obsługi administracyjnej zidentyfikowanie konkretnego urządzenia, które wysłało żądanie.

Aby dostawca usług mógł zarządzać wdrożeniem przy użyciu protokołu HTTPS, dla każdego serwera obsługi administracyjnej, z którym telefony będą się ponownie synchronizowały przez protokół HTTPS, musi być wygenerowany certyfikat serwera. Certyfikat serwera musi być podpisany kluczem głównym wystawionym przez urząd certyfikacji skonfigurowany na serwerze Cisco, a certyfikat tego urzędu musi się znajdować na wszystkich wdrożonych urządzeniach. Aby uzyskać podpisany certyfikat serwera, dostawca usług musi przesłać żądanie podpisania certyfikatu do firmy Cisco. Cisco podpisze certyfikat i odeśle go z prośbą o zainstalowanie na serwerze obsługi administracyjnej.

Certyfikat serwera obsługi administracyjnej musi zawierać pole Nazwa pospolita (CN), a w temacie nazwę FQDN hosta, na którym działa serwer. Opcjonalnie po nazwie FQDN mogą się znajdować dodatkowe informacje, które należy oddzielić znakiem ukośnika (/). Poniżej znajdują się przykłady wpisów CN, które telefon akceptuje jako prawidłowe:

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

Telefon nie tylko weryfikuje certyfikat serwera, ale również sprawdza adres IP serwera poprzez wyszukiwanie w usłudze DNS nazwy serwera podanej w certyfikacie serwera.

## Uzyskiwanie podpisanego certyfikatu serwera

Narzędzie OpenSSL może wygenerować żądanie podpisania certyfikatu. W poniższym przykładzie pokazano polecenie narzędzia **openssl**, które powoduje wygenerowanie pary 1024-bitowych kluczy prywatnego/publicznego RSA oraz żądania podpisania certyfikatu:

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

To polecenie generuje klucz prywatny serwera w pliku **privkey.pem** oraz odpowiednie żądanie podpisania certyfikatu w pliku **provserver.csr**. Dostawca usług zachowuje poufność pliku **privkey.pem**, a plik **provserver.csr** wysyła do Cisco w celu podpisania. Po odebraniu pliku **provserver.csr** Cisco generuje plik **provserver.crt** — podpisany certyfikat serwera.

### Procedura

**Krok 1** Przejdź do strony https://software.cisco.com/software/edos/home i zaloguj się przy użyciu swoich poświadczeń CCO.

**Uwaga** Gdy telefon nawiązuje połączenie z siecią po raz pierwszy lub po przywróceniu do ustawień fabrycznych, to w razie nieskonfigurowania opcji usługi DHCP kontaktuje się z serwerem aktywacji urządzeń w scenariuszu automatycznego inicjowania obsługi administracyjnej (konfiguracji automatycznej). W nowych telefonach inicjowanie obsługi administracyjnej odbywa się przez domenę "activate.cisco.com", a nie "webapps.cisco.com". Telefony z oprogramowaniem sprzętowym w wersji starszej niż 11.2(1) nadal będą używały domeny "webapps.cisco.com". Zaleca się, aby w zaporze zezwolić na ruch z obu domen.

**Krok 2** Wybierz opcję **Zarządzanie certyfikatami** (Certificate Management).

Na karcie **Podpisz żądanie CSR** (Sign CSR) żądanie CSR z poprzedniego kroku jest załadowane i oczekuje na podpisanie.

**Krok 3** Na liście rozwijanej **Wybierz produkt** (Select Product) wybierz pozycję **Oprogramowanie sprzętowe SPA1xx 1.3.3 i nowsze /Oprogramowanie sprzętowe SPA232D 1.3.3 i nowsze / Oprogramowanie sprzętowe SPA5xx 7.5.6 i nowsze /CP-78xx-3PCC/CP-88xx-3PCC** (SPA1xx firmware 1.3.3 and newer/SPA232D firmware 1.3.3 and newer/SPA5xx firmware 7.5.6 and newer/CP-78xx-3PCC/CP-88xx-3PCC).

**Uwaga** Ten produkt obejmuje wieloplatformowe telefony Cisco IP Phone z serii 6800.

**Krok 4** W polu **Plik CSR** (CSR File) kliknij przycisk **Przeglądaj** (Browse) i wybierz żądanie CSR, które chcesz podpisać.

**Krok 5** Wybierz metodę szyfrowania:

- MD5
- SHA1
- SHA256

Cisco zaleca wybór opcji szyfrowania SHA256.

**Krok 6** Na liście rozwijanej **Czas trwania zalogowania** (Sign in Duration) zaznacz odpowiedni czasu trwania (na przykład 1 rok).

**Krok 7** Kliknij przycisk **Podpisz żądanie certyfikatu** (Sign Certificate Request).

**Krok 8** Wybierz jedną z następujących opcji odebrania podpisanego certyfikatu:

- **Wprowadź adres e-mail odbiorcy** (Enter Recipient's Email Address) — Jeśli chcesz otrzymać certyfikat pocztą elektroniczną, w tym polu wpisz swój adres e-mail.
- **Pobierz** (Download) — Ta opcja pozwala bezpośrednio pobrać podpisany certyfikat.

**Krok 9** Kliknij przycisk **Wyślij**.

Podpisany certyfikat serwera zostanie wysłany pocztą e-mail na podany wcześniej adres lub pobrany.

## Certyfikat główny klienta wystawiany przez urząd certyfikacji dla telefonu wieloplatformowego

Wieloplatformowe telefony Cisco okazują dostawcom usług certyfikaty główne klienta. Taki certyfikat główny potwierdza autentyczność certyfikatu klienta znajdującego się na każdym telefonie. Wieloplatformowe telefony obsługują również podpisane certyfikaty innych firm, takich jak Verisign, Cybertrust itd.

Unikatowy certyfikat klienta okazywany przez każde urządzenie podczas sesji komunikacji przy użyciu protokołu HTTPS zawiera informacje identyfikacyjne osadzone w polu tematu. Informacje te mogą być udostępniane przez serwer HTTPS skryptowi CGI wywoływanemu w celu obsługi bezpiecznych żądań. W szczególności temat certyfikatu wskazuje nazwę produktu urządzenia (element OU), adres MAC (element S) i numer seryjny (element L).

W poniższym przykładzie certyfikatu klienta wieloplatformowego telefonu Cisco IP Phone 6841 widać te elementy:

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

Aby ustalić, czy telefon zawiera indywidualny certyfikat, użyj zmiennej makra obsługi administracyjnej $CCERT. Zmienna rozwija się do wartości Zainstalowano lub Nie zainstalowano, zależnie od obecności lub braku unikatowego certyfikatu klienta. W przypadku ogólnego certyfikatu numer seryjny urządzenia można uzyskać z pola User-Agent w nagłówku żądania HTTP.

Na serwerach HTTPS można skonfigurować wysyłanie żądań o certyfikaty SSL z klientów nawiązujących połączenie. Po włączeniu tej opcji serwer może używać głównego certyfikatu klienta umieszczonego przez Cisco na telefonie wieloplatformowym do weryfikowania certyfikatu klienta. Następnie serwer może przekazać informacje z certyfikatu do skryptu CGI w celu dalszego przetwarzania.

Certyfikat może być przechowywany w różnych miejscach. Na przykład w instalacji serwera Apache do przechowywania certyfikatu podpisanego serwer obsługi administracyjnej, jego powiązanego klucza prywatnego oraz głównego certyfikatu klienta wystawionego przez urząd certyfikacji na telefonie wieloplatformowym są używane następujące ścieżki plików:

```
# 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
```

Szczegółowe informacje można znaleźć w dokumentacji serwera HTTPS.

Główny urząd certyfikacji na kliencie Cisco podpisuje każdy unikatowy certyfikat. Odpowiedni certyfikat główny jest udostępniany dostawcom usług na potrzeby uwierzytelniania klienta.

## Zapasowe serwery obsługi administracyjnej

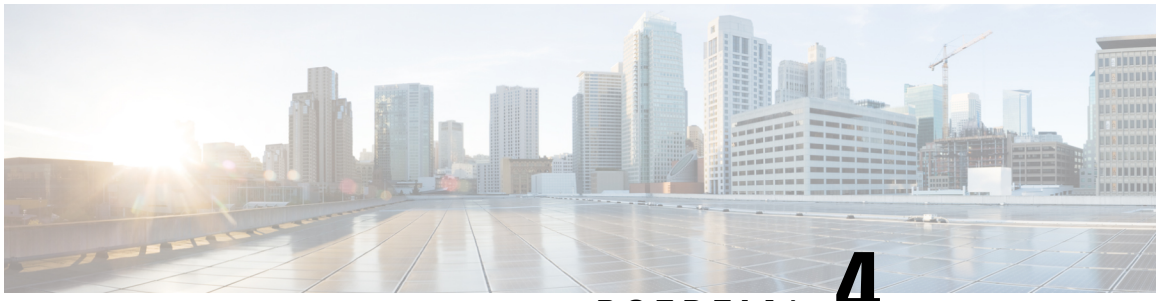
Serwer obsługi administracyjnej można określić za pomocą adresu IP lub w pełni kwalifikowanej nazwy domeny (FQDN). Użycie nazwy FQDN umożliwia dodanie zapasowych serwerów obsługi administracyjnej. Jeżeli serwer obsługi administracyjnej jest identyfikowany za pomocą nazwy FQDN, telefon próbuje zinterpretować nazwę FQDN jako adres IP za pośrednictwem systemu DNS. W obsłudze administracyjnej można stosować wyłącznie rekordy DNS typu A; rozpoznawanie adresów zapisanych w rekordach SRV nie działa. Telefon kontynuuje przetwarzanie rekordów A do uzyskania odpowiedzi serwera. Jeśli żaden serwer skojarzony z rekordem A nie odpowie, telefon zarejestruje błąd na serwerze dziennika systemu.

## Serwer dziennika systemowego

Jeśli serwer dziennika systemowego został skonfigurowany w telefonie przy użyciu parametrów w grupie <Serwer dziennika systemu>, operacje ponownej synchronizacji i uaktualniania będą powodowały wysyłanie komunikatów do tego serwera. Komunikat może być generowany na początku żądania przesłania zdalnego pliku (profilu konfiguracji lub oprogramowania sprzętowego) oraz po zakończeniu operacji (wskazując powodzenie lub niepowodzenie).

Rejestrowane komunikaty konfiguruje się w poniższych parametrach i są one rozwijane w makra do faktycznych komunikatów dziennika systemowego:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



ROZDZIAŁ 4

# Przykłady obsługi administracyjnej



# Przykłady obsługi administracyjnej — omówienie

Ten rozdział zawiera przykładowe procedury wysyłania profili konfiguracji między telefonem a serwerem obsługi administracyjnej.

Informacje na temat tworzenia profili konfiguracji zawiera część Skrypty obsługi administracyjnej, na stronie 13.

# Podstawowa ponowna synchronizacja

W tej części opisano funkcję podstawowej ponownej synchronizacji dostępną w telefonie.

## Ponowna synchronizacja przy użyciu protokołu TFTP

Profile konfiguracji można pobierać na telefon przy użyciu wielu protokołów sieciowych. Podstawowym protokołem wykorzystywanym do przesyłania profili jest protokół TFTP (RFC1350). Protokół TFTP jest szeroko stosowany do obsługi urządzeń sieciowych wewnątrz prywatnych sieci LAN. Wprawdzie nie zaleca się używania protokołu TFTP do wdrażania zdalnych punktów końcowych w Internecie, jednak może on być wygodnym rozwiązaniem podczas wdrożeń w małych organizacjach do zapewnienia wstępnej obsługi administracyjnej w sieci wewnętrznej oraz na potrzeby opracowywania i testowania rozwiązań. Więcej informacji o wstępnej obsłudze administracyjnej w sieci wewnętrznej zawiera temat Wstępna obsługa administracyjna w sieci wewnętrznej, na stronie 42. W poniższej procedurze profil jest modyfikowany po pobraniu pliku z serwera TFTP.

### Procedura

**Krok 1** W środowisku sieci LAN połącz komputer z telefonem za pośrednictwem koncentratora, przełącznika lub małego routera.

**Krok 2** Zainstaluj na komputerze i aktywuj serwer TFTP.

**Krok 3** W edytorze tekstu napisz profil konfiguracji, w którym parametr GPP_A ma wartość 12345678, jak pokazano w przykładzie.

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

**Krok 4** Zapisz profil pod nazwą `basic.txt` w katalogu głównym serwera TFTP.

Można sprawdzić, czy serwer TFTP jest prawidłowo skonfigurowany: wyślij żądanie pobrania pliku `basic.txt` z urządzenia klienckiego TFTP innego niż telefon. Najlepiej użyj klienta TFTP podłączonego do innego hosta (tzn. nie do serwera obsługi administracyjnej).

**Krok 5** W przeglądarce WWW na komputerze otwórz stronę admin/advanced configuration. Na przykład jeśli telefon ma adres IP 192.168.1.100:

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

**Krok 6** Wybierz kartę **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**, a następnie sprawdź wartości parametrów ogólnego przeznaczenia od GPP_A do GPP_P. Powinny być puste.

**Krok 7** Otwórz adres URL ponownej synchronizacji w oknie przeglądarki WWW i wykonaj ponowną synchronizację telefonu do profilu konfiguracji `basic.txt`.

Jeśli serwer TFTP ma adres IP 192.168.1.200, polecenie powinno być podobne do poniższego:

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

Gdy telefon otrzyma to polecenie, urządzenie pod adresem 192.168.1.100 zażąda pliku `basic.txt` z serwera TFTP o adresie IP 192.168.1.200. Następnie w telefonie zostanie sprawdzona składnia pobranego pliku i parametr GPP_A otrzyma wartość 12345678.

**Krok 8** Sprawdź, czy parametr został poprawnie zaktualizowany: Odśwież stronę konfiguracji w przeglądarce internetowej na komputerze i wybierz kartę **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**.

Parametr GPP_A powinien teraz zawierać wartość 12345678.

## Protokołowanie komunikatów w dzienniku systemu

Telefon wysyła komunikat dziennika systemu do wyznaczonego serwera dziennika systemu, gdy urządzenie ma rozpocząć ponowną synchronizację z serwerem obsługi administracyjnej, oraz po udanej lub nieudanej ponownej synchronizacji. W celu zidentyfikowania tego serwera można przejść do strony WWW administrowania telefonem (zobacz Otwieranie strony WWW telefonu, na stronie 8), wybrać kolejno opcje

**Głos (Voice)** > **System**, po czym wskazać serwer w parametrze **Serwer dziennika systemu** (Syslog Server) w sekcji **Opcjonalna konfiguracja sieci** (Optional Network Configuration). Skonfiguruj adres IP serwera dziennika systemu na urządzeniu, a następnie obserwuj komunikaty generowane w trakcie wykonywania pozostałych procedur.

### Procedura

**Krok 1** Zainstaluj i aktywuj serwer dziennika systemu na lokalnym komputerze.

**Krok 2** Zaprogramuj adres IP komputera w parametrze Syslog_Server w profilu i prześlij zmiany:

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

**Krok 3** Kliknij kartę **System** i wprowadź w parametrze Syslog_Server wartość lokalnego serwera dziennika systemu.

**Krok 4** Powtórz operację ponownej synchronizacji zgodnie z opisem w punkcie Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51.

W trakcie ponownej synchronizacji w urządzeniu zostaną wygenerowane dwa komunikaty dziennika systemu. Pierwszy komunikat wskazuje, że trwa wykonywanie żądania. Drugi komunikat informuje o powodzeniu lub niepowodzeniu ponownej synchronizacji.

**Krok 5** Sprawdź, czy serwer dziennika systemu odebrał komunikaty podobne do następującego:

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

Aby otrzymywać szczegółowe komunikaty, należy zaprogramować adres IP serwera dziennika systemu w parametrze Debug_Server (zamiast w parametrze Syslog_Server), a w parametrze Debug_Level ustawić wartość z przedziału od 0 do 3 (3 oznacza najbardziej szczegółowy komunikat):

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

Treść tych komunikatów można skonfigurować za pomocą następujących parametrów:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Jeśli dowolny z tych parametrów będzie pusty, odpowiedni komunikat dziennika systemu nie będzie generowany.

## Automatyczne ponowne synchronizowanie urządzenia

Urządzenie może się okresowo samoczynnie synchronizować z serwerem obsługi administracyjnej. Dzięki temu wszystkie zmiany profilu wprowadzone na serwerze są propagowane do urządzenia punktu końcowego (w odróżnieniu od wysyłania jednoznacznego żądania ponownej synchronizacji do punktu końcowego).

Aby zapewnić regularne automatyczne synchronizowanie się telefonu z serwerem, należy zdefiniować w parametrze Profile_Rule adres URL profilu konfiguracji, a w parametrze Resync_Periodic – okres ponawiania.

### Zanim rozpoczniesz

Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

### Procedura

**Krok 1** Wybierz kolejno opcje **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**.

**Krok 2** Zdefiniuj parametr Profile_Rule. W tym przykładzie założono, że serwer TFTP ma adres IP 192.168.1.200.

**Krok 3** W polu **Okresowa ponowna synchronizacja** (Resync Periodic) wprowadź niewielką wartość na potrzeby testowania, np. **30** sekund.

**Krok 4** Kliknij przycisk **Prześlij wszystkie zmiany** (Submit All Changes).

Przy nowym ustawieniu parametru telefon będzie się synchronizował dwa razy na minutę względem pliku konfiguracyjnego określonego w adresie URL.

**Krok 5** Obserwuj komunikaty rejestrowane w dzienniku systemu (zgodnie z opisem w części Protokołowanie komunikatów w dzienniku systemu, na stronie 52).

**Krok 6** Upewnij się, że w polu **Ponowna synchronizacja po zresetowaniu** (Resync On Reset) ustawiono wartość **Tak** (Yes).

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

**Krok 7** Wyłącz i włącz telefon, co wymusi jego ponowną synchronizację z serwerem obsługi administracyjnej.

Jeśli ponowna synchronizacja zakończy się niepowodzeniem z jakiegokolwiek powodu, np. braku odpowiedzi z serwera, urządzenie poczeka przez liczbę sekund ustawioną w parametrze **Opóźnienie kolejnych prób po błędzie synchronizacji** (Resync Error Retry Delay), a następnie ponowi próbę synchronizacji. Jeśli parametr **Opóźnienie kolejnych prób po błędzie synchronizacji** (Resync Error Retry Delay) ma wartość zero, telefon nie będzie ponawiał synchronizacji po jednej nieudanej próbie.

**Krok 8** (Opcjonalnie) Ustaw w polu **Opóźnienie kolejnych prób po błędzie synchronizacji** (Resync Error Retry Delay) niewielką wartość, np. **30**.

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

**Krok 9** Wyłącz serwer TFTP i obserwuj efekty w dzienniku systemu.

# Unikatowe profile, rozwijanie w makra i protokół HTTP

W ramach wdrożenia, w którym na każdym telefonie należy skonfigurować różne wartości wybranych parametrów, takich jak User_ID lub Display_Name, dostawca usług może utworzyć unikatowy profil dla każdego wdrożonego urządzenia, a następnie obsługiwać te profile na serwerze obsługi administracyjnej. Z

kolei każdy telefon należy skonfigurować do ponownych synchronizacji z własnym profilem zgodnie z wcześniej ustaloną konwencją nazewnictwa profili.

Składnia adresu URL profilu może zawierać informacje identyfikacyjne specyficzne dla każdego telefonu, takie jak adres MAC lub numer seryjny. Do tego celu można użyć wbudowanych zmiennych rozwijanych do makr. Rozwijanie do makr eliminuje konieczność podawania tych wartości w wielu miejscach każdego profilu.

Zanim reguła profilu zostanie zastosowana do telefonu jest rozwijana w makro. Funkcja rozwijania do makr może sterować różnymi wartościami. Na przykład:

- $MA rozwija się do 12-cyfrowego adresu MAC urządzenia (adres zawiera znaki szesnastkowe z małymi literami). Na przykład: 000e08abcdef.
- $SN rozwija się do numeru seryjnego urządzenia. Na przykład: 88012BA01234.

W taki sam sposób do makr mogą się rozwijać również inne wartości, w tym wszystkie parametry ogólnego przeznaczenia — od GPP_A do GPP_P. Przykład tego procesu widać w punkcie Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51. Rozwijanie w makra nie jest ograniczone do nazwy pliku w adresie URL, ale może być stosowane również do dowolnej części parametru reguły profilu. Odwołania do tych parametrów odbywają się za pomocą elementów od $A do $P. Pełną listę zmiennych, które mogą się rozwijać w makra, zawiera punkt Zmienne rozwijane w makra, na stronie 79.

W tym ćwiczeniu profil specyficzny dla telefonu jest obsługiwany administracyjnie na serwerze TFTP.

## Ćwiczenie: Włączanie obsługi administracyjnej profilu konkretnego telefonu IP na serwerze TFTP

### Procedura

**Krok 1** Spisz adres MAC telefonu z jego etykiety produktu. (Adres MAC to numer zapisany cyframi i małymi literami w formacie szesnastkowym, np. 000e08aabbcc.

**Krok 2** Skopiuj plik konfiguracyjny `basic.txt` (opisany w części Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51) do nowego pliku o nazwie `CP-xxxx-3PCC macaddress.cfg` (w miejsce `xxxx` wpisując numer modelu, a w miejsce `macaddress` adres MAC telefonu).

**Krok 3** Przenieś nowy plik do głównego katalogu wirtualnego na serwerze TFTP.

**Krok 4** Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

**Krok 5** Wybierz kolejno opcje **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**.

**Krok 6** Wpisz wyrażenie `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` w polu **Reguła profilu** (Profile Rule).

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

**Krok 7** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany). Spowoduje to natychmiastowe ponowne uruchomienie i synchronizację.

Podczas kolejnej synchronizacji telefon pobierze nowy plik, rozwijając wyrażenie makra $MA w adres MAC.

### Ponowna synchronizacja przy użyciu żądania HTTP GET

Protokół HTTP zapewnia bardziej niezawodny mechanizm ponownej synchronizacji niż protokół TFTP, ponieważ ustanawia połączenie przez protokół TCP, podczas gdy TFTP używa mniej pewnego protokołu UDP. Ponadto serwery HTTP mają lepsze funkcje filtrowania i protokołowania niż serwery TFTP.

Urządzenie klienckie (telefon) nie musi mieć żadnego specjalnego ustawienia konfiguracyjnego dla serwera, aby mogło się synchronizować przez protokół HTTP. Składnia parametru Profile_Rule dotycząca używania protokołu HTTP z metodą GET jest podobna do składni używanej dla protokołu TFTP. Jeśli standardowa przeglądarka internetowa jest w stanie pobrać profil z serwera HTTP, powinien to zrobić również telefon.

*Ćwiczenie: Ponowna synchronizacja przy użyciu żądania HTTP GET*

**Procedura**

**Krok 1** Zainstaluj serwer HTTP na lokalnym komputerze lub innym dostępnym hoście.

Serwer typu open source Apache można pobrać z Internetu.

**Krok 2** Skopiuj profil konfiguracji `basic.txt` (opisany w punkcie Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51) do wirtualnego katalogu głównego na zainstalowanym serwerze.

**Krok 3** W celu zweryfikowania poprawności instalacji serwera i możliwości dostępu do pliku `basic.txt` przejdź do profilu z przeglądarki WWW.

**Krok 4** Na telefonie testowym zmodyfikuj parametr Profile_Rule w taki sposób, aby wskazywał serwer HTTP zamiast serwera TFTP, co pozwoli okresowo pobierać profil.

Na przykład przy założeniu, że serwer HTTP ma adres 192.168.1.300, wprowadź następującą wartość:

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

**Krok 5** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany). Spowoduje to natychmiastowe ponowne uruchomienie i synchronizację.

**Krok 6** Obejrzyj w dzienniku systemu komunikaty wysyłane przez telefon. Okresowa ponowna synchronizacja powinna teraz powodować pobieranie profilu z serwera HTTP.

**Krok 7** W dziennikach serwera HTTP obejrzyj sposób wyświetlania informacji identyfikujących telefon testowy w rejestrze agentów użytkownika.

Informacje te powinny obejmować producenta, nazwę produktu, obecną wersję oprogramowania sprzętowego i numer seryjny.

## Obsługa administracyjna za pomocą funkcji XML Cisco

Dla każdego telefonu, oznaczonego tutaj wyrażeniem xxxx, można uruchomić obsługę administracyjną za pomocą funkcji XML Cisco.

W tym celu można wysłać obiekt XML do telefonu, przy użyciu pakietu SIP Notify, lub żądanie HTTP Post do interfejsu CGI telefonu: `http://adresIPtelefonu/CGI/Execute`.

Znacznik CP-xxxx-3PCC rozszerza możliwości funkcji XML Cisco o wsparcie obsługi administracyjnej przy użyciu obiektu XML:

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

Gdy telefon odbierze obiekt XML, pobierze plik obsługi administracyjnej z lokalizacji [reguła profilu]. Zastosowanie makr w tej regule pozwala uprościć tworzenie aplikacji wykorzystującej usługi XML.

## Rozpoznawanie adresu URL z rozwijaniem w makra

Utworzenie na serwerze podkatalogów z wieloma profilami to wygodny sposób zarządzania dużą liczbą wdrożonych urządzeń. Adres URL profilu może zawierać następujące informacje:

- Nazwa serwera lub jawny adres IP serwera obsługi administracyjnej. Jeśli serwer obsługi administracyjnej jest identyfikowany w profilu za pomocą nazwy, telefon wykonuje wyszukiwanie w usłudze DNS w celu jej rozpoznania.
- Niestandardowy port serwera podany w adresie URL za pomocą standardowej składni `:port` po nazwie serwera.
- Podkatalog wirtualnego katalogu głównego serwera zawierający profil, podany za pomocą standardowego zapisu adresu URL i zarządzany poprzez rozwijanie do makra.

Na przykład następujący parametr Profile_Rule powoduje wysłanie do serwera żądania przesłania pliku profilu ($PN.cfg) znajdującego się w podkatalogu `/cisco/config` serwera TFTP działającego na hoście prov.telco.com nasłuchującym komunikacji na porcie 6900:

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

Profil każdego telefonu może być identyfikowany w parametrze ogólnego przeznaczenia, a do jego wartości we wspólnej regule profili będzie się można odwoływać przy użyciu mechanizmu rozwijania w makro.

Załóżmy na przykład, że w parametrze GPP_B zdefiniowano wartość `Dj6Lmp23Q`.

Parametr Profile_Rule ma następującą wartość:

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

Gdy urządzenie wykonuje synchronizację i następuje rozwinięcie makr, telefon o adresie MAC 000e08012345 żąda profilu o nazwie zawierającej adres MAC urządzenia pod następującym adresem URL:

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

# Bezpieczna ponowna synchronizacja przy użyciu protokołu HTTPS

W telefonie są dostępne następujące mechanizmy ponownej synchronizacji przy użyciu procesu bezpiecznej komunikacji:

- Podstawowa ponowna synchronizacja przy użyciu protokołu HTTPS
- Protokół HTTPS z uwierzytelnianiem przy użyciu certyfikatu klienta
- Filtrowanie klientów i dynamiczna zawartość HTTPS

## Podstawowa ponowna synchronizacja przy użyciu protokołu HTTPS

Protokół HTTPS różni się od HTTP dodatkową ochroną za pomocą protokołu SSL na potrzeby zdalnej obsługi administracyjnej, tak aby:

- telefon mógł uwierzytelnić serwer obsługi administracyjnej;
- serwer obsługi administracyjnej mógł uwierzytelnić telefon;
- była zapewniona poufność informacji wymienianych między telefonem a serwerem obsługi administracyjnej.

Mechanizm protokołu SSL generuje i wymienia tajne klucze (symetryczne) w każdym połączeniu między telefonem a serwerem, używając par kluczy publicznych/prywatnych wstępnie zainstalowanych w telefonie i na serwerze obsługi administracyjnej.

Urządzenie klienckie (telefon) nie wymaga żadnych specjalnych ustawień konfiguracyjnych dla serwera, aby mogło się synchronizować przez protokół HTTPS. Składnia parametru Profile_Rule dotycząca używania protokołu HTTPS z metodą GET jest podobna do składni używanej dla protokołu HTTP lub TFTP. Jeśli standardowa przeglądarka internetowa jest w stanie pobrać profil z serwera HTTPS, powinien to zrobić również telefon.

Na serwerze obsługi administracyjnej musi być zainstalowany nie tylko serwer HTTPS, ale również certyfikat serwera SSL podpisany przez Cisco. Urządzenia nie mogą się ponownie synchronizować z serwerem używającym protokołu HTTPS, jeśli nie ma on certyfikatu serwera podpisanego przez Cisco. Instrukcje tworzenia podpisanego certyfikatu SSL dla urządzeń do komunikacji głosowej znajdują się na stronie https://supportforums.cisco.com/docs/DOC-9852.

### Ćwiczenie: Podstawowa ponowna synchronizacja przy użyciu protokołu HTTPS

**Procedura**

**Krok 1** Zainstaluj serwer HTTPS na hoście, którego adres IP jest znany serwerowi DNS przy użyciu zwykłej operacji translacji nazwy hosta.

Serwer open source Apache można skonfigurować do roli serwera HTTPS po zainstalowaniu na nim pakietu open source mod_ssl.

**Krok 2** Wygeneruj żądanie podpisania certyfikatu serwera. W tym kroku może być konieczne zainstalowanie pakietu open source OpenSSL lub analogicznego oprogramowania. Jeśli używasz narzędzia OpenSSL, polecenie generowania podstawowego pliku żądania CSR wygląda następująco:

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

To polecenie spowoduje utworzenie pary klucz publiczny/prywatny, która zostanie zapisana w pliku `privkey.pem`.

**Krok 3** Prześlij plik CSR (provserver.csr) do Cisco w celu podpisania.

Zostanie zwrócony podpisany certyfikat serwera (provserver.cert) oraz certyfikat główny klienta wystawiony przez urząd certyfikacji Sipura — spacroot.cert.

Więcej informacji można znaleźć w sekcji https://supportforums.cisco.com/docs/DOC-9852.

**Krok 4** Zapisz podpisany certyfikat serwera, plik pary kluczy i certyfikat główny klienta w odpowiednich folderach na serwerze.

W przypadku instalacji serwera Apache w systemie Linux są to zazwyczaj następujące lokalizacje:

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

**Krok 5** Uruchom ponownie serwer.

**Krok 6** Skopiuj plik konfiguracyjny `basic.txt` (opisany w punkcie Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51) do wirtualnego katalogu głównego na serwerze HTTPS.

**Krok 7** Sprawdź, czy serwer HTTPS działa poprawnie, pobierając z niego plik `basic.txt` za pomocą standardowej przeglądarki na lokalnym komputerze.

**Krok 8** Sprawdź certyfikat serwera podawany przez serwer.

Przeglądarka prawdopodobnie nie uznaje certyfikatu za prawidłowy, chyba że skonfigurowano w niej wcześniej akceptowanie firmy Cisco jako głównego urzędu certyfikacji. Tak czy inaczej telefony oczekują, że certyfikat będzie podpisany w ten sposób.

Na urządzeniu testowym zmodyfikuj parametr Profile_Rule, tak aby zawierał odwołanie do serwera HTTPS. Na przykład:

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

W tym przykładzie założono, że serwer HTTPS ma nazwę **`my.server.com`**.

**Krok 9** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

**Krok 10** Obejrzyj w dzienniku systemowym zapis operacji wysłany z telefonu.

Komunikat w dzienniku systemowym powinien wskazywać, że wskutek ponownej synchronizacji pobrano profil z serwera HTTPS.

**Krok 11** (Opcjonalne) Za pomocą analizatora protokołu Ethernet w podsieci telefonu sprawdź, czy pakiety są zaszyfrowane.

W tym ćwiczeniu funkcja weryfikowania certyfikatów klienta nie została włączona. Połączenie między telefonem a serwerem jest szyfrowane. Jednak przesyłanie nie jest bezpieczne, ponieważ każde urządzenie klienckie może się połączyć z serwerem i zażądać pliku, o ile tylko zna jego nazwę i katalog. Aby ponowna synchronizacja przebiegła bezpiecznie, serwer musi dodatkowo uwierzytelnić klienta, jak pokazano w ćwiczeniu opisanym w punkcie Protokół HTTPS z uwierzytelnianiem przy użyciu certyfikatu klienta, na stronie 60.

# Protokół HTTPS z uwierzytelnianiem przy użyciu certyfikatu klienta

W domyślnej konfiguracji fabrycznej serwer nie żąda od klienta certyfikatu SSL. Przesyłanie profilu nie jest bezpieczne, ponieważ dowolny klient może się połączyć z serwerem i zażądać profilu. Dlatego konfigurację można edytować i włączyć w niej uwierzytelnianie klienta. Wtedy serwer przed zaakceptowaniem żądania połączenia będzie wymagał certyfikatu klienta w celu jego uwierzytelnienia.

Ze względu na to wymaganie nie można niezależnie przetestować operacji ponownej synchronizacji przy użyciu przeglądarki, która nie ma odpowiednich poświadczeń. Wymianę kluczy SSL wewnątrz połączenia HTTPS między testowym telefonem a serwerem można obserwować za pomocą narzędzia ssldump. Ślad rejestrowany przez narzędzie pokazuje interakcję między klientem a serwerem.

## Ćwiczenie: Protokół HTTPS z uwierzytelnianiem przy użyciu certyfikatu klienta

**Procedura**

**Krok 1** Włącz na serwerze HTTPS uwierzytelnienie za pomocą certyfikatu klienta.

**Krok 2** W oprogramowaniu Apache (wer. 2) ustaw następujący parametr w pliku konfiguracyjnym serwera:

```
SSLVerifyClient  require
```

Ponadto upewnij się, że certyfikat spacroot.cert został zapisany w sposób pokazany w ćwiczeniu Podstawowa ponowna synchronizacja przy użyciu protokołu HTTPS, na stronie 58.

**Krok 3** Uruchom ponownie serwer HTTPS i obejrzyj w dzienniku systemu zapis dotyczący operacji z telefonu.

Odtąd podczas każdej ponownej synchronizacji z serwerem będzie wykonywane uwierzytelnianie symetryczne, tzn. profil zostanie przesłany dopiero po zweryfikowaniu certyfikatów serwera i klienta.

**Krok 4** Za pomocą narzędzia ssldump przechwyć informacje o połączeniu w celu ponownej synchronizacji między telefonem a serwerem HTTPS.

Jeśli funkcja weryfikowania certyfikatu klienta jest prawidłowo włączona na serwerze, zapis operacji z narzędzia ssldump pokazuje symetryczną wymianę certyfikatów (najpierw z serwera do klienta, a następnie z klienta do serwera) przed przesłaniem zaszyfrowanych pakietów zawierających profil.

Po włączeniu funkcji uwierzytelniania klienta tylko telefon z adresem MAC pasującym do prawidłowego certyfikatu klienta może wysyłać do serwera obsługi administracyjnej żądania przesłania profilu. Serwer odrzuca żądania od zwykłych przeglądarek internetowych i innych nieautoryzowanych urządzeń.

# Filtrowanie klientów i dynamiczna zawartość HTTPS

Jeśli na serwerze HTTPS skonfigurowano wymaganie certyfikatu klienta, informacje zawarte w certyfikacie identyfikują telefon dokonujący ponownej synchronizacji i dostarczają mu odpowiednie informacje o konfiguracji.

Serwer HTTPS udostępnia informacje z certyfikatu skryptom CGI (lub skompilowanym programom CGI), które są wywoływane w ramach żądania ponownej synchronizacji. Dla celów ilustracyjnych w ćwiczeniu jest wykorzystywany język skryptowy open source Perl oraz założono, że rolę serwera HTTPS pełni oprogramowanie serwera Apache (wer. 2).

### Procedura

**Krok 1** Zainstaluj kompilator języka Perl na hoście zawierającym serwer HTTPS.

**Krok 2** Wygeneruj następujący skrypt typu reflector dla języka Perl:

```
#!/usr/bin/perl -wT
use strict;
print “Content-Type: text/plain\n\n”;
print “<flat-profile><GPP_D>”;

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

**Krok 3** Zapisz ten plik pod nazwą `reflect.pl` z uprawnieniem wykonywalności (chmod 755 w systemie Linux) w katalogu skryptów CGI na serwerze HTTPS.

**Krok 4** Sprawdź dostępność skryptów CGI na serwerze (tzn. w folderze `/cgi-bin/…`).

**Krok 5** Zmodyfikuj parametr Profile_Rule na urządzeniu testowym w taki sposób, aby synchronizacja odbywała się ze skryptem typu reflector, jak w przykładzie poniżej:

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

**Krok 6** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

**Krok 7** Obejrzyj ślad w dzienniku systemu i oceń, czy synchronizacja zakończyła się powodzeniem.

**Krok 8** Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

**Krok 9** Wybierz kolejno opcje **Głos (Voice)** > **Obsługa administracyjna (Provisioning)**.

**Krok 10** Sprawdź, czy parametr GPP_D zawiera informacje przechwycone przez skrypt.

Informacje te zawierają nazwę, adres MAC i numer seryjny produktu, o ile urządzenie testowe ma unikatowy certyfikat od producenta. Natomiast jeśli urządzenie zostało wyprodukowane z oprogramowaniem sprzętowym w wersji starszej niż 2.0, informacje zawierają standardowe ciągi.

Podobny skrypt może rozpoznawać informacje o urządzeniu, dla którego jest wykonywana ponowna synchronizacja, a następnie przekazywać do niego odpowiednie wartości parametrów konfiguracyjnych.

# Certyfikaty serwera HTTPS

Telefon udostępnia niezawodną i bezpieczną strategię obsługi administracyjnej opartą na wysyłaniu żądań HTTPS z urządzenia do serwera obsługi administracyjnej. Do uwierzytelniania telefonu na serwerze i serwera na telefonie są używane certyfikaty serwera i klienta.

Aby używać protokołu HTTPS na telefonie, należy wygenerować żądanie podpisania certyfikatu (CSR) i wysłać je do firmy Cisco. W telefonie zostanie wygenerowany certyfikat przeznaczony do zainstalowania na serwerze obsługi administracyjnej. Certyfikat zostanie zaakceptowany w telefonie w trakcie próby nawiązania połączenia przez protokół HTTPS z serwerem obsługi administracyjnej.

## Metodyka działania protokołu HTTPS

Protokół HTTPS szyfruje komunikację między klientem i serwerem, zabezpieczając w ten sposób zawartość komunikatu przed dostępem z innych urządzeń sieciowych. Metoda szyfrowania treści komunikacji między klientem a serwerem bazuje na kryptografii wykorzystującej klucz symetryczny. W kryptografii z kluczem symetrycznym klient i serwer wymieniają się jednym tajnym kluczem przez bezpieczny kanał chroniony kluczem publicznym/prywatnym.

Komunikaty szyfrowane tajnym kluczem mogą być odszyfrowane tylko przy użyciu tego samego klucza. Protokół HTTPS obsługuje wiele różnych algorytmów szyfrowania symetrycznego. W telefonie można zaimplementować szyfrowanie kluczami symetrycznymi o długości do 256 bitów przy użyciu algorytmu AES (American Encryption Standard) oraz szyfrowanie 128-bitowymi kluczami RC4.

Protokół HTTPS zapewnia również uwierzytelnianie serwera i klienta w ramach bezpiecznej transakcji. Ta funkcja gwarantuje, że serwer obsługi administracyjnej i urządzenie klienckie nie zostaną oszukane przez inne urządzenia pracujące w sieci. Jest to niezbędne w kontekście obsługi administracyjnej zdalnych punktów końcowych.

Uwierzytelnianie serwera i klienta odbywa się przy użyciu szyfrowania kluczem prywatnym/publicznym z certyfikatem zawierającym klucz publiczny. Tekst zaszyfrowany kluczem publicznym można odszyfrować tylko za pomocą pasującego klucza prywatnego (i odwrotnie). Telefon obsługuje szyfrowanie kluczami prywatnymi/publicznymi przy użyciu algorytmu RSA (Rivest-Shamir-Adleman).

## Certyfikat serwera SSL

Dla każdego bezpiecznego serwera obsługi administracyjnej jest wystawiany certyfikat serwera SSL (Secure Sockets Layer), który firma Cisco podpisuje bezpośrednio. Oprogramowanie sprzętowe działające w telefonie rozpoznaje jako prawidłowy wyłącznie certyfikat Cisco. Gdy klient nawiązuje połączenie z serwerem za pomocą protokołu HTTPS, odrzuca każdy certyfikat serwera, który nie jest podpisany przez firmę Cisco.

Ten mechanizm chroni dostawcę usług przed nieautoryzowanym dostępem do telefonu oraz wszelkimi próbami oszukania serwera obsługi administracyjnej. Bez takiej ochrony napastnik mógłby zmienić parametry obsługi administracyjnej telefonu, uzyskać informacje o konfiguracji lub używać innej usługi VoIP. Bez

klucza prywatnego odpowiadającego ważnemu certyfikatowi serwera napastnik nie może nawiązać połączenia z telefonem.

## Uzyskiwanie certyfikatu serwera

**Procedura**

**Krok 1** Skontaktuj się z pracownikiem pomocy technicznej w Cisco, który pomoże w procesie uzyskiwania certyfikatu. Jeśli nie współpracujesz z żadną konkretną osobą, wyślij prośbę na adres ciscosb-certadmin@cisco.com.

**Krok 2** Wygeneruj klucz prywatny, który będzie używany w żądaniu podpisania certyfikatu (CSR). Ten klucz jest prywatny i nie trzeba go podawać działowi pomocy technicznej Cisco. Do wygenerowania klucza użyj narzędzia open source „openssl". Na przykład:

```
openssl genrsa -out <plik.klucza> 1024
```

**Krok 3** Wygeneruj żądanie CSR zawierające pola, które identyfikują Twoją organizację i lokalizację. Na przykład:

```
openssl req -new -key <plik.klucza> -out <plik.csr>
```

Potrzebujesz następujących informacji:

- Pole tematu — Wprowadź nazwę pospolitą (CN) w formacie w pełni kwalifikowanej nazwy domeny (FQDN). Podczas uzgadniania poprzez uwierzytelnianie za pomocą protokołu SSL telefon sprawdza, czy certyfikat, który otrzymał, pochodzi z urządzenia, które go okazało.
- Nazwa hosta serwera — Na przykład provserv.domain.com.
- Adres e-mail — Wprowadź adres e-mail, który umożliwi pracownikom działu obsługi klienta kontaktowanie się Tobą w razie potrzeby. Ten adres e-mail jest widoczny w żądaniu CSR.

**Krok 4** Wyślij żądanie CSR (w formacie pliku .zip) do konkretnej osoby w dziale pomocy technicznej Cisco lub na ogólny adres ciscosb-certadmin@cisco.com. Certyfikat zostanie podpisany przez firmę Cisco. Następnie certyfikat zostanie odesłany w celu zainstalowania go na Twoim komputerze.

## Certyfikat klienta

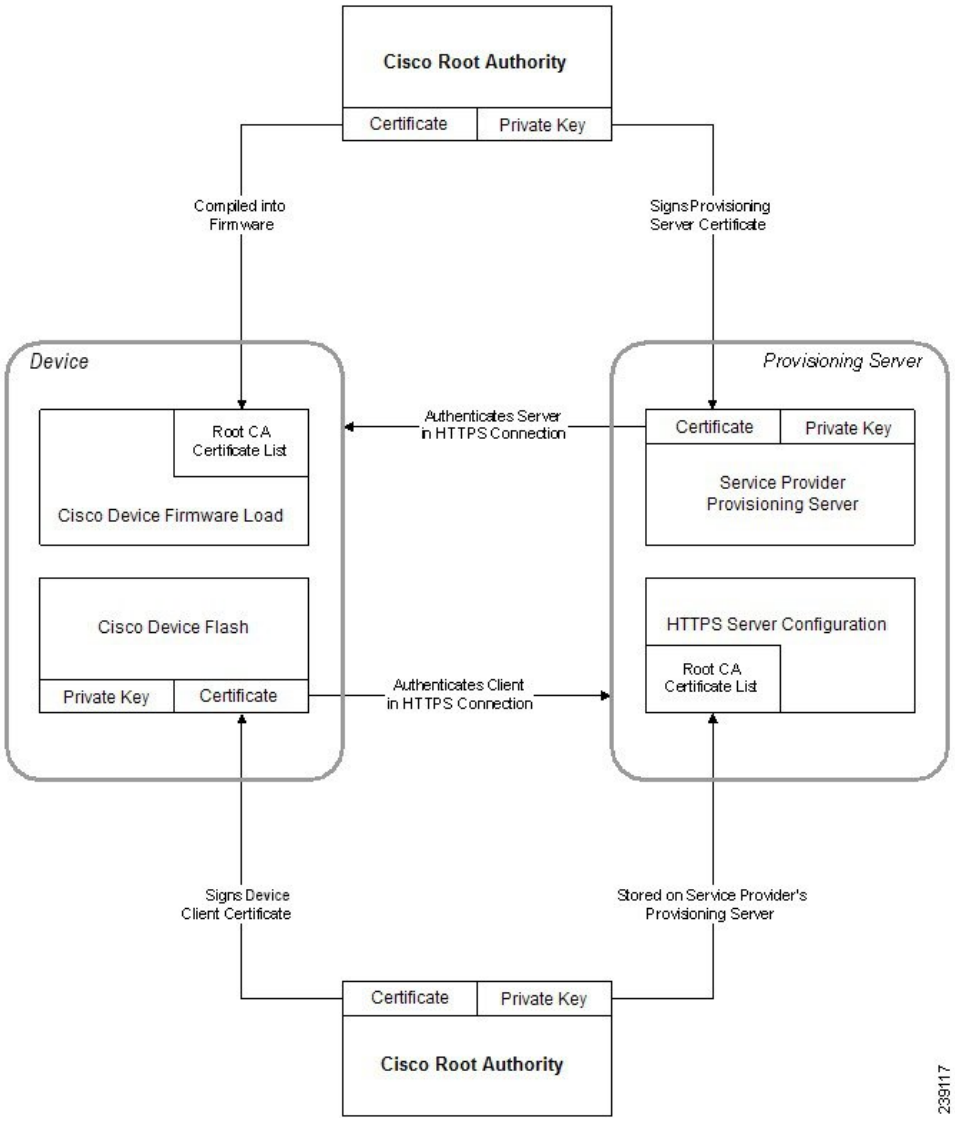
Oprócz bezpośredniego ataku na telefon napastnik może również próbować nawiązać połączenie z serwerem obsługi administracyjnej za pomocą standardowej przeglądarki internetowej lub innego klienta HTTPS w celu pobrania profilu konfiguracji z tego serwera. Aby zapobiec takiemu atakowi, każdy telefon zawiera unikatowy certyfikat klienta podpisany przez firmę Cisco. Zawiera on informacje identyfikacyjne o każdym punkcie końcowym. Każdy dostawca usług otrzymuje certyfikat główny urzędu certyfikacji, który umożliwia uwierzytelnianie certyfikatu urządzenia klienckiego. Dzięki tej ścieżce uwierzytelniania serwer obsługi administracyjnej może odrzucać nieautoryzowane żądania o profile konfiguracji.

## Struktura certyfikatu

Połączenie certyfikatu serwera z certyfikatem klienta gwarantuje bezpieczną łączność między zdalnym telefonem i serwerem obsługi administracyjnej. Na poniższej ilustracji przedstawiono wzajemne relacje i umiejscowienie certyfikatów, par kluczy prywatnych/publicznych i podpisujących głównych urzędów certyfikacji między klientem Cisco, serwerem obsługi administracyjnej i urzędami certyfikacji.

Górna połowa diagramu pokazuje główny urząd certyfikacji serwera obsługi administracyjnej, który podpisuje indywidualny certyfikat serwera obsługi administracyjnej. Odpowiedni certyfikat główny jest kompilowany do oprogramowania sprzętowego, co umożliwia uwierzytelnianie w telefonie autoryzowanych serwerów obsługi administracyjnej.

***Rysunek 2: Przepływ danych między urzędami certyfikacji***




## Konfigurowanie niestandardowego urzędu certyfikacji

Certyfikaty cyfrowe mogą służyć do uwierzytelniania urządzeń sieciowych i użytkowników w sieci. Mogą być używane do negocjowania sesji chronionych protokołem IPSec między węzłami sieci.

Na podstawie certyfikatu urzędu certyfikacji strona trzecia sprawdza i uwierzytelnia dwa lub więcej węzłów, z których następuje próba nawiązania połączenia. Każdy węzeł ma klucze publiczny i prywatny. Klucz publiczny szyfruje dane. Klucz prywatny odszyfrowuje dane. Ponieważ węzły uzyskały swoje certyfikaty z tego samego źródła, mają gwarancję autentyczności tożsamości drugiej strony.

Urządzenie może uwierzytelniać połączenia chronione protokołem IPSec za pomocą cyfrowych certyfikatów dostarczonych przez zewnętrzny urząd certyfikacji (CA).

Telefony obsługują kilka głównych urzędów certyfikacji wbudowanych w oprogramowaniu sprzętowym:

- Cisco Small Business CA
- CyberTrust CA
- Verisign CA
- Sipura CA
- Linksys CA

### Zanim rozpoczniesz

Przejdź do strony WWW administrowania telefonem. Zobacz Otwieranie strony WWW telefonu, na stronie 8.

### Procedura

**Krok 1** Wybierz kolejno opcje **Info (Informacje)** > **Stan (Status)**.

**Krok 2** Przewiń do obszaru **Stan niestandardowego urzędu certyfikacji** (Custom CA Status) i obejrzyj następujące pola:

- Stan obsługi administracyjnej niestandardowego urzędu certyfikacji — wskazuje stan obsługi administracyjnej.
  - Ostatnia obsługa administracyjna powiodła się o mm/dd/rrrr GG:MM:SS; lub
  - Ostatnia obsługa administracyjna nie powiodła się o mm/dd/rrrr GG:MM:SS
- Informacje o niestandardowym urzędzie certyfikacji — pokazuje informacje dotyczące niestandardowego urzędu certyfikacji.
  - Zainstalowano — zawiera informację „CN wartość", gdzie „wartość" to wartość parametru CN z pola Temat w pierwszym certyfikacie.
  - Nie zainstalowano — wskazuje, że nie został zainstalowany żaden certyfikat niestandardowego urzędu certyfikacji.

# Zarządzanie profilami

W tej części przedstawiono sposób tworzenia profili konfiguracji w ramach przygotowań do ich pobrania. Wyjaśnienie działania funkcji pokazano na przykładzie metody ponownej synchronizacji przy użyciu protokołu TFTP z lokalnego komputera, chociaż można użyć również protokołu HTTP lub HTTPS.

# Kompresowanie otwartego profilu za pomocą narzędzia Gzip

Profil konfiguracji w formacie XML może być bardzo duży, jeśli definiuje każdy parametr osobno. Aby zmniejszyć obciążenie serwera obsługi administracyjnej, telefon umożliwia kompresowanie pliku XML przy użyciu formatu kompresji Deflate obsługiwanego przez narzędzie gzip (RFC 1951).

**Uwaga** Aby telefon rozpoznawał skompresowany i zaszyfrowany profil XML, kompresja musi poprzedzać szyfrowanie.

Na potrzeby integracji z niestandardowymi serwerami obsługi administracyjnej działającymi na zapleczu profil można skompresować nie przy użyciu samodzielnego narzędzia gzip, ale biblioteki open source zlib służącej do kompresji danych. Jednak plik pobrany do telefonu powinien zawierać prawidłowy nagłówek gzip.

### Procedura

**Krok 1** Zainstaluj narzędzie gzip na lokalnym komputerze.

**Krok 2** Skompresuj profil konfiguracji `basic.txt` (opisany w punkcie Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51), uruchamiając narzędzie gzip z wiersza poleceń:

```
gzip basic.txt
```

Spowoduje to wygenerowanie pliku `basic.txt.gz` skompresowanego do formatu Deflate.

**Krok 3** Zapisz plik `basic.txt.gz` w wirtualnym katalogu głównym serwera TFTP.

**Krok 4** Zmodyfikuj parametr Profile_Rule na urządzeniu testowym w taki sposób, aby synchronizacja odbywała się przy użyciu pliku w formacie Deflate zamiast oryginalnego pliku XML, jak pokazano w poniższym przykładzie:

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

**Krok 5** Kliknij przycisk **Prześlij wszystkie zmiany**.

**Krok 6** Obejrzyj zapis operacji z telefonu w dzienniku systemowym.

Po ponownej synchronizacji do telefonu zostanie pobrany nowy plik z nowymi wartościami parametrów.

### Tematy pokrewne

Kompresja otwartego profilu, na stronie 18

# Szyfrowanie profilu przy użyciu narzędzia OpenSSL

Skompresowany lub nieskompresowany profil można zaszyfrować (jednak przed zaszyfrowaniem pliku trzeba go koniecznie skompresować). Szyfrowanie jest przydatne, gdy trzeba zapewnić poufność informacji zawartych w profilu, np. jeśli komunikacja między telefonem a serwerem obsługi administracyjnej odbywa się przez protokół TFTP lub HTTP.

Telefon obsługuje szyfrowanie kluczem symetrycznym przy użyciu 256-bitowego algorytmu AES. Do takiego szyfrowania można użyć narzędzia open source OpenSSL.

### Procedura

**Krok 1** Zainstaluj oprogramowanie OpenSSL na swoim komputerze. W celu zapewnienia obsługi algorytmu AES może być konieczne ponowne skompilowanie aplikacji OpenSSL.

**Krok 2** Korzystając z pliku konfiguracyjnego `basic.txt` (opisanego w punkcie Ponowna synchronizacja przy użyciu protokołu TFTP, na stronie 51), wygeneruj zaszyfrowany plik przy użyciu następującego polecenia:

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

Można również użyć skompresowanego pliku `basic.txt.gz` utworzonego w punkcie Kompresowanie otwartego profilu za pomocą narzędzia Gzip, na stronie 66, ponieważ profil XML może być równocześnie skompresowany i zaszyfrowany.

**Krok 3** Zapisz zaszyfrowany plik `basic.cfg` w wirtualnym katalogu głównym serwera TFTP.

**Krok 4** Zmodyfikuj parametr Profile_Rule na urządzeniu testowym, tak aby ponowna synchronizacja następowała przy użyciu zaszyfrowanego pliku, a nie oryginalnego pliku XML. Klucz szyfrowania jest przekazywany do telefonu za pomocą następującej opcji w adresie URL:

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

**Krok 5** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

**Krok 6** Obejrzyj zapis operacji z telefonu w dzienniku systemowym.

Po ponownej synchronizacji do telefonu zostanie pobrany nowy plik z nowymi wartościami parametrów.

### Tematy pokrewne

Szyfrowanie AES-256-CBC, na stronie 19

# Tworzenie profilu podzielonego na partycje

Podczas każdej ponownej synchronizacji telefon pobiera wiele oddzielnych profili. Taki system umożliwia zarządzanie różnymi rodzajami danych profili na różnych serwerach oraz przechowywanie oddzielnie wspólnych wartości parametrów konfiguracyjnych i wartości specyficznych dla kont.

### Procedura

**Krok 1** Utwórz nowy profil XML `basic2.txt` i ustaw w nim wartość parametru inną niż w poprzednich ćwiczeniach. Na przykład w profilu `basic.txt` dodaj następujące informacje:

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

**Krok 2** Umieść profil `basic2.txt` w wirtualnym katalogu głównym serwera TFTP.

**Krok 3** Pozostaw w folderze pierwszą regułę profilu z wcześniejszych ćwiczeń, ale drugą regułę profilu (Profile_Rule_B) skonfiguruj w taki sposób, aby wskazywała nowy plik:

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

**Krok 4** Kliknij przycisk **Submit All Changes** (Prześlij wszystkie zmiany).

Odtąd podczas każdej operacji ponownej synchronizacji telefon będzie się synchronizował z profilami pierwszym i drugim, w tej kolejności.

**Krok 5** Obejrzyj w dzienniku systemu zapis dotyczący operacji i sprawdź, czy odnotowane zachowanie jest zgodne z oczekiwaniami.

# Ustawianie nagłówka prywatności telefonu

Nagłówek prywatności użytkownika w komunikacie SIP konfiguruje ochronę użytkownika dla ruchu w zaufanej sieci.

Za pomocą tagu XML w pliku `config.xml` można ustawić wartość nagłówka prywatności użytkownika dla każdego numeru wewnętrznego na linii.

Dostępne są następujące opcje nagłówka prywatności:

- Wyłączone (wartość domyślna)
- brak — Użytkownik wnioskuje, aby usługa prywatności nie stosowała żadnych funkcji ochrony do tego komunikatu SIP.
- nagłówek — Użytkownik wniokuje, aby usługa prywatności zasłaniała nagłówki, z których nie można usunąć informacji identyfikacyjnych.
- warstwa sesji — Użytkownik wnioskuje, aby usługa prywatności zapewniała anonimowość sesji.
- użytkownik — Użytkownik wnioskuje o ochronę tylko w komunikacji z urządzeniami pośredniczącymi.
- identyfikator — Użytkownik wnioskuje, aby system podstawiał identyfikator, który nie ujawnia nazwy hosta ani adresu IP.

### Procedura

**Krok 1** Otwórz plik `config.xml` telefonu do edycji w edytorze tekstu lub kodu źródłowego XML.

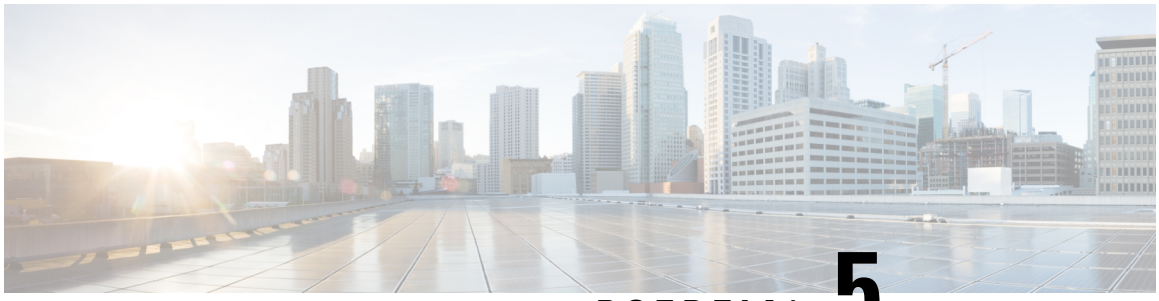
**Krok 2** Wstaw tag **<Privacy_Header_N_ ua="na">*Wartość*</Privacy_Header_N_>**, gdzie N jest numerem wewnętrznym na linii (1–10), i użyj jednej z następujących wartości.

- Wartość domyślna: **Wyłączone**
- **brak**
- **nagłówek**

- **warstwa sesji**
- **użytkownik**
- **identyfikator**

**Krok 3** (Opcjonalne) Za pomocą tego samego tagu skonfiguruj wszystkie pozostałe numery wewnętrzne na linii, podając ich numery.

**Krok 4** Zapisz zmiany dokonane w pliku `config.xml`.



ROZDZIAŁ 5

# Parametry obsługi administracyjnej



## Parametry obsługi administracyjnej — omówienie

W tym rozdziale opisano parametry obsługi administracyjnej, których można używać w skryptach profili konfiguracji.

## Parametry profilu konfiguracji

Poniższa tabela zawiera informacje na temat przeznaczenia i zastosowania parametrów znajdujących się w części **Parametry profilu konfiguracji** (Configuration Profile Parameters) na karcie **Obsługa administracyjna** (Provisioning).

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Włącz obsługę administracyjną (Provision Enable) | Steruje wszystkimi operacjami ponownej synchronizacji niezależnie od operacji uaktualniania oprogramowania sprzętowego. Ustaw wartość **Tak** (Yes), aby umożliwić zdalną obsługę administracyjną.<br><br>Wartość domyślna to Tak. |
| Ponowna synchronizacja po zresetowaniu (Resync On Reset) | Inicjuje ponowną synchronizację po każdym ponownym uruchomieniu, poza restartami spowodowanymi aktualizacją parametrów i uaktualnieniami oprogramowania układowego.<br><br>Wartość domyślna to Tak. |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Losowe opóźnienie ponownej synchronizacji (Resync Random Delay) | Losowe opóźnienie po sekwencji rozruchu, a przed wykonaniem resetu, podawane w sekundach. W puli urządzeń telefonii IP, które mają zaplanowane równoczesne uruchomienie, ta funkcja wprowadza pewną rozpiętość czasową wysyłania żądań ponownej synchronizacji z poszczególnych urządzeń do serwera obsługi administracyjnej. Funkcja może być przydatna w dużych wdrożeniach na terenach mieszkalnych w razie awarii lokalnej sieci elektrycznej.<br><br>Wartość tego pola musi być liczbą całkowitą z zakresu od 0 do 65535.<br><br>Wartość domyślna to 2. |
| Ponowna synchronizacja o (GGmm) (Resync At (HHmm)) | Godzina (GGmm), o której urządzenie ponownie się synchronizuje z serwerem obsługi administracyjnej.<br><br>Wartość tego pola musi być czterocyfrową liczbą z zakresu od 0000 do 2400, wskazującą godzinę w formacie GGmm. Na przykład 0959 oznacza 09:59.<br><br>Wartością domyślną jest puste pole. Nieprawidłowa wartość powoduje ignorowanie parametru. Jeżeli w parametrze zostanie ustawiona prawidłowa wartość, parametr Okresowa ponowna synchronizacja jest ignorowany. |
| Ponowna synchronizacja z losowym opóźnieniem (Resync At Random Delay) | Zapobiega przeciążeniu serwera obsługi administracyjnej podczas włączania dużej liczby urządzeń równocześnie.<br><br>Aby uniknąć zalewania serwera żądaniami ponownej synchronizacji z wielu telefonów, telefon synchronizuje się ponownie w przedziale między godziną i minutą a godziną i minutą powiększoną o losowe opóźnienie (ggmm, ggmm+random_delay). Jeśli na przykład random_delay = (Resynchronizacja przy opóźnieniu losowym + 30)/60 minut, w celu obliczenia ostatecznego interwału random_delay wprowadzona wartość w sekundach jest przeliczana na minuty z zaokrąglaniem do najbliższej minuty.<br><br>Prawidłowy zakres wartości należy do przedziału od 0 do 65535.<br><br>Ta funkcja jest wyłączona, jeśli w parametrze zostanie ustawiona wartość zero. Wartość domyślna to 600 sekund (10 minut). |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Okresowa ponowna synchronizacja (Resync Periodic) | Odstęp czasu między okresowymi ponownymi synchronizacjami z serwerem obsługi administracyjnej. Skojarzony zegar ponownej synchronizacji jest aktywowany dopiero po pierwszej pomyślnej synchronizacji z serwerem.<br><br>Prawidłowe są następujące formaty:<br><br>• Liczba całkowita<br><br>Przykład: dane wejściowe `3000` oznaczają, że następna resynchronizacja nastąpi za 3000 sekund.<br><br>• Wiele liczb całkowitych<br><br>Przykład: dane wejściowe z `600,1200,300` oznaczają, że pierwsza resynchronizacja nastąpi za 600 sekund, druga resynchronizacja nastąpi 1200 sekund po pierwszej, a trzecia resynchronizacja nastąpi 300 sekund po drugiej.<br><br>• Przedział czasu<br><br>Przykład: dane wejściowe `2400+30` oznaczają, że następna resynchronizacja nastąpi w przedziale między 2400 i 2430 sekund po pomyślnej resynchronizacji.<br><br>Ustawienie w tym parametrze wartości zero spowoduje wyłączenie okresowego ponownego synchronizowania.<br><br>Wartość domyślna to 3600 sekund. |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Opóźnienie kolejnych prób po błędzie synchronizacji (Resync Error Retry Delay) | Jeśli operacja ponownej synchronizacji nie udaje się, ponieważ urządzenie telefonii IP nie może pobrać profilu z serwera, pobrany plik jest uszkodzony lub występuje błąd wewnętrzny, urządzenie próbuje zsynchronizować się ponownie po czasie podanym w sekundach.<br><br>Prawidłowe są następujące formaty:<br><br>• Liczba całkowita<br><br>Przykład: dane wejściowe `300` oznaczają, że następna próba resynchronizacji nastąpi za 300 sekund.<br><br>• Wiele liczb całkowitych<br><br>Przykład: dane wejściowe z `600,1200,300` oznaczają, że pierwsza próba nastąpi w 600 sekund po niepowodzeniu, druga próba nastąpi 1200 sekund po niepowodzeniu pierwszej próby, a trzecia próba nastąpi 300 sekund po niepowodzeniu drugiej próby.<br><br>• Przedział czasu<br><br>Przykład: dane wejściowe z `2400+30` oznaczają, że następna próba nastąpi w przedziale między 2400 i 2430 sekund po niepowodzeniu resynchronizacji.<br><br>Ustawienie opóźnienia równego 0 spowoduje, że urządzenie nie będzie próbować ponownej synchronizacji po jednej nieudanej próbie. |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Opóźnienie wymuszonej ponownej synchronizacji (Forced Resync Delay) | Maksymalne opóźnienie (w sekundach), po jakim telefon wykonuje ponowną synchronizację.<br><br>Urządzenie nie synchronizuje się, gdy którakolwiek z jego linii telefonicznych jest aktywna. Ponieważ ponowna synchronizacja może potrwać kilka sekund, najlepiej poczekać z rozpoczęciem synchronizacji, aż urządzenie będzie bezczynne przez dłuższy czas. Dzięki temu użytkownik będzie mógł wykonywać połączenia jedno po drugim bez zakłóceń.<br><br>Urządzenie zawiera zegar, który rozpoczyna odliczanie z chwilą przejścia wszystkich linii w stan bezczynności. Ten parametr jest początkową wartością licznika. Zdarzenia ponownej synchronizacji są opóźnione do momentu, aż wartość tego licznika spadnie do zera.<br><br>Prawidłowy zakres wartości należy do przedziału od 0 do 65535.<br><br>Wartość domyślna to 14 400 sekund. |
| Ponowna synchronizacja przy użyciu protokołu SIP (Resync From SIP) | Umożliwia inicjowanie ponownej synchronizacji za pomocą komunikatu SIP NOTIFY.<br><br>Wartość domyślna to Tak. |
| Ponowna synchronizacja po próbie uaktualnienia (Resync After Upgrade Attempt) | Włącza lub wyłącza operację ponownej synchronizacji po każdym uaktualnieniu. Wartość Tak oznacza, że synchronizacja jest uruchamiana.<br><br>Wartość domyślna to Tak. |
| Wyzwalacz ponownej synchronizacji 1 (Resync Trigger 1), Wyzwalacz ponownej synchronizacji 2 (Resync Trigger 2) | Konfigurowalne warunki inicjowania ponownej synchronizacji. Ponowna synchronizacja jest inicjowana, gdy równanie logiczne w tych parametrach daje wynik PRAWDA.<br><br>Wartością domyślną jest puste pole. |
| Niepowodzenie ponownej synchronizacji z powodu nieznalezienia pliku (Resync Fails On FNF) | Ponowna synchronizacja jest uznawana za nieudaną, jeśli urządzenie nie otrzyma żądanego profilu z serwera. To domyślne zachowanie może zostać zastąpione przez ten parametr. Ustawienie wartości **Nie** (No) spowoduje, że urządzenie potraktuje odpowiedź `Nie znaleziono pliku` otrzymaną z serwera jako pomyślną ponowną synchronizację.<br><br>Wartość domyślna to Tak. |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Reguła profilu<br>Reguła profilu B (Profile Rule B)<br>Reguła profilu C (Profile Rule C)<br>Reguła profilu D (Profile Rule D) | Każda reguła profilu informuje telefon o źródle, z którego należy uzyskać profil (plik konfiguracyjny). Podczas każdej operacji ponownej synchronizacji telefon stosuje wszystkie profile kolejno.<br>Wartość domyślna: **`/$PSN.xml`**<br>Jeśli do plików konfiguracyjnych chcesz zastosować szyfrowanie metodą AES-256-CBC, określ klucz szyfrowania ze słowem kluczowym **`--key`** w następujący sposób:<br>**`[--key <klucz szyfrowania>]`**<br>Opcjonalnie klucz szyfrowania można ująć w podwójny cudzysłów ("). |
| Opcja DHCP do użycia (DHCP Option To Use) | Opcje protokołu DHCP, rozdzielone przecinkami, używane do pobierania oprogramowania sprzętowego i profili.<br>Wartość domyślna to 66,160,159,150,60,43,125. |
| Komunikat o żądaniu jest już w dzienniku (Log Request Msg) | Ten parametr zawiera komunikat wysyłany do serwera dziennika systemu na początku próby ponownej synchronizacji.<br>Wartość domyślna to `$PN $MAC –Żądanie % $SCHEME://$SERVIP:$PORT$PATH`. |
| Komunikat o pomyślnym zakończeniu jest już w dzienniku (Log Success Msg) | Komunikat dziennika systemowego wysyłany po pomyślnym zakończeniu próby ponownej synchronizacji.<br>Wartość domyślna to `$PN $MAC –Pomyślna ponowna synchronizacja % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`. |
| Komunikat o niepowodzeniu jest już w dzienniku (Log Failure Msg) | Komunikat dziennika systemowego wysyłany po nieudanej próbie ponownej synchronizacji.<br>Wartość domyślna to `$PN $MAC -- Ponowna synchronizacja nie powiodła się: $ERR`. |
| Ponowna synchronizacja konfigurowana przez użytkownika (User Configurable Resync) | Umożliwia użytkownikowi ponowne synchronizowanie telefonu IP z jego ekranu.<br>Wartość domyślna to Tak. |

# Parametry uaktualniania oprogramowania sprzętowego

Poniższa tabela zawiera informacje na temat przeznaczenia i zastosowania parametrów znajdujących się w części **Uaktualnianie oprogramowania sprzętowego** (Firmware Upgrade) na karcie **Obsługa administracyjna** (Provisioning).

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Włącz uaktualnianie (Upgrade Enable) | Umożliwia wykonywanie operacji uaktualniania oprogramowania sprzętowego niezależnie od operacji ponownej synchronizacji.<br>Wartość domyślna to Tak. |
| Opóźnienie kolejnych prób po błędzie uaktualniania (Upgrade Error Retry Delay) | Odstęp czasu (w sekundach) między kolejnymi próbami uaktualnienia stosowany w razie błędu uaktualniania. Urządzenie ma specjalny zegar, który aktywuje się po niepowodzeniu próby uaktualnienia. Inicjowaniem zegara steruje wartość tego parametru. Następna próba uaktualnienia rozpocznie się po odliczeniu do zera w tym zegarze.<br>Wartość domyślna to 3600 sekund. |
| Reguła uaktualniania (Upgrade Rule) | Skrypt uaktualniania oprogramowania sprzętowego, który określa warunki uaktualniania oraz powiązane adresy URL oprogramowania sprzętowego. Używa takiej samej składni, jak reguła profilu.<br>Aby wprowadzić regułę uaktualniania, zastosuj następujący format:<br>**<tftp\|http\|https>://<adres ip>/image/<nazwa pakietu>**<br>Na przykład:<br>**tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads**<br>Jeśli protokół nie zostanie podany, domyślnie będzie używany protokół TFTP. Jeśli nazwa serwera nie zostanie podana, jego rolę będzie pełnił host żądający adresu URL. Jeśli port nie zostanie podany, będzie używany port domyślny (69 w protokole TFTP, 80 w protokole HTTP lub 443 w protokole HTTPS).<br>Wartością domyślną jest puste pole. |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| Komunikat o żądaniu uaktualnienia w dzienniku (Log Upgrade Request Msg) | Komunikat dziennika systemowego wysyłany na początku próby uaktualnienia oprogramowania sprzętowego.<br>Wartość domyślna: `$PN $MAC -- Żądanie uaktualnienia $SCHEME://$SERVIP:$PORT$PATH` |
| Komunikat o powodzeniu uaktualnienia w dzienniku (Log Upgrade Success Msg) | Komunikat dziennika systemu wysyłany po pomyślnym ukończeniu próby uaktualnienia oprogramowania sprzętowego.<br>Wartość domyślna to `$PN $MAC -- Pomyślne uaktualnienie $SCHEME://$SERVIP:$PORT$PATH -- $ERR`. |
| Komunikat o niepowodzeniu uaktualnienia w dzienniku (Log Upgrade Failure Msg) | Komunikat dziennika systemowego wysyłany po nieudanej próbie uaktualnienia oprogramowania sprzętowego.<br>Wartość domyślna to `$PN $MAC -- Uaktualnienie nie powiodło się: $ERR`. |
| Równy dostęp do firmware | Włącza lub wyłącza funkcję Równy dostęp do oprogramowania sprzętowego. Wybierz opcję **Tak** lub **Nie**, aby odpowiednio włączyć lub wyłączyć tę funkcję.<br>Wartość domyślna: Tak |
| Serwer dziennika mechanizmu równego dostępu do oprogramowania sprzętowego | Wskazuje adres IP i port, pod który zostanie wysłany komunikat UDP.<br>Na przykład: 10.98.76.123:514, gdzie 10.98.76.123 jest adresem IP, a 514 numerem portu. |

# Parametry ogólnego przeznaczenia

Poniższa tabela zawiera informacje na temat przeznaczenia i zastosowania parametrów znajdujących się w sekcji **Parametry ogólnego przeznaczenia** (General Purpose Parameters) na karcie **Obsługa administracyjna** (Provisioning).

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| GPP_A - GPP_P | Parametry ogólnego przeznaczenia GPP_* pełnią rolę pól tekstowych używanych podczas konfigurowania współpracy telefonów z konkretnym serwerem obsługi administracyjnej. Można skonfigurować przechowywanie w nich różnych wartości, w tym następujących:<br>• Klucze szyfrowania<br>• Adresy URL<br>• Informacje o stanie wielostopniowej obsługi administracyjnej<br>• Szablony żądań POST<br>• Mapy aliasów nazw parametrów<br>• Częściowe wartości ciągów łączone w kompletne wartości parametrów<br>Wartością domyślną jest puste pole. |

# Zmienne rozwijane w makra

Niektóre zmienne makr są rozpoznawane wewnątrz następujących parametrów obsługi administracyjnej:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (w określonych warunkach)

Wewnątrz tych parametrów są rozpoznawane i rozwijane typy składni takie jak $NAZWA lub $(NAZWA).

Podciągi zmiennych makr można definiować za pomocą zapisu $(NAZWA:p) i $(NAZWA:p:q), gdzie „p” i „q” są nieujemnymi liczbami całkowitymi (funkcjonalność dostępna w wersji 2.0.11 i nowszych). Powstałe rozwinięcie w makro jest podciągiem rozpoczynającym się na przesunięciu znaku p i mającym długość q (lub sięgającym do końca ciągu, jeśli atrybut q nie został określony). Na przykład jeśli parametr GPP_A zawiera wartość ABCDEF, to ciąg podrzędny $(A:2) powoduje rozwinięcie do danych wyjściowych CDEF, a ciąg podrzędny $(A:2:3) rozwinięcie do danych wyjściowych CDE.

Nierozpoznawana nazwa nie jest przekształcana, a po rozwinięciu w makro zapis $NAZWA lub $(NAZWA) pozostaje niezmieniony jako wartość parametru.

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| $ | Zapis $$ rozwija się do jednego znaku $. |
| Od A do P | Zastępowane wartościami parametrów ogólnego przeznaczenia od GPP_A do GPP_P. |
| Od SA do SD | Zastępowane wartościami parametrów specjalnego przeznaczenia od GPP_SA do GPP_SD. W tych parametrach są przechowywane klucze lub hasła używane w obsłudze administracyjnej.<br>**Uwaga** Parametry od $SA do $SD są rozpoznawane jako argumenty opcjonalnego kwalifikatora adresu URL ponownej synchronizacji — --key. |
| MA | Adres MAC zapisany kodem szesnastkowym z małymi literami, na przykład 000e08aabbcc. |
| MAU | Adres MAC zapisany kodem szesnastkowym z wielkimi literami, na przykład 000E08AABBCC. |
| MAC | Adres MAC zapisany kodem szesnastkowym z małymi literami, gdzie pary znaków szesnastkowych są rozdzielane dwukropkami. Na przykład: 00:0e:08:aa:bb:cc. |
| PN | Nazwa produktu. Na przykład: CP-6841-3PCC. |
| PSN | Numer seryjny produktu. Na przykład: 6841-3PCC. |
| SN | Ciąg określający numer seryjny, na przykład 88012BA01234. |
| CCERT | Stan certyfikatu SSL klienta: Zainstalowano lub Nie zainstalowano. |
| IP | Adres IP telefonu wewnątrz jego lokalnej podsieci. Na przykład: 192.168.1.100. |
| EXTIP | Zewnętrzny adres IP telefonu widoczny w Internecie. Na przykład: 66.43.16.52. |
| SWVER | Ciąg określający wersję oprogramowania. Na przykład: sip68xx.11-0-1MPP. |
| HWVER | Ciąg określający wersję sprzętu. Na przykład: 2.0.1. |

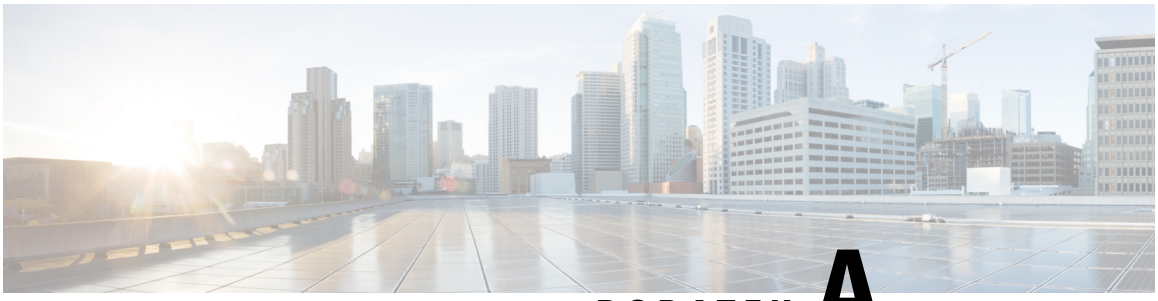
| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| PRVST | Stan obsługi administracyjnej (ciąg liczbowy):<br>-1 = jawne żądanie ponownej synchronizacji<br>0 = ponowna synchronizacja podczas włączania zasilania<br>1 = okresowa ponowna synchronizacja<br>2 = ponowna synchronizacja nie powiodła się, kolejna próba |
| UPGST | Stan uaktualniania (ciąg liczbowy):<br>1 = pierwsza próba uaktualnienia<br>2 = uaktualnianie nie powiodło się, kolejna próba |
| UPGERR | Komunikat o wyniku (ERR) poprzedniej próby uaktualnienia, na przykład „wykonanie żądania http_get nie powiodło się”. |
| PRVTMR | Liczba sekund od ostatniej próby ponownej synchronizacji. |
| UPGTMR | Liczba sekund od ostatniej próby uaktualnienia. |
| REGTMR1 | Liczba sekund od utraty przez linię 1 rejestracji na serwerze SIP. |
| REGTMR2 | Liczba sekund od utraty przez linię 2 rejestracji na serwerze SIP. |
| UPGCOND | Starsza nazwa makra. |
| SCHEME | Schemat dostępu do pliku (TFTP, HTTP lub HTTPS) ustalony po analizie adresu URL polecenia ponownej synchronizacji lub uaktualnienia. |
| SERV | Nazwa hosta docelowego serwera żądania ustalona po analizie adresu URL polecenia ponownej synchronizacji lub uaktualnienia. |
| SERVIP | Adres IP docelowego serwera żądania ustalony po analizie adresu URL polecenia ponownej synchronizacji lub uaktualnienia, być może po wyszukiwaniu w usłudze DNS. |
| PORT | Docelowy port UDP/TCP żądania ustalony po analizie adresu URL polecenia ponownej synchronizacji lub uaktualnienia. |

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| PATH | Docelowa ścieżka pliku żądania ustalona po analizie adresu URL polecenia ponownej synchronizacji lub uaktualnienia. |
| ERR | Komunikat o wyniku próby ponownej synchronizacji lub uaktualnienia. Ten parametr służy tylko do generowania komunikatów o wynikach zapisywanych w dzienniku systemu. W przypadku prób uaktualnienia wartość jest zapisywana w zmiennej UPGERR. |
| UIDn | Wartość parametru konfiguracyjnego identyfikatora użytkownika na linii n (Line n UserID). |
| EMS | Stan funkcji Extension Mobility |
| MUID | Identyfikator użytkownika funkcji Extension Mobility |
| MPWD | Hasło funkcji Extension Mobility |

# Kody błędów wewnętrznych

W telefonie zdefiniowano szereg kodów błędów wewnętrznych (X00–X99), które umożliwiają bardziej precyzyjną kontrolę zachowania urządzenia w pewnych sytuacjach problemowych.

| Nazwa parametru | Opis i wartość domyślna |
|---|---|
| X00 | Błąd warstwy transportowej (lub protokołu ICMP) podczas wysyłania żądania SIP. |
| X20 | Upłynął limit czasu żądania SIP podczas oczekiwania na odpowiedź. |
| X40 | Ogólny błąd protokołu SIP (na przykład nieakceptowalny kodek w protokole SDP w komunikatach 200 i potwierdzenia lub upłynął limit czasu podczas oczekiwania na potwierdzenie). |
| X60 | Wybrany numer jest nieprawidłowy zgodnie z obowiązującym planem wybierania. |



DODATEK A

# Przykładowe profile konfiguracji



# Przykładowy profil XML w formacie otwartym

```
<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>
```

Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

```
<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>
```

Przykładowe profile konfiguracji

```
<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>
```

Przykładowe profile konfiguracji

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

Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

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

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

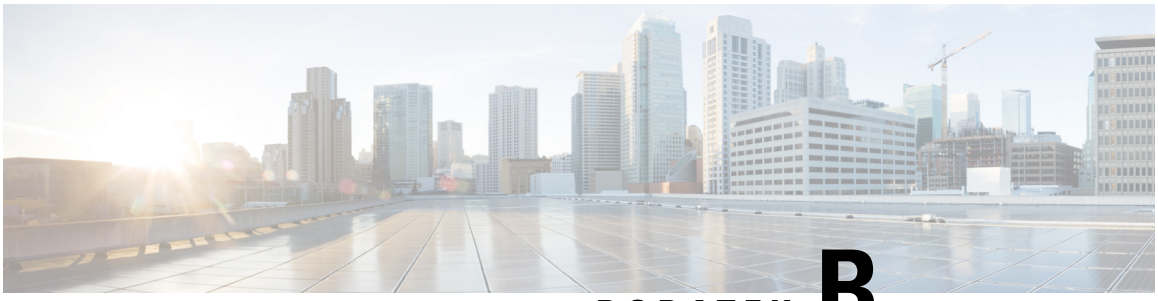
Przykładowe profile konfiguracji

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

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

Przykładowe profile konfiguracji

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



DODATEK B

# Akronimy



## Akronimy

| | |
|---|---|
| AC | Prąd zmienny |
| ACS | Serwer kontroli dostępu |
| A/D | Przetwornik analogowo-cyfrowy |
| AES | Zaawansowany standard szyfrowania (ang. Advanced Encryption Standard) |
| ANC | Połączenie anonimowe |
| AP | Punkt dostępowy |
| ASCII | American Standard Code for Information Interchange |
| B2BUA | Back to Back User Agent (agent dzielący kanał komunikacyjny na dwie odnogi) |
| SZL | Pole sygnalizacji aktywności linii |
| Bool | Wartości logiczne. Określane w profilu jako „tak” i „nie”, lub „1” i „0”. |
| BootP | Protokół Bootstrap |
| CA | Ośrodek certyfikujący |
| CAS | Sygnał alertu CPE |
| CDP | protokół CDP |
| CDR | Zapis szczegółów połączenia |
| CGI | Obrazy generowane komputerowo |
| CID | ID abonenta dzwoniącego |
| CIDCW | Identyfikator abonenta dzwoniącego w połączeniu oczekującym |

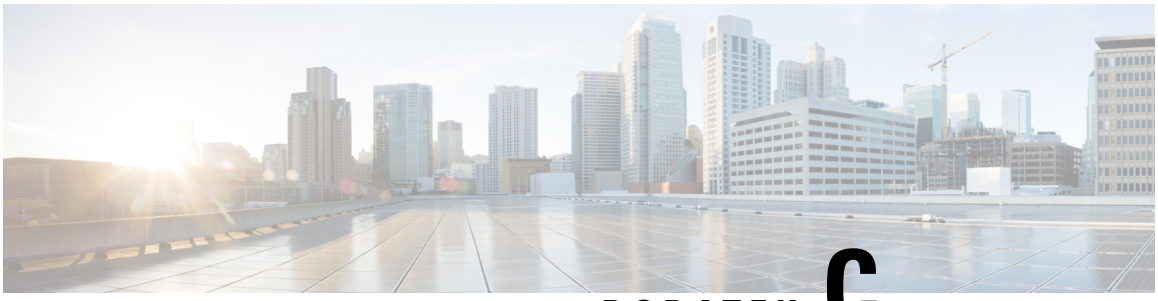
| | |
|---|---|
| CNG | Generowanie szumu |
| CPC | Sterowanie stroną wywołującą |
| CPE | Urządzenia końcowe użytkownika (CPE) |
| CSV | Wartości rozdzielone przecinkami |
| CWCID | Identyfikator abonenta dzwoniącego w połączeniu oczekującym |
| CWT | Sygnał połączenia oczekującego |
| D/A | Przetwornik cyfrowo-analogowy |
| dB | Decybele |
| dBm | Liczba decybeli przypadająca na 1 miliwat |
| DHCP | Protokół DHCP (Dynamic Host Configuration Protocol) |
| NPrzszk | Nie przeszkadzać |
| DNS | DNS (system nazw domenowych) |
| DoS | Odmowa usługi |
| DRAM | Pamięć dynamiczna o dostępie swobodnym |
| DSL | Cyfrowa pętla abonencka |
| DSP | Cyfrowy przetwornik sygnałów |
| DST | Czas letni |
| DTAS | Sygnał alertu urządzenia końcowego (to samo, co CAS) |
| DTMF | Dwutonowe wybieranie wieloczęstotliwościowe (lub po prostu „wybieranie dwutonowe”) |
| FQDN | W pełni kwalifikowana nazwa domeny |
| FSK | Kluczowanie częstotliwości (modulacja kluczem z przesunięciem częstotliwości) |
| FW | Firmware |
| FXS | Foreign eXchange Station |
| GMT | Czas średni Greenwich |
| GW | Gateway |
| HTML | Hypertext Markup Language, język HTML |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Protokół HTTP z zabezpieczeniami SSL |

| | |
|---|---|
| ICMP | protokół ICMP |
| IGMP | Internet Group Management Protocol |
| ILEC | Lokalny operator dominujący |
| IP | Protokół IP |
| IPv4 | Protokół internetowy w wersji 4 |
| IPv6 | Protokół internetowy w wersji 6 |
| ISP | Dostawca usług internetowych (ang. Internet Service Provider) |
| ITSP | Dostawca usług telefonii internetowej |
| ITU | Międzynarodowy Związek Telekomunikacyjny (ang. International Telecommunication Union) |
| IVR | System interaktywnych odpowiedzi głosowych |
| LAN | Sieć lokalna |
| LBR | Niska szybkość transmisji |
| LBRC | Low Bit Rate Codec |
| LCD | Wyświetlacz ciekłokrystaliczny; nazywany również „ekranem” |
| LDAP | Lightweight Directory Access Protocol |
| LED | Dioda świecąca |
| Adres MAC | Adres sprzętowy MAC (Media Access Control) |
| MC | Minicertyfikat |
| MGCP | Media Gateway Control Protocol, protokół MGCP |
| MOH | Muzyka podczas oczekiwania |
| MOS | Mean Opinion Score, średnia ocena opinii (1–5, im wyższy, tym lepiej) |
| MPP | Telefon wieloplatformowy |
| ms | Milisekunda |
| MSA | Music Source Adaptor, adapter audio |
| MWI | Wskaźnik wiadomości oczekującej |
| NAT | Translacja adresów sieciowych |
| NPS | Standardowy serwer obsługi administracyjnej |
| NTP | Protokół NTP (ang. Network Time Protocol) |

| | |
|---|---|
| OOB | Poza zakresem |
| OSI | Open Switching Interval (czas, przed jaki bateria w centrali jest odłączona od linii telefonicznej) |
| Centrala PBX | Private branch exchange (prywatna centrala abonencka) |
| PCB | Płytka drukowana |
| PoE | Power over Ethernet |
| PR | Odwrócenie polaryzacji |
| PS | Serwer obsługi administracyjnej |
| PSQM | Perceptual Speech Quality Measurement, pomiar jakości sygnału mowy (1–5, im niższy, tym lepszy) |
| PSTN | Public Switched Telephone Network |
| QoS | Jakość usług |
| Zdalne sterowanie | Usunięcie dostosowania |
| REQT | Komunikat żądania (SIP) |
| RESP | Komunikat odpowiedzi (SIP) |
| RSC | (SIP) Kod stanu odpowiedzi, np. 404, 302, 600 |
| RTP | Real Time Protocol |
| RTT | Round Trip Time, czas obiegu danych |
| SAS | Serwer strumieniowego przesyłania dźwięku |
| SDP | Session Description Protocol, protokół SDP |
| SDRAM | Synchroniczna pamięć DRAM |
| sec | sekund |
| SIP | Session Initiation Protocol, protokół SIP |
| SLA | Wygląd linii wspólnej |
| SLIC | Interfejs linii abonenckiej |
| SP | Usługodawca |
| SSL | Secure Socket Layer |
| STUN | Przechodzenie sesji UDP dla usługi translacji adresów |

| | |
|---|---|
| TCP | TCP |
| TFTP | Trivial File Transfer Protocol |
| TLS | Transport Layer Security |
| TTL | Time to live (czas wygaśnięcia) |
| ToS | type of service (typ usługi) |
| UA | User Agent, agent użytkownika |
| uC | Mikrokontroler |
| UDP | Protokół UDP (User Datagram Protocol) |
| URI | Identyfikator URI (Uniform Resource Identifier) |
| URL | Adres URL (ang. Uniform Resource Locator) |
| Czas UTC | Uniwersalny czas koordynowany |
| VAR | Sprzedawca VAR (wzbogacający produkt) |
| VLAN | Głosowa sieć LAN |
| VM | Poczta głosowa |
| VMWI | Graficzny wskaźnik wiadomości oczekującej |
| VoIP | Voice over Internet Protocol (protokół transmisji głosu przez sieć) |
| VQ | Jakość dźwięku |
| WAN | Sieć WAN |
| XML | Extensible Markup Language, język XML |

Akronimy



DODATEK C

# Dokumentacja pokrewna



## Dokumentacja pokrewna

Informacje pokrewne można znaleźć w następujących sekcjach.

### Dokumentacja telefonu Cisco IP Phone z serii 6800

Należy zapoznać się z publikacjami dotyczącymi danego języka, modelu telefonu i wersji wieloplatformowego oprogramowania firmware. Należy skorzystać z następujących adresów URL (Uniform Resource Locator):

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

## Zasady pomocy technicznej dla oprogramowania sprzętowego telefonów Cisco IP Phone

Aby uzyskać informacje na temat zasad pomocy technicznej dla telefonów, zobacz https://cisco.com/go/phonefirmwaresupport.