



## **Podręcznik administratora telefonów IP Cisco z serii 8800 dla systemu Cisco Unified Communications Manager**

**Pierwsza publikacja:** 2015-07-13

**Ostatnia modyfikacja:** 2023-06-16

### **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

SPECYFIKACJE PRODUKTÓW I INFORMACJE NA ICH TEMAT ZAWARTE W NINIEJSZYM PODRĘCZNIKU MOGĄ ULEC ZMIANIE BEZ POWIADOMIENIA. WSZYSTKIE OŚWIADCZENIA, INFORMACJE I ZALECENIA ZAWARTE W NINIEJSZYM PODRĘCZNIKU SĄ UWAZANE ZA PRAWDZIWE, ALE NIE JEST UDZIELANA NA NIE ŻADNA GWARANCJA, WYRAŻNA ANI DOMNIEMANA. UŻYTKOWNICY PONOSZĄ PEŁNĄ ODPOWIEDZIALNOŚĆ ZA STOSOWANIE DOWOLNYCH PRODUKTÓW.

LICENCJA NA OPROGRAMOWANIE I OGRANICZONA GWARANCJA NA TOWARZYSZĄCY PRODUKT ZNAJDUJĄ SIĘ W PAKIECIE INFORMACJI DOŁĄCZONYM DO PRODUKTU I STANOWIĄ INTEGRALNĄ CZĘŚĆ NINIEJSZEGO DOKUMENTU PRZEZ ODNIESIENIE. W PRZYPADKU NIEZNALEZIENIA LICENCJI NA OPROGRAMOWANIE LUB OGRANICZONEJ GWARANCJI NALEŻY ZWRÓCIĆ SIĘ DO PRZEDSTAWICIELA FIRMY CISCO Z PROŚBĄ O KOPIĘ.

Informacja dotycząca zgodności urządzeń klasy A z wymaganiami komisji FCC: to urządzenie zostało przebadane z wynikiem pozytywnym pod kątem zgodności z ograniczeniami dla urządzeń cyfrowych klasy A według części 15 wytycznych FCC. Ograniczenia te mają na celu zapewnienie odpowiedniej ochrony przed szkodliwymi zakłóceniami podczas użytkowania sprzętu na obszarach przemysłowych. Urządzenie wytwarza, użytkuje i może emitować energię fal radiowych, które mogą powodować szkodliwe zakłócenia komunikacji radiowej, jeśli instalacja oraz użycie urządzenia nie będą się odbywać zgodnie z instrukcją. Użycie urządzenia na obszarach zamieszkałych może wywołać szkodliwe zakłócenia, które w przypadku ich pojawienia się, powinny zostać skorygowane przez użytkowników na ich koszt.

Informacja dotycząca zgodności urządzeń klasy B z wymaganiami komisji FCC: to urządzenie zostało przebadane z wynikiem pozytywnym pod kątem zgodności z ograniczeniami dla urządzeń cyfrowych klasy B według części 15 wytycznych FCC. Ograniczenia mają na celu zapewnienie stosownej ochrony przed szkodliwymi zakłóceniami w środowisku zamieszkanym. Urządzenie wytwarza, użytkuje i może emitować energię fal radiowych, które mogą powodować szkodliwe zakłócenia komunikacji radiowej, jeśli instalacja oraz użycie urządzenia nie będą się odbywać zgodnie z instrukcją. Nie wyklucza się jednak, że w wypadku konkretnej instalacji zakłócenia takie wystąpią. Jeśli urządzenie powoduje zakłócenia w odbiorze sygnału radiowego lub telewizyjnego, co można sprawdzić, wyłączając i włączając urządzenie, należy podjąć próby wyeliminowania tych zakłóceń, stosując następujące środki zaradcze:

- Obrócić lub przenieść antenę odbiorczą.
- Zwiększyć odległość między urządzeniem a odbiornikiem.
- Podłączyć urządzenie do gniazda w sieci zasilającej innej niż ta, do której podłączony jest odbiornik.
- Skonsultować się ze sprzedawcą lub doświadczonym technikiem radio-telewizyjnym w celu uzyskania pomocy.

Modyfikacje produktu niezatwierdzone przez firmę Cisco mogą spowodować unieważnienie aprobaty komisji FCC oraz prawa użytkownika do obsługi urządzenia.

Stosowany przez firmę Cisco sposób kompresji nagłówka TCP stanowi adaptację programu opracowanego na Uniwersytecie Kalifornijskim, Berkeley (USB) i jest częścią dostępną publicznie wersji systemu operacyjnego Unix, która została stworzona przez UCB. Wszystkie prawa zastrzeżone. Copyright © 1981 Regents of the University of California.

BEZ WZGLĘDU NA JAKIEKOLWIEK INNE GWARANCJE UDZIELONE W NINIEJSZYM DOKUMENCIE WSZYSTKIE PLIKI DOKUMENTACJI I OPROGRAMOWANIE TYCH DOSTAWCÓW SĄ DOSTARCZANE W TAKIM STANIE, W JAKIM SIĘ ZNAJDUJĄ, ZE WSZYSTKIMI WADAMI. FIRMA CISCO I WSKAZANI POWYŻEJ DOSTAWCY ZRZEKAJĄ SIĘ WSZELKICH GWARANCJI, WYRAŻNYCH LUB DOROZUMIANYCH, W TYM MIĘDZY INNYMI DOTYCZĄCYCH PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU I NIENARUSZANIA PRAW WŁASNOŚCI LUB WYNIKAJĄCYCH Z OBSŁUGI, WYKORZYSTANIA LUB PRAKTYK HANDLOWYCH.

W ŻADNYM RAZIE FIRMA CISCO ANI JEJ DOSTAWCY NIE BĘDĄ PONOSIĆ ODPOWIEDZIALNOŚCI ZA ŻADNE SZKODY POŚREDNIE, SZCZEGÓLNE, WTÓRNE LUB PRZYPADKOWE, W TYM MIĘDZY INNYMI UTRATĘ ZYSKÓW LUB UTRATĘ ALBO ZNISZCZENIE DANYCH WYNIKAJĄCE Z UŻYCIA LUB BRAKU MOŻLIWOŚCI UŻYCIA NINIEJSZEGO PODRĘCZNIKA, NAWET JEŚLI FIRMA CISCO LUB JEJ DOSTAWCY ZOSTALI POINFORMOWANI O MOŻLIWOŚCI WYSTĄPIENIA TAKICH SZKÓD.

Wszelkie adresy protokołu komunikacyjnego IP oraz numery telefonów użyte w tym dokumencie nie powinny być traktowane jako adresy lub numery rzeczywiste. Wszelkie przykłady, obrazy ekranów zawierające polecenia, diagramy topologii sieci oraz inne dane zawarte w dokumencie zostały przedstawione wyłącznie w celach demonstracyjnych. Jakikolwiek użycie rzeczywistych adresów IP lub numerów telefonów w treści demonstracyjnej jest przypadkowe i niezamierzone.

Wszystkie wydrukowane i zduplikowane kopie miękkie tego dokumentu uważane są za niekontrolowane. Aby mieć pewność, że korzystasz z najnowszej wersji, zapoznaj się z bieżącą wersją online.

Firma Cisco ma ponad 200 biur na całym świecie. Pełną listę adresów i numerów telefonów można znaleźć na stronie internetowej firmy Cisco pod adresem: [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Nazwa i logo Cisco są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco i/lub jej spółek zależnych w Stanach Zjednoczonych i innych krajach. Aby wyświetlić listę znaków towarowych firmy Cisco, przejdź do następującego adresu URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Znaki towarowe innych podmiotów wymienione w tym dokumencie są własnością ich prawnych właścicieli. Użycie słowa „partner” nie oznacza stosunku partnerstwa między firmą Cisco a jakąkolwiek inną firmą. (1721R)

© 2015–2023 Cisco Systems, Inc. Wszelkie prawa zastrzeżone.



## SPIS TREŚCI

---

### PRZEDMOWA:

#### **Przedmowa** xv

Omówienie xv

Do kogo adresowany jest ten podręcznik? xv

Konwencje przyjęte w podręczniku xv

Dokumentacja pokrewna xvi

Telefon IP Cisco z serii 8800 — Dokumentacja xvii

Cisco Unified Communications Manager — Dokumentacja xvii

Cisco Business Edition 6000 — Dokumentacja xvii

Dokumentacja, pomoc techniczna i wskazówki dotyczące bezpieczeństwa xvii

Ogólne informacje na temat bezpieczeństwa produktu Cisco xvii

---

### ROZDZIAŁ 1

#### **Nowe i zmienione informacje** 1

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.2(1) 1

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.1(1) 2

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.0(1) 2

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.8(1) 3

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.7(1) 4

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.6(1) 4

Nowe informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR3 5

Nowe informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR1 5

Nowe informacje o oprogramowaniu sprzętowym w wersji 12.1(1)SR1 6

Nowe informacje o oprogramowaniu sprzętowym w wersji 12.1(1) 6

Nowe informacje o oprogramowaniu sprzętowym w wersji 12.0(1) 7

Nowe informacje o oprogramowaniu sprzętowym w wersji 11.7(1) 7

Nowe informacje o oprogramowaniu sprzętowym w wersji 11.5(1)SR1 8

Nowe informacje o oprogramowaniu sprzętowym w wersji 11.5(1) 9

Nowe informacje o oprogramowaniu sprzętowym w wersji 11.0 9

---

CZĘŚĆ I:

**Informacje o telefonach IP Cisco 11**

---

ROZDZIAŁ 2

**Szczegóły techniczne 13**

Cechy fizyczne i warunki otoczenia 13

Specyfikacja kabla 14

Styki portu sieciowego i portu komputera 14

Złącze portu sieciowego 14

Złącze portu komputera 15

Wymogi dotyczące zasilania telefonu 16

Przerwa w zasilaniu 17

Oszczędności na zużyciu energii 17

Negocjowanie zasilania przez protokół LLDP 17

Protokoły sieciowe 18

Interakcja z sieciami VLAN 22

Interakcja z programem Cisco Unified Communications Manager 22

Interakcja z programem Cisco Unified Communications Manager Express 23

Interakcje z systemem wiadomości głosowych 24

Omówienie uruchamiania telefonu 24

Urządzenia zewnętrzne 26

Informacje o porcie USB 27

Pliki konfiguracyjne telefonu 27

Działanie telefonu w okresach dużego obciążenia sieci 28

Działanie telefonu w sieci z dwoma routerami sieciowymi 28

Interfejs programowania aplikacji 28

---

ROZDZIAŁ 3

**Telefon IP Cisco — sprzęt 29**

Omówienie telefonu 29

Cisco IP Phone 8811 31

31

Telefony IP Cisco 8841 i 8845 32

Złącza telefonu 32

Telefony IP Cisco 8851 i 8851NR 33

– połączenia telefoniczne	34
Telefony IP Cisco 8861, 8865 i 8865NR	35
Złącza telefonu	35
Przyciski i podzespoły	36
Przyciski programowe, linii i funkcji	38
Ochrona kamery w telefonie	39

---

**CZĘŚĆ II:**
**Instalowanie telefonu IP Cisco 41**


---

**ROZDZIAŁ 4**
**Instalowanie telefonu IP Cisco 43**

Sprawdzanie konfiguracji sieci	43
Wdrażanie za pomocą kodu aktywacyjnego dla telefonów w siedzibie	44
Wdrażanie przy użyciu kodu aktywacyjnego oraz dostęp z urządzeń przenośnych i dostęp zdalny	45
Włączanie automatycznej rejestracji telefonów	46
Instalowanie telefonu IP Cisco	47
Współużytkowanie połączenia sieciowego — telefon i komputer	49
Konfigurowanie telefonu za pomocą menu konfiguracji	49
Ustawianie hasła w telefonie	50
Wprowadzanie tekstu za pomocą telefonu i poruszanie się po jego menu	51
Włącz w telefonie bezprzewodową sieć LAN	51
Konfigurowanie bezprzewodowej sieci LAN w programie Cisco Unified Communications Manager	52
Konfigurowanie bezprzewodowej sieci LAN z telefonu	53
Ustaw liczbę prób uwierzytelniania sieci WLAN	55
Włączanie trybu monitoringu sieci WLAN	56
Konfigurowanie profilu Wi-Fi za pomocą programu Cisco Unified Communications Manager	56
Konfigurowanie grupy Wi-Fi za pomocą programu Cisco Unified Communications Manager	58
Konfigurowanie ustawień sieciowych	59
Pola konfiguracji sieci Ethernet	59
Pola protokołu IPv4	61
Pola protokołu IPv6	63
Konfigurowanie telefonu do korzystania z protokołu DHCP	65
Konfigurowanie telefonu do niekorzystania z protokołu DHCP	65
Serwer pobierania	66

Sprawdzenie przy uruchamianiu telefonu	66
Konfigurowanie usług telefonicznych dla użytkowników	66
Zmień model telefonu użytkownika	67

**ROZDZIAŁ 5****Konfigurowanie telefonu w programie Cisco Unified Communications Manager 69**

Konfigurowanie telefonu IP Cisco	69
Sprawdzanie adresu MAC telefonu	72
Metody dodawania telefonów	73
Dodawanie telefonów pojedynczo	73
Dodawanie telefonów przy użyciu szablonu telefonu narzędzia BAT	74
Dodawanie użytkowników do programu Cisco Unified Communications Manager	74
Dodawanie użytkownika z zewnętrznego katalogu LDAP	75
Dodawanie użytkownika bezpośrednio do systemu Cisco Unified Communications Manager	75
Dodawanie użytkownika do grupy użytkowników końcowych	76
Kojarzenie telefonów z użytkownikami	77
Survivable Remote Site Telephony	77
Enhanced Survivable Remote Site Telephony	80
Strony WWW reguł wybierania numeru aplikacji	81
Konfigurowanie reguł wybierania numeru aplikacji	81

**ROZDZIAŁ 6****Zarządzanie portalem samoobsługowym 83**

Portal samoobsługowy — omówienie	83
Konfigurowanie dostępu użytkownika do portalu Self Care	84
Dostosowywanie wyświetlania w portalu Self Care	84

**CZĘŚĆ III:****Administrowanie telefonami IP Cisco 85****ROZDZIAŁ 7****Zabezpieczenia telefonu IP Cisco 87**

Zwiększone zabezpieczenia Twojej sieci telefonicznej	87
Obsługiwane funkcje zabezpieczeń	88
Konfigurowanie certyfikatu obowiązującego lokalnie	94
Włączanie trybu FIPS	95
Zabezpieczenia połączeń telefonicznych	95

Identyfikacja zabezpieczonych połączeń konferencyjnych	96
Identyfikacja zabezpieczonych połączeń telefonicznych	97
Szyfrowanie dla funkcji wtrącenia	98
Zabezpieczenia sieci WLAN	98
Konfigurowanie trybu uwierzytelniania	102
Poświadczenia zabezpieczeń sieci bezprzewodowej	102
Konfigurowanie nazwy użytkownika i hasła	103
Konfigurowanie klucza wstępnego	103
Szyfrowanie sieci bezprzewodowej	104
Eksportowanie certyfikatu urzędu certyfikacji z serwera ACS za pomocą usługi certyfikatów firmy Microsoft	105
Konfiguracja PEAP	110
Bezpieczeństwo sieci bezprzewodowej	110
Strona administrowania telefonem IP Cisco	111
Konfiguracja protokołu SCEP	114
Uwierzytelnianie 802.1X	115
Dostęp do uwierzytelniania 802.1X	116
Konfigurowanie pola Uwierzytelnianie urzędu	117

**ROZDZIAŁ 8****Dostosowywanie telefonu IP Cisco 119**

Niestandardowe dzwonki telefonu	119
Niestandardowe obrazy tła	119
Konfigurowanie kodeka komunikacji szerokopasmowej	121
Konfigurowanie ekranu bezczynności	122
Dostosowywanie sygnału wybierania	123

**ROZDZIAŁ 9****Funkcje telefonu i ich konfigurowanie 125**

Przegląd funkcji telefonu i ich konfigurowania	125
Pomoc techniczna dla użytkowników telefonu IP Cisco	125
Funkcje telefonu	126
Przyciski funkcyjne i klawisze programowe	146
Konfigurowanie funkcji telefonu	147
Konfigurowanie funkcji wszystkich telefonów	148
Konfigurowanie funkcji grupy telefonów	149

Konfigurowanie funkcji pojedynczego telefonu	149
Konfiguracja specyficzna dla produktu	149
Sprawdzone procedury konfigurowania funkcji	171
Środowiska z dużą liczbą połączeń	172
Środowiska z wieloma liniami	172
Środowisko trybu linii sesji	172
Pole: Always Use Prime Line (Zawsze używaj linii podstawowej)	173
Wyłączenie szyfrowania TLS (Transport Layer Security)	173
Włączanie historii połączeń dla linii wspólnej	174
Planowane oszczędzanie energii Power Save dla telefonów IP Cisco	174
Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco	176
Konfigurowanie funkcji Nie przeszkadzać	180
Włączanie funkcji Agent Greeting (Powitanie przez agenta)	181
Konfigurowanie monitorowania i nagrywania	182
Konfigurowanie powiadamiania o przekierowywaniu połączeń	183
Włączanie SZL dla list połączeń	184
Konfigurowanie protokołu Energy Efficient Ethernet dla przełącznika i portu komputera	184
Konfigurowanie zakresu portów protokołu RTP/sRTP	185
Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway	186
Scenariusze wdrożeń	187
Ścieżki mediów i mechanizmy interaktywnego nawiązywania połączeń (ang. ICE, Interactive Connectivity Establishment)	188
Funkcje telefonu dostępne dla Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway	189
Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway	191
Generowanie kodu QR dla logowania MRA	191
Narzędzie do zgłaszania problemów	191
Konfigurowanie adresu URL do przesyłania plików do pomocy technicznej	192
Konfigurowanie oznaczenia linii	193
Informacje o konfigurowaniu podwójnego zestawu	194
Monitorowanie parkowania	194
Konfigurowanie zegarów monitorowania parkowania	194
Ustawianie parametrów monitorowania parkowania dla numerów telefonów	196



Konfigurowanie monitorowania parkowania dla list poszukiwania	197
Konfigurowanie zakresu portów audio i wideo	197
Konfigurowanie programu Cisco IP Manager Assistant	199
Konfigurowanie wizualnej poczty głosowej	201
Konfigurowanie wizualnej poczty głosowej dla konkretnego użytkownika	202
Konfigurowanie wizualnej poczty głosowej dla grupy użytkowników	202
Assured Services SIP	203
Bezpośrednia migracja telefonu do telefonu wieloplatformowego	204
Wielopoziomowe pierwszeństwo i zastępowanie	204
Konfigurowanie szablonu klawiszy programowych	204
Szablony przycisków telefonu	207
Modyfikowanie szablonu przycisków telefonu	207
Przypisanie szablonu przycisków telefonu dla wszystkich połączeń	207
Konfigurowanie osobistej książki adresowej lub szybkiego wybierania jako usługi telefonu IP	208
Modyfikowanie szablonu przycisków telefonu dla osobistej książki adresowej lub szybkiego wybierania	209
Konfiguracja sieci VPN	210
Konfigurowanie klawiszy linii dodatkowej	211
Funkcje dostępne w trybie rozszerzonym linii	212
Konfigurowanie zegara wznowienia TLS	215
Włączenie funkcji Intelligent Proximity	215
Ustawianie rozdzielczości transmisji wideo	216
Parametry zarządzania zestawem nagłownym w starszych wersjach programu Cisco Unified Communications Manager	217
Pobieranie domyślnego pliku konfiguracyjnego zestawu nagłownego	218
Modyfikowanie domyślnego pliku konfiguracyjnego zestawu nagłownego	218
Instalowanie domyślnego pliku konfiguracyjnego w programie Cisco Unified Communications Manager	221
Ponowne uruchamianie serwera Cisco TFTP	221

---

**ROZDZIAŁ 10**
**Firmowa książka telefoniczna i osobista książka telefoniczna 223**

Konfigurowanie firmowej książki telefonicznej	223
Konfigurowanie osobistej książki adresowej	223
Konfigurowanie wpisów w osobistej książce adresowej użytkownika	224

Pobieranie dodatku Cisco IP Phone Address Book Synchronizer	225
Zastosowanie dodatku Cisco IP Phone Address Book Synchronizer	225
Instalowanie synchronizatora	225
Konfigurowanie dodatku Synchronizer	226

---

<b>CZĘŚĆ IV:</b>	<b>Rozwiązywanie problemów z telefonem IP Cisco</b>	<b>227</b>
------------------	---	------------

---

<b>ROZDZIAŁ 11</b>	<b>Monitorowanie systemów telefonicznych</b>	<b>229</b>
	Stan telefonu IP Cisco	229
	Wyświetlanie okna Informacje o telefonie	229
	Pola w oknie Informacje o telefonie	230
	Wyświetlanie menu Stan	230
	Wyświetlanie okna komunikatów o stanie	231
	Wyświetlanie ekranu informacji o sieci	235
	Wyświetlanie ekranu Statystyki sieci	236
	Wyświetlanie ekranu Statystyki sieci bezprzewodowej	239
	Wyświetlanie okna Statystyki połączeń	241
	Wyświetlanie okna Bieżący punkt dostępu	244
	Strona WWW telefonu IP Cisco	246
	Otwieranie strony WWW telefonu	246
	Informacje o urządzeniu	247
	Konfiguracja sieci	249
	Statystyki sieci	255
	Dzienniki urządzeń	258
	Statystyki strumieniowania	259
	Żądanie informacji z telefonu w formacie XML	263
	Przykładowe dane wyjściowe polecenia CallInfo	264
	Przykładowe dane wyjściowe polecenia LineInfo	265
	Przykładowe dane wyjściowe polecenia ModeInfo	265

---

<b>ROZDZIAŁ 12</b>	<b>Rozwiązywanie problemów</b>	<b>267</b>
	Ogólne informacje o rozwiązywaniu problemów	267
	Problemy z uruchamianiem	268
	Telefon IP Cisco nie przechodzi przez zwykły proces uruchamiania	269

Telefon IP Cisco nie rejestruje się w programie Cisco Unified Communications Manager	270
Telefon wyświetla komunikaty o błędach	270
Telefon nie może połączyć się z serwerem TFTP ani systemem Cisco Unified Communications Manager	270
Telefon nie może połączyć się z serwerem TFTP	270
Telefon nie może połączyć się z serwerem	271
Telefon nie może nawiązać połączenia z użyciem serwera DNS	271
Nie są uruchomione usługi Cisco Unified Communications Manager ani TFTP	271
Uszkodzenie pliku konfiguracyjnego	271
Rejestrowanie telefonu w programie Cisco Unified Communications Manager	272
Telefon IP Cisco nie może uzyskać adresu IP	272
Telefon się nie rejestruje	272
Problemy z resetowaniem się telefonu	273
Telefon resetuje się z powodu chwilowych przerw w działaniu sieci	273
Telefon resetuje się z powodu błędnych ustawień serwera DHCP	273
Telefon resetuje się z powodu nieprawidłowego statycznego adresu IP	273
Telefon resetuje się podczas dużego obciążenia sieci	274
Telefon resetuje się z powodu celowego zresetowania	274
Telefon resetuje się z powodu problemu z serwerem DNS lub innych problemów z łącznością	274
Telefon nie włącza się	275
Telefon nie może się połączyć z siecią LAN	275
Problemy z zabezpieczeniami telefonu IP Cisco	275
Problemy z plikiem CTL	275
Błąd uwierzytelniania, telefon nie może uwierzytelnić pliku CTL	275
Telefon nie może uwierzytelnić pliku CTL	276
Plik CTL jest uwierzytelniony, ale inne pliki konfiguracyjne nie są	276
Plik ITL jest uwierzytelniony, ale inne pliki konfiguracyjne nie są	276
Uwierzytelnianie serwera TFTP nie powiodło się	276
Telefon nie rejestruje się	277
Telefon nie żąda podpisanych plików konfiguracyjnych	277
Problemy z połączeniem wideo	277
Brak wideo między dwoma telefonami wideo IP Cisco	277
Brak płynności obrazu i gubienie ramek	278
Nie można przekierować połączenia wideo	278

Brak transmisji obrazu podczas połączenia konferencyjnego	278
Ogólne problemy z połączeniami telefonicznymi	278
Nie można zestawić połączenia telefonicznego	279
Telefon nie rozpoznaje cyfr DTMF lub cyfry są opóźnione	279
Procedury rozwiązywania problemów	279
Tworzenie raportu o problemie z telefonem w programie Cisco Unified Communications Manager	280
Tworzenie dziennika konsoli za pomocą telefonu	280
Sprawdzanie ustawień TFTP	280
Identyfikowanie problemów z systemem DNS lub łącznością	281
Sprawdzanie ustawień DHCP	281
Tworzenie nowego pliku konfiguracyjnego telefonu	282
Identyfikowanie problemów z uwierzytelnianiem 802.1X	283
Sprawdzanie ustawień DNS	283
Uruchamianie usługi	283
Informacje kontrolne debugowania z programu Cisco Unified Communications Manager	284
Dodatkowe informacje o sposobach rozwiązywania problemów	285

**ROZDZIAŁ 13****Konserwacja 287**

Resetowanie podstawowe	287
Przywracanie fabrycznych ustawień telefonu z klawiatury telefonu	288
Resetowanie wszystkich ustawień za pomocą menu telefonu	288
Ponowne uruchamianie telefonu przy użyciu obrazu kopii zapasowej	289
Resetowanie konfiguracji sieci	289
Resetowanie konfiguracji sieci użytkownika	289
Usuwanie pliku CTL	290
Quality Report Tool	290
Monitorowanie jakości dźwięku	290
Wskazówki dotyczące rozwiązywania problemów z jakością dźwięku	291
Czyszczenie telefonu IP Cisco	292

**ROZDZIAŁ 14****Obsługa użytkowników międzynarodowych 293**

Instalator lokalny punktów końcowych programu Unified Communications Manager	293
Obsługa zapisu połączeń międzynarodowych w dzienniku	293

Ograniczenia językowe 294





## Przedmowa

- Omówienie, na stronie xv
- Do kogo adresowany jest ten podręcznik?, na stronie xv
- Konwencje przyjęte w podręczniku, na stronie xv
- Dokumentacja pokrewna, na stronie xvi
- Dokumentacja, pomoc techniczna i wskazówki dotyczące bezpieczeństwa, na stronie xvii

## Omówienie

*Podręcznik administratora telefonów IP Cisco z serii 8800 do programu Cisco Unified Communications Manager zawiera informacje niezbędne do zrozumienia, zainstalowania, skonfigurowania, zarządzania i rozwiązywania problemów z telefonami w sieci VoIP.*

Ze względu na złożoność sieci telefonicznych IP podręcznik nie zawiera kompletnych ani w pełni szczegółowych informacji o procedurach, które trzeba wykonać w programie Cisco Unified Communications Manager lub na innych urządzeniach sieciowych.

## Do kogo adresowany jest ten podręcznik?

Z podręcznikiem tym powinni się zapoznać inżynierowie ds. sieci, administratorzy systemu i inżynierowie ds. telekomunikacji, aby dowiedzieć się, jak przebiega konfigurowanie telefonu IP Cisco. Zadania opisane w tym dokumencie obejmują konfigurowanie ustawień sieciowych, które nie są przeznaczone dla użytkowników telefonów. Zadania przedstawione w tym podręczniku wymagają znajomości programu Cisco Unified Communications Manager.

## Konwencje przyjęte w podręczniku

W tym dokumencie są używane następujące konwencje zapisu:

Wyróżnienie	Opis
<b>pogrubiona</b> czcionka	Komendy i słowa kluczowe są oznaczone <b>pogrubioną czcionką</b> .
<i>kursywa</i>	Argumenty, do których są przypisywane wartości, są oznaczone <i>kursywą</i> .

Wyróżnienie	Opis
[ ]	Elementy w nawiasach kwadratowych są opcjonalne.
{x   y   z}	Alternatywne słowa kluczowe są ujmowane w nawiasy klamrowe i oddzielane pionowymi kreskami.
[x   y   z]	Opcjonalne alternatywne słowa kluczowe są ujmowane w nawiasy kwadratowe i oddzielane pionowymi kreskami.
łańcuch	Zestaw znaków bez cudzysłowu. Nie należy ujmować łańcucha w cudzysłowy, ponieważ w przeciwnym razie zostaną one zawarte w łańcuchu.
czcionka ekranowa	Sesje terminalowe i informacje wyświetlane przez system są oznaczone czcionką ekranową.
czcionka <b>danych wejściowych</b>	Informacje wprowadzane przez użytkownika są wyróżnione czcionką <b>danych wejściowych</b> .
<i>kursywa ekranowa</i>	Argumenty, do których są przypisywane wartości, są oznaczone <i>kursywą ekranową</i> .
^	Symbol ^ oznacza klawisz Control — na przykład kombinacja ^D na ekranie oznacza „trzymaj wciśnięty klawisz Control, naciśnij klawisz D”.
<>	Znaki niewyświetlane, np. hasła, podano w nawiasach kątowych.



**Uwaga** Oznacza fragment, na który *trzeba zwrócić szczególną uwagę*. Pola uwag zawierają pomocne sugestie lub odsyłacze do materiałów uzupełniających tę publikację.



**Przeostroga** Oznacza, że *należy zachować ostrożność*. Wskazuje sytuację, w której użytkownik może wykonać czynność skutkującą uszkodzeniem sprzętu lub utratą danych.

Dla ostrzeżeń jest stosowana następująca konwencja:



**Uwaga** WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzegawczy oznacza zagrożenie. Wskazuje sytuację mogącą spowodować obrażenia ciała. Obsługując jakiegokolwiek urządzenie, należy zdawać sobie sprawę z możliwości porażenia prądem płynącym w obwodach elektrycznych oraz znać podstawowe zasady zapobiegania wypadkom. Używając numeru umieszczonego na końcu każdego ostrzeżenia, znajdź jego tłumaczenie w przetłumaczonym spisie ostrzeżeń dotyczących bezpieczeństwa dołączonym to tego urządzenia. Instrukcja 1071

INSTRUKCJE NALEŻY ZACHOWAĆ

## Dokumentacja pokrewna

Informacje pokrewne można znaleźć w następujących sekcjach.



## Telefon IP Cisco z serii 8800 — Dokumentacja

Na stronie [pomocy technicznej](#) dotyczącej telefonu IP Cisco z serii 7800 można znaleźć dokumentację właściwą dla danego języka, modelu telefonu i systemu obsługi połączeń.

Podręcznik wdrażania jest dostępny pod następującym adresem URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>

## Cisco Unified Communications Manager — Dokumentacja

Należy zapoznać się z dokumentem *Cisco Unified Communications Manager Documentation Guide* (Przewodnik po dokumentacji programu Cisco Unified Communications Manager) i innymi publikacjami dotyczącymi używanej wersji programu Cisco Unified Communications Manager. Można je znaleźć pod następującym adresem URL dokumentacji:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>

## Cisco Business Edition 6000 — Dokumentacja

Należy zapoznać się z dokumentem *Cisco Business Edition 6000 Documentation Guide* (Podręcznik dokumentacji programu Cisco Business Edition 6000) i innymi publikacjami dotyczącymi używanej wersji programu Cisco Business Edition 6000. Należy skorzystać z następującego adresu URL:

<https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html>

## Dokumentacja, pomoc techniczna i wskazówki dotyczące bezpieczeństwa

Informacje o uzyskiwaniu dokumentacji i pomocy technicznej, przesyłaniu komentarzy do dokumentacji, wytycznych dotyczących bezpieczeństwa, zalecanych aliasach oraz ogólnej dokumentacji firmy Cisco można znaleźć w comiesięcznych aktualizacjach na stronie *Co nowego w dokumentacji technicznej firmy Cisco*. Znajduje się tam również lista nowej i poprawionej dokumentacji technicznej firmy Cisco:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

Biuletyn *Co nowego w dokumentacji technicznej firmy Cisco* można subskrybować przy użyciu formatu sieciowego RSS (ang. Really Simple Syndication, naprawdę proste rozpowszechnianie), tj. w formie automatycznych publikacji na komputerze użytkownika za pośrednictwem czytnika kanałów. Kanały RSS są usługą bezpłatną, a systemy firmy Cisco obsługują obecnie wersję RSS 2.0.

## Ogólne informacje na temat bezpieczeństwa produktu Cisco

Niniejszy produkt zawiera funkcje kryptograficzne i podlega przepisom Stanów Zjednoczonych oraz krajowym przepisom lokalnym regulującym kwestie importu, eksportu, przekazywania oraz użytkowania. Dostarczenie produktów Cisco zawierających funkcje kryptograficzne nie oznacza upoważnienia podmiotu niezależnego

do importu, eksportu, dystrybucji lub użytkowania szyfrowania. Odpowiedzialność za zgodność swojego postępowania z lokalnym prawem krajowym oraz prawem Stanów Zjednoczonych ponoszą importerzy, eksporterzy, dystrybutorzy oraz użytkownicy. Korzystając z niniejszego produktu, użytkownik zgadza się postępować zgodnie z odpowiednimi regulacjami i przepisami prawa. W przypadku braku możliwości zastosowania się do przepisów prawnych lokalnego prawa krajowego oraz przepisów prawnych Stanów Zjednoczonych niniejszy produkt należy niezwłocznie zwrócić.

Więcej informacji na temat obowiązujących w Stanach Zjednoczonych przepisów dotyczących eksportu można znaleźć pod adresem <https://www.bis.doc.gov/policiesandregulations/ear/index.htm>.



## ROZDZIAŁ 1

# Nowe i zmienione informacje

- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.2(1), na stronie 1
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.1(1), na stronie 2
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.0(1), na stronie 2
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.8(1), na stronie 3
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.7(1), na stronie 4
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.6(1), na stronie 4
- Nowe informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR3, na stronie 5
- Nowe informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR1, na stronie 5
- Nowe informacje o oprogramowaniu sprzętowym w wersji 12.1(1)SR1, na stronie 6
- Nowe informacje o oprogramowaniu sprzętowym w wersji 12.1(1), na stronie 6
- Nowe informacje o oprogramowaniu sprzętowym w wersji 12.0(1), na stronie 7
- Nowe informacje o oprogramowaniu sprzętowym w wersji 11.7(1), na stronie 7
- Nowe informacje o oprogramowaniu sprzętowym w wersji 11.5(1)SR1, na stronie 8
- Nowe informacje o oprogramowaniu sprzętowym w wersji 11.5(1), na stronie 9
- Nowe informacje o oprogramowaniu sprzętowym w wersji 11.0, na stronie 9

## Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.2(1)

Poniżej znajdują się nowe lub zmienione informacje o oprogramowaniu sprzętowym w wersji 14.2(1)

Funkcja	Nowe lub zmienione
Obsługa protokołu SIP OAuth w SRST	Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 87
Uproszczone poruszanie się po rozszerzeniach dzięki adapterowi USB zestawu słuchawkowego Cisco 730	Funkcje telefonu, na stronie 126
Synchronizacja wyciszenia Bluetooth dla zestawów słuchawkowych Cisco serii 700	Funkcje telefonu, na stronie 126

Funkcja	Nowe lub zmienione
Nowe ustawienia dla zestawu słuchawkowego Cisco z serii 500: Zdarzenie dokowania i Tryb zawsze włączony	<a href="#">Funkcje telefonu, na stronie 126</a>

## Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.1(1)

Następujące informacje są nowe lub zmienione w wersji oprogramowania sprzętowego 14.1(1).

Funkcja	Nowe lub zmienione
Obsługa SIP OAuth dla Proxy TFTP	<a href="#">Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 87</a>
Udoskonalony alert dotyczący połączenia z grupą wyszukiwania	<a href="#">Funkcje telefonu, na stronie 126</a>
Konfigurowalny numer dzwoniący jest wyświetlany dla trybu linii rozszerzonej	<a href="#">Konfiguracja specyficzna dla produktu</a>
Konfigurowalne opóźnienie PLAR	<a href="#">Funkcje telefonu, na stronie 126</a>
Obsługa MRA dla Extension Mobility Login z zestawami słuchawkowymi Cisco	<a href="#">Funkcje telefonu, na stronie 126</a>
Migracja telefonu bez wcześniejszego obciążenia	<a href="#">Bezpośrednia migracja telefonu do telefonu wieloplatformowego, na stronie 204</a>

## Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 14.0(1)

*Tabela 1: Nowe i zmienione informacje*

Funkcja	Nowe lub zmienione
Ulepszone funkcje monitorowania parkowania połączenia	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>
Udoskonalenia protokołu SIP OAuth	<a href="#">Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 87</a>
Ulepszenia interfejsu użytkownika	<a href="#">Survivable Remote Site Telephony, na stronie 77</a> <a href="#">Funkcje telefonu, na stronie 126</a>

Funkcja	Nowe lub zmienione
Udoskonalenia uwierzytelniania OAuth dla MRA	<a href="#">Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, na stronie 186</a>

Od wersji oprogramowania sprzętowego 14.0, telefony obsługują DTLS 1.2. DTLS 1.2 wymaga Cisco Adaptive Security Appliance (ASA) w wersji 9.10 lub nowszej. Można skonfigurować minimalną wartość wersji DTLS dla połączenia VPN w ASA. Więcej informacji można znaleźć w książce *ASDM Book 3: Podręcznik konfiguracji ASDM VPN Cisco ASA* dostępnym tutaj: <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>

## Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.8(1)

Poniżej znajdują się nowe lub zmienione informacje o oprogramowaniu sprzętowym w wersji 12.8(1)

Funkcja	Nowa lub zmieniona treść
Migracja danych telefonu	<a href="#">Zmień model telefonu użytkownika, na stronie 67</a>
Usprawnienia w aktualizacjach zestawu słuchawkowego	<a href="#">Informacje o urządzeniu, na stronie 247</a>
Uproszczenie logowania do funkcji Extension Mobility za pomocą zestawów słuchawkowych Cisco	<a href="#">Funkcje telefonu, na stronie 126</a>
Zmiany w sterowaniu funkcjami	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a> , nowe pola <b>Alert dotyczący ściszenia głosu</b> oraz <b>Oznacz połączenie jako spam</b>
Ogólne zmiany	Objaśnienie działania sieci Wi-Fi i funkcji portu komputera: <ul style="list-style-type: none"> <li>• <a href="#">Konfigurowanie telefonu za pomocą menu konfiguracji, na stronie 49</a></li> <li>• <a href="#">Włącz w telefonie bezprzewodową sieć LAN, na stronie 51</a></li> </ul>
Dodano dodatkowe informacje o polu dostęp przez WWW	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>
Usuwanie nieobsługiwanej funkcji	<a href="#">Funkcje telefonu, na stronie 126</a>

## Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.7(1)

Tabela 2: Poprawki w Podręczniku administratora telefonu IP Cisco 8800 związane z oprogramowaniem sprzętowym w wersji 12.7(1).

Poprawka	Zaktualizowana część
Zaktualizowano informacje o tapecie Cisco na modułach rozbudowy klawiatury.	<a href="#">Niestandardowe obrazy tła, na stronie 119</a>
Zaktualizowano informacje o obsłudze Zestaw słuchawkowy Cisco 730	<a href="#">Informacje o urządzeniu, na stronie 247</a>
Zaktualizowano Zestaw słuchawkowy Cisco z serii 500 dla oprogramowania sprzętowego w wersji 2.0	<a href="#">Informacje o urządzeniu, na stronie 247</a> <a href="#">Parametry zarządzania zestawem nagłownym w starszych wersjach programu Cisco Unified Communications Manager, na stronie 217</a>
Zaktualizowano w przypadku połączeń przychodzących grup poszukiwania.	<a href="#">Funkcje telefonu, na stronie 126</a>
Usunięto informacje o konfiguracji odłożonej słuchawki.	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>

## Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.6(1)

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

Tabela 3: Poprawki w Podręczniku administratora telefonów IP Cisco z serii 8800 związane z oprogramowaniem sprzętowym w wersji 12.6(1).

Poprawka	Zaktualizowana część
Aktualizacja dla obsługi funkcji powracania do linii podstawowej w trybie linii sesji.	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a> <a href="#">Środowisko trybu linii sesji, na stronie 172</a>

## Nowe informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR3

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

**Tabela 4: Poprawki w Podręczniku administratora telefonów IP Cisco z serii 8800 związane z oprogramowaniem sprzętowym w wersji 12.5(1)SR3.**

Poprawka	Zaktualizowana część
Obsługa wdrażania przy użyciu kodu aktywacyjnego oraz dostępu z urządzeń przenośnych i dostępu zdalnego	Wdrażanie przy użyciu kodu aktywacyjnego oraz dostęp z urządzeń przenośnych i dostęp zdalny, na stronie 45
Obsługa narzędzia do zgłaszania problemów (PRT) w programie Cisco Unified Communications Manager.	Tworzenie raportu o problemie z telefonem w programie Cisco Unified Communications Manager, na stronie 280
Nowy temat	Współużytkowanie połączenia sieciowego — telefon i komputer, na stronie 49
Nowy temat	Ochrona kamery w telefonie, na stronie 39

## Nowe informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR1

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

**Tabela 5: Poprawki w Podręczniku administratora telefonu IP Cisco 8800 związane z oprogramowaniem sprzętowym w wersji 12.5(1)SR1**

Poprawka	Zaktualizowana część
Obsługa certyfikatów Elliptic Curve	Obsługiwane funkcje zabezpieczeń, na stronie 88
Obsługa historii połączeń dla trybu rozszerzonego linii z liniami przewijania	Funkcje dostępne w trybie rozszerzonym linii, na stronie 212
Obsługa funkcji Whisper Paging w programie Cisco Unified Communications Manager Express	Interakcja z programem Cisco Unified Communications Manager Express, na stronie 23
Obsługa języka chińskiego	Ograniczenia językowe, na stronie 294
Obsługa wdrażania za pomocą kodu aktywacyjnego	Wdrażanie za pomocą kodu aktywacyjnego dla telefonów w siedzibie, na stronie 44

Poprawka	Zaktualizowana część
Obsługa ścieżek nośników i mechanizmów interaktywnego nawiązywania połączeń (ang. ICE, Interactive Connectivity Establishment)	<a href="#">Ścieżki mediów i mechanizmy interaktywnego nawiązywania połączeń (ang. ICE, Interactive Connectivity Establishment), na stronie 188</a>
Obsługa funkcji Wyłącz szyfrowanie TLS	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>
Obsługa wyłączenia słuchawki, aby ścieżka dźwięku pozostawała ustawiona na zestaw nagłowny	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>
Obsługa zdalnego konfigurowania parametrów zestawu nagłownego	<a href="#">Parametry zarządzania zestawem nagłownym w starszych wersjach programu Cisco Unified Communications Manager, na stronie 217</a>

## Nowe informacje o oprogramowaniu sprzętowym w wersji 12.1(1)SR1

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

**Tabela 6: Poprawki w Podręczniku administratora telefonów IP Cisco z serii 8800 związane z oprogramowaniem sprzętowym w wersji 12.1(1)SR1**

Poprawka	Zaktualizowana część
Wybieranie blokowe dla rozszerzenia czasomierza między cyframi T.302.	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>

## Nowe informacje o oprogramowaniu sprzętowym w wersji 12.1(1)

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.



**Tabela 7: Poprawki w Podręczniku administratora telefonów IP Cisco z serii 8800 związane z oprogramowaniem sprzętowym w wersji 12.1(1).**

Poprawka	Zaktualizowana część
Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway obsługuje obecnie tryb rozszerzony linii.	<a href="#">Funkcje telefonu dostępne dla Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, na stronie 189</a>
	<a href="#">Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, na stronie 186</a>
	<a href="#">Funkcje dostępne w trybie rozszerzonym linii, na stronie 212</a>
Włączanie i wyłączanie protokołu TLS 1.2 dla dostępu do serwera WWW jest teraz obsługiwane.	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>
Obsługiwany jest teraz kodek audio G722.2 AMR-WB.	<a href="#">Omówienie telefonu, na stronie 29</a>
	<a href="#">Poła na ekranie Statystyki połączeń, na stronie 241</a>

## Nowe informacje o oprogramowaniu sprzętowym w wersji 12.0(1)

Opisy wszystkich nowych funkcji dodano do części [Funkcje telefonu, na stronie 126](#).

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

**Tabela 8: Poprawki w Podręczniku administratora telefonów IP Cisco z serii 8800 związane z oprogramowaniem sprzętowym w wersji 12.0(1).**

Poprawka	Zaktualizowana część
Zaktualizowano informacje o funkcjach Parkowanie połączenia, Stan linii Parkowanie połączenia i Grupowe odebranie oraz o obsłudze grup poszukiwania w trybie rozszerzonym linii	<a href="#">Funkcje dostępne w trybie rozszerzonym linii, na stronie 212</a>

## Nowe informacje o oprogramowaniu sprzętowym w wersji 11.7(1)

Wersja firmware 11.7(1) nie wymaga żadnych aktualizacji administracyjnych.

# Nowe informacje o oprogramowaniu sprzętowym w wersji 11.5(1)SR1

Opisy wszystkich nowych funkcji dodano do części [Funkcje telefonu, na stronie 126](#).

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

**Tabela 9: Poprawki w Podręczniku administratora telefonu IP Cisco 8800 związane z oprogramowaniem sprzętowym w wersji 11.5(1)SR1.**

Poprawka	Zaktualizowana część
Zaktualizowano informacje o obsłudze telefonu IP Cisco 8865NR	<ul style="list-style-type: none"> <li>• <a href="#">Wymogi dotyczące zasilania telefonu, na stronie 16</a></li> <li>• <a href="#">Protokoły sieciowe, na stronie 18</a></li> <li>• <a href="#">Omówienie telefonu, na stronie 29</a></li> <li>• <a href="#">Przyciski i podzespoły, na stronie 36</a></li> </ul>
Zaktualizowano obsługę nagrywania i monitorowania w trybie rozszerzonym linii	<a href="#">Funkcje dostępne w trybie rozszerzonym linii, na stronie 212</a>
Zaktualizowano obsługę listy skanowania sieci WLAN	<a href="#">Włącz w telefonie bezprzewodową sieć LAN, na stronie 51</a>
	<a href="#">Konfigurowanie bezprzewodowej sieci LAN z telefonu, na stronie 53</a>
	<a href="#">Konfigurowanie ustawień sieciowych, na stronie 59</a>
Zaktualizowano pod kątem funkcji Nie przeszkadzać z obsługą MLPP	<a href="#">Konfigurowanie funkcji Nie przeszkadzać, na stronie 180</a>
Zaktualizowano pod kątem obsługi Konfigurowalnego dzwonka	<a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>
Rozszerzone bezpieczeństwo	<a href="#">Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 87</a>
Ogólne zmiany	<p><a href="#">Aktualizacje sekcji Strona WWW telefonu IP Cisco, na stronie 246</a></p> <p><a href="#">Nowa prezentacja konfiguracji funkcji telefonu w programie Cisco Unified Communications Manager Konfigurowanie funkcji telefonu, na stronie 147</a></p>

# Nowe informacje o oprogramowaniu sprzętowym w wersji 11.5(1)

Tabela 10: Poprawki w Podręczniku administratora telefonu IP Cisco 8800 związane z oprogramowaniem sprzętowym w wersji 11.5(1).

Poprawka	Zaktualizowana część
Rozszerzony tryb linii jest obsługiwany.	<a href="#">Konfigurowanie klawiszy linii dodatkowej, na stronie 211</a> <a href="#">Funkcje dostępne w trybie rozszerzonym linii, na stronie 212</a>
Funkcja Nie przeszkadzać (DND) została zaktualizowana w celu dostosowania do nowego ekranu.	<a href="#">Konfigurowanie funkcji Nie przeszkadzać, na stronie 180</a>
Kodek Opus jest obsługiwany.	<a href="#">Omówienie telefonu, na stronie 29</a>
Dodano tryb FIPS.	<a href="#">Włączanie trybu FIPS, na stronie 95</a>
Zaktualizowano konfigurację sieci WLAN.	<a href="#">Konfigurowanie bezprzewodowej sieci LAN z telefonu, na stronie 53</a>
Profil sieci WLAN dla telefonów IP Cisco 8861 i 8865 jest obsługiwany.	<a href="#">Konfigurowanie profilu Wi-Fi za pomocą programu Cisco Unified Communications Manager, na stronie 56</a>
	<a href="#">Konfigurowanie grupy Wi-Fi za pomocą programu Cisco Unified Communications Manager, na stronie 58</a>
Ustawianie liczby prób uwierzytelnienia w sieci WLAN jest obsługiwane.	<a href="#">Ustaw liczbę prób uwierzytelniania sieci WLAN, na stronie 55</a>
Włączanie trybu monitu sieci WLAN jest obsługiwane.	<a href="#">Włączanie trybu monitu sieci WLAN, na stronie 56</a>
Dostosowywanie sygnału wybierania jest obsługiwane.	<a href="#">Dostosowywanie sygnału wybierania, na stronie 123</a>
Wyświetlanie ekranu informacji o sieci jest obsługiwane.	<a href="#">Wyświetlanie ekranu informacji o sieci, na stronie 235</a>

## Nowe informacje o oprogramowaniu sprzętowym w wersji 11.0

Opisy wszystkich nowych funkcji dodano do części [Funkcje telefonu, na stronie 126](#).

Zaktualizowano wszystkie odwołania do dokumentacji programu Cisco Unified Communications Manager, aby odpowiadały one każdej jego wersji.

Tabela 11: Poprawki w Podręczniku administratora telefonu IP Cisco 8800 związane z oprogramowaniem sprzętowym w wersji 11.0.

Poprawka	Zaktualizowana część
Zaktualizowano pod kątem zwiększenia przejrzystości i wyjaśnienia nieścisłości	<ul style="list-style-type: none"> <li>• Konfiguracja sieci VPN, na stronie 210</li> <li>• Konfigurowanie ustawień sieciowych, na stronie 59</li> <li>• Konfigurowanie protokołu Energy Efficient Ethernet dla przełącznika i portu komputera, na stronie 184</li> <li>• Ustawianie rozdzielczości transmisji wideo, na stronie 216</li> <li>• Enhanced Survivable Remote Site Telephony, na stronie 80</li> </ul>
Zaktualizowano w celu poprawy opisu opcji wycinkowego debugowania telefonu	<ul style="list-style-type: none"> <li>• Informacje kontrolne debugowania z programu Cisco Unified Communications Manager, na stronie 284.</li> </ul>
Zaktualizowano w celu poprawy opisu obsługi certyfikatów cyfrowych EAP-TLS + SCEP, PEAP-GTC i X.509	<ul style="list-style-type: none"> <li>• Zabezpieczenia sieci WLAN, na stronie 98.</li> <li>• Konfigurowanie trybu uwierzytelniania, na stronie 102</li> <li>• Poświadczenia zabezpieczeń sieci bezprzewodowej, na stronie 102</li> </ul>
Zaktualizowano w celu poprawy opisu obsługi Narzędzia do zgłaszania problemów (PRT)	<ul style="list-style-type: none"> <li>• Narzędzie do zgłaszania problemów, na stronie 191.</li> <li>• Konfigurowanie adresu URL do przesyłania plików do pomocy technicznej, na stronie 192.</li> </ul>
Dodano obsługę reguł wybierania numeru aplikacji	<ul style="list-style-type: none"> <li>• Strony WWW reguł wybierania numeru aplikacji, na stronie 81</li> </ul>
Dodano etykietę tekstową linii	<ul style="list-style-type: none"> <li>• Konfigurowanie oznaczenia linii, na stronie 193.</li> </ul>



CZĘŚĆ I

## Informacje o telefonach IP Cisco

- [Szczegóły techniczne, na stronie 13](#)
- [Telefon IP Cisco — sprzęt, na stronie 29](#)





## ROZDZIAŁ 2

### Szczegóły techniczne

- Cechy fizyczne i warunki otoczenia, na stronie 13
- Specyfikacja kabla, na stronie 14
- Wymogi dotyczące zasilania telefonu, na stronie 16
- Protokoły sieciowe, na stronie 18
- Interakcja z sieciami VLAN, na stronie 22
- Interakcja z programem Cisco Unified Communications Manager, na stronie 22
- Interakcja z programem Cisco Unified Communications Manager Express, na stronie 23
- Interakcje z systemem wiadomości głosowych, na stronie 24
- Omówienie uruchamiania telefonu, na stronie 24
- Urządzenia zewnętrzne, na stronie 26
- Informacje o porcie USB, na stronie 27
- Pliki konfiguracyjne telefonu, na stronie 27
- Działanie telefonu w okresach dużego obciążenia sieci, na stronie 28
- Działanie telefonu w sieci z dwoma routerami sieciowymi, na stronie 28
- Interfejs programowania aplikacji, na stronie 28

### Cechy fizyczne i warunki otoczenia

W poniższej tabeli podano cechy fizyczne i warunki otoczenia telefonów IP Cisco z serii 8800.

**Tabela 12: Cechy fizyczne i warunki otoczenia**

Specyfikacja	Wartość lub zakres
Temperatura pracy	Od 0 do +40°C (od +32 do +104°F)
Wilgotność względna podczas pracy	Podczas pracy: od 10% do 90% (bez kondensacji) Gdy nie pracuje: od 10% do 95% (bez kondensacji)
Temperatura przechowywania	Od -10 do +60°C (od +14 do +140°F)
Wysokość	229,1 mm (9,02 cala)
Szerokość	257,34 mm (10,13 cala)

Specyfikacja	Wartość lub zakres
Głębokość	40 mm (1,57 cala)
Masa	2,62 lb (1,19 kg)
Gniazdo zasilania	Prąd zmienny 100–240 V, 50–60 Hz, 0,5 A — przy korzystaniu z zasilacza sieciowego Prąd stały 48 V, 0,2 A — przy korzystaniu z zasilania za pośrednictwem kabla sieciowego
Kable	Kategoria 3/5/5e/6 w przypadku kabli o przepustowości 10 Mb/s z 4 parami przewodów Kategoria 5/5e/6 w przypadku kabli o przepustowości 100 Mb/s z 4 parami przewodów Kategoria 5e/6 w przypadku kabli o przepustowości 1000 Mb/s z 4 parami przewodów <b>Uwaga</b> Kable składają się z 4 par przewodów tworzących łącznie 8 przewodów
Wymagania dotyczące odległości	Zgodnie ze specyfikacją sieci Ethernet przyjmuje się, że maksymalna długość kabla między każdym telefonem IP Cisco a przełącznikiem wynosi 100 metrów.

## Specyfikacja kabla

Następujące informacje zawierają specyfikację kabla:

- Gniazdo RJ-9 (4-stykowe) do podłączania słuchawki i zestawu słuchawkowego.
- Gniazdo RJ-45 do połączenia 10/100/1000BaseT sieci LAN (10/100/1000 portu sieci w telefonie)
- Gniazdo RJ-45 dla drugiego połączenia 10/100/1000BaseT (10/100/1000 portu komputera w telefonie)
- Gniazdo typu jack 3,5 mm do podłączenia głośnika (tylko telefon IP Cisco 8861)
- Złącze zasilania prądem stałym 48 V.
- Porty/złącza USB: jeden port USB w telefonie IP Cisco 8851 i dwa porty USB w telefonie IP Cisco 8861
- 3 złącza na moduły rozszerzenia klawiatury traktowane jako złącza USB w telefonach IP Cisco 8851 i 8861

## Styki portu sieciowego i portu komputera

Wprawdzie zarówno port sieciowy, jak i port komputera (dostępowy) służą do komunikacji z siecią, jednak mają różne przeznaczenie i odmienne styki.

- Port sieciowy jest portem programowym 10/100/1000 znajdującym się w telefonie IP Cisco.
- Port komputera (dostępowy) jest portem programowym komputera 10/100/1000 znajdującym się w telefonie IP Cisco.

## Złącze portu sieciowego

W poniższej tabeli opisano styki złącza portu sieciowego.



Tabela 13: Styki złącza portu sieciowego

Numer styku	Funkcja
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
<b>Uwaga</b>	Skrót BI oznacza połączenie dwukierunkowe (ang. bidirectional), a skróty DA, DB, DC i DD to odpowiednio Dane A, Dane B, Dane C i Dane D.

## Złącze portu komputera

W poniższej tabeli opisano styki złącza portu komputera.

Tabela 14: Styki złącza portu komputera (dostępu)

Numer styku	Funkcja
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
<b>Uwaga</b>	Skrót BI oznacza połączenie dwukierunkowe (ang. bidirectional), a skróty DA, DB, DC i DD to odpowiednio Dane A, Dane B, Dane C i Dane D.

## Wymogi dotyczące zasilania telefonu

Telefon IP Cisco można zasilac z zewnętrznego Źródła lub z użyciem zasilania PoE (ang. Power over Ethernet, zasilanie poprzez sieć Ethernet). Zewnętrznym Źródłem zasilania jest osobny zasilacz. Przełącznik może dostarczac zasilanie PoE za pośrednictwem kabla Ethernet telefonu.

Telefony IP Cisco 8861 i 8865 są urządzeniami PoE klasy 4 i do obsługi dodatkowych funkcji wymagają przełącznika lub karty klasy 4 podłączanej na linię.

Więcej informacji o zapotrzebowaniu telefonu na prąd można znaleźć w jego arkuszu danych.

Podczas instalowania telefonu zasilanego z zewnętrznego Źródła należy przed podłączeniem kabla Ethernet podłączyc do telefonu zasilacz. Podczas demontowania telefonu zasilanego z zewnętrznego Źródła należy przed odłączeniem zasilacza odłączyc od telefonu kabel Ethernet.

**Tabela 15: Wskazówki dotyczące zasilania telefonu IP Cisco**

Rodzaj zasilania	Wskazówki
Zewnętrzne Źródło zasilania — zewnętrzny zasilacz CP-PWR-CUBE-4	Telefon IP Cisco korzysta z zasilacza CP-PWR-CUBE-4.
Zasilanie PoE — dostarczane przez przełącznik do podłączonego telefonu za pośrednictwem kabla Ethernet.	Telefony IP Cisco 8851, 8851NR, 8861, 8865 i 8865NR obsługują funkcjonalność 8 PoE dla podłączanych akcesoriów. Więcej informacji zawiera arkusz danych telefonu. W celu zapewnienia niezakłóconego działania telefonu przełącznik musi mieć zapasowy zasilania Należy też sprawdzic, czy działająca w przełączniku wersja systemu operacyjnego Cisco IOS obsługuje wdrażane telefony. Informacje o wersji systemu operacyjnego można znaleźć w dokumentacji przełącznika.
Technologia Universal Power over Ethernet (UPoE)	Telefony IP Cisco 8865 i 8865NR obsługują technologię UPoE.

W poniższej tabeli przedstawiono dokumenty z dodatkowymi informacjami dotyczącymi następujących tematów:

- Przełączniki Cisco, które działają z telefonami IP Cisco
- Wersje systemu Cisco IOS obsługujące dwukierunkowe negocjowanie zasilania
- Inne wymagania i ograniczenia dotyczące zasilania

**Tabela 16: Informacje uzupełniające**

Tematy dokumentów	Adres URL
Rozwiązania PoE	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html">http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html</a>
UPoE	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe">http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe</a>

Tematy dokumentów	Adres URL
Przełączniki Cisco Catalyst	<a href="http://www.cisco.com/c/en/us/products/switches/index.html">http://www.cisco.com/c/en/us/products/switches/index.html</a>
Routery ze zintegrowanymi usługami	<a href="http://www.cisco.com/c/en/us/products/routers/index.html">http://www.cisco.com/c/en/us/products/routers/index.html</a>
Oprogramowanie Cisco IOS	<a href="http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html">http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html</a>

## Przerwa w zasilaniu

Dostęp do usług alarmowych za pomocą telefonu wymaga, aby miał on zasilanie. W przypadku przerwy w zasilaniu nawiązywanie połączeń telefonicznych i alarmowych nie będzie działać do chwili przywrócenia zasilania. W przypadku awarii lub przerwy w zasilaniu może okazać się konieczne ponowne uruchomienie bądź skonfigurowanie urządzenia w celu nawiązywania połączeń telefonicznych lub alarmowych.

## Oszczędności na zużyciu energii

Zużycie energii przez telefon IP Cisco można ograniczyć, włączając tryb Oszczędzanie energii lub EnergyWise (Oszczędzanie energii plus).

### Oszczędzanie energii

W trybie Oszczędzanie energii podświetlenie ekranu jest wyłączone, gdy telefon nie jest używany. Telefon pozostaje w trybie Oszczędzanie energii przez zaplanowany czas albo do momentu, gdy użytkownik podniesie słuchawkę lub naciśnie dowolny przycisk.

### Tryb Oszczędzanie energii plus (EnergyWise)

Telefon IP Cisco obsługuje tryb Cisco EnergyWise (Oszczędzanie energii plus). Jeśli w sieci znajduje się kontroler trybu EnergyWise, np. przełącznik Cisco z włączoną funkcją EnergyWise, można skonfigurować telefony w taki sposób, aby przechodziły w stan uśpienia (wyłączenia zasilania) i wybudzenia (włączenia zasilania) zgodnie z harmonogramem w celu dalszego ograniczenia zużycia energii.

Należy skonfigurować w każdym telefonie ustawienia włączania i wyłączania trybu EnergyWise. Po włączeniu trybu EnergyWise należy skonfigurować pory uśpienia i wybudzenia oraz inne parametry. Parametry te są wysyłane do telefonu w ramach pliku XML jego konfiguracji.

## Negocjowanie zasilania przez protokół LLDP

Ustawienie zasilania używanego przez telefon jest ustalane w wyniku negocjacji między telefonem i przełącznikiem. Telefon IP Cisco działa przy wielu ustawieniach zasilania, przy czym zużycie energii maleje wraz ze zmniejszeniem jej dostępności.

Po ponownym uruchomieniu telefonu przełącznik używa wybranego protokołu (CDP lub LLDP) do negocjowania zasilania. Przełącznik wybiera pierwszy protokół (zawierający wartość TLV, Threshold Limit Value) przesłany przez telefon. Jeśli administrator systemu wyłączył ten protokół w telefonie, telefon nie może zasilić żadnego urządzenia, ponieważ przełącznik nie odpowiada na żądania zasilania wysłane przy użyciu innego protokołu.

Firma Cisco zaleca, aby funkcja negocjowania zasilania była zawsze włączona (domyślnie) podczas łączenia się z przełącznikiem, który obsługuje negocjowanie zasilania.

Po wyłączeniu funkcji negocjowania zasilania przełącznik może wyłączyć zasilanie telefonu. Jeśli przełącznik nie obsługuje negocjowania zasilania, przed włączeniem zasilania urządzeń przy użyciu funkcji PoE należy wyłączyć funkcję negocjowania zasilania. Gdy funkcja negocjowania zasilania jest wyłączona, telefon może zasilać urządzenia do wartości maksymalnej dopuszczanej przez standard IEEE 802.3af-2003.

**Uwaga**

- Przy wyłączonej funkcji CDP i negocjowaniu zasilania telefon może dostarczać urządzeniom do 15,4 W mocy.

## Protokoły sieciowe

Telefony IP Cisco z serii 8800 są zgodne z wieloma standardami branżowymi i protokołami sieciowymi Cisco niezbędnymi do komunikacji głosowej. Poniższa tabela zawiera przegląd protokołów sieciowych obsługiwanych przez te telefony.

**Tabela 17: Protokoły sieciowe obsługiwane przez telefon IP Cisco z serii 8800**

Protokół sieciowy	Przeznaczenie	Uwagi o użyciu
Bluetooth	Bluetooth jest protokołem komunikacji w bezprzewodowej sieci osobistej (WPAN), który określa sposób komunikowania się urządzeń na bliskie odległości.	Telefony IP Cisco 8845, 8865 i 8851 obsługują protokół Bluetooth 4.1. Telefon IP Cisco 8861 obsługuje protokół Bluetooth 4.0. Telefony IP Cisco 8811, 8841, 8851NR i 8865NR nie obsługują funkcji Bluetooth.
Bootstrap Protocol (BootP)	Protokół BootP umożliwia urządzeniu sieciowemu, np. telefonowi IP Cisco, wykrywanie określonych informacji uruchomieniowych, np. jego adresu IP.	—
Cisco Audio Session Tunnel (CAST)	Protokół CAST umożliwia telefonom i skojarzonym z nim aplikacjom komunikowanie się ze zdalnymi telefonami IP bez konieczności wprowadzania zmian w elementach sygnalizacyjnych.	W telefonie IP Cisco protokół CAST służy za interfejs między aplikacją Cisco Unified Video Advantage (CUVA) a programem Cisco Unified Communications Manager, przy czym telefon pełni funkcję serwera proxy protokołu SIP.
Cisco Discovery Protocol (CDP)	CDP to protokół wykrywania urządzeń, który działa we wszystkich urządzeniach produkowanych przez firmę Cisco.  Korzystając z protokołu CDP, urządzenie może ogłaszać swoją obecność innym urządzeniom oraz odbierać informacje o innych urządzeniach znajdujących się w sieci.	W telefonie IP Cisco protokół CDP służy do przekazywania do przełącznika Cisco Catalyst takich informacji jak pomocniczy identyfikator VLAN ID, szczegóły zarządzania zasilaniem poprzez port sieciowy i dane konfiguracyjne QoS (Quality of Service).

Protokół sieciowy	Przeznaczenie	Uwagi o użyciu
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP jest protokołem opracowanym przez firmę Cisco, umożliwiającym tworzenie hierarchii urządzeń równorzędnych. Taka hierarchia służy do dystrybucji plików oprogramowania sprzętowego z urządzeń równorzędnych do urządzeń sąsiednich.	Protokół CPPDP jest używany przez funkcję Równy dostęp do oprogramowania sprzętowego.
Protokół DHCP (ang. Dynamic Host Configuration Protocol),	<p>Protokół DHCP dynamicznie przydziela i przypisuje adresy IP urządzeniom sieciowym.</p> <p>Dzięki niemu można podłączyć telefon IP do sieci i uruchomić bez konieczności ręcznego przypisywania mu adresu IP ani konfigurowania dodatkowych parametrów sieci.</p>	<p>Protokół DHCP jest domyślnie włączony. Po jego wyłączeniu trzeba ręcznie konfigurować adres IP, maskę podsieci, bramkę i serwer TFTP lokalnie w każdym telefonie.</p> <p>Zalecamy używanie w przypadku protokołu DHCP niestandardowej opcji 150. Dzięki temu można skonfigurować adres IP serwera TFTP jako wartość tej opcji. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p> <p><b>Uwaga</b> Jeśli nie można użyć opcji 150, spróbuj użyć opcji DHCP 66.</p>
Protokół HTTP (Hypertext Transfer Protocol)	HTTP to standardowy protokół do przesyłania informacji i dokumentów za pośrednictwem Internetu i sieci WWW.	W telefonach IP Cisco protokół HTTP służy do korzystania z usług XML oraz do rozwiązywania problemów.
Hypertext Transfer Protocol Secure (HTTPS)	Protokół HTTPS stanowi połączenie protokołu HTTP z protokołem SSL/TLS w celu zapewnienia szyfrowania i bezpiecznej identyfikacji serwerów.	Aplikacje internetowe z obsługą protokołów HTTP i HTTPS mają skonfigurowane dwa adresy URL. Telefony IP Cisco, które obsługują protokół HTTPS, wybierają w takiej sytuacji adres URL protokołu HTTPS.
IEEE 802.1X	<p>Standard IEEE 802.1X określa protokół kontroli dostępu i uwierzytelniania oparty na architekturze klient-serwer, który uniemożliwia nieupoważnionym klientom nawiązywanie połączenia z siecią LAN za pośrednictwem dostępnych publicznie portów.</p> <p>Dopóki nie nastąpi uwierzytelnienie klienta, mechanizmy kontroli dostępu 802.1X dopuszczają komunikację w ramach protokołu EAPOL (ang. Extensible Authentication Protocol over LAN, rozszerzalny protokół uwierzytelniania poprzez sieć LAN) tylko za pośrednictwem portu, do którego jest podłączony klient. Po udanym uwierzytelnieniu poprzez ten port może się odbywać zwykła komunikacja.</p>	<p>Wdrożenie standardu IEEE 802.1X w telefonie IP Cisco obejmuje obsługę następujących metod uwierzytelniania: EAP-FAST i EAP-TLS.</p> <p>Po włączeniu w telefonie uwierzytelniania 802.1X należy wyłączyć port komputera i VLAN głosowy.</p>

Protokół sieciowy	Przeznaczenie	Uwagi o użyciu
IEEE 802.11n/802.11ac	Standard IEEE 802.11 określa sposób komunikowania się urządzeń przy użyciu bezprzewodowej sieci lokalnej (WLAN).  Protokół 802.11n działa w paśmie częstotliwości 5 GHz i 2,4 GHz, zaś 802.11ac działa w paśmie częstotliwości 5 GHz.	Interfejs 802.11 jest opcją wdrażania w przypadku, gdy kabel Ethernet jest niedostępny lub niepożądany.  Tylko telefony IP Cisco 8861 i 8865 obsługują sieć WLAN.
IP	IP to protokół komunikacyjny, który służy do adresowania i wysyłania pakietów w sieci.	Aby urządzenia sieciowe mogły się komunikować przy użyciu protokołu IP, należy im przypisać adres IP, podsieć i bramę.  Adresy IP, podsieci i brama są przypisywane automatycznie w przypadku korzystania z telefonu IP Cisco z obsługą protokołu DHCP (Dynamic Host Configuration Protocol, protokół dynamicznego konfigurowania hosta). Jeśli protokół DHCP nie jest używany, trzeba ręcznie przypisywać wspomniane parametry lokalnie każdemu telefonowi.  Telefony IP Cisco obsługują adresy protokołu IPv6. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.
Link Layer Discovery Protocol (LLDP)	LLDP to ustandaryzowany protokół wykrywania sieci (podobny do CDP), który jest obsługiwany przez niektóre urządzenia marki Cisco i innych firm.	Telefon IP Cisco obsługuje protokół LLDP poprzez port komputera.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED to rozszerzenie standardu LLDP opracowane z myślą o produktach do komunikacji głosowej.	Telefon IP Cisco obsługuje rozszerzenie LLDP-MED poprzez port oprogramowania, umożliwiając przesyłanie informacji o następujących elementach: <ul style="list-style-type: none"> <li>• konfiguracja VLAN głosowego,</li> <li>• wykrywanie urządzeń,</li> <li>• zarządzanie zasilaniem,</li> <li>• zarządzanie zapasami.</li> </ul>
Real-Time Transport Protocol (RTP)	RTP to standardowy protokół do przesyłania danych w czasie rzeczywistym, np. na potrzeby interaktywnej komunikacji głosowej, za pośrednictwem sieci transmisji danych.	W telefonach IP Cisco protokół RTP służy do wysyłania i odbierania danych komunikacji głosowej w czasie rzeczywistym do i z innych telefonów bądź bramek.
Real-Time Control Protocol (RTCP)	Protokół RTCP działa w powiązaniu z protokołem RTP, aby dostarczać w strumieniach RTP dane o jakości usług (np. o jitterze, opóźnieniu i czasie błędzenia).	Protokół RTCP jest domyślnie włączony.

Protokół sieciowy	Przeznaczenie	Uwagi o użyciu
Protokół SDP (Session Description Protocol)	SDP jest częścią protokołu SIP, która określa parametry dostępne w trakcie połączenia między dwoma punktami końcowymi. Konferencje są tworzone przy użyciu tylko tych funkcji protokołu SDP, które są obsługiwane przez wszystkie punkty końcowe biorące udział w konferencji.	Funkcje protokołu SDP, takie jak typy kodeków, wykrywanie DTMF, wprowadzany szum, są zwykle konfigurowane globalnie w programie Cisco Unified Communications Manager lub przez działające bramy multimedialne. Niektóre punkty końcowe SIP mogą umożliwiać konfigurację tych parametrów w danym punkcie końcowym.
Session Initiation Protocol (SIP)	SIP to opracowany przez stowarzyszenie Internet Engineering Task Force (IETF, Internetowa Grupa Robocza ds. Technicznych) standard dotyczący obsługi konferencji multimedialnych za pośrednictwem protokołu IP. SIP to oparty na kodzie ASCII protokół kontrolny warstwy aplikacji (zdefiniowany w dokumencie RFC 3261), który służy do nawiązywania, utrzymywania i przerywania połączeń między co najmniej dwoma punktami końcowymi.	Podobnie jak w przypadku protokołów VoIP standard SIP ma na celu obsługę sygnalizacji i zarządzanie sesjami w sieciach telefonii pakietowej. Sygnalizacja umożliwia przekazywanie informacji o połączeniu przez granice sieci. Zarządzanie sesjami zapewnia z kolei sterowanie atrybutami kompleksowego połączenia.  Telefony IP Cisco obsługują protokół SIP w trybach tylko IPv6, tylko IPv4 oraz IPv4 i IPv6.
TCP	TCP to protokół komunikacyjny dla potrzeb połączeń.	W telefonach IP Cisco protokół TCP służy do komunikacji z programem Cisco Unified Communications Manager i do uzyskiwania dostępu do usług XML.
Transport Layer Security (TLS)	TLS to standardowy protokół do zabezpieczania i uwierzytelniania komunikacji.	W przypadku stosowania zabezpieczeń protokół TLS służy w telefonach IP Cisco do ich bezpiecznego rejestrowania w programie Cisco Unified Communications Manager.
Protokół TFTP (ang. Trivial File Transfer Protocol),	Protokół TFTP służy do przesyłania plików za pośrednictwem sieci.  W telefonie IP Cisco protokół TFTP umożliwia pobieranie pliku konfiguracyjnego przeznaczonego do konkretnego modelu telefonu.	Protokół TFTP wymaga obecności w sieci serwera TFTP, który może być automatycznie zidentyfikowany przez serwer DHCP. Jeśli telefon ma korzystać z innego serwera TFTP niż wskazany przez serwer DHCP, należy ręcznie przypisać adres IP serwera TFTP w menu Konfiguracja sieci w telefonie.  Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.
UDP (ang. User Datagram Protocol)	UDP to bezpołączeniowy protokół komunikacyjny, który służy do dostarczania pakietów danych.	Protokół UDP jest używany tylko w strumieniach RTP. Sygnalizacja SIP w telefonach nie obsługuje protokołu UDP.

Aby uzyskać więcej informacji na temat obsługi protokołu LLDP-MED, zobacz oficjalny dokument dotyczący protokołów LLDP-MED i Cisco Discovery Protocol:

[http://www.cisco.com/en/US/tech/tk652/tk701/technologies\\_white\\_paper0900aecd804cd46d.shtml](http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml)

**Tematy pokrewne**

[Uwierzytelnianie 802.1X](#), na stronie 115

[Konfigurowanie ustawień sieciowych](#)

[Sprawdzenie przy uruchamianiu telefonu](#), na stronie 66

[Interakcja z sieciami VLAN](#), na stronie 22

[Interakcja z programem Cisco Unified Communications Manager](#), na stronie 22

[Interakcja z programem Cisco Unified Communications Manager Express](#), na stronie 23

[Konfigurowanie zakresu portów audio i wideo](#), na stronie 197

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Interakcja z sieciami VLAN

Telefon IP Cisco ma wbudowany przełącznik Ethernet, który może przekazywać pakiety do telefonu, do portu komputera i do portu sieci z tyłu urządzenia.

Jeśli do portu komputera jest podłączony komputer, komputer i telefon korzystają z tego samego łącza fizycznego do przełącznika oraz tego samego portu przełącznika. Współużytkowanie łącza fizycznego ma następujące konsekwencje dla konfiguracji sieci VLAN:

- Bieżące sieci VLAN mogą być skonfigurowane na bazie podsieci IP. Jednak z powodu braku dodatkowych adresów IP może być niemożliwe przypisanie telefonu do podsieci, do której należą inne urządzenia podłączone do tego samego portu.
- Przesyłanie danych w sieci VLAN obsługującej telefony może obniżyć jakość połączeń VoIP.
- Ze względu na bezpieczeństwo może być konieczne oddzielenie połączeń głosowych od transmisji danych.

Te problemy można rozwiązać przez izolowanie połączeń głosowych w oddzielnej sieci VLAN. W tym celu port przełącznika, do którego jest podłączony telefon, powinien mieć skonfigurowane oddzielne sieci VLAN do przesyłania:

- Ruchu głosowego do/z telefonu IP (na przykład pomocnicza sieć VLAN w przełącznikach z serii Cisco Catalyst 6000)
- Transmisji danych do/z komputera podłączonego do przełącznika za pośrednictwem portu komputera w telefonie IP (macierzysta sieć VLAN)

Odizolowanie telefonów w oddzielnej pomocniczej sieci VLAN podnosi jakość ruchu głosowego i umożliwia dodanie większej liczby telefonów do istniejącej sieci, w której brakuje adresów IP dla wszystkich telefonów.

Więcej informacji można znaleźć w dokumentacji dołączonej do przełącznika Cisco. Informacje o przełącznikach są dostępne również pod tym adresem URL:

<http://cisco.com/en/US/products/hw/switches/index.html>

## Interakcja z programem Cisco Unified Communications Manager

Cisco Unified Communications Manager to otwarty system przetwarzania połączeń zgodny ze standardami branżowymi. Program Cisco Unified Communications Manager zestawia i przerywa połączenia między



telefonami, integrując funkcje tradycyjnej centrali PBX z korporacyjną siecią IP. Program Cisco Unified Communications Manager zarządza składnikami systemu telefonii, np. telefonami czy bramkami dostępowymi, oraz zasobami niezbędnymi do działania takich funkcji jak połączenia konferencyjne i planowanie tras. Program Cisco Unified Communications Manager zapewnia również:

- Przesyłanie oprogramowania sprzętowego do telefonów
- Dostarczanie plików CTL (ang. Certificate Trust List, lista zaufanych certyfikatów) i ITL (ang. Identity Trust List, lista zaufanych tożsamości) za pośrednictwem usług TFTP i HTTP
- Rejestrowanie telefonów
- Zachowywanie połączeń, dzięki któremu sesja mediów jest kontynuowana mimo utraty sygnalizacji między podstawowym serwerem Communications Manager a telefonem

Więcej informacji o konfigurowaniu programu Cisco Unified Communications Manager pod kątem współpracy z telefonami opisanymi w tym rozdziale można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

**Uwaga**

Jeśli model telefonu do skonfigurowania nie występuje na liście rozwijanej Phone Type (Typ telefonu) w aplikacji Cisco Unified Communications Manager — administracja, należy zainstalować najnowszy pakiet urządzenia do posiadanej wersji programu Cisco Unified Communications Manager, pobrany z witryny Cisco.com.

**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Interakcja z programem Cisco Unified Communications Manager Express

Gdy telefon współpracuje z programem Cisco Unified Communications Manager Express (Unified CME), musi przejść w tryb CME.

Kiedy użytkownik wywołuje funkcję konferencji, tag umożliwia telefonowi korzystanie z lokalnego lub sieciowego sprzętowego mostka konferencyjnego.

Telefony nie obsługują następujących działań:

- Przekierowywanie — obsługiwane tylko w przypadku scenariusza przekazywania trwającego połączenia.
- Konferencja — obsługiwane tylko w przypadku scenariusza przekazywania trwającego połączenia.
- Dołączanie — obsługiwane za pomocą przycisku Konferencja lub w ramach dostępu do usługi Hookflash.
- Zawieszanie — obsługiwane za pomocą przycisku Zawieś.
- Wtrącanie i scalanie — nieobsługiwane.
- Przekazywanie bezpośrednie — nieobsługiwane.
- Wybieranie — nieobsługiwane.

Użytkownicy nie mogą tworzyć połączeń konferencyjnych ani przekazywanych, które obejmują różne linie.

Program Unified CME obsługuje połączenia interkodemem, nazywane także funkcją whisper paging. Jednak przywoływanie jest odrzucane przez telefon podczas połączenia.

W trybie CME obsługiwane są tryb linii sesji i tryb rozszerzony linii.

## Interakcje z systemem wiadomości głosowych

Program Cisco Unified Communications Manager umożliwia integrację z różnymi systemami wiadomości głosowych, w tym z systemem wiadomości głosowych Cisco Unity Connection. Ponieważ można dokonać integracji z różnymi systemami, należy podać użytkownikom informacje dotyczące używania konkretnego systemu.

Aby umożliwić użytkownikowi przekierowywanie połączeń do poczty głosowej, skonfiguruj wzorzec wybierania \*xxxxx i skonfiguruj go jako przekierowanie wszystkich połączeń do poczty głosowej. Więcej wiadomości na ten temat można znaleźć w dokumentacji programu Cisco Unified Communications Manager.

Każdemu użytkownikowi należy podać następujące informacje:

- Jak uzyskać dostęp do konta systemu wiadomości głosowych

Należy się upewnić, że do konfigurowania przycisku Wiadomości na telefonie IP Cisco został użyty program Cisco Unified Communications Manager.

- Początkowe hasło umożliwiające dostęp do systemu wiadomości głosowych.

Skonfiguruj domyślne hasło systemu wiadomości głosowych dla wszystkich użytkowników.

- W jaki sposób telefon wskazuje, że są oczekujące wiadomości głosowe.

W celu skonfigurowania metody wskaźnika wiadomości oczekującej (MWI, message waiting indicator) należy użyć programu Cisco Unified Communications Manager.

## Omówienie uruchamiania telefonu

Podczas nawiązywania połączenia z siecią VoIP telefony IP Cisco przechodzą przez standardowy proces uruchamiania. W zależności od konfiguracji konkretnej sieci, tylko niektóre z następujących czynności mogą mieć zastosowanie w używanym telefonie Cisco IP.

1. Pobieraj zasilanie z przełącznika. Jeśli telefon nie używa zewnętrznego źródła zasilania, przełącznik zapewnia wewnętrzne zasilanie za pośrednictwem kabla Ethernet, który jest podłączony do telefonu.
2. (Tylko w przypadku telefonu IP Cisco 8861 i 8865 w bezprzewodowej sieci LAN) Wyszukiwanie punktu dostępu. Telefon IP Cisco 8861 i 8865 wyszukuje sygnał radiowy w dostępnym obszarze. Telefon wyszukuje profile sieci i punkty dostępu zawierające odpowiednie identyfikatory SSID i typ uwierzytelniania. Następuje powiązanie telefonu z punktem dostępu o zgodnym profilu, dla którego wartość RSSI jest największa.
3. (Tylko w przypadku telefonu IP Cisco 8861 i 8865 w bezprzewodowej sieci LAN) Uwierzytelnianie w punkcie dostępu. Telefon IP Cisco rozpoczyna proces uwierzytelniania. W poniższej tabeli opisano proces uwierzytelniania:

Typ uwierzytelniania	Główne opcje zarządzania	Opis
Otwórz	Brak	W punkcie dostępu można uwierzytelnić każde urządzenie. W celu zwiększenia bezpieczeństwa opcjonalnie można użyć statycznego szyfrowania WEP.
Shared Key	Brak	Telefon szyfruje tekst wyzwania przy użyciu klucza WEP, a przed udzieleniem dostępu do sieci w punkcie dostępu należy sprawdzić poprawność klucza użytego do szyfrowania tekstu wyzwania.
PEAP lub EAP-FAST	Brak	Serwer RADIUS uwierzytelnia nazwę użytkownika i hasło przed udzieleniem dostępu do sieci.

4. Załaduj przechowywany obraz telefonu. Podczas uruchamiania telefonu jest aktywowany program ładowania początkowego, który ładuje obraz oprogramowania sprzętowego telefonu przechowywany w pamięci flash. Korzystając z tego obrazu, telefon inicjuje oprogramowanie i sprzęt.
5. Skonfiguruj sieć VLAN. Po podłączeniu telefonu IP Cisco do przełącznika Cisco Catalyst przełącznik informuje telefon o głosowej sieci VLAN zdefiniowanej w przełączniku. Przed wysłaniem żądania adresu IP do usługi DHCP (Dynamic Host Configuration Protocol) telefon musi otrzymać informacje o członkostwie sieci VLAN.
6. Uzyskaj adres IP Telefon IP Cisco, który używa protokołu DHCP, może odpytać serwer DHCP w celu uzyskania adresu IP. Jeśli protokół DHCP nie jest używany w sieci, należy każdemu telefonowi przypisać lokalnie statyczny adres IP.
7. Załadaj pliku CTL. Plik CTL jest przechowywany na serwerze TFTP. Plik ten zawiera certyfikaty, które są niezbędne do nawiązywania zabezpieczonego połączenia między telefonem i programem Cisco Unified Communications Manager.  
Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.
8. Załadaj pliku ITL. Telefon żąda najpierw pliku CTL, a dopiero później pliku ITL. Plik ITL zawiera certyfikaty jednostek, którym telefon może zaufać. Certyfikaty są używane do uwierzytelniania bezpiecznych połączeń z serwerami lub do uwierzytelniania podpisu cyfrowego podpisanego przez serwery. Program Cisco Unified Communications Manager w wersji 8.5 lub nowszej obsługuje plik ITL.
9. Uzyskaj dostęp do serwera TFTP. Oprócz przypisywania adresu IP serwer DHCP kieruje telefon IP Cisco do serwera TFTP. Jeśli telefon ma statycznie zdefiniowany adres IP, należy skonfigurować serwer TFTP lokalnie w telefonie; dopiero wtedy telefon skontaktuje się bezpośrednio z serwerem TFTP.



**Uwaga** Można także przypisać alternatywny serwer TFTP, używany zamiast serwera przypisanego przez usługę DHCP.

10. Załadaj pliku konfiguracyjnego. Na serwerze TFTP znajdują się pliki konfiguracyjne, które zawierają parametry połączenia z programem Cisco Unified Communications Manager i inne informacje o telefonie.
11. Nawiąż połączenie z programem Cisco Unified Communications Manager. Plik konfiguracyjny określa sposób komunikowania się telefonu IP Cisco z programem Cisco Unified Communications Manager i udostępnia telefonowi identyfikator pobieranych danych. Po otrzymaniu pliku z serwera TFTP telefon próbuje nawiązać połączenie z programem Cisco Unified Communications Manager o najwyższym priorytecie na liście.

Jeśli profil zabezpieczeń telefonu jest skonfigurowany pod kątem bezpiecznej sygnalizacji (szyfrowanie lub uwierzytelnianie) i program Cisco Unified Communications Manager pracuje w trybie zabezpieczonym, wówczas telefon nawiązuje połączenie TLS. W przeciwnym razie telefon nawiązuje niezabezpieczone połączenie TCP.

Jeśli telefon został ręcznie dodany do bazy danych, program Cisco Unified Communications Manager identyfikuje telefon. Jeśli telefonu nie dodano ręcznie do bazy danych i w programie Cisco Unified Communications Manager jest włączona automatyczna rejestracja, wówczas telefon próbuje zarejestrować się w bazie danych programu Cisco Unified Communications Manager.




---

**Uwaga** Automatyczna rejestracja zostaje wyłączona po skonfigurowaniu klienta CTL. W takim przypadku należy ręcznie dodać telefon do bazy danych programu Cisco Unified Communications Manager.

---

#### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Urządzenia zewnętrzne

Zalecamy stosowanie urządzeń zewnętrznych dobrej jakości, ekranowanych przed niepożądanymi sygnałami o częstotliwościach radiowych (RF) i akustycznych (AF). Do urządzeń zewnętrznych należą zestawy słuchawkowe, kable i złącza.

Zależnie od jakości tych urządzeń i ich odległości od innych urządzeń, np. telefonów komórkowych lub krótkofalówek, mogą występować pewne zakłócenia. W takich przypadkach zalecamy podjęcie co najmniej jednego z następujących działań:

- Oddal zewnętrzne urządzenie od źródeł sygnałów RF lub AF.
- Poprowadź przewody zewnętrznego urządzenia z dala od źródeł sygnałów RF lub AF.
- Do podłączenia urządzenia zewnętrznego zastosuj przewody ekranowane lub przewody z lepszym ekranem i złączem.
- Zastosuj krótszy przewód do podłączenia urządzenia zewnętrznego.
- Zastosuj ferryty lub podobne urządzenia na przewodach urządzenia zewnętrznego.

Firma Cisco nie udziela gwarancji na jakość działania urządzeń zewnętrznych, kabli ani złączy.

**Przeostoga**

W krajach Unii Europejskiej stosuj jedynie takie zewnętrzne głośniki, mikrofony i zestawy słuchawkowe, które w pełni odpowiadają Dyrektywie EMC [89/336/EC].

## Informacje o porcie USB

Telefony IP Cisco 8851, 8851NR, 8861, 8865 i 8865NR obsługują maksymalnie 5 urządzeń podłączonych do każdego portu USB. Każde urządzenie podłączane do telefonu jest wliczane do maksymalnej liczby urządzeń. Przykład: telefon może obsługiwać 5 urządzeń USB podłączonych do portu bocznego i 5 kolejnych standardowych urządzeń USB podłączonych do portu tylnego. Wiele produktów USB innych firm należy liczyć jako kilka urządzeń USB, na przykład urządzenie zawierające koncentrator USB i zestaw słuchawkowy należy liczyć jako dwa urządzenia USB. Więcej informacji zawiera dokumentacja danego urządzenia USB.

**Uwaga**

- Koncentratyory niezasilane nie są obsługiwane, podobnie jak koncentratyory zasilane z więcej niż czterema portami.
- Zestawy słuchawkowe USB łączące się z telefonem za pośrednictwem koncentratora USB nie są obsługiwane.

Każdy moduł rozszerzenia klawiatury podłączony do telefonu liczy się jako jedno urządzenie USB. Podłączone do telefonu trzy moduły rozszerzenia klawiatury są liczone jako trzy urządzenia USB.

## Pliki konfiguracyjne telefonu

Pliki konfiguracyjne telefonu znajdują się na serwerze TFTP i definiują parametry połączenia z programem Cisco Unified Communications Manager. Ogólnie rzecz biorąc, każda zmiana wprowadzona w programie Cisco Unified Communications Manager, która wymaga zresetowania telefonu, automatycznie wprowadza zmiany w pliku konfiguracyjnym telefonu.

Pliki konfiguracyjne zawierają również informacje o obrazie załadowanym w telefonie, który powinien zostać uruchomiony. Jeśli ten załadowany obraz różni się od obrazu aktualnie załadowanego w telefonie, telefon kontaktuje się z serwerem TFTP w celu żądania plików do załadowania

Po skonfigurowaniu ustawień związanych z bezpieczeństwem w programie Cisco Unified Communications Manager — administracja plik konfiguracyjny telefonu będzie zawierać poufne informacje. W celu zapewnienia prywatności pliku konfiguracyjnego należy włączyć dla niego opcję szyfrowania danych. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager. Telefon żąda pliku konfiguracyjnego przy każdym resecie i rejestracji w programie Cisco Unified Communications Manager.

Telefon uzyskuje dostęp do domyślnego pliku konfiguracji o nazwie XmlDefault.cnf.xml na serwerze TFTP, gdy są spełnione następujące warunki:

- Jest włączona funkcja automatycznej rejestracji w programie Cisco Unified Communications Manager
- Telefon nie został dodany do bazy danych programu Cisco Unified Communications Manager

- Telefon jest rejestrowany po raz pierwszy

#### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Działanie telefonu w okresach dużego obciążenia sieci

Wszystkie czynniki powodujące zmniejszenie wydajności sieci mogą wpływać na jakość dźwięku i obrazu w połączeniach nawiązywanych za pomocą telefonu, a w niektórych przypadkach mogą nawet powodować zerwanie połączenia. Do źródeł pogorszenia przepustowości sieci należą m.in.:

- zadania administracyjne, np. skanowanie portów wewnętrznych czy skanowanie zabezpieczeń.
- Ataki, które mają miejsce w twojej sieci, takie jak atak typu odmowa usługi (Denial of Service).

## Działanie telefonu w sieci z dwoma routerami sieciowymi

Telefon IP Cisco z serii 8800 używa zapory w celu zapewnienia ochrony przed włamaniami, np. przed atakami typu man-in-the-middle. Tej zapory nie można wyłączyć. Można jednak zatrzymać ruch w telefonie, konfigurując sieć z dwoma routerami sieciowymi w tej samej podsieci z przekierowywaniem adresów IP.

Zapora telefonu zatrzymuje ruch, ponieważ taka konfiguracja sieci przypomina atak man-in-the-middle. Telefon odbiera pakiety przekierowane do innych docelowych adresów IP znajdujących się w podsieci innej niż telefon. Telefon znajduje się w sieci z więcej niż jednym routerem, zaś router domyślny wysyła ruch do drugiego routera.

Jeśli podejrzewasz, że ruch jest wstrzymywany przez zaporę, przejrzyj dzienniki telefonu. Sprawdź, czy podczas próby nawiązania połączenia występuje błąd o kodzie 1 pochodzący z systemu operacyjnego. Jedną z cech charakterystycznych jest komunikat

```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

Sieć złożona z dwóch routerów sieciowych znajdujących się w tej samej podsieci i przekierowująca adresy IP nie jest typową konfiguracją. Jeśli jednak taka konfiguracja sieci jest używana, należy rozważyć wykorzystanie tylko jednego routera w podsieci. Jeśli wymagane są dwa routery sieciowe w podsieci, należy wyłączyć przekierowywanie IP na routerze i ponownie uruchomić telefon.

## Interfejs programowania aplikacji

Firma Cisco obsługuje korzystanie z interfejsu API telefonu przez aplikacje innych firm, które zostały przetestowane i certyfikowane przez firmę Cisco i twórcę aplikacji innej firmy. Wszelkie problemy z telefonami związane z interakcją z niecertyfikowaną aplikacją muszą być rozwiązywane przez stronę trzecią i nie będą rozwiązywane przez Cisco.

Szczegółowe informacje na temat modelu wsparcia certyfikowanych przez Cisco aplikacji/rozwiązań innych firm można znaleźć w witrynie [Cisco Solution Partner Program](#).



## ROZDZIAŁ 3

# Telefon IP Cisco — sprzęt

- Omówienie telefonu, na stronie 29
- Cisco IP Phone 8811, na stronie 31
- Telefony IP Cisco 8841 i 8845, na stronie 32
- Telefony IP Cisco 8851 i 8851NR, na stronie 33
- Telefony IP Cisco 8861, 8865 i 8865NR, na stronie 35
- Przyciski i podzespoły, na stronie 36
- Ochrona kamery w telefonie, na stronie 39

## Omówienie telefonu

Telefony IP Cisco z serii 8800 umożliwiają komunikację głosową za pośrednictwem sieci IP (ang. Internet Protocol, protokół internetowy). Telefon IP Cisco działa bardzo podobnie do dowolnego cyfrowego telefonu biurowego, umożliwiając nawiązywanie i odbieranie połączeń telefonicznych oraz dostęp do różnych funkcji, m.in. wyciszania, zawieszania i przekierowywania. Ponadto telefon ten łączy się z siecią transmisji danych, więc udostępnia rozszerzone funkcje telefonii IP, m.in. dostęp do informacji o sieci i usług sieciowych oraz do funkcji i usług możliwych do dostosowania.

Telefon IP Cisco 8811 jest wyposażony w wyświetlacz LCD o skali szarości. Telefony IP Cisco 8841, 8845, 8851, 8851NR, 8861, 8865 i 8865NR są wyposażone w wyświetlacz LCD o 24-bitowej skali kolorów.

Podczas dodawania funkcji do klawiszy linii telefonicznej ograniczeniem jest liczba dostępnych klawiszy linii. Nie można dodać więcej funkcji niż liczba klawiszy linii na telefonie.

Telefony IP Cisco cechują się następującymi właściwościami:

- Klawisze programowalne funkcji, które obsługują do 5 linii w trybie linii sesji lub do 10 linii w trybie rozszerzonym linii
- Pełny zestaw funkcji wideo (tylko telefony IP Cisco 8845, 8865 i 8865NR)
- Łączność z gigabitową siecią Ethernet
- Obsługa bezprzewodowych zestawów słuchawkowych przez Bluetooth (Tylko telefony Cisco IP Phone 8845, 8851, 8861 i 8865. Ta funkcja nie jest obsługiwana w telefonach IP Cisco 8811, 8841, 8851NR i 8865NR).
- Obsługa mikrofonu zewnętrznego i głośników (tylko telefony IP Cisco 8861, 8865 i 8865NR)

- Połączenie sieciowe przez Wi-Fi (Tylko telefony IP Cisco 8861 i 8865. Łączność Wi-Fi nie jest obsługiwana w telefonie IP Cisco 8865NR).
- Porty USB:
  - Jeden port USB w przypadku telefonów IP Cisco 8851 i 8851NR
  - Dwa porty USB w przypadku telefonów IP Cisco 8861, 8865 i 8865NR

Telefony IP Cisco 8845, 8865 i 8865NR obsługują połączenia wideo przy użyciu wbudowanej kamery. Ta funkcja pozwala na wspólną pracę ze znajomymi i współpracownikami lub na przeprowadzanie osobistych spotkań przez telefon.



**Uwaga** Należy zachować pudełko i opakowanie dla telefonów IP Cisco 8845, 8865 i 8865NR. Kamery znajdujące się w tych telefonach są delikatne. Jeśli telefon będzie przenoszony, sugerujemy, aby spakować go w oryginalne opakowanie w celu ochrony kamery. Aby uzyskać więcej informacji, patrz [Ochrona kamery w telefonie, na stronie 39](#).

Połączenie wideo obejmuje następujące funkcje:

- PIP (funkcja obrazu w obrazie) — można wybrać jedną z czterech lokalizacji: strona prawa/dół, strona prawa/góra, strona lewa/góra lub strona lewa/dół. Można także całkiem wyłączyć funkcję PIP.
- Funkcja Zamień — służy do przełączania widoków w podglądzie PIP. Gdy wyłączona jest funkcja PIP, klawisz programowy Zamień jest również wyłączony.
- Obraz wideo własnego widoku — wybierz opcję obrazu wideo własnego widoku, aby na wideo widzieć obraz samego siebie.
- UI obrazu wideo i rozpoczęcie konferencji/przekazywania — wybierz, aby rozpocząć konferencję.

Aby uzyskać dodatkowe informacje na temat połączeń wideo, zobacz temat *Podręcznik użytkownika programu Cisco Unified Communications Manager dla telefonów IP Cisco z serii 8800* oraz dokumentację używanej wersji programu Cisco Unified Communications Manager.

Podobnie jak inne urządzenia sieciowe, telefon IP Cisco wymaga konfigurowania i zarządzania. W omawianych telefonach sygnał jest kodowany i odkodowywany przy użyciu następujących kodeków:

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus
- iSAC



**Przeostoga**

Korzystanie w pobliżu telefonu IP Cisco z telefonu komórkowego lub krótkofalówki może powodować zakłócenia. Więcej wiadomości na ten temat można znaleźć w dokumentacji udostępnianej przez producenta zakłócającego urządzenia.

Telefon IP Cisco udostępnia tradycyjne funkcje telefoniczne, np. przekierowywanie i Przekierowanie połączeń, ponowne wybieranie, szybkie wybieranie, połączenia konferencyjne i dostęp do systemu poczty głosowej. Telefony IP Cisco mają też cały szereg innych funkcji.

Podobnie jak w przypadku innych urządzeń sieciowych telefony IP Cisco trzeba najpierw skonfigurować, aby przygotować je do dostępu do programu Cisco Unified Communications Manager i reszty sieci IP. Korzystanie z protokołu DHCP znacznie zmniejsza liczbę ustawień do skonfigurowania w telefonie. Jeśli jednak sieć tego wymaga, można ręcznie skonfigurować takie parametry jak adres IP, serwer TFTP i informacje o podsieci.

Telefony IP Cisco mogą współpracować z innymi usługami i urządzeniami w sieci IP, dzięki którym zwiększają swoją funkcjonalność. Program Cisco Unified Communications Manager można np. zintegrować z katalogiem LDAP3 (ang. Lightweight Directory Access Protocol 3, lekki protokół dostępu do usług katalogowych), aby umożliwić użytkownikom wyszukiwanie danych kontaktowych współpracowników bezpośrednio za pomocą telefonów IP. Można też, korzystając z języka XML, umożliwić użytkownikom dostęp do rozmaitych informacji, np. prognoz pogody, notowań giełdowych, cytatów dnia i innych wiadomości pochodzących z sieci WWW.

Telefon IP Cisco jest urządzeniem sieciowym, można więc wprost z niego otrzymywać szczegółowe informacje o jego stanie. Mogą one być pomocne przy rozwiązywaniu wszelkich problemów, na jakie mogą natrafić użytkownicy podczas korzystania z telefonów IP. Można również zapoznać się ze statystykami aktywnych połączeń lub wersją oprogramowania sprzętowego w telefonie.

Aby działać w sieci telefonii IP, telefon IP Cisco musi się połączyć z urządzeniem sieciowym, np. przełącznikiem Cisco Catalyst. Przed rozpoczęciem nawiązywania i odbierania połączeń za pomocą telefonu IP Cisco trzeba go ponadto zarejestrować w systemie Cisco Unified Communications Manager.

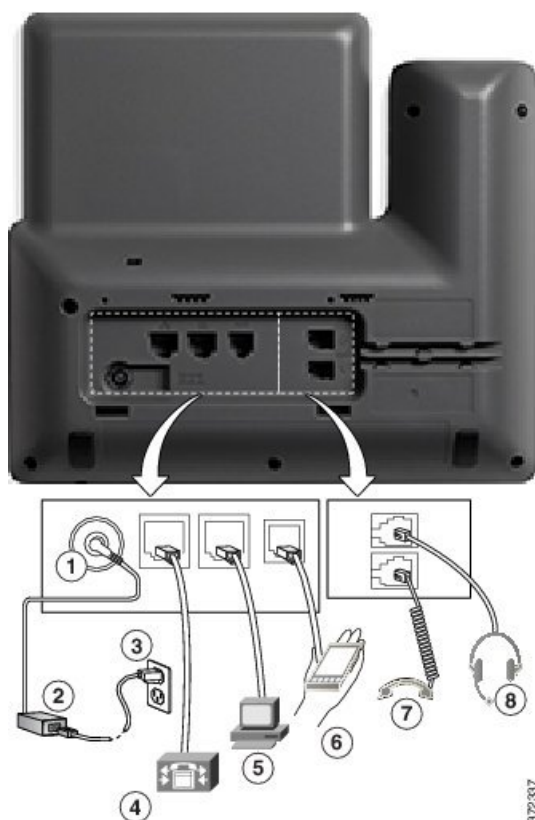
**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Cisco IP Phone 8811

W poniższej sekcji opisano cechy telefonu Cisco IP Phone 8811.

Podłącz swój telefon do sieci telefonii IP w swojej organizacji w sposób przedstawiony na poniższej ilustracji.



1	Port prądu stałego (48 V).	5	Złącze portu dostępu (10/100/1000 PC).
2	Zasilacz sieciowy (opcjonalny).	6	Port pomocniczy.
3	Wtyczka do gniazdka sieci elektrycznej (opcjonalna).	7	Złącze słuchawki.
4	Złącze portu sieci (10/100/1000 SW). Dostosowanie do zasilania IEEE 802.3at.	8	Złącze słuchawek analogowych (opcjonalne).



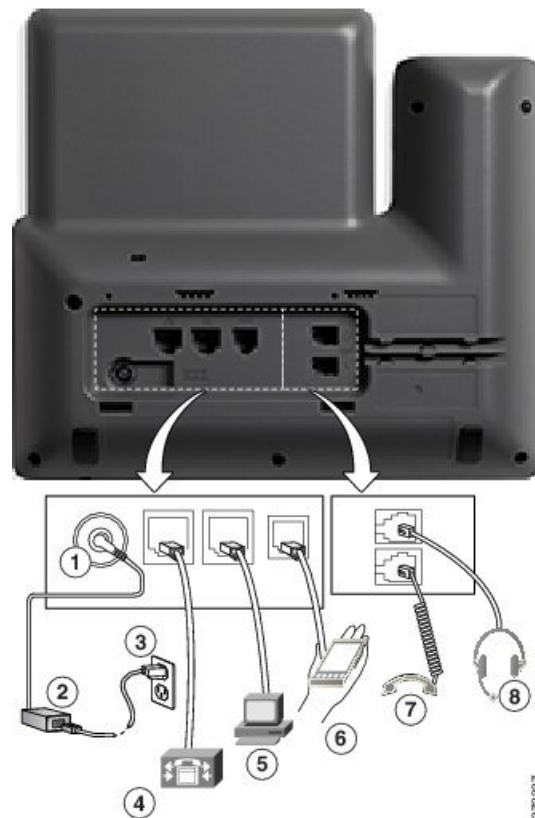
**Uwaga** Cisco IP Phone 8811 nie obsługuje modułów rozszerzenia klawiatury.

## Telefony IP Cisco 8841 i 8845

W poniższej sekcji opisano atrybuty telefonów IP Cisco 8841 i 8845.

### Złącza telefonu

Podłącz swój telefon do firmowej sieci telefonii IP, posługując się poniższym rysunkiem.



1	Gniazdo zasilacza prądu stałego (DC48V).	5	Złącze portu dostępu (10/100/1000 PC).
2	Zasilacz sieciowy (opcjonalny).	6	Port pomocniczy.
3	Wtyczka do gniazdka sieci elektrycznej (opcjonalna).	7	Złącze słuchawki.
4	Złącze portu sieci (10/100/1000 SW). Dostosowanie do zasilania IEEE 802.3at.	8	Złącze słuchawek analogowych (opcjonalne).



**Uwaga** Telefony IP Cisco 8841 i 8845 nie obsługują modułów rozszerzenia klawiatury.

## Telefony IP Cisco 8851 i 8851NR

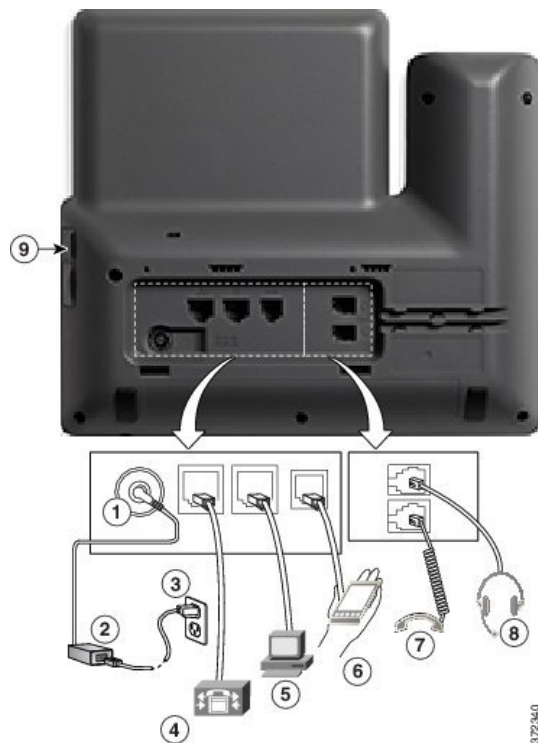
W poniższej sekcji opisano cechy telefonów IP Cisco 8851 i 8851NR.



**Uwaga** Telefon IP Cisco 8851NR nie obsługuje komunikacji Bluetooth. Poza tym telefony IP Cisco 8851 i Cisco 8851NR obsługują te same funkcje.

## – połączenia telefoniczne

Podłącz swój telefon do firmowej sieci telefonii IP, posługując się poniższym rysunkiem.



1	Gniazdo zasilacza prądu stałego (DC48V).	6	Port pomocniczy.
2	Zasilacz sieciowy (opcjonalny).	7	Złącze słuchawki.
3	Wtyczka do gniazdka sieci elektrycznej (opcjonalna).	8	Złącze słuchawek analogowych (opcjonalne).
4	Złącze portu sieci (10/100/1000 SW). Dostosowanie do zasilania IEEE 802.3at.	9	Port USB
5	Złącze portu dostępu (10/100/1000 PC).		



### Uwaga

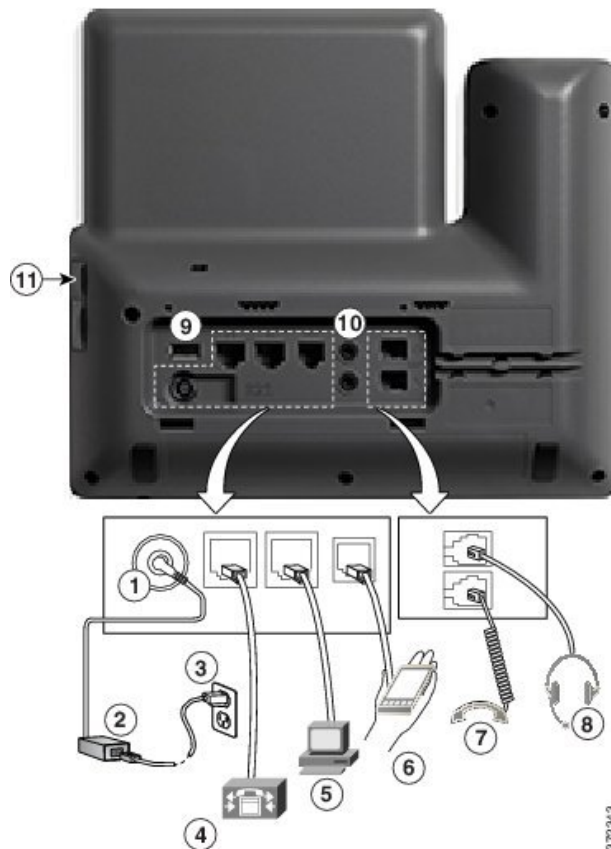
Każdy port USB umożliwia podłączenie do 5 urządzeń obsługiwanych i nieobsługiwanych. Przy zliczaniu maksymalnej liczby urządzeń jest brane pod uwagę każde urządzenie podłączone do telefonu. Za pomocą telefonu można na przykład obsługiwać 5 urządzeń USB podłączonych do portu bocznego (np. dwa moduły rozszerzeń, jeden zestaw nagłowny, jeden koncentrator i jedno inne standardowe urządzenie USB). Wiele produktów USB innych firm należy liczyć jako kilka urządzeń USB, na przykład urządzenie zawierające koncentrator USB i zestaw nagłowny należy liczyć jako dwa urządzenia USB. Więcej informacji zawiera dokumentacja danego urządzenia USB.

# Telefony IP Cisco 8861, 8865 i 8865NR

W poniższej sekcji opisano cechy telefonów IP Cisco 8861, 8865 i 8865NR.

## Złącza telefonu

Podłącz swój telefon do firmowej sieci telefonii IP, posługując się poniższym rysunkiem.



1	Gniazdo zasilacza prądu stałego (DC48V).	7	Złącze słuchawki.
2	Zasilacz sieciowy (opcjonalny).	8	Złącze słuchawek analogowych (opcjonalne).
3	Wtyczka do gniazdka sieci elektrycznej (opcjonalna).	9	Port USB
4	Złącze portu sieci (10/100/1000 SW). Dostosowanie do zasilania IEEE 802.3at.	10	Porty audio we/wy
5	Złącze portu dostępu (10/100/1000 PC).	11	Port USB
6	Port pomocniczy.		

**Uwaga**

Każdy port USB umożliwia połączenie do 5 urządzeń obsługiwanych i nieobsługiwanych. Przy zliczaniu maksymalnej liczby urządzeń jest brane pod uwagę każde urządzenie podłączone do telefonu. Na przykład telefon może obsługiwać 5 urządzeń USB (np. trzy moduły rozszerzenia klawiatury, jeden koncentrator i jedno inne standardowe urządzenie USB) podłączonych do portu bocznego i 5 dodatkowych standardowych urządzeń USB podłączonych do portu tylnego. Wiele produktów USB innych firm należy liczyć jako kilka urządzeń USB, na przykład urządzenie zawierające koncentrator USB i zestaw nagłowny należy liczyć jako dwa urządzenia USB. Więcej informacji zawiera dokumentacja danego urządzenia USB.

## Przyciski i podzespoły

Telefony IP Cisco z serii 8800 dzielą się pod względem konstrukcji na dwa rodzaje:

- Telefony IP Cisco 8811, 8841, 8851, 8851NR i 8861 — nie mają kamery.
- Telefony IP Cisco 8845, 8865 i 8865NR — mają wbudowaną kamerę.

Na poniższym rysunku pokazano telefon IP Cisco 8845.

**Rysunek 1: Przyciski i podzespoły telefonu IP Cisco 8845**





W poniższej tabeli opisano przyciski telefonów IP Cisco z serii 8800.

**Tabela 18: Przyciski telefonów IP Cisco z serii 8800**

1	Słuchawka i jej świecący pasek	Sygnalizuje połączenie przychodzące (miga na czerwono) lub nową wiadomość głosową (świeci się na czerwono).
2	Kamera  Dotyczy tylko telefonów IP Cisco 8845, 8865 i 8865NR	Kamera służy do nawiązywania połączeń wideo.

3	Programowalne przyciski funkcji i przyciski linii	 Dostęp do linii, funkcji i sesji połączeń w telefonie. Podczas dodawania funkcji do klawiszy linii telefonicznej ograniczeniem jest liczba dostępnych klawiszy linii. Nie można dodać więcej funkcji niż liczba klawiszy linii na telefonie. Więcej informacji można znaleźć w sekcji Przyciski programowe, linii i funkcyjne w rozdziale „Telefon IP Cisco — sprzęt”.
4	Przyciski programowe	 Dostęp do funkcji i usług. Więcej informacji można znaleźć w sekcji Przyciski programowe, linii i funkcyjne w rozdziale „Telefon IP Cisco — sprzęt”.
5	<b>Wstecz</b> , grupa Nawigacja i <b>Zwolnij</b>	<b>Wstecz</b>  Powrót do poprzedniego ekranu lub menu. Grupa Nawigacja  Pierścień nawigacyjny i przycisk <b>Wybierz</b> — przewijanie menu oraz zaznaczanie i wybieranie elementów. <b>Zwolnij</b>  Kończenie trwającego połączenia lub sesji.
6	<b>Zawieś/Wznów</b> , <b>Konferencja</b> i <b>Przełącz</b>	<b>Zawieś/Wznów</b>  Zawieszanie aktywnego połączenia i wznowianie zawieszonych połączeń. <b>Konferencja</b>  Tworzenie połączenia konferencyjnego. <b>Przełącz</b>  Przekazywanie połączenia.
7	<b>Zestaw głośnomówiący</b> , <b>Wycisz</b> i <b>Zestaw słuchawkowy</b>	<b>Zestaw głośnomówiący</b>  Włączanie i wyłączenie zestawu głośnomówiącego. Przycisk jest podświetlony, gdy zestaw głośnomówiący jest włączony. <b>Wycisz</b>  Włączanie i wyłączenie mikrofonu. Przycisk jest podświetlony, gdy mikrofon jest wyciszony. <b>Zestaw słuchawkowy</b>  Włączanie zestawu słuchawkowego. Przycisk jest podświetlony, gdy zestaw słuchawkowy jest włączony. Aby opuścić tryb zestawu słuchawkowego, podnieś słuchawkę lub wybierz <b>Telefon głośnomówiący</b>  .
8	<b>Kontakty</b> , <b>Aplikacje</b> i <b>Wiadomości</b>	<b>Kontakty</b>  Dostęp do osobistej i firmowej książki telefonicznej. <b>Aplikacje</b>  Dostęp do historii połączeń, preferencji użytkownika, ustawień telefonu i informacji o modelu telefonu. <b>Wiadomości</b>  Automatyczne nawiązywanie połączenia z systemem poczty głosowej.



9	Przycisk <b>Głośność</b>	  Regulacja głośności słuchawki, zestawu słuchawkowego i telefonu głośnomówiącego (przy podniesionej słuchawce) oraz głośności dzwonka (przy odłożonej słuchawce).
---	--------------------------	--

## Przyciski programowe, linii i funkcji


Funkcji dostępnych w telefonie można używać na kilka sposobów:

- Pod ekranem znajdują się klawisze programowe, które umożliwiają korzystanie z funkcji wyświetlanych bezpośrednio nad nimi. Zmieniają się zależnie od czynności wykonywanych aktualnie przez użytkownika. Przycisk programowy **Więcej...** wskazuje, że dostępne są inne funkcje.
- Przyciski funkcji i linii, które znajdują się po bokach ekranu, zapewniają dostęp do funkcji telefonu i linii telefonicznych.
  - Przyciski funkcyjne — umożliwiają korzystanie z takich funkcji, jak **Szybkie wybieranie** czy **Przejęcie połączenia** oraz do wyświetlania statusu na innej linii.
  - Przyciski linii — służą do odbierania połączeń i wznawiania zawieszonych połączeń. Jeśli nie używa się ich do obsługi aktywnego połączenia, umożliwiają inicjowanie funkcji telefonu, takich jak np. wyświetlanie nieodebranych połączeń.

Podświetlenie przycisków funkcji i linii wskazuje stan.

Kolor i stan diod LED	Tryb linii zwykłej: przyciski linii	Tryb linii zwykłej: przyciski funkcyjne Tryb linii zaawansowanej
 — stały zielony kolor diody LED	Aktywne połączenie lub dwukierunkowe połączenie interkomem, połączenie wstrzymane, prywatność w użyciu	Aktywne połączenie lub dwukierunkowe połączenie interkomem, prywatność w użyciu
 — migający zielony kolor diody LED	Nie dotyczy	Połączenie wstrzymane
 — stały pomarańczowy kolor diody LED	Połączenie przychodzące, połączenie powracające, jednokierunkowe połączenie interkomem, zalogowany do grupy poszukiwania	Jednokierunkowe połączenie interkomem, zalogowane do grupy poszukiwania
 — migający pomarańczowy kolor diody LED	Nie dotyczy	Połączenie przychodzące, połączenie powracające
 — stały czerwony kolor diody LED	Linia zdalna w użyciu, linia zdalna wstrzymana, tryb Nie przeszkadzać aktywny	Linia zdalna w użyciu, tryb Nie przeszkadzać aktywny



Kolor i stan diod LED	Tryb linii zwykłej: przyciski linii	Tryb linii zwykłej: przyciski funkcyjne Tryb linii zaawansowanej
 — migający czerwony kolor diody LED	Nie dotyczy	Linia zdalna wstrzymana

Administrator może skonfigurować niektóre funkcje jako przyciski programowe lub przyciski funkcji. Ponadto do niektórych funkcji można uzyskać dostęp za pomocą powiązanych z nimi przycisków sprzętowych lub przycisków programowych.

## Ochrona kamery w telefonie

Kamera w telefonie jest bardzo delikatna, i może zostać uszkodzona podczas transportu.

### Zanim rozpocznie

Potrzebne są:

- Oryginalne opakowanie i pudełko po telefonie
- Materiały opakowaniowe, np. styropian lub opakowanie bąbelkowe

### Procedura

- 
- Krok 1** Jeśli posiadasz oryginalne pudełko:
- Umieścić styropian na kamerze tak, aby odpowiednio zakryć soczewkę.
  - Umieścić telefon w oryginalnym opakowaniu.
- Krok 2** Jeśli nie masz pudełka, starannie zapakuj telefon w styropian lub folię bąbelkową celem, aby ochronić kamerę. Upewnij się, że styropian chroni i otacza kamerę tak, aby nic nie mogło naciskać na nią z żadnej strony, gdyż inaczej kamera może zostać uszkodzona podczas transportu.
-





## CZĘŚĆ II

# Instalowanie telefonu IP Cisco

- Instalowanie telefonu IP Cisco, na stronie 43
- Konfigurowanie telefonu w programie Cisco Unified Communications Manager, na stronie 69
- Zarządzanie portalem samoobsługowym, na stronie 83





## ROZDZIAŁ 4

# Instalowanie telefonu IP Cisco

- Sprawdzenie konfiguracji sieci, na stronie 43
- Wdrażanie za pomocą kodu aktywacyjnego dla telefonów w siedzibie, na stronie 44
- Wdrażanie przy użyciu kodu aktywacyjnego oraz dostęp z urządzeń przenośnych i dostęp zdalny, na stronie 45
- Włączanie automatycznej rejestracji telefonów, na stronie 46
- Instalowanie telefonu IP Cisco, na stronie 47
- Konfigurowanie telefonu za pomocą menu konfiguracji, na stronie 49
- Włącz w telefonie bezprzewodową sieć LAN, na stronie 51
- Konfigurowanie ustawień sieciowych, na stronie 59
- Sprawdzenie przy uruchamianiu telefonu, na stronie 66
- Konfigurowanie usług telefonicznych dla użytkowników, na stronie 66
- Zmień model telefonu użytkownika, na stronie 67

## Sprawdzanie konfiguracji sieci

Podczas wdrażania nowego systemu telefonicznego IP administratorzy systemu i administratorzy sieci muszą wykonać kilka wstępnych zadań konfiguracyjnych w celu przygotowania sieci do obsługi telefonii IP. Informacje i listę kontrolną dotyczące konfigurowania sieci telefonii IP Cisco można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Aby telefon działał sprawnie jako punkt końcowy sieci, sieć musi spełniać określone wymagania. Jednym z wymagań jest odpowiednia przepustowość. Podczas rejestrowania w programie Cisco Unified Communications Manager telefony wymagają większej przepustowości niż zalecane 32 kb/s. Przy konfigurowaniu szerokości pasma QoS należy rozważyć użycie większej przepustowości. Więcej informacji można znaleźć w podręczniku *Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)* lub innym dla nowszej wersji tego systemu ( [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab12/collab12.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html) ).



### Uwaga

Telefon wyświetla datę i godzinę z Cisco Unified Communications Manager. Czas wyświetlany na telefonie może różnić się od czasu z Cisco Unified Communications Manager o maksymalnie 10 sekund.

## Procedura

---

- Krok 1** Skonfiguruj sieć VoIP tak, aby spełniała następujące wymagania:
- Na routerach i bramach skonfigurowano obsługę VoIP.
  - Cisco Unified Communications Manager jest zainstalowany w sieci i ma skonfigurowane przetwarzanie połączeń.
- Krok 2** Skonfiguruj w sieci jedno z następujących rozwiązań:
- Obsługa protokołu DHCP
  - Ręczne przypisywanie adresu IP, bramy i maski podsieci
- 

## Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

# Wdrażanie za pomocą kodu aktywacyjnego dla telefonów w siedzibie

Wdrażanie za pomocą kodu aktywacyjnego służy do szybkiego konfigurowania nowych telefonów bez automatycznej rejestracji. To rozwiązanie umożliwia kontrolowanie procesu wdrażania za pomocą jednego z następujących składników:

- Narzędzie administracji zbiorczej Cisco Unified Communications (BAT)
- Interfejs administracyjny systemu Cisco Unified Communications Manager
- Administracyjna usługa sieci Web XML (AXL)

Włącz tę funkcję w sekcji **Informacje o urządzeniu** na stronie Konfiguracja telefonu. Wybierz opcję **Wymagają wdrażania przy użyciu kodu aktywacyjnego**, jeśli ta funkcja ma mieć zastosowanie do pojedynczego telefonu w siedzibie firmy.

Użytkownicy muszą wprowadzić kod aktywacyjny, aby ich telefony mogły zostać zarejestrowane. Wdrażanie przy użyciu kodu aktywacyjnego można stosować do poszczególnych telefonów, grup telefonów lub w całej sieci.

Jest to łatwy sposób wdrażania telefonów przez użytkowników, ponieważ muszą oni tylko wprowadzić 16-cyfrowy kod aktywacyjny. Kody można wprowadzić ręcznie lub przy użyciu kodu QR, jeśli telefon jest wyposażony w kamerę wideo. Zalecamy przekazywanie tych informacji użytkownikom w bezpieczny sposób. Jeśli użytkownik został przypisany do telefonu, ta informacja jest dostępna w portalu Self Care. Uzyskanie dostępu przez użytkownika do kodu w portalu jest rejestrowane w dzienniku inspekcji.

Kody aktywacyjne mogą być użyte tylko raz i domyślnie wygasają po upływie 1 tygodnia. W przypadku wygaśnięcia kodu należy dostarczyć użytkownikowi nowy kod.

To rozwiązanie umożliwia łatwe zachowanie bezpieczeństwa sieci, ponieważ rejestracja telefonu jest możliwa dopiero po weryfikacji certyfikatu MIC (Manufacturing Installed Certificate) i kodu aktywacyjnego. Jest to

również wygodny sposób masowego wdrażania telefonów, ponieważ nie wymaga użycia narzędzia do obsługi telefonów rejestrowanych automatycznie (TAPS) ani automatycznej rejestracji. Szybkość wdrażania wynosi jeden telefon na sekundę lub około 3600 telefonów na godzinę. Telefony można dodawać przy użyciu interfejsu administracyjnego systemu Cisco Unified Communications Manager, administracyjnej usługi sieci Web XML (AXL) lub narzędzia BAT.

Istniejące telefony są resetowane po skonfigurowaniu do wdrażania przy użyciu kodu aktywacyjnego. Są one rejestrowane dopiero po wprowadzeniu kodu aktywacyjnego i weryfikacji certyfikatu MIC telefonu. Przed wdrożeniem funkcji wdrażania przy użyciu kodu aktywacyjnego należy o niej poinformować obecnych użytkowników.

Więcej informacji zawiera *Podręcznik administratora systemu Cisco Unified Communications Manager oraz usługi IM i systemu obecności, wersja 12.0(1)* lub nowszy.

## Wdrażanie przy użyciu kodu aktywacyjnego oraz dostęp z urządzeń przenośnych i dostęp zdalny

Podczas wdrażania telefonów IP Cisco dla użytkowników zdalnych można korzystać z funkcji wdrażania przy użyciu kodu aktywacyjnego na potrzeby dostępu z urządzeń przenośnych i dostępu zdalnego. Funkcja ta jest bezpiecznym sposobem wdrożenia telefonów znajdujących się poza siedzibą w przypadku, gdy automatyczna rejestracja nie jest wymagana. Można jednak zastosować taką konfigurację, aby telefon w siedzibie wymagał automatycznej rejestracji, a telefon poza siedzibą — kodów aktywacyjnych. Funkcja ta przypomina funkcję wdrażania za pomocą kodu aktywacyjnego dla telefonów w siedzibie, ale udostępnia również kod aktywacyjny dla telefonów poza siedzibą.

Funkcja wdrażania przy użyciu kodu aktywacyjnego na potrzeby dostępu z urządzeń przenośnych i dostępu zdalnego wymaga programu Cisco Unified Communications Manager 12.5(1)SU1 lub nowszego oraz Cisco Expressway X12.5 lub nowszego. Ponadto powinna być włączona funkcja Smart Licensing.

Funkcję tę możesz włączyć w programie Cisco Unified Communications Manager Administration, pamiętaj jednak, że:

- Włącz tę funkcję w sekcji **Informacje o urządzeniu** na stronie Konfiguracja telefonu.
- Wybierz opcję **Wymagaj wdrażania przy użyciu kodu aktywacyjnego**, jeśli ta funkcja ma mieć zastosowanie tylko do pojedynczego telefonu w siedzibie firmy.
- Wybierz **Zezwól na użycie kodu aktywacyjnego za pośrednictwem usługi MRA** oraz **Wymagaj wdrażania za pomocą kodu aktywacyjnego**, aby użyć wspomnianej funkcji wdrażania w odniesieniu do pojedynczego telefonu w siedzibie. Jeśli telefon jest poza siedzibą, zaczyna korzystać z trybu Dostęp z urządzeń przenośnych i dostęp zdalny, a następnie z usługi Expressway. Jeśli telefon nie może nawiązać połączenia z usługą Expressway, nie rejestruje się, dopóki nie znajdzie się poza siedzibą.

Więcej informacji na ten temat można znaleźć w następujących dokumentach:

- *Podręcznik administratora systemu Cisco Unified Communications Manager oraz usługi IM i systemu obecności, wersja 12.0(1)*
- *Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway dla usług Cisco Expressway w wersji X12.5 lub nowszej*

# Włączanie automatycznej rejestracji telefonów

Telefon IP Cisco wymaga, aby przetwarzaniem połączeń zajmował się program Cisco Unified Communications Manager. Korzystając z informacji podanych w dokumentacji używanej wersji programu Cisco Unified Communications Manager lub w pomocy kontekstowej aplikacji Cisco Unified Communications Manager — administracja, należy upewnić się, że program Cisco Unified Communications Manager jest odpowiednio skonfigurowany pod kątem zarządzania telefonem oraz prawidłowo trasuje i przetwarza połączenia.

Przed zainstalowaniem telefonów IP Cisco należy wybrać metodę ich dodawania do bazy danych Cisco Unified Communications Manager.

Dzięki włączeniu automatycznej rejestracji przed zainstalowaniem telefonów można:

- Dodawać telefony bez uprzedniego sprawdzania ich adresów MAC.
- Automatycznie dodawać telefony IP Cisco do bazy danych Cisco Unified Communications Manager poprzez samo podłączenie ich do sieci telefonii IP. Podczas automatycznej rejestracji program Cisco Unified Communications Manager przypisuje telefonowi kolejny dostępny numer telefonu.
- Szybko wprowadzać telefony do bazy danych Cisco Unified Communications Manager i modyfikować dowolne ich ustawienia, np. numery telefonu, za pomocą programu Cisco Unified Communications Manager.
- Przenosić zarejestrowane automatycznie telefony w nowe miejsca i przypisywać je do różnych pul urządzeń bez powodowania zmiany ich numerów telefonu.

Domyślnie automatyczna rejestracja jest wyłączona. W niektórych przypadkach warto zrezygnować z używania automatycznej rejestracji, np. jeśli chce się przypisać konkretny numer telefonu lub korzystać za pomocą programu Cisco Unified Communications Manager z połączenia zabezpieczonego. Więcej informacji o włączaniu automatycznej rejestracji można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager. Po skonfigurowaniu w klastrze trybu mieszanego za pomocą klienta Cisco CTL automatyczna rejestracja zostaje automatycznie wyłączona, ale można ją włączyć. Po skonfigurowaniu w klastrze trybu niezabezpieczonego za pomocą klienta Cisco CTL automatyczna rejestracja nie włącza się samoczynnie.

Telefony objęte działaniem automatycznej rejestracji i narzędzia TAPS (ang. Tool for AutoRegistered Phones Support, narzędzie do obsługi telefonów zarejestrowanych automatycznie) można dodawać do bazy danych bez uprzedniego sprawdzania ich adresów MAC.

Narzędzie TAPS współpracuje z Narzędziem administracji zbiorczej przy zbiorczym aktualizowaniu telefonów, które zostały już dodane do bazy danych Cisco Unified Communications Manager z fikcyjnymi adresami MAC. Za pomocą narzędzia TAPS można aktualizować adresy MAC i pobierać do telefonów zdefiniowane wstępnie konfiguracje.

Firma Cisco zaleca, aby w celu dodania do sieci mniej niż 100 telefonów użyć automatycznej rejestracji i narzędzia TAPS. W celu dodania do sieci ponad 100 telefonów należy skorzystać z Narzędzia administracji zbiorczej.

Aby zastosować narzędzie TAPS, administrator lub użytkownik końcowy musi wybrać numer telefonu narzędzia TAPS i postępować zgodnie z podawanymi komunikatami głosowymi. Po zakończeniu procedury telefon zawiera numer telefonu i inne ustawienia, a jego prawidłowy adres MAC jest zaktualizowany w aplikacji Cisco Unified Communications Manager — administracja.



Przed podłączeniem do sieci jakiegokolwiek telefonu IP Cisco należy sprawdzić w aplikacji Cisco Unified Communications Manager — administracja, czy automatyczna rejestracja jest włączona i prawidłowo skonfigurowana. Więcej informacji o włączaniu i konfigurowaniu automatycznej rejestracji można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Aby umożliwić działanie narzędzia TAPS, należy włączyć automatyczną rejestrację w aplikacji Cisco Unified Communications Manager — administracja.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja kliknij kolejno przyciski **System** > **Cisco Unified CM**.
- Krok 2** Kliknij przycisk **Znajdź** i wybierz odpowiedni serwer.
- Krok 3** W oknie **Informacje o automatycznej rejestracji** skonfiguruj poniższe pola.
- **Uniwersalny szablon urządzenia**
  - **Uniwersalny szablon linii**
  - **Początkowy numer telefonu**
  - **Końcowy numer telefonu**
- Krok 4** Usuń zaznaczenie pola wyboru **Automatyczna rejestracja wyłączona na tym serwerze programu Cisco Unified Communications Manager**.
- Krok 5** Kliknij przycisk **Zapisz**.
- Krok 6** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
- 

## Instalowanie telefonu IP Cisco

Gdy telefon połączy się z siecią, rozpocznie proces uruchamiania i zarejestruje się w programie Cisco Unified Communications Manager. Aby dokończyć instalowanie telefonu, należy skonfigurować jego ustawienia sieciowe (zależnie od tego, czy włączona jest usługa DHCP).

Jeśli używana jest automatyczna rejestracja, należy zaktualizować określone elementy konfiguracji telefonu, np. skojarzyć telefon z użytkownikiem lub zmienić tabelę przycisków bądź numer telefonu.



**Uwaga** Przed rozpoczęciem używania urządzeń zewnętrznych przeczytaj [Urządzenia zewnętrzne, na stronie 26](#).

Informacje o instalowaniu akcesoriów można znaleźć w przewodniku *po akcesoriach do telefonów IP Cisco z serii 7800 i 8800 współpracujących z oprogramowaniem Cisco Unified Communications Manager*.

Jeśli do biurka jest doprowadzony tylko jeden kabel sieci LAN, można podłączyć go do portu oprogramowania w telefonie, a komputer podłączyć do portu PC. Aby uzyskać więcej informacji, patrz [Współużytkowanie połączenia sieciowego — telefon i komputer, na stronie 49](#).

W ten sposób można również podłączyć szeregowo dwa telefony. Port komputera pierwszego telefonu należy połączyć z portem oprogramowania drugiego.



**Przeostroga** Nie należy podłączać do sieci LAN obu tych portów jednocześnie.

## Procedura

- Krok 1** Wybierz źródło zasilania telefonu:
- Zasilanie Power over Ethernet (PoE)
  - Zasilacz zewnętrzny
- Aby uzyskać więcej informacji, patrz [Wymogi dotyczące zasilania telefonu, na stronie 16](#).
- Krok 2** Podłącz słuchawkę do portu słuchawki i wciśnij kabel do kanału w telefonie.
- Słuchawka szerokopasmowa jest zaprojektowana specjalnie do użytku z telefonami IP Cisco. Słuchawka ma świecący pasek informujący o połączeniach przychodzących i oczekujących wiadomościach głosowych.
- Przeostroga** Niewciśnięcie kabla do kanału w telefonie może doprowadzić do uszkodzenia płytki drukowanej. Kanał na kabel zmniejsza obciążenie złącza i płytki drukowanej.
- Krok 3** Podłącz zestaw nagłowny lub bezprzewodowy zestaw słuchawkowy. Jeśli nie podłączysz zestawu słuchawkowego teraz, możesz go dodać później.
- Wciśnij kabel do kanału na kabel.
- Przeostroga** Jeśli kabel nie zostanie wciśnięty do kanału w telefonie, może to doprowadzić do uszkodzenia płytki drukowanej wewnątrz telefonu. Kanał na kabel zmniejsza obciążenie złącza i płytki drukowanej.
- Krok 4** Podłącz kabel prosty sieci Ethernet od przełącznika do portu sieciowego z etykietą 10/100/1000 SW w telefonie IP Cisco. Każdy telefon IP Cisco jest dostarczany z jednym kablem Ethernet w opakowaniu.
- Połączenia 10 Mb/s wymagają użycia kabli kategorii 3, 5, 5e lub 6; połączenia 100 Mb/s — kabli kategorii 5, 5e lub 6; a połączenia 1000 Mb/s — kabli kategorii 5e lub 6. Więcej informacji i wskazówek można znaleźć w artykule [Styki portu sieciowego i portu komputera, na stronie 14](#).
- Krok 5** Podłącz kablem prostym inne urządzenie sieciowe, np. komputer stacjonarny, do portu komputera w telefonie IP Cisco. Jeśli nie podłączysz innego urządzenia sieciowego teraz, możesz to zrobić później.
- Połączenia 10 Mb/s wymagają użycia kabli kategorii 3, 5, 5e lub 6; połączenia 100 Mb/s — kabli kategorii 5, 5e lub 6; a połączenia 1000 Mb/s — kabli kategorii 5e lub 6. Więcej informacji i wskazówek można znaleźć w artykule [Styki portu sieciowego i portu komputera, na stronie 14](#).
- Krok 6** Jeśli telefon znajduje się na biurku, wyreguluj podstawkę. Jeśli telefon jest zamontowany na ścianie, może być konieczna regulacja oparcia słuchawki, aby nie wypadła z uchwytu.
- Krok 7** Obserwuj proces uruchamiania telefonu. W tym kroku do telefonu są dodawane numery telefonu główny i pomocniczy oraz funkcje związane z numerami telefonów, a także następuje weryfikacja poprawności konfiguracji telefonu.

- Krok 8** Jeśli konfigurujesz w telefonie ustawienia sieciowe, możesz ustawić adres IP telefonu za pomocą protokołu DHCP albo wprowadzić go ręcznie.
- Zobacz [Konfigurowanie ustawień sieciowych, na stronie 59](#) i [Konfiguracja sieci, na stronie 249](#).
- Krok 9** Uaktualnij firmware telefonu do bieżącej wersji.
- Uaktualnienie firmware za pośrednictwem sieci bezprzewodowej może trwać dłużej niż w przypadku wykorzystania sieci przewodowej. Czas zależy od jakości i przepustowości połączenia bezprzewodowego. Niektóre uaktualnienia mogą zająć ponad godzinę.
- Krok 10** Zadzwoń z telefonu IP Cisco, aby sprawdzić, czy działa on poprawnie.
- Zobacz *Podręcznik użytkownika telefonów Cisco IP Phone z serii 8800*.
- Krok 11** Poinformuj użytkowników końcowych, jak mają używać telefonów i jak mogą skonfigurować ich opcje. Dzięki temu użytkownicy dowiedzą się, jak efektywnie korzystać z telefonów IP Cisco .
- 

## Współużytkowanie połączenia sieciowego — telefon i komputer

Zarówno telefon, jak i komputer muszą nawiązać połączenie z siecią, aby działać. Jeśli dostępny jest tylko jeden port sieci Ethernet, urządzenia mogą współdzielić połączenie sieciowe.

### Zanim rozpocznie

Aby można było korzystać z portu PC w programie Cisco Unified Communications Manager, musi on zostać włączony przez administratora.

### Procedura

---

- Krok 1** Podłącz port SW telefonu do sieci LAN za pomocą kabla Ethernetowego.
- Krok 2** Połącz komputer z portem PC telefonu za pomocą kabla Ethernetowego.
- 

## Konfigurowanie telefonu za pomocą menu konfiguracji

Telefon IP Cisco zawiera następujące menu konfiguracji:

- Konfiguracja sieci: zawiera opcje wyświetlania i konfiguracji ustawień protokołów sieciowych takich jak tylko IPv4, tylko IPv6, WLAN i Ethernet.
- Konfiguracja sieci Ethernet: elementy tego podmenu udostępniają opcje konfiguracji telefonu IP Cisco w sieci Ethernet.
- Konfiguracja klienta Wi-Fi: elementy tego podmenu udostępniają opcje konfiguracji telefonu IP Cisco w bezprzewodowej sieci lokalnej (WLAN). Sieć Wi-Fi jest obsługiwana wyłącznie przez telefony IP Cisco 8861 i 8865.



---

**Uwaga** Port komputera w telefonie jest wyłączony, gdy w telefonie włączona jest sieć Wi-Fi.

---

- Konfiguracja protokołu IPv4 i Konfiguracja protokołu IPv6: te podmenu należące do menu konfiguracji sieci Ethernet i do menu konfiguracji klienta Wi-Fi zawierają dodatkowe opcje sieciowe.
- Konfiguracja zabezpieczeń: udostępnia opcje służące do wyświetlania i konfiguracji ustawień zabezpieczeń takich jak tryb zabezpieczeń, lista zaufanych i protokół uwierzytelniania 802.1X.

Przed przystąpieniem do zmian ustawień opcji w menu konfiguracji sieci należy odblokować edytowanie opcji.



---



**Uwaga** Za pomocą pola Settings Access (Dostęp do ustawień) w oknie Konfiguracja telefonu programu Cisco Unified Communications Manager — administracja można określić, czy menu Ustawienia i znajdujące się w nim opcje będą dostępne. W polu Settings Access dozwolone są następujące wartości:

- Włączone: umożliwia dostęp do menu Ustawienia.
- Wyłączone: blokuje dostęp do menu Ustawienia.
- Ograniczone: umożliwia dostęp do menu User Preferences (Preferencje użytkownika) i zapisywanie zmian głośności. Blokuje dostęp do innych opcji w menu Ustawienia.

Jeśli nie masz dostępu do opcji w menu Ustawienia admin., sprawdź wartość w polu Dostęp do ustawień.

---

### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
  - Krok 2** Wybierz opcję **Ustawienia administratora**.
  - Krok 3** Wybierz opcję **Konfiguracja sieci** lub **Konfiguracja zabezpieczeń**.
  - Krok 4** Wprowadź swój identyfikator użytkownika i hasło, jeśli jest to konieczne, i kliknij przycisk **Zaloguj się**.
  - Krok 5** Wykonaj jedną z tych czynności, aby wyświetlić żądane menu:
    - Za pomocą strzałek nawigacyjnych wybierz żądane menu, a następnie naciśnij przycisk **Wybierz**.
    - Za pomocą klawiatury numerycznej telefonu wpisz numer odpowiadający menu.
  - Krok 6** Aby wyświetlić podmenu, powtórz krok 5.
  - Krok 7** Aby wyjść z menu, naciśnij przycisk **Wyjdź** lub strzałkę **Wstecz** .
- 

## Ustawianie hasła w telefonie


W telefonie można ustawić hasło. Po ustawieniu hasła nie można zmienić żadnych opcji administracyjnych telefonu bez wprowadzenia hasła na ekranie Ustawienia administratora.

## Procedura

- Krok 1** W narzędziu Cisco Unified Communications Manager — administracja przejdź do okna konfiguracji wspólnego profilu telefonu, wybierając kolejno opcje **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**.
- Krok 2** Wprowadź hasło w polu Local Phone Unlock Password (Lokalne hasło odblokowywania telefonu).
- Krok 3** Zastosuj hasło dla wspólnego profilu telefonu.

## Wprowadzanie tekstu za pomocą telefonu i poruszanie się po jego menu

Edytując wartość ustawienia opcji, postępuj w następujący sposób:

- Za pomocą strzałek na przycisku nawigacji zaznacz pole, które chcesz edytować, a następnie naciśnij klawisz **Wybierz** na przycisku nawigacyjnym, aby aktywować to pole. Gdy pole jest aktywne, możesz wprowadzić wartości.
- Do wprowadzania cyfr i liter służy klawiatura numeryczna.
- Aby wprowadzać litery za pomocą klawiatury numerycznej, naciskaj odpowiedni klawisz numeryczny. Aby wyświetlić żądaną literę, należy nacisnąć klawisz odpowiednią liczbę razy. Na przykład naciśnij klawisz **2** raz dla „a,” dwa razy szybko dla „b,” i trzy razy szybko dla „c.” Po zatrzymaniu kursor automatycznie przesuwa się, aby umożliwić wprowadzenie kolejnej litery.
- Jeśli zrobisz błąd, naciśnij klawisz programowy ze strzałką . Ten klawisz programowy usuwa znak po lewej stronie kursora.
- Aby odrzucić wszystkie wprowadzone zmiany, naciśnij klawisz **Anuluj**, a następnie klawisz **Zapisz**.
- Aby wprowadzić adres IP, należy wpisać wartości w czterech oddzielonych od siebie segmentach. Po zakończeniu wprowadzania cyfr w segmencie z lewej strony przed pierwszą kropką należy użyć klawisza strzałki w prawo, aby przejść do następnego segmentu. Kropka występująca po cyfrach z lewej strony jest wstawiana automatycznie.
- Aby wpisać dwukropek w adresie IPv6, naciśnij \* na klawiaturze numerycznej.



**Uwaga** Telefon IP Cisco udostępnia kilka metod resetowania/przywracania ustawień opcji, gdy jest to konieczne.

### Tematy pokrewne

[Resetowanie podstawowe](#), na stronie 287

[Ustawianie hasła w telefonie](#), na stronie 50

## Włącz w telefonie bezprzewodową sieć LAN

Przed skonfigurowaniem bezprzewodowej sieci LAN sprawdź, czy telefon obsługuje komunikację bezprzewodową. Telefony IP Cisco 8861 i 8865 obsługują konfiguracje bezprzewodowych sieci LAN. Telefon IP Cisco 8865NR nie obsługuje bezprzewodowych sieci LAN.

Upewnij się, że zasięg sieci Wi-Fi w miejscu, w którym konfigurujesz bezprzewodową sieć LAN, jest odpowiedni do przesyłania pakietów.

Jeśli jest włączone przesyłanie głosu przez sieć Wi-Fi i używasz trybu zabezpieczeń EAP-FAST lub PEAP, uwierzytelnij sieć Wi-Fi za pomocą aplikacji logowania do sieci WLAN. W trybach zabezpieczeń WEP, PSK i otwartym uwierzytelnianiu odbywa się w sieci Wi-Fi.

Użytkownikom sieci Wi-Fi zalecamy używanie metody roamingu Fast-Secure (szybki i bezpieczny).



**Uwaga** Port komputera w telefonie jest wyłączony, gdy w telefonie włączona jest sieć Wi-Fi.

Kompletne informacje o konfiguracji znajdują się w *Podręczniku wdrażania sieci WLAN na urządzeniach IP Cisco z serii 8800* pod następującym adresem:

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>


*Podręcznik wdrażania sieci WLAN na urządzeniach IP Cisco z serii 8800* zawiera następujące informacje o konfiguracji:

- Konfiguracja sieci bezprzewodowej
- Konfiguracja sieci bezprzewodowej w aplikacji Cisco Unified Communications Manager — administracja
- Konfiguracja sieci bezprzewodowej w telefonie IP Cisco

### Zanim rozpoczniesz

Upewnij się, że funkcja Wi-Fi jest włączona w telefonie oraz że kabel Ethernet jest odłączony.

### Procedura

- 
- Krok 1** Aby włączyć aplikację, naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja klienta Wi-Fi** > **Nazwa sieci**.  
Zostanie wyświetlona lista dostępnych punktów dostępu bezprzewodowego, z którymi możesz się połączyć.
- Krok 3** Włącz sieć bezprzewodową.
- 

## Konfigurowanie bezprzewodowej sieci LAN w programie Cisco Unified Communications Manager

W aplikacji Cisco Unified Communications Manager — administracja należy włączyć parametr o nazwie “Wi-Fi” dla bezprzewodowego telefonu IP Cisco.



**Uwaga** Podczas konfigurowania adresu MAC, w aplikacji Cisco Unified Communications Manager — administracja w oknie Konfiguracja telefonu (**Urządzenie > Telefon**), należy użyć adresu MAC linii stacjonarnej. W programie Cisco Unified Communications Manager w funkcji rejestracji nie jest używany adres MAC połączenia bezprzewodowego.

W aplikacji Cisco Unified Communications Manager — administracja wykonaj procedurę opisaną poniżej.

### Procedura

- Krok 1** Aby włączyć obsługę bezprzewodowej sieci LAN w określonym telefonie, wykonaj następujące czynności:
- Wybierz kolejno opcje **Urządzenie > Telefon**.
  - Odszukaj żądany telefon.
  - W sekcji Układ konfiguracji specyficznej dla produktu, w parametrze Wi-Fi, zaznacz pole **Włączone**.
  - Zaznacz pole wyboru **Zastęp ustawienia wspólne**.
- Krok 2** Aby włączyć obsługę bezprzewodowej sieci LAN w grupie telefonów:
- Wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**.
  - Wybierz dla parametru Wi-Fi wartość **Włączone**.
- Uwaga** Aby upewnić się, że konfiguracja działa w tym kroku, usuń zaznaczenie pola wyboru **Zastęp ustawienia wspólne** opisanego w kroku 1d.
- Zaznacz pole wyboru **Zastęp ustawienia wspólne**.
  - Skojarz telefony z tym wspólnym profilem telefonów za pomocą opcji **Urządzenie > Telefon**.
- Krok 3** Aby włączyć obsługę bezprzewodowej sieci LAN dla wszystkich telefonów z tą funkcjonalnością istniejących w firmowej sieci:
- Wybierz kolejno opcje **System > Konfiguracja telefonu przedsiębiorstwa**.
  - Wybierz dla parametru Wi-Fi wartość **Włączone**.
- Uwaga** Aby upewnić się, że konfiguracja działa w tym kroku, usuń zaznaczenie pola wyboru **Zastęp ustawienia wspólne** opisanego w kroku 1d i 2c.
- Zaznacz pole wyboru **Zastęp ustawienia wspólne**.

## Konfigurowanie bezprzewodowej sieci LAN z telefonu

Aby telefon IP Cisco mógł się łączyć z siecią WLAN, należy skonfigurować profil sieci dla telefonu z odpowiednimi ustawieniami sieci WLAN. W telefonie można z menu **Konfiguracja sieci** przejść do podmenu **Konfiguracja klienta Wi-Fi** i skonfigurować ustawienia sieci WLAN.



**Uwaga** Port komputera w telefonie jest wyłączony, gdy w telefonie włączona jest sieć Wi-Fi.



**Uwaga** Opcja **Konfiguracja klienta Wi-Fi** nie jest wyświetlana w menu **Konfiguracja sieci**, gdy w programie Cisco Unified Communications Manager wyłączono funkcję sieci Wi-Fi.


Dodatkowe informacje można znaleźć w *Podręczniku wdrażania dostępu do sieci WLAN na urządzeniach IP Cisco z serii 8800* pod następującym adresem: <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>.

Pole **Użytkownik może modyfikować** w profilu bezprzewodowej sieci LAN decyduje o możliwości konfigurowania trybów zabezpieczeń w telefonie przez użytkownika. Gdy użytkownik nie może zmieniać niektórych pól, są one wyszarzone.

### Zanim rozpoczniesz

W programie Cisco Unified Communications Manager można skonfigurować bezprzewodową sieć LAN.

### Procedura

- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja klienta Wi-Fi**.
- Krok 3** Skonfiguruj ustawienia sieci bezprzewodowej w sposób opisany w poniższej tabeli.

*Tabela 19: Opcje menu Konfiguracja klienta Wi-Fi*

Opcja	Opis	Aby zmienić
Nazwa sieci	Określa identyfikator zestawu usług — unikatowy identyfikator umożliwiający korzystanie z punktów dostępu bezprzewodowego. Wyświetla listę dostępnych punktów dostępu bezprzewodowego.	Zobacz <a href="#">Konfigurowanie ustawień sieci na stronie 59</a> .
Konfiguracja tylko IPv4	W podmenu Konfiguracja protokołu IPv4 można wykonać następujące czynności: <ul style="list-style-type: none"> <li>• Włączenie lub wyłączenie używania przez telefon adresu IP przypisanego przez serwer DHCP.</li> <li>• Ręczne ustawienie adresu IP, maski podsieci, domyślnych routerów, serwera DNS i alternatywnych serwerów TFTP.</li> </ul> Aby uzyskać więcej informacji o polach adresu IPv4, zobacz <a href="#">Pola protokołu IPv4, na stronie 61</a> .	Przewiń do opcji Konfiguracja protokołu i naciśnij przycisk <b>Wybierz</b> .



Opcja	Opis	Aby zmienić
Konfiguracja tylko IPv6	<p>W podmenu Konfiguracja protokołu IPv6 można wykonać następujące czynności:</p> <ul style="list-style-type: none"> <li>• Włączenie lub wyłączenie używania przez telefon adresu IPv6 przypisanego przez serwer DHCPv6 lub pobranego przez mechanizm SLAAC za pośrednictwem routera obsługującego protokół IPv6.</li> <li>• Ręczne ustawienie adresu IPv6, długości prefiksu, domyślnych routerów, serwera DNS i alternatywnych serwerów TFTP.</li> </ul> <p>Aby uzyskać więcej informacji o polach adresu IPv6, zobacz <a href="#">Pola protokołu IPv6, na stronie 63</a>.</p>	Przewiń do opcji Konfiguracja protokołu IPv6 i naciśnij przycisk <b>Wybierz</b> .
Adres MAC	Unikatowy adres MAC (Media Access Control) telefonu.	Tylko wyświetlanie. Opcji tej nie można konfigurować.
Nazwa domeny	Nazwa domeny, w której znajduje się telefon, w systemie DNS (ang. Domain Name System, system nazw domen).	Zobacz <a href="#">Konfigurowanie ustawień DNS, na stronie 59</a> .

**Krok 4** Naciśnij przycisk **Zapisz**, aby dokonać zmian, lub przycisk **Przywróć**, aby odrzucić połączenie.

## Ustaw liczbę prób uwierzytelniania sieci WLAN

Żądanie uwierzytelnienia jest potwierdzeniem poświadczeń logowania użytkownika. Takie żądanie występuje wówczas, gdy telefon, który jest już podłączony do sieci Wi-Fi, podejmuje próbę nawiązania połączenia z serwerem Wi-Fi. Dzieje się tak na przykład po upływie limitu czasu sesji Wi-Fi lub po utracie i ponownym uzyskaniu połączenia Wi-Fi.

Można skonfigurować liczbę żądań uwierzytelnienia wysyłanych przez telefon Wi-Fi do serwera Wi-Fi. Domyślna liczba prób to 2, ale można ustawić ten parametr w zakresie od 1 do 3. Jeśli uwierzytelnienie telefonu nie powiedzie się, użytkownik zostanie poproszony o ponowne zalogowanie się.

Liczbę prób uwierzytelniania sieci WLAN można ustawić dla poszczególnych telefonów, dla puli telefonów lub dla wszystkich telefonów Wi-Fi w sieci.

### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Telefon** i zlokalizuj telefon.
- Krok 2** Przejdź do obszaru Konfiguracja specyficzna dla produktu i ustaw wartość w polu **Próby uwierzytelniania sieci WLAN**.
- Krok 3** Kliknij przycisk **Zapisz**.
- Krok 4** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).

**Krok 5** Uruchom ponownie telefon.

---

## Włączanie trybu monitu sieci WLAN

Włącz tryb monitu profilu sieci WLAN 1, jeśli chcesz, aby użytkownik logował się do sieci Wi-Fi po włączeniu lub zresetowaniu telefonu.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
  - Krok 2** Odszukaj telefon, który chcesz skonfigurować.
  - Krok 3** Przejdź do obszaru Konfiguracja specyficzna dla produktu i w polu **Tryb monitu profilu sieci WLAN 1** wybierz opcję **Włącz**.
  - Krok 4** Kliknij przycisk **Zapisz**.
  - Krok 5** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
  - Krok 6** Uruchom ponownie telefon.
- 

## Konfigurowanie profilu Wi-Fi za pomocą programu Cisco Unified Communications Manager

Można skonfigurować profil Wi-Fi, a następnie przypisać go do telefonów, które obsługują łączność Wi-Fi. Profil zawiera parametry wymagane przez telefony do łączenia się z programem Cisco Unified Communications Manager z siecią Wi-Fi. Po utworzeniu i użyciu profilu Wi-Fi nie ma potrzeby konfigurowania sieci bezprzewodowej dla poszczególnych telefonów.

Profile Wi-Fi są obsługiwane w programie Cisco Unified Communications Manager w wersji 10.5(2) lub nowszych. W programie Cisco Unified Communications Manager w wersji 10.0 i nowszych są obsługiwane są protokoły EAP-FAST, PEAP-GTC i PEAP-MSCHAPv2. W programie Cisco Unified Communications Manager w wersji 11.0 i nowszych jest obsługiwany protokół EAP-TLS.

Profil Wi-Fi pozwala zapobiec zmianom w konfiguracji sieci Wi-Fi telefonu przez użytkownika lub je ograniczyć.

Zalecamy używanie bezpiecznego profilu z włączonym szyfrowaniem TFTP do ochrony kluczy i haseł podczas korzystania z profilu Wi-Fi.

Po skonfigurowaniu telefonów do korzystania z uwierzytelniania EAP-FAST, PEAP-MSCHAPv2 lub PEAP-GTC użytkownicy będą potrzebowali indywidualnych identyfikatorów użytkownika i haseł, aby zalogować się do telefonu.

Telefony obsługują tylko jeden certyfikat serwera, który można zainstalować przy użyciu protokołu SCEP lub metodą ręcznej instalacji, ale nie za pomocą obu tych metod. Telefony nie obsługują instalacji certyfikatu przy użyciu protokołu TFTP.



**Uwaga** W telefonach, które korzystają z usług mobilnego i zdalnego dostępu (Mobile and Remote Access) za pośrednictwem usługi Expressway w celu połączenia z programem Cisco Unified Communications Manager, nie można używać profilu sieci Wi-Fi. Ponieważ użytkownik nie posiada identyfikatora SSID, trybu uwierzytelniania ani poświadczeń logowania użytkownika telefonu, nie może skonfigurować profilu bezprzewodowej sieci LAN dla swojego telefonu.

## Procedura

- Krok 1** W aplikacji Cisco Unified Communications — administracja wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Profil bezprzewodowej sieci LAN**.
- Krok 2** Kliknij opcję **Dodaj nową**.
- Krok 3** W sekcji **Informacje o profilu bezprzewodowej sieci LAN** ustaw parametry:
- **Nazwa** — wprowadź unikatową nazwę profilu sieci Wi-Fi. Ta nazwa jest wyświetlana na telefonie.
  - **Opis** — wprowadź opis profilu sieci Wi-Fi, aby ułatwić odróżnienie tego profilu od innych profili sieci Wi-Fi.
  - **Użytkownik może modyfikować** — wybierz opcję:
    - **Dozwolone** — wskazuje, że użytkownik może dokonywać zmian w ustawieniach sieci Wi-Fi ze swojego telefonu. Ta opcja jest wybrana domyślnie.
    - **Niedozwolone** — wskazuje, że użytkownik nie może dokonywać żadnych zmian w ustawieniach sieci Wi-Fi na swoim telefonie.
    - **Ograniczone** — wskazuje, że użytkownik może zmienić nazwę użytkownika sieci Wi-Fi oraz hasło na swoim telefonie. Jednak użytkownicy nie mogą na telefonie wprowadzać zmian innych ustawień sieci Wi-Fi.
- Krok 4** W sekcji **Ustawienia sieci bezprzewodowej** ustaw parametry:
- **SSID (nazwa sieci)** — wprowadź nazwę sieci dostępną w środowisku użytkownika, z którym telefon może się połączyć. Ta nazwa jest wyświetlana na liście dostępnych sieci na telefonie, a telefon może łączyć się z tą siecią bezprzewodową.
  - **Pasma częstotliwości** — dostępne opcje to Automatyczne, 2,4 GHz i 5 GHz. To pole określa pasmo częstotliwości używane w komunikacji bezprzewodowej. Jeśli wybrano opcję Automatyczne, telefon próbuje najpierw użyć pasma częstotliwości 5 GHz, a pasma 2,4 GHz używa tylko wtedy, gdy pasmo częstotliwości 5 GHz nie jest dostępne.
- Krok 5** W sekcji **Ustawienia uwierzytelniania** ustaw wartość opcji **Metoda uwierzytelniania** na jedną z następujących metod uwierzytelniania: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP lub Brak.
- Po skonfigurowaniu tego pola mogą zostać wyświetlone inne pola wymagające ustawienia.
- **Certyfikat użytkownika** — wymagane dla protokołu uwierzytelniania EAP-TLS. Wybierz opcję **Zainstalowane fabrycznie** lub **Zainstalowane przez użytkownika**. Telefon wymaga zainstalowania

certyfikatu w sposób automatyczny z protokołu SCEP albo ręcznie z poziomu strony administrowania na telefonie.

- **Hasło PSK** — wymagane w przypadku uwierzytelniania PSK. Wprowadź ciąg o długości 8–63 znaków ASCII lub hasło złożone z 64 znaków szesnastkowych.
- **Klucz WEP** — wymagane w przypadku uwierzytelniania WEP. Wprowadź klucz ASCII albo szesnastkowy klucz WEP o długości 40/104 bitów lub 64/128 bitów.
  - Klucz ASCII 40/104 zawiera 5 znaków.
  - Klucz ASCII 64/128 zawiera 13 znaków.
  - Szesnastkowy klucz 40/104 zawiera 10 znaków.
  - Szesnastkowy klucz 64/128 zawiera 26 znaków.
- **Zapewnij wspólne poświadczenia:** wymagane dla uwierzytelniania EAP-FAST, PEAP-MSCHAPv2 i PEAP-GTC.
  - Jeśli użytkownik zarządza nazwą użytkownika i hasłem, należy pozostawić pola **Nazwa użytkownika** i **Hasło** puste.
  - Jeśli wszyscy użytkownicy współdzielą taką samą nazwę użytkownika i hasło, można wprowadzić te dane w polach **Nazwa użytkownika** i **Hasło**.
  - Wprowadź opis w polu **Opis hasła**.

**Uwaga** Jeśli zachodzi potrzeba, aby każdemu użytkownikowi przypisać unikatową nazwę użytkownika i hasło, należy utworzyć profil dla każdego użytkownika.

**Uwaga** Pole **Profil dostępu do sieci** nie jest obsługiwane w telefonach IP Cisco 8861 i 8865.

**Krok 6** Kliknij przycisk **Zapisz**.

#### Co dalej

Zastosuj Grupę profilu sieci WLAN do puli urządzeń (**System > Pula urządzeń**) lub bezpośrednio do telefonu (**Urządzenie > Telefon**).

## Konfigurowanie grupy Wi-Fi za pomocą programu Cisco Unified Communications Manager

Można utworzyć grupę profili bezprzewodowych sieci LAN i dodać do niej dowolne profile bezprzewodowych sieci LAN. Następnie grupę profili można przypisać do telefonu podczas jego konfigurowania.

#### Procedura


**Krok 1** W aplikacji Cisco Unified Communications — administracja wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Grupa profili bezprzewodowych sieci LAN**.

Można również zdefiniować grupę profili bezprzewodowych sieci LAN z okna **System > Pula urządzeń**.

- Krok 2** Kliknij opcję **Dodaj nową**.
- Krok 3** W sekcji **Informacje o grupie profili bezprzewodowych sieci LAN** wprowadź nazwę grupy i opis.
- Krok 4** W sekcji **Profile tej grupy profili bezprzewodowych sieci LAN** wybierz dostępny profil z listy **Dostępne profile** i przenieś go na listę **Wybrane profile**.
- W przypadku wybrania więcej niż jednego profilu bezprzewodowej sieci LAN telefon korzysta tylko z pierwszego profilu.
- Krok 5** Kliknij przycisk **Zapisz**.

## Konfigurowanie ustawień sieciowych

### Procedura

- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Aby uzyskać dostęp do menu Ustawienia sieciowe, wybierz opcję **Ustawienia admin. > Konfiguracja sieci Ethernet**.
- Krok 3** Ustaw pola zgodnie z opisem w [Pola konfiguracji sieci Ethernet, na stronie 59](#).
- Krok 4** Po ustawieniu pól wybierz kolejno opcje **Zastosuj** i **Zapisz**.
- Krok 5** Ponownie uruchom telefon.

## Pola konfiguracji sieci Ethernet

W menu Konfiguracja sieci znajdują się pola i podmenu dotyczące ustawień protokołów IPv4 i IPv6. Aby zmienić niektóre pola, należy najpierw wyłączyć protokół DHCP.

Ustanowienie połączenia VPN powoduje zastąpienie ustawień pól danych sieci Ethernet.

**Tabela 20: Opcje menu Konfiguracja sieci Ethernet**

Trasy	Typ	Opis
Konfiguracja protokołu IPv4	Menu	Patrz sekcja Pola protokołu IPv4. Ta opcja jest dostępna tylko wtedy, gdy telefon jest skonfigurowany w z protokołu IPv4 lub w trybie protokołów IPv4 i IPv6.
Konfiguracja protokołu IPv6	Menu	Patrz sekcja Pola protokołu IPv6.
Adres MAC	Ciąg	Unikatowy adres MAC (Media Access Control) telefonu. Tylko wyświetlanie. Opcji tej nie można konfigurować.

Trasy	Typ	Opis
Nazwa domeny	Ciąg	Nazwa domeny, w której znajduje się telefon, w systemie DNS (ang. Domain Name System, DNS). Aby zmienić to pole, wyłącz DHCP.
Aktywny VLAN ID		Pomocnicza wirtualna sieć lokalna (ang. Virtual Local Area Network, VLAN) przełącznika Cisco Catalyst, do której należy telefon. To ustawienie jest puste, jeśli skonfigurowano pomocniczą sieć VLAN 1. Jeśli telefon nie odebrał pomocniczej sieci VLAN, opcja ta wskazuje adres IP. Telefon nie przejmie aktywnej sieci VLAN od administracyjnej sieci VLAN. Aby uzyskać więcej informacji, zobacz protokół Cisco Discovery Protocol (CDP) lub protokół Link Level Discovery (LLDP-MED). Aby ręcznie przypisać identyfikator VLAN, należy użyć opcji administracyjnej sieci VLAN.
Administracyjny VLAN ID		Pomocnicza sieć VLAN, do której należy telefon. Używana tylko wtedy, gdy przełącznik nie powiadomi telefonu o pomocy. W przeciwnym razie ta wartość jest ignorowana.
PC VLAN		Umożliwia ustawienie telefonu do współpracy z przełącznikami innych firm. Ustawienie to umożliwia sieci VLAN komunikacji głosowej. Przed zmianą tej opcji należy ustawić identyfikator sieci VLAN.
Konfiguracja portu SW	Automatyczna negocjacja 1000 pełny 100 half 10 half 10 full	Prędkość i tryb duplex portu sieci. Prawidłowe wartości oznaczają: <ul style="list-style-type: none"> <li>• Automatyczna negocjacja (domyślnie)</li> <li>• 1000 pełny: 1000-BaseT/pełny duplex</li> <li>• 100 pół: 100-BaseT/półduplex</li> <li>• 100 pełny: 100-BaseT/pełny duplex</li> <li>• 10 pół: 10-BaseT/półduplex</li> <li>• 10 pełny: 10-BaseT/pełny duplex</li> </ul> <p>Jeśli telefon jest podłączony do przełącznika, skonfiguruj w porcie przełącznika tryb duplex jak w telefonie, lub skonfiguruj automatyczną negocjację w obu urządzeniach.</p> <p>Jeśli chcesz edytować to ustawienie, odblokuj opcje konfiguracji sieci. Po wybraniu opcji należy nadać taką samą wartość opcji Konfiguracja portu komputera.</p>

Trasy	Typ	Opis
Konfiguracja portu PC	Automatyczna negocjacja 1000 pełny 100 half 10 half 10 full	<p>Prędkość i tryb dupleks portu komputera (dostępowego). Prawdopodobnie</p> <ul style="list-style-type: none"> <li>• Automatyczna negocjacja (domyślnie)</li> <li>• 1000 pełny: 1000-BaseT/pełny dupleks</li> <li>• 100 pół: 100-BaseT/półdupleks</li> <li>• 100 pełny: 100-BaseT/pełny dupleks</li> <li>• 10 pół: 10-BaseT/półdupleks</li> <li>• 10 pełny: 10-BaseT/pełny dupleks</li> </ul> <p>Jeśli telefon jest podłączony do przełącznika, skonfiguruj w porcie przełącznika jak w telefonie, lub skonfiguruj automatyczną negocjację w obu urządzeniach.</p> <p>Jeśli chcesz zmienić to pole, odblokuj opcje konfiguracji sieci. Po zmianie nadeń taką samą wartość opcji Konfiguracja portu programowego.</p> <p>Aby jednocześnie skonfigurować ustawienia w kilku telefonach, włącz opcję w oknie Konfiguracja telefonu przedsiębiorstwa (<b>System &gt; Konfiguracja</b>).</p> <p>Jeśli porty są skonfigurowane w programie Cisco Unified Communications Manager, konfiguracja portu, nie można zmienić danych w telefonie.</p>

## Pola protokołu IPv4

Tabela 21: Opcje menu Konfiguracja protokołu IPv4

Trasy	Opis
Protokół DHCP włączony	<p>Wskazuje, czy w telefonie protokół DHCP jest włączony lub wyłączony.</p> <p>Jeśli protokół DHCP jest włączony, serwer DHCP przypisze do telefonu adres IP. Jeśli protokół DHCP jest wyłączony, administrator musi ręcznie przypisać adres IP do telefonu.</p> <p>Aby uzyskać więcej informacji, patrz <a href="#">Konfigurowanie telefonu do korzystania z protokołu DHCP, na stronie 65</a> i <a href="#">Konfigurowanie telefonu do niekorzystania z protokołu DHCP, na stronie 65</a>.</p>
Adres IP	<p>Adres IP (ang. Internet Protocol, protokół internetowy) telefonu.</p> <p>Po przypisaniu adresu IP za pomocą tej opcji należy również przypisać maskę podsieci i domyślny router. Zobacz opcje Maska podsieci i Router domyślny w tej tabeli.</p>
Maska podsieci	Maska podsieci używana przez telefon.
Router domyślny	Router domyślny używany przez telefon.
Serwer DNS 1 Serwer DNS 2 Serwer DNS 3	Podstawowy serwer DNS (Serwer DNS 1) i opcjonalne zapasowe serwery DNS (Serwer DNS 2 i 3), z których korzysta telefon.
Alternatywny serwer TFTP	Wskazuje, czy telefon korzysta z alternatywnego serwera TFTP.

Trasy	Opis
Serwer TFTP 1	<p>Podstawowy serwer TFTP (ang. Trivial File Transfer Protocol, trywialny protokół przesyłania plików), z którego korzysta telefon. Jeśli nie używasz protokołu DHCP w sieci i chcesz zmienić ten serwer, musisz użyć opcji Serwer TFTP 1.</p> <p>Jeśli została włączona opcja Alternatywny serwer TFTP, należy wprowadzić wartość niezerową opcji Serwer TFTP 1.</p> <p>Jeśli ani podstawowy, ani zapasowy serwer TFTP nie znajduje się w pliku CTL lub ITL na telefonie, należy odblokować plik, aby można było zapisać zmiany opcji Serwer TFTP 1. W takim przypadku telefon usuwa plik podczas zapisywania zmian opcji Serwer TFTP 1. Nowy plik CTL lub ITL pobiera nowy adres serwera TFTP 1.</p> <p>Podczas poszukiwania serwera TFTP telefon daje pierwszeństwo ręcznie przypisanym serwerom TFTP, niezależnie od protokołu. Jeśli konfiguracja serwerów zawiera zarówno serwery TFTP IPv6, jak i IPv4, telefon najpierw poszukuje przypisanych ręcznie serwerów TFTP IPv6, a następnie serwerów TFTP IPv4. Telefon szuka serwera TFTP w następującej kolejności:</p> <ol style="list-style-type: none"><li>1. Wszystkie ręcznie przypisane serwery TFTP IPv4</li><li>2. Wszystkie ręcznie przypisane serwery IPv6</li><li>3. Serwery TFTP przypisane przez DHCP</li><li>4. Serwery TFTP przypisane przez DHCPv6</li></ol> <p><b>Uwaga</b> Informacje o plikach CTL i ITL można znaleźć w podręczniku <i>Cisco Unified Communications Manager Security Guide</i> (Podręcznik zabezpieczeń programu Cisco Unified Communications Manager).</p>



Trasy	Opis
Serwer TFTP 2	<p>Opcjonalny serwer TFTP kopii zapasowej używany przez telefon, gdy podstawowy serwer TFTP nie jest dostępny.</p> <p>Jeśli ani podstawowy, ani zapasowy serwer TFTP nie znajduje się w pliku CTL lub ITL na telefonie, należy odblokować dowolny z plików, aby można było zapisać zmiany opcji Serwer TFTP 2. W takim przypadku telefon usuwa jeden z plików podczas zapisywania zmian opcji Serwer TFTP 2. Nowy plik CTL lub ITL pobiera nowy adres serwera TFTP 2.</p> <p>Jeśli użytkownik zapomni odblokować plik CTL lub ITL, można zmienić adres serwera TFTP 2 w dowolnym pliku, a następnie skasować go, wybierając polecenie Kasuj z menu Konfiguracja zabezpieczeń. Nowy plik CTL lub ITL pobiera nowy adres serwera TFTP 2.</p> <p>Podczas poszukiwania serwera TFTP telefon daje pierwszeństwo ręcznie przypisanym serwerom TFTP, niezależnie od protokołu. Jeśli konfiguracja serwerów zawiera zarówno serwery TFTP IPv6, jak i IPv4, telefon najpierw poszukuje przypisanych ręcznie serwerów TFTP IPv6, a następnie serwerów TFTP IPv4. Telefon szuka serwera TFTP w następującej kolejności:</p> <ol style="list-style-type: none"> <li>1. Wszystkie ręcznie przypisane serwery TFTP IPv4</li> <li>2. Wszystkie ręcznie przypisane serwery IPv6</li> <li>3. Serwery TFTP przypisane przez DHCP</li> <li>4. Serwery TFTP przypisane przez DHCPv6</li> </ol> <p><b>Uwaga</b> Informacje o plikach CTL i ITL można znaleźć w podręczniku Cisco Unified Communications Manager Security Guide (Podręcznik zabezpieczeń programu Cisco Unified Communications Manager).</p>
Serwer BOOTP	Wskazuje, czy telefon odbiera adres IP z serwera BOOTP zamiast z serwera DHCP.
Adres DHCP zwolniony	<p>Udostępnia adres IP przypisany przez serwer DHCP.</p> <p>To pole można edytować, jeśli jest włączona usługa DHCP. Aby usunąć telefon z sieci VLAN i udostępnić adres IP do następnego przydzielenia, ustaw tę opcję na Tak i naciśnij przycisk Zastosuj.</p>

## Pola protokołu IPv6

Aby umożliwić konfigurację opcji protokołu IPv6 na urządzeniu, należy włączyć i skonfigurować obsługę protokołu IPv6 w programie Cisco Unified Communication — administracja. Następujące pola konfiguracji urządzenia dotyczą konfiguracji protokołu IPv6:

- Tryb adresowania IP
- Ustawienie trybu adresowania IP do sygnalizowania

Jeśli protokół IPv6 zostanie włączony w klastrze Unified, domyślnym trybem adresowania IP jest IPv4 i IPv6. W tym trybie adresowania telefon pozyskuje i stosuje jeden adres IPv4 i jeden adres IPv6. Zgodnie z wymaganiami w zakresie mediów może on używać adresu IPv4 i IPv6. Do sygnalizowania sterowania połączeniami telefon używa albo adresu IPv4, albo IPv6.

Aby uzyskać więcej informacji na temat wdrażania protokołu IPv6, zobacz [IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0](#).

Protokół IPv6 można skonfigurować w jednym z następujących menu:

- Gdy sieć Wi-Fi jest wyłączona: **Konfiguracja sieci Ethernet > Konfiguracja protokołu IPv6**
- Gdy sieć Wi-Fi jest włączona: **Konfiguracja klienta Wi-Fi > Konfiguracja protokołu IPv6**

Wpisz lub edytuj adres IPv6 przy użyciu klawiatury telefonu. Aby wprowadzić dwukropek, naciśnij klawisz gwiazdki (\*) na klawiaturze numerycznej. Aby wprowadzić cyfry szesnastkowe a, b i c, naciśnij przycisk 2 na klawiaturze numerycznej, przewiń listę i wybierz wymaganą cyfrę, a następnie naciśnij klawisz **Enter**. Aby wprowadzić cyfry szesnastkowe d, e i f, naciśnij przycisk 3 na klawiaturze numerycznej, przewiń listę i wybierz wymaganą cyfrę, a następnie naciśnij klawisz **Enter**.

W poniższej tabeli zamieszczono informacje dotyczące protokołu IPv6 znajdujące się w menu IPv6.

**Tabela 22: Opcje menu Konfiguracja protokołu IPv6**


Trasy	Wartość domyślna	Opis
Protokół DHCPv6 włączony	Tak	Wskazuje metodę wykorzystywaną przez telefon. Gdy protokół DHCPv6 jest włączony, telefon otrzymuje adres IP za pomocą komunikatu RA wysłanego przez serwer. Jeśli telefon nie uzyska żadnego stanowego adresu IP, telefon może uzyskać adres IP z serwera DHCPv6.
Adres IPv6	::	Podaje bieżący adres protokołu tylko IPv6. Prawidłowy adres IPv6 ma długość 128 bitów. <ul style="list-style-type: none"> <li>• Osiem zestawów cyfr szesnastkowych</li> <li>• Skompresowany format umożliwiający wyłączenie niepotrzebnych zer reprezentowaną przez podwójny kropkę (::)</li> </ul> Jeśli adres IP jest przypisywany po wybraniu adresu IP, telefon może uzyskać adres IP z serwera DHCPv6.
Długość prefiksu IPv6	0	Podaje bieżącą długość prefiksu podsieci IPv6. Długość prefiksu podsieci to wartość od 0 do 64.
Domyślny router prot.	::	Wskazuje router domyślny, z którego telefon może uzyskać adres IP domyślnego protokołu tylko IPv6.
Serwer DNS 1 IPv6	::	Wskazuje podstawowy serwer DNSv6, z którego telefon może uzyskać adres IP serwera.
Serwer DNS 2 IPv6	::	Wskazuje pomocniczy serwer DNSv6, z którego telefon może uzyskać adres IP pomocniczego serwera DNSv6.
Alternat. serwer TFTP IPv6	Nie	Umożliwia użytkownikowi włączanie alternatywnego podstawowego serwera TFTP.
Serwer TFTP 1 IPv6	::	Wskazuje podstawowy serwer TFTP IPv6, z którego telefon może uzyskać nowego podstawowego serwera TFTP.

Trasy	Wartość domyślna	Opis
Serwer TFTP 2 IPv6	::	(Opcjonalny) Wskazuje pomocniczy adres IP, który jest niedostępny, oraz umożliwia u
Adres IPv6 zwolniony	Nie	Umożliwia użytkownikowi udostęp

## Konfigurowanie telefonu do korzystania z protokołu DHCP

Aby włączyć protokół DHCP i umożliwić serwerowi DHCP automatyczne przypisywanie adresu IP do telefonu IP Cisco oraz przekierowanie telefonu do serwera TFTP, należy wykonać następujące czynności:


### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja sieci Ethernet** > **Konfiguracja protokołu IPv4**.
- Krok 3** Aby włączyć serwer DHCP, nadaj opcji Włączona usługa DHCP wartość **Tak**. Protokół DHCP jest domyślnie włączony.
- Krok 4** Aby skorzystać z alternatywnego serwera TFTP, nadaj opcji Alternatywny serwer TFTP wartość **Taki** i wprowadź adres IP serwera TFTP.
- Uwaga** Skonsultuj się z administratorem sieci, aby określić, czy należy przypisywać alternatywny serwer TFTP zamiast korzystać z serwera TFTP przypisanego przez protokół DHCP.
- Krok 5** Naciśnij przycisk **Zastosuj**.
- 

## Konfigurowanie telefonu do niekorzystania z protokołu DHCP

Jeśli nie jest używany protokół DHCP, konieczne jest skonfigurowanie lokalnie w telefonie adresu IP, maski podsieci, serwera TFTP i routera domyślnego.

### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja sieci Ethernet** > **Konfiguracja protokołu IPv4**.
- Krok 3** Aby wyłączyć protokół DHCP i ręcznie ustawić adres IP:
- Ustaw wartość opcji DHCP włączone na **Nie**.
  - Wprowadź statyczny adres IP dla telefonu.
  - Wpisz maskę podsieci.
  - Wprowadź adresy IP domyślnego routera.

- e) Ustaw wartość opcji Alternatywny serwer TFTP na **Taki** wprowadź adres IP dla w opcji Serwer TFTP 1.

**Krok 4** Naciśnij przycisk **Zastosuj**.

---

## Serwer pobierania

Serwer pobierania służy do optymalizowania pory instalacji uaktualnień oprogramowania sprzętowego telefonu i zmniejszania obciążenia sieci WAN poprzez lokalne przechowywanie obrazów, które eliminuje konieczność przesyłania ich łączem WAN przy każdym uaktualnianiu telefonu.

Serwer pobierania można ustawić na inny adres IP lub nazwę serwera TFTP (inny niż serwer TFTP 1 lub serwer TFTP 2), z którego można pobierać oprogramowanie sprzętowe telefonu podczas aktualizacji. Po ustawieniu opcji serwera pobierania telefon łączy się z wyznaczonym serwerem w celu aktualizacji oprogramowania sprzętowego.



**Uwaga** Opcja Serwer pobierania umożliwia podanie alternatywnego serwera TFTP przeznaczonego wyłącznie do uaktualnień telefonu. Telefon nadal pobiera pliki konfiguracyjne z serwerów TFTP 1 TFTP 2. Opcja Serwer pobierania nie umożliwia zarządzania procesem ani plikami, np. przesyłaniem plików, ich kompresją lub usuwaniem.

---

Serwer pobierania można konfigurować w oknie Konfiguracja telefonu. W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon > Konfiguracja telefonu przedsiębiorstwa**.

## Sprawdzenie przy uruchamianiu telefonu

Po podłączeniu zasilania do telefonu IP Cisco rozpoczyna się proces diagnostyki uruchamiania, składający się z następujących czynności.

1. Podczas sprawdzania sprzętu telefonu przyciski Funkcja i Sesja migają początkowo na żółto, a potem na zielono w zależności od etapu procesu.
2. Na ekranie głównym jest wyświetlany tekst Rejestracja w programie do Cisco Unified Communications Manager.

Jeśli te etapy zakończą się pomyślnie, oznacza to prawidłowe uruchomienie telefonu i przycisk **Wybierz** pozostaje zapalony aż do jego wybrania.

## Konfigurowanie usług telefonicznych dla użytkowników

Można przyznawać użytkownikom dostęp do usług telefonu IP Cisco. Można też przypisywać poszczególne usługi telefoniczne do osobnych przycisków. Usługi te obejmują aplikacje XML oraz aplikacje midlet w języku Java podpisane przez firmę Cisco, umożliwiające wyświetlanie interaktywnych treści tekstowych i

graficznych na telefonie. Telefon IP traktuje każdą usługę jak oddzielną aplikację. Przykładowymi usługami są godziny rozpoczęcia filmów, notowania giełdowe i prognozy pogody.

Zanim użytkownik będzie mógł skorzystać z jakiegokolwiek usługi:

- Należy za pomocą aplikacji Cisco Unified Communications Manager — administracja skonfigurować usługi, które nie są domyślnie dostępne.
- Użytkownik musi abonować usługi za pomocą portalu Portal Self Care Cisco Unified Communications. Ta aplikacja internetowa udostępnia graficzny interfejs użytkownika do konfigurowania w ograniczonym zakresie aplikacji dostępnych w telefonie IP. Użytkownik nie może jednak abonować żadnej usługi, która jest skonfigurowana w ramach subskrypcji firmowej.

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Przed skonfigurowaniem usług należy zebrać adresy URL witryn, które mają wejść w skład konfiguracji, i sprawdzić, czy użytkownicy mają do nich dostęp z poziomu firmowej sieci telefonii IP. Czynność ta nie dotyczy domyślnych usług oferowanych przez firmę Cisco.

### Procedura

**Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Usługi telefoniczne**

**Krok 2** Sprawdź, czy użytkownicy mają dostęp do portalu Portal Self Care Cisco Unified Communications, w którym mogą wybierać i abonować skonfigurowane usługi.

Zestawienie informacji, które należy podać użytkownikom końcowym, można znaleźć w części [Zarządzanie portalem samoobsługowym, na stronie 83](#).

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Zmień model telefonu użytkownika

Można zmienić model telefonu użytkownika. Zmiana może być wymagana z kilku powodów, na przykład:

- Cisco Unified Communications Manager (Unified CM) zaktualizowano do wersji oprogramowania, która nie obsługuje modelu telefonu.
- Użytkownik chce mieć inny model telefonu niż jego obecny model.
- Telefon wymaga naprawy lub wymiany.

Unified CM identyfikuje stary telefon i używa adresu MAC starego telefonu do identyfikowania konfiguracji starego telefonu. Unified CM kopiuje starą konfigurację telefonu do wpisu dla nowego telefonu. Nowy telefon ma taką samą konfigurację jak stary telefon.

W przypadku zmiany starego telefonu z oprogramowaniem sprzętowym SCCP na model w Telefon IP Cisco z serii 8800 nowy telefon zostanie skonfigurowany do pracy w trybie linii sesji.

Jeśli w starym telefonie jest skonfigurowany model ekspansji, system Unified CM jednocześnie kopiuje informacje do nowego telefonu. Gdy użytkownik łączy się z nowym telefonem za pomocą zgodnego z nim modułu rozbudowy klawiatury, w nowym module rozszerzeń zostaną odebrane informacje o zmigrowanych modułach rozszerzeń.

Jeśli w starym telefonie skonfigurowano model rozbudowy klawiatury, a nowy telefon nie obsługuje modułu rozbudowy, Unified CM nie kopiuje informacji o module rozbudowy.

**Ograniczenie:** Jeśli stary telefon ma więcej linii lub przycisków linii niż nowy telefon, nowy telefon nie ma skonfigurowanych dodatkowych linii lub klawiszy linii.

Po zakończeniu konfiguracji telefon ponownie się uruchomi.

### Zanim rozpoczniesz

Cisco Unified Communications Manager należy skonfigurować zgodnie z instrukcjami w *Podręczniku konfiguracji funkcji programu Cisco Unified Communications Manager*.

Potrzebny jest nowy, niewykorzystany telefon, który jest wstępnie zainstalowany z oprogramowaniem układowym w wersji 12,8 (1) lub nowszej.

### Procedura

---

- Krok 1** Wyłącz stary telefon.
  - Krok 2** Włącz nowy telefon.
  - Krok 3** Na nowym telefonie wybierz opcję **Zastąp istniejący telefon**.
  - Krok 4** Wprowadź główny numer wewnętrzny starego telefonu.
  - Krok 5** Jeśli stary telefon miał przypisany kod PIN, wprowadź kod PIN.
  - Krok 6** Naciśnij przycisk **Wyślij**.
  - Krok 7** Jeśli dla użytkownika dostępne jest więcej niż jedno urządzenie, należy wybrać urządzenie do zastąpienia i nacisnąć przycisk **Kontynuuj**.
-



## ROZDZIAŁ 5

# Konfigurowanie telefonu w programie Cisco Unified Communications Manager

---

- Konfigurowanie telefonu IP Cisco, na stronie 69
- Sprawdzanie adresu MAC telefonu, na stronie 72
- Metody dodawania telefonów, na stronie 73
- Dodawanie użytkowników do programu Cisco Unified Communications Manager, na stronie 74
- Dodawanie użytkownika do grupy użytkowników końcowych, na stronie 76
- Kojarzenie telefonów z użytkownikami, na stronie 77
- Survivable Remote Site Telephony, na stronie 77
- Enhanced Survivable Remote Site Telephony, na stronie 80
- Strony WWW reguł wybierania numeru aplikacji, na stronie 81

## Konfigurowanie telefonu IP Cisco

Jeśli automatyczna rejestracja jest wyłączona i telefonu nie ma w bazie danych programu Cisco Unified Communications Manager, telefon IP Cisco należy skonfigurować ręcznie w programie Cisco Unified Communications Manager. Niektóre zadania tej procedury są opcjonalne, w zależności od systemu i potrzeb użytkowników.

Więcej informacji o aplikacji Cisco Unified Communications Manager — administracja można znaleźć w dokumentacji jej konkretnej wersji.

Wykonaj czynności konfiguracyjne w następującej procedurze, korzystając z narzędzia Cisco Unified Communications Manager — administracja.

### Procedura

---

**Krok 1** Zbierz następujące informacje dotyczące telefonu:

- Model telefonu
- Adres MAC
- Fizyczna lokalizacja telefonu
- Nazwa lub identyfikator użytkownika telefonu

- Pula urządzeń
- Partycja, przestrzeń wyszukiwania połączeń i informacje o lokalizacji
- Liczba linii i powiązanych numerów telefonu przypisanych do telefonu
- Użytkownik aplikacji Cisco Unified Communications Manager, który ma zostać powiązany z telefonem
- Informacje o korzystaniu z telefonu wpływające na szablon przycisku telefonu, funkcje telefonu, usługi telefonu IP lub aplikacje telefonu

Informacje zawierają listę wymagań konfiguracyjnych dotyczących konfigurowania telefonów oraz identyfikują wstępne czynności konfiguracyjne, które należy wykonać przed rozpoczęciem konfigurowania poszczególnych telefonów, takie jak szablony przycisków telefonów.

**Krok 2** Sprawdź, czy liczba licencji jednostkowych dla telefonu jest wystarczająca.

**Krok 3** Dostosuj szablony przycisków telefonów (jeśli jest to konieczne), zmieniając liczbę przycisków linii, przycisków szybkiego wybierania i przycisków adresów URL usług. Wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Szablon przycisku telefonu**, aby utworzyć i uaktualnić szablony.

Zgodnie z potrzebami użytkownika można dodać przycisk prywatności, wszystkich połączeń lub mobilności. Aby uzyskać więcej informacji, patrz [Szablony przycisków telefonu, na stronie 207](#).

**Krok 4** Zdefiniuj pulę urządzeń. Wybierz kolejno opcje **System > Pula urządzeń**.

Pule urządzeń określają ogólne cechy urządzeń, takie jak region, grupa daty/godziny, szablon klawiszy programowych i informacje MLPP.

**Krok 5** Zdefiniuj wspólny profil telefonu. Wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**.

Wspólny profil telefonu zawiera dane wymagane przez serwer Cisco TFTP oraz wspólne ustawienia telefonów, takie jak Nie przeszkadzać i opcje kontroli funkcji.

**Krok 6** Zdefiniuj przestrzeń wyszukiwania połączeń. W aplikacji Cisco Unified Communications Manager — administracja kliknij kolejno opcje **Trasowanie połączeń > Klasa sterowania > Przestrzeń wyszukiwania połączeń**.

Przestrzeń wyszukiwania połączeń jest zbiorem partycji, które są przeszukiwane podczas określania trasowania wybranego numeru. Używana jest zarówno przestrzeń wyszukiwania połączeń dla urządzenia, jak i przestrzeń wyszukiwania połączeń dla numeru telefonu. Przestrzeń wyszukiwania połączeń numeru telefonu ma pierwszeństwo przed przestrzenią wyszukiwania połączeń urządzenia.

**Krok 7** Skonfiguruj profil zabezpieczeń dla danego typu urządzenia i protokołu. Wybierz kolejno opcje **System > Zabezpieczenia > Profil zabezpieczeń telefonu**.

**Krok 8** Dodaj i skonfiguruj telefon, uzupełniając wymagane pola w oknie Konfiguracja telefonu. Gwiazdka (\*) obok nazwy pola wskazuje pole wymagane, na przykład pola adresu MAC i puli urządzeń.

W tym kroku urządzenie z domyślnymi ustawieniami jest dodawane do bazy danych programu Cisco Unified Communications Manager.

Informacje o polach dotyczących konkretnie tego produktu zawiera "?". Przycisk pomocy w oknie konfiguracji telefonu.



**Uwaga** Więcej informacji na temat jednoczesnego dodawania telefonu i użytkownika do bazy danych programu Cisco Unified Communications Manager można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

**Krok 9** Dodaj i skonfiguruj w telefonie jego numery (linie), wypełniając odpowiednie pola w oknie Directory Number Configuration (Konfiguracja numerów telefonu). Gwiazdka (\*) obok nazwy pola wskazuje pole wymagane, na przykład pola numeru telefonu i grupy obecności.

W tym kroku do telefonu są dodawane numery telefonu — główny i pomocniczy — oraz funkcje związane z numerami telefonów.

**Uwaga** Jeśli nie skonfigurujesz głównego numeru telefonu, użytkownik zobaczy na wyświetlaczu telefonu komunikat Bez konfiguracji.

**Krok 10** Skonfiguruj przyciski szybkiego wybierania i przypisz im numery szybkiego wybierania.

Użytkownicy mogą zmieniać ustawienia szybkiego wybierania w swoich telefonach, używając Portalu samoobsługowego Cisco Unified Communications.

**Krok 11** Skonfiguruj usługi telefonu IP Cisco Unified i przypisz je (opcjonalnie), aby umożliwić świadczenie usług telefonu IP.

Użytkownicy mogą dodawać lub zmieniać usługi w swoich telefonach, używając Portalu samoobsługowego Cisco Unified Communications.

**Uwaga** Użytkownicy mogą zasubskrybować usługę telefonu IP tylko wtedy, gdy pole wyboru Subskrypcja przedsiębiorstwa nie zostanie zaznaczone podczas konfigurowania po raz pierwszy programu Cisco Unified Communications Manager — administracja.

**Uwaga** Niektóre usługi domyślne dostarczane przez firmę Cisco są klasyfikowane jako subskrypcje firmowe, dlatego użytkownik nie może ich dodawać w Portalu samoobsługowym. Takie usługi znajdują się w telefonie domyślnie i można je usunąć tylko po uprzednim wyłączeniu w aplikacji Cisco Unified Communications Manager — administracja.

**Krok 12** Przypisz usługi do klawiszy programowalnych (opcjonalnie), aby umożliwić dostęp do usługi telefonu IP lub adresu URL.

**Krok 13** Dodaj informacje o użytkowniku, konfigurując wymagane pola. Gwiazdka (\*) obok nazwy pola oznacza pole wymagane; na przykład ID użytkownika i nazwisko. Ten krok powoduje dodanie informacji o użytkowniku do globalnego katalogu programu Cisco Unified Communications Manager.

**Uwaga** Przypisz hasło (do Portalu samoobsługowego) i numer PIN (do funkcji Cisco Extension Mobility i osobistej książki adresowej).

**Uwaga** Jeśli do przechowywania informacji o użytkownikach w firmie jest używany katalog LDAP (Lightweight Directory Access), system Cisco Unified Communications można zainstalować i skonfigurować tak, aby korzystał z istniejącego katalogu LDAP.

**Uwaga** Więcej informacji na temat jednoczesnego dodawania telefonu i użytkownika do bazy danych programu Cisco Unified Communications Manager można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

- Krok 14** Skojarz użytkownika z grupą użytkowników. W tym kroku użytkownikom jest przypisywana wspólna lista ról i uprawnień, które dotyczą wszystkich użytkowników w grupie użytkowników. Administratorzy mogą zarządzać grupami użytkownika, rolami i uprawnieniami w celu kontroli poziomu dostępu (czyli poziomu zabezpieczeń) dla użytkowników systemu. Na przykład użytkowników, którzy mają mieć dostęp do Portalu samoobsługowego programu Cisco Unified Communications Manager, trzeba dodać do standardowej grupy użytkowników końcowych programu Cisco CCM.
- Krok 15** Skojarz użytkownika z telefonem (opcjonalnie). W tym kroku użytkownicy telefonów mogą sterować przekazywaniem połączeń oraz dodawaniem numerów szybkiego wybierania i usług.  
Niektóre telefony, takie jak znajdujące się w pokojach konferencyjnych, nie mają skojarzonych użytkowników.
- Krok 16** Jeśli nie jesteś jeszcze w oknie Konfiguracja użytkownika końcowego, wybierz kolejno opcje **Zarządzanie użytkownikami** > **Użytkownik końcowy** i wykonaj pewne końcowe zadania konfiguracji. Użyj pól wyszukiwania i pola **Znajdź**, aby odnaleźć użytkownika (na przykład Jan Kowalski), a następnie kliknij identyfikator użytkownika, a przejdziesz do okna Konfiguracja użytkownika końcowego dla tej osoby.
- Krok 17** W obszarze Directory Number Associations (Skojarzenia numeru telefonu) ustaw główny numer wewnętrzny, posługując się listą rozwijaną.
- Krok 18** W polu Mobility Information (Informacje o funkcji Mobility) zaznacz pole wyboru Enable Mobility (Włącz funkcję Mobility).
- Krok 19** W obszarze Permissions Information (Informacje o uprawnieniach) użyj przycisków Grupa użytkowników w celu dodania danego użytkownika do dowolnej grupy użytkowników.  
Użytkownika można dodać na przykład do grupy zdefiniowanej jako Standard CCM End User Group (Standardowa grupa CCM użytkowników końcowych).
- Krok 20** Aby wyświetlić wszystkie skonfigurowane grupy użytkowników, wybierz kolejno opcje **Zarządzanie użytkownikami** > **Grupa użytkownika**.
- Krok 21** W obszarze Extension Mobility zaznacz pole wyboru Enable Extension Mobility Cross Cluster (Włącz klaster krzyżowy przenośnego numeru wewnętrznego), jeśli użytkownik ma uprawnienie do korzystania z usługi klastra krzyżowego przenośnego numeru wewnętrznego.
- Krok 22** Kliknij przycisk **Zapisz**.

---

#### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii


## Sprawdzanie adresu MAC telefonu

Aby dodać telefon w programie Cisco Unified Communications Manager, należy sprawdzić jego adres MAC.

#### Procedura

---

Wykonaj jedną z następujących czynności:

- W telefonie naciśnij przycisk **Aplikacje** , wybierz opcję **Informacje o telefonie** i sprawdź zawartość pola Adres MAC.
- Sprawdź etykietę z adresem MAC z tyłu telefonu.

- Wyświetl stronę WWW telefonu i kliknij przycisk **Informacje o urządzeniu**.

---

## Metody dodawania telefonów

Po zainstalowaniu telefonu IP Cisco można wybrać jedną z następujących opcji dodawania telefonów do bazy danych programu Cisco Unified Communications Manager.

- Indywidualne dodawanie telefonów za pomocą narzędzia Cisco Unified Communications Manager — administracja
- Dodawanie wielu telefonów za pomocą Narzędzia administracji zbiorczej (BAT)
- Autorejestrowanie
- Narzędzie administracji zbiorczej (BAT) i Narzędzie pomocy technicznej dotyczącej telefonów autorejestrowanych (TAPS)

Aby można było dodawać telefony pojedynczo lub za pomocą narzędzia BAT, trzeba znać ich adresy MAC. Aby uzyskać więcej informacji, patrz [Sprawdzanie adresu MAC telefonu, na stronie 72](#).

Więcej informacji dotyczących Narzędzia administracji zbiorczej można znaleźć w dokumentacji konkretnej wersji programu Cisco Unified Communications Manager.

## Dodawanie telefonów pojedynczo

Należy sprawdzić adres MAC i informacje o telefonie, który ma zostać dodany do programu Cisco Unified Communications Manager.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
  - Krok 2** Kliknij opcję **Dodaj nową**.
  - Krok 3** Wybierz typ telefonu.
  - Krok 4** Wybierz **Next** (Następny).
  - Krok 5** Wypełnij informacje o telefonie, m.in. adres MAC.
- Pełne instrukcje wykonania tych czynności oraz ogólną charakterystykę programu Cisco Unified Communications Manager można znaleźć w dokumentacji jego konkretnej wersji.
- Krok 6** Kliknij przycisk **Zapisz**.

---

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Dodawanie telefonów przy użyciu szablonu telefonu narzędzia BAT

Narzędzie administracji zbiorczej (BAT) systemu Cisco Unified Communications umożliwia wykonywanie operacji wsadowych, w tym rejestrowanie wielu telefonów naraz.

Aby dodać telefony za pomocą samego narzędzia BAT (bez użycia narzędzia TAPS), trzeba mieć listę adresów MAC wszystkich dodawanych telefonów.

Więcej informacji o korzystaniu z narzędzia BAT można znaleźć w dokumentacji używanej wersji oprogramowania Cisco Unified Communications Manager.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications — administracja wybierz kolejno opcje **Administracja zbiorcza > Telefony > Szablon telefonu**.
  - Krok 2** Kliknij opcję **Dodaj nową**.
  - Krok 3** Wybierz typ telefonu i kliknij przycisk **Dalej**.
  - Krok 4** Wprowadź parametry telefonów, takie jak Pula urządzeń, Szablon przycisków telefonu i Profil zabezpieczeń urządzenia.
  - Krok 5** Kliknij przycisk **Zapisz**.
  - Krok 6** Wybierz kolejno opcje **Urządzenie > Telefon > Dodaj nowy**, aby dodać telefon za pomocą szablonu telefonów narzędzia BAT.
- 

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Dodawanie użytkowników do programu Cisco Unified Communications Manager

Informacje o użytkownikach zarejestrowanych w programie Cisco Unified Communications Manager można wyświetlać i aktualizować. Program Cisco Unified Communications Manager umożliwia również każdemu użytkownikowi wykonywanie następujących zadań:

- Dostęp za pomocą telefonu IP Cisco do firmowej książki telefonicznej i innych dostosowanych książek adresowych.
- Tworzenie osobistej książki adresowej.
- Konfigurowanie numerów szybkiego wybierania i przekierowywania połączeń.
- Subskrybowanie usług dostępnych za pomocą telefonu IP Cisco.

### Procedura

- 
- Krok 1** Aby dodawać użytkowników pojedynczo, patrz [Dodawanie użytkownika bezpośrednio do systemu Cisco Unified Communications Manager](#), na stronie 75.

- Krok 2** Aby dodawać użytkowników zbiorczo, należy skorzystać z Narzędzia administracji zbiorczej. Ta metoda umożliwia również ustawienie identycznego hasła domyślnego dla wszystkich użytkowników.
- Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

---

**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Dodawanie użytkownika z zewnętrznego katalogu LDAP

Jeśli dodano użytkownika z zewnętrznego katalogu LDAP (a nie z książki adresowej serwera Cisco Unified Communications Server), można natychmiast zsynchronizować ten katalog LDAP z serwerem Cisco Unified Communications Manager, do którego chce się dodać użytkownika i jego telefon.



- Uwaga** Jeśli nie wykona się synchronizacji Katalogu LDAP z Cisco Unified Communications Manager natychmiast, o terminie najbliższej automatycznej synchronizacji zdecyduje ustawienie opcji LDAP Directory Synchronization Schedule (Harmonogram synchronizacji z katalogiem LDAP) w oknie Katalog LDAP. Synchronizacja musi nastąpić przed skojarzeniem nowego użytkownika z urządzeniem.

---

**Procedura**

- Krok 1** Zaloguj się do aplikacji Cisco Unified Communications Manager — administracja.
- Krok 2** Wybierz kolejno opcje **System > LDAP > Katalog LDAP**.
- Krok 3** Korzystając z opcji **Znajdź**, odszukaj odpowiedni katalog LDAP.
- Krok 4** Kliknij nazwę katalogu LDAP.
- Krok 5** Kliknij przycisk **Perform Full Sync Now** (Wykonaj teraz pełną synchronizację).

---

## Dodawanie użytkownika bezpośrednio do systemu Cisco Unified Communications Manager

Jeśli nie korzysta się z katalogu LDAP (ang. Lightweight Directory Access Protocol, lekki protokół dostępu do usług katalogowych), użytkowników można dodawać bezpośrednio za pomocą aplikacji Cisco Unified Communications Manager — administracja, wykonując poniższe czynności.



- Uwaga** Jeśli natomiast stosowana jest synchronizacja z katalogiem LDAP, nie można dodawać użytkowników za pomocą aplikacji Cisco Unified Communications Manager — administracja.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Zarządzanie użytkownikami** > **Użytkownik końcowy**.
- Krok 2** Kliknij opcję **Dodaj nową**.
- Krok 3** Na panelu Informacje o użytkowniku wypełnij następujące pola:
- ID użytkownika: Wprowadź nazwę identyfikacyjną użytkownika końcowego. Program Cisco Unified Communications Manager nie pozwala na modyfikowanie identyfikatora użytkownika po jego utworzeniu. Można używać następujących znaków specjalnych: =, +, <, >, #, ;, \, ", "" oraz spacji. **Przykład:** jankowalski
  - Hasło i Potwierdź hasło: wprowadź hasło użytkownika końcowego złożone z co najmniej pięciu znaków alfanumerycznych lub specjalnych. Można używać następujących znaków specjalnych: =, +, <, >, #, ;, \, ", "" oraz spacji.
  - Nazwisko: Wprowadź nazwisko użytkownika końcowego. Można używać następujących znaków specjalnych: =, +, <, >, #, ;, \, ", "" i spacji. **Przykład:** kowalski
  - Numer telefonu: wprowadź główny numer telefonu użytkownika końcowego. Użytkownicy końcowi mogą mieć do dyspozycji w swoich telefonach wiele linii. **Przykład:** 26640 (służbowy numer wewnętrzny Jana Kowalskiego)
- Krok 4** Kliknij przycisk **Zapisz**.
- 

## Dodawanie użytkownika do grupy użytkowników końcowych

Aby dodać użytkownika do standardowej grupy użytkowników końcowych w programie Cisco Unified Communications Manager, wykonaj następujące kroki:

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Zarządzanie użytkownikami** > **Ustawienia użytkowników** > **Grupa kontroli dostępu**.
- Zostanie wyświetlone okno Find and List Users (Znajdowanie i wyświetlanie użytkowników).
- Krok 2** Wprowadź odpowiednie kryteria wyszukiwania i kliknij przycisk **Znajdź**.
- Krok 3** Wybierz link **Standardowi użytkownicy końcowi CCM**. Zostanie wyświetlone okno Konfiguracja grupy użytkowników dla standardowych użytkowników końcowych CCM.
- Krok 4** Wybierz opcję **Dodaj użytkowników końcowych do grupy**. Zostanie wyświetlone okno Znajdowanie i wyświetlanie użytkowników.
- Krok 5** Korzystając z pól listy rozwijanej Znajdź użytkownika, znajdź użytkowników, których chcesz dodać, i kliknij przycisk **Znajdź**.
- Zostanie wyświetlona lista użytkowników spełniających podane kryteria.

- Krok 6** Na wyświetlonej liście rekordów kliknij pola wyboru znajdujące się obok użytkowników, których chcesz dodać do tej grupy użytkowników. Jeśli lista jest długa, skorzystaj z linków u dołu, aby wyświetlić więcej wyników.
- Uwaga** Na liście wyników wyszukiwania nie są wyświetlani użytkownicy, którzy już należą do grupy użytkowników.
- Krok 7** Wybierz opcję **Dodaj wybrane**.
- 

## Kojarzenie telefonów z użytkownikami

Telefony można kojarzyć z użytkownikami w oknie Użytkownik końcowy programu Cisco Unified Communications Manager.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Zarządzanie użytkownikami** > **Użytkownik końcowy**.
- Zostanie wyświetlone okno Znajdowanie i wyświetlanie użytkowników.
- Krok 2** Wprowadź odpowiednie kryteria wyszukiwania i kliknij przycisk **Znajdź**.
- Krok 3** Na wyświetlonej liście rekordów wybierz łącze do użytkownika.
- Krok 4** Wybierz opcję **Device Association** (Skojarzenie urządzenia).
- Pojawi się okno User Device Association (Skojarzenie urządzenia użytkownika).
- Krok 5** Wprowadź odpowiednie kryteria wyszukiwania i kliknij przycisk **Znajdź**.
- Krok 6** Wybierz urządzenie, które chcesz skojarzyć z użytkownikiem, zaznaczając pole wyboru po lewej stronie urządzenia.
- Krok 7** Wybierz opcję **Save Selected/Changes** (Zapisz wybrane elementy/zmiany), aby skojarzyć urządzenie z użytkownikiem.
- Krok 8** Na liście rozwijanej Related Links (Pokrewne łącza) w prawym górnym rogu okna wybierz pozycję **Back to User** (Powrót do użytkownika) i kliknij przycisk **Go** (Przejdź).
- Pojawi się okno Konfiguracja użytkownika końcowego, a wybrane skojarzone urządzenia będą widoczne na panelu Controlled Devices (Kontrolowane urządzenia).
- Krok 9** Wybierz opcję **Save Selected/Changes**.
- 

## Survivable Remote Site Telephony

Dzięki protokołowi SRST (Survivable Remote Site Telephony) podstawowe funkcje telefonu pozostają dostępne po utracie połączenia z siecią WAN. W takiej sytuacji telefon może utrzymać trwałe połączenie,

a użytkownik zachowuje dostęp do podzbioru dostępnych funkcji. Gdy nastąpi przełączenie awaryjne, użytkownik otrzyma w telefonie komunikat alertu.

Więcej informacji na temat obsługiwanego oprogramowania sprzętowego i mechanizmu Survivable Remote Site Telephony można znaleźć w sekcji *Cisco Unified Survivable Remote Site Telephony — informacje o zgodności* na stronie Cisco.com

(<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

W poniższej tabeli opisano dostępność funkcji w trakcie przełączenia awaryjnego.

**Tabela 23: Obsługa funkcji w trybie SRST**

Funkcja	Obsługiwany	Uwagi
NowePoł	Tak	
Rozłączanie	Tak	
Wybierz ponownie	Tak	
Odbierz	Tak	
Zawieszanie	Tak	
Wznów	Tak	
Połączenie konferencyjne	Tak	
Konferencja z aktywnymi połączeniami (dołączenie)	Nie	Klawisz programowy Aktywne poł. nie jest wyświetlany.
Lista konferencji	Nie	
Przenoszenie	Tak	
Przekazywanie do połączeń aktywnych (przekazywanie bezpośrednie)	Nie	
Automatyczne odbieranie	Tak	
Połączenie oczekujące	Tak	
ID abonenta dzwoniącego	Tak	
Wskaźnik dźwiękowy oczekującej wiadomości	Tak	
Klawisz linii programowalnej Wszystkie połączenia	Tak	
Klawisz linii programowalnej Odbierz	Tak	



Funkcja	Obsługiwany	Uwagi
Prezentacja sesji Unified	Tak	Konferencja jest jedyną obsługiwaną funkcją z powodu ograniczeń innych funkcji.
Poczta głosowa	Tak	Nie można synchronizować poczty głosowej z innymi użytkownikami w ramach klastra serwerów Cisco Unified Communications Manager.
Przekierowywanie wszystkich połączeń	Tak	Stan przekazywania jest dostępny tylko w telefonie, który inicjuje przekazywanie, ponieważ w trybie SRST nie występują linie wspólne. Ustawienia funkcji Przekierowywanie wszystkich połączeń nie są zachowywane w przypadku przełączenia awaryjnego w tryb SRST z serwera Cisco Unified Communications Manager ani w przypadku przełączenia powrotnego z trybu SRST na serwer Communications Manager. Wszystkie połączenia w ramach funkcji Przekierowywanie wszystkich połączeń trwające nadal na serwerze Communications Manager powinny zostać oznaczone, gdy telefon ponownie nawiąże komunikację z serwerem Communications Manager po przełączeniu awaryjnym.
Szybkie wybieranie	Tak	
Klawisz linii programowalnej Usługa IRL	Tak	
Dostęp do poczty głosowej (iDivert)	Nie	Klawisz programowy iDivert nie jest wyświetlany.
Filtry linii	Częściowe	Linie są obsługiwane, ale nie można ich udostępniać.
Monitorowanie parkowania	Nie	Klawisz programowy Parkowanie nie jest wyświetlany.
Wtrąć	Nie	Klawisz programowy Wtrąć nie jest wyświetlany.
Rozszerzony wskaźnik wiadomości oczekującej	Nie	Na ekranie telefonu nie pojawiają się znaczki liczby wiadomości.  Wyświetlana jest tylko ikona Wiadomość oczekująca.
Kierowane parkowanie połączenia	Nie	Klawisz programowy nie jest wyświetlany.

Funkcja	Obsługiwany	Uwagi
SZL	Częściowe	Klawisz funkcji SZL działa jak klawisze szybkiego wybierania.
Cofnięcie zawieszenia	Nie	Połączenia pozostają wstrzymane bez końca.
Zdalne zawieszenie	Nie	Połączenia są oznaczane jako zawieszono lokalnie.
Meet Me	Nie	Klawisz programowy PokKonf nie jest wyświetlany.
Przejmij	Nie	Klawisz programowy nie działa.
Przejmij grupę	Nie	Klawisz programowy nie działa.
Przejmij inne	Nie	Klawisz programowy nie działa.
Identyfikator złych połączeń	Nie	Klawisz programowy nie działa.
QRT	Nie	Klawisz programowy nie działa.
Grupa wyszukiwania	Nie	Klawisz programowy nie działa.
Interkom	Nie	Klawisz programowy nie działa.
Przenoszenie	Nie	Klawisz programowy nie działa.
Prywatność	Nie	Klawisz programowy nie działa.
Oddzwon	Nie	Klawisz programowy Oddzwon nie jest wyświetlany.
Wideo	Tak	Konferencje wideo nie są obsługiwane.
Wideo	Tak	Konferencje wideo nie są obsługiwane.
Linia wspólna	Nie	
Szybkie wybieranie SZL	Tak	

## Enhanced Survivable Remote Site Telephony

Mechanizm Enhanced Survivable Remote Site Telephony (E-SRST) zapewnia, że są dodatkowe funkcje telefoniczne pozostają dostępne po utracie połączenia z siecią WAN. Oprócz funkcji obsługiwanych przez mechanizm Survivable Remote Site Telephony (SRST) mechanizm E-SRST obsługuje następujące funkcje:

- Linia wspólna
- Pole sygnalizacji aktywności linii

- Połączenia wideo

Więcej informacji na temat obsługiwanego oprogramowania sprzętowego i mechanizmu Survivable Remote Site Telephony można znaleźć w sekcji *Cisco Unified Survivable Remote Site Telephony — informacje o zgodności* na stronie Cisco.com

(<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

## Strony WWW reguł wybierania numeru aplikacji

Reguły wybierania numerów przez aplikację są używane do zamiany udostępnianych kontaktów mobilnych na wybierane numery sieciowe. Reguły wybierania numerów przez aplikację nie mają zastosowania w przypadku użytkownika wybierającego numer ręcznie, ani w przypadku, gdy numer był edytowany przed nawiązaniem połączenia przez użytkownika.

Reguły wybierania numerów przez aplikację są skonfigurowane w Cisco Unified Communications Manager.

Aby uzyskać dodatkowe informacje dotyczące reguł wybierania numerów, patrz *Podręcznik konfiguracji systemu Cisco Unified Communications Manager*, rozdział "Konfigurowanie reguł wybierania".

## Konfigurowanie reguł wybierania numeru aplikacji

### Procedura

---

- Krok 1** W programie Cisco Unified Communications Manager — administracja przejdź do opcji **Trasowanie połączeń > Reguły wybierania numerów > Reguły wybierania numerów przez aplikację**.
- Krok 2** Wybierz opcję **Dodaj nowy**, aby utworzyć regułę wybierania aplikacji, lub wybierz istniejącą zasadę wybierania aplikacji i zmodyfikuj ją.
- Krok 3** Uzupełnij poniższe informacje:
- **Nazwa** To pole zawiera unikatową nazwę reguły wybierania numerów, która może zawierać do 20 znaków alfanumerycznych i dowolną kombinację spacji, kropek (.), łączników (-) i znaków podkreślenia (\_).
  - **Opis** To pole zawiera krótki opis wprowadzanej reguły wybierania.
  - **Numer zaczyna się od** To pole zawiera początkowe cyfry numerów telefonu, dla których chcesz zastosować daną regułę wybierania numerów aplikacji.
  - **Numer zaczyna się od** To pole zawiera początkowe cyfry numerów telefonu, dla których chcesz zastosować daną regułę wybierania numerów aplikacji.
  - **Liczba cyfr do usunięcia** To pole określa liczbę cyfr, które program Cisco Unified Communications Manager ma usunąć z numerów telefonów, których dotyczy dana reguła wybierania.
  - **Prefiks z wzorcem** To wymagane pole zawiera wzorec umieszczany przed numerami telefonów, których dotyczy dana reguła wybierania numerów aplikacji.
  - **Priorytet reguły wybierania numerów aplikacji** To pole jest wyświetlane podczas wpisywania informacji o prefiksie z wzorcem. W tym polu można ustawić priorytet reguły wybierania numerów aplikacji.
- Krok 4** Uruchom ponownie program Cisco Unified Communications Manager.
-





## ROZDZIAŁ 6

# Zarządzanie portalem samoobsługowym

- [Portal samoobsługowy — omówienie, na stronie 83](#)
- [Konfigurowanie dostępu użytkownika do portalu Self Care, na stronie 84](#)
- [Dostosowywanie wyświetlania w portalu Self Care, na stronie 84](#)

## Portal samoobsługowy — omówienie

Portal samoobsługowy Cisco Unified Communications pozwala użytkownikom dostosować i kontrolować funkcje i ustawienia telefonu.

Dostęp do Portalu samoobsługowego jest kontrolowany przez administratora. Administrator musi też dostarczyć użytkownikom informacje, które umożliwią im dostęp do tego portalu.

Zanim użytkownik uzyska dostęp do Portalu samoobsługowego Cisco Unified Communications, musisz użyć programu Cisco Unified Communications Manager Cisco Unified CM Administration, aby dodać go do Cisco Unified Communications Manager standardowej grupy użytkowników.

Użytkownikom należy dostarczyć następujące informacje o Portalu samoobsługowym.

- Adres URL umożliwiający dostęp do aplikacji. Ten adres URL to:  
`https://<server_name:portnumber>/uzytkownik_ucm/`, gdzie nazwa\_serwera to host, na którym jest zainstalowany serwer WWW, a numer\_portu to numer portu na tym hoście.
- Identyfikator użytkownika i domyślne hasło umożliwiające dostęp do aplikacji.
- Informacje o zadaniach, które użytkownicy mogą wykonać w portalu.

Te ustawienia odpowiadają wartościom wprowadzonym podczas dodawania użytkownika do systemu Cisco Unified Communications Manager.

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Konfigurowanie dostępu użytkownika do portalu Self Care

Zanim użytkownik uzyska dostęp do portalu Self Care, należy go uwierzytelnić.

### Procedura

- 
- Krok 1** W Administracji Cisco Unified Communications Manager, wybierz **Zarządzanie użytkownikami > Użytkownik końcowy**.
  - Krok 2** Odszukaj użytkownika.
  - Krok 3** Kliknij łącze identyfikatora użytkownika.
  - Krok 4** Upewnij się, że użytkownik ma skonfigurowane hasło i kod PIN.
  - Krok 5** Sprawdź w sekcji Permission Information (Informacje o uprawnieniach), czy na liście Grupy znajduje się pozycja **Standard CCM End Users** (Standardowa grupa CCM użytkowników końcowych).
  - Krok 6** Kliknij przycisk **Zapisz**.
- 

## Dostosowywanie wyświetlania w portalu Self Care

Większość opcji jest widoczna w portalu Self Care. Trzeba jednak skonfigurować poniższe opcje, korzystając z ustawień Enterprise Parameters Configuration (Konfiguracja parametrów systemu przedsiębiorstwa) w aplikacji Cisco Unified Communications Manager — administracja:

- Show Ring Settings (Pokaż ustawienia dzwonka)
- Show Line Label Settings (Pokaż ustawienia oznaczenia linii)



---

**Uwaga** Ustawienia te mają zastosowanie do wszystkich stron portalu Self Care w danej siedzibie.

---

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **System > Enterprise Parameters (Parametry systemu przedsiębiorstwa)**.
  - Krok 2** W obszarze Self Care Portal (Portal Self Care) skonfiguruj pole **Self Care Portal Default Server** (Domyślny serwer portalu Self Care).
  - Krok 3** Włącz lub wyłącz parametry, do których użytkownicy mają mieć dostęp w portalu.
  - Krok 4** Kliknij przycisk **Zapisz**.
-



## CZĘŚĆ III

# Administrowanie telefonami IP Cisco

- Zabezpieczenia telefonu IP Cisco, na stronie 87
- Dostosowywanie telefonu IP Cisco, na stronie 119
- Funkcje telefonu i ich konfigurowanie, na stronie 125
- Firmowa książka telefoniczna i osobista książka telefoniczna, na stronie 223







## ROZDZIAŁ 7

# Zabezpieczenia telefonu IP Cisco

- [Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 87](#)
- [Obsługiwane funkcje zabezpieczeń, na stronie 88](#)

## Zwiększone zabezpieczenia Twojej sieci telefonicznej

W aplikacji Cisco Unified Communications Manager w wersji 11.5(1) i 12.0(1) można włączyć środowisko pracy o zwiększonych zabezpieczeniach. Dzięki tym zabezpieczeniom sieć telefoniczna może działać zgodnie z zestawem ścisłych zasad zarządzania ryzykiem, używając formantów zarządzania ryzykiem chroniących Ciebie i Twoich użytkowników.

Aplikacja Cisco Unified Communications Manager 12.5(1) nie obsługuje środowiska pracy o zwiększonych zabezpieczeniach. Przed uaktualnieniem do aplikacji Cisco Unified Communications Manager 12.5 (1) należy wyłączyć tryb FIPS. W przeciwnym razie usługa TFTP i inne usługi nie będą działać prawidłowo.

Środowisko pracy o zwiększonych zabezpieczeniach obejmuje następujące funkcje:

- Uwierzytelnianie kontaktów społecznościowych.
- TCP jako domyślny protokół zdalnego zapisywania wyników inspekcji w dzienniku.
- Tryb FIPS.
- Poprawiona usługa poświadczeń.
- Obsługa funkcji skrótów SHA-2 dla podpisów cyfrowych.
- Obsługa klucza RSA o długościach 512 i 4096 bitów.

W przypadku programu Cisco Unified Communications Manager w wersji 14.0 i oprogramowania sprzętowego telefonu IP Cisco w wersji 14,0 lub nowszej, telefony obsługują uwierzytelnianie OAuth protokołu SIP.

Protokół OAuth jest obsługiwany w przypadku protokołu TFTP (Proxy Trivial File Transfer Protocol) w Cisco Unified Communications Manager wersji 14.0(1)SU1 lub nowszej oraz oprogramowania sprzętowego dla telefonu IP Cisco w wersji 14.1(1). Usługa Proxy TFTP i OAuth for Proxy TFTP nie jest obsługiwana przez aplikację Mobile Remote Access (MRA).

Aby uzyskać dodatkowe informacje o zabezpieczeniach, zobacz:

- *System Configuration Guide for Cisco Unified Communications Manager*, wydanie 14.0(1) lub nowsze (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>).
- *Omówienie zabezpieczeń telefonów IP Cisco z serii 7800 i 8800* (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html>)
- *Podręcznik zabezpieczeń programu Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>)



**Uwaga** W telefonie IP Cisco można przechowywać ograniczoną liczbę plików ITL (Identity Trust List). Należy ograniczyć liczbę plików ITL, które system Cisco Unified Communications Manager może przesłać na telefon, ponieważ nie może ona przekraczać 64 tys.

## Obsługiwane funkcje zabezpieczeń

Funkcje zabezpieczeń chronią przed różnymi zagrożeniami, w tym zagrożeniami dotyczącymi tożsamości telefonu i danych. Te funkcje zakładają i utrzymują uwierzytelnione strumienie komunikacyjne pomiędzy telefonem a serwerem Cisco Unified Communications Manager oraz gwarantują, że telefon korzysta tylko z cyfrowo podpisanych plików.

Program Cisco Unified Communications Manager w wersji 8.5(1) lub nowszej ma domyślnie włączone wszystkie ustawienia zabezpieczeń, co zapewnia działanie następujących funkcji zabezpieczeń telefonów IP Cisco bez konieczności uruchamiania klienta CTL:

- Podpisywanie plików konfiguracyjnych telefonu
- Szyfrowanie pliku konfiguracyjnego telefonu
- HTTPS z Tomcat i inne usługi sieci Web



**Uwaga** Bezpieczne przekazywanie sygnału i funkcje multimedialne wciąż wymagają uruchomienia klienta CTL i użycia sprzętowych eTokenów.

Zaimplementowanie zabezpieczeń w systemie Cisco Unified Communications Manager uniemożliwi wykradanie tożsamości z telefonu i serwera Cisco Unified Communications Manager, zapobiegnie manipulowaniu danymi oraz uniemożliwi manipulowanie sygnałami połączeń i strumieniami mediów.

Aby zredukować te zagrożenia, w sieci telefonii IP firmy Cisco są ustanawiane i utrzymywane bezpieczne (szyfrowane) strumienie komunikacyjne między telefonem a serwerem, pliki są cyfrowo podpisywane przed wysłaniem do telefonu a strumienie mediów i sygnały połączeń między telefonami IP Cisco są szyfrowane.

Po wykonaniu wymaganych zadań związanych z Funkcją pełnomocnictw certyfikatu na telefonach zostanie zainstalowany Certyfikat znaczenia lokalnego (LSC, Locally Significant Certificate). W aplikacji Cisco Unified Communications Manager — administracja można skonfigurować certyfikat LSC, zgodnie z opisem w podręczniku Security Guide for Cisco Unified Communications Manager (Podręcznik zabezpieczeń

programu Cisco Unified Communications Manager). Można również zainicjować instalację certyfikatu LSC z menu Konfiguracja zabezpieczeń na telefonie. Za pośrednictwem tego menu można również zaktualizować lub usunąć certyfikat LSC.

Certyfikat LSC nie może być używany jako certyfikat użytkownika dla protokołu EAP-TLS uwierzytelniania sieci WLAN.


Telefony wykorzystują profil bezpieczeństwa telefonu, który określa, czy urządzenie jest niezabezpieczone, czy zabezpieczone. Więcej informacji na temat stosowania profilu zabezpieczenia w telefonie można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Jeśli w aplikacji Cisco Unified Communications Manager — administracja zostaną skonfigurowane ustawienia związane z bezpieczeństwem, plik konfiguracyjny telefonu będzie zawierać poufne informacje. W celu zapewnienia prywatności pliku konfiguracyjnego należy włączyć dla niego opcję szyfrowania danych. Szczegółowe informacje na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Telefony IP Cisco serii 8800 są zgodne ze standardem FIPS. Do poprawnego funkcjonowania tryb FIPS wymaga klucza o długości co najmniej 2048 bitów. Jeśli certyfikat nie ma przynajmniej 2048 bitów, telefon nie zostanie zarejestrowany w programie Cisco Unified Communications Manager i zostanie wyświetlony komunikat Nie można zarejestrować telefonu. Na telefonie wyświetlany jest komunikat Rozmiar klucza certyfikatu nie jest zgodny ze standardem FIPS.

Jeśli telefon nie ma certyfikatu LSC, przed włączeniem trybu FIPS niezbędne jest uaktualnienie rozmiaru klucza LSC do co najmniej 2048 bitów.

Poniższa tabela zawiera przegląd funkcji zabezpieczeń obsługiwanych przez te telefony. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Aby wyświetlić aktualne ustawienia zabezpieczeń w telefonie, w tym tryb zabezpieczeń, listę zaufanych certyfikatów i status uwierzytelniania 802.1X, naciśnij przycisk **Aplikacje**  i wybierz kolejno opcje **Ustawienia administratora** > **Konfiguracja zabezpieczeń**.

**Tabela 24: Przegląd funkcji zabezpieczeń**

Funkcja	Opis
Uwierzytelnianie obrazów	<p>Podpisane pliki binarne (o rozszerzeniu .sbn) uniemożliwiają manipulowanie obrazem oprogramowania sprzętowego przed wczytaniem go do telefonu.</p> <p>Zmanipulowanie obrazu spowoduje niepowodzenie procesu uwierzytelniania i odrzucenie przez telefon nowego obrazu.</p>
Szyfrowanie obrazu	<p>Zaszyfrowane pliki binarne (o rozszerzeniu .sebn) uniemożliwiają manipulowanie obrazem oprogramowania sprzętowego przed wczytaniem go do telefonu.</p> <p>Zmanipulowanie obrazu spowoduje niepowodzenie procesu uwierzytelniania i odrzucenie przez telefon nowego obrazu.</p>

Funkcja	Opis
Instalacja certyfikatu w siedzibie klienta	Uwierzytelnianie urządzenia wymaga, aby każdy telefon IP Cisco miał niepowtarzalny certyfikat. Telefony zawierają certyfikat instalowany fabrycznie (manufacturing installed certificate, MIC), ale w celu zapewnienia dodatkowego bezpieczeństwa można wybrać w aplikacji Cisco Unified Communications Manager — administracja instalowanie certyfikatu za pomocą funkcji pełnomocnictw certyfikatu (Certificate Authority Proxy Function, CAPF). Można również zainstalować certyfikat ważny lokalnie (Locally Significant Certificate, LSC), korzystając z menu Security Configuration (Konfiguracja zabezpieczeń) w telefonie.
Uwierzytelnianie urządzenia	Zachodzi między serwerem Cisco Unified Communications Manager a telefonem, gdy każda ze stron akceptuje certyfikat drugiej strony. Zależy od tego, czy telefon może nawiązać bezpieczne połączenie z serwerem Cisco Unified Communications Manager. W razie potrzeby między obiema stronami tworzona jest zabezpieczona ścieżka sygnalizacyjna z użyciem protokołu TLS. Program Cisco Unified Communications Manager rejestruje telefony tylko wtedy, gdy może je uwierzytelnić.
Uwierzytelnianie plików	Służy do weryfikowania podpisanych cyfrowo plików, które pobiera telefon. Telefon sprawdza podpis, aby wykluczyć zmanipulowanie pliku po jego utworzeniu. Pliki, które nie przejdą uwierzytelniania, nie są zapisywane w pamięci flash telefonu. Telefon odrzuca takie pliki bez dalszego przetwarzania.
Szyfrowanie plików	Szyfrowanie zapobiega ujawnianiu poufnych informacji w trakcie przesyłania pliku do telefonu. Ponadto telefon sprawdza podpis, aby wykluczyć zmanipulowanie pliku po jego utworzeniu. Pliki, które nie przejdą uwierzytelniania, nie są zapisywane w pamięci flash telefonu. Telefon odrzuca takie pliki bez dalszego przetwarzania.
Uwierzytelnianie sygnalizowania	Protokół TLS jest wykorzystywany do weryfikacji, czy nie zmanipulowano przesyłanych pakietów sygnalizacyjnych.
Certyfikat instalowany fabrycznie	Każdy telefon IP Cisco IP zawiera niepowtarzalny certyfikat instalowany fabrycznie, który służy do uwierzytelniania urządzenia. Certyfikat MIC to trwały, unikatowy dowód tożsamości telefonu, umożliwiający jego uwierzytelnianie w programie Cisco Unified Communications Manager.
Szyfrowanie mediów	Funkcja ta korzysta z protokołu SRTP do weryfikowania bezpieczeństwa strumieni mediów między obsługiwanymi urządzeniami oraz do zagwarantowania, że dane może odebrać i odczytać tylko urządzenie, dla którego zostały przeznaczone. Proces ten obejmuje utworzenie dla urządzeń pary głównych kluczy mediów oraz bezpieczne dostarczenie kluczy do urządzeń.
Funkcja pełnomocnictw certyfikatu (ang. Certificate Authority Proxy Function, CAPF)	Realizuje elementy procedury generowania certyfikatu, które są zbyt obciążające dla telefonu, oraz komunikuje się z nim podczas generowania kluczy i instalowania certyfikatów. Funkcję CAPF można skonfigurować w taki sposób, aby w imieniu telefonu pobierała certyfikaty z urzędów certyfikacji wskazanych przez klienta lub generowała certyfikaty lokalnie.
Profil zabezpieczenia	Określa, czy telefon jest niezabezpieczony, uwierzytelniony, szyfrowany, czy chroniony. Pozostałe wpisy w tej tabeli opisują funkcje zabezpieczeń.
Szyfrowane pliki konfiguracyjne	Funkcja umożliwiająca zapewnienie poufności plików konfiguracyjnych telefonu.

Funkcja	Opis
Opcjonalne wyłączenie serwera WWW w telefonie	Ze względów bezpieczeństwa można zablokować dostęp do stron WWW telefonu (na których są wyświetlane różne statystyki pracy telefonu) i Portalu samoobsługowego.
Zwiększanie bezpieczeństwa telefonu	<p>Dodatkowe opcje zabezpieczeń konfigurowane za pomocą aplikacji Cisco Unified Communications Manager — administracja:</p> <ul style="list-style-type: none"> <li>• Wyłączenie portu komputera</li> <li>• Wyłączenie protokołu Gratuitous ARP (GARP)</li> <li>• Wyłączenie dostępu do sieci Voice VLAN poprzez port komputera</li> <li>• Wyłączenie dostępu do menu Ustawienia lub jego ograniczenie tylko do menu Preferencje i funkcji zapisywania zmian głośności</li> <li>• Wyłączenie dostępu do stron WWW telefonu</li> <li>• Wyłączenie portu akcesoriów Bluetooth</li> <li>• Ograniczanie szyfrów TLS</li> </ul>
Uwierzytelnianie 802.1X	Telefon IP Cisco może korzystać z uwierzytelniania 802.1X przy żądaniu i uzyskiwaniu dostępu do sieci. Więcej informacji można znaleźć w sekcji <a href="#">Uwierzytelnianie 802.1X, na stronie 115</a> .
Bezpieczne przełączanie awaryjne w protokole SIP dla trybu SRST	Po skonfigurowaniu referencji trybu SRST (Survivable Remote Site Telephony) na potrzeby zabezpieczeń, a następnie wyzerowaniu zależnych od niej urządzeń w aplikacji Cisco Unified Communications Manager — administracja serwer TFTP dodaje certyfikat trybu SRST do pliku cnf.xml i wysyła go do telefonu. Zabezpieczony telefon używa później połączenia TLS do komunikacji z routerem zgodnym z trybem SRST.
Szyfrowanie sygnalizowania	Zapewnia, że wszystkie komunikaty sygnalizacyjne SIP wysyłane między urządzeniem a serwerem programu Cisco Unified Communications Manager są szyfrowane.
Alarm o aktualizacji listy zaufanych	Po aktualizacji listy zaufanych w telefonie program Cisco Unified Communications Manager odbiera alarm informujący o powodzeniu lub niepowodzeniu aktualizacji. Poniższa tabela zawiera dodatkowe informacje.

Funkcja	Opis
Szyfrowanie AES 256	<p>Po nawiązaniu połączenia z programem Cisco Unified Communications Manager w wersji 10.5(2) lub nowszej telefony obsługują szyfrowanie AES 256 w przypadku szyfrowania sygnalizacji i mediów w ramach protokołów TLS i SIP. Umożliwia to telefonom inicjowanie i obsługę połączeń TLS 1.2 z użyciem szyfrów opartych na AES 256, które są zgodne ze standardami SHA-2 (ang. Secure Hash Algorithm, bezpieczny algorytm wyznaczania wartości skrótu) i FIPS (Federal Information Processing Standards, federalne standardy przetwarzania informacji). Dostępne są następujące szyfry:</p> <ul style="list-style-type: none"> <li>• W przypadku połączeń TLS: <ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</li> </ul> </li> <li>• W przypadku połączeń sRTP: <ul style="list-style-type: none"> <li>• AEAD_AES_256_GCM</li> <li>• AEAD_AES_128_GCM</li> </ul> </li> </ul> <p>Więcej wiadomości na ten temat można znaleźć w dokumentacji programu Cisco Unified Communications Manager.</p>
Certyfikaty ECDSA (Elliptic Curve Digital Signature Algorithm)	<p>W ramach certyfikacji Common Criteria (CC) do systemu Cisco Unified Communications Manager dodano certyfikaty ECDSA w wersji 11.0. Dotyczy to wszystkich produktów systemu Voice Operating System (VOS) w wersji CUCM 11.5 i nowszych wersjach.</p>

Poniższa tabela zawiera komunikaty alarmowe o aktualizacji listy zaufanych i wyjaśnienie ich znaczenia. Więcej wiadomości na ten temat można znaleźć w dokumentacji programu Cisco Unified Communications Manager.

**Tabela 25: Komunikaty alarmowe o aktualizacji listy zaufanych**

Kod i komunikat	Opis
1 — TL_SUCCESS	Odebrano nowy plik CTL i/lub ITL
2 — CTL_INITIAL_SUCCESS	Odebrano nowy plik CTL, nie istnieje lista zaufanych
3 — ITL_INITIAL_SUCCESS	Odebrano nowy plik ITL, nie istnieje lista zaufanych
4 — TL_INITIAL_SUCCESS	Odebrano nowe pliki CTL i ITL, nie istnieje lista zaufanych
5 — TL_FAILED_OLD_CTL	Aktualizacja do nowego pliku CTL nie powiodła się, ale istnieje poprzednia lista zaufanych
6 — TL_FAILED_NO_TL	Aktualizacja do nowej listy zaufanych nie powiodła się i nie istnieje stara lista zaufanych
7 — TL_FAILED	Błąd ogólny
8 — TL_FAILED_OLD_ITL	Aktualizacja do nowego pliku ITL nie powiodła się, ale istnieje poprzednia lista zaufanych

Kod i komunikat	Opis
9 — TL_FAILED_OLD_TL	Aktualizacja do nowej listy zaufanych nie powiodła się, ale istnieje poprzednia lista zaufanych

Menu Konfiguracja zabezpieczeń zawiera informacje o różnych ustawieniach zabezpieczeń. Menu umożliwia również dostęp do menu Lista zaufanych certyfikatów i wskazuje, czy w telefonie jest zainstalowany plik CTL lub ITL.

W poniższej tabeli opisano opcje dostępne w menu Konfiguracja zabezpieczeń.

Tabela 26: Menu Konfiguracja zabezpieczeń

Opcja	Opis	Aby zmienić
Tryb zabezpieczeń	Podaje ustawiony w telefonie tryb zabezpieczeń.	W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje <b>Urządzenie &gt; Telefon</b> . To ustawienie znajduje się w sekcji Informacje specyficzne dla protokołu w oknie Konfiguracja telefonu.
LSC	Wskazuje, czy w telefonie jest zainstalowany ważny lokalnie certyfikat używany na potrzeby zabezpieczeń (Tak lub Nie).	Więcej informacji na temat zarządzania certyfikatem LSC w telefonie można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.
Lista zaufanych certyfikatów	<p>Menu Lista zaufanych certyfikatów zawiera podmenu dla plików CTL, ITL i podpisanych plików konfiguracyjnych.</p> <p>W podmenu Plik CTL jest wyświetlana zawartość pliku CTL. W podmenu Plik ITL jest wyświetlana zawartość pliku ITL.</p> <p>W menu Lista zaufanych certyfikatów są również wyświetlane następujące informacje:</p> <ul style="list-style-type: none"> <li>• Sygnatura CTL: skrót SHA1 pliku CTL</li> <li>• Serwer Unified CM/TFTP: nazwa serwera programu Cisco Unified Communications Manager i serwera TFTP używanych przez telefon. Pokazuje ikonę certyfikatu, jeśli dla tego serwera jest zainstalowany certyfikat.</li> <li>• Serwer CAPF: nazwa serwera CAPF używanego przez telefon. Pokazuje ikonę certyfikatu, jeśli dla tego serwera jest zainstalowany certyfikat.</li> <li>• Router SRST: adres IP zaufanego routera SRST, z którego może korzystać telefon. Pokazuje ikonę certyfikatu, jeśli dla tego serwera jest zainstalowany certyfikat.</li> </ul>	Aby uzyskać więcej informacji, patrz <a href="#">Konfigurowanie certyfikatu obowiązującego lokalnie, na stronie 94</a> .

Opcja	Opis	Aby zmienić
Uwierzytelnianie 802.1X	Umożliwia włączanie w telefonie uwierzytelniania 802.1X.	Zobacz <a href="#">Uwierzytelnianie 802.1X</a> , na stronie 115.

**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Konfigurowanie certyfikatu obowiązującego lokalnie

To zadanie dotyczy konfigurowania certyfikatu LSC przy użyciu metody ciągu uwierzytelniania.


**Zanim rozpoczniesz**

Należy się upewnić, że zostały już wprowadzone odpowiednie konfiguracje programu Cisco Unified Communications Manager i funkcji pełnomocnictw certyfikatu (ang. Certificate Authority Proxy Function, CAPF):

- Plik CTL lub ITL zawiera certyfikat CAPF.
- W aplikacji Cisco Unified Communications Operating System Administration należy sprawdzić, czy jest zainstalowany certyfikat CAPF.
- Funkcja CAPF działa i jest skonfigurowana.

Więcej informacji o tych ustawieniach można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

**Procedura**

- 
- Krok 1** Sprawdź kod uwierzytelnienia CAPF ustawiony przy konfigurowaniu funkcji CAPF.
- Krok 2** W telefonie naciśnij opcję **Aplikacje** .
- Krok 3** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja zabezpieczeń**.
- Uwaga** Dostęp do menu Ustawienia można kontrolować w polu Settings Access (Dostęp do ustawień) w oknie Konfiguracja telefonu w aplikacji Cisco Unified Communications Manager — administracja.
- Krok 4** Wybierz opcję **LSC** i naciśnij przycisk **Wybierz** lub **Uaktualnij**.  
Telefon wyświetli monit o wprowadzenie ciągu uwierzytelniania.
- Krok 5** Wprowadź kod uwierzytelnienia i naciśnij przycisk **Wyślij**.  
Telefon rozpocznie instalowanie, aktualizowanie lub usuwanie certyfikatu ważnego lokalnie, w zależności od konfiguracji funkcji CAPF. W trakcie procedury w polu opcji LSC w menu Security Configuration pojawia się seria komunikatów, które umożliwiają śledzenie postępów. Po zakończeniu procedury telefon wyświetla komunikat Installed (Zainstalowano) lub Not Installed (Nie zainstalowano).  
Proces instalowania, aktualizowania lub usuwania certyfikatu ważnego lokalnie może długo potrwać.



Po pomyślnym zakończeniu instalowania w telefonie pojawia się komunikat `Installed`. Jeśli w telefonie zostanie wyświetlony komunikat `Nie zainstalowano`, ciąg uwierzytelnienia był nieprawidłowy lub w telefonie nie włączono funkcji uaktualniania. Jeśli w wyniku działania funkcji CAPF nastąpi usunięcie certyfikatu ważnego lokalnie, telefon wyświetli komunikat `Not Installed`, aby zasygnalizować powodzenie operacji. Serwer CAPF zapisuje w dzienniku komunikaty o błędach. Lokalizację dzienników i znaczenie komunikatów o błędach podano w dokumentacji serwera CAPF.

## Włączanie trybu FIPS


### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Telefon** i zlokalizuj telefon.
- Krok 2** Przejdź do obszaru Konfiguracja specyficzna dla produktu.
- Krok 3** W polu **Tryb FIPS** wybierz opcję **Włączone**.
- Krok 4** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
- Krok 5** Kliknij przycisk **Zapisz**.
- Krok 6** Uruchom ponownie telefon.

## Zabezpieczenia połączeń telefonicznych

Gdy w telefonie zastosowane są zabezpieczenia, zabezpieczone połączenia telefoniczne można rozpoznać po ikonach na jego ekranie. Jeśli ponadto na początku połączenia odtwarzany jest sygnał dźwiękowy zabezpieczeń, wskazuje to, że połączony telefon jest zabezpieczony i chroniony.

W ramach połączenia zabezpieczonego wszystkie sygnały połączenia i strumień mediów są szyfrowane. Połączenie zabezpieczone zapewnia wysoki poziom bezpieczeństwa, gwarantując brak zafałszowań i poufność rozmowy. Gdy trwające połączenie jest szyfrowane, jego ikona postępu po prawej stronie licznika czasu

trwania połączenia na ekranie telefonu zmienia się w następującą ikonę: .



**Uwaga** Jeśli połączenie jest trasowane za pośrednictwem dróg połączeń leżących poza siecią IP, np. poprzez publiczną komutowaną sieć telefoniczną, może ono być niezabezpieczone mimo że jest szyfrowane w obrębie sieci IP i oznaczone ikoną z kłódką.

Na początku połączenia zabezpieczonego odtwarzany jest sygnał dźwiękowy zabezpieczeń, wskazujący, że telefon po drugiej stronie również odbiera i wysyła zabezpieczone dane dźwiękowe. Jeśli użytkownik połączy się z niezabezpieczonym telefonem, nie usłyszy sygnału dźwiękowego zabezpieczeń.




**Uwaga** Połączenia zabezpieczone są obsługiwane tylko między dwoma telefonami. Po skonfigurowaniu połączeń zabezpieczonych niektóre funkcje, np. połączenia konferencyjne i linie wspólne, są niedostępne.

Po skonfigurowaniu telefonu w programie Cisco Unified Communications Manager jako zabezpieczonego (szyfrowanego i zaufanego) może mu zostać nadany stan "chroniony". Następnie w razie potrzeby można skonfigurować chroniony telefon w taki sposób, aby na początku połączenia odtwarzał sygnał dźwiękowy zabezpieczeń:

- Protected Device (Chronione urządzenie): aby zmienić stan zabezpieczonego telefonu na chroniony, zaznacz pole wyboru Protected Device w oknie Konfiguracja telefonu w aplikacji Cisco Unified Communications Manager — administracja (**Urządzenie** > **Telefon**).
- Play Secure Indication Tone (Emituj dźwięk wskazania zabezpieczeń): aby włączyć w chronionym telefonie odtwarzanie dźwięku wskazania zabezpieczonego lub niezabezpieczonego połączenia, wybierz dla opcji Play Secure Indication Tone ustawienie Prawda. Domyślnie dla opcji Play Secure Indication Tone wybrane jest ustawienie Fałsz. Można to zmienić w aplikacji Cisco Unified Communications Manager — administracja (**System** > **Parametry usługi**). Wybierz serwer, a następnie wybierz usługę Unified Communications Manager. W oknie Service Parameter Configuration (Konfiguracja parametrów usługi) wybierz odpowiednią opcję w obszarze Funkcja — Secure Tone (Sygnał dźwiękowy zabezpieczeń). Wartość domyślna to Fałsz.

## Identyfikacja zabezpieczonych połączeń konferencyjnych

Można zainicjować zabezpieczone połączenie konferencyjne i monitorować poziom bezpieczeństwa jego uczestników. Procedura nawiązywania zabezpieczonego połączenia konferencyjnego:

1. Użytkownik inicjuje konferencję za pomocą zabezpieczonego telefonu.
2. Program Cisco Unified Communications Manager przypisuje połączeniu zabezpieczony mostek konferencyjny.
3. W miarę dodawania uczestników program Cisco Unified Communications Manager weryfikuje tryb zabezpieczeń każdego telefonu, utrzymując poziom bezpieczeństwa konferencji.
4. Telefon wyświetla poziom bezpieczeństwa połączenia konferencyjnego. Zabezpieczona konferencja powoduje wyświetlanie na ekranie telefonu ikony zabezpieczeń  po prawej stronie komunikatu **Konferencja**.



**Uwaga** Połączenia zabezpieczone są obsługiwane tylko między dwoma telefonami. W przypadku chronionych telefonów niektóre funkcje, np. połączenia konferencyjne, linie wspólne i funkcja Extension Mobility, są niedostępne po skonfigurowaniu połączeń zabezpieczonych.

W poniższej tabeli podano informacje o zmianach poziomu bezpieczeństwa konferencji w zależności od poziomu bezpieczeństwa telefonu jej inicjatora, poziomów bezpieczeństwa uczestników i dostępności zabezpieczonych mostków konferencyjnych.


Tabela 27: Ograniczenia zabezpieczeń w przypadku połączeń konferencyjnych

Poziom bezpieczeństwa telefonu inicjatora	Używana funkcja	Poziom bezpieczeństwa uczestników	Efekty działania
Niezabezpieczony	Połączenie konferencyjne	Secure	Niezabezpieczony mostek konferencyjny Niezabezpieczona konferencja
Secure	Połączenie konferencyjne	Co najmniej jeden członek konferencji jest niezabezpieczony.	Zabezpieczony mostek konferencyjny Niezabezpieczona konferencja
Secure	Połączenie konferencyjne	Secure	Zabezpieczony mostek konferencyjny Konferencja zabezpieczona i szyfrowana
Niezabezpieczony	Meet Me	Minimalny poziom bezpieczeństwa to szyfrowany.	Inicjator odbiera komunikat Nie spełnia bezpieczeństwa, połączenie od
Secure	Meet Me	Minimalny poziom bezpieczeństwa to niezabezpieczony.	Zabezpieczony mostek konferencyjny Konferencja jest otwarta na wszystkie połączenia

## Identyfikacja zabezpieczonych połączeń telefonicznych

Połączenie zabezpieczone można nawiązać, gdy zarówno Twój telefon, jak i telefon rozmówcy jest skonfigurowany pod kątem obsługi takich połączeń. Telefon rozmówcy może należeć do tej samej sieci Cisco IP lub do innej sieci. Połączenia zabezpieczone można nawiązywać tylko między dwoma telefonami. Bezpieczne połączenia konferencyjne można nawiązywać po skonfigurowaniu zabezpieczonego mostka konferencyjnego.

Procedura nawiązywania połączenia zabezpieczonego:

1. Użytkownik inicjuje połączenie za pomocą zabezpieczonego telefonu (działającego w trybie bezpiecznym).
2. Telefon wyświetla na ekranie ikonę zabezpieczeń . Wskazuje ona, że telefon jest skonfigurowany pod kątem obsługi połączeń zabezpieczonych, ale nie oznacza, że telefon rozmówcy również działa w trybie bezpiecznym.
3. Jeśli użytkownik połączy się z innym zabezpieczonym telefonem, usłyszy sygnał dźwiękowy zabezpieczeń, który wskazuje, że rozmowa jest po obu stronach szyfrowana i zabezpieczona. Jeśli użytkownik połączy się z niezabezpieczonym telefonem, nie usłyszy sygnału dźwiękowego zabezpieczeń.



### Uwaga

Połączenia zabezpieczone są obsługiwane tylko między dwoma telefonami. W przypadku chronionych telefonów niektóre funkcje, np. połączenia konferencyjne, linie wspólne i funkcja Extension Mobility, są niedostępne po skonfigurowaniu połączeń zabezpieczonych.

Sygnał dźwiękowy zabezpieczeń emitują tylko zabezpieczone telefony. Niezabezpieczone telefony nigdy nie emitują tego sygnału. Jeśli w trakcie połączenia zmieni się jego ogólny stan, dźwięk wskazania ulegnie zmianie i zabezpieczony telefon wyemituje odpowiedni sygnał.

W poniższych okolicznościach zabezpieczony telefon emituje sygnał dźwiękowy lub nie:

- Gdy włączona jest opcja Play Secure Indication Tone (Emituj dźwięk wskazania zabezpieczeń):
  - Kiedy nawiązano kompleksowe połączenie zabezpieczone, a stan połączenia również wskazuje, że jest ono zabezpieczone, telefon emituje dźwięk wskazania zabezpieczeń (trzy długie sygnały dźwiękowe z przerwami).
  - Kiedy nawiązano kompleksowe połączenie niezabezpieczone, a stan połączenia również wskazuje, że jest ono niezabezpieczone, telefon emituje dźwięk wskazania braku zabezpieczeń (sześć krótkich sygnałów dźwiękowych z krótkimi przerwami).

Gdy opcja Play Secure Indication Tone (Emituj dźwięk wskazania zabezpieczeń) jest wyłączona, nie są emitowane żadne sygnały dźwiękowe.

## Szyfrowanie dla funkcji wtrącenia

Program Cisco Unified Communications Manager sprawdza stan zabezpieczeń telefonu podczas tworzenia konferencji, po czym zmienia wskazania zabezpieczeń konferencji lub blokuje ukończenie połączenia w celu zachowania integralności i bezpieczeństwa systemu.

Użytkownik nie można dokonać wtrącenia w przypadku zaszyfrowanego połączenia, jeśli telefon, który służy do wtrącenia, nie jest skonfigurowany do pracy z szyfrowaniem. Jeśli w takim przypadku wtrącenie nie powiedzie się, na telefonie inicjującym wtrącenie zostanie odtworzony sygnał zmiany ustawień (szybki sygnał zajętości).

Jeśli telefon inicjatora jest skonfigurowany do pracy z szyfrowaniem, inicjator wtrącenia może wtrącić się do niezabezpieczonego połączenia z szyfrowanego telefonu. Po wtrąceniu program Cisco Unified Communications Manager klasyfikuje takie połączenie jako niezabezpieczone.

Jeśli telefon inicjatora jest skonfigurowany do pracy z szyfrowaniem, inicjator wtrącenia może wtrącić się w zaszyfrowane połączenie, a telefon wskaże, że połączenie jest szyfrowane.

## Zabezpieczenia sieci WLAN

Wszystkie urządzenia sieci WLAN znajdujące się w zasięgu mogą odbierać wszystkie dane przesyłane w sieci, dlatego zapewnienie bezpieczeństwa komunikacji głosowej ma krytyczne znaczenie dla sieci WLAN. Aby uniemożliwić intruzom modyfikowanie i przechwytywanie danych głosowych, architektura Cisco SAFE Security obsługuje telefony IP Cisco i punkty dostępu Cisco Aironet. Więcej informacji o zabezpieczeniach w sieci można znaleźć na stronie

[http://www.cisco.com/en/US/netsol/ns744/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html).

Rozwiązania telefonii bezprzewodowej stosowane w telefonach Cisco IP zabezpieczają sieć, uniemożliwiając nieupoważnione logowanie i naruszenie bezpieczeństwa komunikacji, dzięki użyciu następujących metod uwierzytelniania obsługiwanych przez telefony IP Cisco:

- Otwarte uwierzytelnianie: dowolne urządzenie może zażądać uwierzytelnienia w systemie otwartym. Punkt dostępu, który odbiera żądanie, może udzielić uwierzytelnienia dowolnemu żądającemu lub tylko tym żądającym, którzy znajdują się na liście użytkowników. Komunikacja pomiędzy urządzeniem bezprzewodowym a punktem dostępu może być nieszyfrowana lub urządzenia mogą używać kluczy WEP (Wired Equivalent Privacy) w celu zapewnienia bezpieczeństwa. Urządzenia, które do uwierzytelniania używają protokołu WEP, próbują uwierzytelnić się jedynie z punktem dostępu używającym protokołu WEP.

- Uwierzytelnianie EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling): ta architektura zabezpieczeń serwerów klienta szyfruje transakcje EAP w tunelu TLS (Transport Level Security) między punktem dostępu a serwerem RADIUS, takim jak serwer Cisco ACS (Access Control Server).

Tunel TLS do uwierzytelniania między klientem (telefonem) a serwerem RADIUS używa protokołu PACs (Protected Access Credentials). Serwer wysyła do klienta (telefonu) identyfikator uwierzytelnienia (AID), który z kolei wybiera odpowiedni klucz PAC. Klient (telefon) zwraca wiadomość PAC-Opaque do serwera RADIUS. Serwer odszyfrowuje klucz PAC za pomocą klucza głównego. Oba punkty końcowe mają teraz klucz PAC, co umożliwia utworzenie tunelu TLS. Protokół EAP-FAST obsługuje automatyczne dostarczanie kluczy PAC, ale tę funkcję należy włączyć na serwerze RADIUS.



**Uwaga** W przypadku serwera Cisco ACS klucz PAC wygasa po tygodniu. Jeśli klucz PAC w telefonie jest nieważny, uwierzytelnianie z serwerem RADIUS trwa dłużej, gdy telefon pobiera nowy klucz PAC. Aby uniknąć opóźnień związanych z dostarczaniem klucza PAC, na serwerze ACS lub RADIUS ustaw okres ważności klucza PAC na 90 dni lub dłużej.

- Uwierzytelnianie przy użyciu protokołu EAP-TLS (Extensible Authentication Protocol-Transport Layer Security): protokół EAP-TLS wymaga certyfikatu klienta do uwierzytelniania i dostępu do sieci. W przypadku połączeń przewodowych przy użyciu protokołu EAP-TLS certyfikatem klienta może być certyfikat MIC lub LSC telefonu. Certyfikat LSC jest zalecanym certyfikatem uwierzytelniania klienta dla połączeń przewodowych przy użyciu protokołu EAP-TLS.
- Protokół PEAP (Protected Extensible Authentication Protocol): opracowany przez firmę Cisco protokół uwierzytelniania wzajemnego w oparciu o hasło między klientem (telefonem) a serwerem RADIUS. Telefon IP Cisco może używać protokołu PEAP do uwierzytelniania w sieci bezprzewodowej. Obsługiwane są metody uwierzytelniania PEAP-MSCHAPV2 i PEAP-GTC.

Następujące systemy uwierzytelniania korzystają z serwera RADIUS do zarządzania kluczami uwierzytelniania:

- WPA/WPA2: używa informacji serwera RADIUS do generowania unikatowych kluczy uwierzytelniania. Ponieważ klucze te są generowane na centralnym serwerze RADIUS, protokół WPA/WPA2 zapewnia większe bezpieczeństwo w porównaniu z metodą WPA używającą wstępnych kluczy przechowywanych w punkcie dostępu w telefonie.
- Szybki i bezpieczny roaming: używa informacji serwera RADIUS i serwera domeny bezprzewodowej do zarządzania kluczami i ich uwierzytelniania. Protokół WDS tworzy pamięć podręczną poświadczeń zabezpieczeń dla urządzenia klienta usługi CCKM, służącą do szybkiego i bezpiecznego ponownego uwierzytelnienia. Telefony IP Cisco z serii 8800 obsługują protokół 802.11r (FT). Zarówno protokół 11r (FT), jak i protokół CCKM, umożliwia korzystanie z funkcji szybkiego i bezpiecznego roamingu. Jednak firma Cisco zdecydowanie zaleca użycie połączenia bezprzewodowego 802.11r (FT).

Dzięki użyciu protokołów WPA/WPA2 i CCKM klucze szyfrowania nie są wprowadzane w telefonie, ale są automatycznie ustalane między punktem dostępu a telefonem. Jednak nazwę użytkownika i hasło EAP, które są używane do uwierzytelniania, należy wprowadzić w każdym telefonie.

Aby się upewnić, że połączenia głosowe są bezpieczne, telefon IP Cisco obsługuje protokoły szyfrowania WEP, TKIP oraz AES (Advanced Encryption Standard). Jeśli do szyfrowania są używane te mechanizmy,

pakiety sygnalizacyjne SIP i pakiety protokołu RTP (Real-Time Transport) są szyfrowane między punktem dostępu a telefonem IP Cisco.

### WEP

Gdy w sieci bezprzewodowej jest używany protokół WEP, uwierzytelnianie odbywa się w punkcie dostępu za pomocą jawnego lub udostępnianego klucza. Aby połączenie powiodło się, klucz WEP skonfigurowany w telefonie musi odpowiadać kluczowi WEP skonfigurowanemu w punkcie dostępu. Telefon IP Cisco obsługuje klucze WEP używające szyfrowania 40- lub 128-bitowego, które pozostają niezmienione w telefonie i punkcie dostępu.

Uwierzytelnienie EAP i CCKM może używać kluczy WEP do szyfrowania danych. Serwer RADIUS zarządza kluczem WEP i przekazuje unikatowy klucz do punktu dostępu po uwierzytelnieniu w celu zaszyfrowania wszystkich pakietów głosowych; w związku z tym klucze WEP mogą ulegać zmianie przy każdym uwierzytelnieniu.

### TKIP

Protokoły WPA i CCKM używają protokołu szyfrowania TKIP, który zawiera kilka usprawnień w porównaniu z protokołem WEP. Protokół TKIP udostępnia funkcję szyfrowania poszczególnych pakietów przy użyciu klucza oraz dłuższe wektory inicjowania (IV), co poprawia jakość szyfrowania. Ponadto sprawdzanie integralności wiadomości (MIC) zapewnia, że zaszyfrowane pakiety nie zostały zmienione. Protokół TKIP rozwiązuje problem z przewidywalnością protokołu WEP, która umożliwiała intruzom odszyfrowanie klucza WEP.

### AES

Metoda szyfrowania używana na potrzeby uwierzytelniania WPA2. Ten krajowy standard szyfrowania korzysta z algorytmu symetrycznego, używającego tego samego klucza do szyfrowania i odszyfrowywania. Protokół AES używa szyfrowania CBC (Cipher Blocking Chain) dla bloków o rozmiarze 128 bitów, stosując klucze o minimalnej długości 128, 192 i 256 bitów. Telefon IP Cisco obsługuje klucz o długości 256 bitów.



---

**Uwaga** Telefon IP Cisco nie obsługuje protokołu CKIP (Cisco Key Integrity Protocol) w ramach protokołu CMIC.

---

Systemy uwierzytelniania i szyfrowania są konfigurowane w bezprzewodowej sieci LAN. W sieci bezprzewodowej i w punktach dostępu są konfigurowane sieci VLAN, dla których są wybierane różne kombinacje metod uwierzytelniania i szyfrowania. Identyfikator SSID skojarzony z siecią VLAN i określonym schematem uwierzytelniania i szyfrowania. Aby pomyślnie uwierzytelić bezprzewodowe urządzenia klienta, należy skonfigurować te same identyfikatory SSID dla systemów uwierzytelniania i szyfrowania w punkcie dostępu i telefonie IP Cisco.

Niektóre systemy uwierzytelniania wymagają określonych typów szyfrowania. W celu zwiększenia bezpieczeństwa uwierzytelniania otwartego można użyć szyfrowania WEP. Jeśli jednak jest używane uwierzytelnianie z kluczem wspólnym, należy ustawić statyczne szyfrowanie WEP i skonfigurować klucz WEP w telefonie.



**Uwaga**

- Użycie klucza wstępnego WPA lub klucza wstępnego WPA2 wymaga statycznego skonfigurowania klucza wstępnego w telefonie. Te klucze muszą odpowiadać kluczom znajdującym się w punkcie dostępu.
- Telefon IP Cisco nie obsługuje automatycznej negocjacji protokołu EAP; aby użyć trybu EAP-FAST, należy go określić.

Poniższa tabela zawiera listę systemów uwierzytelniania i szyfrowania skonfigurowanych w punkcie dostępu AP Aironet Cisco, które są obsługiwane przez telefon IP Cisco. W tabeli przedstawiono opcję konfiguracji sieci dla telefonu, odpowiadającą konfiguracji punktu dostępu.

**Tabela 28: Systemy uwierzytelniania i szyfrowania**

Konfiguracja telefonu IP Cisco	Konfiguracja punktu dostępu			
	Bezpieczeństwo	Zarządzanie kluczami	Szyfrowanie	Szybki roaming
Tryb zabezpieczeń	Brak	Brak	Brak	N/D
WEP	Statyczny WEP	Statyczny	WEP	N/D
PSK	PSK	WPA	TKIP	Brak
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-GTC	PEAP-GTC	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Więcej informacji na temat konfigurowania systemów uwierzytelniania i szyfrowania w punktach dostępu można znaleźć w *Podręczniku konfiguracji Cisco Aironet* dla używanego modelu i wersji pod następującym adresem URL:

<http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243>

## Konfigurowanie trybu uwierzytelniania

Aby wybrać opcję Tryb uwierzytelniania dla tego profilu, wykonaj następujące czynności:

### Procedura

**Krok 1** Wybierz profil sieci, który chcesz skonfigurować.

**Krok 2** Wybierz tryb uwierzytelniania.

**Uwaga** W zależności od wybranej opcji, należy skonfigurować dodatkowe opcje w polach Zabezpieczenia sieci WLAN lub Szyfrowanie sieci WLAN. Więcej informacji można znaleźć w sekcji [Zabezpieczenia sieci WLAN, na stronie 98](#).

**Krok 3** Kliknij przycisk **Zapisz**, aby wprowadzić zmianę.

## Poświadczenia zabezpieczeń sieci bezprzewodowej

Jeśli do uwierzytelniania użytkownika sieć wykorzystuje protokoły EAP-FAST i PEAP, w razie potrzeby należy skonfigurować zarówno nazwę użytkownika, jak i hasło w usłudze RADIUS (Remote Authentication Dial-In User Service) i w telefonie.



**Uwaga** Jeśli w sieci są używane domeny, należy wprowadzić nazwę użytkownika oraz nazwę domeny w formacie: *domena\nazwa użytkownika*.

W wyniku następujących czynności aktualne hasło Wi-Fi może zostać wyczyszczone:

- Wprowadzenie niepoprawnego identyfikatora użytkownika lub hasła
- Zainstalowanie nieprawidłowego lub wygasłego hasła głównego urzędu certyfikacji, jeśli typ protokołu EAP jest ustawiony na PEAP MSCHAPV2 lub PEAP-GTC
- Wyłączenie typu EAP na serwerze RADIUS używanym w telefonie przed zmianą typu EAP na nowy

Aby zmienić typy EAP, wykonaj następujące czynności w podanej kolejności:

- Włącz nowe typy EAP na serwerze RADIUS.
- Zmień typ protokołu EAP w telefonie na nowy.

Zachowaj bieżący typ EAP skonfigurowany w telefonie, dopóki nowy typ EAP nie zostanie włączony na serwerze RADIUS. Typ EAP w telefonie można zmienić po włączeniu nowego typu EAP na serwerze



RADIUS. Po zmianie typu EAP na nowy we wszystkich telefonach można wyłączyć poprzedni typu EAP, jeśli zajdzie taka potrzeba.

## Konfigurowanie nazwy użytkownika i hasła

Aby wprowadzić lub zmienić nazwę użytkownika lub hasło w profilu sieci, należy użyć tej samej nazwy użytkownika i tego samego hasła, które zostały skonfigurowane na serwerze RADIUS. Maksymalna długość wpisu z nazwą użytkownika i hasłem wynosi 64 znaki.

Aby skonfigurować nazwę użytkownika i hasło w poświadczeniach zabezpieczeń sieci bezprzewodowej, wykonaj następujące czynności:

### Procedura

---

- Krok 1** Wybierz profil sieci.
  - Krok 2** W polu Nazwa użytkownika należy wprowadzić sieciową nazwę użytkownika dla tego profilu.
  - Krok 3** W polu Hasło należy wprowadzić hasło użytkownika sieciowego dla tego profilu.
  - Krok 4** Kliknij przycisk **Zapisz**, aby wprowadzić zmianę.
- 

## Konfigurowanie klucza wstępnego

W poniższych sekcjach przedstawiono procedurę konfigurowania kluczy wstępnych.

### Formaty klucza wstępnego

Telefon IP Cisco obsługuje format ASCII i format szesnastkowy. Podczas konfigurowania klucza wstępnego protokołu WPA należy użyć jednego z następujących formatów:

#### Szesnastkowo

W przypadku kluczy szesnastkowych należy wpisać 64 znaki szesnastkowe (0–9 i A–F), na przykład: AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C.

#### ASCII

W przypadku kluczy ASCII należy wprowadzić ciąg składający się ze znaków 0–9 i A–Z (duże i małe litery) oraz symboli, o długości 8–63 znaków, na przykład: GREG12356789ZXYW.

### Konfigurowanie PSK

Aby skonfigurować klucz PSK w obszarze Poświadczenia sieci bezprzewodowej, wykonaj następujące czynności:

### Procedura

---

- Krok 1** Wybierz profil sieci, który włącza klucz wstępny WPA lub WPA2.
- Krok 2** W obszarze Typ klucza wprowadź odpowiedni klucz.
- Krok 3** W polu Hasło/Klucz wstępny wprowadź ciąg ASCII lub cyfry szesnastkowe.

**Krok 4** Kliknij przycisk **Zapisz**, aby wprowadzić zmianę.

---

## Szyfrowanie sieci bezprzewodowej

Jeśli w sieci bezprzewodowej jest używane szyfrowanie WEP, a jako tryb uwierzytelniania zostanie ustawiona wartość **Otwarte + WEP**, należy wprowadzić klucz WEP jako ciąg znaków ASCII lub szesnastkowych.

Klucze WEP w telefonie muszą być zgodne z kluczami WEP przypisanymi do punktu dostępu. Telefon IP Cisco oraz punkty dostępu Cisco Aironet obsługują klucze szyfrowania 40- i 128-bitowe.

### Formaty klucza WEP

Podczas konfigurowania klucza protokołu WEP należy użyć jednego z następujących formatów:

#### Szesnastkowo

W przypadku kluczy szesnastkowych można użyć kluczy o następujących wielkościach:

##### 40-bitowy

Wprowadź 10-cyfrowy ciąg klucza szyfrowania, który zawiera znaki szesnastkowe (0–9 i A–F); na przykład ABCD123456.

##### 128-bitowy

Wprowadź 26-cyfrowy ciąg klucza szyfrowania, który zawiera znaki szesnastkowe (0–9 i A–F); na przykład AB123456789CD01234567890EF.

#### ASCII

W przypadku kluczy ASCII należy wprowadzić ciąg składający się ze znaków 0–9 i A–Z (duże i małe litery) i/lub symboli, stosując klucz o jednym z poniższych rozmiarów:

##### 40-bitowy

Wprowadź ciąg pięciu znaków, na przykład GREG5.

##### 128-bitowy

Wprowadź ciąg trzynastu znaków, na przykład GREGSSECRET13.

### Konfigurowanie kluczy WEP

Aby skonfigurować klucze WEP, wykonaj następujące czynności.

#### Procedura

---

**Krok 1** Wybierz profil sieci, który używa szyfrowania **Otwarte + WEP** lub **Klucz wspólny + WEP**.

**Krok 2** W obszarze **Typ klucza** wprowadź odpowiedni klucz.

**Krok 3** W obszarze **Rozmiar klucza** wybierz jedną z następujących długości ciągu znaków:

- 40
- 128

- Krok 4** W polu Klucz szyfrowania wprowadź odpowiedni ciąg klucza zgodnie z wybranym typem i rozmiarem klucza. Zobacz [Formaty klucza WEP, na stronie 104](#).
- Krok 5** Kliknij przycisk **Zapisz**, aby wprowadzić zmianę.

## Eksportowanie certyfikatu urzędu certyfikacji z serwera ACS za pomocą usługi certyfikatów firmy Microsoft

Wyeksportuj certyfikat głównego urzędu certyfikacji z serwera ACS. Więcej informacji zawiera dokumentacja urzędu certyfikacji lub serwera RADIUS.

### Certyfikat instalowany fabrycznie

Na etapie wytwarzania telefonu firma Cisco dołącza do niego certyfikat instalowany fabrycznie (MIC, Manufacturing Installed Certificate).

Podczas uwierzytelniania EAP-TLS serwer ACS musi sprawdzić zaufanie telefonu, a telefon — zaufanie serwera ACS.

Aby sprawdzić certyfikat MIC, należy wyeksportować główny certyfikat fabryczny i certyfikat urzędu certyfikacji fabrycznej z telefonu IP Cisco i zainstalować je na serwerze Cisco ACS. Te dwa certyfikaty są częścią łańcucha zaufanych certyfikatów używanych do weryfikowania certyfikatu MIC przez serwer Cisco ACS.

Aby sprawdzić certyfikat Cisco ACS, należy wyeksportować zaufany certyfikat podrzędny i certyfikat główny (utworzony przez urząd certyfikacji) z serwera Cisco ACS i zainstalować go w telefonie. Te certyfikaty są częścią łańcucha zaufanych certyfikatów używanych do sprawdzania zaufania certyfikatu z serwera ACS.

### Certyfikat instalowany przez użytkownika

Aby można było używać certyfikatu zainstalowanego przez użytkownika, zostaje wygenerowane żądanie podpisania certyfikatu (CSR, Certificate Signing Request) i wysłane do urzędu certyfikacji w celu zatwierdzenia. Certyfikat użytkownika może zostać również wygenerowany przez urząd certyfikacji bez żądania CSR.

Podczas uwierzytelniania EAP-TLS serwer ACS sprawdza zaufanie telefonu, a telefon sprawdza zaufanie serwera ACS.

Aby sprawdzić autentyczność certyfikatu zainstalowanego przez użytkownika, należy zainstalować zaufane certyfikaty podrzędne (jeśli istnieją) i główny certyfikat z urzędu certyfikacji, który zatwierdził certyfikat użytkownika na serwerze Cisco ACS. Te certyfikaty są częścią łańcucha zaufanych certyfikatów używanych do sprawdzania zaufania certyfikatu zainstalowanego przez użytkownika.

Aby sprawdzić certyfikat serwera Cisco ACS, należy wyeksportować zaufany certyfikat podrzędny (jeśli istnieje) i certyfikat główny (utworzony przez urząd certyfikacji) z serwera Cisco ACS i zainstalować go w telefonie. Te certyfikaty są częścią łańcucha zaufanych certyfikatów używanych do sprawdzania zaufania certyfikatu z serwera ACS.

### Instalowanie certyfikatów uwierzytelniania EAP-TLS

Aby zainstalować certyfikaty uwierzytelniania protokołu EAP-TLS, wykonaj następujące czynności.

### Procedura

---

- Krok 1** Na stronie WWW telefonu ustaw w telefonie datę i godzinę programu Cisco Unified Communications Manager.
- Krok 2** W przypadku używania certyfikatu MIC (Manufacturing Installed Certificate):
- Na stronie WWW telefonu wyeksportuj certyfikat głównego urzędu certyfikacji i certyfikat urzędu certyfikacji producenta.
  - W programie Internet Explorer zainstaluj certyfikaty na serwerze Cisco ACS i przeprowadź edycję listy zaufanych.
  - Zaimportuj główny urząd certyfikacji do telefonu.

Więcej informacji:

- [Eksportowanie i instalowanie certyfikatów na serwerze ACS, na stronie 107](#)
- [Eksportowanie certyfikatu urzędu certyfikacji z serwera ISE za pomocą usługi certyfikatów firmy Microsoft, na stronie 107](#)

- Krok 3** Za pomocą narzędzia konfiguracyjnego ACS skonfiguruj konto użytkownika.

Więcej informacji:

- [Konfigurowanie konta użytkownika ACS i instalowanie certyfikatu, na stronie 109](#)
- [Podręcznik użytkownika programu Cisco Secure ACS dla systemu Windows](http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html)(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

### Ustawianie daty i godziny

Uwierzytelnianie na podstawie certyfikatu EAP-TLS wymaga, aby wewnętrzny zegar telefonu IP Cisco był poprawnie ustawiony. Data i godzina w telefonie może się zmienić, gdy jest on zarejestrowany w programie Cisco Unified Communications Manager.



- Uwaga** W przypadku żądania nowego certyfikatu uwierzytelniania serwera, jeśli czas lokalny jest późniejszy niż czas Greenwich (GMT), weryfikacja certyfikatów uwierzytelniania może się nie udać. Firma Cisco zaleca ustawienie lokalnej daty i godziny wcześniejszej niż czas Greenwich (GMT).

Aby w telefonie ustawić poprawną lokalną datę i godzinę, wykonaj następujące czynności.

### Procedura

---

- Krok 1** Wybierz opcję **Data i godzina** w lewym okienku nawigacyjnym.
- Krok 2** Jeśli ustawienie w polu Bieżąca data i godzina w telefonie różni się od ustawienia w polu Lokalna data i godzina, kliknij przycisk **Ustaw lokalną datę i godzinę w telefonie**.

**Krok 3** Kliknij przycisk **Ponowne uruchomienie telefonu**, a następnie przycisk **OK**.

---

### Eksportowanie i instalowanie certyfikatów na serwerze ACS

Aby korzystać z certyfikatu MIC, wyeksportuj certyfikat główny producenta i certyfikat urzędu certyfikacji producenta, a następnie zainstaluj je na serwerze Cisco ACS.

Aby wyeksportować certyfikat główny producenta oraz certyfikat urzędu certyfikacji producenta na serwer ACS, wykonaj następujące czynności.

#### Procedura

---

**Krok 1** Na stronie WWW telefonu wybierz opcję **Certyfikaty**.

**Krok 2** Kliknij przycisk **Eksportuj** obok certyfikatu głównego producenta.

**Krok 3** Zapisz certyfikat i skopiuj go na serwer ACS.

**Krok 4** Powtórz kroki 1 i 2 dla certyfikatu urzędu certyfikacji producenta.

**Krok 5** Na stronie Konfiguracja systemu serwera ACS wprowadź ścieżkę do pliku dla każdego certyfikatu i zainstaluj certyfikaty.

**Uwaga** Aby uzyskać więcej informacji o korzystaniu z narzędzia konfiguracyjnego serwera ACS, zobacz pomoc online serwera ACS lub *podręcznik użytkownika programu Cisco Secure ACS dla systemu Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>).

**Krok 6** Strona Edycja listy zaufanych certyfikatów (CTL) umożliwia dodawanie certyfikatów, które mają być zaufane przez serwer ACS.

---

### Metody eksportu certyfikatów ACS

W zależności od typu certyfikatu eksportowanego z serwera ACS należy skorzystać z jednej z następujących metod:

- Aby wyeksportować certyfikat urzędu certyfikacji z serwera ACS, który podpisał certyfikat zainstalowany przez użytkownika lub certyfikat ACS, zobacz [Eksportowanie certyfikatu urzędu certyfikacji z serwera ISE za pomocą usługi certyfikatów firmy Microsoft, na stronie 107](#).
- Aby wyeksportować certyfikat urzędu certyfikacji z serwera ACS, który używa certyfikatu z podpisem własnym, zobacz [Eksportowanie certyfikatu urzędu certyfikacji z serwera ACS za pomocą programu Internet Explorer, na stronie 108](#).

### Eksportowanie certyfikatu urzędu certyfikacji z serwera ISE za pomocą usługi certyfikatów firmy Microsoft

Poniższa metoda umożliwia wyeksportowanie certyfikatu urzędu certyfikacji z serwera ISE, który podpisał certyfikat zainstalowany przez użytkownika lub certyfikat ISE.

Aby wyeksportować certyfikat urzędu certyfikacji przy użyciu strony WWW usług certyfikatów firmy Microsoft, wykonaj następujące czynności:

### Procedura

---

- Krok 1** Na stronie WWW usługi certyfikatów firmy Microsoft wybierz opcję **Pobieranie certyfikatu urzędu certyfikacji, łańcucha certyfikatów lub listy CRL**.
- Krok 2** Na następnej stronie zaznacz w polu tekstowym bieżący certyfikat urzędu certyfikacji, jako metodę kodowania wybierz DER, a następnie kliknij przycisk **Pobierz certyfikat urzędu certyfikacji**.
- Krok 3** Zapisz certyfikat urzędu certyfikacji.
- 

### Eksportowanie certyfikatu urzędu certyfikacji z serwera ACS za pomocą programu Internet Explorer

Użyj tej metody, aby wyeksportować certyfikat urzędu certyfikacji z serwera ACS, który używa certyfikatu z podpisem własnym.

Aby wyeksportować certyfikaty z serwera ACS za pomocą programu Internet Explorer, wykonaj następujące czynności:

### Procedura

---

- Krok 1** W programie Internet Explorer wybierz kolejno polecenia **Narzędzia > Opcje internetowe**, a następnie kliknij kartę **Zawartość**.
- Krok 2** W obszarze **Certyfikaty** kliknij opcję **Certyfikaty**, a następnie kartę **zaufanych głównych urzędów certyfikacji**.
- Krok 3** Zaznacz certyfikat główny i kliknij przycisk **Eksportuj**. Zostanie wyświetlony Kreator eksportu certyfikatów.
- Krok 4** Kliknij przycisk **Dalej**.
- Krok 5** W następnym oknie wybierz **DER zakodowany binarnie algorytmem X.509 (. CER)**, a następnie kliknij przycisk **Dalej**.
- Krok 6** Określ nazwę certyfikatu i kliknij przycisk **Dalej**.
- Krok 7** Zapisz certyfikat urzędu certyfikacji, który ma zostać zainstalowany na telefonie.
- 

### Żądanie i importowanie certyfikatu instalowanego przez użytkownika

W celu zażądania i zainstalowania certyfikatu w telefonie należy wykonać następujące czynności.

### Procedura

---

- Krok 1** Na stronie WWW telefonu należy wybrać profil sieci, w którym jest używany protokół EAP-TLS, i wybrać w polu certyfikatu EAP-TLS polecenie **Zainstalowane przez użytkownika**.
- Krok 2** Kliknij przycisk **Certyfikaty**.

Na stronie **Instalacja certyfikatu użytkownika** pole **Nazwa pospolita** powinno zawierać nazwę użytkownika na serwerze ACS.

**Uwaga** W razie potrzeby można dokonać edycji pola **Nazwa pospolita**. Upewnij się, że jest ona taka sama, jak nazwa użytkownika serwera ACS. Zobacz [Konfigurowanie konta użytkownika ACS i instalowanie certyfikatu, na stronie 109](#).

- Krok 3** Wprowadź informacje, które mają być wyświetlane na certyfikacie, a następnie kliknij przycisk **Wyślij**, aby wygenerować żądanie podpisania certyfikatu (CSR).
- 

### Instalowanie certyfikatu głównego serwera uwierzytelniania

W celu zainstalowania certyfikatu w telefonie należy wykonać następujące czynności.

#### Procedura

---

- Krok 1** Wyeksportuj certyfikat główny serwera uwierzytelniania z ACS. Zobacz [Metody eksportu certyfikatów ACS, na stronie 107](#).
- Krok 2** Przejdź na stronę WWW telefonu i wybierz opcję **Certyfikaty**.
- Krok 3** Kliknij przycisk **Importuj** znajdujący się obok certyfikatu głównego serwera uwierzytelniania.
- Krok 4** Uruchom ponownie telefon.
- 

### Konfigurowanie konta użytkownika ACS i instalowanie certyfikatu

Aby skonfigurować konto użytkownika i zainstalować certyfikat główny MIC telefonu na serwerze ACS, wykonaj następujące czynności.



- Uwaga** Aby uzyskać więcej informacji o korzystaniu z narzędzia konfiguracyjnego serwera ACS, zobacz pomoc online serwera ACS lub *podręcznik użytkownika programu Cisco Secure ACS dla systemu Windows*.
- 

#### Procedura

---

- Krok 1** W narzędziu konfiguracji serwera ACS na stronie Ustawienia użytkownika utwórz konto użytkownika telefonu, jeśli jeszcze nie istnieje.
- Zazwyczaj nazwa użytkownika zawiera na końcu adres MAC telefonu. Dla protokołu EAP-TLS hasło nie jest wymagane.
- Uwaga** Upewnij się, że nazwa użytkownika jest taka sama, jak w polu Nazwa pospolita na stronie Instalacja certyfikatu użytkownika. Zobacz [Żądanie i importowanie certyfikatu instalowanego przez użytkownika, na stronie 108](#).
- Krok 2** Na stronie Konfiguracja systemu w sekcji EAP-TLS włącz następujące pola:
- **Zezwalaj na EAP-TLS**
  - **Porównanie certyfikatu CN**
- Krok 3** Na stronie Ustawienia urzędu certyfikacji ACS dodaj główny certyfikat fabryczny i certyfikat urzędu certyfikacji fabrycznej do serwera ACS.

**Krok 4** Włącz oba certyfikaty na liście zaufanych certyfikatów serwera ACS.

## Konfiguracja PEAP

Protokół Protected Extensible Authentication Protocol (PEAP) używa certyfikatów klucza publicznego po stronie serwera do uwierzytelniania klientów przez utworzenie szyfrowanego tunelu SSL/TLS między klientem a serwerem uwierzytelniania.

Telefon IP Cisco 8865 obsługuje tylko jeden certyfikat serwera, który można zainstalować przy użyciu protokołu SCEP lub metodą ręcznej instalacji, ale nie za pomocą obu tych metod. Telefon nie obsługuje instalacji certyfikatu przy użyciu protokołu TFTP.



**Uwaga** Weryfikację serwera uwierzytelniania można włączyć, importując certyfikat serwera uwierzytelniania.

### Zanim rozpocznie

Przed skonfigurowaniem w telefonie uwierzytelniania PEAP upewnij się, że są spełnione wymagania protokołu Cisco Secure ACS:

- Musi być zainstalowany certyfikat główny ACS.
- Można również zainstalować certyfikat, aby włączyć weryfikację serwera dla uwierzytelniania PEAP. Jeśli certyfikat serwera jest zainstalowany, weryfikacja serwera jest włączona.
- Musi być włączone ustawienie protokołu EAP-MSCHAPv2.
- Należy skonfigurować konto użytkownika i hasło.
- W przypadku uwierzytelniania hasła można użyć lokalnej lub zewnętrznej bazy danych ACS (np. bazy danych systemu Windows lub LDAP).

### Włączanie uwierzytelniania PEAP

#### Procedura

**Krok 1** Na stronie WWW konfiguracji telefonu wybierz tryb uwierzytelniania PEAP.

**Krok 2** Wprowadź nazwę użytkownika i hasło.

## Bezpieczeństwo sieci bezprzewodowej

Telefony Cisco obsługujące sieć Wi-Fi mają więcej wymagań dotyczących zabezpieczeń i wymagają dodatkowej konfiguracji. Te dodatkowe kroki obejmują instalowanie certyfikatów oraz konfigurowanie zabezpieczeń w telefonach i w programie Cisco Unified Communications Manager.

Więcej informacji na ten temat można znaleźć w podręczniku *Security Guide for Cisco Unified Communications Manager* (Podręcznik zabezpieczeń programu Cisco Unified Communications Manager).



## Strona administrowania telefonem IP Cisco

Telefony Cisco obsługujące technologię Wi-Fi mają specjalne strony WWW, które różnią się od stron przeznaczonych dla innych telefonów. Te specjalne strony WWW służą do konfigurowania zabezpieczeń telefonu w przypadku niedostępności protokołu SCEP (Simple Certificate Enrollment Protocol). Użyj tych stron do ręcznego instalowania w telefonie certyfikatów zabezpieczeń, pobierania certyfikatów zabezpieczeń lub do ręcznego konfigurowania daty i godziny telefonu.

Na tych stronach WWW znajdują się również takie same informacje jak wyświetlane na innych stronach WWW telefonu, w tym informacje o urządzeniu, konfiguracji sieci, dziennikach i informacje statystyczne.

### Tematy pokrewne

[Strona WWW telefonu IP Cisco](#), na stronie 246

### Konfigurowanie strony administrowania telefonem

Telefon dostarczony bezpośrednio od producenta ma włączoną stronę WWW administrowania, a ustawionym hasłem jest „Cisco”. Jeśli jednak telefon zostanie zarejestrowany w programie Cisco Unified Communications Manager, strona WWW administrowania musi zostać włączona i musi zostać ustawione nowe hasło.

Włącz tę stronę WWW i ustaw poświadczenia logowania przed pierwszym użyciem strony WWW po zarejestrowaniu telefonu.

Po włączeniu strona WWW administrowania jest dostępna w protokole HTTPS na porcie 8443 (<https://x.x.x.x:8443>, gdzie x.x.x.x jest adresem IP telefonu).

### Zanim rozpocznie

Przed włączeniem strony WWW administrowania wybierz hasło. Hasło może być dowolną kombinacją liter lub cyfr, ale musi mieć długość 8–127 znaków.

Nazwa użytkownika jest ustawiona na stałe jako „admin”.

### Procedura


- 
- |               |   |
|---------------|---|
| <b>Krok 1</b> | W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje <b>Urządzenie &gt; Telefon</b> .           |
| <b>Krok 2</b> | Zlokalizuj swój telefon.  |
| <b>Krok 3</b> | W oknie <b>Układ konfiguracji specyficznej dla produktu</b> ustaw wartość parametru <b>Administracja WWW</b> na <b>Włączone</b> . |
| <b>Krok 4</b> | W polu <b>Hasło administratora</b> wpisz hasło.   |
| <b>Krok 5</b> | Wybierz opcję <b>Zapisz</b> i kliknij przycisk <b>OK</b> .  |
| <b>Krok 6</b> | Wybierz opcję <b>Zastosuj konfigurację</b> i kliknij przycisk <b>OK</b> .   |
| <b>Krok 7</b> | Uruchom ponownie telefon.   |
- 

### Dostęp do strony WWW administrowania telefonem

Aby uzyskać dostęp do strony WWW administracji, należy podać port administracji.

## Procedura

---

- Krok 1** Uzyskaj adres IP telefonu:
- W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon** i zlokalizuj telefon. Adres IP telefonu rejestrującego się w programie Cisco Unified Communications Manager jest widoczny w oknie **Znajdowanie i wyświetlanie telefonów** i w górnej części okna **Konfiguracja telefonu**.
  - W telefonie naciśnij klawisz **Aplikacje** , wybierz opcję **Informacje o telefonie**, a następnie przewiń do pola Adres IPv4.
- Krok 2** Otwórz przeglądarkę internetową i wprowadź następujący adres URL, gdzie *IP\_address* to adres IP telefonu IP Cisco:
- https://<IP\_address>:8443**
- Krok 3** W polu Hasło wpisz hasło.
- Krok 4** Kliknij przycisk **Wyślij**.
- 

## Instalowanie certyfikatu użytkownika ze strony WWW administrowania telefonem

W razie niedostępności protokołu Simple Certificate Enrollment Protocol (SCEP) można ręcznie zainstalować certyfikat użytkownika w telefonie.

Wstępnie zainstalowany Certyfikat instalowany fabrycznie (MIC, Manufacturing Installed Certificate) może służyć jako certyfikat użytkownika dla protokołu EAP-TLS.

Po zainstalowaniu certyfikatu użytkownika należy dodać go do listy zaufanych certyfikatów serwera RADIUS.

### Zanim rozpoczniesz

Zanim będzie można zainstalować certyfikat użytkownika dla telefonu, należy przygotować:

- Certyfikat użytkownika zapisany na komputerze. Certyfikat musi być w formacie PKCS #12.
- Hasło wyodrębniania certyfikatu.

## Procedura

---

- Krok 1** Na stronie WWW administrowania telefonem wybierz opcję **Certyfikaty**.
- Krok 2** Znajdź pole Zainstalowane przez użytkownika i kliknij opcję **Zainstaluj**.
- Krok 3** Przejdź do certyfikatu na swoim komputerze.
- Krok 4** W polu **Hasło wyodrębniania** wprowadź hasła wyodrębniania certyfikatu.
- Krok 5** Kliknij przycisk **Prześlij**.
- Krok 6** Po zakończeniu przekazywania ponownie uruchom telefon.
-

## Instalowanie certyfikatu serwera uwierzytelniania ze strony WWW administrowania telefonem

W razie niedostępności protokołu Simple Certificate Enrollment Protocol (SCEP) można ręcznie zainstalować certyfikat serwera uwierzytelniania w telefonie.

W przypadku protokołu EAP-TLS musi być zainstalowany certyfikat głównego urzędu certyfikacji, który wydał certyfikat serwera RADIUS.

### Zanim rozpocznie

Zanim będzie można zainstalować certyfikat w telefonie, trzeba zapisać na komputerze certyfikat serwera uwierzytelniania. Certyfikat musi być zakodowany w pliku PEM (Base-64) lub DER.

### Procedura

---

- Krok 1** Na stronie WWW administrowania telefonem wybierz opcję **Certyfikaty**.
  - Krok 2** Znajdź pole **Urząd certyfikacji serwera uwierzytelniania (strona internetowa administratora)** i kliknij polecenie **Instaluj**.
  - Krok 3** Przejdź do certyfikatu na swoim komputerze.
  - Krok 4** Kliknij przycisk **Prześlij**.
  - Krok 5** Po zakończeniu przekazywania ponownie uruchom telefon.
- Jeśli instalujesz więcej niż jeden certyfikat, należy zainstalować je wszystkie przed ponownym uruchomieniem telefonu.
- 

## Ręczne usuwanie certyfikatu zabezpieczeń ze strony WWW administrowania telefonem

Jeśli protokół SCEP (Simple Certificate Enrollment Protocol) jest niedostępny, można ręcznie usunąć certyfikat zabezpieczeń z telefonu.

### Procedura

---

- Krok 1** Na stronie WWW administrowania telefonem wybierz opcję **Certyfikaty**.
  - Krok 2** Znajdź certyfikat na stronie **Certyfikaty**.
  - Krok 3** Kliknij pozycję **Usuń**.
  - Krok 4** Uruchom ponownie telefon po zakończeniu procesu usuwania.
- 

## Ręczne ustawianie daty i godziny w telefonie

W przypadku stosowania uwierzytelniania opartego o certyfikat, telefon musi wyświetlać prawidłową datę i godzinę. Serwer uwierzytelniania porównuje datę i godzinę telefonu z datą ważności certyfikatu. Jeśli daty i godziny telefonu i serwera nie są zgodne, telefon przestaje działać.

Ta procedura służy do ręcznego ustawienia daty i godziny w telefonie, jeśli telefon nie odbiera prawidłowych informacji z sieci.

### Procedura

---

- Krok 1** Na stronie WWW administrowania telefonem przewiń do opcji **Data i godzina**.
- Krok 2** Wykonaj jedną z następujących czynności:
- Kliknij przycisk **Ustaw lokalną datę i godzinę w telefonie** w celu zsynchronizowania telefonu z serwerem lokalnym.
  - W polach **Określ datę i godzinę** przy użyciu menu wybierz miesiąc, dzień, rok, godzinę, minutę i sekundę, a następnie kliknij przycisk **Ustaw określoną datę i godzinę w telefonie**.
- 

## Konfiguracja protokołu SCEP

Protokół SCEP (Simple Certificate Enrollment Protocol) jest standardowym rozwiązaniem służącym do automatycznego dostarczania i odnawiania certyfikatów. Pozwala uniknąć ręcznej instalacji certyfikatów w telefonie.

### Konfigurowanie parametrów protokołu SCEP specyficznych dla produktu

Na stronie WWW telefonu należy skonfigurować następujące parametry SCEP

- Adres IP urzędu rejestrowania RA
- Odciski linii papilarnych certyfikatu głównego urzędu certyfikacji serwera protokołu SCEP w formacie SHA-1 lub SHA-256

Urząd rejestrowania Cisco IOS RA (Registration Authority) pełni rolę serwera proxy dla serwera protokołu SCEP. Klient SCEP w telefonie używa parametrów, które są pobierane z programu Cisco Unified Communication Manager. Po skonfigurowaniu parametrów z telefonu jest wysyłane żądanie SCEP `getcs` do urzędu rejestrowania RA, a certyfikat głównego urzędu certyfikacji jest sprawdzany przy użyciu zdefiniowanego odcisku.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon.
- Krok 3** Przewiń do obszaru **Układ konfiguracji specyficznej dla produktu**.
- Krok 4** Zaznacz pole wyboru **Serwer protokołu SCEP WLAN**, aby uaktywnić parametr SCEP.
- Krok 5** Zaznacz pole wyboru **Odcisk głównego urzędu certyfikacji WLAN (SHA256 lub SHA1)**, aby uaktywnić parametr SCEP QED.
- 

### Obsługa serwera protokołu Simple Certificate Enrollment Protocol

W przypadku korzystania z serwera SCEP (Simple Certificate Enrollment Protocol) serwer może automatycznie obsługiwać certyfikaty użytkownika i serwera. Na serwerze SCEP skonfiguruj agenta rejestracji SCEP (RA), aby wykonywał następujące funkcje:

- Pełnienie roli punktu zaufania infrastruktury klucza publicznego
- Pełnienie roli agenta rejestracji infrastruktury kluczy publicznych
- Uwierzytelnianie urządzeń za pomocą serwera RADIUS

Więcej informacji zawiera dokumentacja serwera SCEP.

## Uwierzytelnianie 802.1X

Telefony IP Cisco obsługują uwierzytelnianie 802.1X.

Telefony IP Cisco i przełączniki Cisco Catalyst używają tradycyjnie protokołu CDP (Cisco Discovery Protocol) do identyfikowania siebie nawzajem i ustalania parametrów, np. przydziału sieci VLAN i wymagań dotyczących zasilania poprzez kabel sieciowy. Protokół CDP nie rozpoznaje podłączonych lokalnie stacji roboczych. Telefony IP Cisco udostępniają mechanizm przelotowy protokołu EAPOL. Umożliwia on stacji roboczej podłączonej do telefonu IP Cisco przekazywanie komunikatów protokołu EAPOL stronie uwierzytelniającej 802.1X w przełączniku sieci LAN. Dzięki mechanizmowi przelotowemu telefon IP nie musi pełnić funkcji przełącznika sieci LAN, aby uwierzytelnić punkt końcowy danych przed uzyskaniem dostępu do sieci.

Telefony IP Cisco udostępniają również mechanizm zastępczego wylogowywania w ramach protokołu EAPOL. W sytuacji, gdy podłączony lokalnie komputer przerwie połączenie z telefonem IP, przełącznik sieci LAN nie zauważy awarii łącza fizycznego, ponieważ łącze między przełącznikiem sieci LAN a telefonem IP zostanie zachowane. Aby zapobiec naruszeniu bezpieczeństwa sieci, telefon IP wysyła do przełącznika komunikat wylogowania w ramach protokołu EAPOL w imieniu komputera, co powoduje wyczyszczenie wpisu uwierzytelnienia komputera w przełączniku.

Obsługa uwierzytelniania 802.1X wymaga kilku składników:

- Telefon IP Cisco: telefon inicjuje żądanie dostępu do sieci. Telefony IP Cisco zawierają stronę uwierzytelnianą 802.1X. Dzięki niej administratorzy sieci mogą kontrolować łączność telefonów IP z portami przełącznika sieci LAN. Bieżąca wersja strony uwierzytelnianej 802.1X w telefonach korzysta z opcji EAP-FAST i EAP-TLS do uwierzytelniania sieci.
- Serwer ACS (Cisco Secure Access) (lub serwer uwierzytelniania innej firmy): serwer uwierzytelniania i telefon muszą mieć skonfigurowany klucz współdzielony, który służy do uwierzytelniania telefonu.
- Przełącznik Cisco Catalyst (lub przełącznik innej firmy): przełącznik musi być zgodny ze standardem 802.1X, aby mieć możliwość pełnienia funkcji strony uwierzytelniającej i przekazywania komunikatów między telefonem a serwerem uwierzytelniania. Po zakończeniu wymiany komunikatów przełącznik przyznaje telefonowi dostęp do sieci lub odrzuca jego żądanie.

Aby skonfigurować uwierzytelnianie 802.1X:

- Skonfiguruj pozostałe składniki, zanim włączysz w telefonie uwierzytelnianie 802.1X.
- Skonfiguruj port komputera: w standardzie 802.1X nie uwzględniono sieci VLAN, więc zaleca się uwierzytelnianie tylko jednego urządzenia na każdym porcie przełącznika. Niektóre przełączniki (m.in. Cisco Catalyst) obsługują jednak uwierzytelnianie w wielu domenach. Konfiguracja przełącznika określa, czy do portu komputera w telefonie można podłączyć komputer.
  - Włączone: jeśli korzystasz z przełącznika, który obsługuje uwierzytelnianie w wielu domenach, możesz włączyć port komputera i podłączyć do niego komputer. W takim przypadku telefony IP Cisco obsługują zastępcze wylogowywanie w ramach protokołu EAPOL, aby monitorować wymianę

komunikatów dotyczących uwierzytelniania między przełącznikiem a podłączonym komputerem. Więcej informacji o zgodności przełączników Cisco Catalyst ze standardem IEEE 802.1X można znaleźć w ich podręcznikach konfiguracji pod adresem:


[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

- **Wyłączone:** jeśli przełącznik nie obsługuje na tym samym porcie wielu urządzeń zgodnych ze standardem 802.1X, po włączeniu uwierzytelniania 802.1X wyłącz port komputera. W przeciwnym razie przy próbie podłączenia do niego komputera przełącznik odmówi dostępu do sieci zarówno telefonowi, jak i komputerowi.
- Skonfiguruj opcję VLAN głosowy: w standardzie 802.1X nie uwzględniono sieci VLAN, więc skonfiguruj tę opcję zgodnie z zakresem obsługi uwierzytelniania przez przełącznik.
  - **Włączone:** jeśli korzystasz z przełącznika, który obsługuje uwierzytelnianie w wielu domenach, możesz kontynuować korzystanie z sieci VLAN komunikacji głosowej.
  - **Wyłączone:** jeśli przełącznik nie obsługuje uwierzytelniania w wielu domenach, wyłącz opcję VLAN głosowy i rozważ przypisanie portu macierzystej sieci VLAN.

## Dostęp do uwierzytelniania 802.1X

Dostęp do ustawień uwierzytelniania 802.1X można uzyskać, wykonując następujące czynności:

### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
  - Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja zabezpieczeń** > **Uwierzytelnianie 802.1X**.
  - Krok 3** Skonfiguruj opcje zgodnie z opisem w temacie [Opcje uwierzytelniania 802.1X, na stronie 116](#).
  - Krok 4** Aby opuścić to menu, naciśnij przycisk **Wyjdź**.
- 

### Opcje uwierzytelniania 802.1X

W poniższej tabeli zamieszczono opis opcji uwierzytelniania 802.1X.


**Tabela 29: Ustawienia uwierzytelniania 802.1X**

Opcja	Opis	Aby zmienić
Uwierzyt. urządzenia	Określa, czy uwierzytelnianie 802.1X jest włączone: <ul style="list-style-type: none"> <li>• <b>Włączone:</b> telefon używa uwierzytelniania 802.1X w celu żądania dostępu do sieci.</li> <li>• <b>Wyłączone:</b> ustawienie domyślne. Telefon używa protokołu CDP, aby uzyskać dostęp do sieci i sieci VLAN.</li> </ul>	Zobacz <a href="#">Konfigurowanie pola Uwierzytelniania urządzenia, na stronie 117</a> .

Opcja	Opis	Aby zmienić
Stan transakcji	<p>Stan: wyświetla stan uwierzytelniania 802.1x:</p> <ul style="list-style-type: none"> <li>• Odłączone: wskazuje, że uwierzytelnianie 802.1x nie jest skonfigurowane w telefonie.</li> <li>• Uwierzytelnione: wskazuje, że telefon jest uwierzytelniony.</li> <li>• Zawieszony: wskazuje, że proces uwierzytelniania jest w toku.</li> </ul> <p>Protokół: wyświetla metodę EAP, która jest używana do uwierzytelniania 802.1x (może to być EAP-FAST lub EAP-TLS).</p>	Tylko wyświetlanie. Opcji tej nie można konfigurować.

## Konfigurowanie pola Uwierzytelnianie urządzenia

### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja zabezpieczeń** > **Uwierzytelnianie 802.1X.**
- Krok 3** Ustaw opcję Uwierzytelnianie urządzenia:
- **Tak**
  - **Nie**
- Krok 4** Naciśnij przycisk **Zastosuj.**
-







## ROZDZIAŁ 8

# Dostosowywanie telefonu IP Cisco

- Niestandardowe dzwonki telefonu, na stronie 119
- Niestandardowe obrazy tła, na stronie 119
- Konfigurowanie kodeka komunikacji szerokopasmowej, na stronie 121
- Konfigurowanie ekranu bezczynności, na stronie 122
- Dostosowywanie sygnału wybierania, na stronie 123

## Niestandardowe dzwonki telefonu

Telefon jest wyposażony w trzy dzwonki, które są zaimplementowane sprzętowo: Sunshine, Chirp i Chirp1.

Program Cisco Unified Communications Manager udostępnia ponadto domyślny zestaw dodatkowych dźwięków dzwonka telefonu, które są zaimplementowane w warstwie programowej jako pliki PCM (ang. pulse code modulation, modulacja impulsowo-kodowa). Pliki PCM razem z plikiem XML (o nazwie Ringlist-wb.xml), w którym opisano opcje listy dzwonek dostępnych w siedzibie użytkownika, znajdują się w katalogu TFTP na każdym serwerze Cisco Unified Communications Manager.



**Uwaga** We wszystkich nazwach plików rozróżniana jest wielkość liter. W przypadku użycia pliku o nazwie Ringlist-wb.xml telefon nie zastosuje wprowadzonych w nim zmian.

Więcej informacji można znaleźć w rozdziale „Custom Phone Rings and Backgrounds” w podręczniku [Feature Configuration Guide for Cisco Unified Communications Manager](#) dla systemu Cisco Unified Communications Manager w wersji 12.0 (1) lub nowszej.

## Niestandardowe obrazy tła

Można dostosować obraz tła lub tapetę telefonu IP Cisco. Dostosowana tapeta jest popularnym sposobem wyświetlania logo firm lub obrazów, a wiele organizacji korzysta z nich do ozdoby swoich telefonów.

Od wersji oprogramowania sprzętowego 12.7(1) można dostosowywać tapety zarówno w telefonach, jak i w modułach rozbudowy klawiatury. Plik obrazu potrzebny jest zarówno dla telefonu jak i dla modułu rozszerzenia klawiatury.

Telefon analizuje kolory tapet, zmienia kolory czcionek i ikon, abyś mógł je odczytać. Jeśli tapeta jest ciemna, telefon zmieni czcionki i ikony na białe. Jeśli tapeta jest jasna, na telefonie zostaną wyświetlone czarne czcionki i ikony.

Najlepiej jest wybrać prosty obraz, taki jak jednolity kolor lub wzór dla swojego tła. Należy również unikać obrazów o dużym kontraście.

Dostosowaną tapetę można dodać na jeden z dwóch sposobów:

- za pomocą pliku listy,
- za pomocą wspólnego profilu telefonu.

Jeśli chcesz, aby użytkownik mógł wybierać obraz spośród różnych tapet dostępnych w telefonie, wówczas zmodyfikuj plik listy. Jeśli chcesz natomiast przesłać obraz na telefon, wówczas utwórz lub zmodyfikuj istniejący wspólny profil telefonu.

Niezależnie od wybranego sposobu należy pamiętać o następujących kwestiach:

- Obrazy muszą być w formacie PNG i wymiary pełnego obrazu nie mogą być większe niż:
  - Miniatury mogą mieć szerokość 139 pikseli i wysokość 109 pikseli.
  - Telefon IP Cisco z serii 8800 — 800 pikseli na 480 pikseli
  - Moduł rozbudowy klawiatury Telefonu IP Cisco 8851 i 8861 z podwójnym ekranem LCD — o rozdzielczości 320 na 480 pikseli
  - Moduł rozbudowy klawiatury telefonu IP Cisco 8865 z podwójnym ekranem LCD — o rozdzielczości 320 na 480 pikseli
  - Moduł rozbudowy klawiatury Telefonu IP Cisco 8800 z podwójnym ekranem LCD — o rozdzielczości 272 na 480 pikseli
- Umieść obrazy i plik listy na serwerze TFTP. Katalog:
  - Telefony IP Cisco z serii 8800 — Desktops/800x480x24
  - Moduł rozbudowy klawiatury telefonu IP Cisco 8851/8861 z dwoma ekranami - Desktop/320x480x24
  - Moduł rozbudowy klawiatury telefonu IP Cisco 8865 z dwoma ekranami - Desktops/320x480x24
  - Moduł rozbudowy klawiatury Telefonu IP Cisc 8800 z pojedynczym ekranem LCD — Desktops/272x480x24

Po zakończeniu przekazywania uruchom ponownie serwer.

- Jeśli nie chcesz, aby użytkownik wybierał własną tapetę, wówczas usuń wybór opcji **Zezwól użytkownikowi na ustawianie obrazu tła telefonu**. Zapisz i zastosuj profilu telefonu. Uruchom ponownie telefony, aby zastosować zmiany.



**Uwaga** Obrazy tła telefonu można stosować masowo za pomocą **wspólnego profilu telefonu**. Konfiguracja masowa wymaga jednak wyłączenia opcji **Włączenie dostępu użytkownika końcowego do ustawień obrazu tła telefonu**. Aby uzyskać więcej informacji na temat masowej konfiguracji obrazów tła, zapoznaj się z rozdziałem “Konfiguracja wspólnego profilu telefonu” w rozdziale [Dostosowane tapety: Najlepsze praktyki w telefonach IP Cisco z serii 8800.](#))

Aby uzyskać więcej informacji o dostosowywaniu tapety, zapoznaj się z następującą dokumentacją:

- [Dostosowane tapety: Najlepsze praktyki w telefonach IP Cisco z serii 8800.](#))
- Więcej informacji można znaleźć w rozdziale „Custom Phone Rings and Backgrounds” w podręczniku [Feature Configuration Guide for Cisco Unified Communications Manager](#) dla systemu Cisco Unified Communications Manager w wersji 12.0(1) lub nowszej.
- Rozdział “Ustawienia” w *Podręczniku użytkownika telefonów IP Cisco z serii 8800.*

## Konfigurowanie kodeka komunikacji szerokopasmowej

Domyślnie w telefonie IP Cisco włączony jest kodek G.722. Jeśli program Cisco Unified Communications Manager został skonfigurowany do użycia kodeka G.722 i punkt końcowy po drugiej stronie łącza również obsługuje kodek G.722, połączenie jest realizowane z użyciem kodeka G.722 zamiast G.711.

Odbywa się to niezależnie od tego, czy użytkownik włączył szerokopasmowy zestaw nagłowny lub szerokopasmową słuchawkę, ale jeśli zestaw nagłowny lub słuchawka są włączone, użytkownik może zauważyć podczas rozmowy większą szczegółowość dźwięku. Większa szczegółowość dźwięku przekłada się na wzrost jego wyrazistości, ale oznacza również, że rozmówca może słyszeć więcej szumów tła, np. szeleszczenie papierów czy trwające w pobliżu konwersacje. Nawet bez szerokopasmowego zestawu nagłownego lub szerokopasmowej słuchawki niektórzy użytkownicy mogą uważać zwiększoną szczegółowość dźwięku, jaką zapewnia kodek G.722, za rozpraszającą uwagę. Inni użytkownicy mogą natomiast preferować wzrost szczegółowości uzyskiwany dzięki kodekowi G.722.

Parametr usługi Zgłaszaj obecność kodeka G.722 i iSAC określa, czy obsługa komunikacji szerokopasmowej jest dostępna w przypadku wszystkich urządzeń zarejestrowanych na danym serwerze Cisco Unified Communications Manager, czy tylko dla wybranego telefonu, zależnie od okna aplikacji Cisco Unified Communication Manager, w którym parametr ten zostanie skonfigurowany.

### Procedura

#### Krok 1

Aby skonfigurować obsługę komunikacji szerokopasmowej dla wszystkich urządzeń:

- a) W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **System > Parametry systemu przedsiębiorstwa**.
- b) Skonfiguruj pole Zgłaszaj obecność kodeka G.722 i iSAC.

Wartość domyślna tego parametru systemu przedsiębiorstwa to **Prawda**, co oznacza, że wszystkie modele telefonów IP Cisco zarejestrowane na danym serwerze Cisco Unified Communications Manager zgłaszają

obecność kodeka G.722. Jeśli każdy punkt końcowy nawiązywanego połączenia obsługuje kodek G.722, program Cisco Unified Communications Manager wybiera ten kodek, gdy tylko jest to możliwe.

**Krok 2** Aby skonfigurować obsługę komunikacji szerokopasmowej dla konkretnego urządzenia:

- a) W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- b) Ustaw parametr Zgłaszaj obecność kodeka G.722 i iSAC w obszarze konfiguracji specyficznej dla produktu.

Wartością domyślną tego parametru danego produktu jest użycie wartości określonej w parametrze przedsiębiorstwa. Jeśli chcesz zastąpić tę wartość dla określonego telefonu, wybierz opcję **Włączone** lub **Wyłączone**.

## Konfigurowanie ekranu bezczynności

Można skonfigurować ekran bezczynności (sam tekst; rozmiar pliku tekstowego nie może przekraczać 1 MB), który pojawia się na wyświetlaczu telefonu. Ekran bezczynności to usługa XML, którą telefon wywołuje, gdy jest wolny (nie jest w użyciu) przez określony czas i nie jest wyświetlone żadne menu funkcji.

Szczegółowe instrukcje tworzenia i wyświetlania ekranu bezczynności można znaleźć na stronie *Creating Idle URL Graphics on Cisco IP Phone* (Tworzenie graficznej strony URL bezczynności na telefonie IP Cisco) pod tym adresem URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_tech\\_note09186a00801c0764.shtml](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml)

Ponadto w dokumentacji konkretnej wersji programu Cisco Unified Communications Manager można znaleźć informacje o następujących zagadnieniach:

- Określanie adresu URL usługi XML ekranu bezczynności:
  - W przypadku pojedynczego telefonu: pole Wolny w oknie Konfiguracja telefonu w aplikacji Cisco Unified Communications Manager Administration.
  - W przypadku wielu telefonów naraz: pole Wolny URL w oknie Enterprise Parameters Configuration (Konfiguracja parametrów systemu przedsiębiorstwa) lub pole Wolny w Narzędziu administracji zbiorczej
- Określanie czasu bezczynności telefonu przed wywołaniem usługi XML ekranu bezczynności:
  - W przypadku pojedynczego telefonu: pole Idle Timer (Czasomierz bezczynności) w oknie Konfiguracja telefonu w aplikacji Cisco Unified Communications Manager — administracja.
  - W przypadku wielu telefonów naraz: pole URL Idle Time (Czas wolnego URL) w oknie Enterprise Parameters Configuration (Konfiguracja parametrów systemu przedsiębiorstwa) lub pole Idle Timer (Czasomierz bezczynności) w Narzędziu administracji zbiorczej.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** W polu Wolny wprowadź adres URL usługi XML ekranu bezczynności.
- Krok 3** W polu Idle Timer (Czasomierz bezczynności) wprowadź czas, przez który nieużywany telefon wstrzymuje się z wyświetleniem usługi XML ekranu bezczynności.
- Krok 4** Kliknij przycisk **Zapisz**.
- 

## Dostosowywanie sygnału wybierania

Telefony można skonfigurować w taki sposób, aby użytkownicy słyszeli różne sygnały wybierania w przypadku połączeń wewnętrznych i zewnętrznych. Zależnie od potrzeb można wybrać jedną z trzech opcji sygnału wybierania:

- Domyślny: różne sygnały wybierania w przypadku połączeń wewnętrznych i zewnętrznych.
- Sieć wewnętrzna: w przypadku wszystkich połączeń stosowany jest sygnał wybierania połączeń wewnętrznych.
- Sieć zewnętrzna: w przypadku wszystkich połączeń stosowany jest sygnał wybierania połączeń zewnętrznych.

Wymagane jest skonfigurowanie pola Always Use Dial Tone (Zawsze używaj sygnału wybierania) w programie Cisco Unified Communications Manager.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **System > Service Parameters (Parametry usług)**.
- Krok 2** Wybierz odpowiedni serwer.
- Krok 3** Wybierz **Cisco CallManager** jako usługę.
- Krok 4** Przewiń do panelu Parametr całego klastra.
- Krok 5** Wybierz dla opcji **Zawsze używaj sygnału wybierania** jedno z następujących ustawień:
- Sieć zewnętrzna
  - Sieć wewnętrzna
  - Domyślny
- Krok 6** Kliknij przycisk **Zapisz**.
- Krok 7** Uruchom ponownie telefony.
-





## ROZDZIAŁ 9

# Funkcje telefonu i ich konfigurowanie

- [Przegląd funkcji telefonu i ich konfigurowania, na stronie 125](#)
- [Pomoc techniczna dla użytkowników telefonu IP Cisco, na stronie 125](#)
- [Funkcje telefonu, na stronie 126](#)
- [Przyciski funkcyjne i klawisze programowe, na stronie 146](#)
- [Konfigurowanie funkcji telefonu, na stronie 147](#)
- [Konfigurowanie szablonu klawiszy programowych, na stronie 204](#)
- [Szablony przycisków telefonu, na stronie 207](#)
- [Konfiguracja sieci VPN, na stronie 210](#)
- [Konfigurowanie klawiszy linii dodatkowej, na stronie 211](#)
- [Konfigurowanie zegara wznowienia TLS, na stronie 215](#)
- [Włączenie funkcji Intelligent Proximity, na stronie 215](#)
- [Ustawianie rozdzielczości transmisji wideo, na stronie 216](#)
- [Parametry zarządzania zestawem nagłownym w starszych wersjach programu Cisco Unified Communications Manager, na stronie 217](#)

## Przegląd funkcji telefonu i ich konfigurowania

Po zainstalowaniu telefonów IP Cisco w sieci skonfiguruj ich ustawienia sieciowe i dodaj je do programu Cisco Unified Communications Manager. Aplikacja Cisco Unified Communications Manager — administracja służy do konfigurowania funkcji telefonicznych, opcjonalnego modyfikowania szablonów telefonu, konfigurowania usług i przypisywania użytkowników.

Program Cisco Unified Communications Manager — administracja umożliwia również modyfikowanie dodatkowych ustawień telefonu IP. Ta aplikacja internetowa służy m.in. do ustawiania kryteriów rejestracji telefonu i obszarów wyszukiwania połączeń, a także do modyfikowania szablonów przycisków telefonu.

Podczas dodawania funkcji do klawiszy linii telefonicznej ograniczeniem jest liczba dostępnych klawiszy linii. Nie można dodać więcej funkcji niż liczba klawiszy linii na telefonie.

## Pomoc techniczna dla użytkowników telefonu IP Cisco

Jeśli jesteś administratorem systemu, stanowisz prawdopodobnie główne źródło informacji dla użytkowników telefonów IP Cisco w Twojej sieci lub firmie. Istotną rzeczą jest zapewnienie użytkownikom końcowym aktualnych i szczegółowych informacji.

Aby na telefonie IP Cisco z powodzeniem korzystać z niektórych funkcji (takich jak Usługi i opcje systemu wiadomości głosowych), użytkownicy muszą otrzymać informacje od Ciebie lub Twojego zespołu sieciowego albo muszą mieć możliwość skontaktowania się z Tobą w celu uzyskania pomocy. Zapewnij użytkownikom dostęp do nazwisk osób, z którymi mogą się skontaktować w celu uzyskania pomocy, oraz do instrukcji uzyskania kontaktu z nimi.

Zalecamy utworzenie strony WWW w wewnętrznej witrynie pomocy technicznej, która udostępni użytkownikom końcowym ważne informacje dotyczące ich telefonów IP Cisco.

Rozważ umieszczenie na tej stronie następujących rodzajów informacji:

- Podręczniki użytkownika dla wszystkich wspieranych modeli telefonów IP Cisco
- Informacje o sposobie dostępu do Portalu samoobsługowego Cisco Unified Communications
- Lista wspieranych funkcji
- Podręcznik użytkownika lub skrócona instrukcja obsługi systemu poczty głosowej

## Funkcje telefonu

Po dodaniu telefonów IP Cisco w programie Cisco Unified Communications Manager można do nich dodać funkcje. Poniższa tabela zawiera listę obsługiwanych funkcji telefonicznych, spośród których wiele można skonfigurować za pomocą narzędzia Cisco Unified Communications Manager — administracja.

Informacje na temat korzystania z większości tych funkcji na telefonie można znaleźć w *Podręczniku użytkownika telefonu IP Cisco z serii 8800*. Listę funkcji, które można skonfigurować jako klawisze programowalne, dedykowane klawisze programowe i klawisze funkcji, można znaleźć w sekcji [Przyciski funkcyjne i klawisze programowe, na stronie 146](#).



**Uwaga** Narzędzie Cisco Unified Communications Manager — administracja udostępnia także różne parametry usługi, które można wykorzystać do skonfigurowania różnych funkcji telefonicznych. Więcej informacji na temat uzyskiwania dostępu do parametrów usługi oraz ich konfigurowania można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Aby uzyskać więcej informacji na temat funkcji usługi, wybierz nazwę parametru lub **przycisk pomocy oznaczony znakiem zapytania (?)** w oknie [Konfiguracja specyficzna dla produktu](#).

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Funkcja	Opis i więcej informacji
Skrócone wybieranie	<p>Umożliwia użytkownikom szybkie wybieranie numeru telefonu poprzez wprowadzenie na klawiaturze telefonu przypisanego kodu indeksu (1-199).</p> <p><b>Uwaga</b> Z funkcji skróconego wybierania można korzystać z odłożoną lub podniesioną słuchawką.</p> <p>Użytkownicy przypisują kody indeksu za pośrednictwem Portalu samoobsługowego.</p>



Funkcja	Opis i więcej informacji
Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących)	<p>Udostępnia różne opcje sterowania alertami połączeń przychodzących. Alert połączenia można wyłączyć lub włączyć. Można również włączyć lub wyłączyć wyświetlanie identyfikatora abonenta dzwoniącego.</p> <p>Zobacz Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących), <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>.</p>
Obsługa algorytmu szyfrowania AES 256 w telefonach	<p>Rozszerza zabezpieczenia poprzez obsługę protokołu TLS 1.2 i nowych szyfrów. Aby uzyskać więcej informacji, patrz <a href="#">Obsługiwane funkcje zabezpieczeń, na stronie 88</a>.</p>
Powitanie agenta	<p>Umożliwia agentowi tworzenie i aktualizowanie nagranych powitań, które jest odtwarzane na początku połączenia, zanim agent odezwie się do dzwoniącego. Agent może nagrać jedno powitanie lub większą ich liczbę w zależności od potrzeb.</p> <p>Zobacz <a href="#">Włączanie funkcji Agent Greeting (Powitanie przez agenta), na stronie 181</a>.</p>
Przejmowanie dowolnego połączenia	<p>Umożliwia użytkownikom przejęcie połączenia na dowolnej linii w swoich grupach przejmowania połączeń, niezależnie od sposobu, w jaki połączenie zostało trasowane do telefonu.</p> <p>Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Strony WWW reguł wybierania numeru aplikacji	<p>Konwertuje numery ze współdzielonych kontaktów z urządzeń przenośnych na numery możliwe do wybrania w sieci.</p> <p>Zobacz <a href="#">Strony WWW reguł wybierania numeru aplikacji, na stronie 81</a>.</p>
Wspomagane kierowane parkowanie połączenia	<p>Umożliwia użytkownikom parkowanie połączenia za pomocą funkcji Direct Park (Parkowanie bezpośrednie) poprzez naciśnięcie tylko jednego przycisku. Przycisk Busy Lamp Field (BLF) Assisted Directed Call Park (Pole sygnalizacji aktywności linii przycisku Wspomagane kierowane parkowanie połączenia) musi zostać skonfigurowany przez administratora. Gdy użytkownik naciśnie wolny przycisk Wspomagane kierowane parkowania połączenia z polem SZL dla aktywnego połączenia, aktywne połączenie zostanie zaparkowane w gnieździe połączenia kierowanego związanego z przyciskiem Wspomagane kierowane parkowanie połączenia.</p> <p>Informacje o wspomaganym kierowanym parkowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Słyszalny wskaźnik wiadomości oczekującej	<p>Przerywany sygnał dźwiękowy w słuchawce, zestawie nagłownym lub telefonie głośnomówiącym wskazuje, że użytkownik ma na linii co najmniej jedną nową wiadomość głosową.</p> <p><b>Uwaga</b> Przerywany sygnał dźwiękowy dotyczy linii. Jest słyszalny tylko w przypadku używania linii z wiadomościami oczekującymi.</p>

Funkcja	Opis i więcej informacji
Automatyczne odbieranie	<p>Łączy połączenia przychodzące automatycznie po jednym lub dwóch dzwonkach.</p> <p>Funkcja Automatyczne odbieranie działa z zestawem głośnomówiącym lub zestawem nagłownym.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Automatyczna synchronizacja portów	<p>Synchronizuje porty, używając najniższej prędkości między portami telefonu w celu wyeliminowania utraconych pakietów.</p> <p>Zobacz Automatyczna synchronizacja portów, <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>.</p>
Automatyczne przejmowanie	<p>Umożliwia użytkownikowi przejmowanie połączeń za pomocą funkcji przejmowania jednym dotknięciem.</p> <p>Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Wtrąć	<p>Pozwala użytkownikowi na wtrącenie się do połączenia poprzez ustanowienie połączenia konferencyjnego za pomocą wbudowanego mostka konferencyjnego w telefonie docelowym.</p> <p>Zobacz “WtrąćKon” w tej tabeli.</p>
Blokowanie przekierowywania z zewnątrz na zewnątrz	<p>Uniemożliwia użytkownikom przekazanie zewnętrznego połączenia na inny numer zewnętrzny.</p> <p>Informacje o przekazywaniu połączeń zewnętrznych można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Wiele połączeń Bluetooth	<p>Umożliwia użytkownikowi sparowanie z telefonem wielu urządzeń. Użytkownik może wówczas jednocześnie podłączyć urządzenie przenośne przy użyciu protokołu Bluetooth i zestaw słuchawkowy Bluetooth.</p> <p>Telefon IP Cisco 8851NR nie obsługuje komunikacji Bluetooth.</p>
Pole sygnalizacji aktywności linii	<p>Umożliwia użytkownikowi monitorowanie stanu połączenia związanego numeru telefonu za pomocą przycisku szybkiego wybierania na telefonie.</p> <p>Informacje o obecności można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Pole sygnalizacji aktywności linii — przejęcie	<p>Udostępnia rozszerzenia szybkiego wybierania z funkcją SZL. Umożliwia skonfigurowanie numeru telefonu, dla którego użytkownik może monitorować połączenia przychodzące. Gdy na dany numer telefonu trafia połączenie przychodzące, system wysyła alert do monitorującego użytkownika, który może następnie przejąć połączenie.</p> <p>Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>

Funkcja	Opis i więcej informacji
Oddzwon	<p>Udostępnia alerty dźwiękowe i wizualne na telefonie, gdy jest on zajęty lub gdy osoba, która była niedostępna, jest już dostępna.</p> <p>Informacje o oddzwanianiu można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Ograniczenia w wyświetlaniu połączeń	<p>Określa, jakie informacje dotyczące połączeń lub podłączonych linii będą wyświetlane, zależnie od stron, które są uczestnikami połączenia.</p> <p>Informacje o planach trasowania i ograniczeniach w wyświetlaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Przekazywanie połączenia	<p>Umożliwia użytkownikowi przekierowanie połączenia przychodzącego na inny numer. Do opcji przekierowywania połączenia należą: Przekieruj wszystkie połączenia, Przekieruj połączenie przy braku odpowiedzi, Przekieruj połączenie przy braku dystrybucji.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager i w sekcji <a href="#">Dostosowywanie wyświetlania w portalu Self Care, na stronie 84</a>.</p>
Przekierowywanie wszystkich połączeń — przerwanie pętli	<p>Wykrywa i zapobiega wystąpieniu pętli w funkcji przekierowywania wszystkich połączeń. W razie wykrycia pętli w funkcji Przekierowywanie wszystkich połączeń ustawienia konfiguracyjne są ignorowane i telefon dzwoni bezpośrednio.</p>
Przekierowywanie wszystkich połączeń — zapobieganie wystąpieniu pętli	<p>Wykrywa i zapobiega wystąpieniu pętli w funkcji przekierowywania wszystkich połączeń. W razie wykrycia pętli w funkcji Przekierowywanie wszystkich połączeń ustawienia konfiguracyjne są ignorowane i telefon dzwoni bezpośrednio.</p>
Konfigurowalny wyświetlacz funkcji przekierowywania połączeń	<p>Zapobiega skonfigurowaniu przez użytkownika miejsca docelowego funkcji Przekierowywanie wszystkich połączeń bezpośrednio na telefonie, na którym powstaje pętla funkcji Przekierowywanie wszystkich połączeń lub na którym tworzony jest łańcuch przeskoków dłuższy niż dopuszczalny przez parametr Maksymalna liczba przeskoków przekierowania.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Nadpisanie miejsca docelowego funkcji przekierowywania połączeń	<p>Umożliwia nadpisanie funkcji przekierowywania wszystkich połączeń (CFA) w sytuacji, gdy miejsce docelowe tej funkcji przekazuje połączenie do numeru inicjującego. Ta funkcja umożliwia dotarcie ważnych połączeń do numeru inicjującego funkcję CFA. Nadpisanie działa niezależnie od tego, czy docelowy numer telefonu funkcji CFA jest numerem wewnętrznym czy zewnętrznym.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Powiadomienie o przekierowaniu połączenia	<p>Umożliwia skonfigurowanie informacji, które użytkownik zobaczy w chwili, gdy otrzyma przekierowane połączenie.</p> <p>Zobacz <a href="#">Konfigurowanie powiadamiania o przekierowywaniu połączeń, na stronie 183</a>.</p>

Funkcja	Opis i więcej informacji
Historia połączeń dla linii wspólnej	<p>Umożliwia użytkownikowi wyświetlenie działań na linii wspólnej za pośrednictwem funkcji telefonu Historia połączeń. Ta funkcja powoduje:</p> <ul style="list-style-type: none"> <li>• Rejestrowanie połączeń nieodebranych na wspólnej linii</li> <li>• Rejestrowanie wszystkich odebranych i nawiązanych połączeń na wspólnej linii</li> </ul>
Parkowanie połączenia	<p>Umożliwia użytkownikom parkowanie (tymczasowe zapisanie) połączenia i późniejsze pobranie go za pomocą innego telefonu w systemie Cisco Unified Communications Manager.</p> <p>Można skonfigurować pole <b>Jedna linia zarezerwowana dla połączenia zaparkowanego</b> w okienku <b>Konfiguracja układu specyficzna dla produktu</b>, aby zaparkować połączenie na oryginalnej linii lub na innej linii.</p> <p>Po włączeniu tego pola zaparkowane połączenie pozostaje na linii użytkownika, a w celu odebrania połączenia można wybrać klawisz <b>Wznów</b>. Użytkownik widzi numer wewnętrzny zaparkowanego połączenia na wyświetlaczu telefonu.</p> <p>Gdy to pole jest wyłączone, zaparkowane połączenie zostaje przekierowane do linii parkowania połączeń Linia użytkownika powróci do stanu bezczynności i w wyskakującym okienku pojawi się numer wewnętrzny parkowania połączenia. Użytkownik wybiera numer wewnętrzny w celu odebrania połączenia.</p> <p>Informacje o parkowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Przejmowanie połączeń	<p>Umożliwia użytkownikowi przekierowanie połączenia dzwoniącego na innym telefonie do swojego telefonu w ramach swojej grupy odbierania.</p> <p>Można skonfigurować na telefonie alert dźwiękowy i wizualny dla linii podstawowej. Ten alert informuje użytkowników o dzwoniącym połączeniu w ramach ich grupy odbierania.</p> <p>Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>

Funkcja	Opis i więcej informacji
Nagrywanie rozmów	<p>Umożliwia kierownikowi nagrywanie połączenia aktywnego. Użytkownik może usłyszeć w trakcie połączenia dźwiękowy sygnał alertu nagrywania, gdy połączenie jest nagrywane.</p> <p>Gdy połączenie jest chronione, stan zabezpieczeń połączenia jest wyświetlany na telefonach IP Cisco w postaci ikony blokowania. Połączone osoby mogą również usłyszeć alert dźwiękowy wskazujący, że połączenie jest chronione i nagrywane.</p> <p><b>Uwaga</b> W trakcie trwania monitorowania lub nagrywania połączenia aktywnego użytkownik może odebrać lub nawiązać połączenie interkodemem. Jeśli jednak użytkownik nawiąże połączenie interkodemem, połączenie aktywne zostanie zawieszona, co spowoduje przerwanie sesji nagrywania i zawieszenie sesji monitorowania. W celu przywrócenia sesji monitorowania osoba, której połączenie jest monitorowane, musi przywrócić połączenie.</p> <p>Informacje o monitorowaniu i nagrywaniu można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Połączenie oczekujące	<p>Wskazuje (i umożliwia odebranie przez użytkownika) połączenie przychodzące w trakcie innego połączenia. Informacje o połączeniu przychodzącym są widoczne na wyświetlaczu telefonu.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Dzwonek połączenia oczekującego	<p>Udostępnia użytkownikom funkcji Połączenie oczekujące opcję słyszalnego dzwonka w miejsce standardowego dźwięku.</p> <p>Dostępne opcje to Dzwonek i Jeden dzwonek.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
ID abonenta dzwoniącego	<p>Na wyświetlaczu telefonu widoczne są dane identyfikacyjne abonenta dzwoniącego, takie jak numer telefonu, nazwa lub inny tekst opisowy.</p> <p>Informacje o planie trasowania, ograniczeniach w wyświetlaniu połączeń i numerach telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Blokowanie identyfikatora abonenta dzwoniącego	<p>Umożliwia użytkownikowi zablokowanie wyświetlania swojego numeru telefonu i adresu e-mail na telefonach, w których włączone jest wyświetlanie identyfikatora rozmówcy.</p> <p>Informacje o planie trasowania i numerach telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Normalizacja strony wywołującej	<p>Normalizacja strony wywołującej przedstawia użytkownikowi połączenia telefoniczne za pomocą możliwego do wybrania numeru telefonu. Wszelkie kody Esc są dodawane do numeru, dzięki czemu użytkownik może w łatwy sposób ponownie połączyć się z abonentem dzwoniącym. Wybieralny numer jest zapisywany w historii połączeń i może zostać zapisany w Osobistej książce adresowej.</p>

Funkcja	Opis i więcej informacji
CAST dla SIP	Ustanawia komunikację pomiędzy aplikacją Cisco Unified Video Advantage (CUVA) i telefonami IP Cisco w celu obsługi obrazu wideo na komputerze, nawet w sytuacji, gdy telefon IP nie jest wyposażony w funkcje wideo.
cWtrąć	<p>Umożliwia użytkownikowi dołączenie do nieprywatnego połączenia na współdzielonej linii telefonicznej. Funkcja WtrąćKon dodaje użytkownika do połączenia i przekształca je w konferencję, udostępniając użytkownikowi i innym uczestnikom połączenia funkcje konferencji. Połączenie konferencyjne jest tworzone przy użyciu funkcji mostka konferencyjnego programu Cisco Unified Communications Manager.</p> <p>Należy włączyć zarówno klawisz programowy, jak i funkcję mostka konferencyjnego, w celu zapewnienia poprawnego działania funkcji Wtrąć konf.</p> <p>W wersji oprogramowania sprzętowego 10.2(2) i późniejszych funkcja WtrąćKon jest dostępna za pomocą klawisza programowego Wtrąć.</p> <p>Więcej informacji można znaleźć w rozdziale „Wtrąć” w <a href="#">Podręczniku konfiguracji funkcji programu Cisco Unified Communications Manager</a>.</p>
Ładuj urządzenie przenośne	<p>Umożliwia użytkownikowi ładowanie urządzenia przenośnego przez podłączenie go do portu USB w telefonie IP Cisco.</p> <p>Zobacz <i>Podręcznik użytkownika telefonów IP Cisco z serii 8800</i>.</p>
Przenośny numer wewnętrzny Cisco	<p>Umożliwia użytkownikom dostęp do elementów konfiguracji ich telefonu IP Cisco, takich jak wygląd linii, usługi i szybkie wybieranie ze wspólnego telefonu IP Cisco.</p> <p>Usługa Cisco Extension Mobility jest przydatna, gdy użytkownicy w ramach przedsiębiorstwa pracują w różnych lokalizacjach lub gdy wraz ze współpracownikami korzystają ze wspólnej przestrzeni roboczej.</p>
Klaster krzyżowy przenośnego numeru wewnętrznego firmy Cisco	<p>Umożliwia użytkownikowi skonfigurowanemu w jednym klastrze na zalogowanie się do telefonu IP Cisco w innym klastrze. Użytkownicy z klastra głównego logują się do telefonu IP Cisco w klastrze gościnnym.</p> <p><b>Uwaga</b> Przed skonfigurowaniem usługi EMCC skonfiguruj na telefonach IP Cisco usługę Configure Cisco Extension Mobility.</p>
Cisco IP Manager Assistant (IPMA)	<p>Udostępnia trasowanie połączeń i inne funkcje zarządzania połączeniami, które pozwalają menedżerom i asystentom na efektywniejszą obsługę połączeń telefonicznych.</p> <p>Zobacz <a href="#">Konfigurowanie programu Cisco IP Manager Assistant, na stronie 199</a>.</p>
<p>Moduł rozbudowy klawiatury do telefonów Cisco IP Phone z serii 8800</p> <p>Kluczowy moduł rozszerzeń do telefonów Cisco IP Phone 8851/8861</p> <p>Moduł rozbudowy klawiatury do telefonów Cisco IP Phone z serii 8865</p>	<p>Zapewnia dodatkowe klawisze przez dodanie modułu rozszerzeń do telefonu.</p> <p>Dodatkowe informacje można znaleźć w <i>przewodniku po akcesoriach do telefonów IP Cisco z serii 7800 i 8800 współpracujących z oprogramowaniem Cisco Unified Communications Manager</i>.</p>
Cisco IP Phone 8811 Wsparcie	Zapewnia pomoc techniczną dotyczącą Cisco IP Phone 8811.

Funkcja	Opis i więcej informacji
Pomoc techniczna dla użytkowników telefonu IP Cisco 8851NR	Zapewnia pomoc techniczną dotyczącą telefonu IP Cisco 8851NR
Cisco Unified Communications Manager Express (Unified CME) — negocjowanie wersji	<p>Program Cisco Unified Communication Manager Express używa w danych wysyłanych do telefonu specjalnego tagu, umożliwiającego własną identyfikację. Ten tag umożliwia udostępnianie przez telefon użytkownikowi usług, które obsługuje przełącznik.</p> <p>Patrz:</p> <ul style="list-style-type: none"> <li>• <i>Podręcznik administratora systemu programu Cisco Unified Communications Manager Express</i></li> <li>• <a href="#">Interakcja z programem Cisco Unified Communications Manager Express, na stronie 23</a></li> </ul>
Cisco Unified Video Advantage (CUVA)	<p>Umożliwia użytkownikom przeprowadzanie połączeń wideo przy użyciu telefonu IP Cisco, komputera osobistego i kamery wideo.</p> <p><b>Uwaga</b> Skonfiguruj parametr Możliwości wideo w sekcji Product Specific Configuration Layout (Układ konfiguracji specyficznej dla produktu) w module Konfiguracja telefonu.</p> <p>Zobacz dokumentację usługi Cisco Unified Video Advantage.</p>
Cisco WebDialer	Umożliwia użytkownikowi wykonywanie połączeń z poziomu aplikacji internetowych i stacjonarnych.
Klasyczny sygnał dzwonienia	<p>Obsługuje dzwonki osadzone w oprogramowaniu sprzętowym telefonu lub pobrane z programu Cisco Unified Communications Manager. Funkcja udostępnia sygnały dzwonienia w innych telefonach IP Cisco.</p> <p>Zobacz <a href="#">Niestandardowe dzwonki telefonu, na stronie 119</a>.</p>
Połączenie konferencyjne	<p>Umożliwia użytkownikowi jednoczesną rozmowę z wieloma stronami po indywidualnym wywołaniu każdego uczestnika. Do funkcji konferencyjnych należą: Konferencja i Meet-me.</p> <p>Umożliwia osobie niebędącej inicjatorem konferencji standardowej (niezaplanowanej) dodawanie lub usuwanie uczestników. Pozwala również dowolnemu uczestnikowi konferencji na połączenie na tej samej linii dwóch konferencji standardowych.</p> <p>Parametr usługi Advance Adhoc Conference, domyślnie wyłączony w module Cisco Unified Communications Manager — administracja, umożliwia włączanie tych funkcji przez użytkownika.</p> <p><b>Uwaga</b> Nie zapomnij poinformować użytkowników, czy te funkcje są włączone.</p>
Konfigurowalne rozszerzenie Energy Efficient Ethernet (EEE) dla portu komputera i przełącznika	<p>Udostępnia metodę sterowania funkcjami EEE dla portu komputera osobistego i portu przełącznika poprzez włączanie i wyłączanie technologii EEE. Funkcja steruje indywidualnie oboma rodzajami portów. Wartość domyślna to Włączone.</p> <p>Zobacz <a href="#">Konfigurowanie protokołu Energy Efficient Ethernet dla przełącznika i portu komputera, na stronie 184</a>.</p>

Funkcja	Opis i więcej informacji
Konfigurowalny rozmiar czcionki	<p>Umożliwia użytkownikom zwiększenie lub zmniejszenie maksymalnej liczby znaków wyświetlanej na telefonie IP na ekranie Historia połączeń i Połączenie poprzez zmianę rozmiaru czcionki.</p> <p>Mniejsza czcionka powoduje zwiększenie maksymalnej liczby wyświetlanych znaków, a większa czcionka — zmniejszenie tej liczby.</p>
Aplikacje CTI	<p>Punkt trasy CTI może wskazać urządzenie wirtualne do odbierania wielu jednoczesnych połączeń do przekierowania za pomocą aplikacji.</p>
Odrz. wszy.	<p>Umożliwia użytkownikowi przekazanie dzwoniącego, trwającego lub wstrzymanego połączenia bezpośrednio do systemu wiadomości głosowych. Po odrzuceniu połączenia linia staje się dostępna w celu nawiązywania lub odbierania nowych połączeń.</p> <p>Informacje o przekierowaniu natychmiastowym można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Nagrywanie wywoływane przez urządzenie	<p>Udostępnia użytkownikom końcowym możliwość nagrywania ich połączeń telefonicznych za pomocą klawisza programowego.</p> <p>Dodatkowo administratorzy mogą kontynuować nagrywanie połączeń telefonicznych za pośrednictwem interfejsu użytkownika CTI.</p> <p>Informacje o monitorowaniu i nagrywaniu można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Kierowane parkowanie połączenia	<p>Umożliwia użytkownikowi przekierowanie połączenia aktywnego na dostępny numer kierowanego parkowania połączenia, który użytkownik wybiera w zwykły lub szybki sposób. Przycisk parkowania połączenia z funkcją SZL wskazuje, czy numer kierowanego parkowania połączenia jest zajęty i udostępnia dostęp szybkiego wybierania do numeru kierowanego parkowania połączenia.</p> <p><b>Uwaga</b> W przypadku zaimplementowania funkcji Kierowane parkowanie połączenia należy unikać konfigurowania klawisza programowego funkcji Parkowanie. Zapobiega to pomyleniu przez użytkowników dwóch funkcji parkowania połączenia.</p> <p>Informacje o parkowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Wyświetl ikony stanu naładowania baterii i siły sygnału	<p>Wyświetla stan naładowania baterii i siłę sygnału telefonu komórkowego na telefonie IP, gdy telefon komórkowy jest połączony z telefonem IP za pomocą funkcji Bluetooth. Telefon IP Cisco 8851NR nie obsługuje komunikacji Bluetooth.</p>
Odróżnialny dzwonek	<p>Użytkownicy mogą dostosować sposób wskazywania na telefonie połączenia przychodzącego i nowej wiadomości poczty głosowej.</p> <p>Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>



Funkcja	Opis i więcej informacji
Nie przeszkadzać (DND)	<p>Gdy włączona jest funkcja DND, telefon w stanie dzwonienia nie emituje słyszalnego sygnału dzwonka ani w ogóle nie przekazuje żadnych powiadomień dźwiękowych i wizualnych.</p> <p>Gdy jest włączona, nagłówek telefonu zmienia kolor na czerwony, a na telefonie wyświetlany jest napis „Nie przeszkadzać”.</p> <p>Jeśli skonfigurowana jest funkcja wielopoziomowego pierwszeństwa i zastępowania (MLPP) i użytkownik odbiera połączenie z pierwszeństwem, telefon będzie emitował specjalny rodzaj dzwonka.</p> <p>Zobacz <a href="#">Konfigurowanie funkcji Nie przeszkadzać, na stronie 180</a>.</p>
Włącz/wyłącz JAL/TAL	<p>Umożliwia administratorowi sterowanie funkcjami Dołączanie między liniami (JAL, Join Across Lines) i Przekazywanie bezpośrednio między liniami (TAL, Transfer Across Lines).</p> <p>Zobacz Zasady dołączania i przekazu bezpośredniego, <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>.</p>
EnergyWise	<p>Umożliwia przechodzenie telefonu IP w stan uśpienia (ograniczenie energii) i powrót z niego (wzrost zużycia energii) po upływie wcześniej określonego czasu w celu wspierania oszczędności energii.</p> <p>Zobacz <a href="#">Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 176</a>.</p>
Tryb linii zaawansowanej	<p>Włącz tryb rozszerzony linii, aby korzystać z przycisków po obu stronach wyświetlacza telefonu jako klawiszy linii.</p> <p>Zobacz <a href="#">Konfigurowanie klawiszy linii dodatkowej, na stronie 211</a></p>
Rozszerzony bezpieczny klaster krzyżowy przenośnego numeru wewnętrznego (EMCC)	<p>Usprawnia funkcję Bezpieczny klaster krzyżowy przenośnego numeru wewnętrznego (EMCC) poprzez wprowadzenie ochrony konfiguracji sieci i zabezpieczeń na telefonie logowania. W ten sposób przestrzegane są reguły zabezpieczeń, zachowana zostaje szerokość pasma sieciowego i nie występują błędy sieci w ramach klastra gościnnego (VC).</p>
Usługa szybkiego wybierania	<p>Umożliwia użytkownikowi wprowadzenie kodu szybkiego wybierania w celu nawiązania połączenia. Kody szybkiego wybierania można przypisać do numerów telefonu lub wpisów w Osobistej książce adresowej. Zobacz “Usługi” w tej tabeli.</p> <p>Zobacz <a href="#">Modyfikowanie szablonu przycisków telefonu dla osobistej książki adresowej lub szybkiego wybierania, na stronie 209</a>.</p>
Przejmowanie połączeń grupy	<p>Umożliwia użytkownikowi odbieranie połączenia dzwoniącego na numer telefonu w innej grupie.</p> <p>Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Kontrola samosłyszalności zestawu nagłownego	<p>Umożliwia administratorowi ustawienie poziomu samosłyszalności w przewodowym zestawie nagłownym.</p>

Funkcja	Opis i więcej informacji
Cofnięcie zawieszenia	<p>Ogranicza czas, w jakim połączenie może być zawieszona przed jego przywróceniem na telefon, z którego zostało zawieszona i wysłaniem alertu do użytkownika.</p> <p>Połączenia przywracane można odróżnić od połączeń przychodzących dzięki pojedynczemu dzwoni (lub dźwiękowi, zależnie od ustawionego dla linii wskaźnika nowego połączenia). To powiadomienie jest powtarzane w stałych odstępach czasowych, jeśli połączenie nie zostanie podjęte.</p> <p>Połączenie, które wyzwala Powrót z zawieszenia jest wyświetlane w postaci animowanej ikony w dymku połączenia. Można skonfigurować priorytety połączeń, aby preferować połączenia przychodzące lub przywracane.</p>
Stan zawieszenia	<p>Umożliwia rozróżnianie pomiędzy liniami lokalnymi i zdalnymi, które spowodowały zawieszenie połączenia, na telefonach ze wspólną linią.</p>
Zawieś/Wznów	<p>Umożliwia użytkownikowi przeniesienie trwającego połączenia ze stanu aktywnego do wstrzymanego.</p> <ul style="list-style-type: none"> <li>• Jeśli nie chcesz korzystać z funkcji Music On Hold (Muzyka podczas oczekiwania), nie jest wymagana konfiguracja. Informacje na ten temat można znaleźć w sekcji “Muzyka podczas oczekiwania” w tej tabeli.</li> <li>• Zobacz “Cofnięcie zawieszenia” w tej tabeli.</li> </ul>
HTTP — pobieranie	<p>Usprawnia proces pobierania plików na telefon przez domyślne zastosowanie protokołu HTTP. Jeśli pobieranie za pośrednictwem protokołu HTTP skończy się niepowodzeniem, nastąpi powrót do pobierania na telefon za pośrednictwem protokołu TFTP.</p>
Grupa wyszukiwania	<p>Udostępnia funkcję wspólnego obciążenia dla połączeń na główny numer telefonu. Grupa poszukiwania zawiera szereg numerów telefonów, które mogą odbierać połączenia przychodzące. Gdy pierwszy numer telefonu z grupy poszukiwania jest zajęty, system poszukuje według wcześniej ustalonej kolejności następnego dostępnego numeru telefonu w grupie i przekierowuje do niego połączenie.</p> <p>W alarmie dotyczącym połączenia przychodzącego można wyświetlić <b>ID dzwoniącego</b> (jeśli ID dzwoniącego jest skonfigurowane), <b>numer telefonu</b> i <b>numer pilota grupy poszukiwania</b>. Numer grupy wyszukiwania wyświetlany jest za etykietą „<b>Hunt Group</b>”.</p> <p>Informacje o grupie poszukiwania i planach trasowania można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Zegar powiadomienia o połączeniu przychodzącym	<p>Umożliwia określenie czasu, przez który powiadomienie o przychodzącym połączeniu jest wyświetlane na ekranie telefonu.</p> <p>Zobacz Zegar powiadomienia o połączeniu przychodzącym, <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>.</p>

Funkcja	Opis i więcej informacji
Funkcja Intelligent Proximity	<p>Umożliwia użytkownikom parowanie urządzeń przenośnych z telefonem za pomocą funkcji Bluetooth oraz nawiązywanie i odbieranie połączeń przez telefon komórkowy.</p> <p>Zobacz <a href="#">Włączenie funkcji Intelligent Proximity, na stronie 215</a>.</p> <p>Telefony IP Cisco 8811, 8841 i 8851NR nie obsługują funkcji Bluetooth ani funkcji Intelligent Proximity.</p>
Interkom	<p>Umożliwia użytkownikom nawiązywanie i odbieranie połączeń interkodem przy użyciu klawiszy programowalnych telefonu. Przyciski linii interkodu można skonfigurować do:</p> <ul style="list-style-type: none"> <li>• Bezpośredniego wybierania określonego numeru wewnętrznego interkodu.</li> <li>• Zainicjowania połączenia interkodem i wyświetleniu monitu o wprowadzenie przez użytkownika poprawnego numeru interkodu.</li> </ul> <p><b>Uwaga</b> Jeśli użytkownik loguje się codziennie do tego samego telefonu za pomocą profilu usługi Cisco Extension Mobility, przypisz do jego profilu szablon przycisku telefonu, który zawiera informacje o interkocie i przypisz ten telefon do linii interkodu jako domyślne urządzenie interkodu.</p>
Obsługa protokołu tylko IPv6	<p>Udostępnia obsługę rozszerzonego adresowania IP w telefonach IP Cisco. Konfiguracja IPv4 i IPv6 jest zalecana i w pełni obsługiwana. Niektóre funkcje nie są obsługiwane w konfiguracji autonomicznej. Przypisywane są wyłączenie adresy IPv6.</p> <p>Zobacz <a href="#">Konfigurowanie ustawień sieciowych, na stronie 59</a>.</p>
Bufor jittera	<p>Funkcja Bufor jittera obsługuje jitter o wartości od 10 milisekund (ms) do 1000 ms dla strumieni audio.</p> <p>Działa w trybie adaptacyjnym i dynamicznie dopasowuje się do wielkości jittera.</p>
Dołącz	<p>Umożliwia użytkownikom tworzenie połączenia konferencyjnego przez zestawienie dwóch połączeń na jednej linii i pozostanie w tym połączeniu.</p>
Stan linii na listach połączeń	<p>Umożliwia użytkownikowi zaobserwowanie stanu dostępności stanu linii monitorowanych numerów linii na liście Historia połączeń. Istnieją następujące stany linii:</p> <ul style="list-style-type: none"> <li>• Offline</li> <li>• Dostępny</li> <li>• Zajęty</li> <li>• Nie przeszkadzać</li> </ul> <p>Zobacz <a href="#">Włączanie SZL dla list połączeń, na stronie 184</a>.</p>

Funkcja	Opis i więcej informacji
Stan linii w firmowej książce telefonicznej	<p>Umożliwia wyświetlanie stanu kontaktu w firmowej książce telefonicznej.</p> <ul style="list-style-type: none"> <li>• Offline</li> <li>• Dostępny</li> <li>• Zajęty</li> <li>• Nie przeszkadzać</li> </ul> <p>Zobacz <a href="#">Włączanie SZL dla list połączeń, na stronie 184</a>.</p>
Etykieta tekstowa linii	<p>Ustawia etykietę tekstową dla linii telefonicznej zamiast numeru telefonu.</p> <p>Zobacz <a href="#">Konfigurowanie oznaczenia linii, na stronie 193</a>.</p>
Wylogowanie z grup poszukiwania	<p>Umożliwia użytkownikom wylogowanie się z grupy poszukiwania i tymczasowe wstrzymanie sygnalizowania dzwonkiem połączeń na ich telefonach, gdy nie są oni dostępni do przyjmowania połączeń. Wylogowanie się z grup poszukiwania nie zapobiega sygnalizowaniu dzwonkiem na telefonie połączeń spoza grupy poszukiwania.</p> <p>Informacje o planie trasowania można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Identyfikacja połączeń złośliwych (MCID)	<p>Umożliwia użytkownikom zawiadamianie administratora systemu o otrzymywanych podejrzanych połączeniach.</p>
Konferencja Meet Me	<p>Umożliwia użytkownikowi hostowanie konferencji Meet Me, której inni uczestnicy łączą się z ustalonym wcześniej numerem w zaplanowanym czasie.</p>
Wiadomość oczekująca	<p>Definiuje numery telefonów dla wskaźników włączonych i wyłączonych wiadomości oczekujących. Bezpośrednio podłączony system wiadomości głosowych używa określonego numeru telefonu do ustawienia lub wyczyszczenia wskazania wiadomości oczekujących dla określonego telefonu IP Cisco.</p> <p>Informacje o wiadomościach oczekujących i poczcie głosowej można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Wskaźnik wiadomości oczekującej	<p>Lampka na słuchawce, która wskazuje, że użytkownik ma przynajmniej jedną nową wiadomość głosową.</p> <p>Informacje o wiadomościach oczekujących i poczcie głosowej można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Minimalna głośność dzwonka	<p>Ustawia minimalny poziom głośności dzwonka dla telefonu IP.</p>
Rejestrowanie połączeń nieodebranych	<p>Umożliwia użytkownikowi określenie, czy połączenia nieodebrane będą rejestrowane w katalogu połączeń nieodebranych dla danego wyglądu linii.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>

Funkcja	Opis i więcej informacji
Mobile Connect	<p>Umożliwia użytkownikom zarządzanie połączeniami służbowymi za pomocą pojedynczego numeru telefonu i przejmowanie trwających połączeń na telefonach stacjonarnych i urządzeniach zdalnych, takich jak telefon komórkowy. Użytkownicy mogą ograniczać grupę abonentów dzwoniących w odniesieniu do danego numeru telefonu i pory dnia.</p> <p>Informacje na temat usługi Cisco Unified Mobility można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway	<p>Umożliwia zdalnym pracownikom wygodne i bezpieczne połączenie z siecią firmową bez stosowania tunelu klienta prywatnej sieci wirtualnej (VPN).</p> <p>Zobacz <a href="#">Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, na stronie 186</a></p>
Usługa Mobile Voice Access	<p>Rozszerza możliwości usługi Mobile Connect, umożliwiając użytkownikom dostęp do systemu interaktywnych odpowiedzi głosowych (IVR) w celu zapoczątkowania połączenia z urządzenia zdalnego, takiego jak telefon komórkowy.</p> <p>Informacje na temat usługi Cisco Unified Mobility można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Monitorowanie i nagrywanie	<p>Umożliwia kierownikowi ciche monitorowanie połączenia aktywnego. Żaden z uczestników połączenia nie słyszy kierownika. Użytkownik może usłyszeć w trakcie połączenia dźwiękowy sygnał alertu monitorowania, gdy połączenie jest monitorowane.</p> <p>Gdy połączenie jest chronione, stan zabezpieczeń połączenia jest wyświetlany na telefonach IP Cisco w postaci ikony blokowania. Połączone osoby mogą również usłyszeć alert dźwiękowy wskazujący, że połączenie jest chronione i monitorowane.</p> <p><b>Uwaga</b> W trakcie trwania monitorowania lub nagrywania połączenia aktywnego użytkownik może odebrać lub nawiązać połączenie interkmem. Jeśli użytkownik nawiąże połączenie interkmem, połączenie aktywne zostanie zawieszona, co spowoduje przerwanie sesji nagrywania i zawieszenie sesji monitorowania. W celu przywrócenia sesji monitorowania osoba, której połączenie jest monitorowane, musi przywrócić połączenie.</p>
Wielopoziomowe pierwszeństwo i zastępowanie	<p>Umożliwia użytkownikowi wykonywanie i odbieranie pilnych i krytycznych połączeń w niektórych specjalizowanych środowiskach, takich jak instytucje wojskowe lub rządowe.</p> <p>Zobacz <a href="#">Wielopoziomowe pierwszeństwo i zastępowanie, na stronie 204</a>.</p>
Wiele połączeń na wygląd linii	<p>Każda linia może obsługiwać wiele połączeń. Domyślnie telefon obsługuje dwa połączenia aktywne na linii, ale maksymalna liczba wynosi sześć połączeń. Tylko jedno połączenie może trwać w tym samym czasie. Pozostałe są automatycznie zawieszane.</p> <p>System nie pozwoli na skonfigurowanie maksymalnej wartości wyzwalacza połączeń/zajętości większej niż 6/6. Dowolna konfiguracja wyższa niż 6/6 nie jest oficjalnie obsługiwana.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>

Funkcja	Opis i więcej informacji
Muzyka podczas oczekiwania	Odtwarza muzykę, gdy abonenci dzwoniący oczekują w zawieszeniu.
Wyciszenie	Wycisza mikrofon słuchawki lub zestawu nagłownego.
Brak nazwy alertu	Ułatwia użytkownikom końcowym identyfikowanie połączeń przekazanych dzięki wyświetlaniu numeru telefonu pierwotnego abonenta dzwoniącego. Połączenie jest widoczne jako Połączenie alertu z umieszczonym na końcu numerem telefonu abonenta dzwoniącego.
Wybieranie numerów przy odłożonej słuchawce	Umożliwia użytkownikowi wybranie numeru bez konieczności podniesienia słuchawki. Użytkownik może następnie podnieść słuchawkę lub nacisnąć przycisk Wybierz.
Przejęcie z innej grupy	Umożliwia użytkownikowi odebranie połączenia sygnalizowanego dzwonkiem na telefonie w innej grupie niż przypisana grupa użytkownika.  Informacje o przejmowaniu połączeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.
Komunikat na wyświetlaczu telefonu dla użytkowników usługi Extension Mobility	Funkcja udoskonala interfejs telefonu dla użytkowników usługi Extension Mobility przez udostępnianie przyjaznych komunikatów.
Powiadomienie dotyczące listy zaufanych w telefonie w programie Cisco Unified Communications Manager	Umożliwia wysłanie przez telefon alarmu do programu Cisco Unified Communications Manager podczas aktualizacji listy zaufanych (TL, Trust List).  Zobacz <a href="#">Obsługiwane funkcje zabezpieczeń, na stronie 88</a> .
PLK Support for Queue Statistics (Obsługa PLK dla statystyk kolejki)	Funkcja Obsługa PLK dla statystyk kolejki umożliwia użytkownikom analizowanie statystyk kolejki połączeń pod kątem pilotów poszukiwania, a informacje są wyświetlane na ekranie telefonu.
Wybieranie Plus	Umożliwia użytkownikowi wybieranie numerów planu E.164 z przedrostkiem w postaci znaku plus (+).  Aby wybrać znak +, użytkownik musi nacisnąć i przytrzymać klawisz gwiazdki (*) przez co najmniej 1 sekundę. Odnosi się to do wybierania pierwszej cyfry dla połączenia wykonywanego z odłożoną (w tym w trybie edycji) lub podniesioną słuchawką.
Negocjowanie zasilania przez protokół LLDP	Umożliwia negocjowanie zasilania przez telefon za pomocą protokołu LLDP (Link Level Endpoint Discovery Protocol) i CDP (Cisco Discovery Protocol).  Zobacz Negocjowanie zasilania, <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a> .
Przewidywanie wybieranego numeru	Upraszcza nawiązywanie połączenia. Lista Ostatnie zmienia wygląd i wyświetlane są teraz na niej tylko numery telefonów, w podobny sposób, jak wybierane numery.  Funkcja przewidywania wybieranego numeru jest włączona po włączeniu trybu rozszerzonego linii. Aby funkcja przewidywania wybieranego numeru działała, uproszczony interfejs nowego połączenia musi być wyłączony.

Funkcja	Opis i więcej informacji
Prywatność	<p>Uniemożliwia użytkownikom wspólnie używającym linii dodawanie siebie wzajemnie do połączenia i wyświetlanie na swoim telefonie informacji o połączeniach innego użytkownika.</p> <p>Informacje o wtrącaniu i prywatności można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Funkcja Private Line Automated Ringdown (PLAR)	<p>Administrator programu Cisco Unified Communications Manager może skonfigurować numer telefonu, który zostanie wybrany przez telefon IP Cisco natychmiast po podniesieniu słuchawki. Może to być przydatne dla telefonów przeznaczonych do łączenia się z numerami alarmowymi lub numerami "gorącej linii".</p> <p>Administrator może skonfigurować opóźnienie o maksymalnie 15 sek. Dzięki temu użytkownik ma czas na wykonanie połączenia, zanim telefon przełączy się na numer infolinii. Timer jest konfigurowalny poprzez parametr <b>Zdjęto z widełek do pierwszej cyfry (Off Hook To First Digit Timer)</b> w sekcji <b>Urządzenie &gt; Ustawienia urządzenia &gt; Profil SIP</b>.</p> <p>Więcej informacji można znaleźć w dokumencie <i>Podręcznik konfiguracji funkcji dla programu Cisco Unified Communications Manager</i>.</p>
Narzędzie do zgłaszania problemów (PRT)	<p>Wysyła dzienniki telefonu lub zgłasza problemy do administratora.</p> <p>Zobacz <a href="#">Narzędzie do zgłaszania problemów, na stronie 191</a>.</p>
Klawisze programowalne funkcji	<p>Funkcje takie jak Nowe połączenie, Oddzwanianie lub Przekazywanie wszystkich można przypisać do przycisków linii.</p> <p>Informacje o szablonie przycisków telefonu można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Narzędzie raportowania jakości (QRT)	<p>Umożliwia użytkownikom wysyłanie informacji o sprawiających problemy połączeniach telefonicznych poprzez naciśnięcie przycisku. Narzędzie QRT można skonfigurować w jednym z dwóch trybów, zależnie od wielkości interakcji użytkownika z narzędziem QRT.</p>
Ostatnie	<p>Umożliwia użytkownikom wyświetlenie 150 ostatnich pojedynczych połączeń i grup połączeń. Można wyświetlać ostatnio wybierane numery oraz nieodebrane połączenia i usuwać rekordy połączeń.</p>
Wybierz ponownie	<p>Umożliwia wykonanie połączenia z ostatnio wybieranym numerem poprzez naciśnięcie przycisku lub klawisza programowego Powtórz.</p>



Funkcja	Opis i więcej informacji
Zdalna konfiguracja portu	<p>Umożliwia użytkownikowi zdalne konfigurowanie prędkości i funkcji Dupleks działania portów sieci Ethernet telefonu za pomocą modułu Cisco Unified Communications Manager — administracja. Poprawia to wydajność w dużych wdrożeniach dla określonych ustawień portów.</p> <p><b>Uwaga</b> Jeśli porty są skonfigurowane w programie Cisco Unified Communications Manager do zdalnego konfigurowania portu, danych w telefonie nie można zmienić.</p> <p>Zobacz Zdalna konfiguracja portu, <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>.</p>
Ponowne przekierowanie połączeń bezpośrednich do zdalnego miejsca docelowego na numer firmowy	<p>Ponowne przekierowuje połączenia bezpośrednie na telefon komórkowy użytkownika na numer firmowy (telefon biurowy). W przypadku połączeń przychodzących do zdalnego miejsca docelowego (telefon komórkowy) połączenie jest sygnalizowane dzwonkiem tylko w zdalnym miejscu docelowym. Na telefonie stacjonarnym połączenie nie jest sygnalizowane dzwonkiem. Po odebraniu połączenia na telefonie komórkowym na telefonie stacjonarnym wyświetlany jest komunikat Zdalne połączenie w użyciu. W trakcie trwania tych połączeń użytkownik może korzystać z różnych funkcji na swoim telefonie komórkowym.</p> <p>Informacje na temat usługi Cisco Unified Mobility można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Usuń zegar monitu „Zakończono połączenie”	<p>Skraca czas reakcji funkcji Rozłącz, dezaktywując wyświetlanie komunikatu Zakończono połączenie na ekranie telefonu.</p>
Ustawienie sygnału dzwonienia	<p>Identyfikuje rodzaj dzwonka używanego do linii, gdy telefon ma inne połączenie aktywne.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager i w sekcji <a href="#">Niestandardowe dzwonki telefonu, na stronie 119</a>.</p>
Zawieszenie na porcie RTCP dla SIP	<p>Powoduje, że połączenia wstrzymane nie są usuwane przez bramę. Brama sprawdza stan portu RTCP w celu ustalenia, czy połączenie jest aktywne. Utrzymując port telefonu otwarty, brama nie będzie kończyć połączeń wstrzymanych.</p>
Zabezpieczona konferencja	<p>Umożliwia nawiązywanie połączeń konferencyjnych przez bezpieczne telefony za pomocą bezpiecznego mostka konferencyjnego. Podczas gdy nowi uczestnicy są dodawani za pomocą klawiszy programowych Konf, Dołącz i Wtrąć lub obsługi konferencji Meet-me, ikona połączenia bezpiecznego jest wyświetlana dopóty, dopóki wszyscy uczestnicy korzystają z bezpiecznych telefonów.</p> <p>Funkcja Lista konferencji powoduje wyświetlenie poziomu zabezpieczeń każdego uczestnika konferencji. Inicjatorzy mogą usuwać niechronionych uczestników z Listy konferencji. Pozostałe osoby mogą dodawać lub usuwać uczestników konferencji tylko w sytuacji, gdy ustawiony jest parametr Advanced Adhoc Conference Enabled (Dozwolona zaawansowana niezaplanowana konferencja).</p> <p>Informacje na temat mostka konferencyjnego i zabezpieczeń można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager i w sekcji <a href="#">Obsługiwane funkcje zabezpieczeń, na stronie 88</a>.</p>



Funkcja	Opis i więcej informacji
Secure EMCC (Bezpieczne EMCC)	Usprawnia funkcję EMCC przez wprowadzenie rozszerzonej ochrony użytkownika, który loguje się do swojego telefonu ze zdalnego biura.
Usługi	<p>Umożliwia korzystanie z menu Konfiguracja usług telefonu IP Cisco w narzędziu Cisco Unified Communications Manager — administracja w celu zdefiniowania i obsługi listy usług telefonicznych, które mogą być subskrybowane przez użytkowników.</p> <p>Informacje o usługach można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Przycisk Adres URL usług	<p>Umożliwia użytkownikom dostęp do usług za pomocą klawisza programowalnego zamiast korzystania z menu Usługi na telefonie.</p> <p>Informacje o usługach można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Pokaż identyfikator abonenta dzwoniącego i numer, z którego dzwoni	<p>W przypadku połączeń przychodzących na telefonach może być wyświetlany zarówno identyfikator abonenta dzwoniącego, jak i jego numer. Rozmiar wyświetlacza LCD telefonu IP ogranicza długość wyświetlanego identyfikatora abonenta dzwoniącego i jego numeru.</p> <p>Funkcja Pokaż identyfikator abonenta dzwoniącego i jego numer dotyczy tylko alertów o połączeniu przychodzącym i nie zmienia funkcji przekierowywania połączeń ani Grupy poszukiwania.</p> <p>Zobacz "Identyfikator abonenta dzwoniącego" w tej tabeli.</p>
Uproszczenie logowania do funkcji Extension Mobility za pomocą zestawów słuchawkowych Cisco	<p>Umożliwia użytkownikom logowanie się do funkcji Extension Mobility przy użyciu zestawów słuchawkowych firmy Cisco.</p> <p>Gdy telefon jest w trybie MRA, użytkownik może zalogować się do telefonu za pomocą zestawu słuchawkowego.</p> <p>Ta funkcja wymaga oprogramowania Cisco Unified Communications Manager (UCM) w wersji 11.5(1)SU8, 11.5(1)SU.9, 12.5(1)SU3 lub nowszej.</p> <p>Więcej informacji zawiera <i>Podręcznik konfiguracji systemu programu Cisco Unified Communications Manager</i> w wersji 11.5(1)SU8 bądź późniejszej lub w wersji 12.5(1)SU3 lub późniejszej.</p>
Uproszczona obsługa tabletu	<p>Umożliwia użytkownikowi tabletu z systemem Android lub iOS sparowanie go z telefonem za pomocą funkcji Bluetooth, co pozwoli na przeniesienie na telefon części dźwiękowej połączenia obsługiwane przez tablet.</p> <p>Zobacz <a href="#">Włączenie funkcji Intelligent Proximity, na stronie 215</a>.</p> <p>Telefon IP Cisco 8851NR nie obsługuje komunikacji Bluetooth.</p>
Szybkie wybieranie	Wybiera zapamiętany wcześniej numer.

Funkcja	Opis i więcej informacji
Dostęp przez SSH	<p>Umożliwia użytkownikowi włączanie i wyłączanie ustawienia Dostęp przez SSH w narzędziu Cisco Unified Communications Manager — administracja. Włączenie serwera SSH umożliwia akceptowanie przez telefon połączeń realizowanych za pośrednictwem protokołu SSH. Wyłączenie funkcji serwera SSH w telefonie blokuje dostęp do telefonu za pomocą protokołu SSH.</p> <p>Zobacz Dostęp przez SSH, <a href="#">Konfiguracja specyficzna dla produktu, na stronie 149</a>.</p>
Przekierowywanie zależne od pory dnia	<p>Ogranicza dostęp do określonych funkcji telefonicznych zależnie od okresu czasu.</p> <p>Informacje na temat okresu czasu i trasowania w zależności od pory dnia można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Aktualizacja strefy czasowej	<p>Wprowadza możliwość zmiany strefy czasowej na telefonie IP Cisco.</p> <p>Informacje o dacie i godzinie można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
Przenoszenie	<p>Umożliwia użytkownikowi przekierowanie trwających połączeń z jego telefonu na inny numer.</p>
Przekierowywanie — przekazywanie bezpośrednie	<p>Przekierowywanie: pierwsze wywołanie funkcji Przekierowywanie zawsze inicjuje nowe połączenie przy użyciu tego samego numeru telefonu po zawieszeniu połączenia aktywnego.</p> <p>Użytkownik może przekazywać połączenia bezpośrednio za pomocą funkcji przekazywania aktywnego połączenia.</p> <p>Niektóre aplikacje JTAPI/TAPI nie są zgodne z implementacją funkcji Dołączanie i Przekazywanie bezpośrednie na telefonie IP Cisco, dlatego może zaistnieć potrzeba skonfigurowania zasad funkcji Dołączanie i Przekazywanie bezpośrednie w celu wyłączenia możliwości dołączania i przekazywania bezpośredniego na tej samej linii i ewentualnie między liniami.</p> <p>Informacje na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p>
TVS	<p>Zaufane usługi weryfikacyjne (TVS) umożliwiają uwierzytelnianie podpisanych konfiguracji na telefonach oraz uwierzytelnianie innych serwerów lub obiektów bez konieczności zwiększania rozmiaru Listy zaufanych certyfikatów (CTL) lub wymogu pobrania na telefon zaktualizowanego pliku CTL. Protokół TVS jest domyślnie włączony.</p> <p>W menu Ustawienia zabezpieczeń na telefonie wyświetlane są informacje TVS.</p>
UCR 2013	<p>Telefony IP Cisco wspierają Ujednolicone wymagania funkcjonalne (UCR) 2013, udostępniając następujące funkcje:</p> <ul style="list-style-type: none"> <li>• Obsługa standardu FIPS 140-2</li> <li>• Obsługa 80-bitowych tagów SRTCP</li> </ul> <p>Jako administrator telefonu IP musisz skonfigurować określone parametry w module Cisco Unified Communications Manager — administracja.</p>

Funkcja	Opis i więcej informacji
Powiadomienie o nieskonfigurowanej linii podstawowej	Powiadamia użytkownika, gdy linia podstawowa nie jest skonfigurowana. Użytkownik otrzymuje wiadomość Bez konfiguracji na ekranie telefonu.
Aktualizacje interfejsu użytkownika dla listy, alertu i wizualnej poczty głosowej.	Zwiększa rozmiar okna aplikacji, aby zminimalizować liczbę obciążonych napisów.
Tryb wideo	<p>Umożliwia użytkownikowi wybranie trybu wideo do wyświetlania konferencji wideo w zależności od trybów skonfigurowanych w systemie.</p> <p>Informacje na temat obsługi wideo można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.</p> <p>Dostępne w telefonach IP Cisco 8845, 8865 i 8865NR.</p>
Obsługa wideo	<p>Powoduje włączenie obsługi wideo na telefonie. Parametr Funkcje wideo musi być włączony dla połączeń wideo w oknie konfiguracji telefonu w programie Cisco Unified Communications Manager. Domyślnie jest on włączony.</p> <p>Dostępne w telefonach IP Cisco 8845, 8865 i 8865NR.</p>
Wideo przez komputer	<p>Umożliwia użytkownikom wykonywanie połączeń wideo przy użyciu telefonu IP Cisco Unified, komputera osobistego i zewnętrznej kamery wideo.</p> <p>Funkcja ta umożliwia użytkownikom również wykonywanie połączeń wideo w produktach Cisco Jabber lub Cisco Unified Video Advantage.</p>
Wizualna poczta głosowa	<p>Zastępuje dźwiękowe instrukcje poczty głosowej graficznym interfejsem.</p> <p>Zobacz <i>Podręcznik instalacji i konfiguracji dla wizualnej poczty głosowej</i> znajdujący się pod adresem <a href="http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3">http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3</a>.</p>
System wiadomości głosowych	<p>Umożliwia abonentom dzwoniącym pozostawienie wiadomości w przypadku nieodebrania połączenia.</p> <p>Więcej informacji na temat poczty głosowej można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager i w sekcji <a href="#">Konfigurowanie wizualnej poczty głosowej, na stronie 201</a>.</p>
VPN	<p>Za pomocą protokołu SSL zapewnia połączenie prywatnej sieci wirtualnej (VPN) na telefonie IP Cisco Unified, gdy znajduje się on poza granicami zaufanej sieci lub gdy ruch sieciowy między telefonem a programem Unified Communications Manager musi przejść przez niezufane sieci.</p>
Domyślne wyłączenie dostępu do sieci WWW	<p>Zwiększa bezpieczeństwo poprzez wyłączenie dostępu do wszystkich usług sieciowych, takich jak HTTP. Użytkownicy mogą uzyskać dostęp do usług sieciowych tylko po włączeniu dostępu do sieci WWW.</p>

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Przyciski funkcyjne i klawisze programowe

W poniższej tabeli znajdują się informacje o funkcjach dostępnych na klawiszach programowych, funkcjach dostępnych na specjalnych przyciskach funkcyjnych oraz funkcjach, które trzeba skonfigurować jako klawisze programowalne funkcji. Pozycja "Obsługiwane" w tabeli oznacza, że funkcja jest obsługiwana przez odpowiedni typ przycisku lub klawisz programowy. Tylko klawisze programowalne funkcji wymagają skonfigurowania w ustawieniach telefonu IP Cisco.

Informacje o konfigurowaniu klawiszy programowalnych funkcji znajdują się w [Szablony przycisków telefonu, na stronie 207](#).

**Tabela 30: Funkcje i odpowiadające im przyciski i klawisze programowe**

Nazwa funkcji	Specjalny przycisk funkcyjny	Klawisz programowalny funkcji	Klawisz programowy
Połączenia alarmowe	nieobsługiwany	obsług.	nieobsługiwany
Wszystkie	nieobsługiwany	obsług.	nieobsługiwany
Odbierz	nieobsługiwany	obsług.	obsług.
cWtrąć	nieobsługiwany	nieobsługiwany	obsług.
Oddzwon	nieobsługiwany	obsług.	obsług.
Przekierowywanie wszystkich połączeń	nieobsługiwany	nieobsługiwany	obsług.
Parkowanie połączenia	nieobsługiwany	obsług.	obsług.
Stan linii Parkowanie połączenia	nieobsługiwany	obsług.	nieobsługiwany
Przejęcie połączenia (Przejmij)	nieobsługiwany	obsług.	obsług.
Stan linii Przejęcie połączenia	nieobsługiwany	obsług.	nieobsługiwany
Połączenie konferencyjne	obsług.	nieobsługiwany	obsług.
Przekieruj	nieobsługiwany	nieobsługiwany	obsług.
Nie przeszkadzać	nieobsługiwany	obsług.	obsług.
Przejmij grupę	nieobsługiwany	obsług.	obsług.
Zawieszanie	obsług.	nieobsługiwany	obsług.
Grupy wyszukiwania	nieobsługiwany	obsług.	nieobsługiwany

Nazwa funkcji	Specjalny przycisk funkcyjny	Klawisz programowalny funkcji	Klawisz programowy
Interkom	nieobsługiwany	obsług.	nieobsługiwany
Identyfikacja połączeń złośliwych (Malicious Call Identification, MCID)	nieobsługiwany	obsług.	obsług.
Meet Me	nieobsługiwany	obsług.	obsług.
Scal	nieobsługiwany	nieobsługiwany	obsług.
Mobile Connect (Mobilność)	nieobsługiwany	obsług.	obsług.
Wyciszenie	obsług.	nieobsługiwany	nieobsługiwany
Przejmowanie innych	nieobsługiwany	obsług.	obsług.
Obsługa PLK dla stanu kolejki	nieobsługiwany	nieobsługiwany	obsług.
Prywatność	nieobsługiwany	obsług.	nieobsługiwany
Stan kolejki	nieobsługiwany	obsług.	nieobsługiwany
Narzędzie raportowania jakości (QRT)	nieobsługiwany	obsług.	obsług.
Rejestrowanie	nieobsługiwany	nieobsługiwany	obsług.
Wybierz ponownie	nieobsługiwany	obsług.	obsług.
Szybkie wybieranie	nieobsługiwany	obsług.	nieobsługiwany
Stan linii Szybkie wybieranie	nieobsługiwany	obsług.	nieobsługiwany
Obsługa przycisku Zawieś w zestawie nagłównym USB	nieobsługiwany	nieobsługiwany	obsług.
Przenoszenie	obsług.	nieobsługiwany	obsług.

## Konfigurowanie funkcji telefonu

W telefonie można konfigurować rozmaite funkcje odpowiednio do potrzeb użytkowników. Funkcje można stosować do wszystkich telefonów, do grupy telefonów lub do poszczególnych telefonów.

Podczas konfigurowania funkcji w oknie aplikacji Cisco Unified Communications Manager — administracja — administracja wyświetlane są informacje mające zastosowanie do wszystkich telefonów oraz do konkretnego modelu telefonu. Informacje dotyczące określonego modelu telefonu pojawiają się w obszarze Układ konfiguracji specyficznej dla produktu.

Opis pól mających zastosowanie do wszystkich modeli telefonów można znaleźć w dokumentacji programu Cisco Unified Communications Manager.

Podczas konfigurowania pól okno, w którym wprowadza się ustawienia pola, ma znaczenie, ponieważ okna mają określoną hierarchię pierwszeństwa. Kolejność pierwszeństwa:

1. Poszczególne telefony (najwyższy stopień pierwszeństwa)
2. Grupa telefonów
3. Wszystkie telefony (najniższy stopień pierwszeństwa)

Jeśli np. wybranym użytkownikom ma zostać odebrany dostęp do stron WWW telefonu, ale reszta użytkowników ma mieć możliwość korzystania z tych stron, należy:

1. Włączyć dostęp do stron WWW telefonu dla wszystkich użytkowników.
2. Wyłączyć dostęp do stron WWW telefonu poszczególnym użytkownikom albo utworzyć grupę użytkowników i wyłączyć jej dostęp do stron WWW telefonu.
3. Jeśli pewien użytkownik z tej grupy potrzebuje jednak dostępu do stron WWW telefonu, można go włączyć dla tego konkretnego użytkownika.

## Konfigurowanie funkcji wszystkich telefonów

### Procedura

- 
- Krok 1** Zaloguj się do administracji Cisco Unified Communications Manager jako administrator.
  - Krok 2** Wybierz kolejno opcje **System > Konfiguracja telefonu przedsiębiorstwa**.
  - Krok 3** Ustaw pola, które mają zostać zmienione.
  - Krok 4** Zaznacz pole wyboru **Zastęp ustawienia firmowe** dla każdego ze zmodyfikowanych wcześniej pól.
  - Krok 5** Kliknij przycisk **Zapisz**.
  - Krok 6** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
  - Krok 7** Uruchom ponownie telefony.

**Uwaga** Będzie to miało wpływ na wszystkie telefony w organizacji.

---

## Konfigurowanie funkcji grupy telefonów

### Procedura

- 
- Krok 1** Zaloguj się do administracji Cisco Unified Communications Manager jako administrator.
  - Krok 2** Wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**.
  - Krok 3** Znajdź profil.
  - Krok 4** Przejdź do panelu Układ konfiguracji specyficznej dla produktu i wprowadź wartości w odpowiednich polach.
  - Krok 5** Zaznacz pole wyboru **Zastąp ustawienia firmowe** dla każdego ze zmodyfikowanych wcześniej pól.
  - Krok 6** Kliknij przycisk **Zapisz**.
  - Krok 7** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
  - Krok 8** Uruchom ponownie telefony.
- 

## Konfigurowanie funkcji pojedynczego telefonu

### Procedura

- 
- Krok 1** Zaloguj się do administracji Cisco Unified Communications Manager jako administrator.
  - Krok 2** Wybierz kolejno opcje **Urządzenie > Telefon**.
  - Krok 3** Znajdź telefon skojarzony z użytkownikiem.
  - Krok 4** Przejdź do panelu Układ konfiguracji specyficznej dla produktu i wprowadź wartości w odpowiednich polach.
  - Krok 5** Zaznacz pole wyboru **Override Common Settings** (Zastąp ustawienia wspólne) dla każdego ze zmodyfikowanych wcześniej pól.
  - Krok 6** Kliknij przycisk **Zapisz**.
  - Krok 7** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
  - Krok 8** Uruchom ponownie telefon.
- 

## Konfiguracja specyficzna dla produktu

W poniższej tabeli opisano pola widoczne w okienku Układ konfiguracji specyficznej dla produktu.

**Tabela 31:** Pola konfiguracji specyficznej dla produktu

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Wyłącz telefon głośnomówiący	Pole wyboru	Niezaznaczone	Wyłącza funkcję telefonu głośnomówiącego.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Wyłącz telefon głosnomówiący i zestaw słuchawkowy	Pole wyboru	Niezaznaczone	Wyłącza funkcje telefonu głosnomówiącego i zestawu nagłownego.
Wyłącz słuchawkę telefonu	Pole wyboru	Niezaznaczone	Wyłącza funkcje słuchawki.
Port komputera	włączone Wyłączone	włączone	Kontroluje możliwość użycia portu komputera w celu podłączenia komputera do sieci LAN.
Dostęp do ustawień	Wyłączone włączone Ograniczony	włączone	Włącza, wyłącza i ogranicza dostęp do lokalnych ustawień konfiguracji telefonu w aplikacji Ustawienia. <ul style="list-style-type: none"> <li>Wyłączone — w menu Ustawienia nie są wyświetlane żadne opcje.</li> <li>Włączone — wszystkie pozycje w menu Ustawienia są dostępne.</li> <li>Ograniczone — dostępne jest tylko menu ustawień telefonu.</li> </ul>
Dostęp do sieci VLAN głosowy przez port komputera	włączone Wyłączone	włączone	Wskazuje, czy telefon zezwoli urządzeniu podłączonemu do portu komputera na dostęp do głosowej sieci VLAN. <ul style="list-style-type: none"> <li>Wyłączone — komputer nie może wysyłać ani otrzymywać danych z głosowej sieci VLAN ani z telefonu.</li> <li>Włączone — komputer może wysyłać i otrzymywać dane z głosowej sieci VLAN lub z telefonu. Ustaw w tym polu wartość Włączone, jeśli na komputerze jest uruchomiona aplikacja monitorująca ruch telefoniczny. Mogą to być aplikacje monitorujące i zapisujące rozmowy oraz oprogramowanie do monitorowania sieci służące do analiz.</li> </ul>
Funkcje wideo	włączone Wyłączone	8845, 8865 i 8865NR: włączone 8811, 8851, 8851NR, 8861: wyłączzone	Umożliwia użytkownikom przeprowadzanie połączeń wideo przy użyciu telefonu IP Cisco, komputera osobistego i kamery wideo.
Dostęp przez WWW	Wyłączone włączone	Wyłączone	Włącza lub wyłącza dostęp do stron WWW telefonu za pomocą przeglądarki. <p><b>Przeostroga</b> Jeśli to pole jest włączone, poufne informacje o telefonie mogą zostać ujawnione.</p>



Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Wyłącz protokół TLS 1.0 i TLS 1.1 przy dostępie przez WWW	Wyłączone włączone	Wyłączone	<p>Steruje korzystaniem z protokołu TLS 1.2 przy połączeniu z serwerem WWW.</p> <ul style="list-style-type: none"> <li>• <b>Wyłączone</b> — telefon skonfigurowany dla protokołów TLS1.0, TLS 1.1 lub TLS1.2 może pełnić funkcję serwera HTTPS.</li> <li>• <b>Włączone</b> — tylko telefon skonfigurowany dla protokołów TLS1.0, TLS 1.1 lub TLS1.2 może pełnić funkcję serwera HTTPS.</li> </ul>
Wybieranie blokowe	Wyłączone włączone	Wyłączone	<p>Kontroluje metodę wybierania.</p> <ul style="list-style-type: none"> <li>• <b>Wyłączone</b> — System Cisco Unified Communications Manager czeka na wygaśnięcie czasomierza między cyframi w przypadku nakładania się planu wybierania lub wzorca tras.</li> <li>• <b>Włączone</b> — Cały wybrany ciąg jest wysyłany do systemu Cisco Unified Communications Manager po zakończeniu wybierania. Aby uniknąć przekroczenia limitu czasu czasomierza T.302, należy włączyć wybieranie blokowe, gdy plany numerów lub wzorce tras nakładają się.</li> </ul> <p>Kody wymuszonego uwierzytelniania (FAC) ani kody sprawy klienta (CMC) nie obsługują wybierania blokowego. Jeśli kody FAC lub CMC są używane do uzyskiwania dostępu do połączeń oraz rozliczeń, nie można używać tej funkcji.</p>
Dni nieaktyw. ekranu	Dni tygodnia		<p>Określa dni, w których wyświetlacz nie włącza się automatycznie o godzinie określonej w polu Godz. rozpocz. wyświetl.</p> <p>Wybierz dzień lub dni z listy rozwijanej. Aby wybrać więcej niż jeden dzień, naciśnij klawisz <b>Ctrl</b> i <b>kliknij</b> każdy wybrany dzień.</p>
Godz. rozpocz. wyświetl.	gg:mm		<p>Definiuje godzinę, o której każdego dnia wyświetlacz jest automatycznie włączany (z wyjątkiem dni określonych w polu Dni nieaktyw. ekranu).</p> <p>W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 0:00 oznacza północ.</p> <p>Aby na przykład wyświetlacz automatycznie włączał się o godzinie 7:00 rano. (0700), wprowadź 07:00. Aby włączyć wyświetlacz o godzinie 2:00 po południu (1400), wprowadź 14:00.</p> <p>Jeśli to pole jest puste, wyświetlacz jest automatycznie włączany o godzinie 00:00.</p>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Czas wyświetlania	gg:mm		<p>Określa czas, przez który wyświetlacz pozostaje włączony po godzinie określonej w polu Godz. rozpocz. wyświetl.</p> <p>Aby na przykład wyświetlacz pozostawał włączony przez 4 godziny i 30 minut po automatycznym włączeniu, wprowadź 04:30.</p> <p>Jeśli to pole jest puste, telefon wyłączy się na koniec dnia (00:00).</p> <p>Jeśli w polu Godz. rozpocz. wyświetl. wpisana jest wartość 0:00 i czas włączonego wyświetlacza jest pusty (lub ma wartość 24:00), wyświetlacz nie wyłączy się.</p>
Czas nieakt. ekranu	gg:mm	01:00	<p>Określa czas bezczynności telefonu, po upływie którego zostanie wyłączony wyświetlacz. Działa tylko wtedy, gdy wyświetlacz został wyłączony zgodnie z planem, a następnie został włączony przez użytkownika (przez naciśnięcie przycisku w telefonie lub podniesienie słuchawki).</p> <p>Wprowadź wartość w tym polu w formacie godziny:minuty.</p> <p>Aby na przykład wyświetlacz, po włączeniu go przez użytkownika, wyłączał się po okresie bezczynności równym 1 godzinę i 30 minut, wprowadź 01:30.</p> <p>Aby uzyskać więcej informacji, patrz <a href="#">Konfigurowanie ekranu bezczynności, na stronie 122</a>.</p>
Wł. ekran podczas rozm. przych.	Wyłączone włączone	włączone	Włącza wyświetlacz w momencie nadejścia połączenia przychodzącego.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Włącz Power Save Plus	Dni tygodnia		<p>Określa dni, w których telefon jest wyłączany.</p> <p>Wybierz dzień lub dni z listy rozwijanej. Aby wybrać więcej niż jeden dzień, naciśnij klawisz <b>Ctrl</b> i <b>kliknij</b> każdy wybrany dzień.</p> <p>Po włączeniu opcji Power Save Plus zostanie wyświetlony komunikat ostrzegający o potencjalnych zagrożeniach (e911).</p> <p><b>Przeostroga</b> W trybie Power Save Plus punkty końcowe skonfigurowane dla tego trybu są wyłączane i nie można dokonywać z nich połączeń alarmowych ani odbierać na nich połączeń przychodzących. Wybierając ten tryb, należy uwzględnić następujące kwestie: (i) bierzesz na siebie pełną odpowiedzialność za dostarczenie alternatywnej metody nawiązywania połączeń alarmowych i odbierania połączeń przy uruchomionym trybie; (ii) firma Cisco nie ponosi odpowiedzialności za włączenie tego trybu, a cała odpowiedzialność związana z jego włączeniem trybu spoczywa na Tobie; oraz (iii) poinformujesz wyczerpująco wszystkich użytkowników o wpływie wprowadzenia tego trybu na połączenia, ich nawiązywanie itp.</p> <p>Aby wyłączyć tryb Power Save Plus, należy usunąć zaznaczenie pola wyboru Zezwól na zastąpienie przez EnergyWise. Jeśli pole Zezwól na zastąpienie przez EnergyWise pozostaje zaznaczone, ale w polu Włącz Power Save Plus nie wpisano liczby dni, funkcja Power Save Plus nie jest wyłączona.</p>
Godzina włączenia telefonu	gg:mm		<p>Określa, że telefon włącza się automatycznie w dni wybrane w polu Włącz Power Save Plus.</p> <p>W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ.</p> <p>Aby automatycznie włączyć telefon np. o godzinie 7 rano, (0700), wprowadź 07:00. Aby włączyć telefon o drugiej po południu, (1400), wprowadź 14:00.</p> <p>Wartość domyślna jest pusta, co oznacza 00:00.</p> <p>Godzina włączenia telefonu musi być ustawiona na co najmniej 20 minut później niż Godzina wyłączenia telefonu. Na przykład, jeśli Godzina wyłączenia telefonu jest ustawiona na 07:00, Godzina włączenia telefonu nie może być wcześniejsza niż 07:20.</p>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Godzina wyłączenia telefonu	gg:mm		<p>Określa godzinę, o której telefon będzie wyłączany w tych dniach, które są wybrane w polu Włącz Power Save Plus. Jeśli pola Godzina włączenia telefonu i Godzina wyłączenia telefonu mają taką samą wartość, telefon nie zostanie wyłączony.</p> <p>W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ.</p> <p>Aby automatycznie wyłączyć telefon np. o godzinie 7 rano, (0700), wprowadź 7:00. Aby wyłączyć telefon o drugiej po południu, (1400), wprowadź 14:00.</p> <p>Wartość domyślna jest pusta, co oznacza 00:00.</p> <p>Godzina włączenia telefonu musi być ustawiona na co najmniej 20 minut później niż Godzina wyłączenia telefonu. Na przykład, jeśli Godzina wyłączenia telefonu jest ustawiona na 7:00, Godzina włączenia telefonu nie może być wcześniejsza niż 7:20.</p>
Wyłącz telefon po czasie nieaktywności	Od 20 do 1440 minut	60	<p>Wskazuje czas nieaktywności telefonu, po upływie którego zostanie on wyłączony.</p> <p>Limit czasu jest uwzględniany w następujących okolicznościach:</p> <ul style="list-style-type: none"> <li>• Gdy telefon był w trybie Power Save Plus zgodnie z harmonogramem i wyszedł z tego trybu po naciśnięciu przez użytkownika klawisza Wybierz.</li> <li>• Gdy ponownie włączono zasilanie telefonu za pomocą przełącznika.</li> <li>• Jeśli osiągnięto godzinę określoną przez parametr Godzina wyłączenia telefonu, ale telefon jest nadal używany.</li> </ul>
Włącz alert dźwiękowy	Pole wyboru	Nieznaczane	<p>Po włączeniu tej opcji telefon odtwarza alert dźwiękowy na 10 minut przed godziną podaną w polu Godzina wyłączenia telefonu.</p> <p>To pole wyboru jest uwzględniane tylko wtedy, gdy w polu listy Włącz Power Save Plus zaznaczono co najmniej jeden dzień.</p>
Domena EnergyWise	Do 127 znaków		Wskazuje domenę EnergyWise, w której znajduje się telefon.
Hasło EnergyWise	Do 127 znaków		Określa tajne hasło zabezpieczeń używane podczas komunikacji z punktami końcowymi w domenie EnergyWise.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Zezwól na zastąpienie przez EnergyWise	Pole wyboru	Nieznaczony	<p>Określa, czy zasady kontrolera domeny EnergyWise mogą zezwalać na wysyłanie do telefonu informacji o zmianie poziomu zasilania. Muszą zostać spełnione następujące warunki:</p> <ul style="list-style-type: none"> <li>• W polu Włącz Power Save Plus musi być wybrany co najmniej jeden dzień.</li> <li>• Ustawienia w narzędziu Cisco Unified Communications Manager — administracja są wdrażane nawet wtedy, gdy funkcja EnergyWise przysyła komunikat o zastąpieniu.</li> </ul> <p>Na przykład jeśli Godzina wyłączenia telefonu jest ustawiona na godzinę 22:00, wartość w polu Godzina włączenia telefonu wynosi 06:00 (szósta rano), a w polu Włącz Power Save Plus wybrano co najmniej jeden dzień.</p> <ul style="list-style-type: none"> <li>• Jeśli funkcja EnergyWise powiadomi telefon o wyłączeniu przypadającym na godzinę 20:00, ta dyrektywa pozostanie w mocy (przyjmując brak interwencji użytkownika telefonu) aż do godziny skonfigurowanej w polu Godzina włączenia telefonu, czyli do 6:00.</li> <li>• O godzinie 6:00 rano telefon włączy się i ponownie rozpocznie otrzymywanie informacji o zmianach poziomu mocy w zależności od ustawień w narzędziu Cisco Unified Communications Manager — administracja.</li> <li>• Aby ponownie zmienić poziom zasilania w telefonie, funkcja EnergyWise musi wysłać nowe polecenie o zmianie poziomu zasilania.</li> </ul> <p>Aby wyłączyć tryb Power Save Plus, należy usunąć zaznaczenie pola wyboru Zezwól na zastąpienie przez EnergyWise. Jeśli pole Zezwól na zastąpienie przez EnergyWise pozostaje zaznaczone, ale w polu Włącz Power Save Plus nie wpisano liczby dni, funkcja Power Save Plus nie jest wyłączona.</p>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Zasady dołączania i przekazu bezpośredniego	Ta sama linia, włącz między liniami Tylko ta sama linia Ta sama linia, wyłącz między liniami	Ta sama linia, włącz między liniami	Zarządza możliwością dołączania do połączeń i ich przekazywania przez użytkownika. <ul style="list-style-type: none"> <li>Ta sama linia, włącz między liniami — użytkownicy mogą bezpośrednio dołączać do połączenia lub przekazywać je z bieżącej linii do innego połączenia na innej linii.</li> <li>Tylko ta sama linia — użytkownicy mogą bezpośrednio przekazywać lub dołączać tylko wtedy, gdy oba połączenia znajdują się na tej samej linii.</li> <li>Ta sama linia, wyłącz między liniami — użytkownicy nie mogą dołączać do połączeń ani ich przekazywać na tej samej linii. Funkcje dołączania i przekazywania są wyłączone i użytkownik nie może korzystać z przekazywania bezpośredniego ani dołączania.</li> </ul>
Przekazuj do portu PC	Wyłączone włączone	Wyłączone	Wskazuje, czy telefon przekazuje do portu dostępowego pakiety wysyłane i odbierane poprzez port sieciowy.
Nagrywanie dźwięku	Wyłączone włączone	Wyłączone	Steruje odtwarzaniem sygnału, gdy użytkownik rozpoczyna rejestrowanie połączenia.
Głośność lokalnego nagrywania dźwięku	Liczba całkowita od 0 do 100	100	Określa głośność sygnału nagrywania dla użytkownika lokalnego.
Głośność zdalnego nagrywania dźwięku	Liczba całkowita od 0 do 100	50	Określa głośność sygnału nagrywania dla użytkownika zdalnego.
Czas trwania nagrania dźwięku	Liczba całkowita od 1 do 3000 milisekund		Określa czas trwania sygnału nagrywania.
Serwer dziennika	Ciąg o długości do 256 znaków		Określa serwer dziennika systemowego IPv4 na potrzeby danych stworzonych podczas debugowania telefonu. Format adresu jest następujący: <b>adres : &lt;port&gt;@&lt;base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b>
Cisco Discovery Protocol (CDP): port przełącznika	Wyłączone włączone	włączone	Kontroluje protokół Cisco Discovery Protocol na porcie oprogramowania w telefonie.
Cisco Discovery Protocol (CDP): port komputera	Wyłączone włączone	włączone	Kontroluje protokół Cisco Discovery Protocol na porcie komputera w telefonie.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Link Layer Discovery Protocol — Media Endpoint Discover (LLDP-MED): port przełącznika	Wyłączone włączone	włączone	Włącza protokół LLDP-MED na porcie oprogramowania.
Link Layer Discovery Protocol (LLDP): port komputera	Wyłączone włączone	włączone	Włącza protokół LLDP na porcie komputera.
LLDP Asset ID	Ciąg o długości do 32 znaków		Wskazuje identyfikator zasobu przypisanego do telefonu w celu zarządzania zapasami.
LLDP priorytet mocy	Nieznane Niski Wysoki Kluczowy	Nieznane	Przypisuje do przełącznika priorytet zasilania, umożliwiając przełącznikowi właściwe zasilanie telefonów.
Uwierzyt. 802.1x	Sterowane przez użytkownika włączone Wyłączone	Sterowane przez użytkownika	Określa stan funkcji uwierzytelniania 802.1x. <ul style="list-style-type: none"> <li>• Sterowane przez użytkownika — użytkownik może konfigurować protokół 802.1x na telefonie.</li> <li>• Wyłączone — uwierzytelnianie 802.1x nie jest używane.</li> <li>• Włączone — uwierzytelnianie 802.1x jest używane i można skonfigurować uwierzytelnianie dla telefonów.</li> </ul>
Automatyczna synchronizacja portów	Wyłączone włączone	Wyłączone	Synchronizuje porty, używając najniższej prędkości między portami telefonu w celu wyeliminowania utraconych pakietów.
Zdalna konfiguracja przełączania portu	Wyłączone włączone	Wyłączone	Umożliwia zdalne skonfigurowanie prędkości i funkcji duplexu na porcie oprogramowania w telefonie. Poprawia to wydajność w dużych wdrożeniach dla określonych ustawień portów.  Jeśli porty oprogramowania są skonfigurowane w programie Cisco Unified Communications Manager do zdalnego konfigurowania portu, nie można zmienić danych w telefonie.
Zdalna konfiguracja portu komputera PC	Wyłączone włączone	Wyłączone	Umożliwia zdalne skonfigurowanie prędkości i funkcji duplexu na porcie komputera w telefonie. Poprawia to wydajność w dużych wdrożeniach dla określonych ustawień portów.  Jeśli porty są skonfigurowane w programie Cisco Unified Communications Manager do zdalnego konfigurowania portu, danych w telefonie nie można zmienić.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Dostęp przez SSH	Wyłączone włączone	Wyłączone	Kontroluje dostęp do usługi SSH przez port 22. Pozostawienie otwartego portu 22 powoduje, że telefon jest podatny na ataki typu DoS (Denial of Service).
Zegar powiadomienia o połączeniu przychodzącym	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Podaj czas (w sekundach) wyświetlania powiadomienia. Do tego czasu są wliczane czasy zanikania i rozjaśniania okna. Wartość 0 oznacza, że powiadomienie o połączeniu przychodzącym jest wyłączone.
Ustawienia regionalne dzwonka	Domyślny Japonia	Domyślny	Kontroluje wzorzec dzwonka.
Zegar podjęcia TLS	Liczba całkowita od 0 do 3600 sekund	3600	Steruje wznowieniem sesji TLS bez powtarzania całego procesu uwierzytelniania TLS. Jeśli wartość tego pola wynosi 0, wznowienie sesji TLS jest wyłączone.
Tryb FIPS	Wyłączone włączone	Wyłączone	Włącza lub wyłącza w telefonie tryb FIPS (Federal Information Processing Standard).
Zapisuj dziennik połączeń na linii wspólnej	Wyłączone włączone	Wyłączone	Określa, czy w dzienniku połączeń mają być zapisywane połączenia na linii wspólnej.
Minimalna głośność dzwonka	0 — wyciszony 1–15	0 — wyciszony	Kontroluje minimalną głośność dzwonka telefonu. Można tak ustawić telefon, aby wyłączenie dzwonka było niemożliwe.



Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Oprogramowanie sprzętowe dystrybuowane przez P2P	Wyłączone włączone	włączone	<p>Umożliwia telefonowi znalezienie w podsieci innych telefonów tego samego modelu i udostępnianie plików ze zaktualizowanym oprogramowaniem firmware. Jeśli telefon ma załadowane nowe oprogramowanie firmware, może udostępnić je innym telefonom. Jeśli jeden z pozostałych telefonów ma załadowane nowe oprogramowanie firmware, telefon może pobrać je z tego telefonu, zamiast korzystać z serwera TFTP.</p> <p>Oprogramowanie sprzętowe dystrybuowane przez P2P:</p> <ul style="list-style-type: none"> <li>• Ogranicza przeciążenie przy transferach TFTP ze scentralizowanych serwerów TFTP.</li> <li>• Likwiduje konieczność ręcznego sterowania uaktualnieniami oprogramowania sprzętowego.</li> <li>• Skraca niedostępność telefonów spowodowaną jednoczesnym zresetowaniem wielu telefonów.</li> <li>• Pomaga podczas aktualizacji oprogramowania firmware w oddziałach lub biurach zdalnych połączonych poprzez linie WAN o ograniczonej przepustowości.</li> </ul>
Serwer pobierania	Ciąg o długości do 256 znaków		<p>Wskazuje alternatywny serwer IPv4 używany przez telefony do pobierania oprogramowania firmware i uaktualnień.</p> <p>Format adresu jest następujący:  <b>adres : &lt;port&gt;@&lt;base&gt;=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b></p>
Serwer pobierania IPv6	Ciąg o długości do 256 znaków		<p>Wskazuje alternatywny serwer IPv6 używany przez telefon do pobierania oprogramowania firmware i uaktualnień.</p> <p>Format adresu jest następujący:  <b>[adres] : &lt;port&gt;@&lt;base&gt;=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b></p>
Interfejs słuchawki szerokopasm.	Wyłączone włączone	włączone	<p>Umożliwia użytkownikowi korzystanie z kodeka szerokopasmowego dla słuchawek analogowych.</p>
Zestaw szerokopasmowy	Wyłączone włączone	włączone	<p>Włącza lub wyłącza w telefonie możliwość korzystania ze słuchawki szerokopasmowej. Ta opcja jest używana w połączeniu z funkcją User Control Wideband Headset (Słuchawka szerokopasmowa sterowana przez użytkownika).</p> <p>Aby uzyskać więcej informacji, patrz <a href="#">Konfigurowanie kodeka komunikacji szerokopasmowej, na stronie 121</a>.</p>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Wi-Fi	Wyłączone włączone	włączone	Umożliwia połączenie telefonów IP Cisco 8861 i 8865 z siecią Wi-Fi.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Tyłny port USB	Wyłączone włączone	8861, 8865 i 8865NR: włączone	Służy do włączania i wyłączenia możliwości korzystania z portu USB z tyłu obudowy w telefonach IP Cisco 8861 i 8865.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Boczny port USB	Wyłączone włączone	włączone	Służy do włączania i wyłączenia możliwości korzystania z portu USB z boku obudowy w telefonach IP Cisco 8851, 8851NR, 8861, 8865 i 8865NR.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Dostęp do konsoli	Wyłączone włączone	Wyłączone	Określa, czy konsola szeregową jest włączona lub wyłączona.
Bluetooth	Wyłączone włączone	włączone	Włącza lub wyłącza opcję Bluetooth w telefonie. Jeśli ta opcja jest wyłączona, użytkownik nie może włączyć funkcji Bluetooth w telefonie. Obsługiwane w telefonach IP Cisco 8845, 8851, 8861 i 8865.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Zezwól na import kontaktów Bluetooth	Wyłączone włączone	włączone	Umożliwia użytkownikowi zaimportowanie kontaktów z podłączonego urządzenia przenośnego przy użyciu protokołu Bluetooth. Gdy ta opcja jest wyłączona, użytkownik nie może importować kontaktów z podłączonego urządzenia przenośnego do swojego telefonu. Obsługiwane w telefonach IP Cisco 8845, 8851, 8861 i 8865.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Zezwól na tryb głośnomówiący przenośnych urządzeń Bluetooth	Wyłączone włączone	włączone	<p>Umożliwia użytkownikom wykorzystanie lepszych parametrów dźwiękowych swojego telefonu podczas używania urządzenia przenośnego lub tabletu. Użytkownik paruje urządzenie przenośne lub tablet z telefonem za pomocą protokołu Bluetooth. Gdy ta opcja jest wyłączona, użytkownik nie może sparować urządzenia przenośnego lub tabletu ze swoim telefonem.</p> <p>Po sparowaniu urządzenia przenośnego użytkownik może nawiązywać i odbierać połączenia komórkowe przy użyciu telefonu. Korzystając z tabletu, użytkownik może przekierowywać dźwięk z tabletu na telefon.</p> <p>Użytkownicy mogą sparować z telefonem wiele urządzeń przenośnych, tabletów, a także zestaw słuchawkowy Bluetooth. Jednak jednocześnie może być podłączone tylko jedno urządzenie i jeden zestaw słuchawkowy.</p> <p>Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.</p>
Profile Bluetooth	Zestaw głośnomówiący Urządzenie interfejsu HID	Zestaw głośnomówiący	<p>Wskazuje, które profile Bluetooth w telefonie są włączone lub wyłączone.</p> <p>Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.</p>
Gratuitous ARP	Wyłączone włączone	Wyłączone	Włącza lub wyłącza w telefonie uczenie się adresów MAC na podstawie pakietu Gratuitous ARP. Ta funkcja jest wymagana do monitorowania lub zapisywania strumieni głosu.
Show All Calls on Primary Line (Wyświetlaj wszystkie połączenia na linii podstawowej)	Wyłączone włączone	Wyłączone	<p>Określa, czy wszystkie połączenia trafiające do tego telefonu będą wyświetlane na linii podstawowej, czy też nie.</p> <p>Celem tego pola jest ułatwienie użytkownikowi czytelnego wyświetlania wszystkich połączeń na wszystkich liniach, tak aby nie musiał on wybierać linii w celu wyświetlenia połączeń na tej linii. Innymi słowy, gdy na telefonie jest skonfigurowanych wiele linii, zazwyczaj dobrym rozwiązaniem jest możliwość jednoczesnego wyświetlania wszystkich połączeń na wszystkich liniach. Gdy ta funkcja jest włączona, wszystkie połączenia będą wyświetlane na linii podstawowej, ale nadal można wybrać określoną linię, aby zawęzić wyświetlane wyniki do połączeń przeprowadzonych tylko na tej linii.</p>
Serwer HTTPS	Włączone HTTP i HTTPS Tylko HTTPS	Włączone HTTP i HTTPS	Kontroluje typ komunikacji używanej przez telefon. Wybranie opcji Tylko HTTPS zwiększa bezpieczeństwo komunikacji.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Serwer dziennika protok. IPv6	Ciąg o długości do 256 znaków		Wskazuje serwer dziennika protokołu IPv6. Format adresu jest następujący: <b>[adres] : &lt;port&gt;@@base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b>
Dziennik zdalny	Wyłączone włączone	Wyłączone	Służy do sterowania możliwością wysyłania dzienników do serwera dziennika systemowego.
Profil dziennika	Domyślny Ustawienie wstępne Telefonia SIP IU Network Nośniki Uaktualnienie Urządzenie Bezpieczeństwo Wi-Fi VPN EnergyWise MobileRemoteAc	Ustawienie wstępne	Określa wstępnie zdefiniowany profil dziennika. <ul style="list-style-type: none"> <li>• Domyślny — domyślny poziom dziennika debugowania</li> <li>• Ustawienie wstępne — nie zastępuje lokalnego ustawienia dziennika debugowania w telefonie</li> <li>• Telefonia — zapisuje w dzienniku informacje o połączeniach i funkcjach telefonii</li> <li>• SIP — zapisuje w dzienniku informacje o sygnalizacji SIP</li> <li>• IU — zapisuje w dzienniku informacje o interfejsie użytkownika telefonu</li> <li>• Sieć — zapisuje w dzienniku informacje o sieci</li> <li>• Nośniki — zapisuje w dzienniku informacje o nośnikach</li> <li>• Uaktualnienie — zapisuje w dzienniku informacje o uaktualnieniach</li> <li>• Urządzenie — zapisuje w dzienniku informacje o akcesoriach</li> <li>• Zabezpieczenia — zapisuje w dzienniku informacje o zabezpieczeniach</li> <li>• Wi-Fi — zapisuje w dzienniku informacje o sieciach Wi-Fi</li> <li>• VPN — zapisuje w dzienniku informacje o prywatnej sieci wirtualnej</li> <li>• EnergyWise — zapisuje w dzienniku informacje o oszczędzaniu energii</li> <li>• MobileRemoteAC — zapisuje w dzienniku informacje o dostępie z urządzeń przenośnych i dostępie zdalnym za pośrednictwem usługi Expressway</li> </ul>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Rozgłaszanie kodeków G.722 i iSAC	Użyj domyślnych wartości systemowych  Wyłączone  włączone	Użyj domyślnych wartości systemowych	<p>Wskazuje, czy telefon rozgłasza kodeki G.722 i iSAC w programie Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> <li>• Użyj domyślnych wartości systemowych — odwołuje się do ustawienia określonego w parametrze systemu przedsiębiorstwa Rozgłaszanie kodeka G.722.</li> <li>• Wyłączone — nie rozgłasza kodeka G.722 w programie Cisco Unified Communications Manager.</li> <li>• Włączone — rozgłasza kodek G.722 w programie Cisco Unified Communications Manager.</li> </ul> <p>Aby uzyskać więcej informacji, patrz uwaga pod tabelą.</p>
Wykrywanie uszkodzenia połączenia z Unified CM	Normalny  Opóźnione	Normalny	<p>Określa precyzję, z jaką telefon wykrywa uszkodzenie połączenia z programem Cisco Unified Communications Manager (Unified CM), co jest pierwszym krokiem przy awaryjnym przełączeniu urządzenia do zapasowego systemu Unified CM/SRST.</p> <ul style="list-style-type: none"> <li>• Normalne — wykrywanie uszkodzeń połączenia z Unified CM następuje ze standardową częstotliwością systemu. Wybierz tę wartość, aby szybciej wykrywać uszkodzenia połączenia z systemem Unified CM.</li> <li>• Opóźnione — wykrywanie uszkodzeń połączenia z Unified CM następuje około cztery razy wolniej niż w przypadku opcji Normalne. Wybierz tę opcję, jeśli wolisz, aby przełączenie zostało nieco opóźnione, licząc na samoistne przywrócenie połączenia.</li> </ul> <p>Precyzyjna różnica czasu między wykryciem uszkodzenia połączenia w obu przypadkach zależy od wielu nieustannie zmieniających się czynników.</p> <p>To pole dotyczy tylko połączenia przewodowego z siecią Ethernet.</p>
Ustalanie poziomu mocy	Wyłączone  włączone	włączone	<p>Umożliwia negocjowanie zasilania przez telefon za pomocą protokołu LLDP (Link Level Endpoint Discovery Protocol) i CDP (Cisco Discovery Protocol).</p> <p>Funkcji Power Negotiation nie należy wyłączać, jeśli telefon jest podłączony do przełącznika, który obsługuje negocjowanie zasilania. Po jej wyłączeniu przełącznik taki może odciąć zasilanie telefonu.</p>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Prezentacja sygnału wybierania przy przycisku Zwolnij	Wyłączone włączone	Wyłączone	Określa, czy użytkownik będzie słyszeć sygnał wybierania po wciśnięciu klawisza Zwolnij. <ul style="list-style-type: none"> <li>Wyłączone — użytkownik nie słyszy sygnału wybierania.</li> <li>Włączone — użytkownik usłyszy sygnał wybierania.</li> </ul>
Obraz tła	Ciąg do 64 znaków		Określa plik domyślnej tapety. Jeśli jest ustawiona tapeta domyślna, użytkownik nie może zmienić tapety telefonu.
Uproszczony UI nowego połączenia	Wyłączone włączone	Wyłączone	Kontroluje interfejs użytkownika w przypadku wybierania numeru z podniesioną słuchawką. Po włączeniu tej opcji użytkownik nie może wybrać numeru z listy ostatnich połączeń.  Gdy ta opcja jest włączona, to pole powoduje wyświetlenie użytkownikowi uproszczonego okna w celu nawiązania połączenia. Użytkownik nie widzi okna podręcznego z historią połączeń, które jest wyświetlane po podniesieniu słuchawki telefonu. Wyświetlanie okna podręcznego wydaje się przydatne, dlatego opcja Uproszczony UI nowego połączenia jest domyślnie wyłączona.
Revert to All Calls (Powrót do wszystkich połączeń)	Wyłączone włączone	Wyłączone	Określa, czy po zakończeniu wszystkich połączeń telefon powróci do wyświetlania wszystkich połączeń, jeśli połączenie znajduje się w filtrze innym niż Linia podstawowa, Wszystkie połączenia lub Połączenia ostrzegawcze.
Wyświetlaj historię połączeń tylko dla wybranej linii	Wyłączone włączone	Wyłączone	Steruje wyświetlaniem listy Ostatnie. <ul style="list-style-type: none"> <li>Wyłączone — lista Ostatnie zawiera historię połączeń dla wszystkich linii.</li> <li>Włączone — lista Ostatnie zawiera historię połączeń dla wybranej linii.</li> </ul>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących)	Wyłączone  Show for all Incoming Call (Wyświetlaj dla wszystkich połączeń przychodzących)  Wyświetlaj dla niewidocznych połączeń przychodzących	Show for all Incoming Call (Wyświetlaj dla wszystkich połączeń przychodzących)	<p>Kontroluje typ alertów połączeń przychodzących, które są wyświetlane na ekranie telefonu. To pole służy do zmniejszenia liczby naciśnień przycisków wymaganych do odebrania połączenia przez użytkownika.</p> <ul style="list-style-type: none"> <li>Wyłączone — Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących) jest wyłączony i użytkownik widzi tradycyjny wyskakujący alert połączeń przychodzących.</li> <li>Show for all Incoming Call (Wyświetlaj dla wszystkich połączeń przychodzących) — Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących) jest wyświetlany dla wszystkich połączeń, niezależnie od ich widoczności.</li> <li>Wyświetlaj dla niewidocznych połączeń przychodzących — Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących) jest wyświetlany dla wszystkich połączeń niewyświetlanych na telefonie. Ten parametr zachowuje się podobnie jak wyskakujące powiadomienie alertu połączeń przychodzących.</li> </ul>
Bit DF	0  1	0	<p>Określa, w jaki sposób wysyłane są pakiety sieciowe. Pakiety mogą być wysyłane w porcjach (fragmentach) o różnych rozmiarach.</p> <p>Gdy bit DF w nagłówku pakietu jest ustawiony na 1, łańcuch sieciowy nie jest dzielony na fragmenty podczas przechodzenia przez urządzenia sieciowe takie jak przełączniki i routery. Eliminacja fragmentowania pozwala uniknąć niepoprawnej analizy po stronie odbiorczej, lecz skutkuje nieco mniejszą prędkością.</p> <p>Ustawienie bitu DF nie wpływa na ruch ICMP, VPN, VXC VPN ani DHCP.</p>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Domyślny filtr linii	Lista oddzielonych przecinkami nazw urzędzeń telefonicznych		<p>Wskazuje listę telefonów, które znajdują się w filtrze domyślnym.</p> <p>Po skonfigurowaniu domyślnego filtra linii użytkownicy widzą filtr o nazwie <b>Harmonogram dzienny</b> w sekcji <b>Powiadom. o poł.</b> w menu <b>Ustawienia &gt; Preferencje</b> w telefonie. Ten filtr harmonogramu dziennego jest uzupełnieniem wstępnie ustawionego filtra <b>Wszystkie połączenia</b>.</p> <p>Jeśli nie skonfigurowano domyślnego filtra linii, telefon sprawdza wszystkie udostępniane linie. Jeśli został skonfigurowany, telefon sprawdza linie określone w programie Cisco Unified Communications Manager, jeśli użytkownik wybierze <b>Filtr domyślny</b> jako filtr aktywny lub gdy nie istnieją filtry niestandardowe.</p> <p>Niestandardowe filtry linii umożliwiają filtrowanie linii o wysokim priorytecie, aby zmniejszyć liczbę powiadomień. Priorytet powiadomień o połączeniach przychodzących można ustawić dla podzbioru linii objętych przez filtr powiadomień. Filtr niestandardowy generuje albo tradycyjne powiadomienia wyskakujące, albo umożliwiające podjęcie działań alerty o połączeniach przychodzących na wybranych liniach. Dla każdego filtra tylko obejmowany przez niego podzbiór linii wygeneruje alert. Ta funkcja umożliwia użytkownikom korzystającym z wielu linii zmniejszenie aktywności związanej z alertami poprzez filtrowanie i wyświetlanie alertów tylko z linii o wysokim priorytecie. Użytkownicy końcowi mogą samodzielnie konfigurować tę opcję. Alternatywnie można zaprogramować domyślny filtr linii i przesłać filtr do telefonu.</p>
Najniższy priorytet stanu powiadamiania linii	Wyłączone włączone	Wyłączone	<p>Określa stan alertu w przypadku korzystania z linii wspólnych.</p> <ul style="list-style-type: none"> <li>Wyłączone — gdy pojawi się połączenie przychodzące powodujące alert na linii wspólnej, stan alertu będzie sygnalizowany przez diodę LED/ikonę stanu, a nie przez ikonę zdalnego użycia.</li> <li>Włączone — gdy pojawi się połączenie przychodzące powodujące alert na linii wspólnej, użytkownik zobaczy ikonę zdalnego użycia.</li> </ul>



Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Wyświetlanie jednokolumnowe dla modułu KEM	Wyłączone włączone	Wyłączone	Kontroluje sposób wyświetlania w kluczowym module rozszerzeń.  <ul style="list-style-type: none"> <li>Wyłączone — moduł rozszerzeń używa trybu dwukolumnowego.</li> <li>Włączone — moduł rozszerzeń używa trybu jednokolumnowego.</li> </ul> <p>Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.</p>
Energy Efficient Ethernet (EEE): port komputera	Wyłączone włączone	Wyłączone	Steruje protokołem EEE na porcie komputera.
Energy Efficient Ethernet (EEE): port oprogramowania	Wyłączone włączone	Wyłączone	Steruje protokołem EEE na porcie przełącznika.
Początkowy port wideo			Określa początek zakresu portów dla połączeń wideo.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Końcowy port wideo			Określa koniec zakresu portów dla połączeń wideo.  Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Zachowywanie poświadczeń użytkownika przy logowaniu do usługi Expressway	Wyłączone włączone	Wyłączone	Określa, czy na telefonie są przechowywane poświadczenia logowania użytkowników. Gdy ta opcja jest wyłączona, zawsze pojawia się monit o zalogowanie się na serwerze Expressway w celu uzyskania dostępu do usług MRA (Mobile and Remote Access).  Aby ułatwić użytkownikom logowanie się, włącz tę opcję. Poświadczenia logowania do Expressway będą wtedy trwałe. W takim przypadku użytkownik będzie musiał podać poświadczenia logowania tylko za pierwszym razem. Później (po włączeniu telefonu poza firmą) dane logowania będą automatycznie uzupełniane na ekranie logowania.  Aby uzyskać więcej informacji, patrz <a href="#">Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway</a> , na stronie 186.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Adres URL obsługi klienta	Ciąg, do 256 znaków		Określa adres URL Narzędzia do zgłaszania problemów (PRT). Jeśli urządzenia z funkcją Mobile and Remote Access wdrożono przez usługę Expressway, na serwerze Expressway należy dodać adres serwera PRT do listy dozwolonych serwerów HTTP. Aby uzyskać więcej informacji, patrz <a href="#">Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway</a> , na stronie 186.
Administrator sieci WWW	Wyłączone włączone	Wyłączone	Włącza lub wyłącza dostęp administratora do stron WWW telefonu za pomocą przeglądarki. Aby uzyskać więcej informacji, patrz <a href="#">Konfigurowanie strony administrowania telefonem</a> , na stronie 111. Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Hasło administratora	Ciąg o długości 8–127 znaków		Określa hasło administratora wymagane do uzyskiwania dostępu do stron WWW telefonu jako administrator. Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Serwer WLAN SCEP	Ciąg o długości do 256 znaków		Określa serwer protokołu SCEP używany przez telefon do pobierania certyfikatów do uwierzytelniania w sieci WLAN. Wprowadź nazwę hosta lub adres IP (w standardowym formacie adresów IP) serwera. Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Odcisk palca głównego urzędu certyfikacji WLAN (SHA256 lub SHA1)	Ciąg o długości do 95 znaków		<p>Określa odcisk palca SHA256 lub SHA1 głównego urzędu certyfikacji używany do sprawdzania poprawności podczas procesu SCEP w chwili wydawania certyfikatów w celu uwierzytelniania w sieci WLAN. Zalecamy używanie odcisku palca SHA256, który można uzyskać za pośrednictwem protokołu OpenSSL (np. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) lub przy użyciu przeglądarki WWW, aby sprawdzić szczegóły certyfikatu.</p> <p>Wprowadź 64 znaki szesnastkowe w przypadku odcisku palca SHA256 lub 40 znaków szesnastkowych w przypadku odcisku palca SHA1, z takim samym separatorem (dwukropek, dywiz, kropka, spacja) lub bez separatora. Jeśli używany jest separator, powinien on być umieszczany równomiernie co 2, 4, 8, 16 lub 32 znaki szesnastkowe w przypadku odcisku palca SHA256 lub co 2, 4 lub 8 znaków szesnastkowych w przypadku odcisku palca SHA1.</p> <p>Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.</p>
Liczba prób uwierzytelniania w sieci WLAN			Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Tryb monitu profilu sieci WLAN 1	Wyłączone włączone	Wyłączone	Na telefonach, które nie obsługują tej funkcji, to pole nie jest wyświetlane.
Tryb linii	Tryb linii sesji Tryb linii zaawansowanej	Tryb linii sesji	<p>Kontroluje wyświetlanie linii na telefonie.</p> <ul style="list-style-type: none"> <li>Tryb linii sesji — przyciski po jednej stronie ekranu są klawiszami linii.</li> <li>Tryb rozszerzony linii — przyciski po obu stronach wyświetlacza telefonu są klawiszami linii. W trybie rozszerzonym linii domyślnie włączone są funkcje przewidywania wybieranego numeru oraz realizowanych alertów połączeń przychodzących.</li> </ul>
Konfigurowalny dzwonek administratora	Wyłączone Wschód słońca Chirp1 Chirp2	Wyłączone	<p>Kontroluje sygnał dzwonienia i możliwość jego ustawiania przez użytkowników.</p> <ul style="list-style-type: none"> <li>Po ustawieniu opcji <b>Wyłączone</b> użytkownicy mogą konfigurować domyślny sygnał dzwonienia na swoim telefonie.</li> <li>Dowolna inna wartość uniemożliwia zmianę sygnału dzwonienia. Element menu <b>Dzwonek</b> w menu <b>Ustawienia</b> jest wyszarzony.</li> </ul>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Wsparcie dla klientów	Ciąg o długości do 64 znaków	Puste	Tylko do użytku przez centrum Cisco TAC.
Wyłącz szyfrowanie TLS	Zobacz <a href="#">Wyłącz szyfrowanie TLS (Transport Layer Security)</a> , na stronie 173.	Brak	Wyłącza wybrane szyfrowanie TLS. Wyłącz więcej niż jeden pakiet szyfrowania, przytrzymując klawisz <b>Ctrl</b> na klawiaturze komputera i zaznaczając pakiety. Wybranie wszystkich szyfrów telefonu będzie mieć wpływ na działanie usługi TLS telefonu.
Oobniżenie poziomu dźwięku	włączone Wyłączone	włączone	Steruje funkcją Obniżenie poziomu dźwięku. <ul style="list-style-type: none"> <li>• Wyłączono: <ul style="list-style-type: none"> <li>• W telefonie nie jest wyświetlany element menu <b>Obniżenie poziomu dźwięku</b> w menu <b>Ustawienia</b>.</li> <li>• Użytkownicy nie będą widzieć wiadomości na ekranie, gdy będą mówić głośno.</li> </ul> </li> <li>• Włączony: <ul style="list-style-type: none"> <li>• Użytkownicy sterują funkcją za pomocą pozycji menu <b>Obniżenie poziomu dźwięku</b> w menu <b>Ustawienia</b>. Domyślnie ta opcja jest <b>włączona</b>.</li> </ul> </li> </ul>
Oznaczanie połączeń jako spam	włączone Wyłączone	włączone	Służy do sterowania funkcją Oznaczanie połączeń jako spam. <ul style="list-style-type: none"> <li>• Wyłączono: <ul style="list-style-type: none"> <li>• Telefon nie wyświetla klawisza programowego <b>Oznacz jako spam</b>.</li> <li>• Pozycja <b>Lista spamu</b> w menu <b>Ustawienia</b> nie zostanie wyświetlona.</li> <li>• Jeśli dostępna była lista spamu, dane z listy zostaną usunięte i nie można będzie ich odzyskać.</li> </ul> </li> <li>• Włączony: <ul style="list-style-type: none"> <li>• Telefon wyświetla klawisz programowy <b>Oznacz jako spam</b>.</li> <li>• Zostanie wyświetlona pozycja <b>Lista spamu</b> w menu <b>Ustawienia</b>.</li> </ul> </li> </ul>

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis i zasady użycia
Jedna linia przeznaczona do parkowania połączeń	Wyłączone włączone	włączone	Określa, czy zaparkowane połączenie zajmuje jedną linię, czy nie.  Więcej wiadomości na ten temat można znaleźć w dokumentacji programu Cisco Unified Communications Manager.
Etykieta tekstowa linii: wyświetlanie w ELM	Wyłączone włączone	włączone	Steruje wyświetlaniem etykiety linii podczas połączenia, gdy skonfigurowany jest tryb linii rozszerzonej. <ul style="list-style-type: none"> <li>• włączone <ul style="list-style-type: none"> <li>• Jeśli nazwa abonenta wywołującego jest skonfigurowana, w pierwszym wierszu sesji wywołania wyświetlana jest nazwa, a w drugim wierszu etykieta linii lokalnej.</li> <li>• Jeśli nazwa abonenta wywołującego nie jest skonfigurowana, w pierwszej linii wyświetlany jest numer zdalny, a w drugiej etykieta linii lokalnej.</li> </ul> </li> <li>• Wyłączone <ul style="list-style-type: none"> <li>• Jeśli skonfigurowano nazwę dzwoniącego, w pierwszym wierszu sesji połączeń wyświetlana jest nazwa, a w drugim wierszu numer.</li> <li>• Jeśli nazwa abonenta wywołującego nie jest skonfigurowana, wyświetlany jest <b>tylko</b> numer zdalny.</li> </ul> </li> </ul> <p>To pole jest wymagane.</p>

**Uwaga**

Negocjacja kodeka składa się z dwóch kroków:

1. Telefon zgłasza obsługiwane kodeki do programu Cisco Unified Communications Manager. Nie wszystkie punkty końcowe obsługują ten sam zestaw kodeków.
2. Gdy program Cisco Unified Communications Manager otrzyma listę obsługiwanych kodeków ze wszystkich telefonów próbujących nawiązać połączenie, wybierze kodek obsługiwany przez największą liczbę urządzeń z uwzględnieniem różnych czynników, takich jak ustawienie par regionów.

## Sprawdzone procedury konfigurowania funkcji

Funkcje telefonu można konfigurować odpowiednio do potrzeb użytkowników. Przygotowaliśmy zalecenia, które mogą okazać się przydatne w określonych sytuacjach i rodzajach wdrożeń.

## Środowiska z dużą liczbą połączeń

W przypadku środowiska z dużą liczbą połączeń zalecamy specjalną konfigurację niektórych funkcji.

Pole	Obszar administracji	Zalecane ustawienie
Always Use Prime Line (Zawsze używaj linii podstawowej)	Informacje o urządzeniu	Wyłączone lub Włączone Aby uzyskać więcej informacji, patrz Pole: <a href="#">Always Use Prime Line (Zawsze używaj linii podstawowej)</a> , na stronie 173.
Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących)	Układ konfiguracji specyficznej dla produktu	Show for all Incoming Call (Wyświetlaj dla wszystkich połączeń przychodzących)
Show All Calls on Primary Line (Wyświetlaj wszystkie połączenia na linii podstawowej)	Układ konfiguracji specyficznej dla produktu	włączone
Revert to All Calls (Powrót do wszystkich połączeń)	Układ konfiguracji specyficznej dla produktu	włączone

## Środowiska z wieloma liniami

W przypadku środowiska z wieloma liniami zalecamy specjalną konfigurację niektórych funkcji.

Pole	Obszar administracji	Zalecane ustawienie
Always Use Prime Line (Zawsze używaj linii podstawowej)	Informacje o urządzeniu	Wył Aby uzyskać więcej informacji, patrz Pole: <a href="#">Always Use Prime Line (Zawsze używaj linii podstawowej)</a> , na stronie 173.
Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących)	Układ konfiguracji specyficznej dla produktu	Show for all Incoming Call (Wyświetlaj dla wszystkich połączeń przychodzących)
Show All Calls on Primary Line (Wyświetlaj wszystkie połączenia na linii podstawowej)	Układ konfiguracji specyficznej dla produktu	włączone
Revert to All Calls (Powrót do wszystkich połączeń)	Układ konfiguracji specyficznej dla produktu	włączone

## Środowisko trybu linii sesji

Tryb rozszerzony linii jest preferowanym narzędziem do pracy w większości środowisk połączeń. Jeśli tryb rozszerzony linii nie odpowiada jednak potrzebom, wówczas można użyć trybu linii sesji.

Pole	Obszar administracji	Zalecane ustawienie dla trybu linii sesji
Show All Calls on Primary Line (Wyświetlaj wszystkie połączenia na linii podstawowej)	Układ konfiguracji specyficznej dla produktu	Wyłączone
Revert to All Calls (Powrót do wszystkich połączeń)	Układ konfiguracji specyficznej dla produktu	Wyłączone
Actionable Incoming Call Alert (Realizowany alert połączeń przychodzących)	Układ konfiguracji specyficznej dla produktu	Funkcja włączana domyślnie (firmware w wersji 11.5 (1) i nowsze).

#### Tematy pokrewne

[Konfigurowanie klawiszy linii dodatkowej](#), na stronie 211

[Funkcje dostępne w trybie rozszerzonym linii](#), na stronie 212

## Pole: Always Use Prime Line (Zawsze używaj linii podstawowej)

Pole to określa, czy po podniesieniu słuchawki przez użytkownika telefon IP ma zawsze wybierać linię podstawową. Jeśli dla tego parametru wybrane jest ustawienie Prawda, po podniesieniu słuchawki wybierana jest linia podstawowa, która staje się aktywna. Nawet jeśli dzwonek sygnalizuje połączenie na drugiej linii użytkownika, podniesienie słuchawki spowoduje uaktywnienie pierwszej linii. Połączenie przychodzące na drugiej linii nie zostanie odebrane. W takim przypadku w celu odebrania połączenia użytkownik musi samodzielnie wybrać drugą linię. Wartość domyślna tego parametru to Fałsz.

Przeznaczenie pola Always Use Prime Line jest bardzo podobne do kombinacji parametrów Show All Calls on the Primary Line (Wyświetlaj wszystkie połączenia na linii podstawowej) i Revert to All Calls (Powrót do wszystkich połączeń), gdy oba są włączone naraz. Główna różnica polega jednak na tym, że po włączeniu pola Always Use Prime Line połączenia przychodzące na drugiej linii nie są odbierane. Na linii podstawowej słychać tylko sygnał wybierania. Występują pewne środowiska z dużą liczbą połączeń, w których jest to przydatna funkcja telefonu. Ogólnie lepiej pozostawić to pole wyłączone z wyjątkiem wspomnianych środowisk, które wymagają jego włączenia.

## Wyłącz szyfrowanie TLS (Transport Layer Security)

Można wyłączyć szyfry protokołu TLS (Transport Layer Security) przy użyciu parametru **Wyłącz szyfrowanie TLS**. Dzięki temu można dostosować zabezpieczenia pod kątem znanych luk i zapewnić zgodność sieci z zasadami dotyczącymi szyfrów obowiązującymi w firmie.

Domyślnym ustawieniem jest Brak.

Wyłącz więcej niż jeden pakiet szyfrowania, przytrzymując klawisz **Ctrl** na klawiaturze komputera i zaznaczając pakiety. Wybranie wszystkich szyfrów telefonu będzie mieć wpływ na działanie usługi TLS telefonu. Dostępne są następujące opcje:

- Brak
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

Aby uzyskać więcej informacji o zabezpieczeniach telefonu, zobacz *Omówienie zabezpieczeń telefonów IP Cisco z serii 7800 i 8800* (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html>).

## Włączanie historii połączeń dla linii wspólnej

Umożliwia wyświetlenie Twoich aktywności na linii wspólnej w ramach funkcji Historia połączeń. Ta funkcja:

- Rejestruje połączenia nieodebrane na wspólnej linii
- Rejestruje wszystkie odebrane i nawiązane połączenia na wspólnej linii

### Zanim rozpoczniesz

Przed włączeniem historii połączeń dla linii wspólnej wyłącz funkcję Prywatność. W przeciwnym razie w historii połączeń nie zostaną wyświetlone połączenia odbierane przez innych użytkowników.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Telefon**.
  - Krok 2** Odszukaj telefon do skonfigurowania.
  - Krok 3** W obszarze Konfiguracja specyficzna dla produktu przejdź do listy rozwijanej Zapisuj dziennik połączeń na linii wspólnej.
  - Krok 4** Z listy rozwijanej wybierz pozycję **Włączone**.
  - Krok 5** Kliknij przycisk **Zapisz**.
- 

## Planowane oszczędzanie energii Power Save dla telefonów IP Cisco

W celu oszczędzania energii elektrycznej i zwiększenia trwałości wyświetlacza telefonu można skonfigurować wyłączenie ekranu, gdy nie jest używany.

W aplikacji Cisco Unified Communications Manager — administracja można skonfigurować wyłączenie wyświetlacza o ustalonej porze w wybrane dni i przez całą dobę w pozostałe dni. Można np. ustawić wyłączenie wyświetlacza po godzinach pracy w dni robocze oraz przez całe dni w soboty i niedziele.

W dowolnej chwili, gdy wyświetlacz jest wyłączony, użytkownik może wykonać jedną z następujących czynności, aby go włączyć:



- Naciśnij dowolny przycisk na telefonie.

Po włączeniu wyświetlacza telefon podejmuje działanie określone przez ten przycisk.

- Podnieś słuchawkę.

Po włączeniu wyświetlacza pozostanie on włączony do momentu, gdy telefon będzie bezczynny przez określony czas, a następnie automatycznie się wyłączy.

Aby uzyskać więcej informacji, patrz [Konfiguracja specyficzna dla produktu, na stronie 149](#).

### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon, który chcesz skonfigurować.
- Krok 3** Przejdź do obszaru Konfiguracja specyficzna dla produktu i ustaw wartości poniższych pól:
- Dni nieaktyw. ekranu
  - Godz. rozpocz. wyświetl.
  - Czas wyświetlania
  - Czas nieakt. ekranu

**Tabela 32: Pola konfiguracji funkcji Oszczędzanie energii**

Pole	Opis
Dni nieaktyw. ekranu	Dni, w których wyświetlacz nie włącza się automatycznie o godzinie określonej w polu Godz. rozpocz. wyświetl.  Wybierz dzień lub dni z listy rozwijanej. Aby wybrać więcej niż jeden dzień, kliknij każdy wybierany dzień, trzymając wciśnięty klawisz Ctrl.
Godz. rozpocz. wyświetl.	Godzina, o której każdego dnia wyświetlacz jest automatycznie włączany (z wyjątkiem dni określonych w polu Dni nieaktyw. ekranu).  W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ.  Aby na przykład wyświetlacz automatycznie włączał się o godzinie 7:00 rano (0700), wprowadź <b>07:00</b> . Aby włączyć wyświetlacz o godzinie 2:00 po południu (1400), wprowadź <b>14:00</b> .  Jeśli to pole jest puste, wyświetlacz automatycznie włączy się o godzinie 00:00.

Pole	Opis
Czas wyświetlania	<p>Czas, przez który wyświetlacz pozostaje włączony po włączeniu o godzinie określonej w polu Godz. rozpocz. wyświetl.</p> <p>Wprowadź wartość w tym polu w formacie <i>godziny:minuty</i>.</p> <p>Aby na przykład wyświetlacz pozostawał włączony przez 4 godziny i 30 minut po automatycznym włączeniu, wprowadź <b>04:30</b>.</p> <p>Jeśli to pole jest puste, telefon wyłączy się na koniec dnia (0:00).</p> <p><b>Uwaga</b> Jeśli w polu Godz. rozpocz. wyświetl. wpisana jest wartość 0:00 i czas włączonego wyświetlacza jest pusty (lub ma wartość 24:00), wyświetlacz pozostanie włączony przez cały czas.</p>
Czas nieakt. ekranu	<p>Czas bezczynności telefonu, po upływie którego wyświetlacz zostanie wyłączony. Działa tylko wtedy, gdy wyświetlacz został wyłączony zgodnie z planem, a następnie został włączony przez użytkownika (przez naciśnięcie przycisku w telefonie lub podniesienie słuchawki).</p> <p>Wprowadź wartość w tym polu w formacie <i>godziny:minuty</i>.</p> <p>Aby na przykład wyświetlacz, po włączeniu go przez użytkownika, wyłączał się po okresie bezczynności równym 1 godzinę i 30 minut, wprowadź <b>01:30</b>.</p> <p>Wartość domyślna to 01:00.</p>

- Krok 4** Kliknij przycisk **Zapisz**.
- Krok 5** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
- Krok 6** Uruchom ponownie telefon.

## Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco

Jeśli system zawiera kontroler EnergyWise, można zmniejszyć zużycie energii, konfigurując telefon do przechodzenia w stan uśpienia i wychodzenia z niego.

W narzędziu Cisco Unified Communications Manager — administracja można skonfigurować ustawienia włączające usługę EnergyWise oraz określające godziny wchodzenia i wychodzenia ze stanu uśpienia. Te parametry są bezpośrednio powiązane z parametrami konfiguracji wyświetlacza telefonu.

Po włączeniu usługi EnergyWise i ustawieniu godziny przechodzenia w stan uśpienia telefon wysyła do przełącznika żądanie wybudzenia o skonfigurowanej godzinie. Przełącznik akceptuje lub odrzuca żądanie. W przypadku odrzucenia żądania przez przełącznik lub w braku odpowiedzi telefon nie przechodzi w stan uśpienia. W przypadku zaakceptowania żądania bezczynny telefon przechodzi w stan uśpienia, zmniejszając zużycie energii do określonego poziomu. Telefon, który nie pozostaje bezczynny, ustawia zegar bezczynności i przechodzi w stan uśpienia po upływie ustawionego czasu.

Aby telefon wyszedł ze stanu uśpienia, naciśnij przycisk Wybierz. O zaplanowanej godzinie wznawiania system przywraca dostarczanie energii do telefonu, wyprowadzając go ze stanu uśpienia.

Aby uzyskać więcej informacji, patrz [Konfiguracja specyficzna dla produktu, na stronie 149](#).

**Procedura**

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon, który chcesz skonfigurować.
- Krok 3** Przejdź do obszaru Product Specific Configuration (Konfiguracja specyficzna dla produktu) i skonfiguruj poniższe pola.
- Włącz Power Save Plus
  - Godzina włączenia telefonu
  - Godzina wyłączenia telefonu
  - Wyłącz telefon po czasie nieaktywności
  - Włącz alert dźwiękowy
  - Domena EnergyWise
  - Hasło EnergyWise
  - Zezwól na zastąpienie przez EnergyWise

**Tabela 33: Pola konfiguracji funkcji EnergyWise**

Pole	Opis
Włącz Power Save Plus	<p>Określa dni, w których telefon jest wyłączany. Aby wybrać większą liczbę dni, wciśnij i przytrzymaj klawisz Control, jednocześnie klikając dni na harmonogramie.</p> <p>Domyślnie żadne dni nie są zaznaczone.</p> <p>Po zaznaczeniu opcji Power Save Plus zostanie wyświetlony komunikat ostrzegający o potencjalnych zagrożeniach (e911).</p> <p><b>Przeostroga</b> W trybie Power Save Plus punkty końcowe skonfigurowane dla tego trybu (“Tryb”) są wyłączone i nie można dokonywać z nich połączeń alarmowych ani odbierać na nich połączeń przychodzących. Wybierając ten tryb, należy uwzględnić następujące kwestie: (i) bierzesz na siebie pełną odpowiedzialność za dostarczenie alternatywnej metody nawiązywania połączeń alarmowych i odbierania połączeń przy uruchomionym trybie; (ii) firma Cisco nie ponosi odpowiedzialności za włączenie tego trybu, a cała odpowiedzialność związana z jego włączeniem trybu spoczywa na Tobie; oraz (iii) poinformujesz wyczerpująco wszystkich użytkowników o wpływie wprowadzenia tego trybu na połączenia, ich nawiązywanie itp.</p> <p><b>Uwaga</b> Aby wyłączyć tryb Power Save Plus, należy usunąć zaznaczenie pola wyboru Zezwól na zastąpienie przez EnergyWise. Jeśli pole Zezwól na zastąpienie przez EnergyWise pozostaje zaznaczone, ale w polu Włącz Power Save Plus nie wpisano liczby dni, funkcja Power Save Plus nie jest wyłączona.</p>

Pole	Opis
Godzina włączenia telefonu	<p>Określa, że telefon włącza się automatycznie w dni wybrane w polu Włącz Power Save Plus.</p> <p>W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ.</p> <p>Aby automatycznie włączyć telefon np. o godzinie 7 rano, (0700), wprowadź 07:00. Aby włączyć telefon o drugiej po południu, (1400), wprowadź 14:00.</p> <p>Wartość domyślna jest pusta, co oznacza 00:00.</p> <p><b>Uwaga</b> Godzina włączenia telefonu musi być ustawiona na co najmniej 20 minut później niż Godzina wyłączenia telefonu. Na przykład, jeśli Godzina wyłączenia telefonu jest ustawiona na 07:00, Godzina włączenia telefonu nie może być wcześniejsza niż 07:20.</p>
Godzina wyłączenia telefonu	<p>Godzina, o której telefon jest wyłączany w dni wybrane w polu Włącz Power Save Plus. Jeśli pola Godzina włączenia telefonu i Godzina wyłączenia telefonu mają taką samą wartość, telefon nie zostanie wyłączony.</p> <p>W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ.</p> <p>Aby automatycznie wyłączyć telefon np. o godzinie 7 rano, (0700), wprowadź 7:00. Aby wyłączyć telefon o drugiej po południu, (1400), wprowadź 14:00.</p> <p>Wartość domyślna jest pusta, co oznacza 00:00.</p> <p><b>Uwaga</b> Godzina włączenia telefonu musi być ustawiona na co najmniej 20 minut później niż Godzina wyłączenia telefonu. Na przykład, jeśli Godzina wyłączenia telefonu jest ustawiona na 7:00, Godzina włączenia telefonu nie może być wcześniejsza niż 7:20.</p>
Wyłącz telefon po czasie nieaktywności	<p>Czas nieaktywności telefonu, po upływie którego zostanie on wyłączony.</p> <p>Limit czasu jest uwzględniany w następujących okolicznościach:</p> <ul style="list-style-type: none"> <li>• Gdy telefon był w trybie Power Save Plus zgodnie z harmonogramem i wyszedł z tego trybu po naciśnięciu przez użytkownika klawisza <b>Wybierz</b>.</li> <li>• Gdy ponownie włączono zasilanie telefonu za pomocą przełącznika.</li> <li>• Jeśli osiągnięto godzinę określoną przez parametr Godzina wyłączenia telefonu, ale telefon jest nadal używany.</li> </ul> <p>Pole może przyjmować wartości z zakresu od 20 do 1440 minut.</p> <p>Wartość domyślna to 60 minut.</p>

Pole	Opis
Włącz alert dźwiękowy	<p>Po włączeniu tej opcji telefon odtwarza alert dźwiękowy na 10 minut przed godziną podaną w polu Godzina wyłączenia telefonu.</p> <p>Alarm dźwiękowy wykorzystuje dzwonek telefonu, który odtwarza krótki dźwięk o określonych porach w 10-minutowym okresie alertu. Dzwonek, służący jako alarm, jest odtwarzany z głośnością wyznaczoną przez użytkownika. Obowiązuje następujący harmonogram alertu:</p> <ul style="list-style-type: none"> <li>• Na 10 minut przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany czterokrotnie.</li> <li>• Na 7 minut przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany czterokrotnie.</li> <li>• Na 4 minuty przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany czterokrotnie.</li> <li>• Na 30 sekund przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany 15 razy lub do momentu wyłączenia telefonu.</li> </ul> <p>To pole wyboru jest uwzględniane tylko wtedy, gdy w polu listy Włącz Power Save Plus zaznaczono co najmniej jeden dzień.</p>
Domena EnergyWise	<p>Domena EnergyWise, w której znajduje się telefon.</p> <p>Maksymalna długość tego pola to 127 znaków.</p>
Hasło EnergyWise	<p>Tajne hasło zabezpieczeń używane podczas komunikacji z punktami końcowymi w domenie EnergyWise.</p> <p>Maksymalna długość tego pola to 127 znaków.</p>

Pole	Opis
Zezwól na zastąpienie przez EnergyWise	<p>Pole wyboru określa, czy zasady kontrolera domeny EnergyWise mogą zezwalać na wysyłanie do telefonu informacji o zmianie poziomu zasilania. Muszą zostać spełnione następujące warunki:</p> <ul style="list-style-type: none"> <li>• W polu Włącz Power Save Plus musi być wybrany co najmniej jeden dzień.</li> <li>• Ustawienia w narzędziu Cisco Unified Communications Manager — administracja są wdrażane nawet wtedy, gdy funkcja EnergyWise przysyła komunikat o zastąpieniu.</li> </ul> <p>Na przykład jeśli Godzina wyłączenia telefonu jest ustawiona na godzinę 22:00, wartość w polu Godzina włączenia telefonu wynosi 06:00 (szósta rano), a w polu Włącz Power Save Plus wybrano co najmniej jeden dzień.</p> <ul style="list-style-type: none"> <li>• Jeśli funkcja EnergyWise powiadomi telefon o wyłączeniu przypadającym na godzinę 20:00, ta dyrektywa pozostanie w mocy (przyjmując brak interwencji użytkownika telefonu) aż do godziny skonfigurowanej w polu Godzina włączenia telefonu, czyli do 6:00.</li> <li>• O godzinie 6:00 rano telefon włączy się i ponownie rozpocznie otrzymywanie informacji o zmianach poziomu mocy w zależności od ustawień w narzędziu Unified Communications Manager — administracja.</li> <li>• Aby ponownie zmienić poziom zasilania w telefonie, funkcja EnergyWise musi wysłać nowe polecenie o zmianie poziomu zasilania.</li> </ul> <p><b>Uwaga</b> Aby wyłączyć tryb Power Save Plus, należy usunąć zaznaczenie pola wyboru Zezwól na zastąpienie przez EnergyWise. Jeśli pole Zezwól na zastąpienie przez EnergyWise pozostaje zaznaczone, ale w polu Włącz Power Save Plus nie wpisano liczby dni, funkcja Power Save Plus nie jest wyłączona.</p>

**Krok 4** Kliknij przycisk **Zapisz**.

**Krok 5** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).

**Krok 6** Uruchom ponownie telefon.

## Konfigurowanie funkcji Nie przeszkadzać

Gdy włączona jest funkcja Nie przeszkadzać, telefon w stanie dzwonienia nie emituje sygnału dzwonka albo w ogóle nie przekazuje żadnych powiadomień dźwiękowych ani wizualnych.

Gdy włączona jest funkcja Nie przeszkadzać, zmienia się kolor sekcji nagłówka ekranu telefonu oraz widoczny jest na nim komunikat Nie przeszkadzać.

W szablonie przycisków telefonu można przypisać funkcję Nie przeszkadzać do jednego z przycisków.

Więcej wiadomości na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager w sekcji dotyczącej funkcji Nie przeszkadzać.

## Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon do skonfigurowania.
- Krok 3** Ustaw następujące parametry.
- Nie przeszkadzać: to pole wyboru umożliwia włączanie w telefonie funkcji Nie przeszkadzać.
  - DND Option (Opcja funkcji Nie przeszkadzać): Ring Off (Dzwonek wyłączony), Call Reject (Odrzucanie połączeń) lub Use Common Phone Profile Setting (Użyj ustawienia ze wspólnego profilu telefonu).  
Nie należy wybierać opcji Call Reject, jeśli priorytetowe połączenia (MLPP) mają powodować emitowanie sygnału dzwonka pomimo włączonej funkcji Nie przeszkadzać.
  - DND Incoming Call Alert (Alert o połączeniu przychodzącym podczas działania funkcji Nie przeszkadzać): w razie potrzeby wybierz rodzaj alertu, który ma być odtwarzany przez telefon w przypadku połączeń przychodzących, gdy aktywna jest funkcja Nie przeszkadzać.
- Uwaga** Ten parametr znajduje się w oknach Wspólny profil telefonu i Konfiguracja telefonu. Pierwszeństwo ma wartość występująca w oknie Konfiguracja telefonu.
- Krok 4** Kliknij przycisk **Zapisz**.

## Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

# Włączanie funkcji Agent Greeting (Powitanie przez agenta)

Funkcja Agent Greeting umożliwia agentowi tworzenie i aktualizowanie nagranych powitań, które jest odtwarzane na początku połączenia, np. połączenia z klientem, zanim agent odezwie się do rozmówcy. Agent może zależnie od potrzeb nagrać jedno lub wiele powitań oraz je później aktualizować.

Gdy zadzwoni klient, i on, i agent słyszą nagrane powitanie. Agent może mieć wyciszony telefon w trakcie całego powitania lub odebrać połączenie przed jego zakończeniem.

Wszystkie kodeki obsługiwane przez telefon są też dostępne w ramach połączeń z funkcją Agent Greeting.

Więcej wiadomości na ten temat można znaleźć w dokumentacji konkretnej wersji programu Cisco Unified Communications Manager w sekcjach dotyczących wtrącania i prywatności.

## Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon IP, który chcesz skonfigurować.
- Krok 3** Przewiń do panelu Device Information Layout (Układ informacji o urządzeniu) i wybierz dla opcji **Wbudowany mostek** ustawienie **Wł.** lub **Domyślne**.
- Krok 4** Kliknij przycisk **Zapisz**.

- Krok 5** Sprawdź ustawienie mostka:
- Wybierz kolejno opcje **System > Parametry usługi**.
  - Wybierz odpowiedni serwer i właściwą usługę.
  - Przełącz do panelu Parametry całego klastra (Urządzenie — Telefon) i wybierz dla opcji **Built-in Bridge Enable** (Wbudowany mostek włączony) ustawienie **Wł**.
  - Kliknij przycisk **Zapisz**.

---

#### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Konfigurowanie monitorowania i nagrywania

Funkcja Monitorowanie i nagrywanie umożliwia przełożonemu dyskretne monitorowanie aktywnego połączenia. Żaden z uczestników połączenia nie słyszy przełożonego. Gdy połączenie jest monitorowane, użytkownik może usłyszeć w jego trakcie alert dźwiękowy.

Jeśli połączenie jest zabezpieczone, wyświetlana jest ikona z kłódką. Rozmówcy również mogą usłyszeć alert dźwiękowy sygnalizujący monitorowanie połączenia. Podłączone strony również mogą usłyszeć alert dźwiękowy sygnalizujący, że połączenie jest zabezpieczone i monitorowane.

Gdy trwa monitorowanie lub nagrywanie aktywnego połączenia, użytkownik może odbierać i nawiązywać połączenia interkodem. Jeśli nawiąże połączenie interkodem, aktywne połączenie zostanie zawieszona. Spowoduje to przerwanie sesji nagrywania i zawieszenie sesji monitorowania. W celu przywrócenia sesji monitorowania osoba, której połączenie jest monitorowane, musi je wznowić.

Więcej wiadomości na ten temat można znaleźć w dokumentacji konkretnej wersji programu Cisco Unified Communications Manager w częściach dotyczących monitorowania i nagrywania.

Poniższa procedura umożliwia dodanie użytkownika do standardowych grup użytkowników monitorujących.

#### Zanim rozpocznie

Aby program Cisco Unified Communications Manager obsługiwał monitorowanie i nagrywanie, należy go odpowiednio skonfigurować.

#### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Zarządzanie użytkownikami > Użytkownik aplikacji**.
- Krok 2** Zaznacz grupy użytkowników Standard CTI Allow Call Monitoring (Standardowa usługa CTI umożliwiająca monitorowanie połączeń) i Standard CTI Allow Call Recording (Standardowa usługa CTI umożliwiająca nagrywanie połączeń).
- Krok 3** Kliknij przycisk **Add Selected** (Dodaj wybrane).
- Krok 4** Kliknij przycisk **Add to User Group** (Dodaj do grupy użytkowników).
- Krok 5** Dodaj telefony użytkownika do listy kontrolowanych urządzeń użytkowników aplikacji.
- Krok 6** Kliknij przycisk **Zapisz**.
-



**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Konfigurowanie powiadamiania o przekierowywaniu połączeń

Ustawienia przekierowywania połączeń można modyfikować.

**Procedura**

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon do skonfigurowania.
- Krok 3** Skonfiguruj pola Call Forward Notification (Powiadamianie o przekierowywaniu połączeń).

Pole	Opis
Caller Name	Po zaznaczeniu tego pola wyboru nazwa rozmówcy jest wyświetlana w oknie powiadomienia.  Domyślnie to pole wyboru jest zaznaczone.
Caller Number	Po zaznaczeniu tego pola wyboru numer rozmówcy jest wyświetlany w oknie powiadomienia.  Domyślnie to pole wyboru nie jest zaznaczone.
Redirected Number (Przekierowany numer)	Po zaznaczeniu tego pola wyboru informacje o rozmówcy, który jako ostatni przekierował połączenie, są wyświetlane w oknie powiadomienia.  Przykład: jeśli rozmówca A dzwoni do B, ale B przekierował wszystkie połączenia do C, a C przekierował wszystkie połączenia do D, w oknie powiadomienia widocznym dla rozmówcy D wyświetlane są informacje o telefonie rozmówcy C.  Domyślnie to pole wyboru nie jest zaznaczone.
Wybrany numer	Po zaznaczeniu tego pola wyboru informacje o pierwotnym odbiorcy połączenia są wyświetlane w oknie powiadomienia.  Przykład: jeśli rozmówca A dzwoni do B, ale B przekierował wszystkie połączenia do C, a C przekierował wszystkie połączenia do D, w oknie powiadomienia widocznym dla rozmówcy D wyświetlane są informacje o telefonie rozmówcy B.  Domyślnie to pole wyboru jest zaznaczone.

- Krok 4** Kliknij przycisk **Zapisz**.

## Włączanie SZL dla list połączeń

Pole SZL dla list połączeń kontroluje również stan linii dla funkcji firmowej książki telefonicznej.

### Procedura

**Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **System > Enterprise Parameters (Parametry systemu przedsiębiorstwa)**.

**Krok 2** Pole SZL dla list połączeń umożliwia włączenie lub wyłączenie tej funkcji.

Domyślnie ta funkcja jest wyłączona.

Parametry ustawiane w obszarze konfiguracji specyficznej dla produktu mogą pojawiać się także w oknie Konfiguracja urządzenia dla różnych urządzeń oraz w oknie Enterprise Phone Configuration (Firmowa konfiguracja telefonów). Jeśli te same parametry zostaną ustawione również w tych innych oknach, ustawienie mające priorytet jest ustalane w następującej kolejności:

1. ustawienia w oknie Konfiguracja urządzenia
2. ustawienia w oknie Wspólny profil telefonu
3. ustawienia w oknie Enterprise Phone Configuration

**Krok 3** Kliknij przycisk **Zapisz**.

## Konfigurowanie protokołu Energy Efficient Ethernet dla przełącznika i portu komputera

IEEE 802.3az Energy Efficient Ethernet (EEE) jest rozszerzeniem standardowego protokołu 802.3 IEEE, które umożliwia zmniejszenie zużycia energii, nie wpływając przy tym na podstawowe funkcje karty sieciowej. Skonfigurowanie protokołu EEE umożliwia administratorowi sterowanie jego funkcjami EEE na porcie komputera osobistego i porcie przełącznika.



**Uwaga** Administratorzy muszą się upewnić, że pole wyboru zastąpienia jest zaznaczone na wszystkich stronach UCM, w przeciwnym razie protokół EEE nie będzie działać.

Administrator steruje funkcjami EEE za pomocą dwóch następujących parametrów:

- **Energy Efficient Ethernet:** port komputera: zapewnia nieprzerwane połączenie z komputerami osobistymi. Administrator może włączyć lub wyłączyć tę funkcję.
- **Energy Efficient Ethernet:** port przełącznika: zapewnia nieprzerwane połączenie

Aby uzyskać więcej informacji, patrz [Konfiguracja specyficzna dla produktu, na stronie 149](#)

## Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz jedno z następujących okien:
- **Urządzenie > Telefon**
  - **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**
  - **System > Konfiguracja telefonu przedsiębiorstwa**
- Jeśli ten parametr zostanie skonfigurowany w kilku oknach, obowiązuje następująca kolejność:
1. **Urządzenie > Telefon**
  2. **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**
  3. **System > Konfiguracja telefonu przedsiębiorstwa**
- Krok 2** Jeśli to konieczne, odzyskaj telefon.
- Krok 3** Ustaw wartości w polach **Energy Efficient Ethernet: port komputera** i **Energy Efficient Ethernet: port przełącznika**.
- Energy Efficient Ethernet: port komputera
  - Energy Efficient Ethernet: port przełącznika
- Krok 4** Kliknij przycisk **Zapisz**.
- Krok 5** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
- Krok 6** Uruchom ponownie telefon.
- 

## Konfigurowanie zakresu portów protokołu RTP/sRTP

Wartości portów protokołów RTP (ang. Real-Time Transport Protocol, protokół transmisji w czasie rzeczywistym) i sRTP (ang. secure Real-Time Transport Protocol, bezpieczny protokół transmisji w czasie rzeczywistym) konfiguruje się w profilu SIP. Wartości portów RTP i sRTP mieszczą się w zakresie od 2048 do 65535, z domyślnym zakresem od 16384 do 32764. Niektóre wartości portów w zakresie portów RTP i sRTP są przeznaczone dla innych usług telefonicznych. Nie można ich więc skonfigurować na potrzeby protokołu RTP ani sRTP.

Więcej wiadomości na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager w części dotyczącej funkcji Profil SIP.

## Procedura

---

- Krok 1** Wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Profil SIP**.
- Krok 2** Wybierz kryteria wyszukiwania, których chcesz użyć, i kliknij przycisk **Znajdź**.
- Krok 3** Wybierz profil do zmodyfikowania.

**Krok 4** W polach Start Media Port (Początkowy port nośnika) i Stop Media Port (Końcowy port nośnika) wprowadź odpowiednio początkową i końcową wartość zakresu portów.

Na poniższej liście podano porty protokołu UDP, które są używane przez inne usługi telefoniczne i dlatego niedostępne w przypadku protokołów RTP i sRTP:

**port 4051**

używany przez funkcję Równy dostęp do firmware

**port 5060**

służy do przekazywania profilu SIP poprzez protokół UDP

**zakres portów od 49152 do 53247**

używany na potrzeby lokalnych portów tymczasowych

**zakres portów od 53248 do 65535**

używany przez funkcję VxC single tunnel VPN (Sieć VPN z pojedynczym tunelem VxC)

**Krok 5** Kliknij przycisk **Zapisz**.

**Krok 6** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).

---

**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway

Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway (MRA) umożliwia pracownikom zdalnym wygodne i bezpieczne łączenie się z siecią firmową bez korzystania z tunelu klienta prywatnej sieci wirtualnej (VPN). Do zapewnienia bezpieczeństwa ruchu sieciowego usługa Expressway używa protokołu TLS (Transport Layer Security). Aby telefon mógł uwierzytelnić certyfikat Expressway i ustanowić sesję TLS, certyfikat Expressway musi być podpisany przez publiczny urząd certyfikacji zaufany przez firmware telefonu. Nie jest możliwa instalacja innych certyfikatów urzędu certyfikacji lub określenie zaufania do nich w celu uwierzytelnienia certyfikatu Expressway.

Lista certyfikatów urzędów certyfikacyjnych osadzonych w firmware telefonu jest dostępna na stronie <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html>.

Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway (MRA) współpracuje z usługą Cisco Expressway. Należy się zapoznać z dokumentacją usługi Cisco Expressway, w tym z podręcznikiem *Cisco Expressway Administrator Guide* (Podręcznik administratora Cisco Expressway) oraz *Cisco Expressway Basic Configuration Deployment Guide* (Przewodnik po wdrażaniu podstawowej konfiguracji usługi Cisco Expressway). Dokumentacja usługi Cisco Expressway jest dostępna pod adresem <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html>.

W przypadku użytkowników Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway obsługiwany jest tylko protokół IPv4.

Dodatkowe informacje o pracy z usługą Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway można znaleźć w następujących dokumentach:

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview (Preferowana architektura firmy Cisco do współpracy w przedsiębiorstwie — omówienie projektowe)*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD (Preferowana architektura firmy Cisco do współpracy w przedsiębiorstwie — CVD)*
- *Podręcznik wdrażania dostępu z urządzeń przenośnych i dostępu zdalnego za pośrednictwem usługi Cisco VCS*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides (Przewodniki po konfigurowaniu serwera Cisco TelePresence Video Communication)*
- *Podręcznik wdrażania dostępu z urządzeń przenośnych i dostępu zdalnego za pośrednictwem usługi Cisco Expressway*

Podczas procesu rejestracji telefon jest synchronizowany z serwerem NTP (Network Time Protocol) w celu uzyskania przeznaczonej do wyświetlania daty i godziny. W usłudze (MRA) jest używana opcja DHCP 42 służąca do lokalizacji adresu IP serwerów NTP wyznaczonych do synchronizacji godziny i daty. Jeśli w informacji o konfiguracji nie znaleziono tagu opcji DHCP 42, telefon szuka tagu 0.tandberg.pool.ntp.org w celu identyfikacji serwerów NTP.

Po zarejestrowaniu telefon korzysta z informacji pochodzącej z komunikatów SIP do synchronizowania wyświetlanej daty i godziny, o ile w konfiguracji telefonu w programie Cisco Unified Communications Manager nie ma skonfigurowanego serwera NTP.



**Uwaga** Jeśli w profilu bezpieczeństwa dowolnego telefonu zaznaczono opcję szyfrowanej konfiguracji TFTP, telefonu tego nie można używać do dostępu mobilnego ani zdalnego. To ograniczenie wynika z tego, że rozwiązanie MRA nie obsługuje urządzeń współdziałających z funkcją CAPF (Certificate Authority Proxy Function).

Usługa Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway obsługuje tryb rozszerzony linii.

W systemie usług MRA Mobile jest obsługiwany tryb SIP OAuth Ten tryb umożliwia korzystanie z tokenów dostępu OAuth na potrzeby uwierzytelniania w środowiskach zabezpieczonych.



**Uwaga** W przypadku protokołu SIP OAuth w trybie urządzeń przenośnych i dostępu zdalnego (MRA) przy wdrażaniu telefonu należy stosować tylko dostęp do numeru aktywacji przy użyciu urządzeń przenośnych i dostępu zdalnego. Aktywacja przy użyciu nazwy użytkownika i hasła nie jest obsługiwana.

Tryb SIP OAuth wymaga Expressway w wersji x14.0(1) lub nowszej lub programu Cisco Unified Communications Manager w wersji 14.0(1) lub nowszej.

Więcej informacji na temat trybu SIP OAuth zawiera *Podręcznik konfiguracji systemu programu Cisco Unified Communications Manager* w wersji 14.0(1) lub nowszej.

## Scenariusze wdrożeń

W poniższych sekcjach przedstawiono różne scenariusze wdrażania usługi Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.

### Użytkownik w siedzibie firmy loguje się do sieci przedsiębiorstwa

Po wdrożeniu Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway zaloguj się do sieci przedsiębiorstwa w siedzibie firmy. Telefon wykrywa sieć i rejestruje się w programie Cisco Unified Communications Manager.

### Użytkownik poza siedzibą firmy loguje się do sieci przedsiębiorstwa

Gdy znajdujesz się poza biurem, telefon wykrywa, że działa w trybie pracy poza siedzibą. Zostaje wyświetlone okno logowania Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway umożliwiające połączenie z siecią przedsiębiorstwa.

Pamiętaj o następujących kwestiach:

- Aby połączyć się z siecią, należy podać prawidłową domenę usługi, nazwę użytkownika i hasło.
- Należy zresetować tryb usługi, aby wyczyścić ustawienie Alternatywny serwer TFTP przed uzyskaniem dostępu do sieci firmy. Powoduje to wyzerowanie ustawienia Alternatywny serwer TFTP, dzięki czemu telefon wykryje sieć poza siedzibą firmy i zapobiegnie tworzeniu połączenia VPN. Jeśli telefon jest wdrażany po raz pierwszy, należy pominąć ten krok.
- Jeśli w routerze sieciowym jest ustawiona opcja 150 lub 66 dla serwera DHCP, mogą wystąpić problemy z zalogowaniem się do sieci firmy. Należy zresetować tryb usługi, aby przejść do trybu MRA.

### Użytkownik poza siedzibą firmy loguje się do sieci przedsiębiorstwa za pomocą połączenia VPN

Użytkownik znajdujący się poza siedzibą firmy loguje się do jej sieci za pomocą połączenia VPN po wdrożeniu usługi Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.

Wykonaj Resetowanie podstawowe, aby zresetować konfigurację telefonu w przypadku wystąpienia błędu w telefonie.

Należy skonfigurować ustawienie Alternatywny serwer TFTP (**Ustawienia admin.** > **Ustawienia sieci** > **IPv4**, pole **Alternatywny serwer TFTP 1**).

#### Tematy pokrewne

[Resetowanie podstawowe](#), na stronie 287

## Ścieżki mediów i mechanizmy interaktywnego nawiązywania połączeń (ang. ICE, Interactive Connectivity Establishment)

Można wdrożyć mechanizmy interaktywnego nawiązywania połączeń (ang. ICE, Interactive Connectivity Establishment) w celu zwiększenia niezawodności połączeń z urządzeń przenośnych i przy użyciu dostępu zdalnego (MRA), które przechodzą przez zaporę lub usługę NAT. Mechanizmy ICE są składnikiem wdrażanym opcjonalnie, który używa tunelowania szeregowego i omijania usług NAT przy użyciu przekaźników w celu wybierania najlepszej ścieżki mediów dla połączenia.

Pomocniczy serwer przekierowań i przywracanie po awarii serwera przekierowań nie są obsługiwane.

Więcej informacji na temat rozwiązań MRA i ICE zawiera *Podręcznik konfiguracji systemu programu Cisco Unified Communications Manager w wersji 12.0(1)* lub nowszej. Dodatkowe informacje można znaleźć również w dokumentach RFC (ang. Request for Comment) komisji IETF (ang. Internet Engineering Task Force):

- *Rozwiązanie TURN (ang. Traversal Using Relays around NAT): rozszerzenia przekaźników dla rozwiązania STUN (Session Traversal Utilities for NAT)(RFC 5766)*
- *Mechanizm ICE (ang. Interactive Connectivity Establishment): protokół omijania usługi NAT dla protokołów oferowania/odbierania (RFC 5245)*

## Funkcje telefonu dostępne dla Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway

Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway zapewnia bezpieczny dostęp do usług współpracy dla mobilnych i zdalnych użytkowników urządzeń Cisco, nie korzystając przy tym z usługi VPN. Jednak w celu zachowania bezpieczeństwa sieci dostęp do niektórych funkcji telefonu został ograniczony.

Następująca lista zawiera funkcje telefonu dostępne podczas pracy z aplikacją Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.

**Tabela 34: Obsługa funkcji i Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway**

Funkcje telefonu	Wersja oprogramowania sprzętowego
Skrócone wybieranie	10.3(1) i nowsze
Odpowiedz na najstarsze	11.5(1)SR1 i nowsze
Wspomagane kierowane parkowanie połączenia	10.3(1) i nowsze
Automatyczne odbieranie	11.5(1)SR1 i nowsze
Wtrąć i WtrąćKon	11.5(1)SR1 i nowsze
Pole sygnalizacji aktywności linii	10.3(1) i nowsze
Pole sygnalizacji aktywności linii — przejęcie	10.3(1) i nowsze
Pole sygnalizacji aktywności linii — szybkie wybieranie	10.3(1) i nowsze
Oddzwon	10.3(1) i nowsze
Przekazywanie połączenia	10.3(1) i nowsze
Powiadomienie o przekierowaniu połączenia	10.3(1) i nowsze
Parkowanie połączenia	10.3(1) i nowsze
Przejmowanie połączeń	10.3(1) i nowsze
Cisco Unified Serviceability	11.5(1)SR1 i nowsze
Licencja dostępu klienta (CAL)	11.5(1)SR1 i nowsze
Połączenie konferencyjne	10.3(1) i nowsze
Lista konferencji/usuwanie uczestnika	11.5(1)SR1 i nowsze

<b>Funkcje telefonu</b>	<b>Wersja oprogramowania sprzętowego</b>
Firmowa książka telefon.	11.5(1)SR1 i nowsze
Aplikacje CTI (sterowane przez interfejs CTI)	11.5(1)SR1 i nowsze
Przekaz bezpośredni	10.3(1) i nowsze
Kierowane parkowanie połączenia	10.3(1) i nowsze
Odróżnialny dzwonek	11.5(1)SR1 i nowsze
Przekieruj	10.3(1) i nowsze
Tryb rozszerzony linii	12.1(1) i nowsze
Przekieruj	10.3(1) i nowsze
Wymuszone kody dostępu i kody spraw klientów	11.5(1)SR1 i nowsze
Przejmowanie połączeń grupy	10.3(1) i nowsze
Zawieś/Wznów	10.3(1) i nowsze
Cofnięcie zawieszenia	10.3(1) i nowsze
Natychmiastowe przekierowanie	10.3(1) i nowsze
Dołącz	10.3(1) i nowsze
Identyfikacja połączeń złośliwych (MCID)	11.5(1)SR1 i nowsze
Konferencja Meet Me	10.3(1) i nowsze
Wskaźnik wiadomości oczekującej	10.3(1) i nowsze
Mobile Connect	10.3(1) i nowsze
Usługa Mobile Voice Access	10.3(1) i nowsze
Wielopoziomowe pierwszeństwo i zastępowanie (MLPP)	11.5(1)SR1 i nowsze
Obsługa wielu linii	11.5(1)SR1 i nowsze
Muzyka podczas oczekiwania	10.3(1) i nowsze
Wyciszenie	10.3(1) i nowsze
Profile sieci (automatyczne)	11.5(1)SR1 i nowsze
Wybieranie z podniesioną słuchawką	10.3(1) i nowsze
Wybieranie z odłożoną słuchawką	10.3(1) i nowsze
Wybieranie Plus	10.3(1) i nowsze



Funkcje telefonu	Wersja oprogramowania sprzętowego
Prywatność	11.5(1)SR1 i nowsze
Funkcja Private Line Automated Ringdown (PLAR)	11.5(1)SR1 i nowsze
Wybierz ponownie	10.3(1) i nowsze
Szybkie wybieranie (nie obsługuje pauzy)	10.3(1) i nowsze
Przycisk Adres URL usług	11.5(1)SR1 i nowsze
Przenoszenie	10.3(1) i nowsze
Wybieranie URI (Uniform Resource Identifier)	10.3(1) i nowsze

## Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway

Gdy użytkownik loguje się do sieci za pomocą Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, wyświetlany jest monit o podanie domeny usługi, nazwy użytkownika i hasła. Jeśli zostanie włączony parametr „Zachowywanie poświadczeń użytkownika przy logowaniu do usługi Expressway”, poświadczenia logowania użytkowników są przechowywane, dzięki czemu nie trzeba ich ponownie wprowadzać. Ten parametr jest domyślnie wyłączony.

Można wybrać, czy poświadczenia mają być zachowywane dla pojedynczego telefonu, grupy telefonów lub wszystkich telefonów.

### Tematy pokrewne

[Konfigurowanie funkcji telefonu](#), na stronie 147

[Konfiguracja specyficzna dla produktu](#), na stronie 149

## Generowanie kodu QR dla logowania MRA

Użytkownicy, którzy mają telefon z aparatem fotograficznym, mogą zeskanować kod QR w celu zalogowania się do MRA, unikając w ten sposób ręcznego wprowadzania swojej nazwy użytkownika i domeny usługi.

### Procedura

- 
- Krok 1** Za pomocą generatora kodu QR wygeneruj kod QR zawierający domenę usług lub domenę usług i nazwę użytkownika oddzielone przecinkiem. Na przykład: mra.example.com lub mra.example.com,nazwa użytkownika.
- Krok 2** Wydrukuj kod QR i dostarcz go użytkownikowi.
- 

## Narzędzie do zgłaszania problemów

Użytkownicy zgłaszają problemy za pomocą Narzędzia do zgłaszania problemów (PRT).



**Uwaga** Dzienniki tego narzędzia są wymagane przez zespół Cisco TAC do rozwiązywania problemów. Dzienniki są kasowane po ponownym uruchomieniu telefonu. Zarchiwizuj dzienniki przed ponownym uruchomieniem telefonów.

Aby utworzyć zgłoszenie problemu, użytkownicy korzystają z narzędzia PRT oraz podają datę i godzinę wystąpienia problemu i jego opis.

Jeśli przestanie pliku PRT nie powiedzie się, możesz uzyskać dostęp do pliku PRT dla telefonu z adresu URL `http://<phone-ip-address>/FS/<prt-file-name>`. Ten adres URL jest wyświetlany w telefonie w następujących przypadkach:

- Gdy telefon jest w domyślnym stanie fabrycznym. Adres URL pozostaje aktywny przez 1 godzinę. Po 1 godzinie użytkownik powinien ponownie dostarczyć dzienniki telefonu.
- Jeśli telefon pobrał plik konfiguracyjny i system kontroli połączeń zezwala na dostęp WWW do telefonu.

Adres serwera należy dodać w polu **Customer Support Upload URL** (Adres URL do przesyłania plików do pomocy technicznej) w programie Cisco Unified Communications Manager.

Jeśli urządzenia z funkcją Mobile and Remote Access wdrożono przez usługę Expressway, na serwerze Expressway należy dodać adres serwera PRT do listy dozwolonych serwerów HTTP.

## Konfigurowanie adresu URL do przesyłania plików do pomocy technicznej

Do odbierania plików z narzędzia PRT potrzebny jest serwer ze skryptem do przesyłania plików. Narzędzie PRT korzysta z mechanizmu HTTP POST. Przesyłane dane zawierają następujące parametry (zakodowane jako wiadomość wieloczęściowa MIME):

- devicename (nazwa urządzenia, np. "SEP001122334455")
- serialno (nr seryjny, np. "FCH12345ABC")
- username (nazwa użytkownika skonfigurowana w programie Cisco Unified Communications Manager, właściciel urządzenia)
- prt\_file (plik PRT, np. "probrep-20141021-162840.tar.gz")

Poniżej znajduje się przykładowy skrypt. Ten skrypt przedstawiono wyłącznie w celach referencyjnych. Firma Cisco nie świadczy pomocy technicznej dotyczącej skryptu do przesyłania zainstalowanego na serwerze klienta.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, '"\'');

```

```

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "\\");

$username = $_POST['username'];
$username = trim($username, "\\");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}

?>

```



**Uwaga** Telefony obsługują tylko adresy URL HTTP.

### Procedura

- Krok 1** Skonfiguruj serwer, na którym może działać skrypt do przesyłania plików PRT.
  - Krok 2** Napisz skrypt obsługujący wymienione wyżej parametry albo zmodyfikuj przedstawiony tu przykładowy skrypt odpowiednio do potrzeb.
  - Krok 3** Umieść skrypt na serwerze.
  - Krok 4** W programie Cisco Unified Communications Manager przejdź do obszaru Układ konfiguracji specyficznej dla produktu w oknie konfiguracji konkretnego urządzenia, oknie Common Phone Profile (Wspólny profil telefonu) albo oknie Enterprise Phone Configuration (Firmowa konfiguracja telefonów).
  - Krok 5** Kliknij pole **Customer support upload URL** (Adres URL do przesyłania plików do pomocy technicznej) i wprowadź adres URL skryptu na serwerze.
- Przykład:**  
<http://example.com/prtscript.php>
- Krok 6** Zapisz zmiany.

## Konfigurowanie oznaczenia linii

Można skonfigurować w telefonie wyświetlanie etykiety tekstowej zamiast numeru telefonu. Etykieta ta może służyć do identyfikowania linii według jej nazwy lub przeznaczenia. Jeśli np. użytkownik współdzieli linie w telefonie, można identyfikować daną linię po nazwisku osoby, która z niej korzysta.

W przypadku dodania oznaczenia do kluczowego modułu rozszerzeń na linii wyświetlanych jest tylko pierwszych 25 znaków.

**Procedura**

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
  - Krok 2** Odszukaj telefon do skonfigurowania.
  - Krok 3** Odszukaj odpowiednią linię i skonfiguruj pole Etykieta tekstowa linii.
  - Krok 4** (Opcjonalne) Jeśli oznaczenie ma być stosowane do innych urządzeń współdzielących daną linię, zaznacz pole wyboru Aktualizuj współdzielone ustawienia urządzeń i kliknij przycisk **Propaguj wybrane**.
  - Krok 5** Kliknij przycisk **Zapisz**.
- 

## Informacje o konfigurowaniu podwójnego zestawu

Aby skonfigurować informacje o podwójnym zestawie, wykonaj następujące czynności:

**Procedura**

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Domyślne ustawienia urządzenia**.
  - Krok 2** Zapoznaj się z informacjami o ładowaniu w polu Informacje o nieaktywnym ładowaniu.
  - Krok 3** Wybierz kolejno opcje **Administracja zbiorcza > Import/Eksport > Eksportuj > Domyślne ustawienia urządzenia** i zaplanuj zadania eksportu.
  - Krok 4** Pobierz wyeksportowany plik tar i rozpakuj go.
  - Krok 5** Sprawdź format wyeksportowanego pliku CSV i upewnij się, że kolumna Inactive Load Information (Informacje o nieaktywnym obciążeniu) ma prawidłową wartość.
- Uwaga** Wartość w pliku CSV musi odpowiadać wartości „Domyślne ustawienia urządzenia” w oknie aplikacji Cisco Unified Communications Manager — administracja.
- 

## Monitorowanie parkowania

Monitorowanie parkowania jest obsługiwane tylko wtedy, gdy telefon IP Cisco parkuje połączenie. Wtedy funkcja monitorowania parkowania monitoruje stan zaparkowanego połączenia. Dymek połączenia w funkcji monitorowania parkowania znika dopiero wtedy, gdy zaparkowane połączenie zostanie odebrane lub porzucone. Zaparkowane połączenie można odebrać przy użyciu tego samego dymku połączenia w telefonie, który zaparkował połączenie.

## Konfigurowanie zegarów monitorowania parkowania

Aplikacja Cisco Unified Communications Manager — administracja udostępnia trzy parametry dotyczące zegara obowiązujące w klastrze i służące do monitorowania: Zegar cofnięcia monitorowania parkowania, Zegar okresowego przywracania monitorowania parkowania i Zegar przekazywania bez odtwarzania monitorowania parkowania. Każdy parametr usługi ma wartość domyślną i nie wymaga specjalnej konfiguracji.

Te parametry zegara służą wyłącznie do monitorowania parkowania; parametry Zegar wyświetlania parkowania połączeń i Zegar przywracania parkowania połączeń nie są używane do monitorowania parkowania. Opisy tych parametrów można znaleźć w poniższej tabeli.

Zegary można skonfigurować na stronie parametrów usług programu Cisco Unified Communications Manager.

**Procedura**

**Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **System > Parametry usługi**.

**Krok 2** W okienku Parametry klastra (funkcje ogólne) zaktualizuj wartości pól Zegar cofnięcia monitorowania parkowania, Zegar okresowego przywracania monitorowania parkowania i Zegar przekazywania bez odtwarzania monitorowania parkowania.

*Tabela 35: Parametry usługi Monitorowanie parkowania*

Pole	Opis
Zegar cofnięcia monitorowania parkowania	<p>Wartość domyślna: 60 sekund. Ten parametr określa czas (w sekundach), przez który program Cisco Unified Communications Manager czeka, zanim użytkownikowi zostanie wyświetlony monit o zaparkowanym połączeniu, które zaparkował. Zegar rozpoczyna odliczanie, gdy użytkownik naciśnie przycisk na telefonie, a po odliczeniu zadanego czasu generowane jest przypomnienie.</p> <p>W sekcji Monitorowanie parkowania w oknie Konfiguracja numeru telefonu można zastąpić parametr usługi dla poszczególnych linii (w aplikacji Cisco Unified Communications Manager administracja wybierz kolejno opcje <b>Trasowanie połączeń &gt; Numer telefonu</b>). Podaj wartość natychmiast użyć wartości odstępu okresowego cofnięcia określonego przez parametr usługi okresowego cofnięcia monitorowania parkowania. (Zobacz poniższy opis). Jeśli na przykład parametr wynosi zero, zaś wartość parametru Zegar okresowego cofnięcia monitorowania wynosi 15, użytkownik jest informowany o zaparkowanym połączeniu natychmiast, a następnie 15 sekund, aż do wyzerowania wartości Zegara przekazywania bez odtwarzania monitorowania parkowania (zobacz opis poniżej).</p>
Zegar okresowego cofnięcia monitorowania parkowania	<p>Wartość domyślna: 30 sekund. Ten parametr określa liczbę sekund, po upływie których program Cisco Unified Communications Manager informuje ponownie użytkownika o zaparkowanym połączeniu. Aby odebrać zaparkowane połączenie, użytkownik może po prostu podnieść słuchawkę podczas trwania tych monitów. Aplikacja Cisco Unified Communications Manager wyświetla monit o zaparkowanym połączeniu, dopóki połączenie pozostaje zaparkowane i do momentu upłygnięcia czasu wskazanego przez Zegar przekazywania bez odtwarzania monitorowania parkowania (zobacz opis poniżej). Aby wyłączyć okresowe monity dotyczące zaparkowanego połączenia, ustaw wartość 0.</p>

Pole	Opis
Zegar przekazywania bez odtwarzania monitorowania parkowania	Wartość domyślna: 300 sekund. Ten parametr określa liczbę sekund, przez które pojawiają się przypomnienia o zaparkowanym połączeniu, zanim to połączenie nie zostanie przekazane do monitorowania bez odtwarzania monitorowania parkowania określonego oknie Konfiguracja numeru telefonu osoby parkującej. (Jeśli miejsce przekazania nie zostało określone przez aplikację Cisco Communications Manager — administracja, połączenie powraca na linię, na której je zaparkowaliśmy. Ten parametr jest uruchamiany po przekroczeniu limitu czasu określonego w parametrze usługi Zegar monitorowania parkowania. Po wygaśnięciu czasu określonego parametrem Zegar przekazywania bez odtwarzania monitorowania parkowania połączenie jest usuwane z parkowania i przekazywane do miejsca docelowego lub na linię osoby, która je zaparkowała.

## Ustawianie parametrów monitorowania parkowania dla numerów telefonów

W oknie konfiguracji numeru telefonu znajduje się obszar Monitorowanie parkowania, w którym można skonfigurować trzy parametry.

### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Trasowanie połączeń** > **Numer telefonu**.
- Krok 2** Ustaw pola monitorowania parkowania zgodnie z opisem w poniższej tabeli.

*Tabela 36: Parametry monitorowania parkowania*

Pole	Opis
Zewnętrzne miejsce docelowe przekierowywania nieprzejętych połączeń monitorowania parkowania	Gdy strona parkowana jest stroną zewnętrzną, połączenie jest przekierowywane do określonego miejsca docelowego opisanego w parametrze Zewnętrzne miejsce docelowe przekierowywania nieprzejętych połączeń monitorowania parkowania strony parkującej. Jeśli wartość pola Zewnętrzne miejsce docelowe przekierowywania nieprzejętych połączeń jest pusta, strona parkowana jest przekierowywana na linię strony parkującej.
Wewnętrzne miejsce docelowe przekierowywania nieprzejętych połączeń monitorowania parkowania	Gdy strona parkująca jest stroną wewnętrzną, połączenie jest przekierowywane do określonego miejsca docelowego opisanego w parametrze Wewnętrzne miejsce docelowe przekierowywania nieprzejętych połączeń monitorowania parkowania strony parkowanej. Jeśli wartość pola Wewnętrzne miejsce docelowe przekierowywania nieprzejętych połączeń jest pusta, strona parkowana jest przekierowywana na linię strony parkującej.

Pole	Opis
Zegar cofnięcia monitorowania parkowania	Ten parametr określa czas (w sekundach), przez który program Cisco Unified Communications Manager czeka, zanim użytkownikowi zostanie wyświetlony monit o przejęcie połączenia, które zaparkował. Zegar rozpoczyna odliczanie, gdy użytkownik naciśnie przycisk Parkuj na telefonie, a po odliczeniu zadanego czasu generowane jest przypomnienie.  Wartość domyślna: 60 sekund  Jeśli zostanie ustawiona wartość niezerowa, zastąpi ona wartość tego zestawu parametrów w oknie Parametry usługi. Jednak jeśli w tym polu będzie ustawiona wartość 0, zostanie użyta wartość z okna Parametry usługi.

## Konfigurowanie monitorowania parkowania dla list poszukiwania

Po zaparkowaniu połączenia, które zostało przekierowane za pomocą listy poszukiwania, po wygaśnięciu zegara przekazywania bez zwracania monitorowania parkowania jest używany parametr miejsca docelowego przekazywania bez zwracania monitorowania parkowania pilota poszukiwania.

### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz opcję **Trasowanie połączeń > Trasowanie/poszukiwanie > Pilot poszukiwania**.
- Krok 2** Ustaw parametr miejsca docelowego przekazywania bez zwracania monitorowania parkowania pilota poszukiwania.

Jeśli wartość parametru miejsca docelowego przekazywania bez zwracania monitorowania parkowania pilota poszukiwania jest pusta, połączenie jest przekazywane do miejsca docelowego skonfigurowanego w oknie Konfiguracja numeru telefonu po wygaśnięciu zegara przekazywania bez zwracania monitorowania parkowania.

## Konfigurowanie zakresu portów audio i wideo

W celu poprawienia jakości usług (QoS) ruch w połączeniach audio i wideo może być przesyłany przez porty RTP należące do różnych zakresów.

W aplikacji Cisco Unified Communications Manager — administracja następujące pola sterują zakresami portów:

- Porty audio
  - Początkowy port mediów (domyślny: 16384)
  - Końcowy port mediów (domyślny: 32766)
- Porty wideo
  - Uruchom wideo (ustawia początkowy port wideo).

- Minimalnie: 2048
- Maksymalnie: 65535
- Zatrzymaj wideo (ustawia końcowy port wideo)
  - Minimalnie: 2048
  - Maksymalnie: 65535

Podczas konfigurowania pól portów dla połączeń wideo obowiązują następujące reguły:

Po skonfigurowaniu początkowego i końcowego portu RTP wideo w telefonie dla ruchu wideo są używane porty z tego zakresu. Dla ruchu w połączeniach audio używane są porty mediów.

Jeśli zakresy portów audio i wideo nakładają się, porty ze wspólnego zakresu mogą obsługiwać zarówno ruch w połączeniach audio, jak i wideo. Jeśli zakres portów wideo nie jest prawidłowo skonfigurowany, telefon używa dla ruchu w połączeniach audio i wideo portów skonfigurowanych dla ruchu audio.

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Profil SIP**.
- Krok 2** W polach **Początkowy port mediów** i **Końcowy port mediów** ustaw zakres portów audio.
- Krok 3** Kliknij przycisk **Zapisz**.
- Krok 4** Wybierz jedno z następujących okien:
- **System > Firmowa konfiguracja telefonów**
  - **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**
  - **Urządzenie > Telefon > Konfiguracja telefonu**
- Krok 5** W polach **Początkowy port RTP wideo** i **Końcowy port RTP wideo** wybierz wymagany zakres portów. Podczas konfigurowania pól portów dla połączeń wideo obowiązują następujące reguły:
- Wartość w polu **Końcowy port RTP wideo** musi być większa niż wartość w polu **Początkowy port RTP wideo**.
  - Różnica między wartościami pól **Początkowy port RTP wideo** a **Końcowy port RTP wideo** musi wynosić co najmniej 16.
- Krok 6** Kliknij przycisk **Zapisz**.

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii



## Konfigurowanie programu Cisco IP Manager Assistant

Program Cisco IP Manager Assistant (Cisco IPMA) umożliwia przekierowywanie połączeń i udostępnia inne funkcje, które pozwalają menedżerom i asystentom efektywniej obsługiwać połączenia.

Przed rozpoczęciem korzystania z usług IPMA należy je skonfigurować w programie Cisco Unified Communications Manager. Aby uzyskać szczegółowe informacje na temat konfigurowania programu IPMA, zobacz *Podręcznik konfiguracji funkcji programu Cisco Unified Communications Manager*.

Program IPMA składa się z trzech podstawowych składników:

### Menedżer

Menedżer zawiera połączenia przechwycone przez usługę routingu połączenia.

### Asystent

Asystent obsługuje połączenia w imieniu menedżera.

### Assistant Console

Konsola asystenta jest aplikacją, która może być używana przez asystentów do wykonywania zadań i zarządzania większością funkcji.

Program IPMA działa w dwóch trybach: obsługi linii pośredniej i obsługi linii wspólnej. W obu trybach menedżer ma dostęp do wielu połączeń na linii. Usługa IPMA obsługuje zarówno linię pośrednią, jak i linię wspólną w klastrze.

W trybie linii wspólnej menedżer i asystent mają wspólny numer telefonu i połączenia są obsługiwane na linii wspólnej. Oba telefony, menedżera i asystenta, dzwonią po odebraniu połączenia na linii wspólnej. Tryb linii wspólnej nie umożliwia wyboru asystenta domyślnego, nadzoru asystenta, filtrowania połączeń ani funkcji przekierowywania wszystkich połączeń.

W przypadku skonfigurowania Cisco IPMA w trybie współdzielonej linii, menedżer i asystent współdzielą numer katalogowy, na przykład 1701. Asystent obsługuje połączenia dla menedżera na współdzielonym numerze katalogowym. W przypadku nadejścia połączenia dla menedżera na numer 1701, dzwoni zarówno telefon menedżera, jak i telefon asystenta.

W trybie linii wspólnej program Cisco IPMA nie udostępnia wszystkich funkcji, takich jak wybór asystenta domyślnego, nadzór asystenta, filtrowanie połączeń i przekierowywanie wszystkich połączeń. Asystent nie widzi tych funkcji ani nie ma do nich dostępu w aplikacji Assistant Console. Telefon asystenta nie jest wyposażony w klawisz programowy funkcji przekierowywania wszystkich połączeń. Telefon menedżera nie jest wyposażony w klawisze programowe nadzoru asystenta, przechwytywania połączeń ani funkcji przekierowywania wszystkich połączeń.

Aby włączyć obsługę linii wspólnej w urządzeniach użytkownika, należy najpierw użyć programu Cisco Unified Communications Manager — administracja do skonfigurowania i uruchomienia usługi Cisco IP Manager Assistant.

W trybie linii pośredniej asystent obsługuje połączenia w imieniu menedżera, używając numeru pośredniego. W trybie linii pośredniej są obsługiwane wszystkie funkcje programu IPMA.

Po skonfigurowaniu programu Cisco IPMA w trybie linii pośredniej menedżer i asystent nie mają wspólnego numeru telefonu. Asystent obsługuje połączenia w zastępstwie menedżera, używając numeru pośredniego. Numer pośredni nie jest numerem telefonu menedżera. Jest odrębnym numerem wybranym przez system i jest używany przez asystenta do obsługi połączeń menedżera. W trybie linii pośredniej menedżer i asystent mają dostęp do wszystkich funkcji programu Cisco IPMA, w tym do funkcji wyboru asystenta domyślnego, funkcji nadzoru asystenta, funkcji filtrowania połączeń i funkcji przekierowywania wszystkich połączeń.

Aby włączyć obsługę linii pośredniej w urządzeniach użytkownika, należy najpierw użyć programu Cisco Unified Communications Manager — administracja do skonfigurowania i uruchomienia usługi Cisco IP Manager Assistant.

Funkcje programu IPMA są dostępne za pośrednictwem klawiszy programowych i za pośrednictwem usług telefonu. Szablon klawiszy programowych jest skonfigurowany w programie Cisco Unified Communications Manager. Program IPMA obsługuje następujące standardowe szablony klawiszy programowych:

#### Menedżer — standardowy

Obsługuje menedżera w trybie linii pośredniej.

#### Menedżer — standardowy tryb linii wspólnej

Obsługuje menedżera w trybie linii wspólnej.

#### Asystent — standardowy

Obsługuje asystenta w trybie linii wspólnej lub pośredniej.

W poniższej tabeli opisano klawisze programowe dostępne w szablonach klawiszy programowych.

**Tabela 37: Klawisze programowe IPMA**

Klawisz programowy	Stan połączenia	Opis
Przekieruj	Dzwonienie, Nawiązane, Zawieszone	Przekieruj wybrane połączenie do wstępnie skonfigurowanego miejsca docelowego.
Przechwyć	Wszystkie stany	Przekieruj połączenie z telefonu asystenta do telefonu menedżera i odpowiedz automatycznie.
WłNadzrAsyst	Wszystkie stany	Wyświetl stan połączenia obsługiwanego przez asystenta.
Przełącz do poczty głosowej	Dzwonienie, Nawiązane, Zawieszone	Przekieruj wybrane połączenie do poczty głosowej menedżera.
Przekieruj wszystkie	Wszystkie stany	Przekieruj wszystkie połączenia, które są kierowane do menedżera, do wstępnie skonfigurowanego miejsca docelowego.



**Uwaga** Opcje Przechwycen., Wł. nadzór i Przekieruj wszystkie powinny być skonfigurowane tylko na telefonie menedżera w trybie linii pośredniej.

Poniższa procedura zawiera przegląd wymaganych czynności.

#### Procedura

##### Krok 1

Skonfiguruj telefony i użytkowników.

- Krok 2** Skojarz telefony z użytkownikami.
- Krok 3** Uaktywuj usługę Cisco IP Manager Assistant w oknie aktywacji usług.
- Krok 4** Skonfiguruj parametry administracji systemu.
- Krok 5** W razie potrzeby skonfiguruj parametry usługi IPMA dla całego klastra.
- Krok 6** (Opcjonalne) Skonfiguruj profil CAPF użytkownika
- Krok 7** (Opcjonalne) Skonfiguruj parametry usługi IPMA dla zabezpieczeń
- Krok 8** Zatrzymaj i ponownie uruchom usługę IPMA.
- Krok 9** Skonfiguruj parametr telefonu, ustawienia menedżera i asystenta, w tym również szablony klawiszy programowych.
- Krok 10** Skonfiguruj aplikację Cisco Unified Communications Manager Assistant.
- Krok 11** Skonfiguruj reguły wybierania numeru.
- Krok 12** Zainstaluj aplikację konsoli asystenta.
- Krok 13** Skonfiguruj aplikacje konsoli menedżera i asystenta.

## Konfigurowanie wizualnej poczty głosowej

Wizualną pocztę głosową można skonfigurować dla wszystkich telefonów IP Cisco albo dla poszczególnych użytkowników lub grup użytkowników, przy użyciu aplikacji Cisco Unified Communications Manager — administracja.



**Uwaga** Informacje o konfiguracji można znaleźć w dokumentacji wizualnej poczty głosowej firmy Cisco na stronie <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Klient wizualnej poczty głosowej nie jest obsługiwany jako aplikacja typu midlet na żadnym telefonie IP serii Cisco 8800.

### Procedura

- Krok 1** W oknie Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Usługi telefonu**.
- Krok 2** Wybierz opcję **Dodaj nowy**, aby utworzyć nową usługę dla wizualnej poczty głosowej.
- Krok 3** W oknie Konfiguracja usług telefonu IP wprowadź następujące informacje w odpowiednich polach:
- Nazwa usługi — wprowadź **VisualVoiceMail**.
  - Nazwa usługi ASCII — wprowadź **VisualVoiceMail**.
  - Adres URL usługi — wpisz **Application: Cisco/VisualVoiceMail**.
  - Kategoria usługi — z menu rozwijanego wybierz opcję **Usługa XML**.
  - Typ usługi — z menu rozwijanego wybierz **Wiadomości**.
- Krok 4** Zaznacz pole wyboru **Włącz** i kliknij przycisk **Zapisz**.

**Uwaga** Upewnij się, że opcja **Subskrypcja przedsiębiorstwa** nie jest zaznaczona.

- Krok 5** W oknie Informacje o parametrach usługi kliknij opcję **Nowy parametr** i wprowadź w odpowiednich polach następujące informacje:
- Nazwa parametru. Wprowadź voicemail\_server.
  - Nazwa wyświetlana parametru. Wprowadź voicemail\_server.
  - Wartość domyślna. Wprowadź nazwę hosta podstawowego serwera Unity.
  - Opis parametru
- Krok 6** Zaznacz pole wyboru **Parametr jest wymagany** i kliknij przycisk **Zapisz**.
- Uwaga** Upewnij się, że pole wyboru **Parametr jest hasłem (zawartość maski)** nie jest zaznaczone.
- Krok 7** Zamknij okno i ponownie wybierz przycisk **Zapisz** w oknie Konfiguracja usług telefonu.

## Konfigurowanie wizualnej poczty głosowej dla konkretnego użytkownika

Poniższa procedura umożliwia skonfigurowanie wizualnej poczty głosowej dla konkretnego użytkownika.



**Uwaga** Informacje o konfiguracji można znaleźć w dokumentacji wizualnej poczty głosowej firmy Cisco na stronie <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Wybierz urządzenie skojarzone z użytkownikiem, którego szukasz.
- Krok 3** Z listy rozwijanej **Łączy pokrewne** wybierz **Aktywuj/Dezaktywuj usługi** i kliknij przycisk **Idź**.
- Krok 4** Wybierz utworzoną usługę VisualVoiceMail, a następnie wybierz kolejno opcje **Dalej > Subskrybuj**.

## Konfigurowanie wizualnej poczty głosowej dla grupy użytkowników

W celu dodania partii telefonów IP Cisco do aplikacji Cisco Unified Communications Manager z subskrypcją wizualnej poczty głosowej, utwórz szablon telefonu w narzędziu BAT dla każdego typu telefonu i w każdym szablonie telefonu. Następnie możesz zasubskrybować usługę wizualnej poczty głosowej i użyć szablonu, aby wstawić telefony.

Jeśli telefony IP Cisco są już zarejestrowane i chcesz pobrać telefony z subskrypcją usługi wizualnej poczty głosowej, utwórz szablon telefonu w narzędziu BAT, zasubskrybuj usługę wizualnej poczty głosowej w szablonie, a następnie zaktualizuj telefony za pomocą narzędzia BAT.

Aby uzyskać więcej informacji, patrz <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

## Assured Services SIP

Protokół AS-SIP (Assured Services SIP) to zbiór funkcji i protokołów, które oferują dobre zabezpieczenia przepływu połączeń dla telefonów IP Cisco o telefonów innych firm. Następujące funkcje są nazywane zbiorczo AS-SIP:

- Wielopoziomowe pierwszeństwo i zastępowanie (MLPP)
- DSCP (Differentiated Services Code Point)
- TLS (Transport Layer Security) i SRTP (Secure Real-time Transport Protocol)
- Protokół internetowy w wersji 6 (IPv6)

Protokół AS-SIP jest często używany z funkcją wielopoziomowego pierwszeństwa i zastępowania (ang. MLPP, Multilevel Precedence and Preemption) do priorytetyzowania połączeń w sytuacji alarmowej. Usługa MLPP umożliwia przypisywanie poziomu priorytetu do połączeń wychodzących — od poziomu 1 (niski) do poziomu 5 (wysoki). Gdy użytkownik odbiera połączenie, na telefonie wyświetlana jest ikona poziomu pierwszeństwa, która informuje o priorytecie połączenia.

Aby skonfigurować protokół AS-SIP, należy wykonać poniższe czynności w systemie Cisco Unified Communications Manager:

- Konfigurowanie użytkownika digest — Skonfiguruj użytkownika końcowego korzystającego z uwierzytelniania digest dla żądań SIP.
- Konfigurowanie bezpiecznego portu telefonu SIP — System Cisco Unified Communications Manager używa tego portu do nasłuchiwania telefonów SIP w celu rejestracji linii SIP za pośrednictwem protokołu TLS.
- Ponowne uruchomienie usług — Po skonfigurowaniu bezpiecznego portu należy ponownie uruchomić system Cisco Unified Communications Manager i dostawcę usług Cisco CTL. Konfigurowanie profilu SIP dla protokołu AS-SIP — Skonfiguruj profil SIP przy użyciu ustawień SIP dla punktów końcowych AS-SIP i łącza magistralowych SIP. Parametry poszczególnych telefonów nie są pobierane na telefon AS-SIP innej firmy. Są one używane tylko przez program Cisco Unified Manager. Telefony innych firm należy skonfigurować lokalnie przy użyciu takich samych ustawień.
- Konfigurowanie profilu zabezpieczeń telefonu dla protokołu AS-SIP — Profil zabezpieczeń telefonu umożliwia przypisywanie ustawień zabezpieczeń, takich jak TLS, SRTP i uwierzytelnianie digest.
- Konfigurowanie punktu końcowego AS-SIP — Skonfiguruj telefon IP Cisco lub punkt końcowy innej firmy z obsługą protokołu AS-SIP.
- Kojarzenie urządzeń i użytkowników końcowych — Skojarz punkty końcowe z użytkownikami.
- Konfigurowanie profilu zabezpieczeń łącza magistralowego SIP dla protokołu AS-SIP — Profil zabezpieczeń łącza magistralowego SIP umożliwia przypisywanie funkcji zabezpieczeń, takich jak TLS i uwierzytelnianie digest, do łącza magistralowego SIP.
- Konfigurowanie łącza magistralowego SIP dla protokołu AS-SIP — Skonfiguruj łącze magistralowe SIP z obsługą protokołu AS-SIP.
- Konfigurowanie funkcji protokołu AS-SIP — Skonfiguruj dodatkowe funkcje protokołu AS-SIP, takie jak MLPP, TLS, V.150 i IPv6.

Aby uzyskać szczegółowe informacje na temat konfigurowania protokołu AS-SIP, zobacz rozdział „Konfigurowanie punktów końcowych AS-SIP” w *Podręczniku konfiguracji funkcji programu Cisco Unified Communications Manager*.

## Bezpośrednia migracja telefonu do telefonu wieloplatformowego

Telefon korporacyjny można łatwo zmigrować do telefonu wieloplatformowego w jednym kroku, bez konieczności ładowania przejściowego oprogramowania sprzętowego. Wszystko czego potrzebujesz to uzyskanie i autoryzacja licencji migracyjnej z serwera.

Aby uzyskać więcej informacji, patrz [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip\\_b\\_conversion-guide-iphone.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-iphone.html)

## Wielopoziomowe pierwszeństwo i zastępowanie

Funkcja wielopoziomowego pierwszeństwa i zastępowania (MLPP) umożliwia priorytetyzowanie połączeń w sytuacjach awaryjnych lub innych sytuacjach kryzysowych. Do połączeń wychodzących można przypisać priorytet w zakresie od 1 do 5. W przypadku połączeń przychodzących wyświetlana jest ikona wskazująca priorytet połączenia. Uwierzytelnieni użytkownicy mogą zastępować połączenia na docelowych stacjach lub za pośrednictwem magistrali TDM z pełną subskrypcją.

Ta funkcja zapewnia personelowi wyższego szczebla możliwość komunikacji z krytycznymi organizacjami i personelem.

Usługa MLPP jest często używana z protokołem Assured Services SIP (AS-SIP). Aby uzyskać szczegółowe informacje na temat konfigurowania usługi MLPP, zobacz rozdział „Konfigurowanie wielopoziomowego pierwszeństwa i zastępowania (MLPP)” w *Podręczniku konfiguracji funkcji programu Cisco Unified Communications Manager*.

## Konfigurowanie szablonu klawiszy programowych

Za pomocą aplikacji Cisco Unified Communications Manager — administracja można skojarzyć maksymalnie 18 klawiszy programowych z aplikacjami obsługiwanymi przez telefon. Program Cisco Unified Communications Manager obsługuje szablon klawiszy programowych Standard User and Standard Feature (Standardowy użytkownik i standardowe funkcje).

Z każdą aplikacją, która obsługuje klawisze programowe, jest skojarzony co najmniej jeden standardowy szablon klawiszy programowych. Standardowy szablon klawiszy programowych można zmodyfikować poprzez jego skopiowanie, zmianę nazwy, a następnie aktualizację nowego szablonu. Można też modyfikować niestandardowy szablon klawiszy programowych.

Parametr Sterowanie klawiszami programowymi wskazuje, czy klawisze programowe telefonu są kontrolowane przez funkcję Szablon klawiszy programowych. Parametr Sterowanie klawiszami programowymi jest polem wymaganym.

Więcej informacji o konfigurowaniu tej funkcji można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Telefony IP Cisco nie obsługują niektórych klawiszy programowych, które można konfigurować w oknie Konfiguracja szablonu klawiszy programowych w aplikacji Cisco Unified Communications Manager — administracja. Program Cisco Unified Communications Manager umożliwia włączanie lub wyłączenie

niektórych klawiszy programowych w ustawieniach konfiguracyjnych reguł sterowania. W poniższej tabeli zamieszczono listę funkcji i klawiszy programowych, które można konfigurować w szablonie klawiszy programowych, a także wskazano, czy są one obsługiwane przez telefony IP Cisco.



**Uwaga** Program Cisco Unified Communications Manager umożliwia konfigurowanie dowolnego klawisza programowego w szablonie klawiszy programowych, ale nieobsługiwane klawisze programowe nie będą wyświetlane na ekranie telefonu.

**Tabela 38: Konfigurowalne klawisze programowe**

Funkcja	Konfigurowalne klawisze programowe w konfiguracji szablonu klawiszy programowych	Obsługiwane jako klawisz prog
Odbierz	Odbierz (Odbierz)	obsług.
Oddzwoń	Oddzwoń (Oddzwoń)	obsług.
Przekierowywanie wszystkich połączeń	Forward All (Przekierowywanie wszystkich) (cfwdAll)	obsług.
Parkowanie połączenia	Parkowanie połączenia (Park (Parkuj))	obsług.
Przejmowanie połączeń	Przejmowanie (Pickup (Przejmij))	obsług.
Wtrąć	Wtrąć	obsług.
cWtrąć	Conference Barge	obsług.
Połączenie konferencyjne	Konferencja (Konf.)	obsług.
Lista konferencji	Lista konferencji (Listak)	obsług.
Przekieruj	Natychmiastowe przek. (PrzkNat)	obsług.
Nie przeszkadzać	Toggle Do Not Disturb (Przełączanie Nie przeszkadzać) (DND)	obsług.
Rozłączanie	Rozłączanie (EndCall (Rozłącz))	obsług.
Przejmij grupę	Przejmij grupę (PrzGrupę)	obsług.
Zawieszanie	Zawieszanie (Hold (Zawieś))	obsług.
Grupa wyszukiwania	GrWyszuk (HLog (GrWyszuk))	obsług.
Dołącz	Dołącz (Join (Dołącz))	nieobsługiwany

Funkcja	Konfigurowalne klawisze programowe w konfiguracji szablonu klawiszy programowych	Obsługiwane jako klawisz programowy
Identyfikacja połączeń złośliwych (MCID)	Toggle Malicious Call Identification (Przełączanie identyfikacji połączeń złośliwych) (MCID)	obsług.
Meet Me	PokKonf (PokKonf)	obsług.
Mobile Connect	Mobilność (Mobilność)	obsług.
NowePoł	NowePoł (NowePoł)	obsług.
Przejmowanie innych	Przejmowanie innych (oPickup (przejInnych))	obsług.
PLK Support for Queue Statistics (Obsługa PLK dla statystyk kolejki)	Stan kolejki	nieobsługiwany
Raportowanie o jakości	Narzędzie raportowania jakości (QRT)	obsług.
Wybierz ponownie	Ponowne wybieranie (Powtórz)	obsług.
Remove Last Conference Participant (Usuwanie ostatniego uczestnika konferencji)	Remove Last Conference Participant (Usuń ostatniego uczestnika konferencji) (Usuń)	nieobsługiwany
Wznów	Wznów (Wznów)	obsług.
Wybierz	Wybierz (Wybierz)	nieobsługiwany
Szybkie wybieranie	Skrócone wybieranie (AbbrDial (SkrócWyb))	obsług.
Przenoszenie	Przekierowanie (Przek.)	obsług.
Video Mode Command	Video Mode Command (Polecenie trybu wideo) (TrybWid)	nieobsługiwany

## Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz jedno z następujących okien:
- Aby skonfigurować szablony klawiszy programowych, wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Szablon klawiszy programowych**.
  - Aby przypisać szablon klawiszy programowych do telefonu, wybierz kolejno opcje **Urządzenie > Telefon** i ustaw odpowiednią wartość w polu Szablon klawiszy programowych.
- Krok 2** Zapisz zmiany.
-



**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Szablony przycisków telefonu

Dzięki szablonom przycisków telefonu można przypisywać pozycje szybkiego wybierania i funkcje obsługi połączeń do programowalnych przycisków. Funkcje obsługi połączeń, które można przypisywać do przycisków, to: Answer (Odbieranie), Przenoszenie i All Calls (Wszystkie połączenia).

Najlepiej jest zmodyfikować szablony przed zarejestrowaniem telefonów w sieci. Dzięki temu podczas rejestrowania można za pomocą programu Cisco Unified Communications Manager uzyskać dostęp do opcji niestandardowego szablonu przycisków telefonu.

## Modyfikowanie szablonu przycisków telefonu

Więcej informacji na temat usług udostępnianych przez telefon IP i konfigurowania przycisków linii można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

**Procedura**

- 
- Krok 1** W oknie Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Device Settings (Ustawienia urządzenia)** > **Szablon przycisków telefonu**.
  - Krok 2** Kliknij przycisk **Find** (Znajdź).
  - Krok 3** Wybierz model telefonu.
  - Krok 4** Wybierz opcję **Copy** (Kopiuj), wprowadź nazwę nowego szablonu, a następnie wybierz opcję **Zapisz**.  
Pojawi się okno Phone Button Template Configuration (Konfiguracja szablonu przycisków telefonu).
  - Krok 5** Odszukaj przycisk, który chcesz przypisać, i na powiązanej z daną linią liście rozwijanej **Features (Funkcje)** wybierz pozycję **Adres URL usługi**.
  - Krok 6** Wybierz opcję **Zapisz**, aby utworzyć nowy szablon przycisków telefonu, który korzysta z adresu URL usługi.
  - Krok 7** Wybierz kolejno opcje **Urządzenie** > **Telefon** i otwórz okno Konfiguracja telefonu.
  - Krok 8** Na liście rozwijanej Szablon przycisków telefonu wybierz nowy szablon przycisków telefonu.
  - Krok 9** Wybierz opcję **Zapisz**, aby zachować zmiany, a następnie wybierz opcję **Apply Config** (Zastosuj konfigurację), aby zastosować zmiany.

Użytkownik telefonu może teraz uzyskiwać dostęp do usługi Portal Self Care i przypisać ją do jednego z przycisków telefonu.

**Tematy pokrewne**

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Przypisanie szablonu przycisków telefonu dla wszystkich połączeń

W szablonie telefonu przypisz przycisk Wszystk. tym użytkownikom, którzy mają kilka linii wspólnych.

Po skonfigurowaniu przycisku Wszystk. na telefonie, użytkownicy mogą go używać, aby:

- Wyświetlić skonsolidowaną listę bieżących połączeń ze wszystkich linii na telefonie.
- Wyświetlić (w obszarze Historia połączeń) listę wszystkich połączeń nieodebranych ze wszystkich linii na telefonie.
- Nawiązać połączenie na linii głównej użytkownika, gdy użytkownik podniesie słuchawkę. Dla połączeń wychodzących opcja wszystkich połączeń automatycznie dotyczy linii głównej użytkownika.

### Procedura

- 
- Krok 1** Zmodyfikować szablony przycisków telefonu, aby uwzględnić przycisk Wszystk.  
**Krok 2** Przypisać szablony do telefonu.
- 

## Konfigurowanie osobistej książki adresowej lub szybkiego wybierania jako usługi telefonu IP

Adres URL usługi można powiązać z klawiszem programowalnym, modyfikując szablony przycisków telefonu. W ten sposób można umożliwić użytkownikom dostęp za pomocą jednego klawisza do osobistej książki adresowej i szybkiego wybierania. Przed zmodyfikowaniem szablonu przycisków telefonu należy skonfigurować osobistą książkę adresową i szybkie wybieranie jako usługę telefonu IP. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Aby skonfigurować osobistą książkę adresową i szybkie wybieranie jako usługę telefonu IP (jeśli nie zrobiono tego wcześniej), wykonaj następujące czynności:

### Procedura

- 
- Krok 1** W oknie Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Ustawienia urządzenia > Usługi telefonu**.  
 Zostanie wyświetlone okno Find and List IP Phone Services (Znajdowanie i wyświetlanie listy usług telefonu IP).
- Krok 2** Kliknij opcję **Dodaj nową**.  
 Zostanie wyświetlone okno IP Phone Services Configuration (Konfiguracja usług telefonu IP).
- Krok 3** Wprowadź następujące ustawienia:
- Nazwa usługi: wprowadź wartość **Osobista książka adresowa**.
  - Opis usługi: wprowadź opcjonalny opis usługi.
  - Adres URL usługi
- W przypadku osobistej książki adresowej wprowadź następujący adres URL:

**http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

W przypadku szybkiego wybierania wprowadź następujący adres URL:

**http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**

- Bezpieczny adres URL usługi

W przypadku osobistej książki adresowej wprowadź następujący adres URL:

**https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

W przypadku szybkiego wybierania wprowadź następujący adres URL:

**https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**

- Kategoria usługi: wybierz wartość **XML Service** (Usługa XML).
- Typ usługi: wybierz wartość **Directories** (Książki telefoniczne).
- Włącz: zaznacz to pole wyboru.

*http://<IP\_address>* lub *https://<IP\_address>* (W zależności od protokołu obsługiwanego przez telefon IP Cisco).

**Krok 4** Kliknij przycisk **Zapisz**.

**Uwaga** Jeśli zmienisz adres URL usługi, usuniesz parametr usługi telefonu IP lub zmienisz nazwę parametru usługi telefonu, którą subskrybują użytkownicy, musisz kliknąć przycisk **Update Subscriptions** (Aktualizuj subskrypcje), aby zastosować zmiany dla wszystkich aktualnie subskrybujących użytkowników. Jeśli tego nie zrobisz, użytkownicy będą musieli ponownie zasubskrybować usługę, aby ponownie uzyskać poprawny adres URL.

#### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Modyfikowanie szablonu przycisków telefonu dla osobistej książki adresowej lub szybkiego wybierania

Adres URL usługi można powiązać z klawiszem programowalnym, modyfikując szablon przycisków telefonu. W ten sposób można umożliwić użytkownikom dostęp za pomocą jednego klawisza do osobistej książki adresowej i szybkiego wybierania. Przed zmodyfikowaniem szablonu przycisków telefonu należy skonfigurować osobistą książkę adresową i szybkie wybieranie jako usługę telefonu IP.

Więcej informacji na temat usług udostępnianych przez telefon IP i konfigurowania przycisków linii można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

#### Procedura

**Krok 1** W oknie Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Device Settings (Ustawienia urządzenia) > Szablon przycisków telefonu**.

**Krok 2** Kliknij przycisk **Find** (Znajdź).

- Krok 3** Wybierz model telefonu.
- Krok 4** Wybierz opcję **Copy** (Kopiuj), wprowadź nazwę nowego szablonu, a następnie wybierz opcję **Zapisz**.  
Pojawi się okno Phone Button Template Configuration (Konfiguracja szablonu przycisków telefonu).
- Krok 5** Odszukaj przycisk, który chcesz przypisać, i na powiązanej z daną linią liście rozwijanej Features (Funkcje) wybierz pozycję **Adres URL usługi**.
- Krok 6** Wybierz opcję **Zapisz**, aby utworzyć nowy szablon przycisków telefonu, który korzysta z adresu URL usługi.
- Krok 7** Wybierz kolejno opcje **Urządzenie > Telefon** i otwórz okno Konfiguracja telefonu.
- Krok 8** Na liście rozwijanej Szablon przycisków telefonu wybierz nowy szablon przycisków telefonu.
- Krok 9** Wybierz opcję **Zapisz**, aby zachować zmiany, a następnie wybierz opcję **Apply Config** (Zastosuj konfigurację), aby zastosować zmiany.
- Użytkownik telefonu może teraz uzyskiwać dostęp do usługi Portal Self Care i przypisać ją do jednego z przycisków telefonu.

---

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Konfiguracja sieci VPN

Funkcja Cisco VPN pomoże zachować bezpieczeństwo sieci, jednocześnie umożliwiając użytkownikom bezpieczną i niezawodną metodę nawiązywania połączenia z siecią korporacyjną. Używaj tej funkcji, kiedy:

- Telefon znajduje się poza siecią zaufaną
- Ruch sieciowy między telefonem a programem Cisco Unified Communications Manager przechodzi przez sieć niezaufaną

W ramach sieci VPN dostępne są trzy ogólnie przyjęte sposoby uwierzytelniania klientów:

- Certyfikaty cyfrowe
- Hasła
- Nazwa użytkownika i hasło

Każda metoda ma swoje zalety. Jeśli jednak firmowe zasady zabezpieczeń na to pozwalają, zalecamy używanie podejścia opartego o certyfikaty, ponieważ ich użyciu umożliwia jednolite logowania bez interwencji użytkownika. Obsługiwane są certyfikaty typów LSC i MIC.

Aby skonfigurować dowolną funkcję sieci VPN, należy najpierw skonfigurować urządzenia w siedzibie firmy, a dopiero potem skonfigurować urządzenie poza firmą.

Aby uzyskać więcej informacji na temat uwierzytelniania przy pomocy certyfikacji i pracy w sieci VPN, zapoznaj się z uwagą techniczną *AnyConnect VPN Phone with Certificate Authentication on an ASA Configuration Example* (Telefon w sieci AnyConnect VPN uwierzytelniany przy pomocy certyfikatów w przykładowej konfiguracji ASA). Dokument ten znajduje się pod następującym adresem URL:  
<http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>

Gdy stosowane jest hasło lub nazwa użytkownika i hasło, użytkownik jest proszony o podanie poświadczeń logowania. Ustaw poświadczenia logowania zgodnie z zasadami zabezpieczeń firmy. Również ustawienie **Włącz trwałość hasła** można skonfigurować tak, aby hasło użytkownika zostało zapisane w telefonie. Hasło użytkownika jest zapisywane aż do próby logowania zakończonej niepowodzeniem, ręcznego usunięcia hasła przez użytkownika lub do zresetowania telefonu lub utraty przez niego zasilania.

Innym przydatnym narzędziem jest ustawienie **Włącz automatyczne wykrywanie sieci**. Gdy to pole wyboru jest zaznaczone, klient sieci VPN może zostać uruchomiony tylko po wykryciu, że znajduje się poza siecią korporacyjną. To ustawienie jest domyślnie wyłączone.

Telefon Cisco obsługuje typ klienta Cisco SVC IP Phone Client w wersji 1.0.

Aby uzyskać dodatkowe informacje na temat konserwacji, konfigurowania i obsługi prywatnej sieci wirtualnej w ramach sieci VPN, zobacz podręcznik *Security Guide for Cisco Unified Communications Manager* (Podręcznik zabezpieczeń programu Cisco Unified Communications Manager), rozdział „Konfiguracja wirtualnej sieci prywatnej”. Dokument ten znajduje się pod następującym adresem URL:

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

Funkcja Cisco VPN używa protokołu SSL (Secure Sockets Layer) do zapewnienia bezpieczeństwa sieci.



**Uwaga** Podczas konfigurowania telefonu poza siedzibą firmy dla protokołu SSL VPN dla serwera ASA przy użyciu wbudowanego klienta, należy wprowadzić ustawienie alternatywnego serwera TFTP.

## Konfigurowanie klawiszy linii dodatkowej

Włącz tryb rozszerzony linii, aby korzystać z przycisków po obu stronach wyświetlacza telefonu jako klawiszy linii. W trybie rozszerzonym linii domyślnie włączone są funkcje przewidywania wybieranego numeru oraz realizowanych alertów połączeń przychodzących.

### Zanim rozpocznie

Należy utworzyć nowy, dostosowany szablon przycisków telefonu.

### Procedura

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Odszukaj telefon, który chcesz skonfigurować.
- Krok 3** Przejdź do obszaru Konfiguracja specyficzna dla produktu i w polu **Tryb linii** wybierz opcję **Tryb rozszerzony linii**.
- Krok 4** Przejdź do obszaru informacji o urządzeniu i w polu **Szablon przycisków telefonu** wybierz szablon dostosowany.
- Krok 5** Kliknij przycisk **Apply Config** (Zastosuj konfigurację).
- Krok 6** Kliknij przycisk **Zapisz**.
- Krok 7** Uruchom ponownie telefon.

**Tematy pokrewne**

[Środowisko trybu linii sesji](#), na stronie 172

**Funkcje dostępne w trybie rozszerzonym linii**

Trybu rozszerzonego linii (ELM) można używać wraz z usługą Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.

Tryb ELM może być również używany z linią przewijania w konfiguracji z trasowaniem połączeń, w której połączenia są przekazywane do innej linii wspólnej, jeśli początkowa linia wspólna jest zajęta. Gdy tryb ELM jest używany z linią przewijania, ostatnie połączenia z liniami wspólnymi są konsolidowane w ramach jednego numeru telefonu. Więcej informacji na temat linii przewijania można znaleźć w *Podręczniku konfiguracji funkcji systemu Cisco Unified Communications Manager* dla systemu Cisco Unified Communications Manager w wersji 12.0(1) lub nowszej.

W trybie ELM obsługiwana jest większość funkcji, ale nie wszystkie. Włączenie funkcji nie oznacza jej dostępności. Zapoznaj się z poniższą tabelą, aby potwierdzić, że funkcja jest obsługiwana.

**Tabela 39: Obsługa funkcji w trybie rozszerzonym linii**

<b>Funkcja</b>	<b>obsług.</b>	<b>Wersja oprogramowania sprzętowego</b>
Odbierz	Tak	11.5(1) i nowsze
Automatyczne odbieranie połączeń	Tak	11.5(1) i nowsze
Wtrąć/WtrąćKon	Tak	11.5(1) i nowsze
Parkowanie połączenia kierowanego przy użyciu funkcji SZL	Tak	12.0(1) i nowsze
Integracja Bluetooth Smartphone	Nie	-
Zestawy słuchawkowe Bluetooth USB	Tak	11.5(1) i nowsze
Oddzwon	Tak	11.5(1) i nowsze
Nadzorca połączenia	Nie	-
Przekierowywanie wszystkich połączeń	Tak	11.5(1) i nowsze
Parkowanie połączenia	Tak	12.0(1) i nowsze
Stan linii Parkowanie połączenia	Tak	12.0(1) i nowsze
Przejmowanie połączeń	Tak	11.5(1) i nowsze
Stan linii Przejęcie połączenia	Tak	11.5(1) i nowsze

<b>Funkcja</b>	<b>obsług.</b>	<b>Wersja oprogramowania sprzętowego</b>
Przekierowywanie wszystkich połączeń na wiele linii	Tak	11.5(1) i nowsze
Klaster krzyżowy przenośnego numeru wewnętrznego Cisco	Tak	Ta funkcja jest obsługiwana w wersji 12.0(1) i nowszych.
Cisco IP Manager Assistant (IPMA)	Nie	-
Cisco Unified Communications Manager Express	Nie	-
Połączenie konferencyjne	Tak	11.5(1) i nowsze
Aplikacje CTI (Computer Telephony Integration)	Tak	11.5(1) i nowsze
Odrzuć	Tak	11.5(1) i nowsze
Nagrywanie wywoływane przez urządzenie	Tak	11.5(1)SR1 i nowsze
Nie przeszkadzać	Tak	11.5(1) i nowsze
Rozszerzone SRST	Nie	-
Przenośny numer wewnętrzny	Tak	11.5(1) i nowsze
Przejmij grupę	Tak	Ta funkcja jest obsługiwana w wersji 12.0(1) i nowszych.
Zawieszanie	Tak	11.5(1) i nowsze
Grupy wyszukiwania	Tak.	12.0(1) i nowsze
Powiadomienie o nadchodzącym połączeniu z konfigurowanym zegarem	Nie	-
Interkom	Tak	11.5(1) i nowsze
Moduł rozszerzający przyciski	Tryb rozszerzony linii jest obsługiwany przez moduł rozszerzeń klawiatury do telefonów IP Cisco 8851/8861 oraz moduł rozszerzeń klawiatury do telefonu IP Cisco 8865	12.0(1) i nowsze
Identyfikacja połączeń złośliwych (Malicious Call Identification, MCID)	Tak	11.5(1) i nowsze

Funkcja	obsług.	Wersja oprogramowania sprzętowego
Meet Me	Tak	11.5(1) i nowsze
Mobile Connect	Tak	11.5(1) i nowsze
Wielopoziomowe pierwszeństwo i zastępowanie	Nie	-
Wyciszenie	Tak	11.5(1) i nowsze
Przejmij inne	Tak	12.0(1) i nowsze
Obsługa PLK (Programmable Line Key) dla stanu kolejki	Tak	11.5(1) i nowsze
Prywatność	Tak	11.5(1) i nowsze
Stan kolejki	Tak	11.5(1) i nowsze
Narzędzie raportowania jakości (QRT)	Tak	11.5(1) i nowsze
Obsługa ustawień regionalnych dla języków wprowadzanych od prawej do lewej	Nie	-
Wybierz ponownie	Tak	11.5(1) i nowsze
Bezobsługowe monitorowanie i nagrywanie	Tak	11.5(1)SR1 i nowsze
Szybkie wybieranie	Tak	11.5(1) i nowsze
SRST (Survivable Remote Site Telephony)	Tak	11.5(1) i nowsze
Przenoszenie	Tak	11.5(1) i nowsze
Wybieranie URI (Uniform Resource Identifier)	Tak	11.5(1) i nowsze
Połączenia wideo	Tak	11.5(1) i nowsze
Wizualna poczta głosowa	Tak	11.5(1) i nowsze
Poczta głosowa	Tak	11.5(1) i nowsze

**Tematy pokrewne**

[Środowisko trybu linii sesji](#), na stronie 172



## Konfigurowanie zegara wznowienia TLS

Funkcja wznowienia sesji TLS umożliwia wznowienie pracy sesji TLS bez powtarzania całego procesu uwierzytelniania TLS. Skraca to istotnie czas połączenia TLS w celu wymiany danych.

Telefony obsługują sesje TLS, ale nie wszystkie sesje TLS obsługują funkcję wznowienia TLS. Następująca lista zawiera opis różnych sesji i obsługi wznowienia TLS:

- Sesje TLS dla sygnalizacji SIP: obsługuje wznowienie
- Klient HTTPS: obsługuje wznowienie
- CAPF: obsługuje wznowienie
- TVS: obsługuje wznowienie
- EAP-TLS: nie obsługuje wznowienia
- EAP-FAST: nie obsługuje wznowienia
- Klient VPN: nie obsługuje wznowienia

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie > Telefon**.
- Krok 2** Ustaw parametr Zegar podjęcia TLS.  
Zakres timera wynosi od 0 do 3600 sekund. Domyślną wartością jest 3600. Jeśli pole jest ustawione na 0, wznowianie sesji TLS jest wyłączone.

---

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Włączenie funkcji Intelligent Proximity



**Uwaga** Ta procedura dotyczy tylko telefonów z funkcją Bluetooth. Telefony IP Cisco 8811, 8841, 8851NR i 8865NR nie obsługują funkcji Bluetooth.

Funkcja Intelligent Proximity umożliwia użytkownikom wykorzystanie w urządzeniu przenośnym lub w tablecie akustycznych właściwości telefonu. Użytkownik paruje urządzenie przenośne lub tablet z telefonem za pomocą protokołu Bluetooth.

Po sparowaniu urządzenia przenośnego użytkownik może nawiązywać i odbierać połączenia komórkowe przy użyciu telefonu. Korzystając z tabletu, użytkownik może przekierowywać dźwięk z tabletu na telefon.

Użytkownicy mogą sparować z telefonem wiele urządzeń przenośnych, tabletów, a także zestaw słuchawkowy Bluetooth. Jednak jednocześnie może być podłączone tylko jedno urządzenie i jeden zestaw słuchawkowy.

### Procedura

- 
- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Telefon > Urządzenie**.
- Krok 2** Zlokalizuj telefon, który chcesz zmodyfikować.
- Krok 3** Znajdź odpowiednie pole Bluetooth i ustaw wartość pola **Włączone**.
- Krok 4** Znajdź pole Zezwól na głosnomówiący tryb telefonu komórkowego Bluetooth i ustaw wartość pola **Włączone**.
- Krok 5** Zapisz zmiany, a następnie zastosuj je w telefonie.
- 

## Ustawianie rozdzielczości transmisji wideo

Telefony IP Cisco 8845, 8865 i 8865NR obsługują następujące formaty wideo:

- 720p (1280 x 720)
- WVGA (800x480)
- 360p (640 x 360)
- 240p (432 x 240)
- VGA (640 x 480)
- CIF (352 x 288)
- SIF (352 x 240)
- QCIF (176 x 144)

Telefony IP Cisco obsługujące wideo negocjują najlepszą rozdzielczość dla danego pasma, biorąc pod uwagę konfigurację telefonu i ograniczenia rozdzielczości. Przykład: Przy bezpośrednim połączeniu pomiędzy telefonami 88x5 nie będzie używany format 720p, zamiast niego będzie wysyłany obraz 800 x 480. To ograniczenie wynika wyłącznie z rozdzielczości 5-calowego ekranu WVGA telefonu 88x5 wynoszącej 800 x 480.

Typ wideo	Rozdzielczość grafiki	Ramki na sekundę (k/s)	Zakres szybkości bitowej transmisji wideo
720p	1280 x 720	30	1360-2500 Kb/s
720p	1280 x 720	15	790-1359 Kb/s
WVGA	800 x 480	30	660-789 Kb/s

Typ wideo	Rozdzielczość grafiki	Ramki na sekundę (k/s)	Zakres szybkości bitowej transmisji wideo
WVGA	800 x 480	15	350-399 Kb/s
360p	640 x 360	30	400-659 Kb/s
360p	640 x 360	15	210-349 Kb/s
240p	432 x 240	30	180-209 Kb/s
240p	432 x 240	15	64-179 Kb/s
VGA	640 x 480	30	520-1500 Kb/s
VGA	640 x 480	15	280-519 Kb/s
CIF	352 x 288	30	200-279 Kb/s
CIF	352 x 288	15	120-199 Kb/s
SIF	352 x 240	30	200-279 Kb/s
SIF	352 x 240	15	120-199 Kb/s
QCIF	176 x 144	30	94-119 Kb/s
QCIF	176 x 144	15	64-93 Kb/s

## Parametry zarządzania zestawem nagłownym w starszych wersjach programu Cisco Unified Communications Manager

Jeśli użytkownik ma wersję programu Cisco Unified Communications Manager starszą niż 12.5(1)SU1, może zdalnie skonfigurować ustawienia zestawu nagłownego Cisco do używania z telefonami lokalnymi.

Konfiguracja zdalnego zestawu nagłownego w programie Cisco Unified Communication Manager w wersji 10.5 (2), 11.0 (1), 11.5 (1), 12.0 (1) i 12.5 (1) wymaga pobrania pliku z [Witryny pobierania oprogramowania firmy Cisco](#), edycji pliku i wysłania pliku na serwerze TFTP systemu Cisco Unified Communications Manager. Plik jest plikiem JSON (JavaScript Object Notification). Zaktualizowana konfiguracja zestawu nagłownego jest stosowana we wszystkich zestawach nagłownych w przedsiębiorstwie w czasie od 10 do 30 minut po przesłaniu, aby zapobiec zaległościom ruchu sieciowego w usłudze TFTP programu.



**Uwaga** Można zarządzać zestawami nagłownymi za pośrednictwem programu Cisco Unified Communications Manager — Administracja w wersji 11.5(1)SU7.

Podczas pracy z plikiem JSON należy pamiętać o następujących kwestiach:

- Ustawienia nie zostaną zastosowane, jeśli w kodzie brakuje nawiasu lub nawiasów. Należy sprawdzić format pliku przy użyciu narzędzia online, na przykład JSON Formatter.

- Wartością ustawienia **updatedTime** musi być czas bieżącej epoki. W przeciwnym razie konfiguracja nie zostanie zastosowana. Alternatywnie można zwiększyć wartość **updatedTime** o 1, aby była większa niż w poprzedniej wersji.
- Nie zmieniaj nazw parametrów. W przeciwnym razie ustawienia nie będą stosowane.

Więcej informacji o usłudze TFTP znajduje się w rozdziale „Manage Device Firmware” (Zarządzanie oprogramowaniem sprzętowym urządzeń) *Podręcznika administratora systemu Cisco Unified Communications Manager oraz usługi IM i systemu obecności.*

Przed zastosowaniem pliku `defaultheadsetconfig.json` należy zaktualizować oprogramowanie sprzętowe telefonów do najnowszej wersji. W poniższej tabeli opisano ustawienia domyślne, które można dostosować przy użyciu pliku JSON.

## Pobieranie domyślnego pliku konfiguracyjnego zestawu nagłownego

Przed przystąpieniem do zdalnego konfigurowania parametrów zestawu nagłownego należy pobrać najnowszy przykładowy plik notacji JSON (ang. JavaScript)

### Procedura

- 
- Krok 1** Przejdź do następującego adresu URL: <https://software.cisco.com/download/home/286320550>
  - Krok 2** Wybierz **Zestawy nagłowne Cisco z serii 500**.
  - Krok 3** Wybierz serię zestawów nagłownych.
  - Krok 4** Wybierz folder publikacji i wybierz plik zip.
  - Krok 5** Kliknij przycisk **Pobierz** lub **Dodaj do koszyka**, a następnie postępuj zgodnie z monitami.
  - Krok 6** Rozpakuj plik do folderu w komputerze.
- 

### Co dalej

[Modyfikowanie domyślnego pliku konfiguracyjnego zestawu nagłownego, na stronie 218](#)

## Modyfikowanie domyślnego pliku konfiguracyjnego zestawu nagłownego

Podczas pracy z plikiem JSON należy pamiętać, że:

- Ustawienia nie zostaną zastosowane, jeśli w kodzie brakuje nawiasu lub nawiasów. Należy sprawdzić format pliku przy użyciu narzędzia online, na przykład JSON Formatter.
- Wartością ustawienia „**updatedTime**” musi być czas bieżącej epoki. W przeciwnym razie konfiguracja nie zostanie zastosowana.
- Upewnij się, że dla opcji **firmwareName** wybrano ustawienie `LATEST`. W przeciwnym razie konfiguracja nie zostanie zastosowana.
- Nie zmieniaj nazw parametrów. W przeciwnym razie ustawienia nie będą stosowane.

## Procedura

**Krok 1** Otwórz plik `defaultheadsetconfig.json` za pomocą edytora tekstów.

**Krok 2** Zmodyfikuj wartość **updatedTime** i wartości odpowiednich parametrów zestawu nagłownego.

Poniżej znajduje się przykładowy skrypt. Ten skrypt przedstawiono wyłącznie w celach referencyjnych. Użyj tego jako pomocy w konfiguracji ustawień zestawu nagłownego. Użyj pliku JSON dołączonego do oprogramowania sprzętowego.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
                  "value": 7
                },
                {
                  "name": "Microphone Gain",
                  "access": "Both",
                  "usageId": 33,
                  "value": 2
                },
                {
                  "name": "Sidetone",
                  "access": "Both",
                  "usageId": 34,
                  "value": 1
                },
                {
                  "name": "Equalizer",
                  "access": "Both",
                  "usageId": 35,
                  "value": 3
                }
              ]
            }
          ]
        }
      ]
    },
    {
      "modelSeries": "560",
```



```
}  
}
```

**Krok 3** Zapisz `defaultheadsetconfig.json`.

---

#### Co dalej

Zainstaluj domyślny plik konfiguracyjny

## Instalowanie domyślnego pliku konfiguracyjnego w programie Cisco Unified Communications Manager

Po zmodyfikowaniu pliku `defaultheadsetconfig.json` należy go zainstalować w programie Cisco Unified Communications Manager przy użyciu narzędzia do zarządzania plikami TFTP.

#### Procedura

---

- Krok 1** W narzędziu administrowanie systemem Cisco Unified OS wybierz kolejno opcje **Uaktualnianie oprogramowania** > **Zarządzanie plikiem TFTP**.
  - Krok 2** Wybierz opcję **Wyślij plik**.
  - Krok 3** Wybierz opcję **Wybierz plik** i przejdź do pliku `defaultheadsetconfig.json`.
  - Krok 4** Wybierz opcję **Wyślij plik**.
  - Krok 5** Kliknij opcję **Zamknij**.
- 

## Ponowne uruchamianie serwera Cisco TFTP

Po wysłaniu pliku `defaultheadsetconfig.json` do katalogu TFTP uruchom ponownie serwer TFTP Cisco i zresetuj telefony. Po około 10 – 15 minutach rozpocznie się proces pobierania i zostaną zastosowane nowe konfiguracje zestawów nagłownych. Zastosowanie ustawień trwa od 10 do 30 minut.

#### Procedura

---

- Krok 1** Zaloguj się do usługi Cisco Unified Serviceability — następnie wybierz **Narzędzia** > **Centrum zarządzania** — **Włączone usługi**.
  - Krok 2** W polu listy rozwijanej **Serwer** wybierz serwer, na którym działa usługa Cisco TFTP.
  - Krok 3** Kliknij przycisk opcji odpowiadający usłudze **Cisco TFTP**.
  - Krok 4** Kliknij przycisk **Uruchom ponownie**.
-







## ROZDZIAŁ 10

# Firmowa książka telefoniczna i osobista książka telefoniczna

- [Konfigurowanie firmowej książki telefonicznej, na stronie 223](#)
- [Konfigurowanie osobistej książki adresowej, na stronie 223](#)
- [Konfigurowanie wpisów w osobistej książce adresowej użytkownika, na stronie 224](#)

## Konfigurowanie firmowej książki telefonicznej

Firmowa książka telefoniczna umożliwia użytkownikowi wyszukiwanie numerów telefonów współpracowników. Do obsługi tej funkcji niezbędne jest skonfigurowanie firmowych książek telefonicznych.

Cisco Unified Communications Manager używa katalogu Lightweight Directory Access Protocol (LDAP) do przechowywania informacji o uwierzytelnianiu i autoryzacji użytkowników Cisco Unified Communications Manager aplikacji, które łączą się z Cisco Unified Communications Manager. Uwierzytelnianie służy do ustalania uprawnień użytkowników do dostępu do systemu. Autoryzacja wskazuje natomiast zasoby telefoniczne, z których może korzystać dany użytkownik, np. określony numer wewnętrzny.

Telefony IP Cisco używają przydzielania dynamicznego dla rozwiązania SecureApp na klientach i serwerach. Umożliwia to odczytywanie certyfikatów o rozmiarze większym niż 4KB przez telefon i zmniejsza częstotliwość występowania komunikatów o błędach `Nie znaleziono hosta`, gdy użytkownik uzyskuje dostęp do książki adresowej.

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Po zakończeniu konfigurowania katalogu LDAP użytkownicy mogą korzystać w swoich telefonach z usługi Firmowa książka telefoniczna w celu wyszukiwania użytkowników w firmowej książce telefonicznej.

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Konfigurowanie osobistej książki adresowej

Osobista książka adresowa umożliwia użytkownikowi przechowywanie zestawu osobistych numerów telefonów.

Osobista książka adresowa ma następujące funkcje:

- Osobista książka adresowa (PAB)
- klawisze szybkiego wybierania
- Narzędzie synchronizacji książki adresowej (TABSynch)

Aby uzyskać dostęp do funkcji książki adresowej, użytkownicy mogą używać następujących metod:

- Przy użyciu przeglądarki WWW — użytkownicy mają dostęp do osobistej książki adresowej i funkcji szybkiego wybierania z Portalu samoobsługowego Cisco Unified Communications.
- Z telefonu IP Cisco — wybierz opcję **Kontakty**, aby wyszukiwać w firmowej lub osobistej książce adresowej.
- Z aplikacji dla systemu Microsoft Windows — użytkownicy mogą używać narzędzia TABSynch do synchronizowania swoich prywatnych książek adresowych z książką adresową systemu Windows (Microsoft Windows Address Book, WAB). Klienci, którzy chcą korzystać z książki adresowej programu Microsoft Outlook (OAB), powinni rozpocząć od zaimportowania danych z OAB do WAB. Do synchronizacji książki WAB z osobistą książką adresową można użyć narzędzia TabSync. Instrukcje dotyczące korzystania z narzędzia TABSync można znaleźć w sekcji [Pobieranie dodatku Cisco IP Phone Address Book Synchronizer, na stronie 225](#) i [Konfigurowanie dodatku Synchronizer, na stronie 226](#).

Telefony IP Cisco używają przydzielania dynamicznego dla rozwiązania SecureApp na klientach i serwerach. Umożliwia to odczytywanie certyfikatów o rozmiarze większym niż 4KB przez telefon i zmniejsza częstotliwość występowania komunikatów o błędach *Nie znaleziono hosta*, gdy użytkownik uzyskuje dostęp do książki adresowej.

Aby zapewnić, że użytkownicy dodatku Cisco IP Phone Address Book Synchronizer mają dostęp wyłącznie do własnych danych użytkowników końcowych, aktywuj usługę Cisco UXL Web Service w usłudze serwisowania systemu Cisco Unified.

Aby skonfigurować osobistą książkę adresową w przeglądarce WWW, użytkownicy muszą mieć dostęp do Portalu samoobsługowego. Należy podać użytkownikom adres URL i dane logowania.

## Konfigurowanie wpisów w osobistej książce adresowej użytkownika

Użytkownicy mogą konfigurować wpisy w osobistych książkach adresowych na swoich telefonach IP Cisco. Aby móc skonfigurować osobistą książkę adresową, użytkownicy muszą mieć dostęp do następujących źródeł:

- Portal samoobsługowy: upewnij się, że użytkownicy wiedzą, jak uzyskać dostęp do tego portalu. Więcej informacji zawiera sekcja [Konfigurowanie dostępu użytkownika do portalu Self Care, na stronie 84](#).
- Dodatek Cisco IP Phone Address Book Synchronizer: upewnij się, że użytkownicy mają program instalacyjny. Zobacz [Pobieranie dodatku Cisco IP Phone Address Book Synchronizer, na stronie 225](#).



**Uwaga** Dodatek Cisco IP Phone Address Book Synchronizer jest obsługiwany wyłącznie w nieobsługiwanych wersjach systemu Windows (na przykład Windows XP i wcześniejszych). To narzędzie nie jest obsługiwane w nowszych wersjach systemu Windows. W przyszłości zostanie usunięta z listy wtyczek programu Cisco Unified Communications Manager.

## Pobieranie dodatku Cisco IP Phone Address Book Synchronizer

Aby pobrać kopię tego dodatku w celu wysłania go swoim użytkownikom:

### Procedura

- Krok 1** Aby pobrać instalator, w aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Aplikacja > Plugins (Dodatki)**.
- Krok 2** Wybierz opcję **Pobierz**, która znajduje się obok nazwy dodatku Cisco IP Phone Address Book Synchronizer.
- Krok 3** Po pojawieniu się okna dialogowego pobierania pliku wybierz opcję **Zapisz**.
- Krok 4** Wyślij plik TabSyncInstall.exe i instrukcje podane w części [Zastosowanie dodatku Cisco IP Phone Address Book Synchronizer, na stronie 225](#) do wszystkich użytkowników, którzy potrzebują tego dodatku.

## Zastosowanie dodatku Cisco IP Phone Address Book Synchronizer

Dodatek Cisco IP Phone Address Book Synchronizer synchronizuje dane przechowywane w książce adresowej systemu Microsoft Windows z katalogiem programu Cisco Unified Communications Manager i osobistą książką adresową Portalu samoobsługowego.



**Wskazówka** Aby zsynchronizować książkę adresową systemu Windows z osobistą książką adresową, wszyscy użytkownicy książki adresowej systemu Windows powinni zostać wprowadzeni do tej książki przed wykonaniem opisanych dalej procedur.

## Instalowanie synchronizatora

Aby zainstalować Dodatek Cisco IP Phone Address Book Synchronizer, wykonaj następujące czynności:

### Procedura

- Krok 1** Uzyskaj plik instalatora dodatku Cisco IP Phone Address Book Synchronizer od administratora systemu.
- Krok 2** Kliknij dwukrotnie plik TabSyncInstall.exe otrzymany od administratora.
- Krok 3** Kliknij przycisk **Uruchom**.
- Krok 4** Wybierz **Next (Następny)**.

- Krok 5** Prze czytaj informacje o umowie licencyjnej i wybierz opcję **I Accept** (Zgadzam się). Wybierz **Next** (Następny).
- Krok 6** Wybierz katalog, w którym chcesz zainstalować aplikację, i kliknij przycisk **Dalej**.
- Krok 7** Kliknij przycisk **Zainstaluj**.
- Krok 8** Kliknij przycisk **Zakończ**.
- Krok 9** Aby dokończyć proces instalacji, wykonaj czynności opisane w artykule [Konfigurowanie dodatku Synchronizer, na stronie 226](#).

## Konfigurowanie dodatku Synchronizer

Aby skonfigurować dodatek Cisco IP Phone Address Book Synchronizer:

### Procedura

- Krok 1** Uruchom dodatek Cisco IP Phone Address Book Synchronizer.  
Jeśli został zaakceptowany domyślny katalog instalacyjny, dodatek ten można uruchomić, wybierając kolejno pozycje **Start > Wszystkie programy > Cisco Systems > TabSync**.
- Krok 2** Aby skonfigurować informacje o użytkowniku, wybierz opcję **Użytkownik**.
- Krok 3** Wprowadź nazwę i hasło użytkownika telefonu IP Cisco, a następnie kliknij przycisk **OK**.
- Krok 4** Aby skonfigurować informacje o serwerze Cisco Unified Communications Manager, wybierz opcję **Serwer**.
- Krok 5** Wprowadź adres IP lub nazwę hosta i numer portu serwera Cisco Unified Communications Manager i kliknij przycisk **OK**.  
Jeśli nie posiadasz tych informacji, skontaktuj się z administratorem systemu.
- Krok 6** Aby rozpocząć proces synchronizowania książki adresowej, wybierz opcję **Synchronizuj**.  
W oknie Synchronization Status (Stan synchronizacji) podawany jest stan synchronizowania książki adresowej. Jeśli w przypadku reguł zduplikowanych pozycji wybrana zostanie interwencja użytkownika, a w książce adresowej znajdują się zduplikowane pozycje, wyświetlone zostanie okno Duplicate Selection.
- Krok 7** Wybierz pozycję, którą chcesz dodać do swojej osobistej książki adresowej, i kliknij przycisk **OK**.
- Krok 8** Po zakończeniu synchronizowania wybierz opcję **Wyjdź**, aby zamknąć dodatek Cisco Unified CallManager Address Book Synchronizer.
- Krok 9** Aby sprawdzić, czy synchronizacja się powiodła, zaloguj się do portalu Self Care i wybierz opcję **Osobista książka adresowa**. Powinni się w niej znajdować użytkownicy z Twojej książki adresowej systemu Windows.



## CZĘŚĆ **IV**

### **Rozwiązywanie problemów z telefonem IP Cisco**

- [Monitorowanie systemów telefonicznych, na stronie 229](#)
- [Rozwiązywanie problemów, na stronie 267](#)
- [Konservacja, na stronie 287](#)
- [Obsługa użytkowników międzynarodowych, na stronie 293](#)





# ROZDZIAŁ 11

## Monitorowanie systemów telefonicznych

- [Stan telefonu IP Cisco, na stronie 229](#)
- [Strona WWW telefonu IP Cisco, na stronie 246](#)
- [Żądanie informacji z telefonu w formacie XML, na stronie 263](#)

### Stan telefonu IP Cisco

W tej sekcji opisano, jak wyświetlić informacje o modelu, komunikaty o stanie i statystyki sieci na telefonie IPCisco z serii 8800.

- Informacje o modelu: informacje o sprzęcie i oprogramowaniu telefonu.
- Menu stanu: daje dostęp do ekranów z komunikatami o stanie, statystykami sieci i statystykami bieżącego połączenia.

Informacje wyświetlane na tych ekranach umożliwiają monitorowanie działania telefonu i pomagają w rozwiązywaniu problemów.


Wiele z tych oraz inne powiązane informacje są dostępne zdalnie na stronie WWW telefonu.

Aby uzyskać więcej informacji o rozwiązywaniu problemów, zobacz [Rozwiązywanie problemów, na stronie 267](#).

### Wyświetlanie okna Informacje o telefonie

Aby wyświetlić ekran Informacje o modelu, wykonaj następujące czynności:

#### Procedura

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

**Krok 2** Wybierz opcję **Informacje o telefonie**.

Jeśli użytkownik ma połączenie z zabezpieczonym lub uwierzytelnionym serwerem, odpowiednia ikona (z kłódką lub z certyfikatem) pojawi się na ekranie Informacje o telefonie po prawej stronie opcji serwera. Jeśli użytkownik nie ma połączenia z zabezpieczonym lub uwierzytelnionym serwerem, nie pojawia się żadna ikona.

**Krok 3** Aby opuścić ekran Informacje o modelu, naciśnij przycisk **Wyjdź**.

## Pola w oknie Informacje o telefonie

W poniższej tabeli opisano ustawienia informacji o telefonie.

**Tabela 40: Ustawienia w oknie Informacji o telefonie**

Opcja	Opis
Numer modelu	Numer modelu telefonu.
Adres IPv4	Adres IP telefonu.
Nazwa hosta	Nazwa hosta telefonu.
Aktywna wersja	Wersja oprogramowania sprzętowego zainstalowanego na telefonie. Użytkownik może nacisnąć przycisk <b>Szczegóły</b> , aby uzyskać więcej informacji.
Wersja nieaktywna	<p>Bieżąca wersja jest nieaktywna tylko wtedy, gdy pobieranie jest w toku. Ikona pobierania i stan "Aktualizacja w toku" lub "Aktualizacja nie powiodła się" są również wyświetlane. Gdy w trakcie uaktualniania użytkownik naciśnie przycisk <b>Szczegóły</b>, zostaną wyświetlone nazwy pobieranego pliku oraz składników.</p> <p>Można zaplanować pobranie nowego obrazu oprogramowania sprzętowego wcześniej niż podczas zaplanowanej konserwacji. Dzięki temu zamiast oczekiwać na pobranie oprogramowania sprzętowego przez wszystkie telefony, można natychmiast zresetować istniejącą wersję do stanu nieaktywnego i zainstalować nową wersję.</p> <p>Po zakończeniu pobierania ikona zmienia się i wskazuje stan zakończenia; pomyślne pobranie jest oznaczone znacznikiem wyboru, a niepomyślne znakiem "X". Jeśli to możliwe, pozostałe pliki wersji są nadal pobierane.</p>
Ostatnia aktualizacja	Data najnowszej aktualizacji oprogramowania sprzętowego.
Serwer aktywny	Nazwa domeny serwera, na którym jest zarejestrowany telefon.
Serwer rezerwowy	Nazwa domeny serwera rezerwowego.

## Wyświetlanie menu Stan

Menu Stan zawiera następujące opcje, które dostarczają informacji o telefonie i operacjach telefonu:


- Komunikaty o stanie: wyświetla ekran Komunikaty o stanie, na którym przedstawiana jest lista ważnych komunikatów systemowych.



- Statystyki sieci Ethernet: wyświetla ekran Statystyki sieci Ethernet, na którym przedstawiane są statystyki ruchu w sieci Ethernet.
- Statystyki sieci bezprzewodowej: wyświetla ekran Statystyki sieci bezprzewodowej, jeśli ma to zastosowanie.
- Statystyki połączeń: wyświetla liczniki i statystyki dotyczące bieżącego połączenia.
- Bieżący punktu dostępu: wyświetla ekran Bieżący punkt dostępu, jeśli ma to zastosowanie.

Aby wyświetlić menu Stan, wykonaj następujące kroki:


#### Procedura

- 
- Krok 1** Aby wyświetlić menu Stan, naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Stan**.
- Krok 3** Aby wyjść z menu Stan, naciśnij przycisk **Wyjdź**.
- 

## Wyświetlanie okna komunikatów o stanie

Okno Komunikaty o stanie: jest tu wyświetlanych 30 najnowszych komunikatów o stanie, które telefon wygenerował od czasu ostatniego uruchomienia. Ten ekran jest dostępny w dowolnym momencie, nawet jeśli telefon nie zakończył uruchamiania.

#### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia administracyjne** > **Stan** > **Status messages (Komunikaty o stanie)**.
- Krok 3** Aby usunąć bieżące komunikaty o stanie, naciśnij przycisk **Wyczyść**.
- Krok 4** Aby opuścić ekran komunikatów o stanie, naciśnij przycisk **Wyjdź**.
- 

### Pola komunikatów o stanie

W poniższej tabeli opisano komunikaty o stanie wyświetlane na telefonie na ekranie Komunikaty o stanie.

**Tabela 41: Komunikaty o stanie w telefonie IP Cisco Unified**

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Błąd rozmiaru CFG TFTP	Plik konfiguracyjny jest zbyt duży dla systemu plików w telefonie.	Wyłącz telefon i włącz go ponownie.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Błąd sumy kontrolnej	Pobrany plik oprogramowania jest uszkodzony.	Uzyskaj nową kopię oprogramowania i umieść ją w katalogu TFTPPath. Dodaj do tego katalogu tylko wtedy, gdy zakończysz komunikację z serwerem TFTP. W przeciwnym razie pliki mogą zostać nadpisane.
Nie można uzyskać adresu IP z serwera DHCP	Telefon nie uzyskał poprzednio adresu IP z serwera DHCP. Może się to zdarzyć po zresetowaniu telefonu do ustawień domyślnych lub fabrycznych.	Sprawdź, czy serwer DHCP działa dla telefonu.
Zainstalowano pliki CTL i ITL	Pliki CTL i ITL są zainstalowane w telefonie.	Żadna. Ten komunikat ma charakter informacyjny. Wcześniej nie zainstalowano pliku ITL.
Zainstalowano CTL	W telefonie jest zainstalowany plik listy zaufanych certyfikatów (CTL).	Żadna. Ten komunikat ma charakter informacyjny. Wcześniej nie zainstalowano pliku CTL.
Niepowodzenie aktualizacji CTL	W telefonie nie można zaktualizować pliku listy zaufanych certyfikatów (CTL).	Wystąpił problem z plikiem CTL.
Limit czasu DHCP	Serwer DHCP nie odpowiedział.	Sieć jest zajęta: błędy powinny zmniejszyć obciążenia sieci. Brak połączenia sieciowego pomiędzy telefonem: sprawdź połączenia sieciowe. Serwer DHCP jest wyłączony: sprawdź konfigurację serwera DHCP. Nadal występują błędy: rozważ zmianę adresu IP.
Limit czasu DNS	Serwer DNS nie odpowiedział.	Sieć jest zajęta: błędy powinny zmniejszyć obciążenia sieci. Brak połączenia sieciowego pomiędzy telefonem: sprawdź połączenia sieciowe. Serwer DNS jest wyłączony: sprawdź konfigurację DNS.
DNS — nieznanym hostem	Serwer DNS nie może rozpoznać nazwy serwera TFTP lub systemu Cisco Unified Communications Manager.	Sprawdź, czy nazwy hosta serwera TFTP i Cisco Unified Communications Manager są skonfigurowane w ustawieniach serwera. Rozważ użycie adresów IP zamiast nazw hostów.
Powtórzony adres IP	Inne urządzenie korzysta z adresu IP przypisanego do telefonu.	Jeśli telefon ma statyczny adres IP, sprawdź, czy przydzielony duplikat adresu IP. Jeśli używasz protokołu DHCP, sprawdź konfigurację serwera DHCP.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Czyszczenie plików CTL i ITL	Czyszczenie pliku CTL lub ITL.	Żadna. Ten komunikat ma charakter informacyjny.
Błąd aktualizacji ustawień regionalnych	W katalogu TFTPPath nie znaleziono co najmniej jednego pliku lokalizacyjnego lub plik był nieprawidłowy. Nie zmieniono ustawień regionalnych.	<p>W narzędziu Cisco Unified Operations Administration sprawdź, czy następujące pliki znajdują się w podkatalogach systemu zarządzania:</p> <ul style="list-style-type: none"> <li>• Znajduje się w podkatalogu ustawienie regionalne sieci <ul style="list-style-type: none"> <li>• tones.xml</li> </ul> </li> <li>• Znajduje się w podkatalogu ustawienie regionalne używane <ul style="list-style-type: none"> <li>• glyphs.xml</li> <li>• dictionary.xml</li> <li>• kate.xml</li> </ul> </li> </ul>
Nie znaleziono pliku <Cfg File>	Na serwerze TFTP nie znaleziono pliku konfiguracyjnego o podanej nazwie ani pliku domyślnego.	<p>Plik konfiguracyjny telefonu jest dodawany do bazy danych programu Cisco Unified Communications Manager. Jeśli nie ma danych programu Cisco Unified Communications Manager, serwer TFTP tworzy odpowiedni plik konfiguracyjny. (Nie znaleziono pliku konfiguracyjnego)</p> <ul style="list-style-type: none"> <li>• Telefon nie jest zarejestrowany w systemie Cisco Unified Communications Manager</li> </ul> <p>Jeśli nie zezwolono na aktualizację danych telefonu, należy dodać go do bazy danych programu Cisco Unified Communications Manager. Więcej informacji zawiera <a href="#">rozdział 73, Telefonów, na stronie 73</a>.</p> <ul style="list-style-type: none"> <li>• Jeśli używasz protokołu DHCP, DHCP wskazuje na prawidłową konfigurację serwera TFTP</li> <li>• Jeśli używasz statycznych adresów IP, sprawdź konfigurację serwera TFTP</li> </ul>
Nie znaleziono pliku <CTLFile.tlv>	Ten komunikat jest wyświetlany na telefonie, gdy klaster Cisco Unified Communications Manager nie znajduje się w trybie bezpiecznym.	Nie ma to znaczenia; telefon może być w trybie bezpiecznym w systemie Cisco Unified Communications Manager.
Adres IP zwolniony	Telefon jest skonfigurowany do zwolnienia adresu IP.	Telefon pozostaje bezczynny aż do dostarczenia zasilania lub do zresetowania adresu IP.
Zainstalowano plik ITL	Plik ITL jest zainstalowany w telefonie.	Żadna. Ten komunikat ma charakter informacyjny. Wcześniej nie zainstalowano pliku ITL.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Nie można załadować kodu	Pobrana aplikacja nie jest zgodna ze sprzętem telefonu.	Taka sytuacja występuje podczas instalacji wersji oprogramowania na telefonie po zmianach sprzętowych telefonu.  Zaznacz identyfikator obciążenia pakietu (w programie Cisco Unified Communications Manager wybierz kolejno opcje <b>Urządzenie</b> i <b>Wprowadź obciążenie</b> wyświetlany
Brak routera domyślnego	Protokół DHCP lub konfiguracja statyczna nie określają routera domyślnego.	Jeśli telefon posiada statyczny adres domyślny router jest skonfigurowany.  Jeśli używasz protokołu DHCP, serwer udostępnia domyślnego routera. Sprawdź adres serwera DHCP.
Brak adresu IP serwera DNS	Podano nazwę, ale protokół DHCP lub statycznie skonfigurowany adres IP nie określił adresu serwera DNS.	Jeśli telefon posiada statyczny adres DNS jest skonfigurowany.  Jeśli używasz protokołu DHCP, serwer udostępnia serwera DNS. Sprawdź adres serwera DHCP.
Nie zainstalowano listy zaufanych certyfikatów	Plik CTL lub plik ITL nie jest zainstalowany w telefonie.	Lista zaufanych nie jest skonfigurowana w Cisco Unified Communications Manager, który obsługuje zabezpieczeń.
Telefon nie zarejestrował się. Rozmiar klucza certyfikatu jest niezgodny z protokołem FIPS.	Protokół FIPS wymaga, aby długość certyfikatu serwera RSA wynosiła co najmniej 2048 bitów.	Zaktualizuj certyfikat.
System Cisco Unified Communications Manager zażądał ponownego uruchomienia	Telefon jest ponownie uruchamiany w wyniku żądania systemu Cisco Unified Communications Manager.	Prawdopodobnie zmieniono konfigurację systemu Cisco Unified Communications Manager. Naciśnięto przycisk Zastosuj, co spowodowało zmianę.
Błąd dostępu protokołu TFTP	TFTP wskazuje nieistniejący katalog.	Jeśli używasz protokołu DHCP, serwer wskazuje na prawidłowy serwer TFTP.  Jeśli używasz statycznych adresów IP, sprawdź konfigurację serwera TFTP.
Błąd protokołu TFTP	Telefon nie rozpoznaje kodu błędu przekazanego przez serwer TFTP.	Skontaktuj się z Cisco TAC.
Limit czasu TFTP	Serwer TFTP nie odpowiedział.	Sieć jest zajęta: błędy powinny zmniejszyć obciążenia sieci.  Brak połączenia sieciowego pomiędzy telefonem: sprawdź połączenia sieciowe.  Serwer TFTP jest wyłączony: sprawdź konfigurację TFTP.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Przekroczono limit czasu	Suplikant próbował przeprowadzić transakcję 802.1X, ale upłynął limit czasu z powodu braku wystawcy uwierzytelnienia.	Uwierzytelnianie przekracza li wówczas, gdy na przełączniku protokół 802.1X.
Aktualizacja listy zaufanych certyfikatów nie powiodła się	Aktualizacja plików CTL i ITL zakończyła się niepowodzeniem.	Na telefonie były zainstalowane udało się ich zaktualizować.  Prawdopodobna przyczyna nie <ul style="list-style-type: none"> <li>• Wystąpiła awaria sieci.</li> <li>• Serwer TFTP był wyłączony.</li> <li>• Wprowadzono nowy token podpisywania pliku CTL był używany do podpisywa one dostępne w aktualnym telefonie.</li> <li>• Wystąpiła wewnętrzna aw</li> </ul> Możliwe rozwiązania: <ul style="list-style-type: none"> <li>• Sprawdź łączność w siec</li> <li>• Sprawdź, czy serwer TFTP poprawnie.</li> <li>• Jeśli serwer TVS (Transac jest obsługiwany w system Communications Manage jest aktywny i czy pracuje</li> <li>• Sprawdź poprawność tok TFTP.</li> </ul> Jeśli poprzednie czynności nie usuń pliki CTL i ITL, po czym
Lista zaufanych certyfikatów została zaktualizowana	Plik CTL, plik ITL, lub oba te pliki zostały uaktualnione.	Żadna. Ten komunikat ma char informacyjny.
Błąd wersji	Nazwa obciążenia telefonu jest nieprawidłowa.	Upewnij się, że plik obciążeni nazwę.
XmlDefault.cnf.xml lub .cnf.xml — odpowiednio do nazwy urządzenia telefonicznego	Nazwa pliku konfiguracyjnego.	Żadna. Ten komunikat wskazu konfiguracyjnego telefonu.

**Tematy pokrewne**


[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

**Wyświetlanie ekranu informacji o sieci**

Wiadomości wyświetlane na ekranie Network Info (Informacje o sieci) przydają się do rozwiązywania w telefonie problemów z połączeniami.

Gdy użytkownik ma problem z nawiązaniem połączenia z siecią telefoniczną, na ekranie telefonu pojawia się odpowiedni komunikat.

### Procedura


- 
- Krok 1** Aby wyświetlić menu Stan, naciśnij przycisk **Aplikacje** .
  - Krok 2** Wybierz kolejno opcje **Ustawienia administracyjne > Stan > Status messages (Komunikaty o stanie)**.
  - Krok 3** Wybierz opcję **Network Info**.
  - Krok 4** Aby opuścić ekran Network Info, naciśnij przycisk **Wyjdź**.
- 

## Wyświetlanie ekranu Statystyki sieci

Na ekranie Statystyki sieci są wyświetlane informacje o działaniu telefonu i sieci.

Aby wyświetlić ekran Statystyki sieci, wykonaj następujące czynności:

### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
  - Krok 2** Wybierz kolejno opcje **Ustawienia admin.>Stan>Statystyki sieci**.
  - Krok 3** Aby wyzerować statystyki w polach Rx Frames (Odebrane ramki), Wysł. ramki i Odb. emisja, naciśnij przycisk **Wyczyść**.
  - Krok 4** Aby opuścić ekran statystyk sieci Ethernet, naciśnij przycisk **Wyjdź**.
- 

## Informacje o statystykach sieci Ethernet

W poniższej tabeli opisano informacje widoczne na ekranie Statystyki sieci Ethernet.

*Tabela 42: Informacje o statystykach sieci Ethernet*

Element	Opis
Wysł. ramki	Liczba pakietów odebranych przez telefon.
Wysł. ramki	Liczba pakietów wysłanych przez telefon.
Odb. emisja	Liczba odebranych przez telefon pakietów rozgłoszeniowych.

Element	Opis
Przyczyna restartu	Przyczyna ostatniego zresetowania telefonu. Jedna z następujących wartości: <ul style="list-style-type: none"> <li>• Zainicjowany</li> <li>• TCP-timeout</li> <li>• CM-closed-TCP</li> <li>• TCP-Bad-ACK</li> <li>• CM-reset-TCP</li> <li>• CM-aborted-TCP</li> <li>• CM-NAKed</li> <li>• KeepaliveTO</li> <li>• Failback</li> <li>• Phone-Keypad</li> <li>• Phone-Re-IP</li> <li>• Reset-Reset</li> <li>• Reset-Restart</li> <li>• Phone-Reg-Rej</li> <li>• Nie można załadować kodu</li> <li>• CM-ICMP-Unreach</li> <li>• Telefon-przerwij</li> </ul>
Czas, który upłynął	Czas, jaki upłynął od ostatniego ponownego uruchomienia telefonu.
Port 1	Stan łącza i typ połączenia portu sieciowego. Na przykład <b>Auto 100 Mb pełny duplex</b> oznacza, że port sieciowy ma aktywne łącze i automatycznie wynegocjował połączenie pełnodupleksowe 100 Mb/s.
Port 2	Stan łącza i typ połączenia portu komputera
Stan protokołu DHCP (IPv4 lub IPv6)	<ul style="list-style-type: none"> <li>• W trybie Tylko IPv4 jest wyświetlany tylko stan DHCPv4, taki jak DHCP BOUND.</li> <li>• W trybie IPv6 jest wyświetlany tylko stan DHCPv6, taki jak ROUTER ADVERTISE.</li> <li>• Wyświetlane są informacje o stanie DHCPv6.</li> </ul>

W poniższych tabelach opisano komunikaty o stanie wyświetlane dla wersji DHCPv4 i DHCPv6.

**Tabela 43: Komunikaty o statystykach sieci Ethernet — DHCPv4**

Stan DHCPv4	Opis
CDP INIT	Protokół CDP nie jest powiązany lub WLAN nie działa
DHCP BOUND	DHCPv4 jest w stanie BOUND
DHCP DISABLED	DHCPv4 jest wyłączony

Stan DHCPv4	Opis
DHCP INIT	DHCPv4 jest w stanie INIT
DHCP INVALID	DHCPv4 jest w stanie INVALID; jest to stan początkowy
DHCP RENEWING	DHCPv4 jest w stanie RENEWING
DHCP REBINDING	DHCPv4 jest w stanie REBINDING
DHCP REBOOT	DHCPv4 inicjuje ponowne uruchomienie
DHCP REQUESTING	DHCPv4 wysyła żądanie
DHCP RESYNC	DHCPv4 jest w stanie RESYNCH
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 jest uruchamiany
DHCP UNRECOGNIZED	Nierozpoznany stan DHCPv4
DISABLED DUPLICATE IP	Powtórzony adres IPv4
DHCP TIMEOUT	DHCPv4 upłynął limit czasu
IPV4 STACK TURNED OFF	Telefon jest w trybie pracy protokołu IPv6, stos protokołu IPv4 jest wyłączony
ILLEGAL IPV4 STATE	Nieprawidłowy stan IPv4, który nie powinien się zdarzyć

Tabela 44: Komunikaty o statystykach sieci Ethernet — DHCPv6

Stan DHCPv6	Opis
CDP INIT	Trwa inicjowanie CDP
DHCP6 BOUND	DHCPv6 jest w stanie BOUND
DHCP6 DISABLED	DHCPv6 jest w stanie DISABLED
DHCP6 RENEW	DHCPv6 jest w stanie RENEWING
DHCP6 REBIND	DHCPv6 jest w stanie REBINDING
DHCP6 INIT	DHCPv6 jest w stanie INITIALIZING
DHCP6 SOLICIT	DHCPv6 jest w stanie SOLICITING
DHCP6 REQUEST	DHCPv6 jest w stanie REQUESTING
DHCP6 RELEASING	DHCPv6 jest w stanie RELEASING
DHCP6 RELEASED	DHCPv6 jest w stanie RELEASED
DHCP6 DISABLING	DHCPv6 jest w stanie DISABLING




Stan DHCPv6	Opis
DHCP6 DECLINING	DHCPv6 jest w stanie DECLINING
DHCP6 DECLINED	DHCPv6 jest w stanie DECLINED
DHCP6 INFOREQ	DHCPv6 jest w stanie INFOREQ
DHCP6 INFOREQ DONE	DHCPv6 jest w stanie INFOREQ DONE
DHCP6 INVALID	DHCPv6 jest w stanie INVALID; jest to stan początkowy
DISABLED DUPLICATE IPV6	DHCP6 jest w stanie DISABLED, ale wykryto zduplikowany adres IPV6
DHCP6 DECLINED DUPLICATE IP	DHCP6 jest w stanie DECLINED — wykryto zduplikowany adres IPV6
ROUTER ADVERTISE., (DUPLICATE IP)	Zduplikowany skonfigurowany automatycznie adres IPv6
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 jest uruchamiany
DHCP6 TIMEOUT USING RESTORED VAL	Limit czasu DHCPv6; zostanie użyta wartość zapisana w pamięci flash
DHCP6 TIMEOUT CANNOT RESTORE	Limit czasu DHCPv6; w pamięci flash brak kopii zapasowej
IPV6 STACK TURNED OFF	Telefon jest w trybie pracy protokołu IPv4, stos protokołu IPv6 jest wyłączony
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	Adres IPv6 nie pochodzi od routera ani serwera DHCPv6
ILLEGAL IPV6 STATE	Nieprawidłowy stan IPv6, który nie powinien się zdarzyć

## Wyświetlanie ekranu Statystyki sieci bezprzewodowej

Ta procedura dotyczy tylko telefonu IP Cisco 8861.

Aby wyświetlić ekran Statystyki sieci bezprzewodowej, wykonaj następujące czynności:

### Procedura

- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Stan** > **Statystyki sieci bezprzewodowej**.

**Krok 3** Aby wyzerować statystyki sieci bezprzewodowej, naciśnij przycisk **Wyczyść**.

**Krok 4** Aby opuścić ekran Statystyki sieci bezprzewodowej, naciśnij przycisk **Wyjdź**.

## Statystyki sieci WLAN

W poniższej tabeli opisano statystyki sieci WLAN wyświetlane w telefonie.

**Tabela 45: Statystyki sieci WLAN w telefonie IP Cisco Unified**

Element	Opis
Bajty wysłane	Liczba bajtów wysłanych przez telefon.
Bajty odebrane	Liczba bajtów odebranych przez telefon.
Pakiety wysłane	Liczba pakietów wysłanych przez telefon.
Pakiety odebrane	Liczba pakietów odebranych przez telefon.
Porzucone pakiety wysłane	Liczba pakietów porzuconych w trakcie wysyłania.
Porzucone pakiety odebrane	Liczba pakietów porzuconych w trakcie odbierania.
Błędy pakietów wysłanych	Liczba błędnych pakietów wysłanych przez telefon.
Błędy pakietów odebranych	Liczba błędnych pakietów odebranych przez telefon.
Ramki wysłane	Liczba pomyślnie wysłanych jednostek MSDU.
Wysłane ramki multimijsji	Liczba pomyślnie wysłanych jednostek MSDU multimijsji.
Ponowna próba wysłania	Liczba jednostek MSDU pomyślnie wysłanych po jednej lub większej liczbie prób ponownego wysyłania.
Wiele prób wysłania	Liczba jednostek MSDU multimijsji pomyślnie wysłanych po jednej lub większej liczbie prób ponownego wysyłania.
Błąd pakietu TX	Jest to liczba jednostek MSDU, które nie zostały wysłane pomyślnie z powodu przekroczenia limitu dozwolonej liczby prób ponownego wysyłania.
RTS — powodzenie	Wartość tego licznika zwiększa się po odebraniu sygnału CTS w odpowiedzi na sygnał RTS.
Błąd pakietu RTS	Wartość tego licznika zwiększa się, jeśli w odpowiedzi na sygnał RTS nie zostanie odebrany sygnał CTS.
ACK - niepowodzenie	Wartość tego licznika zwiększa się, gdy potwierdzenie nie zostanie odebrane w oczekiwanym momencie.
Wysłane duplikaty ramek	Numer odebranej ramki, która w polu Sequence Control (Kontrola kolejności) została wskazana jako duplikat.

Element	Opis
Pofragmentowane wysłane pakiety	Liczba pomyślnie odebranych jednostek MPDU o typie Dane lub Zarządzanie.
Licznik roamingu	Liczba pomyślnie nawiązanych połączeń z sieciami obcymi (roamingowych).

## Wyświetlanie okna Statystyki połączeń


Na ekranie Statystyki połączeń w telefonie można wyświetlać liczniki, statystyki i dane o jakości dźwięku dotyczące ostatniego połączenia.



**Uwaga** Informacje o statystykach połączeń można też wyświetlać zdalnie za pomocą przeglądarki WWW, przechodząc na stronę WWW o nazwie Statystyki strumieniowania. Znajdują się na niej dodatkowe dane statystyczne, które są niedostępne w telefonie.

Pojedyncze połączenie może korzystać z wielu strumieni transmisji głosowej, ale gromadzone dane dotyczą tylko ostatniego z nich. Strumień transmisji głosowej to strumień pakietów przesyłanych między dwoma punktami końcowymi. Jeśli jeden punkt końcowy zostanie wstrzymany, następuje przerwanie strumienia transmisji głosowej, mimo że połączenie trwa nadal. Po wznowieniu połączenia zaczyna płynąć nowy strumień pakietów transmisji głosowej, a nowe dane o połączeniu zastępują stare.

### Procedura

- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Stan** > **Statystyki połączeń**.
- Krok 3** Aby opuścić ekran statystyk połączeń, naciśnij przycisk **Wyjdź**.

### Pola na ekranie Statystyki połączeń

W poniższej tabeli opisano elementy widoczne na ekranie Statystyki połączeń.

Tabela 46: Elementy na ekranie Statystyki połączeń telefonu Cisco Unified


Element	Opis
Kodek odbiornika	<p>Typ odbieranego strumienia dźwiękowego (dźwięk przesyłany jako strumień RTP z kodeka):</p> <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G722.2 AMR-WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC</li> <li>• Opus</li> <li>• iSAC</li> </ul>
Kodek nadajnika	<p>Typ wysyłanego strumienia dźwiękowego (dźwięk przesyłany jako strumień RTP z kodeka):</p> <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G722.2 AMR-WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC.</li> <li>• Opus</li> <li>• iSAC</li> </ul>
Rozmiar po stronie odbiorcy	Rozmiar w milisekundach pakietów dźwiękowych odbieranego strumienia (dźwięk przesyłany jako strumień RTP).
Rozmiar po stronie nadawcy	Rozmiar w milisekundach pakietów dźwiękowych wysyłanego strumienia.
Pakiety odbiornika	<p>Liczba pakietów dźwiękowych RTP odebranych od momentu otwarcia strumienia.</p> <p><b>Uwaga</b> Ta liczba nie musi być identyczna z liczbą pakietów dźwiękowych RTP odebranych od momentu rozpoczęcia połączenia, ponieważ połączenie mogło być wstrzymane.</p>

Element	Opis
Liczba nadanych pakietów	Liczba pakietów dźwiękowych RTP wysłanych od momentu otwarcia strumienia.  <b>Uwaga</b> Ta liczba nie musi być identyczna z liczbą pakietów dźwiękowych RTP wysłanych od momentu rozpoczęcia połączenia, ponieważ połączenie mogło być wstrzymane.
Średni jitter	Szacowane średnie wahania opóźnień pakietów RTP (dynamiczne opóźnienie występujące podczas przesyłania pakietu przez sieć) w milisekundach zaobserwowane od momentu otwarcia odbiorczego strumienia dźwiękowego.
Maks. jitter	Maksymalne wahania opóźnień w milisekundach zaobserwowane od momentu otwarcia odbiorczego strumienia dźwiękowego.
Odbiornik odrzucony	Liczba pakietów RTP w odbiorczym strumieniu dźwiękowym, które zostały odrzucone (z powodu uszkodzenia pakietu, zbytniego opóźnienia itd.).  <b>Uwaga</b> Telefon odrzuca pakiety z ładunkiem typu 19 (comfort noise) generowane przez bramy Cisco, ponieważ zwiększają one ten licznik.
Utracone pakiety odbiornika	Brakujące pakiety RTP (utracone po drodze).
<b>Metryki jakości dźwięku</b>	
Współczynnik ukrywania kumulatywnego	Łączna liczba ramek ukrywania podzielona przez łączną liczbę ramek transmisji głosowej odebranych od początku strumienia transmisji głosowej.
Współczynnik ukrywania w interwale	Stosunek liczby ramek ukrywania do liczby ramek transmisji głosowej w poprzedzającym 3-sekundowym interwale trwającej rozmowy. Jeśli używana jest funkcja wykrywania aktywności transmisji głosowej (VAD), może być wymagany dłuższy interwał w celu zebrania trzech sekund aktywnej transmisji głosowej.
Maks. współczynnik ukrywania	Najwyższy współczynnik ukrywania w interwale od początku strumienia transmisji głosowej.
Ukrywanie (s)	Liczba sekund, w których występowały zdarzenia ukrywania (utracone ramki), od początku strumienia transmisji głosowej (obejmuje sekundy z intensywnym ukrywaniem).
Intensywne ukrywanie (s)	Liczba sekund, w których zdarzenia ukrywania (utracone ramki) obejmowały ponad 5%, od początku strumienia transmisji głosowej.
Opóźnienie	Oszacowanie opóźnienia sieci wyrażonego w milisekundach. Stanowi określane na bieżąco średnie opóźnienie przesyłania danych w obie strony, mierzone w trakcie odbierania bloków raportu odbiornika RTCP.

## Wyświetlanie okna Bieżący punkt dostępu

Na ekranie bieżącego punktu dostępu są wyświetlane statystyki danego punktu dostępu, który jest używany przez telefon IP Cisco 8861 do komunikacji bezprzewodowej.

### Procedura

- 
- Krok 1** Naciśnij przycisk **Aplikacje** .
- Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Stan** > **Bieżący punkt dostępu**.
- Krok 3** Aby opuścić ekran bieżącego punktu dostępu, naciśnij klawisz **Zakończ**.
- 

### Pola na ekranie Bieżące punkty dostępu

W poniższej tabeli opisano pola na ekranie Bieżące punkty dostępu.

**Tabela 47: Elementy ekranu Bieżący punkt dostępu**

Element	Opis
Nazwa AP	Nazwa punktu dostępu, jeśli jest zgodna z CCX; w przeciwnym razie w tym miejscu wyświetlany jest adres MAC.
Adres MAC	Adres MAC punktu dostępu.
Częstotliwość	Ostatnia częstotliwość, na której zaobserwowano ten punkt dostępu.
Bieżący kanał	Ostatni kanał, na którym zaobserwowano ten punkt dostępu.
Ostatni RSSI	Ostatnia wartość wskaźnika RSSI, z którą zaobserwowano ten punkt dostępu.
Interwał sygnałów nawigacyjnych	Liczba jednostek czasu między sygnałami nawigacyjnymi. Jednostka czasu to 1,024 ms.
funkcjonalność,	To pole zawiera określoną liczbę pól podrzędnych, które są używane do wskazywania żądanych lub rozgłaszanych funkcji opcjonalnych.
Szybkości podstawowe	Wymagana przez punkt dostępu szybkość transmisji danych, z jaką stacja musi być w stanie pracować.
Szybkości opcjonalne	Obsługiwane przez punkt dostępu opcjonalne szybkości transmisji danych, z jakimi może pracować stacja.
Obsługiwane prędkości VHT(rx)	Zestaw obsługiwanych wartości RX MCS VHT odbieranych z punktu dostępu.
Obsługiwane prędkości VHT(tx)	Zestaw obsługiwanych wartości TX MCS VHT odbieranych z punktu dostępu.
Obsługiwane HT MCS	Zestaw obsługiwanych wartości TX MCS HT odbieranych z punktu dostępu.

Element	Opis
Okres pakietów DTIM	Każdy n-ty sygnał nawigacyjny oznacza okres czasu. Po każdym sygnale nawigacyjnym DTIM punkt dostępu wysyła pakiety emisji lub multiemisji znajdujące się w kolejce dla urządzeń oszczędzających energię.
Kod kraju	Dwucyfrowy kod kraju. Informacje dotyczące kraju mogą nie być wyświetlane, jeśli w sygnale nawigacyjnym nie ma elementu informacji (IE) o kraju.
Kanały	Lista obsługiwanych kanałów (na podstawie IE kraju).
Ograniczenie mocy	Wielkość mocy, o którą powinna zostać zmniejszona maksymalna moc transmisji zgodnie z limitem wymaganym prawnie.
Ograniczenie zasilania	Maksymalna moc transmisji w dBm dozwolona dla tego kanału.
Wykorzystanie kanału	Procent czasu, znormalizowany do 255, w którym punkt dostępu wykrył zajętość nośnika, wskazywany z wykorzystaniem mechanizmu fizycznego lub wirtualnego wykrywania fali nośnej (CS).
Liczba stacji	Łączna liczba stacji STA aktualnie skojarzonych z tym punktem dostępu.
Pojemność dla wstępu	Liczba całkowita bez znaku określająca pozostały odcinek czasu dla nośnika, który jest dostępny za pośrednictwem kontroli dostępu, wyrażona w jednostkach 32 mikrosekund na sekundę.  Jeśli wartość wynosi 0, punkt dostępu nie obsługuje tego elementu informacji i pojemność jest nieznana.
Obsługa WMM	Obsługa rozszerzeń multimediiów sieci Wi-Fi.
Obsługa UAPSD	Punkt dostępu obsługuje mechanizm Unscheduled Automatic Power Save Delivery (UAPSD). Może być dostępna wyłącznie w przypadku obsługi WMM. Jest to funkcja o decydującym znaczeniu dla czasu rozmów i uzyskania maksymalnego zagęszczenia połączeń w telefonie bezprzewodowym IP.
Proxy ARP	Punkt dostępu zgodny z CCX obsługuje odpowiedzi na zapytania protokołu IP ARP w imieniu powiązanej stacji. Ta funkcja ma decydujące znaczenie dla czasu pracy telefonu bezprzewodowego IP w trybie czuwania.
Wersja CCX	Jeśli punkt dostępu jest zgodny z CCX, w tym polu wyświetlana jest wersja CCX.
Brak standardów obsługi	Zawiera informacje związane z kolejką Best Effort.
Informacje podstawowe	Zawiera informacje związane z kolejką Tło.
Wideo	Zawiera informacje związane z kolejką Wideo.
Głos	Zawiera informacje związane z kolejką Głos.

## Strona WWW telefonu IP Cisco

Każdy telefon IP Cisco ma stronę WWW, na której można wyświetlać różne informacje o nim, m.in.:

- Informacje o urządzeniu: ustawienia urządzenia i powiązane informacje dotyczące telefonu.
- Konfiguracja sieci: informacje o konfiguracji sieci oraz o innych ustawieniach telefonu.
- Statystyki sieci: łączy do informacji o ruchu sieciowym.
- Dzienniki urządzeń: łączy do informacji pomocnych przy rozwiązywaniu problemów.
- Statystyki strumieniowania: łączy do różnych statystyk strumieniowania.
- System: łączy do ponownego uruchomienia telefonu.

W tej części przedstawiono informacje, które można uzyskać ze strony WWW telefonu. Umożliwiają one zdalne monitorowanie działania telefonu i pomagają w rozwiązywaniu problemów.

Większość z tych informacji można znaleźć bezpośrednio w telefonie.


## Otwieranie strony WWW telefonu

Aby otworzyć stronę WWW dla telefonu, wykonaj następujące czynności:



**Uwaga** Jeśli nie możesz otworzyć strony, być może jest ona domyślnie wyłączona.

### Procedura

- Krok 1** Ustal adres IP telefonu IP Cisco na jeden z tych sposobów:
- Wyszukaj telefon w aplikacji Cisco Unified Communications Manager — administracja, wybierając kolejno opcje **Urządzenie** > **Telefon**. Adres IP telefonu rejestrującego się w programie Cisco Unified Communications Manager jest widoczny w oknie **Znajdowanie i wyświetlanie telefonów** i w górnej części okna **Konfiguracja telefonu**.
  - W telefonie IP Cisco Unified naciśnij kolejno opcje **Aplikacje** , wybierz opcję **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja sieci Ethernet** > **Konfiguracja protokołu IPv4**, a następnie przewiń do pola Adres IP.
- Krok 2** Otwórz przeglądarkę internetową i wprowadź następujący adres URL, gdzie *IP\_address* to adres IP telefonu IP Cisco:
- http://adres\_IP**



## Informacje o urządzeniu

W obszarze Informacje o urządzeniu na stronie WWW telefonu znajdują się ustawienia urządzenia i powiązane informacje dotyczące telefonu. Elementy te opisano w poniższej tabeli.



**Uwaga** Część elementów widocznych w poniższej tabeli nie ma zastosowania w przypadku niektórych modeli telefonów.

Aby wyświetlić obszar **Informacje o urządzeniu**, należy przejść do strony WWW telefonu zgodnie z opisem w temacie [Otwieranie strony WWW telefonu, na stronie 246](#), a następnie kliknąć łącze **Informacje o urządzeniu**.

**Tabela 48: Elementy w obszarze Informacje o urządzeniu**

Element	Opis
Tryb usługi	Tryb usługi telefonu.
Nazwa usługi	Domena usługi.
Stan usługi	Bieżący stan usługi.
Adres MAC	Adres MAC (ang. Media Access Control, kontrola dostępu do mediów) telefonu.
Nazwa hosta	Niepowtarzalna stała nazwa, która jest automatycznie przypisywana telefonowi na podstawie jego adresu MAC.
Numer telefonu	Numer telefonu przypisany telefonowi.
App Load ID	Wersja oprogramowania sprzętowego działającego w telefonie.
Boot Load ID	Wersja rozruchowego oprogramowania sprzętowego.
Wersja	Identyfikator oprogramowania sprzętowego działającego w telefonie.
Moduł rozszerzenia klawiatury 1	Identyfikator pierwszego modułu rozszerzenia klawiatury, jeśli ma zastosowanie. Dotyczy wyłącznie telefonów IP Cisco 8851, 8851NR, 8861, 8865 oraz 8865NR.
Moduł rozszerzenia klawiatury 2	Identyfikator drugiego modułu rozszerzenia klawiatury, jeśli ma zastosowanie. Dotyczy wyłącznie telefonów IP Cisco 8851, 8851NR, 8861, 8865 oraz 8865NR.
Moduł rozszerzenia klawiatury 3	Identyfikator trzeciego modułu rozszerzenia klawiatury, jeśli ma zastosowanie. Dotyczy wyłącznie telefonów IP Cisco 8851, 8851NR, 8861, 8865 oraz 8865NR.
Wersja sprzętu	Drobna zmiana wersji warstwy sprzętowej telefonu.
Numer seryjny	Niepowtarzalny numer seryjny telefonu.
Numer modelu	Numer modelu telefonu.

Element	Opis
Wiadomość oczekująca	Wskazuje, czy na głównej linii telefonu oczekuje wiadomość głosowa.
UDI	Podane są tu następujące informacje o telefonie zawarte w identyfikatorze Cisco UDI (ang. Unique Device Identifier, niepowtarzalny identyfikator urządzenia): <ul style="list-style-type: none"> <li>• Typ urządzenia — wskazuje typ sprzętu. Na przykład w przypadku wszystkich modeli telefonów jest to „telefon”.</li> <li>• Opis urządzenia — nazwa telefonu skojarzonego ze wskazanym typem modelu.</li> <li>• Identyfikator produktu — model telefonu.</li> <li>• Identyfikator wersji (VID) — określa główny numer wersji sprzętu.</li> <li>• Numer seryjny — niepowtarzalny numer seryjny telefonu.</li> </ul>
Identyfikator UDI modułu rozszerzenia klawiatury	Unikatowy identyfikator urządzenia firmy Cisco (UDI) modułu rozszerzenia klawiatury. Dotyczy wyłącznie telefonów IP Cisco 8851, 8851NR, 8861, 8865 oraz 8865NR.
Imię i nazwisko zestawu nagłownego	Nazwa dołączonego zestawu nagłownego Cisco jest wyświetlana w lewej kolumnie. Prawa kolumna zawiera następujące informacje: <ul style="list-style-type: none"> <li>• Port — pokazuje, w jaki sposób zestaw nagłowny łączy się z telefonem. <ul style="list-style-type: none"> <li>• USB</li> <li>• AUX</li> </ul> </li> <li>• Wersja — wersja oprogramowania układowego zestawu nagłownego.</li> <li>• Zasięg radia — pokazuje intensywność skonfigurowaną dla radia świecą. Dotyczy wyłącznie Zestaw słuchawkowy Cisco z serii 560 .</li> <li>• Przepustowość — pokazuje, czy zestaw nagłowny korzysta z szerokiego lub wąskiego pasma. Dotyczy wyłącznie Zestaw słuchawkowy Cisco z serii 560 .</li> <li>• Bluetooth — pokazuje, czy protokół Bluetooth jest włączony, czy wyłączony. Dotyczy wyłącznie Zestaw słuchawkowy Cisco z serii 560 .</li> <li>• Konferencja — pokazuje, czy funkcja Konferencja jest włączona czy wyłączona. Dotyczy wyłącznie Zestaw słuchawkowy Cisco z serii 560 .</li> <li>• Źródło oprogramowania sprzętowego — wyświetla dozwoloną metodę aktualizacji oprogramowania sprzętowego: <ul style="list-style-type: none"> <li>• Ograniczenie tylko do UCM</li> <li>• Zezwalaj z poziomu UCM lub chmury Cisco</li> </ul> </li> </ul> <p>Dotyczy wyłącznie Zestaw słuchawkowy Cisco z serii 560 .</p>

Element	Opis
Godzina	Godzina Grupy daty/godziny, do której należy telefon. Informacja ta pochodzi z programu Cisco Unified Communications Manager.
Strefa czasu	Strefa czasowa Grupy daty/godziny, do której należy telefon. Informacja ta pochodzi z programu Cisco Unified Communications Manager.
Data	Data Grupy daty/godziny, do której należy telefon. Informacja ta pochodzi z programu Cisco Unified Communications Manager.
Wolna pamięć systemu	Ilość nieużywanej pamięci w telefonie
Wolna pamięć sterty Java	Ilość wolnej wewnętrznej pamięci sterty Java.
Wolna pamięć puli Java	Ilość wolnej wewnętrznej pamięci puli Java.
Tryb FIPS włączony	Wskazuje, czy włączony jest tryb FIPS (ang. Federal Information Processing Standard, federalny standard przetwarzania informacji).

## Konfiguracja sieci

W obszarze Konfiguracja sieci na stronie WWW telefonu widoczne są informacje o konfiguracji sieci i o innych ustawieniach telefonu. Elementy te opisano w poniższej tabeli.

Wiele z nich można wyświetlać i konfigurować w menu Konfiguracja sieci w telefonie IP Cisco.



**Uwaga** Część elementów widocznych w poniższej tabeli nie ma zastosowania w przypadku niektórych modeli telefonów.

Aby wyświetlić obszar **Konfiguracja sieci**, należy przejść do strony WWW telefonu zgodnie z opisem w temacie [Otwieranie strony WWW telefonu, na stronie 246](#), a następnie kliknąć łącze **Konfiguracja sieci**.

**Tabela 49: Elementy w obszarze Konfiguracja sieci**

Element	Opis
Adres MAC	Adres MAC (ang. Media Access Control, kontrola dostępu do mediów) telefonu.
Nazwa hosta	Nazwa hosta przypisana telefonowi przez serwer DHCP.
Nazwa domeny	Nazwa domeny, w której znajduje się telefon, w systemie DNS (ang. Domain Name System, nazw domen).
Serwer DHCP	Adres IP serwera protokołu DHCP (ang. Dynamic Host Configuration Protocol, protokół dykfigurowania hosta), z którego telefon otrzymuje adres IP.

Element	Opis
Serwer BOOTP	Wskazuje, czy telefon pobiera konfigurację z serwera protokołu BootP (ang. Bootstrap Protocol, protokół samorozruchu).
DHCP	Wskazuje, czy telefon korzysta z protokołu DHCP.
Adres IP	Adres IPv4 (Internet Protocol) telefonu.
Maska podsieci	Maska podsieci używana w telefonie.
Router domyślny	Domyślny router, z którego korzysta telefon.
Serwer DNS 1-3	Podstawowy serwer DNS (Serwer DNS 1) i opcjonalne zapasowe serwery DNS (Serwer DNS 2 i Serwer DNS 3), z których korzysta telefon.
Alternatywny serwer TFTP	Wskazuje, czy telefon korzysta z alternatywnego serwera TFTP.
Serwer TFTP 1	Podstawowy serwer TFTP (ang. Trivial File Transfer Protocol, trywialny protokół przesyłania plików), z którego korzysta telefon.
Serwer TFTP 2	Zapasowy serwer TFTP, z którego korzysta telefon.
Adres DHCP zwolniony	Wskazuje ustawienie opcji Adres DHCP zwolniony w menu Konfiguracja sieci telefonu.
Aktywny VLAN ID	Aktywna wirtualna sieć lokalna (ang. Virtual Local Area Network, VLAN) skonfigurowana przełączniku Cisco Catalyst, do której należy telefon.
Administracyjny VLAN ID	Pomocnicza sieć VLAN, do której należy telefon.
Serwer CUCM 1-5	<p>Nazwy hosta lub adresy IP serwerów Cisco Unified Communications Manager (uszeregowane w kolejności priorytetów), na których telefon może się zarejestrować. Ten element może również wskazywać adres IP routera SRST, który (o ile istnieje) udostępnia częściową funkcjonalność Cisco Unified Communications Manager.</p> <p>W przypadku dostępnego serwera w polu tym widoczny jest adres IP serwera Cisco Unified Communications Manager i jeden z następujących stanów:</p> <ul style="list-style-type: none"> <li>• <b>Włączony:</b> serwer Cisco Unified Communications Manager, z którego telefon uzyskuje usługi przetwarzania połączeń</li> <li>• <b>Rezerwowany:</b> serwer Cisco Unified Communications Manager, na który telefon przełącza się, gdy bieżący serwer stanie się niedostępny</li> <li>• <b>Pusty:</b> obecnie brak połączenia z danym serwerem Cisco Unified Communications Manager</li> </ul> <p>Element ten może również zawierać nominację trybu Survivable Remote Site Telephony (SRST), która wskazuje router SRST mogący udostępniać częściową funkcjonalność serwera Cisco Unified Communications Manager. Router ten przejmuje kontrolę nad przetwarzaniem połączeń, jeśli wszystkie inne serwery Cisco Unified Communications Manager staną się niedostępne. Serwer SRST Cisco Unified Communications Manager zawsze występuje na końcu listy serwerów, nawet jeśli jest to adres routera SRST można skonfigurować w części Pula urządzeń w oknie Konfiguracja w panelu Konfiguracja Cisco Unified Communications Manager.</p>

Element	Opis
Adres URL informacji	Adres URL tekstu pomocy widocznego w telefonie.
Adres URL książek telef.	Adres URL serwera, z którego telefon pobiera książkę telefoniczną.
Adres URL wiadomości	Adres URL serwera, z którego telefon uzyskuje usługi dotyczące wiadomości.
Adres URL usług	Adres URL serwera, z którego telefon uzyskuje usługi telefonu IP Cisco.
Idle URL	Adres URL wyświetlany przez telefon, który pozostaje w stanie bezczynności przez czas w polu Wolny URL i nie jest na nim otwarte żadne menu.
Czas nieaktywności adresu URL	Liczba sekund bezczynności telefonu, gdy nie jest otwarte żadne menu, jakie muszą upłynąć, aby włączy się usługa XML wskazana w polu Wolny URL.
Adres URL serwera proxy	Adres URL serwera proxy, który w imieniu klienta HTTP telefonu kieruje żądania HTTP hosta nielokalnego i przekazuje do niego odpowiedzi hosta.
Adres URL uwierzytelniania	Adres URL, którego telefon używa do weryfikowania żądań kierowanych do jego serwera.
Konfiguracja portu SW	Prędkość i tryb dupleks portu przełącznika, gdzie: <ul style="list-style-type: none"> <li>• A = automatyczne negocjowanie</li> <li>• 10H = 10-BaseT/półdupleks</li> <li>• 10F = 10-BaseT/pełny dupleks</li> <li>• 100H = 100-BaseT/półdupleks</li> <li>• 100F = 100-BaseT/pełny dupleks</li> <li>• 1000F = 1000-BaseT/pełny dupleks</li> <li>• No Link = brak połączenia z portem przełącznika</li> </ul>
Konfiguracja portu PC	Prędkość i tryb dupleks portu komputera, gdzie: <ul style="list-style-type: none"> <li>• A = automatyczne negocjowanie</li> <li>• 10H = 10-BaseT/półdupleks</li> <li>• 10F = 10-BaseT/pełny dupleks</li> <li>• 100H = 100-BaseT/półdupleks</li> <li>• 100F = 100-BaseT/pełny dupleks</li> <li>• 1000F = 1000-BaseT/pełny dupleks</li> <li>• No Link = brak połączenia z portem komputera</li> </ul>
Port PC wyłączony	Wskazuje, czy port komputera w telefonie jest włączony, czy wyłączony.
Ustawienia regionalne użytkownika	Ustawienia regionalne skojarzone z użytkownikiem telefonu. Stanowią zbiór szczegółowych ustawień na temat obsługi użytkowników, m.in. języka, czcionki, formatowania daty i godziny oraz alfanumerycznej służącej do wprowadzania tekstu.
Sieciowe ustawienia regionalne	Sieciowe ustawienia regionalne skojarzone z użytkownikiem telefonu. Stanowią zbiór szczegółowych informacji na temat obsługi telefonu w określonym kraju, m.in. definicje sygnałów dźwiękowych i interwałów stosowanych w telefonie.

Element	Opis
Wersja ustawień regionalnych użytkownika	Wersja ustawień regionalnych użytkownika wczytanych do telefonu.
Wersja ustawień regionalnych sieci	Wersja sieciowych ustawień regionalnych użytkownika wczytanych do telefonu.
Głośnik włączony	Wskazuje, czy w telefonie jest włączona funkcja telefonu głośnomówiącego.
Włączono protokół GARP	Wskazuje, czy telefon odczytuje adresy MAC z odpowiedzi protokołu GARP (Gratuitous ARP Resolution Protocol, nieodpłatny protokół rozpoznawania adresów).
Przekazuj do portu PC	Wskazuje, czy telefon przekazuje do portu dostępowego pakiety wysyłane i odbierane poprzez sieć.
Włączono obsługę wideo	Wskazuje, czy telefon może uczestniczyć w połączeniach wideo, gdy nawiąże komunikację z odpowiednio wyposażoną kamerą.
Włączono obsługę Voice VLAN	Wskazuje, czy telefon umożliwia urządzeniu podłączonemu do portu komputera dostęp do sieci transmisji głosowej.
Włączono sieć VLAN komputera	Sieć VLAN, która wykrywa i usuwa tagi 802.1P/Q z pakietów wysłanych do komputera.
Włączono automatyczny wybór linii	Wskazuje, czy telefon automatycznie wybiera linię przy podniesieniu słuchawki.
Kontrola protokołu DSCP	Klasyfikacja adresów IP DSCP w przypadku sygnalizacji sterowania połączeniami.
DSCP dla konfiguracji	Klasyfikacja adresów IP DSCP w przypadku każdego przesyłania konfiguracji telefonu.
DSCP dla usług	Klasyfikacja adresów IP DSCP w przypadku usług telefonu.
Tryb zabezpieczeń (niezabezpieczony)	Ustawiony w telefonie tryb zabezpieczeń.
Dostęp przez WWW możliwy	Wskazuje, czy dostęp przez WWW do telefonu jest włączony (Tak), czy wyłączony (Nie).
Dostęp SSH możliwy	Wskazuje, czy port SSH został włączony czy wyłączony.

Element	Opis
CDP: port SW	<p>Wskazuje, czy port przełącznika obsługuje protokół CDP (domyślnie opcja ta jest włączona).</p> <p>Włączenie obsługi protokołu CDP przez port przełącznika umożliwia przypisywanie telefonów do VLAN, negocjowanie zasilania i działanie zabezpieczeń 802.1x.</p> <p>Obsługę protokołu CDP przez port przełącznika należy włączyć, jeśli telefon komunikuje się z przełącznikiem Cisco.</p> <p>Jeśli w programie Cisco Unified Communications Manager obsługa protokołu CDP jest włączona, widoczne jest ostrzeżenie informujące, że obsługę protokołu CDP przez port przełącznika należy wyłączyć tylko, gdy telefon komunikuje się z przełącznikiem innej firmy niż Cisco.</p> <p>Aktualny stan obsługi protokołu CDP przez port komputera i przełącznika jest widoczny w konfiguracji Ustawienia.</p>
CDP: port PC	<p>Wskazuje, czy port komputera obsługuje protokół CDP (domyślnie opcja ta jest włączona).</p> <p>Jeśli w programie Cisco Unified Communications Manager obsługa protokołu CDP jest włączona, widoczne jest ostrzeżenie informujące, że wyłączenie obsługi protokołu CDP przez port komputera uniemożliwia działanie aplikacji Cisco VT Advantage (CVTA).</p> <p>Aktualny stan obsługi protokołu CDP przez port komputera i przełącznika jest widoczny w konfiguracji Ustawienia.</p>
LLDP-MED: port SW	<p>Wskazuje, czy w porcie przełącznika włączone jest rozszerzenie LLDP-MED (ang. Link Layer Protocol Media Endpoint Discovery, wykrywanie punktów końcowych nośników za pomocą LLDP-MED na poziomie łącza).</p>
LLDP-MED: port komputera	<p>Wskazuje, czy protokół LLDP-MED jest włączony na porcie komputera.</p>
LLDP priorytet mocy	<p>Przypisuje do przełącznika priorytet zasilania, umożliwiając właściwe zasilanie telefonów. Dostępne ustawienia:</p> <ul style="list-style-type: none"> <li>• Nieznany: wartość domyślna.</li> <li>• Niski</li> <li>• Wysoki</li> <li>• Kluczowy</li> </ul>
LLDP Asset ID	<p>Identyfikator zasobu przypisanego do telefonu w celu zarządzania zapasami.</p>
Plik CTL	<p>Skrót MD5 pliku CTL.</p>
Plik ITL	<p>Plik ITL zawiera początkową listę zaufanych.</p>
Sygnatura ITL	<p>Skrót MD5 pliku ITL.</p>
Serwer CAPF	<p>Serwer CPF w użyciu</p>
TVS	<p>Główny składnik funkcji Security by Default (Domyślne bezpieczeństwo). Usługa Trust Verification Service (TVS) umożliwia telefonom IP Cisco Unified uwierzytelnianie serwerów aplikacji, w tym EM, książki adresowej i midletów, w trakcie nawiązywanie połączenia za pośrednictwem HTTPS.</p>

Element	Opis
Serwer TFTP	Nazwa serwera TFTP używanego przez telefon.
Serwer TFTP	Nazwa serwera TFTP używanego przez telefon.
Automatyczna synchronizacja portów	Wskazuje, czy telefon automatycznie synchronizuje szybkość portu w celu wyeliminowania pakietów.
Zdalna konfiguracja portu przełącznika	Wskazuje, czy port programowy jest sterowany zdalnie.
Zdalna konfiguracja portu komputera	Wskazuje, czy port komputera jest sterowany zdalnie.
Tryb adresowania IP	Identyfikuje tryb adresowania: <ul style="list-style-type: none"> <li>• Tylko IPv4</li> <li>• IPv4 i IPv6</li> <li>• Tylko IPv6</li> </ul>
Kontrola trybu preferencji protokołu IP	Wskazuje wersję adresu IP, której telefon używa podczas komunikacji z programem Cisco Unified Communications Manager, gdy ma dostępne obie wersje, czyli IPv4 i IPv6.
Tryb preferencji protokołu IP dla nośników	
Automatyczna konfiguracja IPv6	Wskazuje, czy w przypadku nośników urządzenie korzysta z adresu IPv4 do nawiązywania połączenia z programem Cisco Unified Communications Manager.
Ochrona przed powtarzaniem adresów IPv6	
Akceptacja przekierowania wiadomości IPv6	Wskazuje, czy telefon przyjmuje przekierowane wiadomości z tego samego routera, który służy numer docelowy.
Żądanie echa odpowiedzi multimijsji IPv6	Wskazuje, czy telefon wysyła komunikat Echo Reply w odpowiedzi na komunikat Echo Request nadesłany na adres tylko IPv6.
Serwer pobierania IPv6	Służy do optymalizowania pory instalacji uaktualnień oprogramowania sprzętowego telefonu, zmniejszania obciążenia sieci WAN poprzez lokalne przechowywanie obrazów, które eliminują konieczność przesyłania ich łączem WAN przy każdym uaktualnieniu telefonu.
Serwer dziennika protokołu IPv6	
Serwer CAPF protokołu IPv6	Podaje adres IP i port zdalnego urządzenia rejestrującego, do którego telefon wysyła komunikat dziennika.



Element	Opis
Protokół DHCPv6	<p>Wskazuje metodę wykorzystywaną przez telefon w celu uzyskania adresu tylko IPv6.</p> <p>Gdy protokół DHCPv6 jest włączony, telefon uzyskuje adres IPv6 z serwera DHCPv6 lub z SLAAC za pomocą komunikatu RA wysłanego przez router obsługujący protokół IPv6. Gdy protokół DHCPv6 jest wyłączony, telefon nie uzyska żadnego stanowego (z serwera DHCP) lub bezstanowego (z mechanizmu SLAAC) adresu IPv6.</p> <p><b>Uwaga</b> W przeciwieństwie do protokołu DHCPv4, nawet przy wyłączonym protokole DHCPv6 telefon może nadal generować adres SLAAC, jeśli jest włączona automatyczna konfiguracja.</p>
Adres IPv6	<p>Wyświetla bieżący adres telefonu tylko IPv6.</p> <p>Obsługiwane są dwa formaty adresu:</p> <ul style="list-style-type: none"> <li>• Osiem zestawów cyfr szesnastkowych rozdzielonych dwukropkami X:X:X:X:X:X:X:X</li> <li>• Skompresowany format umożliwia zwinięcie pojedynczego ciągu grup złożonych z jedną grupę reprezentowaną przez podwójny dwukropek.</li> </ul>
Długość prefiksu IPv6	Wyświetla bieżącą długość prefiksu podsieci tylko IPv6.
Domyślny router protokołu IPv6	Wyświetla domyślny router IPv6 używany przez telefon.
Serwer DNS IPv6 1-2	Wyświetla podstawowy i pomocniczy serwer DNSv6 używany przez telefon
Alternat. serwer TFTP IPv6	Wyświetla, czy jest używany alternatywny serwer IPv6 TFTP.
Serwer 1-2 TFTP IPv6	Wyświetla podstawowy i pomocniczy serwer IPv6 TFTP używany przez telefon.
Adres IPv6 zwolniony	Wyświetla informację, czy użytkownik zwolnił informacje dotyczące protokołu IPv6.
Poziom zasilania EnergyWise	Poziom zasilania wykorzystywany przez uśpiony telefon.
Domena EnergyWise	Domena EnergyWise, w której znajduje się telefon.
DF_BIT	Wskazuje ustawienie bitu DF dla pakietów.

## Statystyki sieci

Poniższe łącza do statystyk sieci znajdujące się na stronie WWW telefonu dają dostęp do informacji o ruchu sieciowym telefonu:

- Informacje o sieci Ethernet: informacje o ruchu sieci Ethernet.
- Dostęp: informacje o ruchu sieciowym na porcie PC telefonu.
- Sieć: informacje o ruchu sieciowym na porcie sieciowym telefonu.

Aby wyświetlić obszar statystyk sieci, otwórz stronę WWW telefonu, a następnie kliknij pozycję **Informacje o sieci Ethernet** i łącze **Dostęp** lub **Sieć**.

### Strona WWW Ethernet Information (Informacje o sieci Ethernet)

W poniższej tabeli opisano zawartość strony WWW Ethernet Information (Informacje o sieci Ethernet).

**Tabela 50: Elementy na stronie WWW Ethernet Information**

Element	Opis
Wysł. ramki	Łączna liczba pakietów wysłanych przez telefon.
Wysł. emisja	Łączna liczba wysłanych przez telefon pakietów rozgłoszeniowych.
Wysł. multiemisja	Łączna liczba wysłanych przez telefon pakietów multiemisji.
Transmisja pojedyncza	Łączna liczba wysłanych przez telefon pakietów emisji pojedynczej.
Wysł. ramki	Łączna liczba pakietów odebranych przez telefon.
Odb. emisja	Łączna liczba odebranych przez telefon pakietów rozgłoszeniowych.
Odb. multiemisja	Łączna liczba odebranych przez telefon pakietów multiemisji.
Odb. poj. emisja	Łączna liczba odebranych przez telefon pakietów emisji pojedynczej.
Rx PacketNoDes	Łączna liczba pakietów odrzuconych z powodu braku deskryptora bezpośredniego dostępu do pamięci (ang. Direct Memory Access, DMA).

### Strony WWW Dostęp i Sieć

W poniższej tabeli przedstawiono informacje widoczne na stronach WWW Dostęp i Sieć.

**Tabela 51: Pola na stronach Dostęp i Sieć**

Element	Opis
Odb. pak. łącznie	Łączna liczba pakietów odebranych przez telefon.
Odb. błąd CRC	Łączna liczba pakietów odebranych z błędami CRC (ang. Cyclic Redundancy Check, cykliczny kod nadmiarowy).
Odb. błąd wyrówn.	Łączna liczba odebranych pakietów o długości od 64 do 1522 bajtów, które miały nieprawidłową sekwencję kontrolną ramki (ang. Frame Check Sequence, FCS).
Odb. multiemisja	Łączna liczba odebranych przez telefon pakietów multiemisji.
Odb. emisja	Łączna liczba odebranych przez telefon pakietów rozgłoszeniowych.
Odb. poj. emisja	Łączna liczba odebranych przez telefon pakietów emisji pojedynczej.

Element	Opis
Odb. popr. kr.	Łączna liczba odebranych pakietów z błędami FCS lub z błędami dopasowania, których rozmiar nie osiąga 64 bajtów.
Odb. popr. kr.	Łączna liczba odebranych prawidłowych pakietów, których rozmiar nie osiąga 64 bajtów.
Odb. popr. dług.	Łączna liczba odebranych prawidłowych pakietów, których rozmiar przekracza 1522 bajty.
Odb. bł. dług.	Łączna liczba odebranych pakietów z błędami FCS lub z błędami dopasowania, których rozmiar przekracza 1522 bajty.
Odb. 64	Łączna liczba odebranych pakietów, w tym pakietów z błędami, których rozmiar wynosi od 0 do 64 bajtów.
Odb. od65do127	Łączna liczba odebranych pakietów, w tym pakietów z błędami, których rozmiar wynosi od 65 do 127 bajtów.
Odb. od128do255	Łączna liczba odebranych pakietów, w tym pakietów z błędami, których rozmiar wynosi od 128 do 255 bajtów.
Odb. od256do511	Łączna liczba odebranych pakietów, w tym pakietów z błędami, których rozmiar wynosi od 256 do 511 bajtów.
Odb. od512do1023	Łączna liczba odebranych pakietów, w tym pakietów z błędami, których rozmiar wynosi od 512 do 1023 bajtów.
Odb. od1024do1518	Łączna liczba odebranych pakietów, w tym pakietów z błędami, których rozmiar wynosi od 1024 do 1518 bajtów.
Odb. odrz. żeton	Łączna liczba pakietów odrzuconych z powodu braku zasobów (np. przepełnienia bufora FIFO).
Wysł. nadm. różn.	Łączna liczba pakietów opóźnionych z powodu zajętego medium.
Wysł. kolizje opóźn.	Liczba przypadków kolizji, które wystąpiły później niż po wysłaniu 512 bitów od początku transmisji pakietów.
Wysł. popr. pak. łącznie	Łączna liczba odebranych przez telefon prawidłowych pakietów (multiemisji, rozgłoszeniowych i emisji pojedynczej).
Wysł. kolizje	Łączna liczba kolizji, które wystąpiły podczas przesyłania pakietu.
Wysł. zbyt dł.	Łączna liczba pakietów, które nie zostały wysłane, ponieważ podjęto 16 nieudanych prób ich wysłania.
Wysł. emisja	Łączna liczba wysłanych przez telefon pakietów rozgłoszeniowych.
Wysł. multiemisja	Łączna liczba wysłanych przez telefon pakietów multiemisji.
LLDP FramesOutTotal	Łączna liczba wysłanych przez telefon ramek protokołu wykrywania warstwy łącza (ang. Link Layer Discovery Protocol, LLDP).

Element	Opis
LLDP AgeoutsTotal	Łączna liczba ramek LLDP, w których przypadku upłynął limit czasu w pamięci podręcznej.
LLDP FramesDiscardedTotal	Łączna liczba ramek LLDP, które zostały odrzucone, gdy jeden z obowiązkowych elementów TLV (ang. type-length-value, typ-długość-wartość) był nieobecny, nie działał lub zawierał ciąg o długości przekraczającej prawidłowy zakres.
LLDP FramesInErrorsTotal	Łączna liczba ramek LLDP odebranych z co najmniej jednym wykrywalnym błędem.
LLDP FramesInTotal	Łączna liczba odebranych przez telefon ramek LLDP.
LLDP TLVDiscardedTotal	Łączna liczba odrzuconych elementów TLV w ramach LLDP.
LLDP TLVUnrecognizedTotal	Łączna liczba elementów TLV w ramach LLDP, które nie zostały rozpoznane przez telefon.
Identyfikator sąsiedniego urządzenia CDP	Identyfikator urządzenia podłączonego do tego portu, które zostało wykryte przez protokół CDP (ang. Cisco Discovery Protocol).
Adres IPv6 sąsiedniego urządzenia CDP	Adres IP sąsiedniego urządzenia wykrytego przez protokół CDP.
Port sąsiedniego urządzenia CDP	Wykryty przez protokół CDP port sąsiedniego urządzenia, do którego podłączony jest telefon.
Identyfikator sąsiedniego urządzenia LLDP	Identyfikator urządzenia podłączonego do tego portu, które zostało wykryte przez protokół LLDP.
Adres IPv6 sąsiedniego urządzenia LLDP	Adres IP sąsiedniego urządzenia wykrytego przez protokół LLDP.
Port sąsiedniego urządzenia LLDP	Wykryty przez protokół LLDP port sąsiedniego urządzenia, do którego jest podłączony telefon.
Informacje o porcie	Informacje o prędkości i funkcji duplexu.

## Dzienniki urządzeń

Poniższe łącza do dzienników urządzenia znajdujące się na stronie WWW telefonu umożliwiają dostęp do informacji pomocnych przy monitorowaniu działania telefonu i rozwiązywaniu problemów go dotyczących.

- Console Logs (Dzienniki konsoli): zawiera łącza do poszczególnych plików dzienników. Pliki dzienników konsoli zawierają odebrane przez telefon komunikaty dotyczące debugowania i błędów.
- Core Dumps (Zrzuty podstawowe): zawiera łącza do poszczególnych plików zrzutów. Pliki zrzutów podstawowych zawierają dane o awariach telefonu.
- Status Messages (Komunikaty o stanie): wyświetlane jest tu 10 najnowszych komunikatów o stanie, które telefon wygenerował od czasu ostatniego uruchomienia. Informacje te znajdują się również na ekranie Status Messages w telefonie.

- Debug Display (Obszar debugowania): są tu wyświetlane komunikaty dotyczące debugowania, które mogą być przydatne zespołowi Cisco TAC w przypadku zasięgnięcia jego porady przy rozwiązywaniu problemów.

## Statystyki strumieniowania

Telefon IP Cisco może równocześnie strumieniować informacje do i z maksymalnie trzech urządzeń. Telefon strumieniuje informacje, gdy trwa połączenie głosowe albo gdy jest w nim uruchomiona usługa, która wysyła lub odbiera dźwięk bądź dane.

W obszarach Statystyki strumieniowania na stronie WWW telefonu podane są informacje o strumieniach.

W poniższej tabeli opisano elementy widoczne w obszarach Statystyki strumieniowania.

**Tabela 52: Elementy w obszarach Statystyki strumieniowania**

Element	Opis
Adres zdalny	Adres IP i port UDP miejsca docelowego strumienia.
Adres lokalny	Adres IP i port UDP telefonu.
Godzina rozpoczęcia	Wewnętrzny znacznik czasu wskazujący, kiedy serwer Cisco Unified Communications zażądał od telefonu rozpoczęcia przesyłania pakietów.
Stan strumienia	Wskazanie aktywności strumieniowania lub jej braku.
Nazwa hosta	Niepowtarzalna stała nazwa, która jest automatycznie przypisywana telefonowi na jego adres MAC.
Liczba nadanych pakietów	Łączna liczba pakietów danych RTP, które telefon wysłał od początku tego połączenia. Ta wartość wynosi 0, jeśli połączenie działa w trybie samego odbioru.
Liczba nadanych oktetów	Łączna liczba oktetów ładunku, które telefon wysłał w pakietach danych RTP od początku połączenia. Wartość ta wynosi 0, jeśli połączenie działa w trybie samego odbioru.
Kodek nadajnika	Typ kodowania dźwięku zastosowany w wysyłanym strumieniu.
Wysłano raporty nadajnika (patrz uwaga)	Liczba przypadków wysłania raportu nadajnika RTCP.
Wysłano godzinę raportu nadajnika (patrz uwaga)	Wewnętrzny znacznik czasu wskazujący, kiedy został wysłany ostatni raport nadajnika.
Utracone pakiety odbiornika	Łączna liczba pakietów danych RTP, które zostały utracone od początku odbioru danych w ramach tego połączenia. Obliczana według wzoru: liczba oczekiwanych pakietów minus liczba faktycznie odebranych pakietów, przy czym liczba odebranych pakietów obejmuje pakiety spóźnione i będące duplikatami. Wartość ta wynosi 0, jeśli połączenie działa w trybie samego wysyłania.

Element	Opis
Średni jitter	Oszacowanie średniego odchylenia czasu docierania kolejnych pakietów danych RTP, mierzonego w milisekundach. Wartość ta wynosi 0, jeśli połączenie działa w trybie samego wysyłania.
Kodek odbiornika	Typ kodowania dźwięku zastosowany w odbieranym strumieniu.
Wysłano raporty odbiornika (patrz uwaga)	Liczba przypadków wysłania raportu odbiornika RTCP.
Wysłano godzinę raportu odbiornika (patrz uwaga)	Wewnętrzny znacznik czasu wskazujący, kiedy został wysłany raport odbiornika RTCP.
Liczba odebranych pakietów	Łączna liczba pakietów danych RTP, które zostały odebrane przez telefon od początku do końca danych w ramach tego połączenia. Obejmuje pakiety odebrane z różnych źródeł, jeśli to połączenie ma charakter multimedialny. Wartość ta wynosi 0, jeśli połączenie działa w trybie samego wysyłania.
Liczba odebranych oktetów	Łączna liczba oktetów ładunku, które zostały odebrane przez telefon w pakietach danych od początku odbioru danych w ramach tego połączenia. Obejmuje pakiety odebrane z różnych źródeł, jeśli to połączenie ma charakter multimedialny. Wartość ta wynosi 0, jeśli połączenie działa w trybie samego wysyłania.
MOS LQK	Ocena, będąca obiektywnym oszacowaniem średniej oceny opinii (Mean Opinion Score), dotyczącej jakości odsłuchu (Listening Quality, LQK), z przedziału od 5 (doskonała) do 1 (nie do zaakceptowania). Ta ocena jest oparta na słyszalnych wystąpieniach ukrywania dźwięku wynikającego z utraty ramek w poprzednim ośmiosekundowym fragmencie strumienia transmisji głosowej. Aby uzyskać więcej informacji, patrz <a href="#">Monitorowanie jakości dźwięku, na stronie 290</a> .  <b>Uwaga</b> Wynik MOS LQK może zależeć od typu kodeka wykorzystywanego przez telefon IP Cisco Unified.
Śr. MOS LQK	Średnia ocena MOS LQK zaobserwowana dla całego strumienia.
Min. MOS LQK	Najniższa ocena MOS LQK zaobserwowana od początku strumienia transmisji głosowej.
Maks. MOS LQK	Podstawowa (najwyższa) ocena MOS LQK zaobserwowana od początku strumienia transmisji głosowej.  W normalnych warunkach, bez utraty ramek, te kodeki zapewniają następującą wartość MOS LQK: <ul style="list-style-type: none"> <li>• G.711 — 4,5.</li> <li>• G.729 A /AB — 3,7.</li> </ul>
Wersja MOS LQK	Wersja opracowanego przez firmę Cisco algorytmu używanego do obliczania ocen MOS LQK.
Współczynnik ukrywania kumulatywnego	Łączna liczba ramek ukrywania podzielona przez łączną liczbę ramek transmisji głosowej odebranych od początku strumienia transmisji głosowej.

Element	Opis
Współczynnik ukrywania w interwale	Stosunek liczby ramek ukrywania do liczby ramek transmisji głosowej w poprzedzającym 3-sekundowym interwale trwającej rozmowy. Jeśli działa funkcja wykrywania aktywności transmisji głosowej (VAD), może być wymagany dłuższy interwał w celu zebrania danych o aktywności transmisji głosowej.
Maks. współczynnik ukrywania	Najwyższy współczynnik ukrywania w interwale od początku strumienia transmisji głosowej.
Ukrywanie (sek.)	Liczba sekund, w których występowały zdarzenia ukrywania (utracone ramki), od początku strumienia transmisji głosowej (obejmuje sekundy z intensywnym ukrywaniem).
Intensywne ukrywanie (sek.)	Liczba sekund, w których zdarzenia ukrywania (utracone ramki) obejmowały ponad połowę czasu od początku strumienia transmisji głosowej.
Opóźnienie (patrz uwaga)	Oszacowanie opóźnienia sieci wyrażonego w milisekundach. Stanowi określone na podstawie średnie opóźnienie przesyłania danych w obie strony, mierzone w trakcie odbierania raportu odbiornika RTCP.
Maks. jitter	Maksymalna wartość bieżącego jittera, w milisekundach.
Rozmiar po stronie nadawcy	Rozmiar pakietów RTP wysłanego strumienia, w milisekundach.
Odebrano raporty nadajnika (patrz uwaga)	Liczba przypadków odebrania raportu nadajnika RTCP.
Odebrano godzinę raportu nadajnika (patrz uwaga)	Czas odebrania ostatniego raportu nadajnika RTCP.
Rozmiar po stronie odbiorcy	Rozmiar pakietów RTP odbieranego strumienia, w milisekundach.
Odbiornik odrzucony	Pakiety RTP, które zostały odebrane z sieci, ale odrzucone z buforów jittera.
Odebrano raporty odbiornika (patrz uwaga)	Liczba przypadków odebrania raportu odbiornika RTCP.
Odebrano godzinę raportu odbiornika (patrz uwaga)	Czas odebrania ostatniego raportu odbiornika RTCP.
Szyfrowane przez odbiornik	Wskazuje, czy odbiornik używa szyfrowania.
Szyfrowane przez nadajnik	Wskazuje, czy nadajnik używa szyfrowania.
Ramki po stronie nadajnika	Liczba wysłanych ramek.
Ramki częściowe po stronie nadajnika	Liczba wysłanych częściowych ramek.
Ramki I po stronie nadajnika	Liczba wysłanych ramek I. Ramki I są stosowane przy transmisji wideo.

Element	Opis
Ramki IDR po stronie nadajnika	Liczba wysłanych ramek natychmiastowego odświeżania dekodera (IDR). Ramki IDR stosowane przy transmisji wideo.
Szybkość wysyłania ramek przez nadajnik	Szybkość, z jaką nadawca wysyła ramki.
Przepustowość po stronie nadajnika	Pasmo nadawcy.
Rozdzielczość po stronie nadajnika	Rozdzielczość wideo nadawcy.
Ramki po stronie odbiornika	Liczba otrzymanych ramek.
Ramki częściowe po stronie odbiornika	Liczba otrzymanych częściowych ramek.
Otrzymane ramki I	Liczba otrzymanych ramek I.
Ramki IDR po stronie odbiornika	Liczba otrzymanych ramek IDR.
Żądanie dotyczące ramek iFrame po stronie odbiornika	Liczba otrzymanych zażądanych ramek IDR.
Szybkość odbierania ramek przez odbiornik	Szybkość, z jaką odbiorca odbiera ramki.
Ramki zagubione po stronie odbiornika	Liczba ramek, które nie zostały odebrane.
Błędy ramek po stronie odbiornika	Liczba ramek, które nie zostały odebrane.
Przepustowość po stronie odbiornika	Szerokość pasma odbiorcy.
Rozdzielczość po stronie odbiornika	Rozdzielczość wideo odbiorcy.
Domena	Domena, w której znajduje się telefon.
Połączenia nadajnika	Liczba przypadków dołączenia nadawcy.
Połączenia odbiornika	Liczba przypadków dołączenia odbiorcy.
Zakończone połączenia	Liczba ramek "Bye"
Godzina uruchomienia nadajnika	Godzina rozpoczęcia pracy nadawcy.
Godzina uruchomienia odbiornika	Godzina rozpoczęcia pracy odbiorcy.



Element	Opis
Stan wiersza	Czy telefon korzystał z przesyłania strumieniowego
Narzędzie nadajnika	Typ kodowania dźwięku zastosowany w strumieniu
Raporty nadajnika	Raporty nadajnika RTCP
Godzina raportowania nadajnika	Godzina wysłania ostatniego raportu nadajnika RTCP.
Jitter odbiornika	Maksymalne wahania strumienia
Narzędzie odbiornika	Typ kodowania dźwięku zastosowany w strumieniu
Raporty odbiornika	Liczba dostępów do raportu statystyk strumieniowych uzyskanych ze strony WWW
Godzina raportu odbiornika	Wewnętrzny znacznik czasu wskazujący wygenerowanie danego raportu statystyki strumieniowania
Połączenie wideo	Wskazuje, czy połączenie było połączeniem wideo, czy jedynie audio.
ID dzwoniącego	Identyfikacja połączenia.
ID grupy	Identyfikacja grupy, w której znajduje się telefon.



**Uwaga** Gdy protokół sterujący RTP jest wyłączony, w przypadku tego pola nie są generowane żadne dane i dlatego występuje w nim wartość 0.

## Żądanie informacji z telefonu w formacie XML

W celu rozwiązywania problemów można wysłać żądanie informacji z telefonu. Dane wynikowe otrzymuje się w formacie XML. Dostępne są następujące informacje:

- CallInfo to informacje o sesjach połączeń dotyczące konkretnej linii.
- LineInfo to informacje o konfiguracji linii telefonu.
- ModeInfo to informacje o trybie telefonu.

### Zanim rozpoczniesz

Uzyskiwanie tych informacji wymaga włączenia funkcji Dostęp przez WWW.

Telefon musi być skojarzony z użytkownikiem.

### Procedura

**Krok 1** Aby uzyskać informacje CallInfo, należy wprowadzić w przeglądarce następujący adres URL:  
**http://<phone ip address>/CGI/Java/CallInfo<x>**

gdzie

- *<phone ip address>* to adres IP telefonu
- *<x>* to numer linii, której mają dotyczyć informacje.

Polecenie zwraca dokument XML.

**Krok 2** Aby uzyskać informacje Line Info, należy wprowadzić w przeglądarce następujący adres URL:  
**http://<phone ip address>/CGI/Java/LineInfo**

gdzie

- *<phone ip address>* to adres IP telefonu

Polecenie zwraca dokument XML.

**Krok 3** Aby uzyskać informacje Model Info, należy wprowadzić w przeglądarce następujący adres URL:  
**http://<phone ip address>/CGI/Java/ModeInfo**

gdzie

- *<phone ip address>* to adres IP telefonu

Polecenie zwraca dokument XML.

## Przykładowe dane wyjściowe polecenia CallInfo

Poniższy kod XML to przykład danych wyjściowych polecenia CallInfo.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
    <CallState>CONNECTED</CallState>
    <CallType>INBOUND</CallType>
    <CallingPartyName/>
    <CallingPartyDirNum>9700</CallingPartyDirNum>
    <CalledPartyName/>
    <CalledPartyDirNum>1030</CalledPartyDirNum>
    <HuntPilotName/>
    <CallReference>30303060</CallReference>
    <CallDuration>12835</CallDuration>
    <CallStatus>null</CallStatus>
    <CallSecurity>UNAUTHENTICATED</CallSecurity>
    <CallPrecedence>ROUTINE</CallPrecedence>
    <FeatureList/>
  </CiscoIPPhoneCallInfo>
  <VisibleFeatureList>
    <Feature Position="1" Enabled="true" Label="End Call"/>
    <Feature Position="2" Enabled="true" Label="Show Detail"/>
  </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

## Przykładowe dane wyjściowe polecenia LineInfo

Poniższy kod XML to przykład danych wyjściowych polecenia LineInfo.

```
<CiscoIPPhoneLineInfo>
  <Prompt/>
  <Notify/>
  <Status>null</Status>
  <CiscoIPPhoneLines>
    <LineType>9</LineType>
    <lineDirNum>1028</lineDirNum>
    <MessageWaiting>NO</MessageWaiting>
    <RingerName>Chirp1</RingerName>
    <LineLabel/>
    <LineIconState>ONHOOK</LineIconState>
  </CiscoIPPhoneLines>
  <CiscoIPPhoneLines>
    <LineType>9</LineType>
    <lineDirNum>1029</lineDirNum>
    <MessageWaiting>NO</MessageWaiting> <RingerName>Chirp1</RingerName>
    <LineLabel/>
    <LineIconState>ONHOOK</LineIconState>
  </CiscoIPPhoneLines>
  <CiscoIPPhoneLines>
    <LineType>9</LineType>
    <lineDirNum>1030</lineDirNum>
    <MessageWaiting>NO</MessageWaiting>
    <RingerName>Chirp1</RingerName>
    <LineLabel/>
    <LineIconState>CONNECTED</LineIconState>
  </CiscoIPPhoneLines>
  <CiscoIPPhoneLines>
    <LineType>2</LineType>
    <lineDirNum>9700</lineDirNum>
    <MessageWaiting>NO</MessageWaiting>
    <LineLabel>SD9700</LineLabel>
    <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

## Przykładowe dane wyjściowe polecenia ModelInfo

Poniższy kod XML to przykład danych wyjściowych polecenia ModelInfo.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
  <PlaneTitle>Applications</PlaneTitle>
  <PlaneFieldCount>12</PlaneFieldCount>
  <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
  <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
  <Prompt></Prompt>
  <Notify></Notify>
  <Status></Status>
  <CiscoIPPhoneFields>
    <FieldType>0</FieldType>
    <FieldAttr></FieldAttr>
    <FieldHelpIndex>0</fieldHelpIndex>
    <FieldName>Call History</FieldName>
    <FieldValue></FieldValue>
  </CiscoIPPhoneFields>
</CiscoIPPhoneModeInfo>
```

```
<FieldType>0</FieldType>
<FieldAttr></FieldAttr>
<fieldHelpIndex>0</fieldHelpIndex>
<FieldName>Preferences</FieldName>
<FieldValue></FieldValue>
</CiscoIPPhoneFields>
...
</CiscoIPPhoneModeInfo>
```



# ROZDZIAŁ 12

## Rozwiązywanie problemów

- [Ogólne informacje o rozwiązywaniu problemów, na stronie 267](#)
- [Problemy z uruchamianiem, na stronie 268](#)
- [Problemy z resetowaniem się telefonu, na stronie 273](#)
- [Telefon nie może się połączyć z siecią LAN, na stronie 275](#)
- [Problemy z zabezpieczeniami telefonu IP Cisco, na stronie 275](#)
- [Problemy z połączeniem wideo, na stronie 277](#)
- [Ogólne problemy z połączeniami telefonicznymi, na stronie 278](#)
- [Procedury rozwiązywania problemów, na stronie 279](#)
- [Informacje kontrolne debugowania z programu Cisco Unified Communications Manager, na stronie 284](#)
- [Dodatkowe informacje o sposobach rozwiązywania problemów, na stronie 285](#)

## Ogólne informacje o rozwiązywaniu problemów

W poniższej tabeli podano ogólne informacje na temat rozwiązywania problemów z telefonem IP Cisco.

*Tabela 53: Rozwiązywanie problemów z telefonem IP Cisco*

Podsumowanie	Objaśnienie
Łączenie telefonu IP Cisco z innym telefonem IP Cisco	Firma Cisco nie zapewnia obsługi łączenia telefonu IP z innym telefonem IP za pośrednictwem portu komputera. Każdy telefon IP powinien być podłączony bezpośrednio do portu przełącznika. Jeśli telefony zostaną połączone za pomocą portu komputera, nie będą działać.
Długotrwałe burze rozgłoszeniowe powodują zerowanie się telefonów IP lub uniemożliwiają nawiązywanie połączeń	Długotrwała burza rozgłoszeniowa w warstwie 2 (trwająca kilka minut) w transmisji głosowej może powodować zerowanie się telefonów IP, utratę połączenia albo brak możliwości nawiązywania lub odbierania połączeń. Po ustaniu burzy rozgłoszeniowej telefony mogą nie wznowić prawidłowego działania.

Podsumowanie	Objaśnienie
Przenoszenie połączenia sieciowego z telefonu na stację roboczą	<p>Jeśli telefon jest zasilany z użyciem połączenia sieciowego, należy z namyśle podejmować decyzję o odłączeniu kabla sieciowego od telefonu i podłączeniu go do komputera.</p> <p><b>Przeostroga</b> Karta sieciowa w komputerze nie może pobierać prądu za pośrednictwem połączenia sieciowego. Pojawienie się prądu w sieciowym może spowodować zniszczenie karty sieciowej. W celu ochrony karty sieciowej należy po odłączeniu kabla od telefonu odczekać co najmniej 10 sekund przed podłączeniem go do komputera. Dzięki temu opóźnieniu przełącznik ma dostatecznie dużo czasu, aby wykryć brak telefonu na linii i przestać dostarczać prąd do karty sieciowej.</p>
Zmiana konfiguracji telefonu	<p>Domyślnie opcje konfiguracji sieci są zablokowane, aby zapobiec wprowadzaniu przez użytkowników zmian, które mogłyby zakłócić komunikację z siecią. Aby zmienić opcje konfiguracji sieci, należy je najpierw odblokować. Więcej informacji zawiera sekcja <a href="#">Ustawianie hasła w telefonie, na stronie 50</a>.</p> <p><b>Uwaga</b> Jeśli we wspólnym profilu telefonu nie ma ustawionego hasła administratora, użytkownik może modyfikować ustawienia sieci.</p>
Niedopasowanie kodeka między telefonem a innym urządzeniem	<p>Dane statystyczne RxType i TxType wskazują kodek używany do komunikacji między telefonem IP Cisco a innym urządzeniem. Wartości tych danych statystycznych powinny się ze sobą zgadzać. W przeciwnym razie należy sprawdzić, czy inne urządzenie obsługuje komunikację za pośrednictwem kodeka lub czy dostępny jest odpowiedni transkoder.</p>
Niedopasowanie wielkości próbki dźwięku między telefonem a innym urządzeniem	<p>Dane statystyczne RxSize i TxSize wskazują rozmiar pakietów dźwięku używanych do komunikacji między telefonem IP Cisco a innym urządzeniem. Wartości tych danych statystycznych powinny się ze sobą zgadzać.</p>
Stan pętli zwrotnej	<p>Stan pętli zwrotnej może wystąpić, gdy są spełnione następujące warunki:</p> <ul style="list-style-type: none"> <li>• Opcja Konfiguracja portu oprogramowania, w menu Konfiguracja sieci w telefonie ma wartość 10 Half (10-BaseT/półdupleks).</li> <li>• Telefon pobiera prąd z zewnętrznego zasilacza.</li> <li>• Telefon jest wyłączony (ma odłączony zasilacz).</li> </ul> <p>W takim przypadku port przełącznika w telefonie może zostać wyłączony. W dzienniku konsoli przełącznika pojawi się następujący komunikat:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>Aby rozwiązać ten problem, należy ponownie uaktywnić port za pomocą przełącznika.</p>

## Problemy z uruchamianiem

Po zainstalowaniu telefonu w sieci i dodaniu go do programu Cisco Unified Communications Manager telefon powinien się uruchamiać w sposób opisany w odpowiednim temacie podanym poniżej.

Jeśli telefon nie uruchamia się prawidłowo, należy poszukać w poniższych częściach informacji o rozwiązywaniu problemów.

#### Tematy pokrewne

[Sprawdzenie przy uruchamianiu telefonu](#), na stronie 66

## Telefon IP Cisco nie przechodzi przez zwykły proces uruchamiania

### Problem

Po podłączeniu telefonu IP Cisco do portu sieciowego nie przechodzi on przez zwykły proces uruchamiania w sposób opisany w odpowiednim temacie, a na jego ekranie nie są wyświetlane żadne informacje.

### Przyczyna

Jeśli telefon nie przechodzi przez zwykły proces uruchamiania, może to być spowodowane uszkodzeniem kabli, nieprawidłowym podłączeniem, awarią sieci, brakiem zasilania lub usterką telefonu.

### Rozwiązania

Aby określić, czy telefon działa prawidłowo, należy skorzystać z poniższych porad w celu wyeliminowania innych potencjalnych źródeł problemów.

- Sprawdź, czy port sieciowy działa prawidłowo:
  - Wymień kable Ethernet na takie, o których wiesz, że na pewno są sprawne.
  - Odłącz od innego portu działający prawidłowo telefon IP Cisco i podłącz go do portu sieciowego, którego funkcjonowanie chcesz sprawdzić.
  - Podłącz nieuruchamiający się telefon IP Cisco do innego portu sieciowego, o którym wiesz, że na pewno jest sprawny.
  - Podłącz nieuruchamiający się telefon IP Cisco bezpośrednio do portu w przełączniku, eliminując w ten sposób połączenie za pośrednictwem panelu krosowniczego w biurze.
- Sprawdź, czy telefon ma zasilanie:
  - Jeśli korzystasz z zewnętrznego zasilacza, sprawdź działanie gniazdka sieci elektrycznej.
  - Jeśli korzystasz z zasilania za pośrednictwem sieci LAN, użyj w zamian zewnętrznego zasilacza.
  - Jeśli korzystasz z zewnętrznego zasilacza, zamień go na egzemplarz, o którym wiesz, że na pewno jest sprawny.
- Jeśli telefon nadal nie uruchamia się prawidłowo, włącz go przy użyciu obrazu kopii zapasowej oprogramowania.
- Jeśli telefon nadal nie uruchamia się prawidłowo, przywróć w nim fabryczne ustawienia domyślne.
- Jeśli mimo wypróbowania tych rozwiązań ekran telefonu IP Cisco nadal nie wyświetla żadnych znaków po upływie co najmniej pięciu minut, należy zwrócić się o dalsze porady do przedstawiciela działu pomocy technicznej firmy Cisco.

**Tematy pokrewne**

[Sprawdzenie przy uruchamianiu telefonu](#), na stronie 66

## Telefon IP Cisco nie rejestruje się w programie Cisco Unified Communications Manager

Jeśli telefon przechodzi pierwszy etap procesu uruchamiania (miganie diod LED na przyciskach), ale później wyświetla na ekranie niekończący się cykl komunikatów, prawdopodobnie nie uruchamia się poprawnie. Telefon nie może uruchomić się całkowicie, jeśli nie połączy się z siecią Ethernet i nie zarejestruje na serwerze Cisco Unified Communications Manager.

Również problemy z zabezpieczeniami mogą uniemożliwiać poprawne uruchomienie telefonu. Więcej informacji można znaleźć w sekcji [Procedury rozwiązywania problemów, na stronie 279](#).

## Telefon wyświetla komunikaty o błędach

**Problem**

Podczas uruchamiania w komunikatach o stanie pojawiają się informacje o błędach.

**Rozwiązania**

Gdy telefon przechodzi przez proces uruchamiania, można uzyskać dostęp do komunikatów o jego stanie, które dostarczają informacji o przyczynie problemu.

**Tematy pokrewne**

[Wyświetlanie okna komunikatów o stanie](#), na stronie 231

## Telefon nie może połączyć się z serwerem TFTP ani systemem Cisco Unified Communications Manager

**Problem**

Jeśli nie działa sieć pomiędzy telefonem a serwerem TFTP lub systemem Cisco Unified Communications Manager, telefon nie uruchomi się poprawnie.

**Rozwiązania**

Zapewnij działanie sieci.

## Telefon nie może połączyć się z serwerem TFTP

**Problem**

Ustawienia serwera TFTP mogą być nieprawidłowe.

**Rozwiązania**

Sprawdź ustawienia protokołu TFTP.



**Tematy pokrewne**

[Sprawdzanie ustawień TFTP](#), na stronie 280

## Telefon nie może połączyć się z serwerem

**Problem**

Adresy IP i pola trasowania mogą być niepoprawnie skonfigurowane.

**Rozwiązania**

Należy sprawdzić adresy IP i ustawienia trasowania na telefonie. Jeśli jest używany protokół DHCP, prawidłowe wartości powinien dostarczyć serwer DHCP. Jeśli do telefonu jest przypisany statyczny adres IP, należy ręcznie wprowadzić te wartości.

## Telefon nie może nawiązać połączenia z użyciem serwera DNS

**Problem**

Ustawienia serwera DNS mogą być nieprawidłowe.

**Rozwiązania**

W przypadku korzystania z serwera DNS do uzyskiwania dostępu do serwera TFTP lub do serwera Cisco Unified Communications Manager należy sprawdzić, czy wskazano serwer DNS.

## Nie są uruchomione usługi Cisco Unified Communications Manager ani TFTP

**Problem**

Jeśli usługi Cisco Unified Communications Manager lub TFTP nie są uruchomione, telefony mogą nie uruchamiać się poprawnie. W takiej sytuacji prawdopodobnie ma miejsce awaria całego systemu i nie uruchamiają się również inne telefony oraz urządzenia.

**Rozwiązania**

Jeśli usługa Cisco Unified Communications Manager nie jest uruchomiona, wpływa to na wszystkie urządzenia w sieci, które potrzebują jej do nawiązywania połączeń telefonicznych. Jeśli nie jest uruchomiona usługa TFTP, wiele urządzeń nie uruchamia się poprawnie. Aby uzyskać więcej informacji, patrz [Uruchamianie usługi](#), na stronie 283.

## Uszkodzenie pliku konfiguracyjnego

**Problem**

Jeśli inne wskazówki podane w tym rozdziale nie pozwoliły rozwiązać problemów z danym telefonem, być może uszkodzony jest plik konfiguracyjny.

**Rozwiązania**

Utwórz nowy plik konfiguracyjny telefonu.

## Rejestrowanie telefonu w programie Cisco Unified Communications Manager

**Problem**

Telefon nie jest zarejestrowany w programie Cisco Unified Communications Manager.

**Rozwiązania**

Telefon IP Cisco może zarejestrować się w programie Cisco Unified Communications Manager wyłącznie wtedy, gdy został dodany do serwera lub też włączona została opcja rejestracji automatycznej. Zapoznaj się z informacjami i procedurami w sekcji [Metody dodawania telefonów, na stronie 73](#), aby upewnić się, że telefon został dodany do bazy danych programu Cisco Unified Communications Manager.

Aby sprawdzić, czy telefon znajduje się w bazie danych programu Cisco Unified Communications Manager, wybierz kolejno opcje **Urządzenie > Telefon** w narzędziu Cisco Unified Communications Manager — administracja. Kliknij przycisk **Znajdź**, aby wyszukać telefon na podstawie jego adresu MAC. Informacje o ustalaniu adresu MAC można znaleźć w sekcji [Sprawdzanie adresu MAC telefonu, na stronie 72](#).

Jeśli telefon jest już w bazie danych programu Cisco Unified Communications Manager, może to oznaczać uszkodzenie pliku konfiguracyjnego. W celu uzyskania pomocy zobacz temat [Uszkodzenie pliku konfiguracyjnego, na stronie 271](#).

## Telefon IP Cisco nie może uzyskać adresu IP

**Problem**

Jeśli telefon nie może przy uruchamianiu uzyskać adresu IP, prawdopodobnie znajduje się w innej fizycznej lub wirtualnej sieci LAN niż serwer DHCP albo port przełącznika, do którego jest podłączony, został wyłączony.

**Rozwiązania**

Upewnij się, że fizyczna lub wirtualna sieć LAN, z którą łączy się telefon, ma dostęp do serwera DHCP, a port przełącznika jest włączony.

## Telefon się nie rejestruje

**Problem**

Na ekranie telefonu jest wyświetlany monit „Wprowadź kod aktywacyjny lub domenę usługi”.

**Rozwiązania**

Telefon nie ma adresu serwera TFTP. Sprawdź, czy serwer DHCP ma opcję 150 lub czy alternatywny serwer TFTP jest skonfigurowany ręcznie.

## Problemy z resetowaniem się telefonu

Jeśli użytkownicy zgłaszają, że ich telefony zerują się w trakcie połączeń lub w czasie bezczynności, należy zbadać przyczynę tego zjawiska. Jeśli połączenie z siecią i programem Cisco Unified Communications Manager jest stabilne, telefon nie powinien się zerować.

Zwykle zerowanie się telefonu oznacza, że ma on problemy z nawiązaniem połączenia z siecią lub z programem Cisco Unified Communications Manager.

### Telefon resetuje się z powodu chwilowych przerw w działaniu sieci

#### Problem

Być może sieć miewa chwilowe przerwy w działaniu.

#### Rozwiązania

Chwilowe awarie sieci w różny sposób wpływają na przesyłanie danych i mowy. W sieci mogą występować chwilowe, niewykrywalne awarie. W takim przypadku utracone pakiety danych mogą zostać przesłane ponownie, a operacje wysyłania i odbioru pakietów są potwierdzane. Jednak podczas przesyłania głosu nie można odtworzyć utraconych pakietów. Po utracie połączenia sieciowego następuje zerowanie telefonu i próba odzyskania połączenia zamiast próby ponownego przesłania pakietów. Należy dowiedzieć się od administratora systemu, czy nie występują jakieś znane problemy z siecią transmisji głosowej.

### Telefon resetuje się z powodu błędnych ustawień serwera DHCP

#### Problem

Ustawienia serwera DHCP mogą być nieprawidłowe.

#### Rozwiązania

Należy sprawdzić, czy prawidłowo skonfigurowano w telefonie korzystanie z serwera DHCP. Należy sprawdzić, czy prawidłowo skonfigurowano serwer DHCP. Należy sprawdzić czas trwania dzierżawy serwera DHCP. Zalecamy ustawienie czasu trwania dzierżawy na 8 dni.

### Telefon resetuje się z powodu nieprawidłowego statycznego adresu IP

#### Problem

Przydzielony telefonowi statyczny adres IP może być nieprawidłowy.

#### Rozwiązania

Jeśli telefon ma przydzielony statyczny adres IP, sprawdź, czy ustawienia są poprawne.

## Telefon resetuje się podczas dużego obciążenia sieci

### Problem

Jeśli telefon resetuje się podczas dużego obciążenia sieci, możliwe, że nie jest skonfigurowana sieć VLAN transmisji głosowej.

### Rozwiązania


Oddzielenie telefonów od pozostałych urządzeń sieciowych w ramach osobnej pomocniczej sieci VLAN polepsza jakość obsługi połączeń głosowych.

## Telefon resetuje się z powodu celowego zresetowania

### Problem

Jeśli nie jesteś jedynym administratorem mającym dostęp do programu Cisco Unified Communications Manager, należy sprawdzić, czy nikt inny nie zresetował celowo telefonów.

### Rozwiązania

Sprawdź, czy telefon IP Cisco otrzymał polecenie z programu Cisco Unified Communications Manager, naciskając na telefonie przycisk **Aplikacje**  i wybierając kolejno opcje **Ustawienia administratora** > **Stan** > **Statystyka sieci**.

- Jeśli w polu Przyczyna restartu jest wyświetlana opcja **Reset-Reset**, telefon otrzymał polecenie zresetowania z narzędzia Cisco Unified Communications Manager — administracja.
- Jeśli w polu Przyczyna restartu jest wyświetlana opcja **Reset-Restart**, telefon zakończył pracę z powodu otrzymania polecenia zresetowania i ponownego uruchomienia z narzędzia systemu Cisco Unified Communications Manager — administracja.

## Telefon resetuje się z powodu problemu z serwerem DNS lub innych problemów z łącznością

### Problem

Telefon nadal się resetuje, co może wynikać z problemów z serwerem DNS lub innych problemów z łącznością.

### Rozwiązania

Jeśli telefon cały czas się resetuje, wyklucz występowanie problemów z serwerem DNS lub łącznością, wykonując czynności opisane w sekcji [Identyfikowanie problemów z systemem DNS lub łącznością, na stronie 281](#).

## Telefon nie włącza się

### Problem

Telefon nie włącza się.

### Rozwiązania

W większości przypadków telefon uruchomi się ponownie, jeśli utraci połączenie z zewnętrznym zasilaczem, z którego pobiera prąd, i przełączy się na zasilanie PoE. Podobnie telefon może uruchomić się ponownie, jeśli utraci zasilanie PoE i przełączy się na zasilacz zewnętrzny.

## Telefon nie może się połączyć z siecią LAN

### Problem

Uszkodzone może być fizyczne połączenie z siecią LAN.

### Rozwiązania

Sprawdź, czy działa połączenie Ethernet, z którego korzysta telefon IP Cisco. Na przykład sprawdź, czy działa port lub przełącznik, do którego jest podłączony telefon, i czy nie trwa akurat ponowne uruchamianie przełącznika. Sprawdź też, czy nie jest uszkodzony żaden kabel.

## Problemy z zabezpieczeniami telefonu IP Cisco

W poniższych sekcjach podano informacje na temat rozwiązywania problemów z zabezpieczeniami telefonu IP Cisco. Informacje na temat eliminowania tych nieprawidłowości i omówienie dodatkowych kwestii związanych z zabezpieczeniami można znaleźć w *Cisco Unified Communications Manager Security Guide (Podręczniku zabezpieczeń programu Cisco Unified Communications Manager)*.

## Problemy z plikiem CTL

W poniższej sekcji opisano rozwiązywanie problemów z plikiem CTL.

### Błąd uwierzytelniania, telefon nie może uwierzytelnić pliku CTL

#### Problem

Występuje błąd uwierzytelniania urządzenia.

#### Przyczyna

Plik CTL nie zawiera certyfikatu systemu Cisco Unified Communications Manager lub ma nieprawidłowy certyfikat.

**Rozwiązania**

Zainstaluj prawidłowy certyfikat.

**Telefon nie może uwierzytelnić pliku CTL****Problem**

Telefon nie może uwierzytelnić pliku CTL.

**Przyczyna**

Token zabezpieczający przypisany do zaktualizowanego pliku CTL nie występuje w pliku CTL w telefonie.

**Rozwiązania**

Należy zmienić token zabezpieczający w pliku CTL i zainstalować w telefonie nowy plik.

**Plik CTL jest uwierzytelniony, ale inne pliki konfiguracyjne nie są****Problem**

Telefon nie może wykonać uwierzytelnienia żadnych plików konfiguracyjnych oprócz pliku CTL.

**Przyczyna**

Istnieje błędny rekord TFTP albo plik konfiguracyjny nie jest podpisany przy użyciu odpowiedniego certyfikatu z listy zaufanych w telefonie.

**Rozwiązania**

Sprawdź rekord TFTP i certyfikat na liście zaufanych.

**Plik ITL jest uwierzytelniony, ale inne pliki konfiguracyjne nie są****Problem**

Telefon nie może wykonać uwierzytelnienia żadnych plików konfiguracyjnych oprócz pliku ITL.

**Przyczyna**

Plik konfiguracyjny nie jest podpisany przy użyciu odpowiedniego certyfikatu z listy zaufanych w telefonie.

**Rozwiązania**

Należy ponownie podpisać plik konfiguracyjny przy użyciu prawidłowego certyfikatu.

**Uwierzytelnianie serwera TFTP nie powiodło się****Problem**

Telefon zgłasza niepowodzenie uwierzytelniania serwera TFTP.

**Przyczyna**

Adres serwera TFTP przeznaczonego do telefonu nie występuje w pliku CTL w telefonie.

Jeśli utworzono nowy plik CTL z nowym rekordem serwera TFTP, plik CTL znajdujący się w telefonie może nie zawierać rekordu odpowiedniego dla nowego serwera TFTP.

**Rozwiązania**

Należy sprawdzić konfigurację adresu serwera TFTP w pliku CTL telefonu.

**Telefon nie rejestruje się****Problem**

Telefon nie rejestruje się w programie Cisco Unified Communications Manager.

**Przyczyna**

Plik CTL nie zawiera prawidłowych informacji o serwerze programu Cisco Unified Communications Manager.

**Rozwiązania**

Należy zmienić w pliku CTL informacje o serwerze programu Cisco Unified Communications Manager.

**Telefon nie żąda podpisanych plików konfiguracyjnych****Problem**

Telefon nie żąda podpisanych plików konfiguracyjnych.

**Przyczyna**

Plik CTL nie zawiera żadnych pozycji dotyczących serwerów TFTP z certyfikatami.

**Rozwiązania**

Skonfiguruj w pliku CTL pozycje dotyczące serwerów TFTP z certyfikatami.

**Problemy z połączeniem wideo****Brak wideo między dwoma telefonami wideo IP Cisco****Problem**

Brak strumieniowania wideo między dwoma telefonami wideo IP Cisco.

**Rozwiązania**

Sprawdź, czy na pewno żaden punkt zakończenia mediów (MTP) nie jest używany w przepływie połączeń.

## Brak płynności obrazu i gubienie ramek

### Problem

W trakcie połączenia wideo ramki są buforowane lub gubione.

### Rozwiązania

Jakość obrazów zależy od przepustowości połączenia. Zwiększenie szybkości transmisji poprawia jakość wideo, ale wymaga dodatkowych zasobów sieci. Zawsze należy używać szybkości transmisji bitów najlepiej dopasowanej do typu wideo. Połączenie wideo w standardzie 720p o prędkości 15 ramek na sekundę wymaga szybkości transmisji 790 Kb/s lub większej. Połączenie wideo w standardzie 720p o prędkości 30 ramek na sekundę wymaga szybkości transmisji 1360 Kb/s lub większej.

Dodatkowe informacje o przepustowości można znaleźć w sekcji Ustawienia rozdzielczości transmisji wideo, rozdział „Funkcje i ustawienia telefonu”.

### Rozwiązania

Upewnij się, że parametr Maksymalna szybkość transmisji bitowej połączenia wideo ma wartość nie mniejszą niż minimalna szybkość transmisji bitowej wideo. W programie Cisco Unified Communications Manager przejdź do opcji **System > Informacje o regionie > Region**.

## Nie można przekierować połączenia wideo

### Problem

Nie można przekierować połączenia wideo z telefonu stacjonarnego na urządzenie przenośne.

### Rozwiązania

Usługa Cisco Unified Mobility nie obejmuje połączeń wideo. Połączenia wideo, które są odbierane w telefonie biurkowym, nie mogą zostać pobrane na telefon komórkowy.

## Brak transmisji obrazu podczas połączenia konferencyjnego

### Problem

Połączenie wideo zmienia się w połączenie dźwiękowe po dodaniu dwóch lub więcej osób do połączenia.

Do połączeń wideokonferencyjnych ad hoc i Meet-me należy użyć mostka konferencji wideo.

## Ogólne problemy z połączeniami telefonicznymi

W poniższych sekcjach opisano rozwiązywanie ogólnych problemów z połączeniami telefonicznymi.



## Nie można zestawić połączenia telefonicznego

### Problem

Użytkownik zgłasza, że nie może wykonywać połączeń.

### Przyczyna

Telefon nie ma adresu IP z serwera DHCP, nie jest w stanie zarejestrować się w programie Cisco Unified Communications Manager. Na telefonach z wyświetlaczem LSD prezentowany jest komunikat *Konfigurowanie IP lub Rejestrowanie*. W przypadku telefonów bez wyświetlacza LSD w chwili, gdy użytkownik próbuje wykonać połączenie, w słuchawce odtwarzany jest sygnał zmiany ustawień (zamiast sygnału wybierania).

### Rozwiązania

1. Sprawdź, czy:
  1. Kabel Ethernet jest podłączony.
  2. Usługa Cisco CallManager jest uruchomiona na serwerze programu Cisco Unified Communications Manager.
  3. Oba telefony są zarejestrowane w tym samym systemie Cisco Unified Communications Manager.
2. Debugowanie i dzienniki przechwytywania serwera dźwiękowego są włączone dla obu telefonów. Jeśli to konieczne, włącz debugowanie Java.

## Telefon nie rozpoznaje cyfr DTMF lub cyfry są opóźnione

### Problem

Użytkownik zgłasza, że cyfry są pomijane lub opóźnione podczas korzystania z klawiatury numerycznej.

### Przyczyna

Zbyt szybkie naciskanie klawiszy może prowadzić do pomijania lub opóźnienia cyfr.

### Rozwiązania

Nie należy naciskać klawiszy zbyt szybko.

## Procedury rozwiązywania problemów

Procedury te służą do identyfikowania i eliminowania problemów.

## Tworzenie raportu o problemie z telefonem w programie Cisco Unified Communications Manager

W programie Cisco Unified Communications Manager można generować raporty o problemach z telefonami. Działanie to wygeneruje takie same informacje jak narzędzie do zgłaszania problemów (PRT) uruchamiane klawiszem programowym na telefonie.

Raport o problemie zawiera informacje o telefonie i zestawach słuchawkowych.

### Procedura

---

- Krok 1** W programie Cisco Unified — administracja CM wybierz kolejno **Urządzenie > Telefon**.
  - Krok 2** Kliknij **Znajdź** i wybierz co najmniej jeden telefon IP Cisco.
  - Krok 3** Kliknij **Utwórz raport PRT**, aby zarejestrować dzienniki PRT dla zestawów słuchawkowych używanych z wybranymi telefonami IP Cisco.
- 

## Tworzenie dziennika konsoli za pomocą telefonu


Dziennik konsoli jest generowany, gdy telefon nie nawiąże połączenia z siecią i nie można uzyskać dostępu do narzędzia do zgłaszania problemów (PRT).

### Zanim rozpoczniesz

Podłącz kabel konsoli do portu pomocniczego z tyłu telefonu.

### Procedura


---

- Krok 1** W telefonie naciśnij przycisk **Aplikacje** .
  - Krok 2** Przejdź **Ustawień administracyjnych > Portu pomocniczego**.
  - Krok 3** Wybierz opcję **Zbierz dziennik konsoli**, aby zebrać dzienniki urządzeń.
- 

## Sprawdzanie ustawień TFTP

### Procedura

---

- Krok 1** W telefonie IP Cisco naciśnij przycisk **Aplikacje** , a następnie wybierz kolejno opcje **Ustawienia admin. > Konfiguracja sieci > Konfiguracja sieci Ethernet > Konfiguracja protokołu IPv4 > Serwer TFTP 1**.
- Krok 2** Jeśli do telefonu jest przypisany statyczny adres IP, należy ręcznie wprowadzić ustawienie dla opcji Serwer TFTP 1.

- Krok 3** Jeśli używasz protokołu DHCP, telefon otrzymuje adres serwera TFTP z serwera DHCP. Sprawdź, czy adres IP jest skonfigurowany w opcji 150.
- Krok 4** Możesz również zezwolić telefonowi na korzystanie z alternatywnego serwera TFTP. Takie ustawienie jest szczególnie przydatne, jeśli telefon ostatnio przenoszono między lokalizacjami.
- Krok 5** Jeśli lokalny serwer DHCP nie podaje prawidłowego adresu serwera TFTP, włącz telefon, aby skorzystać z alternatywnego serwera TFTP.
- Jest to konieczne w przypadku korzystania z sieci VPN.

## Identyfikowanie problemów z systemem DNS lub łącznością

### Procedura

- Krok 1** Przywróć wartości domyślne ustawień telefonu, korzystając z menu **Resetuj ustawienia**.
- Krok 2** Zmień ustawienia protokołów DHCP i IP:
- Wyłącz protokół DHCP.
  - Przypisz telefonowi statyczny adres IP. Zastosuj to samo domyślne ustawienie routera, z którego korzystają inne telefony.
  - Przypisz serwer TFTP. Zastosuj ten sam serwer TFTP, z którego korzystają inne telefony.
- Krok 3** Sprawdź na serwerze Cisco Unified Communications Manager, czy pliki hostów lokalnych zawierają prawidłową nazwę serwera Cisco Unified Communications Manager przypisaną do właściwego adresu IP.
- Krok 4** W programie Cisco Unified Communications Manager wybierz kolejno opcje **System > Serwer** i sprawdź, czy odwołanie do serwera odbywa się poprzez adres IP, a nie poprzez nazwę DNS.
- Krok 5** W programie Cisco Unified Communications Manager wybierz kolejno opcje **Urządzenie > Telefon**. Kliknij przycisk **Znajdź**, aby wyszukać telefon. Sprawdź, czy telefonowi IP Cisco został przypisany prawidłowy adres MAC.
- Krok 6** Wyłącz telefon i włącz go ponownie.


### Tematy pokrewne

[Resetowanie podstawowe](#), na stronie 287

[Sprawdzanie adresu MAC telefonu](#), na stronie 72

## Sprawdzanie ustawień DHCP

### Procedura

- Krok 1** Naciśnij przycisk **Aplikacje**  w telefonie.
- Krok 2** Wybierz kolejno opcje **Wi-Fi > Konfiguracja sieci > Konfiguracja protokołu IPv4** i spójrz na następujące opcje:

- Serwer DHCP: jeśli telefon ma przypisany statyczny adres IP, nie trzeba ręcznie wprowadzać wartości opcji Serwer DHCP. Jeśli natomiast jest używany serwer DHCP, ta opcja musi mieć wartość. W przypadku braku wartości sprawdź konfigurację routingu IP i sieci VLAN. Zobacz dokument *Troubleshooting Switch Port and Interface Problems* (Rozwiązywanie problemów z interfejsami i portami przełączników) pod tym adresem URL:

[http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html)

- Adres IP, Maska podsieci, Router domyślny: jeśli telefon ma przypisany statyczny adres IP, należy ręcznie wprowadzić ustawienia tych opcji.

**Krok 3** Jeśli używany jest protokół DHCP, sprawdź adresy IP przydzielane przez serwer DHCP.

Zobacz dokument *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* (Rozpoznawanie i rozwiązywanie problemów z protokołem DHCP w przełącznikach Catalyst i sieciach firmowych) pod tym adresem URL:

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a00800f0804.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml)

## Tworzenie nowego pliku konfiguracyjnego telefonu

Po usunięciu telefonu z bazy danych Cisco Unified Communications Manager następuje skasowanie jego pliku konfiguracyjnego z serwera TFTP programu Cisco Unified Communications Manager. Numer lub numery telefonu pozostają w bazie danych Cisco Unified Communications Manager. Trafiają one do puli nieprzypisanych numerów telefonu, których można używać dla innych urządzeń. Jeśli nieprzypisane numery telefonu nie są używane dla innych urządzeń, należy je usunąć z bazy danych Cisco Unified Communications Manager. Korzystając z raportu planów tras, można wyświetlać i usuwać nieprzypisane numery telefonu. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Zmiana przycisków w szablonie przycisków telefonu lub przypisanie do telefonu innego szablonu przycisków może spowodować, że niektóre numery telefonu przestaną być dostępne w telefonie. Takie numery telefonu są wprawdzie nadal przypisane do telefonu w bazie danych Cisco Unified Communications Manager, ale na telefonie nie ma przycisku, którym można by odbierać przychodzące na nie połączenia. Takie numery telefonu należy w razie potrzeby usuwać z telefonu i bazy danych.

### Procedura

**Krok 1** W programie Cisco Unified Communications Manager wybierz kolejno opcje **Urządzenie > Telefon** i kliknij przycisk **Znajdź**, aby odnaleźć telefon, którego dotyczą problemy.

**Krok 2** Wybierz opcję **Usuń**, aby usunąć telefon z bazy danych Cisco Unified Communications Manager.

**Uwaga** Po usunięciu telefonu z bazy danych Cisco Unified Communications Manager następuje skasowanie jego pliku konfiguracyjnego z serwera TFTP programu Cisco Unified Communications Manager. Numer lub numery telefonu pozostają w bazie danych Cisco Unified Communications Manager. Trafiają one do puli nieprzypisanych numerów telefonu, których można używać dla innych urządzeń. Jeśli nieprzypisane numery telefonu nie są używane dla innych urządzeń, należy je usunąć z bazy danych Cisco Unified Communications Manager. Korzystając z raportu planów tras, można wyświetlać i usuwać nieprzypisane numery telefonu.

**Krok 3** Ponownie dodaj telefon do bazy danych Cisco Unified Communications Manager.

**Krok 4** Wyłącz telefon i włącz go ponownie.

---

#### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

[Metody dodawania telefonów](#), na stronie 73

## Identyfikowanie problemów z uwierzytelnianiem 802.1X

---

#### Procedura

**Krok 1** Sprawdź, czy prawidłowo skonfigurowano wymagane elementy.

**Krok 2** Upewnij się, że w telefonie skonfigurowano klucz współdzielony.

- Jeśli klucz współdzielony jest skonfigurowany, sprawdź, czy ten sam klucz znajduje się na serwerze uwierzytelniania.
- Jeśli klucz współdzielony nie jest skonfigurowany w telefonie, wprowadź go i upewnij się, że jest on zgodny z kluczem znajdującym się na serwerze uwierzytelniania.


---

## Sprawdzanie ustawień DNS

Aby sprawdzić ustawienia DNS, wykonaj poniższe czynności:

---

#### Procedura

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

**Krok 2** Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja protokołu IPv4** > **Serwer DNS 1**.

**Krok 3** Należy również sprawdzić, czy w serwerze DNS znajduje się wpis CNAME dla serwera TFTP i dla systemu Cisco Unified Communications Manager.

Należy również upewnić się, że usługa DNS jest skonfigurowana do wyszukiwania wstecznego.

---

## Uruchamianie usługi

Aby można było uruchamiać i zatrzymywać usługę, należy ją najpierw aktywować.

### Procedura

---

- Krok 1** W aplikacji Cisco Unified Communications Manager — administracja wybierz opcję **Serwisowanie systemu Cisco Unified** z listy rozwijanej Nawigacja i kliknij przycisk **Go** (Przejdź).
- Krok 2** Kliknij kolejno opcje **Narzędzia > Control Center - Feature Services** (Centrum kontrolne — usługi funkcji).
- Krok 3** Wybierz główny serwer Cisco Unified Communications Manager z listy rozwijanej Serwer.  
Zostanie wyświetlone okno z nazwami usług na wybranym serwerze, stanem tych usług oraz panelem sterowania usługami umożliwiającym ich uruchamianie i zatrzymywanie.
- Krok 4** Jeśli usługa jest zatrzymana, kliknij jej przycisk radiowy, a następnie przycisk **Uruchom**.  
Symbol stanu usługi zmieni się z kwadratu na strzałkę.
- 

## Informacje kontrolne debugowania z programu Cisco Unified Communications Manager

W przypadku problemów z telefonem, których nie potrafisz rozwiązać, możesz uzyskać pomoc w Centrum pomocy technicznej Cisco (TAC). Konieczne będzie włączenie funkcji debugowania na telefonie, ponowne wygenerowanie problemu, wyłączenie funkcji debugowania i wysłanie zapisów z dzienników do centrum TAC w celu przeprowadzenia analizy.

Ponieważ funkcja debugowania przechwytuje szczegółowe informacje, ruch komunikacyjny może spowolnić telefon, powodując, że będzie gorzej odpowiadał. Po przechwyceniu zapisów z dzienników należy wyłączyć funkcję debugowania, aby zapewnić normalne działanie telefonu.

Informacje debugowania mogą zawierać jednocyfrowy kod, który odzwierciedla stopień dotkliwości sytuacji. Sytuacje są oceniane w następujący sposób:

- 0 — alarmowa
- 1 — alert
- 2 — krytyczna
- 3 — błąd
- 4 — ostrzeżenie
- 5 — powiadomienie
- 6 — informacja
- 7 — debugowanie

Skontaktuj się z centrum Cisco TAC w celu uzyskania dodatkowych informacji i pomocy.

## Procedura

---

**Krok 1** W narzędziu Cisco Unified Communications Manager — administracja wybierz jedno z następujących okien:

- **Urządzenie > Ustawienia urządzenia > Wspólny profil telefonu**
- **System > Firmowa konfiguracja telefonów**
- **Urządzenie > Telefon**

**Krok 2** Ustaw następujące parametry:

- Profile dziennika — wartości: Stan początkowy (domyślne), Domyślne, Telefonia, SIP, UI, Sieć, Multimedia, Uaktualnienie, Akcesorium, Bezpieczeństwo, Wi-Fi, VPN, Energywise, MobileRemoteAccess (Przenośny zdalny dostęp)

**Uwaga** Aby zaimplementować wielopoziomową i wielosekcyjną obsługę parametrów, zaznacz pole wyboru Profil dziennika.

- Zdalny dziennik — wartości: Wyłącz (domyślne), Włącz
- Serwer rejestrowania IPv6 lub Serwer rejestrowania — adres IP (adres IPv4 lub IPv6)

**Uwaga** Gdy nie będzie można uzyskać dostępu do Serwera rejestrowania, telefon zatrzyma wysyłanie komunikatów debugowania.

- Format adresu IPv4 Serwera rejestrowania jest następujący  
**adres : <port>@<base=<0-7>;pfs=<0-1>**
- Format adresu IPv6 Serwera rejestrowania jest następujący  
**[adres] : <port>@<base=<0-7>;pfs=<0-1>**
- Gdzie:
  - elementy adresu IPv4 są rozdzielone kropką (.)
  - elementy adresu IPv6 są rozdzielone dwukropkiem (:)

---

## Dodatkowe informacje o sposobach rozwiązywania problemów

Jeśli masz inne pytania dotyczące rozwiązywania problemów z telefonem, otwórz poniższą witrynę firmy Cisco i znajdź tam swój model telefonu:

<https://www.cisco.com/cisco/web/psa/troubleshoot.html>







# ROZDZIAŁ 13

## Konserwacja




- Resetowanie podstawowe, na stronie 287
- Resetowanie konfiguracji sieci, na stronie 289
- Resetowanie konfiguracji sieci użytkownika, na stronie 289
- Usuwanie pliku CTL, na stronie 290
- Quality Report Tool, na stronie 290
- Monitorowanie jakości dźwięku, na stronie 290
- Czyszczenie telefonu IP Cisco, na stronie 292

## Resetowanie podstawowe

Podstawowe zerowanie telefonu IP Cisco umożliwia przywrócenie jego prawidłowego działania po wystąpieniu błędu oraz wyzerowanie lub odtworzenie różnych ustawień konfiguracji i zabezpieczeń.

W poniższej tabeli opisano sposoby przeprowadzenia zerowania podstawowego. Po uruchomieniu telefonu można go wyzerować, wykonując dowolną z podanych niżej procedur. Należy wybrać procedurę odpowiednią do danej sytuacji.

**Tabela 54: Metody zerowania podstawowego**

Działanie	Czynność	Objas
Ponowne uruchomienie telefonu	Naciśnij przycisk <b>Aplikacje</b>  . Przejdź do opcji <b>Ustawienia admin.</b> > <b>Resetuj ustawienia</b> > <b>Resetuj urządzenie</b> .	Powroc sieci, zapis
Resetuj ustawienia	Aby zresetować ustawienia, naciśnij przycisk <b>Aplikacje</b>  i wybierz kolejno opcje <b>Ustawienia admin.</b> > <b>Resetuj ustawienia</b> > <b>Sieć</b> .	Spow oraz
	Aby zresetować plik CTL, naciśnij przycisk <b>Aplikacje</b>  i wybierz kolejno opcje <b>Ustawienia admin.</b> > <b>Resetuj ustawienia</b> > <b>Zabezpieczenia</b> .	Powoc

## Przywracanie fabrycznych ustawień telefonu z klawiatury telefonu

W telefonie można przywrócić ustawienia fabryczne. Resetowanie powoduje wyczyszczenie wszystkich parametrów telefonu.

### Procedura

---

**Krok 1** Odłącz zasilanie telefonu w jeden z następujących sposobów:

- Odłącz zasilacz.
- Odłącz kabel sieci LAN.

**Krok 2** Odczekaj 5 sekund.

**Krok 3** Naciśnij i przytrzymaj #, a następnie podłącz telefon z powrotem. Zwolnij # tylko wtedy, gdy przyciski **zestawu słuchawkowego** i **głośnika** są podświetlone.

**Uwaga** W niektórych wersjach sprzętowych po ponownym podłączeniu telefonu do gniazdka przycisk **Wyciesznia** świeci się razem z przyciskami **Słuchawki** i **Głośnika**. W takim przypadku poczekaj, aż wszystkie one zgasną i puść # dopiero wtedy, gdy przyciski **Słuchawki** i **Głośnika** ponownie się zaświecą.

**Krok 4** Wprowadź następującą kombinację klawiszy:

**123456789\*0#**

Przycisk **Zestaw nagłowny** przestanie świecić po naciśnięciu klawisza **1**. Po wprowadzeniu sekwencji klawiszy zaświeci się przycisk **Wycisz**.

**Przeostroga** Nie należy wyłączać zasilania telefonu, dopóki nie zakończy procedury przywracania fabrycznych ustawień domyślnych i nie pojawi się jego ekran główny.

Telefon zostanie zresetowany.


---

## Resetowanie wszystkich ustawień za pomocą menu telefonu

Wykonaj to zadanie, jeśli chcesz przywrócić wartości domyślne ustawień użytkowników i konfiguracji sieci.

### Procedura

---

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

**Krok 2** Wybierz kolejno opcje **Ustawienia administratora** > **Resetuj ustawienia** > **Wszystkie ustawienia**.

Jeśli jest to wymagane, odblokuj opcje telefonu.

---

## Ponowne uruchamianie telefonu przy użyciu obrazu kopii zapasowej

Telefon IP Cisco ma drugi, zapasowy obraz, który umożliwia odzyskanie telefonu w przypadku uszkodzenia obrazu domyślnego.

Aby uruchomić ponownie telefon przy użyciu obrazu kopii zapasowej, należy wykonać następujące czynności.

### Procedura

---

- Krok 1** Odłącz zasilacz.
  - Krok 2** Naciśnij i przytrzymaj klawisz gwiazdki (\*).
  - Krok 3** Ponownie podłącz zasilanie. Naciskaj klawisz gwiazdki, aż dioda LED wyciszenia zgaśnie.
  - Krok 4** Zwolnij klawisz gwiazdki.  
Telefon zostanie ponownie uruchomiony przy użyciu obrazu kopii zapasowej.
- 

## Resetowanie konfiguracji sieci

Powoduje przywrócenie domyślnych wartości ustawień konfiguracji sieci i zresetowanie telefonu. Ta metoda powoduje, że usługa DHCP ponownie konfiguruje adres IP telefonu.

### Procedura

---

- Krok 1** W razie potrzeby odblokuj opcje telefonu w menu Ustawienia admin.
  - Krok 2** Wybierz kolejno opcje **Resetuj ustawienia** > **Konfiguracja sieci**.
- 

## Resetowanie konfiguracji sieci użytkownika

Powoduje zresetowanie wszelkich wprowadzonych zmian w konfiguracji użytkownika i sieci, które nie zostały zapisane w pamięci flash telefonu, czyli przywrócenie poprzednio zapisanych ustawień.

### Procedura

---

- Krok 1** W razie potrzeby odblokuj opcje telefonu w menu Ustawienia admin.
  - Krok 2** Wybierz kolejno opcje **Resetuj ustawienia** > **Resetuj urządzenie**.
-

## Usuwanie pliku CTL

Umożliwia usuwanie z telefonu samego pliku CTL.

### Procedura

- 
- Krok 1** W razie potrzeby odblokuj opcje telefonu w menu Ustawienia admin.
- Krok 2** Wybierz kolejno opcje **Resetuj ustawienia** > **Ustawienia zabezpieczeń**.
- 

## Quality Report Tool

Quality Report Tool (QRT) to narzędzie do tworzenia raportów o jakości dźwięku i ogólnych problemach, przeznaczone dla telefonów IP Cisco. Narzędzie QRT jest instalowane razem z oprogramowaniem Cisco Unified Communications Manager.

Telefony IP Cisco użytkowników można skonfigurować do współpracy z narzędziem QRT. Dzięki temu użytkownicy będą mogli zgłaszać problem z połączeniami telefonicznymi, naciskając przycisk Raport dotyczący jakości. Ten klawisz programowy lub przycisk jest dostępny tylko wtedy, gdy telefon IP Cisco jest w stanie Connected (Połączono), Connected Conference (Połączono — konferencja), Connected Transfer (Połączono — przekazanie) lub OnHook (Odłożona słuchawka).

Gdy użytkownik naciśnie przycisk Raport dotyczący jakości, zostanie wyświetlona lista kategorii problemów. Po wybraniu kategorii problemu dane z telefonu użytkownika zostaną zapisane w pliku XML. To, jakie dokładnie informacje zostaną zapisane, zależy od wybranej przez użytkownika kategorii i tego, czy urządzenie docelowe jest telefonem IP Cisco.

Więcej informacji o korzystaniu z narzędzia QRT można znaleźć w dokumentacji używanej wersji oprogramowania Cisco Unified Communications Manager.

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Monitorowanie jakości dźwięku

Do pomiaru jakości dźwięku połączeń wysyłanych i odbieranych w sieci telefony Cisco IP Phone wykorzystują poniższe metryki statystyczne oparte na zdarzeniach ukrywania. Mechanizm cyfrowego przetwarzania dźwięku (DSP) odtwarza ramki ukrywania, aby zamaskować utratę ramek w strumieniu pakietów dźwięku.

- Metryki współczynnika ukrywania — pokazują stosunek liczby ramek ukrywania do łącznej liczby ramek przenoszących dźwięk. Interwałowy współczynnik ukrywania jest obliczany co 3 sekundy.
- Metryki sekund ukrywania — pokazują czas w sekundach, przez który mechanizm DSP odtwarza ramki ukrywania z powodu utraty ramek. Poważnie "ukryta sekunda" to sekunda, w której ponad pięć procent ramek to ramki ukrywania.



**Uwaga** Współczynnik ukrywania i sekundy ukrywania to główne miary oparte na utracie ramek. Współczynnik ukrywania równy zero oznacza, że sieć IP dostarcza ramki i pakiety na czas bez żadnych strat.

Metryki jakości dźwięku są dostępne w telefonie IP Cisco na ekranie Statystyki połączeń oraz zdalnie w narzędziu Statystyki strumieniowania.

## Wskazówki dotyczące rozwiązywania problemów z jakością dźwięku

W przypadku zauważenia dużych i trwałych zmian metryk należy skorzystać z podanych w poniższej tabeli ogólnych informacji o sposobach rozwiązywania problemów.

*Tabela 55: Zmiany metryk jakości dźwięku*

Zmiana metryki	Warunek
Znaczny wzrost współczynnika ukrywania i sekund ukrywania	Problemy z działaniem sieci polegające na utracie pakietów lub dużymi wahaniami opóźnień.
Współczynnik ukrywania jest bliski lub równy zeru, ale jakość dźwięku jest niska.	<ul style="list-style-type: none"> <li>• Szumy lub zniekształcenia dźwięku, takie jak echo lub zmiany poziomu.</li> <li>• Połączenia z wieloma etapami kodowania i dekodowania, takie jak połączenia z telefonami komórkowymi lub telefonami na kartę.</li> <li>• Problemy akustyczne powodowane przez telefon głośnomówiący, telefon komórkowy w trybie głośnomówiącym albo bezprzewodowy zestaw słuchawkowy.</li> </ul> <p>Sprawdź liczniki pakietów wysłanych (TxCnt) i pakietów odebranych (RxCnt), aby sprawdzić przepływ pakietów z dźwiękiem.</p>
Znaczne obniżenie wyników MOS LQK	<p>Problemy z działaniem sieci polegające na utracie pakietów lub dużych wahaniami opóźnień:</p> <ul style="list-style-type: none"> <li>• Średni spadek MOS LQK może wskazywać na powszechne i jednolite problemy.</li> <li>• Pojedyncze spadki MOS LQK mogą wskazywać na nagłe i krótkotrwałe problemy.</li> </ul> <p>Sprawdź, czy współczynnik ukrywania i sekundy ukrywania wskazują na utratę pakietów i wahania opóźnień.</p>
Znaczny wzrost wyników MOS LQK	<ul style="list-style-type: none"> <li>• Sprawdź, czy telefon nie używa innego kodeka niż powinien (RxType i TxType).</li> <li>• Sprawdź, czy po uaktualnieniu oprogramowania sprzętowego zmieniła się wersja MOS LQK.</li> </ul>



---

**Uwaga** Metryki jakości dźwięku nie są związane z szumami i zniekształceniami, a jedynie utratą ramek.

---

## Czyszczenie telefonu IP Cisco

Telefon IP Cisco można czyścić tylko przez delikatne wycieranie telefonu i jego ekranu za pomocą suchej, miękkiej ściereczki. Nie wolno stosować płynów ani proszków bezpośrednio na powierzchnię telefonu. Tak jak w przypadku wszystkich urządzeń elektronicznych bez uszczelnionej obudowy, płyny i proszki mogą uszkodzić podzespoły i spowodować awarię.

Gdy telefon znajduje się w trybie uśpienia, ekran jest pusty, a przycisk Wybierz nie świeci się. Gdy telefon znajduje się w tym stanie, można wyczyścić ekran, o ile wiadomo, że telefon pozostanie w stanie uśpienia do momentu zakończenia czyszczenia.



## ROZDZIAŁ 14

# Obsługa użytkowników międzynarodowych

- [Instalator lokalny punktów końcowych programu Unified Communications Manager, na stronie 293](#)
- [Obsługa zapisu połączeń międzynarodowych w dzienniku, na stronie 293](#)
- [Ograniczenia językowe, na stronie 294](#)

## Instalator lokalny punktów końcowych programu Unified Communications Manager

Domyślnie w telefonach IP Cisco ustawiona jest wersja językowa Angielski (Stany Zjednoczone). Aby korzystać z telefonów IP Cisco w innych krajach, należy zainstalować zlokalizowaną wersję instalatora lokalnego punktów końcowych programu Unified Communications Manager na każdym serwerze programu Cisco Unified Communications Manager w klastrze. Instalator lokalny instaluje w systemie najnowsze tłumaczenie interfejsu użytkownika telefonu i odpowiednie do danego kraju sygnały dźwiękowe, aby były dostępne w telefonach IP Cisco.

Aby uzyskać dostęp do instalatora lokalizacji wymaganego dla danego wydania, należy przejść do strony [Pobieranie oprogramowania](#), przejść do modelu telefonu i wybrać łącze Instalator lokalizacji Unified Communications Manager Endpoints.

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.



**Uwaga** Najnowsza wersja instalatora lokalnego może nie być natychmiast dostępna. Należy regularnie sprawdzać, czy we wskazanej powyżej witrynie internetowej pojawiły się aktualizacje.

### Tematy pokrewne

[Cisco Unified Communications Manager — Dokumentacja](#), na stronie xvii

## Obsługa zapisu połączeń międzynarodowych w dzienniku

Jeśli system telefonu jest skonfigurowany do zapisu w dzienniku połączeń międzynarodowych (normalizacja strony wywołującej), we wpisach dzienników połączeń, ponownego wybierania lub połączeń może być wyświetlany symbol plus (+) reprezentujący międzynarodowy kod Esc dla lokalizacji użytkownika. W

zależności od konfiguracji systemu telefonu znak + można zastąpić poprawnym międzynarodowym kodem wybierania lub przed rozpoczęciem wybierania użytkownik musi dokonać edycji numeru, ręcznie zmieniając znak + na międzynarodowy kod Esc dla lokalizacji użytkownika. Chociaż wpisy w dzienniku połączeń lub książce telefonicznej mogą zawierać pełny numer międzynarodowy odebranego połączenia, na ekranie telefonu może być także wyświetlana skrócona lokalna wersja numeru bez kodów międzynarodowych i kodów kraju.

## Ograniczenia językowe

Obsługa wprowadzania tekstów alfanumerycznych za pomocą klawiatury (KATE, Keyboard Alphanumeric Text Entry) nie jest zlokalizowana dla następujących azjatyckich ustawień regionalnych:

- Chiński (Hongkong)
- Chiński (Tajwan)
- Japoński (Japonia)
- Koreański (Republika Korei)

Użytkownikowi zamiast tego prezentowana jest domyślna wersja angielska (Stany Zjednoczone) wprowadzania KATE.

Na przykład na wyświetlaczu telefonu będzie wyświetlany tekst w języku koreańskim, ale wciśnięcie na klawiaturze numerycznej klawisza **2** spowoduje pojawienie się znaków **a b c 2 A B C**.

Wprowadzanie tekstu w języku chińskim działa podobnie, jak na komputerach i telefonach komórkowych w języku chińskim. Do działania funkcji wprowadzania tekstu w języku chińskim wymagany jest instalator języka chińskiego.