Podręcznik administratora telefonów konferencyjnych IP Cisco 8832 dla systemu Cisco Unified Communications Manager

Pierwsza publikacja: 2017-09-15

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 UWAŻANE ZA PRAWDZIWE, ALE NIE JEST UDZIELANA NA NIE ŻADNA GWARANCJA, WYRAŹNA 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 zamieszkanych 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 radiowo-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 dostępnej 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, WYRAŹNYCH 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.

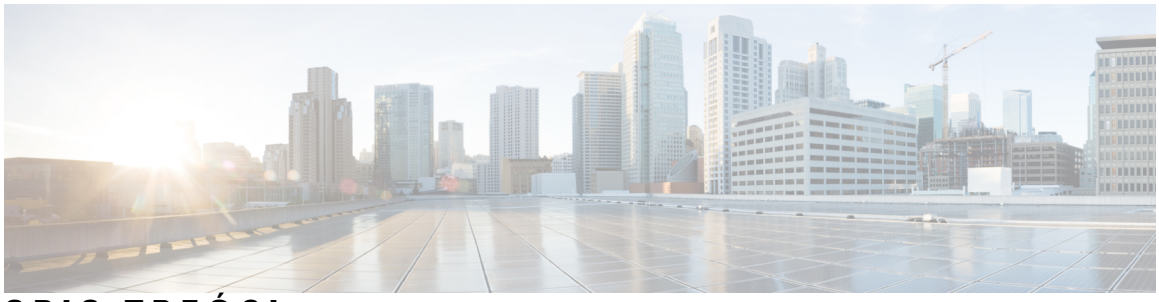
Wszelkie adresy protokołu komunikacyjnego IP oraz numery telefonów użyte w tym dokumencie nie powinny być traktowane jako adresy lub numery rzeczywiste. Wszelkie przykłady, obrazy ekranów zawierające polecenia, diagramy topologii sieci oraz inne dane zawarte w dokumencie zostały przedstawione wyłącznie w celach demonstracyjnych. Jakiekolwiek 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.

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)

© 2017–2023 Cisco Systems, Inc. Wszelkie prawa zastrzeżone.



SPIS TREŚCI

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) 1

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) 2

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.7(1) 3

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.6(1) 3

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR3 3

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR2 3

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR1 4

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1) 4

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.1(1) 4

CZĘŚĆ I: **Informacje o telefonie konferencyjnym IP Cisco** 7

ROZDZIAŁ 2 **Telefon konferencyjny IP Cisco — sprzęt** 9

Telefon konferencyjny IP Cisco 8832 9

Przyciski i sprzęt telefonu konferencyjnego IP Cisco 8832 11

Dodatkowy mikrofon przewodowy (tylko 8832) 12

Dodatkowy mikrofon bezprzewodowy (tylko 8832) 13

Dokumentacja pokrewna 14

Dokumentacja telefonu konferencyjnego IP Cisco 8832 14

Cisco Unified Communications Manager — Dokumentacja 14

Cisco Unified Communications Manager Express — Dokumentacja 15

Dokumentacja usługi Cisco Hosted Collaboration Service 15

Dokumentacja systemu Cisco Business Edition 4000 15

Dokumentacja, pomoc techniczna i wskazówki dotyczące bezpieczeństwa 15
Ogólne informacje na temat bezpieczeństwa produktu Cisco 15
Różnice terminologiczne 16

ROZDZIAŁ 3 **Szczegóły techniczne 17**
Cechy fizyczne i warunki otoczenia 17
Wymogi dotyczące zasilania telefonu 18
Przerwa w zasilaniu 19
Oszczędności na zużyciu energii 19
Protokoły sieciowe 20
Interakcja z programem Cisco Unified Communications Manager 22
Interakcja z programem Cisco Unified Communications Manager Express 23
Interakcje z systemem wiadomości głosowych 24
Pliki konfiguracyjne telefonu 24
Działanie telefonu w okresach dużego obciążenia sieci 25
Interfejs programowania aplikacji 25

CZĘŚĆ II: **Instalowanie telefonu konferencyjnego IP Cisco 27**

ROZDZIAŁ 4 **Instalowanie telefonu 29**
Sprawdzanie konfiguracji sieci 29
Wdrażanie za pomocą kodu aktywacyjnego dla telefonów w siedzibie 30
Wdrażanie przy użyciu kodu aktywacyjnego oraz dostęp z urządzeń przenośnych i dostęp zdalny 31
Włączanie automatycznej rejestracji telefonów 32
Tryb połączenia szeregowego 33
Instalowanie telefonu konferencyjnego 34
Sposoby zasilania telefonu konferencyjnego 35
Instalowanie dodatkowych mikrofonów przewodowych 37
Instalowanie dodatkowych mikrofonów bezprzewodowych 38
Instalowanie podstawki ładującej mikrofonu bezprzewodowego 39
Instalowanie telefonu konferencyjnego w trybie połączenia szeregowego 40
Ponowne uruchamianie telefonu konferencyjnego przy użyciu obrazu kopii zapasowej 41
Konfigurowanie telefonu za pomocą menu konfiguracji 42
Ustawianie hasła w telefonie 43

Wprowadzanie tekstu za pomocą telefonu i poruszanie się po jego menu 43
Konfigurowanie ustawień sieciowych 44
Pola w obszarze Konfiguracja sieci 44
Konfigurowanie pola Nazwa domeny 48
Włącz w telefonie bezprzewodową sieć LAN 48
Konfigurowanie bezprzewodowej sieci LAN w programie Cisco Unified Communications Manager 49
Konfigurowanie bezprzewodowej sieci LAN z telefonu 50
Ustaw liczbę prób uwierzytelniania sieci WLAN 51
Włączanie trybu monitu sieci WLAN 52
Konfigurowanie profilu Wi-Fi za pomocą programu Cisco Unified Communications Manager 52
Konfigurowanie grupy Wi-Fi za pomocą programu Cisco Unified Communications Manager 54
Sprawdzanie uruchamiania telefonu 55
Zmień model telefonu użytkownika 55

ROZDZIAŁ 5 **Instalowanie telefonu w systemie Cisco Unified Communications Manager 57**
Konfigurowanie telefonu konferencyjnego IP Cisco 57
Sprawdzanie adresu MAC telefonu 62
Metody dodawania telefonów 62
Dodawanie telefonów pojedynczo 63
Dodawanie telefonów przy użyciu szablonu telefonu narzędzia BAT 63
Dodawanie użytkowników do programu Cisco Unified Communications Manager 64
Dodawanie użytkownika z zewnętrznego katalogu LDAP 64
Dodawanie użytkownika bezpośrednio do systemu Cisco Unified Communications Manager 65
Dodawanie użytkownika do grupy użytkowników końcowych 66
Kojarzenie telefonów z użytkownikami 66
Survivable Remote Site Telephony 67

ROZDZIAŁ 6 **Zarządzanie portalem samoobsługowym 71**
Portal samoobsługowy — omówienie 71
Konfigurowanie dostępu użytkownika do portalu Self Care 72
Dostosowywanie wyświetlania w portalu Self Care 72

CZĘŚĆ III: **Administrowanie telefonem konferencyjnym IP Cisco 73**

ROZDZIAŁ 7 **Zabezpieczenia telefonu konferencyjnego IP Cisco** 75

Zabezpieczenia telefonu IP Cisco — przegląd 75

Zwiększone zabezpieczenia Twojej sieci telefonicznej 76

Obsługiwane funkcje zabezpieczeń 77

Konfigurowanie certyfikatu obowiązującego lokalnie 80

Włączanie trybu FIPS 81

Zabezpieczenia połączeń telefonicznych 81

Identyfikacja zabezpieczonych połączeń konferencyjnych 82

Identyfikacja zabezpieczonych połączeń telefonicznych 83

Szyfrowanie dla funkcji wtrącenia 84

Zabezpieczenia sieci WLAN 84

Bezpieczeństwo sieci bezprzewodowej 88

Strona administrowania telefonem IP Cisco 88

Konfiguracja protokołu SCEP 91

Uwierzytelnianie 802.1x 92

ROZDZIAŁ 8 **Dostosowywanie telefonu konferencyjnego IP Cisco** 93

Niestandardowe sygnały dzwonka 93

Konfigurowanie niestandardowego dzwonka telefonu 93

Formaty plików dzwonków niestandardowych 94

Dostosowywanie sygnału wybierania 95

ROZDZIAŁ 9 **Funkcje i konfiguracja telefonu konferencyjnego IP Cisco** 97

Pomoc techniczna dla użytkowników telefonu IP Cisco 97

Bezpośrednia migracja telefonu do telefonu wieloplatformowego 98

Konfigurowanie nowego szablonu klawiszy programowych 98

Konfigurowanie usług telefonicznych dla użytkowników 99

Konfigurowanie funkcji telefonu 100

Konfigurowanie funkcji wszystkich telefonów 100

Konfigurowanie funkcji grupy telefonów 101

Konfigurowanie funkcji pojedynczego telefonu 101

Konfiguracja specyficzna dla produktu 102

Wyłącz szyfrowanie TLS (Transport Layer Security) 114
Planowane oszczędzanie energii Power Save dla telefonów IP Cisco 115
Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco 116
Konfigurowanie funkcji Nie przeszkadzać 120
Konfigurowanie powiadamiania o przekierowywaniu połączeń 121
Konfiguracja trybu UCR 2008 122
Konfigurowanie trybu UCR 2008 we wspólnej konfiguracji urządzenia 123
Konfigurowanie trybu UCR 2008 we wspólnym profilu telefonu 123
44Konfigurowanie trybu UCR 2008 w oknie Enterprise Phone Configuration (Firmowa konfiguracja telefonów) 123
Konfigurowanie trybu UCR 2008 w telefonie 124
Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway 124
Scenariusze wdrożeń 126
Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway 126
Narzędzie do zgłaszania problemów 127
Konfigurowanie adresu URL do przesyłania plików do pomocy technicznej 127
Konfigurowanie oznaczenia linii 128

ROZDZIAŁ 10 **Firmowa książka telefoniczna i osobista książka telefoniczna 131**
Konfigurowanie firmowej książki telefonicznej 131
Konfigurowanie osobistej książki adresowej 131

CZĘŚĆ IV: **Rozwiązywanie problemów z telefonem konferencyjnym IP Cisco 133**

ROZDZIAŁ 11 **Monitorowanie systemów telefonicznych 135**
Monitorowanie systemów telefonicznych — przegląd 135
Stan telefonu IP Cisco 135
Wyświetlanie okna Informacje o telefonie 136
Wyświetlanie menu Stan 136
Wyświetlanie okna komunikatów o stanie 136
Wyświetlanie okna Statystyki sieci 141
Wyświetlanie okna Statystyki połączeń 144
Strona WWW telefonu IP Cisco 146

Otwieranie strony WWW telefonu 146
Strona WWW Informacje o urządzeniu 147
Strona WWW Konfiguracja sieci 148
Strona WWW Ethernet Information (Informacje o sieci Ethernet) 153
Strony WWW dotyczące sieci 153
Strony WWW Dzienniki konsoli, Zrzuty rdzenia, Komunikaty o stanie oraz Ekran debugowania 155
Strona WWW Statystyki strumieniowania 155
Żądanie informacji z telefonu w formacie XML 158
Przykładowe dane wyjściowe polecenia CallInfo 159
Przykładowe dane wyjściowe polecenia LineInfo 159
Przykładowe dane wyjściowe polecenia ModeInfo 160

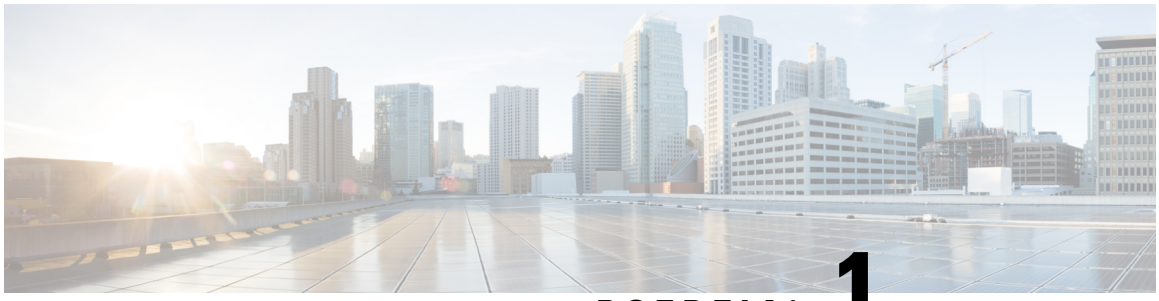
ROZDZIAŁ 12 **Rozwiązywanie problemów z telefonem 161**
Ogólne informacje o rozwiązywaniu problemów 161
Problemy z uruchamianiem 162
Telefon IP Cisco nie przechodzi przez zwykły proces uruchamiania 163
Telefon IP Cisco nie rejestruje się w programie Cisco Unified Communications Manager 164
Telefon wyświetla komunikaty o błędach 164
Telefon nie może połączyć się z serwerem TFTP ani systemem Cisco Unified Communications Manager 164
Telefon nie może połączyć się z serwerem TFTP 164
Telefon nie może połączyć się z serwerem 165
Telefon nie może nawiązać połączenia z użyciem serwera DNS 165
Nie są uruchomione usługi Cisco Unified Communications Manager ani TFTP 165
Uszkodzenie pliku konfiguracyjnego 166
Rejestrowanie telefonu w programie Cisco Unified Communications Manager 166
Telefon IP Cisco nie może uzyskać adresu IP 166
Problemy z resetowaniem się telefonu 167
Telefon resetuje się z powodu chwilowych przerw w działaniu sieci 167
Telefon resetuje się z powodu błędnych ustawień serwera DHCP 167
Telefon resetuje się z powodu nieprawidłowego statycznego adresu IP 167
Telefon resetuje się podczas dużego obciążenia sieci 168
Telefon resetuje się z powodu celowego zresetowania 168
Telefon resetuje się z powodu problemu z serwerem DNS lub innych problemów z łącznością 168

Telefon nie włącza się 169
Telefon nie może się połączyć z siecią LAN 169
Problemy z zabezpieczeniami telefonu IP Cisco 169
Problemy z plikiem CTL 169
Błąd uwierzytelniania, telefon nie może uwierzytelnić pliku CTL 169
Telefon nie może uwierzytelnić pliku CTL 170
Plik CTL jest uwierzytelniony, ale inne pliki konfiguracyjne nie są 170
Plik ITL jest uwierzytelniony, ale inne pliki konfiguracyjne nie są 170
Uwierzytelnianie serwera TFTP nie powiodło się 170
Telefon nie rejestruje się 171
Telefon nie żąda podpisanych plików konfiguracyjnych 171
Problemy z dźwiękiem 171
Brak dźwięku 171
Przerywanie głosu 172
Podłączenie jednego telefonu w trybie połączenia szeregowego nie jest możliwe 172
Ogólne problemy z połączeniami telefonicznymi 172
Nie można zestawić połączenia telefonicznego 172
Telefon nie rozpoznaje cyfr DTMF lub cyfry są opóźnione 173
Procedury rozwiązywania problemów 173
Tworzenie raportu o problemie z telefonem w programie Cisco Unified Communications Manager 173
Sprawdzanie ustawień TFTP 174
Identyfikowanie problemów z systemem DNS lub łącznością 174
Sprawdzanie ustawień DHCP 175
Tworzenie nowego pliku konfiguracyjnego telefonu 175
Sprawdzanie ustawień DNS 176
Uruchamianie usługi 176
Informacje kontrolne debugowania z programu Cisco Unified Communications Manager 177
Dodatkowe informacje o sposobach rozwiązywania problemów 178

ROZDZIAŁ 13 **Konserwacja** 179
Ponowne uruchamianie lub resetowanie telefonu konferencyjnego 179
Ponowne uruchamianie telefonu konferencyjnego 179
Resetowanie ustawień telefonu konferencyjnego za pomocą menu telefonu 179

Przywracanie ustawień fabrycznych telefonu konferencyjnego za pomocą klawiatury numerycznej 180
Monitorowanie jakości dźwięku 181
Wskazówki dotyczące rozwiązywania problemów z jakością dźwięku 181
Czyszczenie telefonu IP Cisco 182

ROZDZIAŁ 14 **Obsługa użytkowników międzynarodowych 183**
Instalator lokalny punktów końcowych programu Unified Communications Manager 183
Obsługa zapisu połączeń międzynarodowych w dzienniku 183
Ograniczenia językowe 184



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 1
- 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 2
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.7(1), na stronie 3
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.6(1), na stronie 3
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR3, na stronie 3
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR2, na stronie 3
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR1, na stronie 4
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1), na stronie 4
- Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.1(1), na stronie 4

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 76

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	Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 76

Funkcja	Nowe lub zmienione
Migracja telefonu bez wcześniejszego obciążenia	Bezpośrednia migracja telefonu do telefonu wieloplatformowego, na stronie 98

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	Konfiguracja specyficzna dla produktu, na stronie 102
Udoskonalenia protokołu SIP OAuth	Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 76
Udoskonalenia uwierzytelniania OAuth dla MRA	Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, na stronie 124
Ulepszenia interfejsu użytkownika	Survivable Remote Site Telephony, na stronie 67

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	Zmień model telefonu użytkownika, na stronie 55
Dodano dodatkowe informacje o polu dostęp przez WWW	Konfiguracja specyficzna dla produktu, na stronie 102

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

Podręcznik administratora dotyczący oprogramowania sprzętowego w wersji 12.7(1) nie wymagał żadnych aktualizacji.

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

Podręcznik administratora dotyczący oprogramowania sprzętowego w wersji 12.6(1) nie wymagał żadnych aktualizacji.

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

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

Tabela 2: Poprawki w Podręczniku administratora telefonów IP Cisco z serii 8832 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 31
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 173

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)SR2

Podręcznik administratora dotyczący oprogramowania sprzętowego w wersji 12.5(1)SR2 nie wymagał żadnych aktualizacji.

Oprogramowanie sprzętowe w wersji 12.5(1)SR2 zastępuje oprogramowanie sprzętowe w wersji 12.5(1) oraz 12.5(1)SR1. Oprogramowanie sprzętowe w wersji 12.5(1) oraz 12.5(1)SR1 zostało odroczone na korzyść oprogramowania sprzętowego w wersji 12.5(1)SR2.

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

Poniższa tabela zawiera listę zmian w dokumencie *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* (Podręcznik administratora programu Cisco Unified Communications Manager dla telefonu konferencyjnego IP Cisco 8832) dotyczących oprogramowania sprzętowego w wersji 12.5(1)SR1.

Tabela 3: Poprawki w Podręczniku administratora telefonu konferencyjnego IP Cisco 8832 związane z oprogramowaniem sprzętowym w wersji 12.5(1)SR1.

Poprawka	Nowa lub zaktualizowana sekcja
Obsługa certyfikatów Elliptic Curve	Obsługiwane funkcje zabezpieczeń, na stronie 77

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.5(1)

Poniższa tabela zawiera listę zmian w dokumencie *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* (Podręcznik administratora programu Cisco Unified Communications Manager dla telefonu konferencyjnego IP Cisco 8832) dotyczących oprogramowania sprzętowego w wersji 12.5(1).

Tabela 4: Poprawki w Podręczniku administratora telefonu konferencyjnego IP Cisco 8832 związane z oprogramowaniem sprzętowym w wersji 12.5(1).

Poprawka	Nowa lub zaktualizowana sekcja
Obsługa funkcji Whisper Paging w programie Cisco Unified Communications Manager Express	Interakcja z programem Cisco Unified Communications Manager Express, na stronie 23
Obsługa funkcji Wyłącz szyfrowanie TLS	Konfiguracja specyficzna dla produktu, na stronie 102
Obsługa wybierania blokowego dla rozszerzenia czasomierza między cyframi T.302.	Konfiguracja specyficzna dla produktu, na stronie 102

Nowe i zmienione informacje o oprogramowaniu sprzętowym w wersji 12.1(1)

W poniższej tabeli opisano zmiany w dokumencie *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* (Podręcznik administratora programu Cisco Unified

Communications Manager dla telefonu konferencyjnego IP Cisco 8832) dotyczące oprogramowania sprzętowego w wersji 12.1(1).

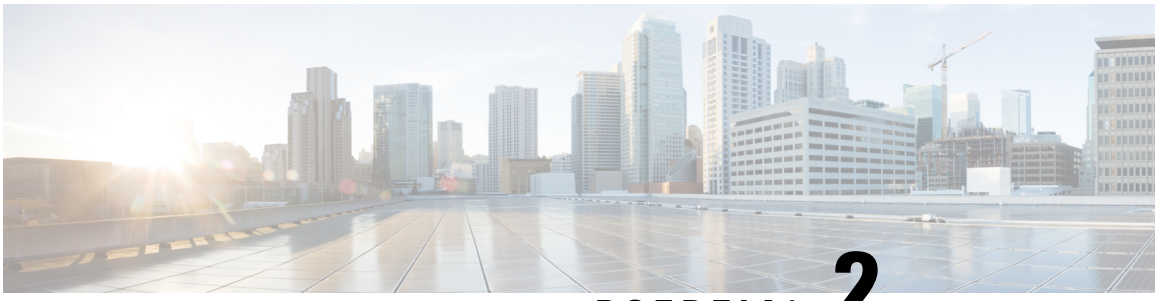
Poprawka	Nowa lub zaktualizowana sekcja
Obsługa: Iniektor PoE do telefonu konferencyjnego IP Cisco 8832	• Wymogi dotyczące zasilania telefonu, na stronie 18 • Sposoby zasilania telefonu konferencyjnego, na stronie 35 • Instalowanie telefonu konferencyjnego, na stronie 34
Obsługa mikrofonów bezprzewodowych	• Telefon konferencyjny IP Cisco 8832, na stronie 9 • Dodatkowy mikrofon bezprzewodowy (tylko 8832), na stronie 13 • Instalowanie dodatkowych mikrofonów bezprzewodowych, na stronie 38 • Instalowanie podstawki ładującej mikrofonu bezprzewodowego, na stronie 39
Obsługa połączenia szeregowego	• Telefon konferencyjny IP Cisco 8832, na stronie 9 • Tryb połączenia szeregowego, na stronie 33 • Instalowanie telefonu konferencyjnego w trybie połączenia szeregowego, na stronie 40 • Podłączenie jednego telefonu w trybie połączenia szeregowego nie jest możliwe, na stronie 172
Obsługa: Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832	• Instalowanie telefonu konferencyjnego, na stronie 34 • Sposoby zasilania telefonu konferencyjnego, na stronie 35

Poprawka	Nowa lub zaktualizowana sekcja
Obsługa łączności Wi-Fi	• Instalowanie telefonu konferencyjnego, na stronie 34 • Sposoby zasilania telefonu konferencyjnego, na stronie 35 • Konfigurowanie pola Nazwa domeny, na stronie 48 • Włącz w telefonie bezprzewodową sieć LAN, na stronie 48 • Konfigurowanie bezprzewodowej sieci LAN w programie Cisco Unified Communications Manager, na stronie 49 • Konfigurowanie bezprzewodowej sieci LAN z telefonu, na stronie 50 • Ustaw liczbę prób uwierzytelniania sieci WLAN, na stronie 51 • Włączanie trybu monitu sieci WLAN, na stronie 52 • Konfigurowanie profilu Wi-Fi za pomocą programu Cisco Unified Communications Manager, na stronie 52 • Konfigurowanie grupy Wi-Fi za pomocą programu Cisco Unified Communications Manager, na stronie 54
Obsługa dostępu z urządzeń przenośnych i dostępu zdalnego za pośrednictwem usługi Expressway	• Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, na stronie 124 • Scenariusze wdrożeń, na stronie 126 • Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway, na stronie 126
Obsługa włączania i wyłączania protokołu TLS 1.2 dla dostępu do serwera WWW.	Konfiguracja specyficzna dla produktu, na stronie 102
Obsługa kodeka audio G722.2 AMR-WB	• Telefon konferencyjny IP Cisco 8832, na stronie 9 • Pola na ekranie Statystyki połączeń, na stronie 144

CZĘŚĆ I

Informacje o telefonie konferencyjnym IP Cisco

- Telefon konferencyjny IP Cisco — sprzęt, na stronie 9
- Szczegóły techniczne, na stronie 17



ROZDZIAŁ 2

Telefon konferencyjny IP Cisco — sprzęt

- Telefon konferencyjny IP Cisco 8832, na stronie 9
- Przyciski i sprzęt telefonu konferencyjnego IP Cisco 8832, na stronie 11
- Dokumentacja pokrewna, na stronie 14
- Dokumentacja, pomoc techniczna i wskazówki dotyczące bezpieczeństwa, na stronie 15
- Różnice terminologiczne, na stronie 16

Telefon konferencyjny IP Cisco 8832

Telefon Cisco IP Conference Phone 8832 i 8832NR poprawiają jakość komunikacji między osobami. Łączy nadzwyczajną jakość dźwięku HD (high-definition) i zasięg 360 stopni na użytek średnich i dużych sal konferencyjnych oraz biur zarządu. Szerokopasmowy (G.722) głośnik pełnodupleksowego dwukierunkowego zestawu głośnomówiącego gwarantuje jakość brzmienia na poziomie audiofilskim. Ten telefon to proste rozwiązanie, które spełnia wymagania najróżniejszych sal konferencyjnych.

Rysunek 1: Telefon konferencyjny IP Cisco 8832

Telefon konferencyjny wyposażono w czułe mikrofony o charakterystyce kołowej (360 stopni). Dzięki temu możesz mówić w naturalny sposób, a Twoje wypowiedzi będą wyraźnie słyszalne z odległości nawet 3 m. W modelu tym zastosowano też rozwiązanie techniczne, które przeciwdziała interferencjom ze strony telefonów

komórkowych i innych urządzeń bezprzewodowych, co zapewnia stabilną komunikację bez zakłóceń. Telefon ma kolorowy na ekran i przyciski klawiszy programowych służące do uzyskiwania dostępu do funkcji użytkownika. W przypadku użycia samej jednostki bazowej telefon zapewnia zasięg w pokoju o rozmiarach 6,1 x 6,1 m (20 x 20 stóp) dla maksymalnie 10 osób.

Do użytku z telefonem są dostępne dwa przewodowe mikrofony rozszerzające. Umieszczenie mikrofonów rozszerzających z dala od jednostki podstawowej zapewnia większy zasięg w obszerniejszych salach konferencyjnych. W przypadku użycia jednostki bazowej i przewodowych mikrofonów rozszerzających telefon konferencyjny zapewnia zasięg w pokoju o rozmiarach 6,1 x 10 m (20 x 34 stopy) dla maksymalnie 22 osób.

Telefon obsługuje również opcjonalny zestaw dwóch bezprzewodowych mikrofonów rozszerzających. W przypadku użycia jednostki bazowej i bezprzewodowych mikrofonów rozszerzających telefon konferencyjny zapewnia zasięg w pokoju o rozmiarach 6,1 x 10 m (20 x 34 stopy) dla maksymalnie 22 osób. W celu zapewnienia dobrego zasięgu w pomieszczeniu o wymiarach 6,1 x 12,2 m zalecamy umieszczenie poszczególnych mikrofonów w maksymalnej odległości 3 m od stacji bazowej.

Można połączyć dwie jednostki bazowe, aby zwiększyć zasięg w pomieszczeniu. Ta konfiguracja wymaga opcjonalnego zestawu do łączenia szeregowego i umożliwia obsługę dwóch mikrofonów rozszerzających (przewodowych lub bezprzewodowych, ale nie obu typów naraz). W przypadku korzystania z mikrofonów przewodowych z zestawem do łączenia szeregowego konfiguracja zapewnia zasięg w pomieszczeniu o wymiarach do 6,1 x 15,2 m i obsługę do 38 osób. W przypadku korzystania z mikrofonów bezprzewodowych z zestawem do łączenia szeregowego konfiguracja zapewnia zasięg w pomieszczeniu o wymiarach do 6,1 x 17,4 m i obsługę do 42 osób.

Wersja Telefon konferencyjny IP Cisco 8832NR (bez funkcji radio) nie obsługuje łączności Wi-Fi, Bluetooth ani bezprzewodowych mikrofonów rozszerzających.

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

⚠

Przestroga 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.

Przyciski i sprzęt telefonu konferencyjnego IP Cisco 8832

Na poniższym rysunku przedstawiono telefon konferencyjny IP Cisco 8832.

Rysunek 2: Przyciski i funkcje telefonu konferencyjnego IP Cisco 8832

W poniższej tabeli opisano przyciski telefonu konferencyjnego IP Cisco 8832.

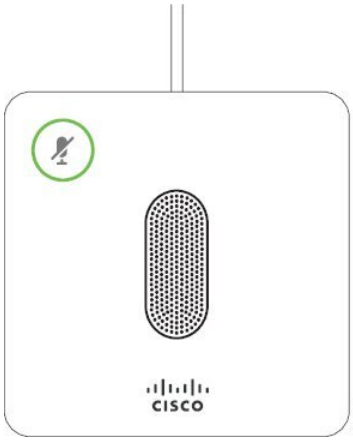
Tabela 5: Przyciski i funkcje telefonu konferencyjnego IP Cisco 8832

1	Pasek LED	Wskazuje stany połączeń: • Zielone, ciągłe — aktywne połączenie • Zielone, migające — połączenie przychodzące • Zielone, pulsujące — połączenie wstrzymane • Czerwone, ciągłe — połączenie wyciszone
2	Port mikrofonu z możliwością wyprowadzenia	Kabel mikrofonu przewodowego z możliwością wyprowadzenia należy podłączyć do portu.
3	Pasek **wyciszenia**	Przycisk włącza i wyłącza mikrofon. Gdy mikrofon jest wyciszony, światełko LED świeci na czerwono.
4	Przyciski programowe	Przycisk Funkcje i usługi.
5	Pasek nawigacji i przycisk **Wybierz**	Przewijanie pomiędzy menu, podświetlanie pozycji i wybór podświetlonej pozycji.
6	Przycisk **Głośność**	Regulacja poziomu głośności telefonu głośnomówiącego (przy podniesionej słuchawce) oraz poziomu głośności dzwonka (przy odłożonej słuchawce). Podczas regulacji głośności pasek LED świeci na biało i wskazuje zmianę głośności.

Dodatkowy mikrofon przewodowy (tylko 8832)

Telefon Cisco IP Conference Phone 8832 obsługuje dwa mikrofony przewodowe z możliwością wyprowadzenia dostępne w zestawie opcjonalnym. Należy korzystać z mikrofonów dodatkowych w większych pomieszczeniach lub w pomieszczeniach z większą ilością osób. Aby uzyskać najlepszy efekt, zaleca się umieszczenie mikrofonów w odległości od 0,91 m do 2,1 m od telefonu.

Rysunek 3: Dodatkowy mikrofon przewodowy



Gdy jesteś w trakcie połączenia, dioda LED mikrofonu dodatkowego otaczająca przycisk **wyciszenia** świeci na zielono.

Gdy mikrofon jest wyciszony, światełko LED świeci na czerwono. Po naciśnięciu przycisku **wyciszenia** telefon i mikrofony z możliwością wyprowadzenia zostaną wyciszone.

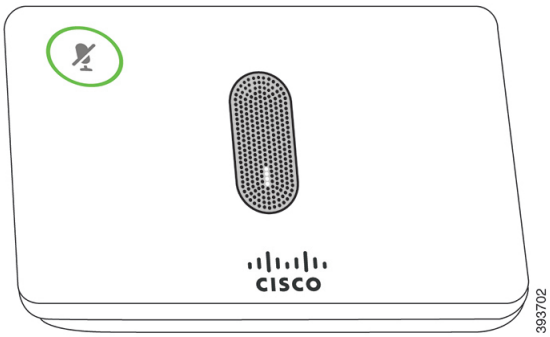
Tematy pokrewne

Instalowanie dodatkowych mikrofonów przewodowych, na stronie 37

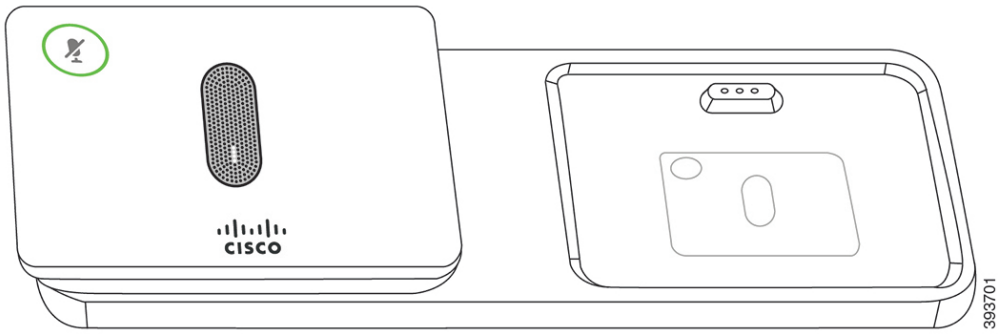
Dodatkowy mikrofon bezprzewodowy (tylko 8832)

Telefon Cisco IP Conference Phone 8832 obsługuje dwa bezprzewodowe mikrofony rozszerzające dostępne w zestawie opcjonalnym. Gdy mikrofon bezprzewodowy jest ładowany na podstawce ładującej, dioda LED w podstawce świeci na biało.

Rysunek 4: Mikrofon bezprzewodowy



Rysunek 5: Mikrofon bezprzewodowy umieszczony na podstawce ładującej



Gdy telefon konferencyjny jest w trakcie połączenia, dioda LED mikrofonu z możliwością wyprowadzenia otaczająca przycisk **wyciszenia** świeci na zielono.

Gdy mikrofon jest wyciszony, dioda LED świeci na czerwono. Po naciśnięciu przycisku **wyciszenia** telefon i mikrofony z możliwością wyprowadzenia zostaną wyciszone.

Gdy telefon jest sparowany z mikrofonem bezprzewodowym (na przykład mikrofonem bezprzewodowym 1), a mikrofon bezprzewodowy zostanie podłączony do ładowarki, naciśnięcie klawisza programowego **Szczegóły** spowoduje wyświetlenie wskaźnika poziomu naładowania tego mikrofonu.

Gdy telefon jest sparowany z mikrofonem bezprzewodowym, podłączenie mikrofonu przewodowego spowoduje rozłączenie sparowanego mikrofonu bezprzewodowego i sparowanie telefonu z mikrofonem przewodowym. Na ekranie telefonu zostanie wyświetlone powiadomienie o podłączeniu mikrofonu przewodowego.

Tematy pokrewne

Instalowanie dodatkowych mikrofonów bezprzewodowych, na stronie 38
Instalowanie podstawki ładującej mikrofonu bezprzewodowego, na stronie 39

Dokumentacja pokrewna

Informacje pokrewne można znaleźć w następujących sekcjach.

Dokumentacja telefonu konferencyjnego IP Cisco 8832

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

Cisco Unified Communications Manager — Dokumentacja

Należy zapoznać się z dokumentem *Cisco Unified Communications ManagerDocumentation 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 Unified Communications Manager Express — Dokumentacja

Należy zapoznać się z publikacjami dotyczącymi danego języka, modelu telefonu i wersji programu Cisco Unified Communications Manager Express. Można je znaleźć pod następującym adresem URL dokumentacji:

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

Dokumentacja usługi Cisco Hosted Collaboration Service

Należy zapoznać się z dokumentem *Rozwiązanie Cisco Hosted Collaboration Solution Documentation Guide* (Przewodnik po dokumentacji programu Cisco Unified Communications Manager) i innymi publikacjami dotyczącymi używanej wersji programu Rozwiązanie Cisco Hosted Collaboration Solution. Należy skorzystać z następującego adresu URL:

https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Dokumentacja systemu Cisco Business Edition 4000

Należy zapoznać się z dokumentem *Cisco Business Edition 4000Documentation Guide* (Przewodnik po dokumentacji programu Cisco Unified Communications Manager) i innymi publikacjami dotyczącymi używanej wersji programu Cisco Business Edition 4000. Należy skorzystać z następującego adresu URL:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/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/index.php/regulations/export-administration-regulations-ear.

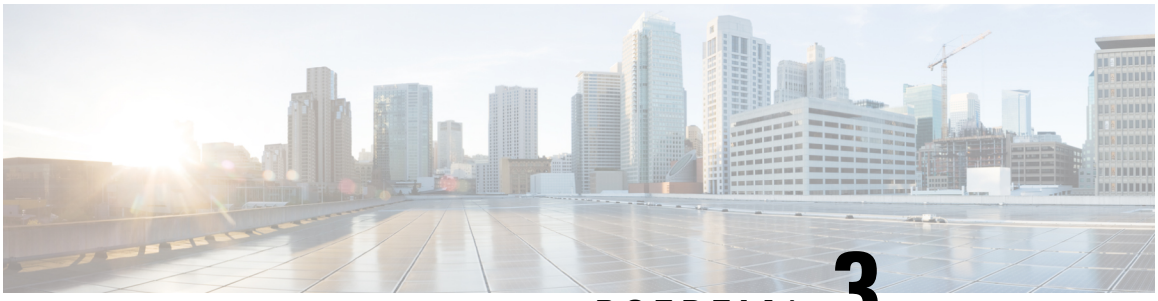
Różnice terminologiczne

W tym dokumencie termin *telefon IP Cisco* obejmuje zakresem telefon konferencyjny IP Cisco 8832.

W poniższej tabeli podano niektóre różnice terminologiczne między dokumentami *telefon konferencyjny IP 8832 User Guide*, *telefon konferencyjny IP Cisco 8832 Administration Guide for Cisco Unified Communications Manager* i dokumentacją programu Cisco Unified Communications Manager.

Tabela 6: Różnice terminologiczne

Podręcznik użytkownika	Podręcznik administratora
Wskaźniki wiadomości	Wskaźnik wiadomości oczekującej (MWI)
System poczty głosowej	System wiadomości głosowych



ROZDZIAŁ 3

Szczegóły techniczne

- Cechy fizyczne i warunki otoczenia, na stronie 17
- Wymogi dotyczące zasilania telefonu, na stronie 18
- Protokoły sieciowe, na stronie 20
- 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
- Pliki konfiguracyjne telefonu, na stronie 24
- Działanie telefonu w okresach dużego obciążenia sieci, na stronie 25
- Interfejs programowania aplikacji, na stronie 25

Cechy fizyczne i warunki otoczenia

W poniższej tabeli podano cechy fizyczne i warunki otoczenia telefonu konferencyjnego.

Tabela 7: 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	Od 10% do 90% (bez kondensacji)
Temperatura przechowywania	Od –10 do +60°C (od +14 do +140°F)
Wysokość	278 mm (10,9 cala)
Szerokość	278 mm (10,9 cala)
Głębokość	61,3 mm (2,4 cala)
Masa	1852 g (4,07 funta)
Gniazdo zasilania	Zasilanie IEEE PoE klasy 3 za pomocą adaptera PoE. Telefon jest obsługuje protokoły Cisco Discovery Protocol (CDP) oraz Link La Inne opcje obejmują zasilacz Ethernet inny niż PoE w przypadku po przy użyciu sieci Wi-Fi wymagany jest zasilacz telefonu konferen

Specyfikacja	Wartość lub zakres
Zapewnianie bezpieczeństwa	Bezpieczny rozruch
Kable	USB-C
Wymagania dotyczące odległości	Zgodnie ze specyfikacją sieci Ethernet przyjmuje się, że maksymalna może wynosić 100 metrów (330 stóp).

Aby uzyskać więcej informacji, patrz *arkusz danych telefonu telefonu konferencyjnego IP Cisco 8832*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

Wymogi dotyczące zasilania telefonu

Telefon Cisco IP Conference Phone 8832 może używać następujących źródeł energii:

- Wdrożenie PoE (Power over Ethernet) przy użyciu urządzenia Iniektor PoE do telefonu konferencyjnego IP Cisco 8832
- Wdrożenie sieci Ethernet innej niż PoE przy użyciu urządzenia Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832
- Wdrożenie przy użyciu sieci WiFi wymaga użycia zasilacza telefonu konferencyjnego IP Cisco 8832.

Tabela 8: Wskazówki dotyczące zasilania telefonu konferencyjnego IP Cisco

Rodzaj zasilania	Wskazówki
Zasilanie PoE — dostarczane przy użyciu Iniektor PoE do telefonu konferencyjnego IP Cisco 8832 lub Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832 i kabla USB-C podłączonego do telefonu.	Jeśli używane jest urządzenie Iniektor PoE do telefonu konferencyjnego IP Cisco 8832 i Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832, w celu zapewnienia nieprzerwanego działania telefonu należy zadbać o podłączenie przełącznika do zasilacza awaryjnego. Należy też sprawdzić, czy działająca w przełączniku wersja systemu operacyjnego CatOS lub IOS obsługuje wdrażane telefony. Informacje o wersji systemu operacyjnego można znaleźć w dokumentacji przełącznika. Podczas instalowania telefonu zasilanego przez PoE przed podłączeniem kabla USB-C do telefonu należy podłączyć iniektor do sieci LAN. Podczas odłączania telefonu zasilanego przez PoE przed odłączeniem zasilania od adaptera należy odłączyć kabel USB-C od telefonu.

Rodzaj zasilania	Wskazówki
Zewnętrzne źródło zasilania • Wdrożenie sieci Ethernet innej niż PoE przy użyciu urządzenia Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832 • Wdrożenie przy użyciu sieci WiFi wymaga użycia zasilacza telefonu konferencyjnego IP Cisco 8832. • Wdrożenie w sieci Ethernet inne niż PoE przy użyciu urządzenia Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832 i zasilacza telefonu konferencyjnego IP Cisco 8832	Podczas instalowania telefonu zasilanego z zewnętrznego zasilacza przed podłączeniem kabla USB-C do telefonu należy podłączyć iniektor do sieci Ethernet. Podczas odłączania telefonu zasilanego przez zewnętrzne źródło zasilania przed odłączeniem zasilania od adaptera należy odłączyć kabel USB-C od telefonu.

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 wyłączane, gdy telefon nie jest używany. Telefon pozostaje w trybie Oszczędzanie energii przez zaplanowany czas lub do momentu, gdy użytkownik 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 wybudzania oraz inne parametry. Parametry te są wysyłane do telefonu w ramach pliku XML jego konfiguracji.

Tematy pokrewne

Planowane oszczędzanie energii Power Save dla telefonów IP Cisco, na stronie 115
Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116

Protokoły sieciowe

Telefon Cisco IP Conference Phone 8832 jest zgodny z wieloma standardami branżowymi i protokołami sieciowymi Cisco niezbędnymi do komunikacji głosowej. Poniższa tabela zawiera przegląd protokołów sieciowych obsługiwanych przez te telefony.

Tabela 9: Protokoły sieciowe obsługiwane przez telefon konferencyjny IP Cisco

Protokół sieciowy	Przeznaczenie	Uwagi o użyciu
Bootstrap Protocol (BootP)	Protokół BootP umożliwia urządzeniu sieciowemu, takiemu jak telefon, wykrycie określonych informacji potrzebnych podczas uruchamiania, np. własnego adresu IP.	—
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 protokół CDP służy do przekazywania d VLAN ID, szczegóły zarządzania zasilaniem poprz QoS).
Protokół DHCP (ang. Dynamic Host Configuration Protocol)	Protokół DHCP dynamicznie przydziela i przypisuje adresy IP urządzeniom sieciowym. Dzięki niemu można podłączyć telefon IP do sieci i uruchomić bez konieczności ręcznego przypisywania mu adresu IP ani konfigurowania dodatkowych parametrów sieci.	Protokół DHCP jest domyślnie włączony. Po jego w serwer TFTP lokalnie w każdym telefonie. Zalecamy używanie w przypadku protokołu DHCP n TFTP jako wartość tej opcji. Opis dodatkowych ob konkretnej wersji programu Cisco Unified Commun **Uwaga** Jeśli w przypadku protokołu DHCP nie
Protokół HTTP (Hypertext Transfer Protocol)	HTTP to standardowy protokół do przesyłania informacji i przenoszenia dokumentów za pośrednictwem Internetu i sieci WWW.	W telefonach protokół HTTP służy do korzystania z 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 obsługujące protokoły HTTP protokół HTTPS, wybierają adres URL dla protoko Jeśli połączenie z usługą odbywa się za pośrednict

Protokół sieciowy	Przeznaczenie	Uwagi o użyciu
IEEE 802.1X	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. 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.	Wdrożenie standardu IEEE 802.1X w telefonie c Po włączeniu w telefonie uwierzytelniania 802.
IP	IP to protokół komunikacyjny, który służy do adresowania i wysyłania pakietów w sieci.	Do komunikowania się za pośrednictwem proto Adresy IP, podsieci i bramy są przypisywane au używany, trzeba ręcznie przypisywać wspomnia Telefony obsługują adresy protokołu IPv6. Więc programu Cisco Unified Communications Mana
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 obsługuje protokół LLDP poprzez port k
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED to rozszerzenie standardu LLDP opracowane z myślą o produktach do komunikacji głosowej.	Telefon obsługuje rozszerzenie LLDP-MED pop • konfiguracja VLAN głosowego, • wykrywanie urządzeń, • zarządzanie zasilaniem, • zarządzanie zapasami. Aby uzyskać więcej informacji na temat obsług *LLDP-MED i Cisco Discovery Protocol* dostępn https://www.cisco.com/en/US/tech/tk652/tk701/
Real-Time Transport Protocol (RTP)	RTP to standardowy protokół do przesyłania danych w czasie rzeczywistym, np. na potrzeby interaktywnej komunikacji głosowej i wideo, za pośrednictwem sieci transmisji danych.	W telefonach protokół RTP służy do wysyłania i 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 błądzenia).	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, wy programie Cisco Unified Communications Manager mogą umożliwiać konfigurację tych parametrów w
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 standar telefonii pakietowej. Sygnalizowanie umożliwia prz zapewnia z kolei sterowanie atrybutami kompleksow
Secure Real-Time Transfer Protocol (SRTP)	SRTP jest rozszerzeniem profilu audio-wideo protokołu RTP (ang. Real-Time Protocol, protokół komunikacji w czasie rzeczywistym), które zapewnia nienaruszalność pakietów RTP i RTCP (ang. Real-Time Control Protocol, protokół sterowania komunikacją w czasie rzeczywistym). Umożliwia to uwierzytelnianie, zabezpieczanie integralności i szyfrowanie pakietów danych multimedialnych między dwoma punktami końcowymi.	W telefonach protokół SRTP służy do szyfrowania
TCP	TCP to protokół komunikacyjny dla potrzeb połączeń.	W telefonach protokół TCP służy do komunikacji z usług XML.
Transport Layer Security (TLS)	TLS to standardowy protokół do zabezpieczania i uwierzytelniania komunikacji.	Gdy są stosowane zabezpieczenia, protokół TLS słu Communications Manager. Więcej informacji na te Unified Communications Manager.
Protokół TFTP (ang. Trivial File Transfer Protocol)	Protokół TFTP służy do przesyłania plików za pośrednictwem sieci. W telefonie protokół TFTP umożliwia pobieranie pliku konfiguracyjnego przeznaczonego dla konkretnego modelu telefonu.	Protokół TFTP wymaga obecności w sieci serwera Jeśli telefon ma korzystać z innego serwera TFTP TFTP w menu Konfiguracja sieci w telefonie. Więcej informacji na ten temat można znaleźć w dok
UDP (ang. User Datagram Protocol)	UDP to bezpołączeniowy protokół komunikacyjny, który służy do dostarczania pakietów danych.	Protokół UDP jest używany tylko w strumieniach R

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

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 14

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 interkomem, nazywane także funkcją whisper paging. Jednak przywoływanie jest odrzucane przez telefon podczas połączenia.

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.

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

Działanie telefonu w okresach dużego obciążenia sieci

Czynniki powodujące zmniejszenie wydajności sieci mogą wpływać na jakość połączeń głosowych 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).

Interfejs programowania aplikacji

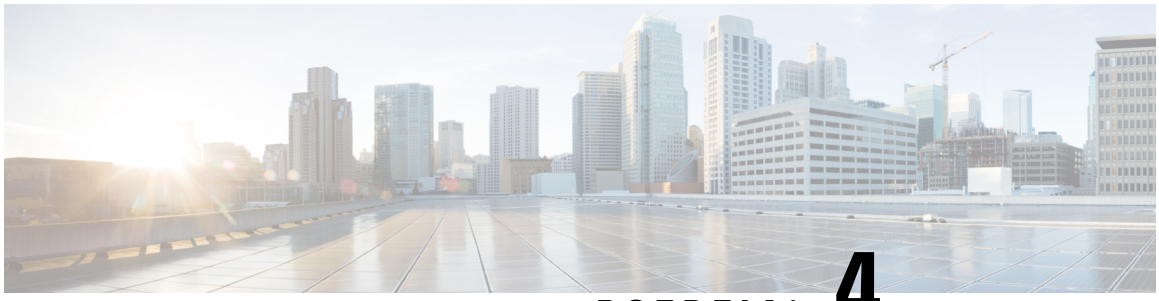
Firma Cisco obsługuje korzystanie z interfejsu API telefonu przez aplikacje innych firm, które zostały przetestowane i certyfikowane przez firmę Cisco i twórcę aplikacji innej firmy. Wszelkie problemy z telefonami związane z interakcją z niecertyfikowaną aplikacją muszą być rozwiązywane przez stronę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

CZĘŚĆ II

Instalowanie telefonu konferencyjnego IP Cisco

- Instalowanie telefonu, na stronie 29
- Instalowanie telefonu w systemie Cisco Unified Communications Manager, na stronie 57
- Zarządzanie portalem samoobsługowym, na stronie 71



ROZDZIAŁ 4

Instalowanie telefonu

- Sprawdzanie konfiguracji sieci, na stronie 29
- Wdrażanie za pomocą kodu aktywacyjnego dla telefonów w siedzibie, na stronie 30
- Wdrażanie przy użyciu kodu aktywacyjnego oraz dostęp z urządzeń przenośnych i dostęp zdalny, na stronie 31
- Włączanie automatycznej rejestracji telefonów, na stronie 32
- Tryb połączenia szeregowego, na stronie 33
- Instalowanie telefonu konferencyjnego, na stronie 34
- Konfigurowanie telefonu za pomocą menu konfiguracji, na stronie 42
- Włącz w telefonie bezprzewodową sieć LAN, na stronie 48
- Sprawdzanie uruchamiania telefonu, na stronie 55
- Zmień model telefonu użytkownika, na stronie 55

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).

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 14

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 **Wymagaja 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).

Tryb połączenia szeregowego

Można połączyć dwa telefony konferencyjne, stosując Adapter inteligentny i kable USB-C dostarczane z zestawem do łączenia szeregowego w celu zwiększenia zasięgu dźwięku w pomieszczeniu.

W trybie połączenia szeregowego oba urządzenia są zasilane przez adapter inteligentny podłączony do zasilacza. Można użyć tylko jednego mikrofonu zewnętrznego na urządzenie. Urządzenia umożliwiają użycie pary mikrofonów przewodowych lub pary mikrofonów bezprzewodowych, ale nie obu tych typów mikrofonów naraz. Podłączenie mikrofonu przewodowego do jednego z urządzeń powoduje rozparowanie wszystkich mikrofonów bezprzewodowych podłączonych do tego samego urządzenia. Zawsze gdy połączenie jest aktywne, diody LED i opcje menu na ekranach telefonów obu urządzeń są synchronizowane.

Tematy pokrewne

Instalowanie telefonu konferencyjnego w trybie połączenia szeregowego, na stronie 40
Podłączenie jednego telefonu w trybie połączenia szeregowego nie jest możliwe, na stronie 172

Instalowanie telefonu konferencyjnego

Gdy telefon połączy się z siecią, rozpocznie proces uruchamiania i zarejestruje się w programie Cisco Unified Communications Manager. Jeśli wyłączysz usługę DHCP, musisz skonfigurować ustawienia sieciowe w telefonie.

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

Po nawiązaniu połączenia telefon sprawdza, czy trzeba zainstalować nową wersję firmware.

Jeśli telefon konferencyjny jest używany w trybie połączenia szeregowego, zobacz Instalowanie telefonu konferencyjnego w trybie połączenia szeregowego, na stronie 40.

Zanim rozpoczniesz

Upewnij się, że w systemie Cisco Unified Communications Manager jest zainstalowana najnowsza wersja firmware. Sprawdź tutaj, czy są dostępne aktualizacje pakietów urządzeń:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Procedura

Krok 1 Wybierz źródło zasilania telefonu:

- Wdrożenie PoE (Power over Ethernet) przy użyciu urządzenia Iniektor PoE do telefonu konferencyjnego IP Cisco 8832
- Wdrożenie sieci Ethernet innej niż PoE przy użyciu urządzenia Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832
- Wdrożenie przy użyciu sieci WiFi wymaga użycia zasilacza telefonu konferencyjnego IP Cisco 8832.

Aby uzyskać więcej informacji, patrz Sposoby zasilania telefonu konferencyjnego, na stronie 35.

Krok 2 Podłącz telefon do przełącznika.

- Jeśli korzystasz z PoE:
  1. Podłącz kabel Ethernet do portu LAN.
  2. Podłącz drugi koniec kabla Ethernet do urządzenia Iniektor PoE do telefonu konferencyjnego IP Cisco 8832 lub Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832.
  3. Podłącz iniektor do telefonu konferencyjnego za pomocą kabla USB-C.
- Jeśli nie używasz PoE:
  1. Jeśli używane jest urządzenie Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832, podłącz zasilacz do gniazdka elektrycznego.
  2. Podłącz kabel zasilający do iniektora Ethernet za pomocą kabla USB-C.

LUB

Jeśli używane jest urządzenie Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832, podłącz je do gniazdka elektrycznego.

3. Podłącz kabel Ethernet do iniektora Ethernet innego niż PoE lub iniektora Ethernet.
4. Podłącz kabel Ethernet do portu LAN.
5. Podłącz iniektor Ethernet inny niż PoE lub iniektor Ethernet do telefonu konferencyjnego przy użyciu kabla USB-C.

- Jeśli używana jest sieć Wi-Fi:
  1. Podłącz zasilacz telefonu konferencyjnego IP Cisco 8832 do gniazdka elektrycznego.
  2. Podłącz zasilacz do telefonu konferencyjnego przy użyciu kabla USB-C.

     Uwaga Zamiast zasilacza telefon może być zasilany przy użyciu iniektora Ethernet innego niż PoE. Jednak należy odłączyć kabel sieci LAN. Telefon łączy się z siecią Wi-Fi tylko wtedy, gdy połączenie Ethernet jest niedostępne.

Krok 3 Obserwuj proces uruchamiania telefonu. Na tym etapie można sprawdzić, czy telefon jest prawidłowo skonfigurowany.

Krok 4 Jeśli nie używasz automatycznej rejestracji, ręcznie skonfiguruj ustawienia zabezpieczeń w telefonie.

Krok 5 Zaczekaj, aż telefon zainstaluje uaktualnienie firmware dostępne w systemie Cisco Unified Communications Manager.

Krok 6 Zadzwoń z telefonu, aby sprawdzić, czy działa on poprawnie.

Krok 7 Poinformuj użytkowników końcowych, jak mają używać telefonów i jak mogą skonfigurować ich opcje. Dzięki temu użytkownicy dowiedzą się, jak efektywnie korzystać z telefonów Cisco.

Sposoby zasilania telefonu konferencyjnego

Telefon konferencyjny wymaga zasilania z jednego z następujących źródeł:

- Zasilanie Power over Ethernet (PoE)
  - Ameryka Północna
    - Iniektor PoE do telefonu konferencyjnego IP Cisco 8832
    - Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832
  - Poza Ameryką Północną — Iniektor PoE do telefonu konferencyjnego IP Cisco 8832
- Ethernet bez funkcji zasilania PoE
  - Ameryka Północna
    - Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832

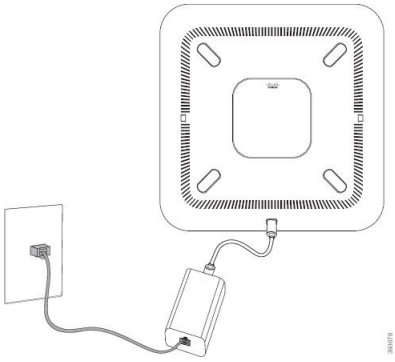
- Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832 z zasilaczem telefonu konferencyjnego IP Cisco 8832 podłączonym do gniazdka elektrycznego.

- Poza Ameryką Północną — Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832

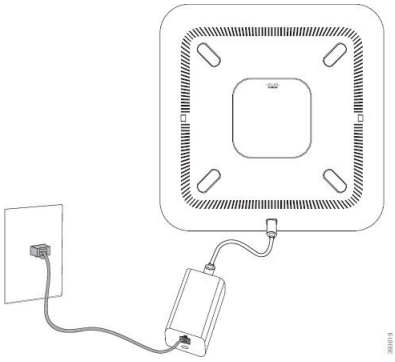
- Wi-Fi — należy uzyć zasilacza telefonu konferencyjnego IP Cisco 8832 podłączonego do gniazdka elektrycznego.

Rysunek 6: Opcje zasilania PoE telefonu konferencyjnego

Na poniższym rysunku przedstawiono dwie opcje zasilania PoE.



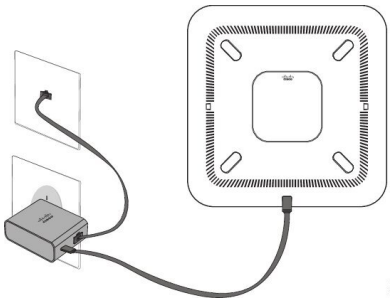
Iniektor PoE do telefonu konferencyjnego IP Cisco 8832 przy użyciu opcji zasilania PoE



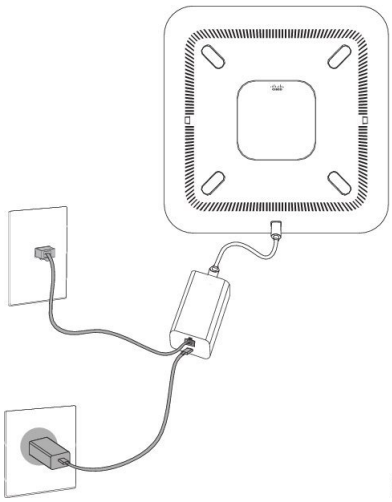
Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832 przy użyciu opcji zasilania PoE

Rysunek 7: Opcje zasilania telefonu konferencyjnego z sieci Ethernet

Na poniższym rysunku przedstawiono dwie opcje zasilania z sieci Ethernet.

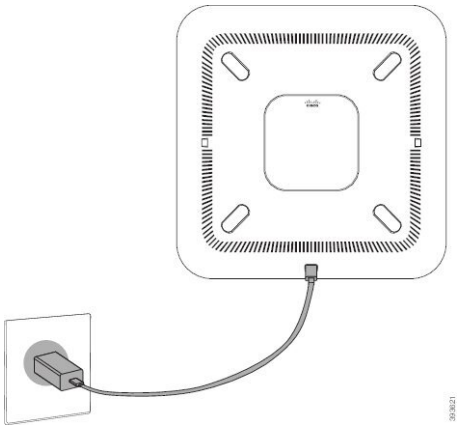


Iniektor Ethernet (bez PoE) do telefonu konferencyjnego IP Cisco 8832 przy użyciu opcji zasilania Ethernet



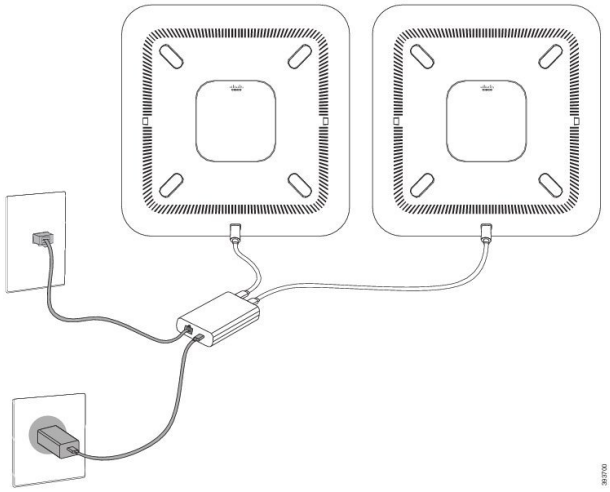
Adapter Ethernet do telefonu konferencyjnego IP Cisco 8832 przy użyciu opcji zasilania Ethernet

Rysunek 8: Opcja zasilania telefonu konferencyjnego po podłączeniu do sieci Wi-Fi



Rysunek 9: Opcja zasilania telefonu konferencyjnego w trybie połączenia szeregowego

Na poniższym rysunku przedstawiono opcję zasilania, gdy telefon jest połączony w trybie połączenia szeregowego.



Instalowanie dodatkowych mikrofonów przewodowych

Telefon obsługuje zestaw opcjonalny zawierający dwa dodatkowe mikrofony przewodowe. Mikrofony można wyprowadzić na odległość do 2,13 m od telefonu. Dla najlepszego efektu zaleca się umieszczenie mikrofonów w odległości od 0,91 m do 2,1 m od telefonu.

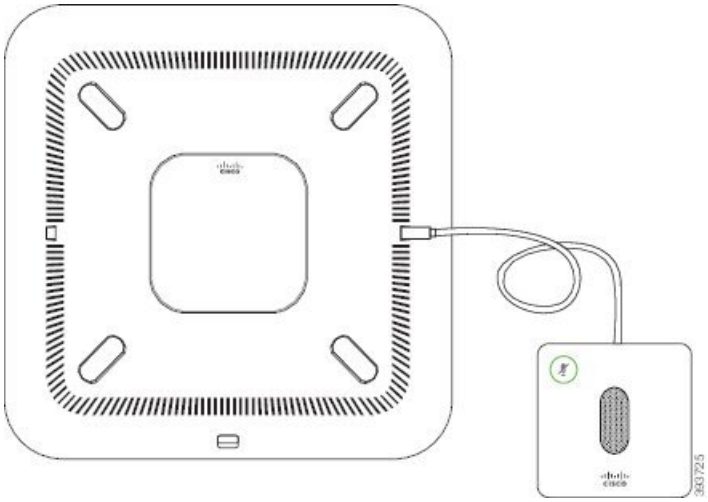
Procedura

Krok 1 Podłącz wtyk kabla mikrofonu do portu z boku telefonu.

Krok 2 Wyprowadź kabel mikrofonu w wybrane miejsce.

Na poniższym rysunku przedstawiono instalację dodatkowego mikrofonu przewodowego.

Rysunek 10: Instalowanie dodatkowego mikrofonu przewodowego



Instalowanie dodatkowych mikrofonów bezprzewodowych

Do tego telefonu konferencyjnego można podłączyć dwa dodatkowe bezprzewodowe mikrofony.

Uwaga Należy użyć dwóch mikrofonów przewodowych lub dwóch mikrofonów bezprzewodowych z telefonem, ale nie połączenia mieszanego.

Gdy telefon jest w trakcie połączenia, dioda LED mikrofonu rozszerzającego świeci na zielono. Aby wyciszyć mikrofon rozszerzający, naciśnij przycisk **wyciszenia**. Gdy mikrofon jest wyciszony, dioda LED świeci na czerwono. Gdy bateria w mikrofonie jest rozładowana, wskaźnik LED stanu baterii szybko miga.

Zanim rozpoczniesz

Przed zainstalowaniem dodatkowych mikrofonów bezprzewodowych odłącz dodatkowe mikrofony przewodowe. Nie można używać jednocześnie przewodowych i bezprzewodowych mikrofonów.

Procedura

Krok 1 Ustaw płytkę montażową na blacie stołu, gdzie ma być umiejscowiony mikrofon.

Krok 2 Usuń warstwę dwustronnej taśmy samoprzylepnej na dole płytki montażowej. Umieść płytkę montażową tak, aby przylegała do powierzchni stołu.

Krok 3 Przymocuj mikrofon do płytki montażowej. Magnesy osadzone w mikrofonie przytwierdzą jednostkę na miejscu.

W razie potrzeby można przenieść mikrofon z dołączonym mocowaniem w inne miejsce na blacie stołu. Zachowaj ostrożność podczas przenoszenia w celu ochrony jednostki.

Tematy pokrewne

Dodatkowy mikrofon bezprzewodowy (tylko 8832), na stronie 13
Instalowanie podstawki ładującej mikrofonu bezprzewodowego, na stronie 39

Instalowanie podstawki ładującej mikrofonu bezprzewodowego

Do ładowania baterii mikrofonu bezprzewodowego służy podstawka ładująca.

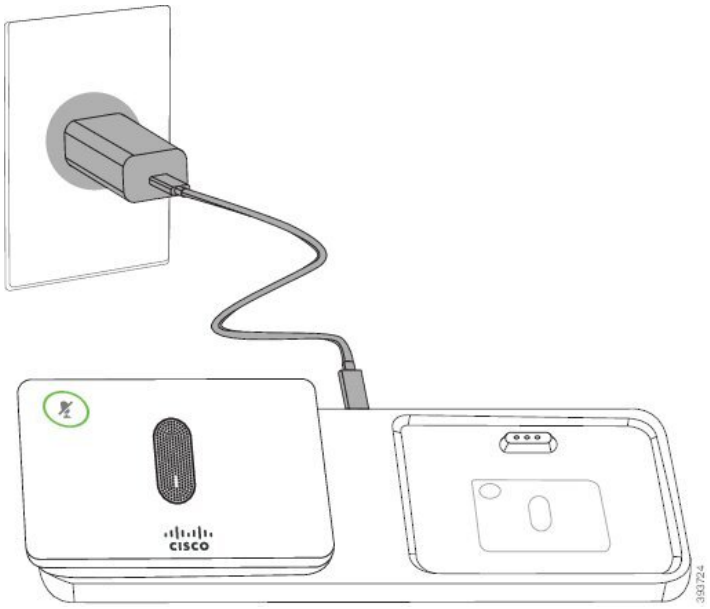
Procedura

Krok 1 Podłącz zasilacz podstawki ładującej do gniazdka elektrycznego.

Krok 2 Podłącz jeden koniec kabla USB-C do podstawki ładującej, a drugi do zasilacza.

Na poniższym rysunku przedstawiono instalację podstawki ładującej mikrofonu bezprzewodowego.

Rysunek 11: Instalowanie podstawki ładującej mikrofonu bezprzewodowego



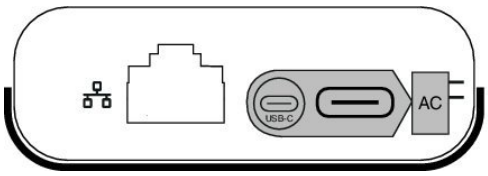
Tematy pokrewne

Dodatkowy mikrofon bezprzewodowy (tylko 8832), na stronie 13
Instalowanie dodatkowych mikrofonów bezprzewodowych, na stronie 38

Instalowanie telefonu konferencyjnego w trybie połączenia szeregowego

Zestaw do łączenia szeregowego zawiera urządzenie Adapter inteligentny, krótki kabel LAN, dwa długie i grubsze kable USB-C oraz krótszy i cieńszy kabel USB-C. W trybie połączenia szeregowego telefony konferencyjne wymagają zewnętrznego zasilania z gniazdka elektrycznego. Telefony należy połączyć ze sobą przy użyciu urządzenia Adapter inteligentny. Długie kable USB-C należy podłączyć do telefonu, a krótki kabel do zasilacza. Na poniższym rysunku przedstawiono sposób podłączania zasilacza i portu sieci LAN do urządzenia Adapter inteligentny.

Rysunek 12: Port zasilania i port sieci LAN adaptera inteligentnego



Można użyć tylko jednego mikrofonu na urządzenie.

Uwaga Należy użyć dwóch mikrofonów przewodowych lub dwóch mikrofonów bezprzewodowych z telefonem, ale nie połączenia mieszanego.

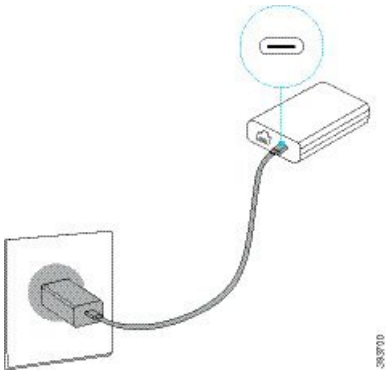
Kabel USB-C zasilacza jest cieńszy niż kable USB-C podłączane do telefonu.

Procedura

Krok 1 Podłącz kabel zasilający do gniazdka elektrycznego.

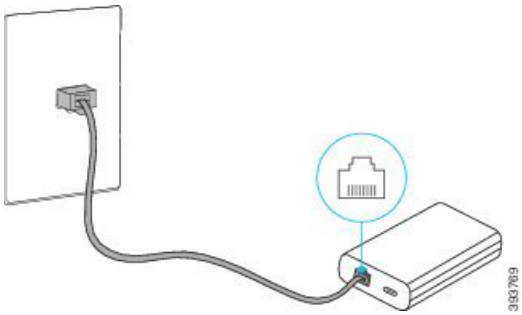
Krok 2 Podłącz krótszy i cieńszy kabel USB-C do zasilacza i urządzenia Adapter inteligentny.

Rysunek 13: Port USB adaptera inteligentnego podłączony do gniazdka elektrycznego



Krok 3 Wymagane: Podłącz kabel sieci Ethernet do urządzenia Adapter inteligentny i portu LAN.

Rysunek 14: Port sieci LAN adaptera inteligentnego połączony z portem LAN w gniazdku ściennym

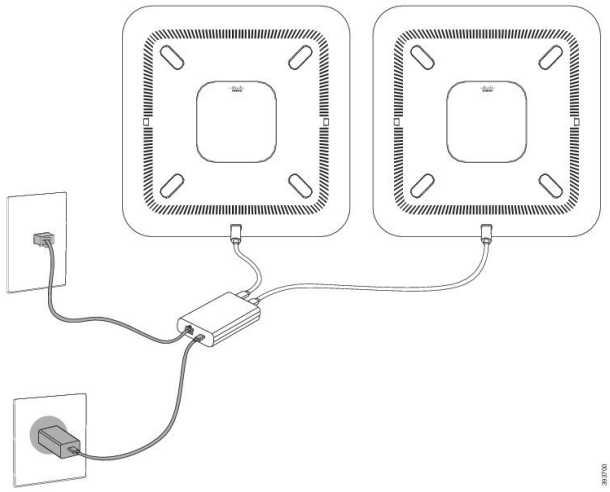


Krok 4 Podłącz pierwszy telefon do urządzenia Adapter inteligentny przy użyciu dłuższego i grubszego kabla USB-C.

Krok 5 Podłącz drugi telefon do urządzenia Adapter inteligentny przy użyciu kabla USB-C.

Na poniższym rysunku przedstawiono instalację telefonu konferencyjnego w trybie połączenia szeregowego.

Rysunek 15: Instalacja telefonu konferencyjnego w trybie połączenia szeregowego



Tematy pokrewne

Tryb połączenia szeregowego, na stronie 33
Podłączenie jednego telefonu w trybie połączenia szeregowego nie jest możliwe, na stronie 172

Ponowne uruchamianie telefonu konferencyjnego przy użyciu obrazu kopii zapasowej

Telefon konferencyjny IP Cisco 8832 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 Przytrzymaj wciśnięty klawisz * podczas podłączania zasilania do telefonu konferencyjnego.

Krok 2 Gdy pasek LED zaświeci się na zielono, a następnie wyłączy się, można zwolnić klawisz *.

Krok 3 Telefon konferencyjny zostanie ponownie uruchomiony z obrazu kopii zapasowej.

Konfigurowanie telefonu za pomocą menu konfiguracji

Telefon ma wiele konfigurowalnych ustawień sieciowych. Przed rozpoczęciem korzystania z telefonu może być konieczna zmiana tych ustawień. Można je wyświetlić i zmodyfikować za pomocą menu telefonu.

Telefon ma następujące menu konfiguracyjne:

- Konfiguracja sieci: wyświetlanie i konfigurowanie różnych ustawień sieciowych.
  - Konfiguracja protokołu IPv4: to podmenu zawiera dodatkowe opcje sieciowe.
  - Konfiguracja protokołu IPv6: to podmenu zawiera dodatkowe opcje sieciowe.
- Konfiguracja zabezpieczeń: wyświetlanie i konfigurowanie różnych ustawień zabezpieczeń.

Uwaga Można określić, czy telefon ma dostęp do menu Ustawienia oraz do zawartych w nim opcji. Sterowanie takim dostępem odbywa się za pomocą pola **Dostęp do ustawień** w oknie Konfiguracja telefonu w aplikacji Cisco Unified Communications Manager — administracja. W polu **Dostęp do ustawień** dozwolone są następując wartości:

- Włączone: umożliwia dostęp do menu Ustawienia.
- Wyłączone: blokuje dostęp do większości opcji w menu Ustawienia. Użytkownik nadal ma dostęp do pola **Ustawienia** > **Stan**.
- Ograniczone: umożliwia dostęp do opcji w menu Preferencje użytkownika i Stan oraz zapisywanie zmian głośności. Blokuje dostęp do innych opcji w menu Ustawienia.

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

Ustawienia, które są wyświetlane bez możliwości zmiany w telefonie, można skonfigurować w Cisco Unified Communications Manager — administracja.

Procedura

Krok 1 Naciśnij przycisk **Ustawienia**.

Krok 2 Wybierz opcję **Ustawienia administratora**.

Krok 3 Jeśli jest to wymagane, wpisz hasło, a następnie kliknij przycisk **Zaloguj się**.

Krok 4 Wybierz opcję **Konfiguracja sieci** lub **Konfiguracja zabezpieczeń**.

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 zamknąć menu, naciśnij przycisk **Wstecz**.

Tematy pokrewne

Ponowne uruchamianie lub resetowanie telefonu konferencyjnego, na stronie 179
Konfigurowanie ustawień sieciowych, na stronie 44
Konfigurowanie ustawień zabezpieczeń

Ustawianie hasła w telefonie

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. Na przycisku nawigacji naciśnij klawisz **Wybierz**, 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 . Ten klawisz programowy usuwa znak po lewej stronie kursora.
- Naciśnij klawisz **Przywróć** przed naciśnięciem **Zastosuj**, aby odrzucić wszystkie wprowadzone zmiany.
- Aby wpisać kropkę (na przykład w adresie IP), naciśnij ***** na klawiaturze numerycznej.
- 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.

Konfigurowanie ustawień sieciowych

Procedura

Krok 1 Naciśnij przycisk **Ustawienia**.

Krok 2 Wybierz kolejno **Ustawienia administratora** > **Konfiguracja sieci** > **Konfiguracja sieci Ethernet**.

Krok 3 Ustaw pola zgodnie z opisem w Pola w obszarze Konfiguracja sieci, na stronie 44.
Po ustawieniu pól może być wymagane ponowne uruchomienie telefonu.

Pola w obszarze Konfiguracja sieci

W menu Konfiguracja sieci znajdują się pola i podmenu dotyczące ustawień protokołów IPv4 i IPv6.

Aby zmienić niektóre pola, trzeba wyłączyć DHCP.

Tabela 10: Menu Konfiguracja sieci

Trasy	Typ	Domyślny	Opis
Konfiguracja protokołu IPv4	Menu		Patrz tabela "Podmenu Konfiguracja protokołu IPv4". Ta opcja jest dostępna tylko w trybie IPv4 i trybie podwójnego stosu.
Konfiguracja protokołu IPv6	Menu		Patrz tabela "Podmenu Konfiguracja protokołu IPv6".
Nazwa hosta	Ciąg		Nazwa hosta telefonu. Jeśli jest używany serwer DHCP, ta nazwa jest przypisywana automatycznie.
Nazwa domeny	Ciąg		Nazwa domeny, w której znajduje się telefon, w systemie DNS (ang. Domain Name System, system nazw domen). Aby zmienić to pole, wyłącz DHCP.
Aktywny VLAN ID			Aktywna wirtualna sieć lokalna (ang. Virtual Local Area Network, VLAN) skonfigurowana w przełączniku Cisco Catalyst, do której należy telefon.
Administracyjny VLAN ID			Pomocnicza sieć VLAN, do której należy telefon.

Trasy	Typ	Domyślny	Opis
Konfig. portu SW	Automatyczna negocjacja 10 half 10 full 100 half 100 full	Automatyczna negocjacja	Prędkość i tryb dupleks portu przełącznika, gdzie: • 10 Half = 10-BaseT/półdupleks • 10 Full = 10-BaseT/pełny dupleks • 100 Half = 100-BaseT/półdupleks • 100 Full = 100-BaseT/pełny dupleks
LLDP-MED: port SW	Wyłączony włączone	włączona	Wskazuje, czy w porcie przełącznika włączone jest rozszerzenie LLDP-MED (ang. Link Layer Discovery Protocol Media Endpoint Discovery, wykrywanie punktów końcowych nośników za pomocą protokołu wykrywania na poziomie łącza).

Tabela 11: Podmenu Konfiguracja protokołu IPv4

Trasy	Typ	Domyślny	Opis
DHCP	Wyłączony włączone	włączona	Włącza lub wyłącza używanie protokołu DHCP.
Adres IP			Adres IPv4 telefonu. Aby zmienić to pole, wyłącz DHCP.
Maska podsieci			Maska podsieci używana w telefonie. Aby zmienić to pole, wyłącz DHCP.
Domyślny router 1			Domyślny router, z którego korzysta telefon. Aby zmienić to pole, wyłącz DHCP.
Serwer DNS 1			Podstawowy serwer DNS (Serwer DNS 1) używany przez telefon. Aby zmienić to pole, wyłącz DHCP.
Serwer DNS 2			Podstawowy serwer DNS (Serwer DNS 2) używany przez telefon.
Serwer DNS 3			Podstawowy serwer DNS (Serwer DNS 3) używany przez telefon.

Trasy	Typ	Domyślny	Opis
Alternatywny serwer TFTP	Nie Tak	Nie	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. Jeśli została włączona opcja Alternatywny serwer TFTP, należy wprowadzić wartość niezerową opcji Serwer TFTP 1. 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. Zobacz uwagi dotyczące protokołu TFTP pod ostatnią tabelą.
Serwer TFTP 2			Pomocniczy serwer TFTP używany przez telefon. 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 2. W takim przypadku telefon usuwa plik podczas zapisywania zmian opcji Serwer TFTP 2. Nowy plik CTL lub ITL pobiera nowy adres serwera TFTP 2. Zobacz uwagi dotyczące protokołu TFTP pod ostatnią tabelą.
Adres DHCP zwolniony	Nie Tak	Nie	

Tabela 12: Podmenu Konfiguracja protokołu IPv6

Trasy	Typ	Domyślny	Opis
Protokół DHCPv6 włączony	Wyłączony włączone	włączona	Włącza lub wyłącza używanie protokołu IPv6 DHCP.

Trasy	Typ	Domyślny	Opis
Adres IPv6			Adres IPv6 telefonu. Aby zmienić to pole, wyłącz DHCP.
Długość prefiksu IPv6			Długość adresu IPv6. Aby zmienić to pole, wyłącz DHCP.
Domyś. router 1 protok. IPv6			Domyślny router IPv6. Aby zmienić to pole, wyłącz DHCP.
Serwer DNS 1 IPv6			Podstawowy serwer IPv6 DNS Aby zmienić to pole, wyłącz DHCP.
Alternat. serwer TFTP IPv6	Nie Tak	Nie	Wskazuje, czy telefon korzysta z alternatywnego serwera IPv6 TFTP.
Serwer TFTP 1 IPv6			Podstawowy serwer IPv6 TFTP używany przez telefon. Zobacz uwagi dotyczące protokołu TFTP pod tą tabelą.
Serwer TFTP 2 IPv6			Pomocniczy serwer IPv6 TFTP używany przez telefon. Zobacz uwagi dotyczące protokołu TFTP pod tą tabelą.
Adres IPv6 zwolniony	Nie Tak	Nie	

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 protokołu IPv6, zobacz:

- "Wspólna konfiguracja urządzenia" w *Podręcznik opisujący funkcje i usługi programu Cisco Unified Communications Manager*, rozdział "Obsługa adresów IPv6 w urządzeniach Cisco Unified Communications".

- Podręcznik *IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0*, dostępny tutaj: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Uwagi dotyczące protokołu TFTP

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:

1. Wszystkie ręcznie przypisane serwery TFTP IPv4
2. Wszystkie ręcznie przypisane serwery IPv6
3. Serwery TFTP przypisane przez DHCP
4. Serwery TFTP przypisane przez DHCPv6

Informacje o plikach CTL i ITL można znaleźć w podręczniku *Cisco Unified Communications Manager Security Guide* (Podręcznik zabezpieczeń programu Cisco Unified Communications Manager).

Konfigurowanie pola Nazwa domeny

Procedura

Krok 1 Dla opcji Serwer DHCP włączony wybierz ustawienie **Nie**.

Krok 2 Przewiń do opcji Nazwa domeny, kliknij przycisk **Wybierz** i wpisz nową nazwę domeny.

Krok 3 Naciśnij przycisk **Zastosuj**.

Włącz w telefonie bezprzewodową sieć LAN

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

Użytkownikom sieci Wi-Fi zalecamy używanie metody roamingu Fast-Secure (szybki i bezpieczny). Zalecane jest użycie połączenia 802.11r (FT).

Kompletne informacje o konfiguracji znajdują się w *Podręczniku wdrażania sieci WLAN na urządzeniach IP Cisco z serii 8832* pod następującym adresem:

https://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 8832 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 **Ustawienia**.

Krok 2 Wybierz kolejno opcje **Ustawienia admin.** > **Konfiguracja sieci** > **Konfiguracja klienta Wi-Fi** > **Łączność bezprzewodowa**.

Krok 3 Naciśnij klawisz **Włącz**.

Konfigurowanie bezprzewodowej sieci LAN w programie Cisco Unified Communications Manager

W aplikacji Cisco Unified Communications Manager — administracja należy włączyć parametr "Wi-Fi" dla telefonu konferencyjnego.

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:

a) Wybierz kolejno opcje **Urządzenie** > **Telefon**.
b) Odszukaj żądany telefon.
c) W sekcji Układ konfiguracji specyficznej dla produktu, w parametrze Wi-Fi, zaznacz pole **Włączone**.
d) Zaznacz pole wyboru **Zastąp ustawienia wspólne**.

Krok 2 Aby włączyć obsługę bezprzewodowej sieci LAN w grupie telefonów:

a) Wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Wspólny profil telefonu**.
b) Wybierz dla parametru Wi-Fi wartość **Włączone**.

Uwaga Aby upewnić się, że konfiguracja działa w tym kroku, usuń zaznaczenie pola wyboru **Zastąp ustawienia wspólne** opisanego w kroku 1d.

c) Zaznacz pole wyboru **Zastąp ustawienia wspólne**.
d) 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:

a) Wybierz kolejno opcje **System** > **Konfiguracja telefonu przedsiębiorstwa**.

b) Wybierz dla parametru Wi-Fi wartość **Włączone**.

Uwaga Aby upewnić się, że konfiguracja działa w tym kroku, usuń zaznaczenie pola wyboru **Zastąp ustawienia wspólne** opisanego w kroku 1d i 2c.

c) Zaznacz pole wyboru **Zastąp 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 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 wdrożenia dostępu do sieci WLAN na telefonach konferencyjnych IP Cisco 8832* pod następującym adresem: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Zanim rozpoczniesz

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

Procedura

Krok 1 Naciśnij przycisk **Ustawienia**.

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 13: Opcje menu Konfiguracja klienta Wi-Fi

Opcja	Opis	Aby zmienić
Sieć bezprzewodowa	Włącza lub wyłącza radiową komunikację bezprzewodową w telefonie IP Cisco.	Przewiń do opcji **Łączność bezprzew** za pomocą przełącznika zmieniaj usta między Wł. i Wył.
Nazwa sieci	Umożliwia nawiązanie połączenia z siecią bezprzewodową za pomoca okna **Wybieranie sieci**. W tym oknie znajdują się dwa klawisze programowe **— Wstecz** i **Inne**.	W oknie **Wybieranie sieci** wybierz si chcesz nawiązać połączenie.

Opcja	Opis	Aby zmienić
Logowanie w sieci W-Fi	Umożliwia wyświetlenie okna logowania w sieci Wi-Fi.	Przewiń do opcji **Logowanie w si** pomocą przełącznika zmieniaj ustaw Wł. i Wył.
Konfiguracja protokołu IPv4	W podmenu Konfiguracja protokołu IPv4 można wykonać następujące czynności: • Włączenie lub wyłączenie używania przez telefon adresu IP przypisanego przez serwer DHCP. • Ręczne ustawienie adresu IP, maski podsieci, domyślnych routerów, serwera DNS i alternatywnych serwerów TFTP. Więcej informacji o polach adresu IPv4 zawiera tabela „Podmenu konfiguracji IPv4”.	Przewiń do opcji **Konfiguracja pr** i naciśnij przycisk **Wybierz**.
Konfiguracja protokołu IPv6	W podmenu Konfiguracja protokołu IPv6 można wykonać następujące czynności: • Włączenie lub wyłączenie używania przez telefon adresu IPv6 przypisanego przez serwer DHCPv6 lub pobranego przez mechanizm SLAAC za pośrednictwem routera obsługującego protokół IPv6. • Ręczne ustawienie adresu IPv6, długości prefiksu, domyślnych routerów, serwera DNS i alternatywnych serwerów TFTP. Więcej informacji o polach adresu IPv6 zawiera tabela „Podmenu konfiguracji IPv6”.	Przewiń do opcji **Konfiguracja pr** i naciśnij przycisk **Wybierz**.
Adres MAC	Unikatowy adres MAC (Media Access Control) telefonu.	Tylko wyświetlanie. Opcji tej nie konfigurować.
Nazwa domeny	Nazwa domeny, w której znajduje się telefon, w systemie DNS (ang. Domain Name System, system nazw domen).	Zobacz Konfigurowanie pola Nazw stronie 48.

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 upłynięciu 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 programu 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.

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.
- **Pasmo 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.

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**.

Sprawdzanie uruchamiania telefonu

Po podłączeniu zasilania telefon automatycznie wykonuje uruchomieniowy proces diagnostyczny.

Procedura

Włącz telefon.

Wyświetlenie ekranu głównego oznacza, że telefon uruchomił się poprawnie.

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.

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.

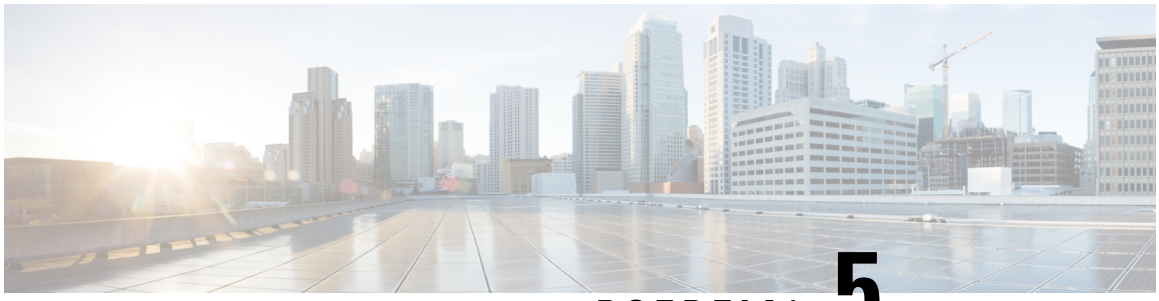
Krok 3 Na nowym telefonie wybierz opcję **Zastąp istniejący telefon**.

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

Instalowanie telefonu w systemie Cisco Unified Communications Manager

- Konfigurowanie telefonu konferencyjnego IP Cisco, na stronie 57
- Sprawdzanie adresu MAC telefonu, na stronie 62
- Metody dodawania telefonów, na stronie 62
- Dodawanie użytkowników do programu Cisco Unified Communications Manager, na stronie 64
- Dodawanie użytkownika do grupy użytkowników końcowych, na stronie 66
- Kojarzenie telefonów z użytkownikami , na stronie 66
- Survivable Remote Site Telephony, na stronie 67

Konfigurowanie telefonu konferencyjnego 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 aplikacji Cisco Unified Communications Manager — administracja. Niektóre zadania tej procedury są opcjonalne, w zależności od systemu i potrzeb użytkowników.

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

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: patrz Sprawdzanie adresu MAC telefonu, na stronie 62
- Fizyczna lokalizacja telefonu
- Nazwa lub identyfikator użytkownika telefonu
- Pula urządzeń

- Partycja, przestrzeń wyszukiwania połączeń i informacje o lokalizacji
- Numer telefonu, który ma zostać przypisany do telefonu
- Użytkownik aplikacji Cisco Unified Communications Manager, który ma zostać powiązany z telefonem
- Informacje o korzystaniu z telefonu wpływające na szablon klawiszy programowych, funkcje telefonu, usługi telefonu IP lub aplikacje telefonu

Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager i korzystając z pokrewnych łączy.

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

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

Krok 3 Zdefiniuj pule urządzeń. Wybierz kolejno opcje **System** > **Pula urządzeń**.

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

Krok 4 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 5 Zdefiniuj przestrzeń wyszukiwania połączeń. W oknie 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 6 Skonfiguruj profil zabezpieczeń dla danego typu urządzenia i protokołu. Wybierz kolejno opcje **System** > **Zabezpieczenia** > **Profil zabezpieczeń telefonu**.

Krok 7 Skonfiguruj telefon. Wybierz kolejno opcje **Urządzenie** > **Telefon**.

a) Zlokalizuj telefon, który chcesz zmodyfikować, lub dodaj nowy telefon.
b) Skonfiguruj telefon, uzupełniając wymagane pola w okienku informacji o urządzeniu znajdującym się w oknie Konfiguracja telefonu.
    - Adres MAC (wymagane): sprawdź, czy wartość składa się z dwunastu znaków szesnastkowych.
    - Opis: wprowadź opis zawierający użyteczne informacje o użytkowniku.
    - Pula urządzeń (wymagane)
    - Wspólny profil telefonu
    - Calling Search Space
    - Lokalizacja

- Właściciel (Użytkownik lub Anonimowy) i, jeśli wybrano opcję Użytkownik, identyfikator właściciela

Urządzenie ze swoimi domyślnymi ustawieniami jest dodawane do bazy danych programu Cisco Unified Communications Manager.

Informacje o polach dotyczących konkretnie tego produktu można znaleźć w "?" Przycisk pomocy w oknie Konfiguracja telefonu i pokrewne łącza.

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.

c) W obszarze Protocol Specific Information (Informacje dotyczące protokołu) tego okna wybierz opcję Device Security Profile (Profil zabezpieczeń urządzenia) i ustaw tryb zabezpieczeń.

Uwaga Wybierz profil zabezpieczeń w zależności od ogólnej strategii zabezpieczeń wdrożonej w firmie. Jeśli telefon nie obsługuje funkcji zabezpieczeń, wybierz profil niezabezpieczony.

d) W obszarze Extension Information (Informacje o funkcji Extension) zaznacz pole wyboru Enable Extension Mobility (Włącz funkcję Extension Mobility), jeśli telefon obsługuje funkcję Cisco Extension Mobility.
e) Kliknij przycisk **Zapisz**.

Krok 8 Wybierz **Urządzenie** > **Ustawienia urządzenia** > **Profil SIP**, aby ustawić parametry protokołu SIP.

Krok 9 Wybierz kolejno opcje **Urządzenie** > **Telefon**, aby skonfigurować w telefonie jego numery (linie), wypełniając odpowiednie pola w oknie Directory Number Configuration (Konfiguracja numerów telefonu).

a) Znajdź telefon.
b) W oknie Phone Configuration (Konfiguracja telefonu) kliknij pozycję Line 1 (Linia 1) w okienku po lewej stronie.

Telefony konferencyjne mają tylko jedną linię.

c) W polu Numer telefonu wprowadź prawidłowy numer, który może zostać wybrany.

Uwaga To pole powinno zawierać ten sam numer, który znajduje się w polu Telephone Number (Numer telefonu) w oknie End User Configuration (Konfiguracja użytkownika końcowego).

d) Z listy rozwijanej Route Partition (Partycja tras) wybierz partycję, do której należy numer telefonu. Jeśli nie chcesz ograniczać dostępu do numeru telefonu, wybierz dla partycji opcję <None>.
e) Z listy Calling Search Space (Przestrzeń wyszukiwania połączeń) wybierz odpowiednią przestrzeń wyszukiwania połączeń. Wybrana wartość jest stosowana w przypadku wszystkich urządzeń używających danego numeru telefonu.
f) W obszarze Call Forward and Call Pickup Settings (Ustawienia przekierowywania i przejmowania połączeń) wybierz odpowiednie pozycje — np. Forward All (Przekieruj wszystkie), Forward Busy Internal (Przekieruj zajęte wewnętrzne) — oraz odpowiednie miejsca docelowe, do których będą przesyłane połączenia.

Przykład:

Jeśli przychodzące połączenia wewnętrzne i zewnętrzne, które otrzymały sygnał zajętości, mają być przekierowywane do poczty głosowej dla tej linii, zaznacz pole wyboru Voice Mail (Poczta głosowa) znajdujące się obok pozycji Forward Busy Internal (Przekieruj zajęte wewnętrzne) i Forward Busy External (Przekieruj zajęte zewnętrzne) w obszarze Call Pickup and Call Forward Settings.

g) W polu Line 1 w okienku Urządzenie skonfiguruj następujące pola:

- Display (Internal Caller ID field) (Wyświetl (pole identyfikatora wewnętrznego użytkownika dzwoniącego)): możesz wprowadzić imię i nazwisko użytkownika urządzenia, tak aby wyświetlać je w przypadku wszystkich połączeń wewnętrznych. Pozostaw to pole puste, jeśli system ma wyświetlać numer wewnętrzny telefonu.
- External Phone Number Mask (Maska zewnętrznego numeru telefonu): wskazuje numer telefonu (tzw. maskę), który będzie używany w przesyłanych informacjach o identyfikatorze abonenta dzwoniącego przy nawiązywaniu połączenia na tej linii. Można wprowadzić do 24 cyfr i znaków "X". Znaki X oznaczają numer telefonu i muszą znajdować się na końcu szablonu.

Przykład:

Jeśli podano maskę 408902XXXX, połączenie zewnętrzne z numeru wewnętrznego 6640 będzie wskazywało identyfikator abonenta dzwoniącego o postaci 4089026640.

To ustawienie dotyczy tylko bieżącego urządzenia, o ile nie zostanie zaznaczone pole wyboru po prawej stronie (Update Shared Device Settings — Aktualizuj współdzielone ustawienia urządzeń) i nie kliknięto przycisku **Propagate Selected** (Propaguj wybrane). Pole wyboru po prawej stronie jest wyświetlane tylko wtedy, gdy inne urządzenia współdzielą dany numer telefonu.

h) Kliknij przycisk **Zapisz**.

Więcej informacji na temat numerów telefonów można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager i korzystając z pokrewnych łączy.

Krok 10 (Opcjonalne) Skojarz użytkownika z telefonem. Kliknij przycisk **Associate End Users** (Skojarz użytkowników końcowych) u dołu okna Phone Configuration (Konfiguracja telefonu), aby powiązać użytkownika z konfigurowaną linią.

a) Użyj przycisku **Znajdź** w połączeniu z polami wyszukiwania, aby znaleźć użytkownika.
b) Zaznacz pole wyboru obok nazwy użytkownika i kliknij przycisk **Add Selected** (Dodaj wybrane).

Nazwa i identyfikator użytkownika zostaną wyświetlone w okienku Users Associated With Line (Użytkownicy skojarzeni z linią) w oknie Directory Number Configuration (Konfiguracja numeru telefonu).

c) Kliknij przycisk **Zapisz**.

Użytkownik jest teraz skojarzony z Linią 1 w telefonie.

Krok 11 (Opcjonalne) Skojarz użytkownika z urządzeniem:

a) Wybierz kolejno opcje **Zarządzanie użytkownikami** > **Użytkownik końcowy**.
b) Użyj pól wyszukiwania i przycisku **Znajdź**, aby odnaleźć dodanego użytkownika.
c) Kliknij identyfikator użytkownika.
d) W obszarze Directory Number Associations (Skojarzenia numeru telefonu) ustaw główny numer wewnętrzny, posługując się listą rozwijaną.
e) (Opcjonalne) W polu Mobility Information (Informacje o funkcji Mobility) zaznacz pole wyboru Enable Mobility (Włącz funkcję Mobility).
f) W obszarze Permissions Information (Informacje o uprawnieniach) użyj przycisków **Add to Access Control Group** (Dodaj do grupy kontroli dostępu) 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).

g) Aby wyświetlić szczegółowe informacje o grupie, wybierz ją i kliknij przycisk **View Details** (Wyświetl szczegóły).
h) W obszarze Extension Mobility zaznacz pole wyboru Enable Extension Mobility Cross Cluster (Włącz klaster krzyżowy przenośnego numeru wewnętrznego), jeśli użytkownik może korzystać z usługi klastra krzyżowego przenośnego numeru wewnętrznego.
i) W obszarze Device Information (Informacje o urządzeniu) kliknij przycisk **Device Associations** (Skojarzenia urządzenia).
j) Użyj pól wyszukiwania oraz przycisku **Znajdź**, aby odnaleźć urządzenie, które chcesz skojarzyć z użytkownikiem.
k) Wybierz urządzenie i kliknij przycisk **Save Selected/Changes** (Zapisz wybrane/zmiany).
l) Kliknij przycisk **Przejdź** obok odpowiedniego łącza "Back to User" (Powrót do użytkownika) w prawym górnym rogu ekranu.
m) Kliknij przycisk **Zapisz**.

Krok 12 Dostosuj do swoich potrzeb szablony klawiszy programowych. Wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Szablon klawiszy programowych**.

Użyj tej strony, aby dodać, usunąć lub zmienić kolejność funkcji klawisza programowego wyświetlanego na telefonie użytkownika, aby dostosować je do jego potrzeb.

Telefon konferencyjny ma specjalne wymagania dotyczące klawiszy programowych. Pokrewne łącza pozwolą uzyskać więcej informacji.

Krok 13 Skonfiguruj usługi telefonu IP Cisco i przypisz je. Wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Common Phone Profile** (Wspólny profil telefonu).

Udostępnia w telefonie usługi telefonu IP.

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

Krok 14 (Opcjonalne) Dodaj informacje o użytkowniku do globalnej książki telefonicznej programu Cisco Unified Communications Manager. Wybierz kolejno opcje **Zarządzanie użytkownikami** > **Użytkownik końcowy**, a następnie kliknij przycisk **Dodaj nowy** i skonfiguruj wymagane pola. Wymagane pola są oznaczone gwiazdką (*).

Uwaga Jeśli do przechowywania informacji o użytkownikach w firmie jest używany katalog LDAP (Lightweight Directory Access Protocol), system Cisco Unified Communications można zainstalować i skonfigurować tak, aby korzystał z istniejącego katalogu LDAP. Patrz Konfigurowanie firmowej książki telefonicznej, na stronie 131. Po zaznaczeniu pola Enable Synchronization (Włącz synchronizację) na serwerze LDAP nie będzie możliwe dodanie nowych użytkowników w narzędziu Cisco Unified Communications Manager — administracja.

a) Ustaw pola identyfikatora i nazwiska użytkownika.
b) Przypisz hasło (do Portalu samoobsługowego).
c) Przypisz kod PIN (do funkcji Cisco Extension Mobility i osobistej książki adresowej).
d) Skojarz użytkownika z telefonem.

Umożliwia użytkownikowi kontrolowanie funkcji telefonu, np. przekazywanie połączeń lub dodawanie numerów szybkiego wywoływania albo usług.

Uwaga Niektóre telefony, takie jak znajdujące się w pokojach konferencyjnych, nie mają skojarzonych użytkowników.

Krok 15 (Opcjonalne) Skojarz użytkownika z grupą użytkownika. Wybierz kolejno opcje **Zarządzanie użytkownikami** > **Ustawienia użytkowników** > **Grupa kontroli dostępu**.

Przypisz do użytkowników wspólną listę ról i uprawnień, które dotyczą wszystkich użytkowników w grupie użytkownika. Administratorzy mogą zarządzać grupami użytkownika, rolami i uprawnieniami w celu kontroli poziomu dostępu (czyli poziomu zabezpieczeń) dla użytkowników systemu.

Aby użytkownicy końcowi mieli dostęp do Portalu samoobsługowego Cisco Unified Communications, należy dodać ich do standardowej grupy użytkowników końcowych programu Cisco Communications Manager:

Tematy pokrewne

Konfiguracja specyficzna dla produktu, na stronie 102
Funkcje i konfiguracja telefonu konferencyjnego IP Cisco, na stronie 97
Cisco Unified Communications Manager — Dokumentacja, na stronie 14
Konfigurowanie nowego szablonu klawiszy programowych, na stronie 98

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 wybierz kolejno opcje **Ustawienia** > **Informacje o telefonie** i sprawdź zawartość pola Adres MAC.
- Sprawdź etykietę z adresem MAC z tylu 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 62.

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

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

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 14

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 14

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 65.

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 14

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 trybowi Survivable Remote Site Telephony (SRST) podstawowe funkcje telefonu pozostają dostępne po zerwaniu komunikacji z kontrolującym go serwerem Cisco Unified Communications Manager. W takiej sytuacji telefon może utrzymać trwające połączenie, a użytkownik zachowuje dostęp do podzbioru dostępnych funkcji. Gdy nastąpi przełączenie awaryjne, użytkownik otrzyma w telefonie komunikat alertu.

Informacje o trybie SRST można znaleźć w https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

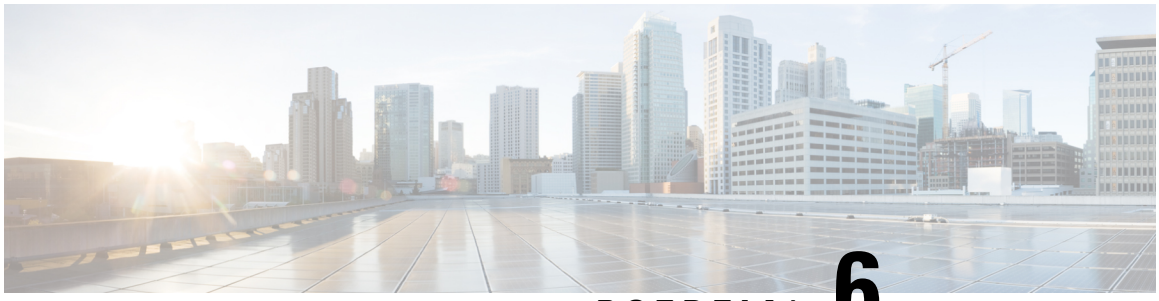
W poniższej tabeli opisano dostępność funkcji w trakcie przełączenia awaryjnego.

Tabela 14: Obsługa funkcji w trybie SRST

Funkcja	Obsługiwany	Uwagi
NowePoł	Tak	
Rozłączanie	Tak	
Wybierz ponownie	Tak	
Odbierz	Tak	

Funkcja	Obsługiwany	Uwagi
Zawieszanie	Tak	
Wznów	Tak	
Połączenie konferencyjne	Tak	Tylko 3-stronna i lokalne miksowanie dźwięku.
Lista konferencji	Nie	
Przenoszenie	Tak	Tylko połączenie konsultacyjne.
Przekazywanie do połączeń aktywnych (przekazywanie bezpośrednie)	Nie	
Automatyczne odbieranie	Tak	
Połączenie oczekujące	Tak	
ID abonenta dzwoniącego	Tak	
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	
Dostęp do poczty głosowej (iDivert)	Nie	Klawisz programowy iDivert nie jest wyświetlany.

Funkcja	Obsługiwany	Uwagi
Filtry linii	Częściowe	Linie są obsługiwane, ale nie można ich udostępniać.
Monitorowanie parkowania	Nie	Klawisz programowy Parkowanie nie jest wyświetlany.
Rozszerzony wskaźnik wiadomości oczekującej	Tak	Na wyświetlaczu telefonu pojawiają się znaczki liczby wiadomości.
Kierowane parkowanie połączenia	Nie	Klawisz programowy nie jest wyświetlany.
Cofnięcie zawieszenia	Tak	
Zdalne zawieszenie	Nie	Połączenia są oznaczane jako zawieszone lokalnie.
Meet Me	Nie	Klawisz programowy PokKonf nie jest wyświetlany.
Przejmij	Tak	
Przejmij grupę	Nie	Klawisz programowy nie jest wyświetlany.
Przejmij inne	Nie	Klawisz programowy nie jest wyświetlany.
Identyfikator złych połączeń	Tak	
QRT	Tak	
Grupa wyszukiwania	Nie	Klawisz programowy nie jest wyświetlany.
Przenoszenie	Nie	Klawisz programowy nie jest wyświetlany.
Prywatność	Nie	Klawisz programowy nie jest wyświetlany.
Oddzwoń	Nie	Klawisz programowy Oddzwoń nie jest wyświetlany.
Adres URL usługi	Tak	Klawisz linii programowalnej z przypisanym adresem URL usługi nie jest wyświetlany.



ROZDZIAŁ 6

Zarządzanie portalem samoobsługowym

- Portal samoobsługowy — omówienie, na stronie 71
- Konfigurowanie dostępu użytkownika do portalu Self Care, na stronie 72
- Dostosowywanie wyświetlania w portalu Self Care, na stronie 72

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 ManagerCisco Unified CM Administration, aby dodać go do Cisco Unified Communications Managerstandardowej grupy użytkowników.

Użytkownikom należy dostarczyć następujące informacje o Portalu samoobsługowym.

- Adres URL umożliwiający dostęp do aplikacji. Ten adres URL to:

  `https://<server_name:portnumber>/użytkownik_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 14

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).

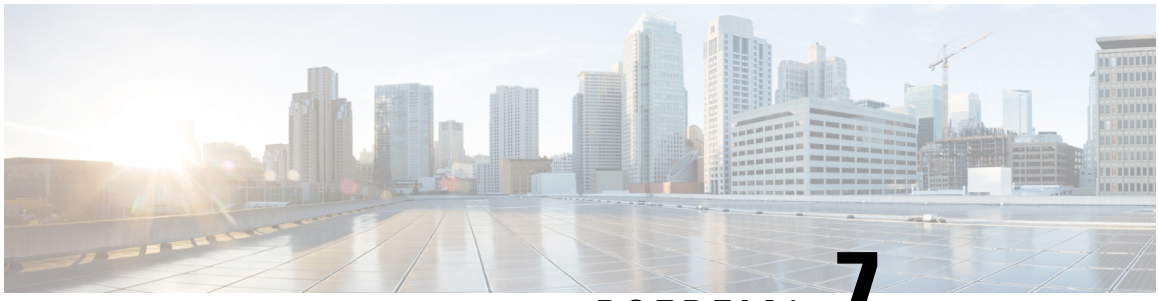
Krok 3 Włącz lub wyłącz parametry, do których użytkownicy mają mieć dostęp w portalu.

Krok 4 Kliknij przycisk **Zapisz**.

CZĘŚĆ III

Administrowanie telefonem konferencyjnym IP Cisco

- Zabezpieczenia telefonu konferencyjnego IP Cisco, na stronie 75
- Dostosowywanie telefonu konferencyjnego IP Cisco, na stronie 93
- Funkcje i konfiguracja telefonu konferencyjnego IP Cisco, na stronie 97
- Firmowa książka telefoniczna i osobista książka telefoniczna, na stronie 131



ROZDZIAŁ 7

Zabezpieczenia telefonu konferencyjnego IP Cisco

- Zabezpieczenia telefonu IP Cisco — przegląd, na stronie 75
- Zwiększone zabezpieczenia Twojej sieci telefonicznej, na stronie 76
- Obsługiwane funkcje zabezpieczeń, na stronie 77

Zabezpieczenia telefonu IP Cisco — przegląd

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.

Więcej informacji o tych funkcjach zabezpieczeń można znaleźć w dokumentacji konkretnej wersji programu Cisco Unified Communications Manager.

Po wykonaniu wymaganych zadań związanych z Funkcją pełnomocnictw certyfikatu na telefonach zostanie zainstalowany Certyfikat znaczenia lokalnego (LSC, Locally Significant Certificate). Do skonfigurowania certyfikatu LSC można wykorzystać moduł Cisco Unified Communications Manager — administracja. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

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

Można również zainicjować instalację certyfikatu LSC z menu Konfiguracja zabezpieczeń na telefonie. Za pośrednictwem tego menu można również zaktualizować lub usunąć certyfikat LSC.

Telefony konferencyjne IP Cisco 8832 są zgodne ze standardem FIPS. Do poprawnego funkcjonowania tryb FIPS wymaga klucza RSA o długości co najmniej 2048 bitów. Jeśli certyfikat RSA serwera nie ma przynajmniej 2048 bitów, telefon nie zostanie zarejestrowany w programie Cisco Unified Communications Manager, a na telefonie zostanie wyświetlony komunikat `Telefon nie zarejestrował się. Na ekranie komunikatu o stanie widnieje komunikat Rozmiar klucza certyfikatu jest niezgodny ze standardem FIPS`.

W trybie FIPS nie można stosować kluczy prywatnych (LSC lub MIC).

Jeśli telefon ma certyfikat LSC o rozmiarze mniejszym niż 2048 bitów, przed włączeniem trybu FIPS należy go zastąpić kluczem LSC o rozmiarze co najmniej 2048 bitów.

Tematy pokrewne

Konfigurowanie certyfikatu obowiązującego lokalnie, na stronie 80
Cisco Unified Communications Manager — Dokumentacja, na stronie 14

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 teefonu 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).
- *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)
- SIP OAuth w *Podręczniku konfiguracji funkcji programu Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-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.

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.

Poniższa tabela zawiera przegląd funkcji zabezpieczeń obsługiwanych przez telefon konferencyjny IP Cisco 8832. Więcej informacji o tych funkcjach, systemie Cisco Unified Communications Manager i zabezpieczeniach telefonów IP Cisco można znaleźć w dokumentacji konkretnej wersji systemu Cisco Unified Communications Manager.

Tabela 15: Przegląd funkcji zabezpieczeń

Funkcja	Opis
Uwierzytelnianie obrazów	Podpisane pliki binarne (o rozszerzeniu SBN) zapobiegają zm telefonu. Zmanipulowanie obrazu spowoduje niepowodzenie p
Instalacja certyfikatu w siedzibie klienta	Uwierzytelnianie urządzenia wymaga, aby każdy telefon miał r (ang. manufacturing installed certificate, MIC), ale w celu zapew Communications Manager — administracja instalowanie certyf Proxy Function, CAPF). Można również zainstalować certyfik Security Configuration (Konfiguracja zabezpieczeń) w telefon
Uwierzytelnianie urządzenia	Zachodzi między serwerem Cisco Unified Communications M Zależy od tego, czy telefon może nawiązać bezpieczne połącz między obiema stronami tworzona jest zabezpieczona ścieżka s Manager nie rejestruje telefonów, które nie przeszły jego uwie
Uwierzytelnianie plików	Służy do weryfikowania podpisanych cyfrowo plików, które po po jego utworzeniu. Pliki, które nie przejdą uwierzytelniania, dalszego przetwarzania.
Uwierzytelnianie sygnalizowania	Korzysta z protokołu TLS do weryfikacji, czy nie zmanipulow
Certyfikat instalowany fabrycznie	Każdy telefon zawiera niepowtarzalny certyfikat instalowany fa dowód tożsamości telefonu, umożliwiający jego uwierzytelni

Funkcja	Opis
Bezpieczna referencja trybu SRST	Po skonfigurowaniu referencji trybu SRST na potrzeby zab Unified Communications Manager — administracja serwe Zabezpieczony telefon używa później połączenia TLS do
Szyfrowanie mediów	Funkcja ta korzysta z protokołu SRTP do weryfikowania b gwarantowania, że dane może odebrać i odczytać tylko ur urządzeń pary głównych kluczy mediów oraz bezpieczne
Funkcja pełnomocnictw certyfikatu (ang. Certificate Authority Proxy Function, CAPF)	Realizuje elementy procedury generowania certyfikatu, któ kluczy i instalowania certyfikatów. Funkcję CAPF można urzędów certyfikacji wskazanych przez klienta lub generow
Profile zabezpieczeń	Określa, czy telefon jest niezabezpieczony, uwierzytelnion
Szyfrowane pliki konfiguracyjne	Funkcja umożliwiająca zapewnienie poufności plików ko
Opcjonalne wyłączanie w telefonie funkcji serwera WWW	Można zapobiegać dostępowi do strony WWW telefonu,
Zwiększanie bezpieczeństwa telefonu	Dodatkowe opcje zabezpieczeń konfigurowane za pomocą • Wyłączanie dostępu do stron WWW telefonu **Uwaga** Bieżące ustawienia opcji Włączono protokół telefonu.
Uwierzytelnianie 802.1X	Telefon może korzystać z uwierzytelniania 802.1X przy ża
Szyfrowanie AES 256	Po nawiązaniu połączenia z programem Cisco Unified Com AES 256 w przypadku szyfrowania sygnalizacji i mediów połączeń TLS 1.2 z użyciem szyfrów opartych na AES 256 algorytm wyznaczania wartości skrótu) i FIPS (Federal In Nowe szyfry: • W przypadku połączeń TLS: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • W przypadku połączeń sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Więcej wiadomości na ten temat można znaleźć w dokum
Certyfikaty ECDSA (Elliptic Curve Digital Signature Algorithm)	W ramach certyfikacji Common Criteria (CC) do systemu C Dotyczy to wszystkich produktów systemu Voice Operating

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

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 wybierz opcję **Ustawienia**.

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 uwierzytelnienia.

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.

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

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 strumienie 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. Zabezpieczone połączenia konferencyjne, funkcję Cisco Extension Mobility i linie wspólne można skonfigurować za pomocą zabezpieczonego mostka konferencyjnego.

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 16: 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 spełni bezpieczeństwa, połączenie od`
Secure	Meet Me	Minimalny poziom bezpieczeństwa to niezabezpieczony.	Zabezpieczony mostek konferencyjny Konferencja jest otwarta na wszystkie poła

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.

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 uwierzytelniania 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. Jedyną obsługiwaną wersją protokołu jest PEAP MSCHAPV2. Wersja PEAP-GTC nie jest obsługiwana.

Następujące systemy uwierzytelnianie 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 roadmingu. 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 uwierzytelnianiu.

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 uwierzytelniać 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 17: Systemy uwierzytelniania i szyfrowania

Konfiguracja telefonu IP Cisco	**Konfiguracja punktu dostępu**			
Tryb zabezpieczeń	Bezpieczeństwo	Zarządzanie kluczami	Szyfrowanie	Szybki roaming
Brak	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

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

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.

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 rozpoczniesz

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

Krok 1 W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Telefon**.

Krok 2 Zlokalizuj swój telefon.

Krok 3 W oknie **Układ konfiguracji specyficznej dla produktu** ustaw wartość parametru **Administracja WWW** na **Włączone**.

Krok 4 W polu **Hasło administratora** wpisz hasło.

Krok 5 Wybierz opcję **Zapisz** i kliknij przycisk **OK**.

Krok 6 Wybierz opcję **Zastosuj konfigurację** i kliknij przycisk **OK**.

Krok 7 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**.

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 Certififcate) 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 Przejdź do certyfikatu na swoim komputerze.

Krok 3 W polu **Hasło wyodrębniania** wprowadź hasła wyodrębniania certyfikatu.

Krok 4 Kliknij przycisk **Prześlij**.

Krok 5 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 rozpoczniesz

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.

Obsługa uwierzytelniania 802.1X wymaga kilku składników:

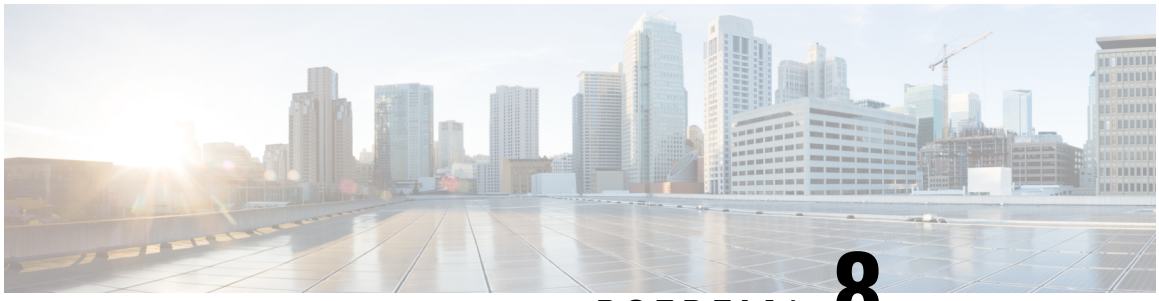
- Telefon IP Cisco: telefon inicjuje żądanie dostępu do sieci. Telefony zawierają stronę uwierzytelnianą 802.1X. Dzięki niej administratorzy sieci mogą kontrolować łączność telefonów IP z portami przełącznika sieci LAN. Bieżąca wersja strony uwierzytelnianej 802.1X w telefonach korzysta z opcji EAP-FAST i EAP-TLS do uwierzytelniania sieci.
- 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 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 do macierzystej sieci VLAN.

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14



ROZDZIAŁ 8

Dostosowywanie telefonu konferencyjnego IP Cisco

- Niestandardowe sygnały dzwonka, na stronie 93
- Dostosowywanie sygnału wybierania, na stronie 95

Niestandardowe sygnały dzwonka

Telefon IP Cisco jest fabrycznie wyposażony w dwa domyślne sygnały dzwonka, które są zapisane w jego warstwie sprzętowej: Chirp1 i Chirp2. Program Cisco Unified Communications Manager udostępnia ponadto domyślny zestaw dodatkowych sygnałów dzwonka, które są zaimplementowane w warstwie programowej jako pliki PCM (ang. pulse code modulation, modulacja impulsowo-kodowa). Pliki PCM razem z plikiem XML, w którym opisano opcje listy dzwonków 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 niepoprawnej wielkości liter w nazwie pliku telefon nie zastosuje wprowadzonych w nim zmian.

Aby uzyskać więcej informacji, patrz rozdział „Custom Phone Rings and Backgrounds” (Niestandardowe sygnały dzwonka i tła) w Podręczniku konfiguracji funkcji programu Cisco Unified Communications Manager.

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

Konfigurowanie niestandardowego dzwonka telefonu

Procedura

Krok 1 Utwórz plik PCM dla każdego niestandardowego dzwonka (jeden dzwonek na plik).

Upewnij się, że pliki PCM są zgodne z wytycznymi formatu podanymi w części Formaty plików dzwonków niestandardowych.

Krok 2 Prześlij nowe utworzone przez siebie pliki PCM na serwer TFTP Cisco odpowiedni dla każdego serwera Cisco Unified Communications Manager należącego do klastra.

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

Krok 3 Zapisz zmiany i zamknij plik Ringlist-wb.

Krok 4 Aby zapisać nowy plik Ringlist-wb w pamięci podręcznej:

- Zatrzymaj i uruchom ponownie usługę TFTP za pomocą funkcji serwisowania systemu Cisco Unified
- Wyłącz i włącz ponownie parametr usługi TFTP "Enable Caching of Constant and Bin Files at Startup" (Włącz zapisywanie do pamięci podręcznej plików stałych i binarnych podczas uruchamiania) znajdujący się w obszarze Advanced Service Parameters (Zaawansowane parametry usługi).

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

Formaty plików dzwonków niestandardowych

W pliku Ringlist-wb.xml znajdują się definicje obiektów XML zawierających listę typów dzwonków telefonu. Taki plik zawiera do 50 typów dzwonków. Każdy typ dzwonka zawiera wskaźnik do pliku PCM używanego przez dany typ dzwonka oraz tekst wyświetlany dla tego dzwonka w menu typu dzwonka telefonu IP Cisco. Taki plik jest przechowywany na serwerze TFTP programu Cisco Unified Communications Manager.

Do opisu informacji obiekt XML CiscoIPPhoneRinglist używa następującego zestawu prostych tagów:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

Nazwy definicji mają następujące cechy. Każdy typ dzwonka telefonu musi mieć nazwy DisplayName (nazwa wyświetlana) i FileName (nazwa pliku).

- Nazwa DisplayName określa nazwę niestandardowego dzwonka w skojarzonym pliku PCM, która jest wyświetlana w menu Typ dzwonka telefonu IP Cisco.
- Nazwa FileName określa nazwę niestandardowego pliku PCM, który ma zostać skojarzony z nazwą DisplayName.

Uwaga Pola DisplayName i FileName nie mogą zawierać więcej niż 25 znaków.

W tym przykładzie pokazano plik Ringlist-wb.xml zawierający definicje dwóch typów dzwonków telefonu.

```
<CiscoIPPhoneRingList>
 <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.rwb</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
```

```
      <FileName>Analog2.rwb</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

Pliki PCM, które mogą być odtwarzane w telefonach IP Cisco, muszą spełniać następujące wymagania:

- Plik PCM typu „raw” (bez nagłówka)
- 8000 próbek na sekundę
- 8 bitów na próbkę
- Kompresja mu-law
- Maksymalna wielkość dzwonka = 16 080 próbek
- Minimalna wielkość dzwonka = 240 próbek
- Liczba próbek w dzwonku = wielokrotność 240.
- Dzwonek rozpoczyna się i kończy przy przejściu sygnału przez zero.

Aby utworzyć pliki PCM dla niestandardowych dzwonków, należy użyć dowolnego pakietu do edycji standardowych plików audio, który obsługuje wymagany format pliku.

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.

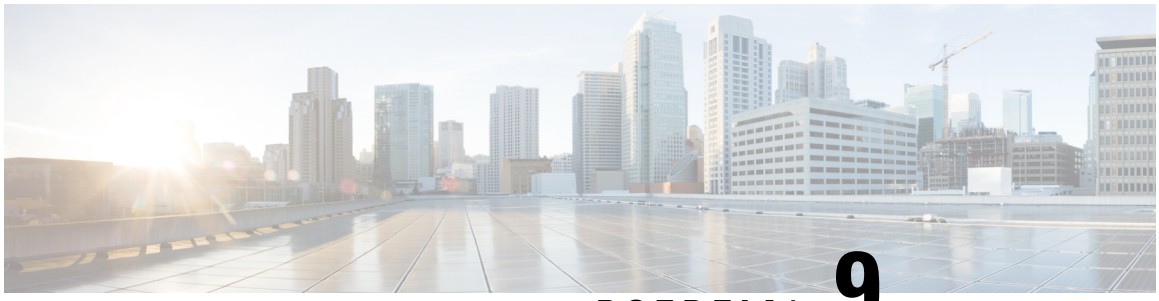
Krok 5 Wybierz dla opcji **Zawsze używaj sygnału wybierania** jedno z następujących ustawień:

- Sieć zewnętrzna
- Sieć wewnętrzna

- Domyślny

Krok 6 Kliknij przycisk **Zapisz**.

Krok 7 Uruchom ponownie telefony.



ROZDZIAŁ 9

Funkcje i konfiguracja telefonu konferencyjnego IP Cisco

- Pomoc techniczna dla użytkowników telefonu IP Cisco, na stronie 97
- Bezpośrednia migracja telefonu do telefonu wieloplatformowego, na stronie 98
- Konfigurowanie nowego szablonu klawiszy programowych, na stronie 98
- Konfigurowanie usług telefonicznych dla użytkowników, na stronie 99
- Konfigurowanie funkcji telefonu, na stronie 100

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

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-ipphone.html

Konfigurowanie nowego szablonu klawiszy programowych

Aby umożliwić użytkownikom dostęp do niektórych funkcji, do szablonu klawiszy programowych trzeba dodać odpowiednie klawisze. Na przykład aby użytkownicy mogli korzystać z funkcji nie przeszkadzać, trzeba włączyć odpowiadający jej klawisz programowy. Więcej informacji na ten temat można znaleźć w dokumentacji używanej wersji programu Cisco Unified Communications Manager.

Można utworzyć kilka szablonów. Na przykład jeden szablon dla telefonu w sali konferencyjnej i drugi dla telefonu w gabinecie dyrektora.

Ta procedura przedstawia krok po kroku tworzenie nowego szablonu klawiszy programowych i przypisywanie go do określonego telefonu. Podobnie jak inne funkcje telefonu, szablon można zastosować do wszystkich telefonów konferencyjnych lub do grupy telefonów.

Procedura

Krok 1 Zaloguj się jako administrator w aplikacji Cisco Unified Communications Manager — administracja.

Krok 2 Wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Szablon klawiszy programowych**.

Krok 3 Kliknij przycisk **Find** (Znajdź).

Krok 4 Wybierz jedną z następujących opcji:

- Cisco Unified Communications Manager 11.5 i wcześniejsze wersje — **użytkownik standardowy**
- Cisco Unified Communications Manager 12.0 i nowsze wersje — **użytkownik konferencji osobistych** lub **użytkownik konferencji publicznych**.

Krok 5 Kliknij przycisk **Kopiuj**.

Krok 6 Zmień nazwę szablonu.

Na przykład Szablon dla sali konferencyjnej 8832.

Krok 7 Kliknij przycisk **Zapisz**.

Krok 8 Za pomocą menu w prawym górnym rogu otwórz stronę **Konfigurowanie układu klawiszy programowych**.

Krok 9 Ustaw wyświetlane funkcje dla każdego stanu połączenia.

Krok 10 Kliknij przycisk **Zapisz**.

Krok 11 Za pomocą menu w prawym górnym rogu wróć na stronę **Znajdź/Lista**.

Nowy szablon będzie widoczny na liście szablonów.

Krok 12 Wybierz kolejno opcje **Urządzenie** > **Telefon**.

Krok 13 Znajdź i wybierz telefon, na którym chcesz używać nowego szablonu.

Krok 14 W polu **Szablon klawiszy programowych** wybierz nowy szablon klawiszy programowych.

Krok 15 Kliknij kolejno **Zapisz** i **Zastosuj konfigurację**.

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

Konfigurowanie usług telefonicznych dla użytkowników

Można przyznawać użytkownikom dostęp do usług telefonu IP Cisco. Można też przypisywać poszczególne usługi telefoniczne do osobnych przycisków. Telefon IP traktuje każdą usługę jak oddzielną aplikację.

Zanim użytkownik będzie mógł skorzystać z jakiejkolwiek 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 Portal samoobsługowy — omówienie, na stronie 71.

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

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.

Tematy pokrewne

Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway, na stronie 126

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 **Zastąp 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.

Tematy pokrewne

Konfiguracja specyficzna dla produktu, na stronie 102

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.

Tematy pokrewne

Konfiguracja specyficzna dla produktu, na stronie 102

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.

Tematy pokrewne

Konfiguracja specyficzna dla produktu, na stronie 102

Konfiguracja specyficzna dla produktu

W poniższej tabeli opisano pola widoczne w okienku Układ konfiguracji specyficznej dla produktu. Niektóre pola z tej tabeli są wyświetlane tylko na stronie **Urządzenie** > **Telefon**.

Tabela 18: Pola konfiguracji specyficznej dla produktu

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Dostęp do ustawień	Wyłączone włączone Ograniczony	włączone	Włącza i wyłącza lokalną konfigurację w aplikacji Ustawienia i ogranicza dostęp do niej. W przypadku ograniczonego dostępu można używać menu Preferencje i Informacje o systemie. Dostępne są również niektóre ustawienia w menu Wi-Fi. Przy wyłączonym dostępie w menu Ustawienia nie są wyświetlane żadne opcje.
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.
Dostęp przez WWW	Wyłączone włączone	Wyłączone	Włącza lub wyłącza dostęp do stron WWW telefonu za pomocą przeglądarki. **Przestroga** Jeśli to pole jest włączone, poufne informacje o telefonie mogą zostać ujawnione.
Wyłącz protokół TLS 1.0 i TLS 1.1 przy dostępie przez WWW	Wyłączone włączone	włączone	Steruje korzystaniem z protokołu TLS 1.2 przy połączeniu z serwerem WWW. • Wyłączone — telefon skonfigurowany dla protokołów TLS1.0, TLS 1.1 lub TLS1.2 może pełnić funkcję serwera HTTPS. • Włączone — tylko telefon skonfigurowany dla protokołów TLS1.0, TLS 1.1 lub TLS1.2 może pełnić funkcję serwera HTTPS.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Wybieranie blokowe	Wyłączone włączone	Wyłączone	Kontroluje metodę wybierania. • Wyłączone — System Cisco Unified Communications Manager czeka na wygaśnięcie czasomierza między cyframi w przypadku nakładania się planu wybierania lub wzorca tras. • Włączone — 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. 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.
Dni nieaktywn. podświet.	Dni tygodnia		Określa dni, w których podświetlenie nie włącza się automatycznie o godzinie określonej w polu Godz. wł. podświetl. Wybierz dzień lub dni z listy rozwijanej. Aby wybrać więcej niż jeden dzień, naciśnij klawisz **Ctrl i kliknij** każdy wybrany dzień. Zobacz Planowane oszczędzanie energii Power Save dla telefonów IP Cisco, na stronie 115.
Godz. wł. podświetl.	gg:mm		Określa godzinę, o której każdego dnia jest automatycznie włączane podświetlenie (z wyjątkiem dni określonych w polu Dni nieaktywn. podświet.). W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 0:00 oznacza północ. Aby na przykład podświetlenie automatycznie włączało się o godzinie 7:00 rano. (0700), wprowadź 07:00. Aby włączyć podświetlenie o drugiej po południu, (1400), wprowadź 14:00. Jeśli to pole jest puste, podświetlenie jest automatycznie włączane o godzinie 00:00. Zobacz Planowane oszczędzanie energii Power Save dla telefonów IP Cisco, na stronie 115.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Czas trwania podświetlenia	gg:mm		Określa czas, przez który podświetlenie pozostaje włączone po godzinie określonej w polu Godz. wł. podświetl. Aby zachować podświetlenie np. przez 4 godziny i 30 minut po włączeniu, wprowadź 04:30. Jeśli to pole jest puste, telefon wyłączy się na koniec dnia (00:00). Jeśli wartość pola Godz. wł. podświetl. wynosi 00:00 i czas trwania podświetlenia jest pusty (lub wynosi 24:00), podświetlenie nie jest włączane. Zobacz Planowane oszczędzanie energii Power Save dla telefonów IP Cisco, na stronie 115.
Limit czasu nieakt. podświetl.	gg:mm		Określa czas bezczynności telefonu, po upłynięciu którego zostanie wyłączone podświetlenie. Działa tylko wtedy, gdy podświetlenie zostało wyłączone zgodnie z planem, po czym użytkownik włączył je ponownie (naciskając przycisk telefonu lub podnosząc słuchawkę). Aby wyłączyć podświetlenie po okresie bezczynności równym np. 1 godzinę i 30 minut, wprowadź 01:30. Zobacz Planowane oszczędzanie energii Power Save dla telefonów IP Cisco, na stronie 115.
Wł. podśw. podczas rozm. przych.	Wyłączone włączone	włączone	Włącza podświetlenie po nadejściu połączenia przychodzącego.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Włącz Power Save Plus	Dni tygodnia		Określa dni, w których telefon jest wyłączany. Wybierz dzień lub dni z listy rozwijanej. Aby wybrać więcej niż jeden dzień, naciśnij klawisz **Ctrl i kliknij** każdy wybrany dzień. Po włączeniu opcji Power Save Plus zostanie wyświetlony komunikat ostrzegający o potencjalnych zagrożeniach (e911). **Przestroga** 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. 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. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Godzina włączenia telefonu	gg:mm		Określa, że telefon włącza się automatycznie w dni wybrane w polu Włącz Power Save Plus. W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ. Aby automatycznie włączyć telefon np. o godzinie 7 rano, (0700), wprowadź 07:00. Aby włączyć telefon o drugiej po południu, (1400), wprowadź 14:00. Wartość domyślna jest pusta, co oznacza 00:00. 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. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.
Godzina wyłączenia telefonu	gg:mm		Określa godzinę, 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. W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ. Aby automatycznie wyłączyć telefon np. o godzinie 7 rano, (0700), wprowadź 7:00. Aby wyłączyć telefon o drugiej po południu, (1400), wprowadź 14:00. Wartość domyślna jest pusta, co oznacza 00:00. 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. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Wyłącz telefon po czasie nieaktywności	gg:mm		Wskazuje czas nieaktywności telefonu, po upłynięciu którego zostanie on wyłączony. Limit czasu jest uwzględniany w następujących okolicznościach: • Gdy telefon był w trybie Power Save Plus zgodnie z harmonogramem i wyszedł z tego trybu po naciśnięciu przez użytkownika klawisza Wybierz. • Gdy ponownie włączono zasilanie telefonu za pomocą przełącznika. • Jeśli osiągnięto godzinę określoną przez parametr Godzina wyłączenia telefonu, ale telefon jest nadal używany. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.
Włącz alert dźwiękowy	Pole wyboru	Niezaznaczone	Po włączeniu tej opcji telefon odtwarza alert dźwiękowy na 10 minut przed godziną podaną w polu Godzina wyłączenia telefonu. To pole wyboru jest uwzględniane tylko wtedy, gdy w polu listy Włącz Power Save Plus zaznaczono co najmniej jeden dzień. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.
Domena EnergyWise	Do 127 znaków		Wskazuje domenę EnergyWise, w której znajduje się telefon. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.
Hasło EnergyWise	Do 127 znaków		Określa tajne hasło zabezpieczeń używane podczas komunikacji z punktami końcowymi w domenie EnergyWise. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Zezwól na zastąpienie przez EnergyWise	Pole wyboru	Niezaznaczone	Określa, czy zasady kontrolera domeny EnergyWise mogą zezwalać na wysyłanie do telefonu informacji o zmianie poziomu zasilania. Muszą zostać spełnione następujące warunki: • W polu Włącz Power Save Plus musi być wybrany co najmniej jeden dzień. • Ustawienia w narzędziu Cisco Unified Communications Manager — administracja są wdrażane nawet wtedy, gdy funkcja EnergyWise przysyła komunikat o zastąpieniu. 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. • 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. • 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. • Aby ponownie zmienić poziom zasilania w telefonie, funkcja EnergyWise musi wysłać nowe polecenie o zmianie poziomu zasilania. 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. Zobacz Tworzenie harmonogramu funkcji EnergyWise w telefonie IP Cisco, na stronie 116.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Zasady dołączania i przekazu bezpośredniego	Włącz na tej samej linii Wyłącz na tej samej linii	Ta sama linia, włącz między liniami	Zarządza możliwością dołączania do połączeń i ich przekazywania przez użytkownika. • Włącz na tej samej linii — użytkownicy mogą bezpośrednio dołączać do połączenia lub przekazywać je z bieżącej linii do innego połączenia na tej samej linii. • Wyłącz na tej samej linii — 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.
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: **`adres:<port>@@base=<0-7>;pfs=<0-1>`**
Dziennik zdalny	Wyłączone włączone	Wyłączone	Służy do sterowania możliwością wysyłania dzienników do serwera dziennika systemowego.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Profil dziennika	Domyślny Ustawienie wstępne Telefonia SIP IU Network Nośniki Uaktualnienie Urządzenie Bezpieczeństwo EnergyWise MobileRemoteAccess	Ustawienie wstępne	Określa wstępnie zdefiniowany profil dziennika. • Domyślny — domyślny poziom dziennika debugowania • Ustawienie wstępne — nie zastępuje lokalnego ustawienia dziennika debugowania w telefonie • Telefonia — zapisuje w dzienniku informacje o połączeniach i funkcjach telefonii • SIP — zapisuje w dzienniku informacje o sygnalizacji SIP • IU — zapisuje w dzienniku informacje o interfejsie użytkownika telefonu • Sieć — zapisuje w dzienniku informacje o sieci • Nośniki — zapisuje w dzienniku informacje o nośnikach • Uaktualnienie — zapisuje w dzienniku informacje o uaktualnieniach • Urządzenie — zapisuje w dzienniku informacje o akcesoriach • Zabezpieczenia — zapisuje w dzienniku informacje o zabezpieczeniach • EnergyWise — zapisuje w dzienniku informacje o oszczędzaniu energii • MobileRemoteAccess — zapisuje w dzienniku informacje o dostępie z urządzeń przenośnych i dostępie zdalnym za pośrednictwem usługi Expressway
Serwer dziennika protok. IPv6	Ciąg o długości do 256 znaków		Określa serwer dziennika systemowego IPv6 na potrzeby danych stworzonych podczas debugowania telefonu.
Cisco Discovery Protocol (CDP): port przełącznika	Wyłączone włączone	włączone	Kontroluje protokół CDP w telefonie.
Link Layer Discovery Protocol — Media Endpoint Discover (LLDP-MED): port przełącznika	Wyłączone włączone	włączone	Włącza protokół LLDP-MED na porcie oprogramowania.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
LLDP Asset ID	Ciąg o długości do 32 znaków		Wskazuje identyfikator zasobu przypisanego do telefonu w celu zarządzania zapasami.
Energy Efficient Ethernet (EEE): port przełącznika	Wyłączone włączone	Wyłączone	Steruje protokołem EEE na porcie przełącznika.
LLDP priorytet mocy	Nieznane Niski Wysoki Kluczowy	Nieznane	Przypisuje do przełącznika priorytet zasilania, umożliwiając przełącznikowi właściwe zasilanie telefonów.
Uwierzyt. 802.1x	Sterowane przez użytkownika Wyłączone włączone	Sterowane przez użytkownika	Określa stan funkcji uwierzytelniania 802.1x. • Sterowane przez użytkownika — użytkownik może konfigurować protokół 802.1x na telefonie. • Wyłączone — uwierzytelnianie 802.1x nie jest używane. • Włączone — uwierzytelnianie 802.1x jest używane i można skonfigurować uwierzytelnianie dla telefonów.
Zdalna konfiguracja przełączania portu	Wyłączone Automatyczna negocjacja 10 half 10 full 100 half 100 full	Wyłączone	Umożliwia zdalne skonfigurowanie prędkości i funkcji dupleksu 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.
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).
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).

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
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.
Oprogramowanie sprzętowe dystybuowane przez P2P	Wyłączone włączone	włączone	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 udostępniać 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. Oprogramowanie sprzętowe dystybuowane przez P2P: • Ogranicza przeciążenie przy transferach TFTP ze scentralizowanych serwerów TFTP. • Likwiduje konieczność ręcznego sterowania uaktualnieniami oprogramowania sprzętowego. • Skraca niedostępność telefonów spowodowaną jednoczesnym zresetowaniem wielu telefonów. • Pomaga podczas aktualizacji oprogramowania firmware w oddziałach lub biurach zdalnych połączonych poprzez linie WAN o ograniczonej przepustowości.
Serwer pobierania	Ciąg o długości do 256 znaków		Wskazuje alternatywny serwer IPv4 używany przez telefony do pobierania oprogramowania firmware i uaktualnień.
Serwer pobierania IPv6	Ciąg o długości do 256 znaków		Wskazuje alternatywny serwer IPv6 używany przez telefon do pobierania oprogramowania firmware i uaktualnień.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
Wykrywanie uszkodzenia połączenia z Unified CM	Normalny Opóźnione	Normalny	Określa precyzję, z jaką telefon wykrywa uszkodzenie połączenia z programem Cisco Unified Communications Manager (Unified CM), co jest pierwszym krokiem przy awaryjnym przełączaniu urządzenia do zapasowego systemu Unified CM/SRST. Poprawne wartości to Normalne (wykrywanie niepowodzenia połączenia z serwerem Unified CM ze standardową szybkością) i Opóźnione (wykrywanie niepowodzenia połączenia z serwerem Unified CM jest około cztery razy wolniejsze niż przy wartości Normalne). Aby szybciej wykrywać niepowodzenia połączenia z serwerem Unified CM, wybierz wartość Normalne. Jeśli liczysz na samoistne przywrócenie połączenia i wolisz, aby przełączenie awaryjne zostało nieco opóźnione, wybierz wartość Opóźnione. Precyzyjna różnica czasu między wykryciem uszkodzenia połączenia w obu przypadkach zależy od wielu nieustannie zmieniających się czynników.
Identyfikator wymagań specjalnych	Ciąg		Kontroluje niestandardowe funkcje obciążeń ES (Engineering Special).
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.
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, włącz tę opcję. Poświadczenia logowania do usługi Expressway będą wtedy trwałe. W takim przypadku użytkownik będzie musiał podać poświadczenia logowania tylko za pierwszym razem. Później (po włączeniu telefonu poza siedzibą) dane logowania będą automatycznie uzupełniane na ekranie logowania. Aby uzyskać więcej informacji, patrz Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway, na stronie 126.

Nazwa pola	Typ pola lub dostępne opcje	Domyślny	Opis
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 Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway, na stronie 126.
Wyłącz szyfrowanie TLS	Zobacz Wyłącz szyfrowanie TLS (Transport Layer Security), na stronie 114.	Brak	Wyłącza wybrane szyfrowanie TLS. Wyłącz więcej niż jeden pakiet szyfrowania, przytrzymując klawisz **Ctrl** na klawiaturze komputera i zaznaczając pakiety.
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.

Tematy pokrewne

Konfigurowanie zachowywania poświadczeń użytkownika przy logowaniu do usługi Expressway, na stronie 126

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).

Planowane oszczędzanie energii Power Save dla telefonów IP Cisco

W celu oszczędzania energii elektrycznej i zwiększenia trwałości wyświetlacza telefonu można skonfigurować wyłączanie ekranu, gdy nie jest używany.

W aplikacji Cisco Unified Communications Manager — administracja można skonfigurować wyłączanie wyświetlacza o ustalonej porze w wybrane dni i przez całą dobę w pozostałe dni. Można np. ustawić wyłączanie wyświetlacza po godzinach pracy w dni robocze oraz przez całe dnie 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.

  Poza włączeniem 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.

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 19: 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.

Pole	Opis
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 **07:00**. Aby włączyć wyświetlacz o godzinie 2:00 po południu (1400), wprowadź **14:00**. Jeśli to pole jest puste, wyświetlacz automatycznie włączy się o godzinie 00:00.
Czas wyświetlania	Czas, przez który wyświetlacz pozostaje włączony po włączeniu o godzinie określonej w polu Godz. rozpocz. wyświetl. Wprowadź wartość w tym polu w formacie *godziny:minuty*. Aby na przykład wyświetlacz pozostawał włączony przez 4 godziny i 30 minut po automatycznym włączeniu, wprowadź **04:30**. Jeśli to pole jest puste, telefon wyłączy się na koniec dnia (0:00). **Uwaga** 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.
Czas nieakt. ekranu	Czas bezczynności telefonu, po upłynięciu 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). Wprowadź wartość w tym polu w formacie *godziny:minuty*. Aby na przykład wyświetlacz, po włączeniu go przez użytkownika, wyłączał się po okresie bezczynności równym 1 godzinę i 30 minut, wprowadź **01:30**. Wartość domyślna to 01:00.

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 upłynięciu 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.

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 20: Pola konfiguracji funkcji EnergyWise

Pole	Opis
Włącz Power Save Plus	Określa dni, w których telefon jest wyłączany. Aby wybrać większą liczbę dni, wciśnij i przytrzymaj klawisz Control, jednocześnie klikając dni na harmonogramie. Domyślnie żadne dni nie są zaznaczone. Po zaznaczeniu opcji Power Save Plus zostanie wyświetlony komunikat ostrzegający o potencjalnych zagrożeniach (e911). **Przestroga** W trybie Power Save Plus punkty końcowe skonfigurowane dla tego trybu ("Tryb") 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. **Uwaga** 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.
Godzina włączenia telefonu	Określa, że telefon włącza się automatycznie w dni wybrane w polu Włącz Power Save Plus. W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ. Aby automatycznie włączyć telefon np. o godzinie 7 rano, (0700), wprowadź 07:00. Aby włączyć telefon o drugiej po południu, (1400), wprowadź 14:00. Wartość domyślna jest pusta, co oznacza 00:00. **Uwaga** 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.
Godzina wyłączenia telefonu	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. W tym polu wprowadź godzinę w formacie 24-godzinnym, gdzie 00:00 oznacza północ. Aby automatycznie wyłączyć telefon np. o godzinie 7 rano, (0700), wprowadź 7:00. Aby wyłączyć telefon o drugiej po południu, (1400), wprowadź 14:00. Wartość domyślna jest pusta, co oznacza 00:00. **Uwaga** 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.

Pole	Opis
Wyłącz telefon po czasie nieaktywności	Czas nieaktywności telefonu, po upłynięciu którego zostanie on wyłączony. Limit czasu jest uwzględniany w następujących okolicznościach: • Gdy telefon był w trybie Power Save Plus zgodnie z harmonogramem i wyszedł z tego trybu po naciśnięciu przez użytkownika klawisza **Wybierz** . • Gdy ponownie włączono zasilanie telefonu za pomocą przełącznika. • Jeśli osiągnięto godzinę określoną przez parametr Godzina wyłączenia telefonu, ale telefon jest nadal używany. Pole może przyjmować wartości z zakresu od 20 do 1440 minut. Wartość domyślna to 60 minut.
Włącz alert dźwiękowy	Po włączeniu tej opcji telefon odtwarza alert dźwiękowy na 10 minut przed godziną podaną w polu Godzina wyłączenia telefonu. 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: • Na 10 minut przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany czterokrotnie. • Na 7 minut przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany czterokrotnie. • Na 4 minuty przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany czterokrotnie. • Na 30 sekund przed wyłączeniem zasilania sygnał dzwonka będzie odtwarzany 15 razy lub do momentu wyłączenia telefonu. To pole wyboru jest uwzględniane tylko wtedy, gdy w polu listy Włącz Power Save Plus zaznaczono co najmniej jeden dzień.
Domena EnergyWise	Domena EnergyWise, w której znajduje się telefon. Maksymalna długość tego pola to 127 znaków.
Hasło EnergyWise	Tajne hasło zabezpieczeń używane podczas komunikacji z punktami końcowymi w domenie EnergyWise. Maksymalna długość tego pola to 127 znaków.

Pole	Opis
Zezwól na zastąpienie przez EnergyWise	Pole wyboru określa, czy zasady kontrolera domeny EnergyWise mogą zezwalać na wysyłanie do telefonu informacji o zmianie poziomu zasilania. Muszą zostać spełnione następujące warunki: • W polu Włącz Power Save Plus musi być wybrany co najmniej jeden dzień. • Ustawienia w narzędziu Cisco Unified Communications Manager — administracja są wdrażane nawet wtedy, gdy funkcja EnergyWise przysyła komunikat o zastąpieniu. 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. • 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. • 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. • Aby ponownie zmienić poziom zasilania w telefonie, funkcja EnergyWise musi wysłać nowe polecenie o zmianie poziomu zasilania. **Uwaga** 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.

Krok 4 Kliknij przycisk **Zapisz**.

Krok 5 Kliknij przycisk **Apply Config** (Zastosuj konfigurację).

Krok 6 Uruchom ponownie telefon.

Konfigurowanie funkcji Nie przeszkadzać

Po włączeniu funkcji Nie przeszkadzać (DND) nagłówek na wyświetlaczu telefonu konferencyjnego jest czerwony.

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).
- 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 14

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.

Pole	Opis
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**.

Konfiguracja trybu UCR 2008

Parametry, które obsługują tryb UCR 2008, znajdują się w oknie Cisco Unified Communications Manager — administracja. W poniższej tabeli opisano poszczególne parametry i podano ścieżki dostępu do zmiany ich ustawień.

Tabela 21: Lokalizacja parametru trybu UCR 2008

Parametr	Ścieżka dostępu w oknie Administracja
Tryb FIPS	**Urządzenie** > **Ustawienia urządzenia** > **Wspólny profil telefonu**
	System > **Firmowa konfiguracja telefonów**
	Urządzenie > **Telefony**
Dostęp przez SSH	**Urządzenie** > **Telefon**
	Urządzenie > **Ustawienia urządzenia** > **Wspólny profil telefonu**
Dostęp przez WWW	**Urządzenie** > **Telefon**
	System > **Firmowa konfiguracja telefonów**
	Urządzenie > **Ustawienia urządzenia** > **Wspólny profil telefonu**
System > **Firmowa konfiguracja telefonów**	
Tryb adresowania IP	**Urządzenie** > **Ustawienia urządzenia** > **Wspólna konfiguracja urządzenia**
IP Addressing Mode Preference for Signaling (Ustawienie trybu adresowania IP do sygnalizowania)	**Urządzenie** > **Ustawienia urządzenia** > **Wspólna konfiguracja urządzenia**

Konfigurowanie trybu UCR 2008 we wspólnej konfiguracji urządzenia

Użyj tej procedury, aby ustawić następujące parametry trybu UCR 2008:

- Tryb adresowania IP
- IP Addressing Mode Preference for Signaling (Ustawienie trybu adresowania IP do sygnalizowania)

Procedura

Krok 1 W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Wspólna konfiguracja urządzenia**.

Krok 2 Ustaw parametr Tryb adresowania IP.

Krok 3 Ustaw parametr IP Addressing Mode Preference for Signaling (Ustawienie trybu adresowania IP do sygnalizowania).

Krok 4 Kliknij przycisk **Zapisz**.

Konfigurowanie trybu UCR 2008 we wspólnym profilu telefonu

Użyj tej procedury, aby ustawić następujące parametry trybu UCR 2008:

- Tryb FIPS
- Dostęp przez SSH
- Dostęp przez WWW

Procedura

Krok 1 W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Ustawienia urządzenia** > **Wspólny profil telefonu**.

Krok 2 Parametr Tryb FIPS ustaw na wartość **Włączone**.

Krok 3 Parametr Dostęp przez SSH ustaw na wartość **Wyłączone**.

Krok 4 Parametr Dostęp przez WWW ustaw na wartość **Wyłączone**.

Krok 5 Parametr 80-bitowy protokół SRTCP ustaw na wartość **Włączone**.

Krok 6 Kliknij przycisk **Zapisz**.

44Konfigurowanie trybu UCR 2008 w oknie Enterprise Phone Configuration (Firmowa konfiguracja telefonów)

Użyj tej procedury, aby ustawić następujące parametry trybu UCR 2008:

- Tryb FIPS
- Dostęp przez WWW

Procedura

Krok 1 W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **System** > **Enterprise Phone Configuration (Firmowa konfiguracja telefonów)**.

Krok 2 Parametr Tryb FIPS ustaw na wartość **Włączone**.

Krok 3 Parametr Dostęp przez WWW ustaw na wartość **Wyłączone**.

Krok 4 Kliknij przycisk **Zapisz**.

Konfigurowanie trybu UCR 2008 w telefonie

Użyj tej procedury, aby ustawić następujące parametry trybu UCR 2008:

- Tryb FIPS
- Dostęp przez SSH
- Dostęp przez WWW

Procedura

Krok 1 W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Telefon**.

Krok 2 Parametr Dostęp przez SSH ustaw na wartość **Wyłączone**.

Krok 3 Parametr Tryb FIPS ustaw na wartość **Włączone**.

Krok 4 Parametr Dostęp przez WWW ustaw na wartość **Wyłączone**.

Krok 5 Kliknij przycisk **Zapisz**.

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).

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 poniższej tabeli podano różne scenariusze wdrażania usługi Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.

Scenariusz	Czynności
Użytkownik w siedzibie firmy loguje się do jej sieci po wdrożeniu usługi Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.	Następuje wykrycie sieci firmy, a telefon w zwykły sposób rejestruje się w programie Cisco Unified Communications Manager.
Użytkownik poza siedzibą firmy loguje się do jej sieci za pomocą usługi Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway.	Telefon wykrywa, że znajduje się w trybie działania poza siedzibą firmy, pojawia się okno logowania w usłudze Dostęp z urządzeń przenośnych i dostęp zdalny za pośrednictwem usługi Expressway, a użytkownik nawiązuje połączenie z siecią firmy. Aby nawiązać połączenie z siecią, użytkownicy muszą podawać prawidłową nazwę usługi, nazwę użytkownika i hasło. Muszą ponadto zresetować tryb usługi, aby wyczyścić ustawienie Alternatywny serwer TFTP przed uzyskaniem dostępu do sieci firmy. Spowoduje to wyzerowanie ustawienia Alternatywny serwer TFTP, dzięki czemu telefon wykryje sieć poza siedzibą firmy. Jeśli wdrożenie dotyczy nowego telefonu, użytkownicy mogą pominąć wymóg zerowania ustawień sieciowych. Jeśli użytkownicy mają w swoim routerze sieciowym ustawioną dla serwera DHCP opcję 150 lub 66, zalogowanie się do sieci korporacyjnej może im się nie udać. Użytkownicy powinni wyłączyć te ustawienia serwera DHCP lub bezpośrednio skonfigurować statyczny adres IP.

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 100
Konfiguracja specyficzna dla produktu, na stronie 102

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 przesłanie 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

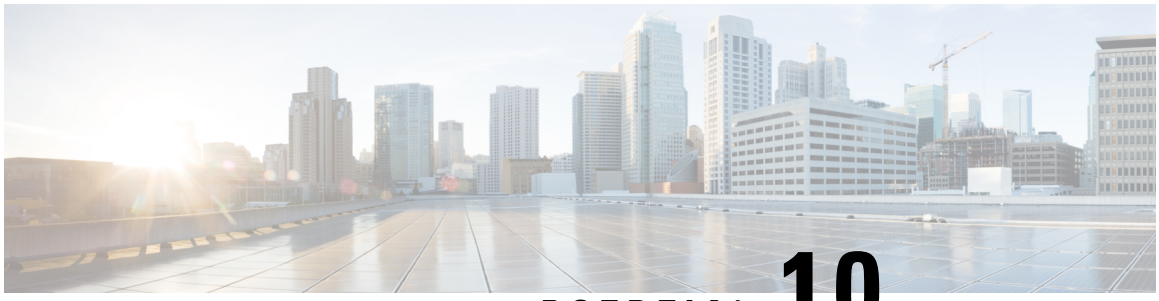
Krok 1 W aplikacji Cisco Unified Communications Manager — administracja wybierz kolejno opcje **Urządzenie** > **Telefon**.

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**.



ROZDZIAŁ 10

Firmowa książka telefoniczna i osobista książka telefoniczna

- Konfigurowanie firmowej książki telefonicznej, na stronie 131
- Konfigurowanie osobistej książki adresowej, na stronie 131

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 aplikacje, 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.

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 14

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

Aby uzyskać dostęp do funkcji książki adresowej, użytkownicy mogą używać następujących metod:

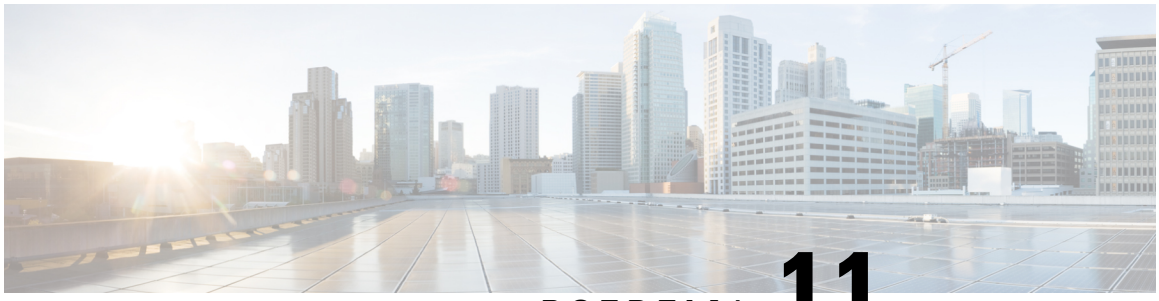
- Przy użyciu przeglądarki WWW — użytkownicy mają dostęp do osobistej książki adresowej i funkcji szybkiego wybierania z Portalu samoobsługowego Cisco Unified Communications.
- Z telefonu IP Cisco — wybierz opcję **Kontakty**, aby wyszukiwać w firmowej lub osobistej książce adresowej.

Aby skonfigurować osobistą książkę adresową w przeglądarce WWW, użytkownicy muszą mieć dostęp do Portalu samoobsługowego. Należy podać użytkownikom adres URL i dane logowania.

CZĘŚĆ IV

Rozwiązywanie problemów z telefonem konferencyjnym IP Cisco

- Monitorowanie systemów telefonicznych, na stronie 135
- Rozwiązywanie problemów z telefonem, na stronie 161
- Konserwacja, na stronie 179
- Obsługa użytkowników międzynarodowych, na stronie 183



ROZDZIAŁ 11

Monitorowanie systemów telefonicznych

- Monitorowanie systemów telefonicznych — przegląd, na stronie 135
- Stan telefonu IP Cisco, na stronie 135
- Strona WWW telefonu IP Cisco, na stronie 146
- Żądanie informacji z telefonu w formacie XML, na stronie 158

Monitorowanie systemów telefonicznych — przegląd

Różne informacje o telefonie są dostępne w jego menu stanu oraz na stronach WWW telefonu. Informacje te powinny zawierać:

- Informacje o urządzeniu
- Informacje o konfiguracji sieci
- Statystyki sieci
- Dzienniki urządzeń
- Statystyki strumieniowania

W tym rozdziale przedstawiono informacje, które można uzyskać ze strony WWW telefonu. Umożliwiają one zdalne monitorowanie działania telefonu i pomagają w rozwiązywaniu problemów.

Tematy pokrewne

Rozwiązywanie problemów z telefonem, na stronie 161

Stan telefonu IP Cisco

W poniższych sekcjach opisano, jak wyświetlić informacje o modelu, komunikaty o stanie i statystyki sieci telefonu IP Cisco.

- 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.

Wyświetlanie okna Informacje o telefonie

Procedura

Krok 1 Naciśnij kolejno **Ustawienia** > **Informacje systemowe**.

Krok 2 Aby wyjść z menu, naciśnij przycisk **Wyjdź**.

Wyświetlanie menu Stan

Procedura

Krok 1 Naciśnij kolejno **Ustawienia** > **Stan**.

Krok 2 Aby wyjść z menu, naciśnij przycisk **Wyjdź**.

Wyświetlanie okna komunikatów o stanie

Procedura

Krok 1 Naciśnij kolejno **Ustawienia** > **Stan** > **Komunikaty o stanie**.

Krok 2 Aby wyjść z menu, naciśnij przycisk **Wyjdź**.

Pola komunikatów o stanie

W poniższej tabeli opisano komunikaty o stanie wyświetlane na telefonie na ekranie Komunikaty o stanie.

Tabela 22: Komunikaty o stanie w telefonie IP Cisco

Komunikat	Opis	Wyjaśnienie i zalecane czynności
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 i jes telefonu.
Błąd rozmiaru 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 pamięci ROM	Pobrany plik oprogramowania jest uszkodzony.	Uzyskaj nową kopię oprogramowa umieść ją w katalogu TFTPPath. Pl katalogu tylko wtedy, gdy oprogran serwerem TFTP jest wyłączone. W p zostać uszkodzone.
Powtórzony adres IP	Inne urządzenie korzysta z adresu IP przypisanego do telefonu.	Jeśli telefon ma statyczny adres IP, przydzielony duplikat adresu IP. Jeśli używasz protokołu DHCP, spr DHCP.
Czyszczenie plików CTL i ITL	Czyszczenie pliku CTL lub ITL.	Żadna. Ten komunikat ma charakte
Błąd aktualizowania Locale	Nie można znaleźć co najmniej jednego pliku lokalizacyjnego w katalogu TFTP Path lub plik był nieprawidłowy. Nie zmieniono ustawień regionalnych.	W narzędziu Cisco Unified Operati sprawdź, czy następujące pliki zna systemu zarządzania plikami TFTP • Znajduje się w podkatalogu o ustawienie regionalne sieci: • tones.xml • Znajduje się w podkatalogu o ustawienie regionalne użytkov • glyphs.xml • dictionary.xml • kate.xml
Nie znaleziono pliku <Cfg File>	Na serwerze TFTP nie znaleziono pliku konfiguracyjnego o podanej nazwie ani pliku domyślnego.	Plik konfiguracyjny telefonu jest tw dodawany do bazy danych program Communications Manager. Jeśli tel danych programu Cisco Unified Co serwer TFTP tworzy odpowiedź CF znaleziono pliku konfiguracyjnego) • Telefon nie jest zarejestrowany Communications Manager. Jeśli nie zezwolono na automa należy dodać go ręcznie do ba Unified Communications Man • Jeśli używasz protokołu DHCP wskazuje na prawidłowy serw • Jeśli używasz statycznych adr konfigurację serwera TFTP.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
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 można na systemie Cisco Unified Communicatio
Adres IP zwolniony	Telefon jest skonfigurowany do zwolnienia adresu IP.	Telefon pozostaje bezczynny aż do wy zasilania lub do zresetowania adresu D
Serw. DHCP pr. IPv4 - limit czasu	Serwer DHCP protokołu IPv4 nie odpowiedział.	Sieć jest zajęta: błędy powinny znikną obciążenia sieci. Brak połączenia sieciowego pomiędzy protokołu IPv4 a telefonem: sprawdź p Serwer DHCP protokołu IPv4 jest wyłą konfigurację serwera DHCP protokołu Nadal występują błędy: rozważ przypi IPv4.
Serwer DHCP protokołu IPv6 - limit czasu	Serwer DHCP protokołu IPv6 nie odpowiedział.	Sieć jest zajęta: błędy powinny znikną obciążenia sieci. Brak połączenia sieciowego pomiędzy protokołu IPv6 a telefonem: sprawdź p Serwer DHCP protokołu IPv6 jest wyłą konfigurację serwera DHCP protokołu Nadal występują błędy: rozważ przypi IPv6.
Serw. DNS pr. IPv4 - limit czasu	Serwer DNS protokołu IPv4 nie odpowiedział.	Sieć jest zajęta: błędy powinny znikną obciążenia sieci. Brak połączenia sieciowego pomiędzy s IPv4 a telefonem: sprawdź połączenia Serwer DNS protokołu IPv4 jest wyłąc konfigurację serwera DNS protokołu I
Serwer DNS protokołu IPv6 - limit czasu	Serwer DNS protokołu IPv6 nie odpowiedział.	Sieć jest zajęta: błędy powinny znikną obciążenia sieci. Brak połączenia sieciowego pomiędzy s IPv6 a telefonem: sprawdź połączenia Serwer DNS protokołu IPv6 jest wyłąc konfigurację serwera DNS protokołu I
DNS nieznany host IPv4	Serwer DNS protokołu IPv4 nie może rozwiązać nazwy serwera TFTP lub systemu Cisco Unified Communications Manager.	Sprawdź, czy nazwy hosta serwera TF Unified Communications Manager są skonfigurowane w serwerze DNS proto Rozważ stosowania adresów protokołu

Komunikat	Opis	Wyjaśnienie i zalecane czynności
DNS nieznany host IPv6	Serwer DNS protokołu IPv6 nie może rozwiązać nazwy serwera TFTP lub systemu Cisco Unified Communications Manager.	Sprawdź, czy nazwy hosta serwera Unified Communications Manager skonfigurowane w serwerze DNS p Rozważ użycie adresów protokołu
Nie można załadować kodu	Pobrana aplikacja nie jest zgodna ze sprzętem telefonu.	Taka sytuacja występuje podczas p telefonie wersji oprogramowania, k sprzętowych telefonu. Zaznacz identyfikator obciążenia p programie Cisco Unified Communi kolejno opcje **Urządzenie** > **Telefo** obciążenie wyświetlane na telefon
Brak routera domyślnego	Protokół DHCP lub konfiguracja statyczna nie określają routera domyślnego.	Jeśli telefon posiada statyczny adres router jest skonfigurowany. Jeśli używasz protokołu DHCP, ser domyślnego routera. Sprawdź konf
Brak serwera DNS protok. IPv4	Podano nazwę, ale protokół DHCP lub statycznie skonfigurowany adres IP nie określa adresu serwera DNS protokołu IPv4.	Jeśli telefon posiada statyczny adre DNS protokołu IPv4 jest skonfigur Jeśli używasz protokołu DHCP, ser serwera DNS protokołu IPv4. Spraw DHCP.
Brak serwera DNS protokołu IPv6	Podano nazwę, ale protokół DHCP lub statycznie skonfigurowany adres IP nie określa adresu serwera DNS protokołu IPv6.	Jeśli telefon posiada statyczny adre DNS protokołu IPv6 jest skonfigur Jeśli używasz protokołu DHCP, ser serwera DNS protokołu IPv6. Spraw DHCP.
Nie zainstalowano listy zaufanych certyfikatów	Plik CTL lub plik ITL nie jest zainstalowany w telefonie.	Lista zaufanych nie jest skonfiguro Unified Communications Manager, obsługuje zabezpieczeń. Lista zaufanych nie jest skonfiguro Więcej informacji o listach zaufany dokumentacji konkretnej wersji pro Communications Manager.
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 konfig Cisco Unified Communications Ma **Apply Config** (Zastosuj konfigurac wdrożenie zmian.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Błąd dostępu protokołu TFTP	TFTP wskazuje nieistniejący katalog.	Jeśli używasz protokołu DHCP, sprawd wskazuje na prawidłowy serwer TFTP. Jeśli używasz statycznych adresów IP, serwera TFTP.
Błąd protokołu TFTP	Telefon nie rozpoznaje kodu błędu przekazanego przez serwer TFTP.	Skontaktuj się z Cisco TAC.
TFTP limit czasu	Serwer TFTP nie odpowiedział.	Sieć jest zajęta: błędy powinny znikna obciążenia sieci. Brak połączenia sieciowego pomiędzy telefonem: sprawdź połączenia sieciow Serwer TFTP jest wyłączony: sprawdź TFTP.
Przekroczono limit czasu	Suplikant próbował przeprowadzić transakcję 802.1X, ale upłynął limit czasu z powodu braku wystawcy uwierzytelnienia.	Uwierzytelnianie przekracza limit czas gdy na przełączniku nie jest skonfiguro
Aktualizacja listy zaufanych certyfikatów nie powiodła się	Aktualizacja plików CTL i ITL zakończyła się niepowodzeniem.	Na telefonie były zainstalowane pliki C się ich zaktualizować. Prawdopodobna przyczyna niepowodz • Wystąpiła awaria sieci. • Serwer TFTP był wyłączony. • Wprowadzono nowy token zabezp podpisywania pliku CTL oraz cert używany do podpisywania pliku I dostępne w aktualnych plikach C • Wystąpiła wewnętrzna awaria tel Możliwe rozwiązania: • Sprawdź łączność w sieci. • Sprawdź, czy serwer TFTP jest ak poprawnie. • Jeśli serwer TVS (Transactional V obsługiwany w systemie Cisco Un Manager, sprawdź, czy serwer TV pracuje poprawnie. • Sprawdź poprawność tokenu zabez Jeśli poprzednie czynności nie przynio pliki CTL i ITL, po czym zresetuj telef Więcej informacji o listach zaufanych dokumentacji konkretnej wersji progra Communications Manager.

Komunikat	Opis	Wyjaśnienie i zalecane czynności
Lista zaufanych certyfikatów została zaktualizowana	Plik CTL, plik ITL, lub oba te pliki zostały uaktualnione.	Żadna. Ten komunikat ma charakte Więcej informacji o listach zaufany dokumentacji konkretnej wersji pro Communications Manager.
Błąd wersji	Nazwa obciążenia telefonu jest nieprawidłowa.	Upewnij się, że plik obciążenia tele
XmlDefault.cnf.xml lub .cnf.xml — odpowiednio do nazwy urządzenia telefonicznego	Nazwa pliku konfiguracyjnego.	Żadna. Ten komunikat wskazuje naz telefonu.

Tematy pokrewne

Cisco Unified Communications Manager — Dokumentacja, na stronie 14

Wyświetlanie okna Statystyki sieci

Procedura

Krok 1 Naciśnij kolejno **Ustawienia** > **Stan** > **Statystyki sieci**.

Krok 2 Aby wyjść z menu, naciśnij przycisk **Wyjdź**.

Pola na ekranie Statystyki sieci

W poniższej tabeli opisano informacje widoczne na ekranie Statystyki sieci.

Tabela 23: Pola na ekranie Statystyki sieci

Element	Opis
Wysł. ramki	Liczba pakietów wysłanych przez telefon
Wysł. emisja	Liczba pakietów rozgłoszeniowych wysłanych przez telefon
Transmisja pojedyncza	Łączna liczba pakietów unicast wysłanych przez telefon
Wysł. ramki	Liczba pakietów odebranych przez telefon
Odb. emisja	Liczba pakietów rozgłoszeniowych odebranych przez telefon
Odb. poj. emisja	Łączna liczba pakietów unicast odebranych przez telefon.
Identyfikator sąsiedniego urządzenia CDP	Identyfikator urządzenia podłączonego do tego portu, które zostało wykryte przez protokół CDP.
Adres IP sąsiedniego urządzenia CDP	Identyfikator urządzenia podłączonego do tego portu, które zostało wykryte przez protokół CDP z użyciem protokołu IP.
Port sąsiedniego urządzenia CDP	Identyfikator urządzenia podłączonego do tego portu, które zostało wykryte przez protokół CDP.

Element	Opis
Przyczyna ponownego uruchomienia: jedna z tych wartości: • Reset sprzętowy (włączenie zasilania) • Reset programowy (zresetowano również kontroler pamięci) • Reset programowy (nie zresetowano kontrolera pamięci) • Reset przez mechanizm monitorujący • Zainicjowany • Nieznane	Przyczyna ostatniego zresetowania telefonu
Port 1	Stan łącza i typ połączenia portu sieciowego (na przykład **`100 Full`** oznacza, że port PC ma aktywne łącze i automatycznie wynegocjowane połączenie pełnodupleksowe 100 Mb/s)
IPv4	Informacje o stanie DHCP. Może podawać następujące stany: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Element	Opis
IPv6	Informacje o stanie DHCP. Może podawać następujące stany: • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Wyświetlanie okna Statystyki połączeń

Procedura

Krok 1 Naciśnij kolejno **Ustawienia** > **Stan** > **Statystyki połączeń**.

Krok 2 Aby wyjść z menu, naciśnij przycisk **Wyjdź**.

Pola na ekranie Statystyki połączeń

W poniższej tabeli opisano elementy widoczne na ekranie Statystyki połączeń.

Tabela 24: Elementy na ekranie Statystyki połączeń

Element	Opis
Kodek odbiornika	Typ odbieranego strumienia dźwiękowego (dźwięk przesyłany jako strumień RTP z kodeka): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Kodek nadajnika	Typ wysyłanego strumienia dźwiękowego (dźwięk przesyłany jako strumień RTP z kodeka): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
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.

Element	Opis
Liczba odebranych pakietów	Liczba pakietów dźwiękowych RTP odebranych od momentu otwarcia strumienia. **Uwaga** Ta liczba nie musi być identyczna z liczbą pakietów dźwiękowych RTP odebranych od momentu rozpoczęcia połączenia, ponieważ połączenie mogło być wstrzymane.
Liczba nadanych pakietów	Liczba pakietów dźwiękowych RTP wysłanych od momentu otwarcia strumienia. **Uwaga** 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.). **Uwaga** 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).
Metryki jakości dźwięku	
Kumulatywny współ. ukr.	Łączna liczba ramek ukrywania podzielona przez łączną liczbę ramek transmisji głosowej odebranych od początku strumienia transmisji głosowej.
Współ. ukr. 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.

Element	Opis
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.

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 pokrewne informacje dotyczące telefonu.
- Konfiguracja sieci: informacje o konfiguracji sieci oraz o innych ustawieniach telefonu.
- Statystyki sieci: łącza do informacji o ruchu sieciowym.
- Dzienniki urządzeń: łącza do informacji pomocnych przy rozwiązywaniu problemów.
- Statystyki strumieniowania: łącza do różnych statystyk strumieniowania.

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

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:

a) 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 Find and List Phones (Znajdowanie telefonów i wyświetlanie ich listy) i na górze okna Phone Configuration (Konfiguracja telefonu).

b) Na telefonie naciśnij kolejno **Ustawienia** > **Informacje systemowe**, 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:

http://<IP_address>

Strona WWW 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.

Aby wyświetlić obszar Informacje o urządzeniu, należy przejść do strony WWW telefonu, a następnie kliknąć łącze **Informacje o urządzeniu**.

Tabela 25: Pola na stronie WWW Informacje o urządzeniu

Pole	Opis
Tryb usługi	Tryb usługi telefonu.
Domena 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	Wskazuje wersję oprogramowania aplikacji.
Boot Load ID	Wskazuje wersję oprogramowania uruchomieniowego.
Wersja	Identyfikator oprogramowania sprzętowego działającego w telefonie.
Wersja sprzętu	Drobna zmiana wersji warstwy sprzętowej telefonu.
Numer seryjny	Niepowtarzalny numer seryjny telefonu.
Numer modelu	Numer modelu telefonu.
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): • Typ sprzętu • Nazwa modelu telefonu • Identyfikator produktu • Identyfikator wersji (VID) — określa główny numer wersji sprzętu. • Numer seryjny
Godzina	Godzina Grupy daty/godziny, do której należy telefon. Informacja ta pochodzi z programu Cisco Unified Communications Manager.

Pole	Opis
Time Zone (Strefa czasowa)	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 dostępnej pamięci systemu.
Wolna pamięć sterty Java	Ilość wolnej pamięci sterty Java.
Wolna pamięć puli Java	Ilość wolnej pamięci puli Java.
Tryb FIPS włączony	Wskazuje, czy włączony jest tryb FIPS (ang. Federal Information Processing Standard, federalny standard przetwarzania informacji).

Strona WWW 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.

Aby wyświetlić obszar Konfiguracja sieci, należy przejść do strony WWW telefonu, a następnie kliknąć łącze **Konfiguracja sieci**.

Tabela 26: 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 dynam konfigurowania hosta), z którego telefon otrzymuje adres IP.
Serwer BOOTP	Wskazuje, czy telefon pobiera konfigurację z serwera protokołu BootP (ang. Bootstrap Proto protokół samorozruchu).
DHCP	Wskazuje, czy telefon korzysta z protokołu DHCP.
Adres IP	Adres IP (ang. Internet Protocol, protokół internetowy) telefonu.
Maska podsieci	Maska podsieci używana w telefonie.
Domyślny router 1	Domyślny router, z którego korzysta telefon.
Serwer DNS 1-3	Podstawowy serwer DNS (Serwer DNS 1) i opcjonalne zapasowe serwery DNS (Serwer DN z których korzysta telefon.

Element	Opis
Alternatywny serwer TFTP	Wskazuje, czy telefon korzysta z alternatywnego serwera TFTP.
Serwer TFTP 1	Podstawowy serwer TFTP (ang. Trivial File Transfer Protocol, trywialny protokół przesyła z którego korzysta telefon.
Serwer TFTP 2	Zapasowy serwer TFTP, z którego korzysta telefon.
Adres DHCP zwolniony	Wskazuje ustawienie opcji Adres DHCP zwolniony.
Aktywny VLAN ID	Aktywna wirtualna sieć lokalna (ang. Virtual Local Area Network, VLAN) skonfigurowa przełączniku Cisco Catalyst, do której należy telefon.
Administracyjny VLAN ID	Pomocnicza sieć VLAN, do której należy telefon.
Unified CM 1–5	Nazwy hosta lub adresy IP serwerów Cisco Unified Communications Manager (uszerego kolejności priorytetów), na których telefon może się zarejestrować. Ten element może r wskazywać adres IP routera SRST, który (o ile istnieje) udostępnia częściową funkcjonaln Cisco Unified Communications Manager. W przypadku dostępnego serwera w polu tym widoczny jest adres IP serwera Cisco Unif Communications Manager i jeden z następujących stanów: • Włączony: serwer Cisco Unified Communications Manager, z którego telefon uzysku usługi przetwarzania połączeń • Standby (Rezerwowy): serwer Cisco Unified Communications Manager, na który telef się, jeśli bieżący serwer stanie się niedostępny • Blank (Pusty): brak aktualnie połączenia z danym serwerem Cisco Unified Commu Manager Element ten może również zawierać nominację trybu Survivable Remote Site Telephony która wskazuje router SRST mogący udostępniać częściową funkcjonalność serwera Ci Communications Manager. Router ten przejmuje kontrolę nad przetwarzaniem połączeń, je inne serwery Cisco Unified Communications Manager staną się niedostępne. Serwer SR Unified Communications Manager zawsze występuje na końcu listy serwerów, nawet jeśli j Adres routera SRST można skonfigurować w części Pula urządzeń w oknie Konfiguracja Cisco Unified Communications Manager.
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.
Idle URL czas nieaktywności	Liczba sekund bezczynności telefonu, gdy nie jest otwarte żadne menu, jakie muszą upły włączy się usługa XML wskazana w polu Wolny URL.

Element	Opis
Adres URL proxy serwera	Adres URL serwera proxy, który w imieniu klienta HTTP telefonu kieruje żądania HTTP na hosta nielokalnego i przekazuje do niego odpowiedzi hosta.
Adres URL uwierzytelniania	Adres URL, którego telefon używa do weryfikowania żądań kierowanych do jego serwera W
Konfig. portu SW	Prędkość i tryb dupleks portu przełącznika, gdzie: • A = automatyczne negocjowanie • 10H = 10-BaseT/półdupleks • 10F = 10-BaseT/pełny dupleks • 100H = 100-BaseT/półdupleks • 100F = 100-BaseT/pełny dupleks • 1000F = 1000-BaseT/pełny dupleks • No Link = brak połączenia z portem przełącznika
Ustawienia regionalne użytkownika	Ustawienia regionalne skojarzone z użytkownikiem telefonu. Stanowią zbiór szczegółowych in na temat obsługi użytkowników, m.in. języka, czcionki, formatowania daty i godziny oraz kl alfanumerycznej służącej do wprowadzania tekstu.
Sieciowe ustawienia regionalne	Sieciowe ustawienia regionalne skojarzone z użytkownikiem telefonu. Stanowią zbiór szczeg informacji na temat obsługi telefonu w określonym kraju, m.in. definicje sygnałów dźwięko interwałów stosowanych w telefonie.
Wersja User Locale	Wersja ustawień regionalnych użytkownika wczytanych do telefonu.
Wersja Network Locale	Wersja sieciowych ustawień regionalnych użytkownika wczytanych do telefonu.
Głośnik włączony	Wskazuje, czy w telefonie jest włączona funkcja telefonu głośnomówiącego.
Słuchanie grupowe	Wskazuje, czy w telefonie jest włączona funkcja słuchania grupowego. Umożliwia ona jedno mówienie do słuchawki i słuchanie poprzez głośnik.
Włączono protokół GARP	Wskazuje, czy telefon odczytuje adresy MAC z odpowiedzi protokołu GARP (Gratuitous Ad Resolution Protocol, nieodpłatny protokół rozpoznawania adresów).
Włączono autom. wybór linii	Wskazuje, czy telefon na wszystkich liniach zmienia priorytet połączeń na połączenia przych
DSCP dla sterowania połączeniami	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	Ustawiony w telefonie tryb zabezpieczeń.
Dostęp przez WWW możliwy	Wskazuje, czy dostęp przez WWW do telefonu jest włączony (Tak), czy wyłączony (Nie).

Element	Opis
Dostęp SSH możliwy	Wskazuje, czy telefon przyjmuje, czy blokuje połączenia SSH.
CDP: port SW	Wskazuje, czy port przełącznika obsługuje protokół CDP (domyślnie opcja ta jest włączo Włączenie obsługi protokołu CDP przez port przełącznika umożliwia przypisywanie tele VLAN, negocjowanie zasilania i działanie zabezpieczeń 802.1x. Obsługę protokołu CDP przez port przełącznika należy włączyć, jeśli telefon komunikuj przełącznikiem Cisco. Jeśli w programie Cisco Unified Communications Manager obsługa protokołu CDP jest w widoczne jest ostrzeżenie informujące, że obsługę protokołu CDP przez port przełącznik wyłączać tylko, gdy telefon komunikuje się z przełącznikiem innej firmy niż Cisco. Aktualny stan obsługi protokołu CDP przez port komputera i przełącznika jest widoczny Ustawienia.
LLDP-MED: port SW	Wskazuje, czy w porcie przełącznika włączone jest rozszerzenie LLDP-MED (ang. Link Lay Protocol Media Endpoint Discovery, wykrywanie punktów końcowych nośników za pomo wykrywania na poziomie łącza).
LLDP priorytet mocy	Nakazuje przełącznikowi priorytet zasilania telefonów, umożliwiając mu ich prawidłowe Dostępne ustawienia: • Nieznany: wartość domyślna. • Niski • Wysoki • Kluczowy
LLDP Asset ID	Wskazuje identyfikator zasobu przypisanego do telefonu w celu zarządzania zapasami.
Plik CTL	Wskazuje plik CTL.
Plik ITL	Plik ITL zawiera początkową listę zaufanych.
Sygnatura ITL	Zwiększa bezpieczeństwo, stosując w plikach CTL i ITL bezpieczny algorytm wyznacza skrótu (SHA-1).
Serwer CAPF	Nazwa serwera CAPF używanego przez telefon.
TVS	Główny składnik funkcji Security by Default (Domyślne bezpieczeństwo). Usługa Trust Service (TVS) umożliwia telefonom IP Cisco Unified uwierzytelnianie serwerów aplikac EM, książki adresowej i midletów, w trakcie nawiązywanie połączenia za pośrednictwe HTTPS.
Serwer TFTP	Nazwa serwera TFTP używanego przez telefon.
Automatyczna synchronizacja portów	Umożliwia synchronizację portów z niższą prędkością w celu wyeliminowania utraty p
Zdalna konfiguracja przełączania portu	Umożliwia administratorowi zdalne konfigurowanie prędkości i działania portu tabeli Ci Collaboration Experience za pomocą aplikacji Cisco Unified Communications Manager — a

Element	Opis
Zdalna konfiguracja portu komputera PC	Wskazuje, czy zdalne konfigurowanie prędkości i trybu dupleksu portu komputera jest włącz wyłączone.
Tryb adresowania IP	Wskazuje dostępny w telefonie tryb adresowania IP.
Kontrola trybu preferencji protokołu IP	Wskazuje wersję adresu IP, której telefon używa podczas komunikacji z programem Cisco U Communications Manager, gdy ma dostępne obie wersje, czyli IPv4 i IPv6.
Tryb preferencji protokołu IP dla nośników	Wskazuje, czy w przypadku nośników urządzenie korzysta z adresu IPv4 do nawiązywania po z programem Cisco Unified Communications Manager.
Automat. konfig. IPv6	Wskazuje, czy automatyczne konfigurowanie jest w telefonie włączone, czy wyłączone.
IPv6 DAD	Służy do sprawdzania niepowtarzalności nowych adresów IPv6 pojedynczej emisji, zanim z one przypisane interfejsom.
Akceptacja przekierowania wiadomości IPv6	Wskazuje, czy telefon przyjmuje przekierowane wiadomości z tego samego routera, który sł numer docelowy.
Żądanie echa odpowiedzi multiemisji IPv6	Wskazuje, czy telefon wysyła komunikat Echo Reply w odpowiedzi na komunikat Echo Req nadesłany na adres IPv6.
Serwer pobierania IPv6	Służy do optymalizowania pory instalacji uaktualnień oprogramowania sprzętowego telefon zmniejszania obciążenia sieci WAN poprzez lokalne przechowywanie obrazów, które elimin konieczność przesyłania ich łączem WAN przy każdym uaktualnianiu telefonu.
Serwer dziennika protok. IPv6	Podaje adres IP i port zdalnego urządzenia rejestrującego, do którego telefon wysyła komun dziennika.
Serwer CAPF protokołu IPv6	Nazwa pospolita (z certyfikatu serwera Cisco Unified Communications Manager) serwera C używanego przez telefon.
Protokół DHCPv6	Protokół DHCP automatycznie przypisuje adresy IPv6 urządzeniom po ich połączeniu z siec telefonach IP Cisco Unified protokół DHCP jest domyślnie włączony.
Adres IPv6	Podaje bieżący adres IPv6 telefonu oraz umożliwia użytkownikowi wprowadzenie nowego IPv6.
Długość prefiksu IPv6	Podaje bieżącą długość prefiksu podsieci oraz umożliwia użytkownikowi wprowadzenie no długości prefiksu.
Domyś. router 1 protok. IPv6	Wskazuje router domyślny, z którego korzysta telefon, oraz umożliwia użytkownikowi wprov nowego routera domyślnego IPv6.
Serwer DNS 1 IPv6	Wskazuje podstawowy serwer DNSv6, z którego korzysta telefon, oraz umożliwia użytkown wprowadzenie nowego serwera.
Serwer DNS 2 IPv6	Wskazuje pomocniczy serwer DNSv6, z którego korzysta telefon, oraz umożliwia użytkown wyznaczenie nowego pomocniczego serwera DNSv6.

Element	Opis
Alternat. serwer TFTP IPv6	Umożliwia użytkownikowi włączanie korzystania z alternatywnego (pomocniczego) serw IPv6.
Serwer TFTP 1 IPv6	Wskazuje podstawowy serwer TFTP IPv6, z którego korzysta telefon, oraz umożliwia uży wyznaczenie nowego podstawowego serwera TFTP.
Serwer TFTP 2 IPv6	Wskazuje pomocniczy serwer TFTP IPv6, z którego telefon korzysta, gdy podstawowy s IPv6 jest niedostępny, oraz umożliwia użytkownikowi wyznaczenie nowego pomocnicze TFTP.
Adres IPv6 zwolniony	Umożliwia użytkownikowi udostępnianie informacji związanych z protokołem IPv6.
Poziom zasilania EnergyWise	Pomiar zużycia energii przez urządzenia należące do sieci zgodnej z trybem EnergyWise
Domena EnergyWise	Administracyjne grupowanie urządzeń w celu monitorowania i kontroli zasilania.

Strona WWW Ethernet Information (Informacje o sieci Ethernet)

W poniższej tabeli opisano zawartość strony WWW Ethernet Information.

Tabela 27: 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 dotyczące sieci

W poniższej tabeli przedstawiono informacje widoczne na stronach WWW Network Area (Obszar sieci).

Uwaga Po kliknięciu łącza **Sieć** w obszarze Statystyki sieci otwierana jest strona "Informacje o porcie".

Tabela 28: Elementy w obszarze Network Area (Obszar sieci)

Element	Opis
Odb. pak. łącznie	Łączna liczba pakietów odebranych przez telefon.
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.
Odb. odrz. żeton	Łączna liczba pakietów odrzuconych z powodu braku zasobów (np. przepełnienia bufora FIFO).
Wysł. popr. pak. łącznie	Łączna liczba odebranych przez telefon prawidłowych pakietów (multiemisji, rozgłoszeniowych i emisji pojedynczej).
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).
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 ramkach LLDP.
LLDP TLVUnrecognizedTotal	Łączna liczba elementów TLV w ramkach 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 IP sąsiedniego urządzenia CDP	Adres IP sąsiedniego urządzenia wykrytego przez protokół CDP.

Element	Opis
Adres IPv6 sąsiedniego urządzenia CDP	Adres IPv6 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 IP sąsiedniego urządzenia LLDP	Adres IP sąsiedniego urządzenia wykrytego przez protokół LLDP.
Adres IPv6 sąsiedniego urządzenia LLDP	Adres IPv6 sąsiedniego urządzenia wykrytego przez protokół CDP.
Port sąsiedniego urządzenia LLDP	Wykryty przez protokół LLDP port sąsiedniego urządzenia, do którego jest podłączony telefon.
Informacje o porcie	Informacje o prędkości i funkcji dupleksu.

Strony WWW Dzienniki konsoli, Zrzuty rdzenia, Komunikaty o stanie oraz Ekran debugowania

W obszarze Dzienniki urządzeń znajdują się łącza Dzienniki konsoli, Zrzuty rdzenia, Komunikaty o stanie i Ekran debugowania, które dają dostęp do informacji przydatnych podczas monitorowania telefonu i rozwiązywania problemów.

- Dzienniki konsoli — zawiera łącza do poszczególnych plików dziennika. Pliki dzienników konsoli zawierają odebrane przez telefon komunikaty dotyczące debugowania i błędów.
- Zrzuty rdzenia — zawiera łącza do poszczególnych plików zrzutów. Pliki zrzutów podstawowych zawierają dane o awariach telefonu.
- 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 Komunikaty o stanie w telefonie.
- Ekran debugowania — są tu wyświetlane komunikaty debugowania, które mogą być przydatne zespołowi Cisco TAC w przypadku korzystania z jego pomocy przy rozwiązywaniu problemów.

Strona WWW Statystyki strumieniowania

Telefon IP Cisco może strumieniować informacje do i z maksymalnie pięciu urządzeń jednocześnie. 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.

Aby wyświetlić obszar Statystyki strumieniowania, otwórz stronę WWW telefonu, a następnie kliknij łącze **Stream** (Strumień).

W poniższej tabeli opisano elementy widoczne w obszarach Statystyki strumieniowania.

Tabela 29: Pola na stronie Statystyki strumieniowania

Element	Opis
Adres zdalny	Adres IP i port UDP miejsca docelowego strumienia.
Adres lokalny	Adres IP i port UPD telefonu.
Godzina rozpoczęcia	Wewnętrzny znacznik czasu wskazujący, kiedy serwer Cisco Unified Communications M 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 pod jego adresu MAC.
Liczba nadanych pakietów	Łączna liczba pakietów danych RTP, które telefon wysłał od początku tego połączenia. W ta wynosi 0, jeśli połączenie działa w trybie samego odbioru.
Liczba nadanych oktetów	Łączna liczba oktetów ładunku, które telefon wysłał w pakietach danych RTP od początk 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 danyc ramach tego połączenia. Obliczana według wzoru: liczba oczekiwanych pakietów minus faktycznie odebranych pakietów, przy czym liczba odebranych pakietów obejmuje wsz pakiety spóźnione i będące duplikatami. Wartość ta wynosi 0, jeśli połączenie działa w samego wysyłania.
Średni jitter	Oszacowanie średniego odchylenia czasu docierania kolejnych pakietów danych RTP, mierzonego w milisekundach. Wartość ta wynosi 0, jeśli połączenie działa w trybie sa wysyłania.
Kodek odbiornika	Typ kodowania dźwięku zastosowany w odbieranym strumieniu.
Wysłano raporty odbiornika (patrz uwaga)	Liczba przypadków wysłania raportu odbiornika RTCP.

Element	Opis
Wysłano godzinę raportu odbiornika (patrz uwaga)	Wewnętrzny znacznik czasu wskazujący, kiedy został wysłany raport odbiornika R
Liczba odebranych pakietów	Łączna liczba pakietów danych RTP, które zostały odebrane przez telefon od począ danych w ramach tego połączenia. Obejmuje pakiety odebrane z różnych źródeł, je połączenie ma charakter multiemisji. Wartość ta wynosi 0, jeśli połączenie działa samego wysyłania.
Liczba odebranych oktetów	Łączna liczba oktetów ładunku, które zostały odebrane przez telefon w pakietach da od początku odbioru danych w ramach tego połączenia. Obejmuje pakiety odebrane źródeł, jeśli to połączenie ma charakter multiemisji. Wartość ta wynosi 0, jeśli poł działa w trybie samego wysyłania.
Kumulatywny współ. ukr.	Łączna liczba ramek ukrywania podzielona przez łączną liczbę ramek transmisji g odebranych od początku strumienia transmisji głosowej.
Współ. ukr. w interwale	Stosunek liczby ramek ukrywania do liczby ramek transmisji głosowej w poprzedz 3-sekundowym interwale trwającej rozmowy. Jeśli działa funkcja wykrywania akty transmisji głosowej (VAD), może być wymagany dłuższy interwał w celu zebrania sekund aktywnej transmisji głosowej.
Maks. współczynnik ukrywania	Najwyższy współczynnik ukrywania w interwale od początku strumienia transmisj
Ukrywanie (s)	Liczba sekund, w których występowały zdarzenia ukrywania (utracone ramki), od strumienia transmisji głosowej (obejmuje sekundy z intensywnym ukrywaniem).
Intensywne ukrywanie (s)	Liczba sekund, w których zdarzenia ukrywania (utracone ramki) obejmowały pona początku strumienia transmisji głosowej.
Opóźnienie (patrz uwaga)	Oszacowanie opóźnienia sieci wyrażonego w milisekundach. Stanowi określane n średnie opóźnienie przesyłania danych w obie strony, mierzone w trakcie odbieran raportu odbiornika RTCP.
Maks. jitter	Maksymalna wartość bieżącego jittera, w milisekundach.
Rozmiar po stronie nadawcy	Rozmiar pakietów RTP wysyłanego 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.

Element	Opis
Odebrano raporty odbiornika (patrz uwaga)	Liczba przypadków odebrania raportu odbiornika RTCP.
Odebrano godzinę raportu odbiornika (patrz uwaga)	Czas odebrania ostatniego raportu odbiornika RTCP.

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.

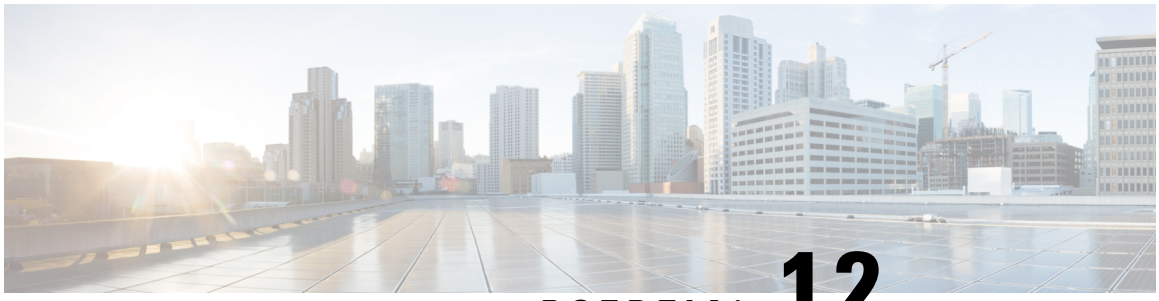
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
```

```
   </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 ModeInfo

Poniższy kod XML to przykład danych wyjściowych polecenia ModeInfo.

```
<?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>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



ROZDZIAŁ 12

Rozwiązywanie problemów z telefonem

- Ogólne informacje o rozwiązywaniu problemów, na stronie 161
- Problemy z uruchamianiem, na stronie 162
- Problemy z resetowaniem się telefonu, na stronie 167
- Telefon nie może się połączyć z siecią LAN, na stronie 169
- Problemy z zabezpieczeniami telefonu IP Cisco, na stronie 169
- Problemy z dźwiękiem, na stronie 171
- Ogólne problemy z połączeniami telefonicznymi, na stronie 172
- Procedury rozwiązywania problemów, na stronie 173
- Informacje kontrolne debugowania z programu Cisco Unified Communications Manager, na stronie 177
- Dodatkowe informacje o sposobach rozwiązywania problemów, na stronie 178

Ogólne informacje o rozwiązywaniu problemów

W poniższej tabeli podano ogólne informacje na temat rozwiązywania problemów z telefonem IP Cisco.

Tabela 30: Rozwiązywanie problemów z telefonem IP Cisco

Podsumowanie	Objaśnienie
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, utrat połączenia albo brak możliwości nawiązywania lub odbierania połącz mogą nie wznowić prawidłowego działania po ustaniu burzy rozgłosze
Przenoszenie połączenia sieciowego z telefonu na stację roboczą	Jeśli telefon jest zasilany z użyciem połączenia sieciowego, należy z n podejmować decyzję o odłączeniu kabla sieciowego od telefonu i podł do komputera. **Przestroga** Karta sieciowa w komputerze nie może pobierać prądu za pośrednictwem połączenia sieciowego. Pojawienie się pra sieciowym może spowodować zniszczenie karty sieciowej ochrony karty sieciowej należy po odłączeniu kabla od tel odczekać co najmniej 10 sekund przed podłączeniem go do Dzięki temu opóźnieniu przełącznik ma dostatecznie dużo wykryć brak telefonu na linii i przestać dostarczać prąd d

Podsumowanie	Objaśnienie
Zmiana konfiguracji telefonu	Domyślnie ustawienia hasła administratora są zablokowane, aby zapobiec wprowadzaniu przez użytkowników zmian, które mogłoby zakłócić komu siecią. Aby zmienić ustawienia hasła administratora, należy je najpierw odb Więcej informacji zawiera sekcja Ustawianie hasła w telefonie, na stronie **Uwaga** Jeśli we wspólnym profilu telefonu nie ma ustawionego hasła administratora, użytkownik może modyfikować ustawienia si
Niedopasowanie kodeka między telefonem a innym urządzeniem	Dane statystyczne RxType i TxType wskazują kodek używany do komuni między telefonem IP Cisco a innym urządzeniem. Wartości tych danych statystycznych powinny się ze sobą zgadzać. W przeciwnym razie należy sp czy inne urządzenie obsługuje komunikację za pośrednictwem kodeka lub dostępny jest odpowiedni transkoder. Więcej informacji zawiera sekcja Wyś okna Statystyki połączeń, na stronie 144.
Niedopasowanie wielkości próbki dźwięku między telefonem a innym urządzeniem	Dane statystyczne RxSize i TxSize wskazują rozmiar pakietów dźwięku uż do komunikacji między telefonem IP Cisco a innym urządzeniem. Wartoś danych statystycznych powinny się ze sobą zgadzać. Więcej informacji za sekcja Wyświetlanie okna Statystyki połączeń, na stronie 144.
Stan pętli zwrotnej	Stan pętli zwrotnej może wystąpić, gdy są spełnione następujące warunk • Dla opcji SW Port Configuration (Konfiguracja portu oprogramowan telefonie wybrane jest ustawienie 10 Half (10-BaseT/półdupleks). • Telefon pobiera prąd z zewnętrznego zasilacza. • Telefon jest wyłączony (ma odłączony zasilacz). W takim przypadku port przełącznika w telefonie może zostać wyłączony dzienniku konsoli przełącznika pojawi się następujący komunikat: HALF_DUX_COLLISION_EXCEED_THRESHOLD Aby rozwiązać ten problem, należy ponownie uaktywnić port za pomocą przełącznika.

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

Sprawdzanie uruchamiania telefonu, na stronie 55

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

Sprawdzanie uruchamiania telefonu, na stronie 55

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 173.

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. W części “Wyświetlanie okna komunikatów o stanie” można znaleźć instrukcje uzyskiwania dostępu do komunikatów o stanie oraz listę potencjalnych błędów wraz z objaśnieniami i sposobami eliminacji.

Tematy pokrewne

Wyświetlanie okna komunikatów o stanie, na stronie 136

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 174

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.

Tematy pokrewne

Sprawdzanie ustawień DHCP, na stronie 175

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.

Tematy pokrewne

Sprawdzanie ustawień DNS, na stronie 176

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 176.

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.

Tematy pokrewne

Tworzenie nowego pliku konfiguracyjnego telefonu, na stronie 175

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 62, 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 62.

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 166.

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.

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.

Tematy pokrewne

Sprawdzanie ustawień DHCP, na stronie 175

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

Możesz sprawdzić, czy telefon IP Cisco otrzymał polecenie resetowania z systemu Cisco Unified Communications Manager, naciskając na telefonie przycisk **Ustawienia** i wybierając kolejno opcje **Ustawienia admin.** > **Stan** > **Statystyki 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 174.

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 dźwiękiem

W poniższych sekcjach opisano sposoby rozwiązywania problemów z dźwiękiem.

Brak dźwięku

Problem

Co najmniej jeden z uczestników połączenia nic nie słyszy.

Rozwiązania

Jeśli co najmniej jedna osoba nie słyszy sygnałów audio, oznacza to brak połączenia IP między telefonami. Sprawdź konfigurację routerów i przełączników, aby zapewnić prawidłowe działanie połączeń.

Przerywanie głosu

Problem

Użytkownik skarży się na przerywanie głosu podczas połączenia.

Przyczyna

Może to wynikać z niedokładnej konfiguracji jittera.

Rozwiązania

Sprawdź statystyki AvgJtr i MaxJtr. Duża różnica między tymi statystykami może oznaczać problem z jitterem w sieci lub okresowe duże natężenie aktywności sieciowej.

Podłączenie jednego telefonu w trybie połączenia szeregowego nie jest możliwe

Problem

Jeden telefon konferencyjny w trybie połączenia szeregowego nie działa.

Rozwiązania

Sprawdź, czy kable podłączone do adaptera inteligentnego są prawidłowe. Do adaptera inteligentnego należy podłączyć dwa grubsze kable. Cieńszy kabel należy podłączyć do adaptera inteligentnego i zasilacza.

Tematy pokrewne

Tryb połączenia szeregowego, na stronie 33
Instalowanie telefonu konferencyjnego w trybie połączenia szeregowego, na stronie 40

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.

Sprawdzanie ustawień TFTP

Procedura

Krok 1 Sprawdź pole Serwer TFTP 1.

Jeśli do telefonu jest przypisany statyczny adres IP, należy ręcznie wprowadzić ustawienie dla opcji Serwer TFTP 1.

Jeśli używasz protokołu DHCP, telefon otrzymuje adres serwera TFTP z serwera DHCP. Sprawdź, czy adres IP jest skonfigurowany w opcji 150.

Krok 2 Możesz również zezwolić telefonowi na korzystanie z alternatywnego serwera TFTP. Takie ustawienie jest szczególnie przydatne, jeśli telefon ostatnio przenoszono między lokalizacjami.

Krok 3 Jeśli lokalny serwer DHCP nie podaje prawidłowego adresu serwera TFTP, włącz telefon, aby skorzystać z alternatywnego serwera TFTP.

Często 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:

a) Wyłącz protokół DHCP.

b) Przypisz telefonowi statyczny adres IP. Zastosuj to samo domyślne ustawienie routera, z którego korzystają inne telefony.

c) 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

Sprawdzanie adresu MAC telefonu, na stronie 62
Ponowne uruchamianie lub resetowanie telefonu konferencyjnego, na stronie 179

Sprawdzanie ustawień DHCP

Procedura

Krok 1 Naciśnij przycisk **Ustawienia** w telefonie.

Krok 2 Wybierz kolejno **Ustawienia admin.** > **Konfiguracja sieci Ethernet** > **Konfiguracja protokołu IPv4**.

Krok 3 Sprawdź pole Serwer DHCP.

Jeśli telefon ma przypisany statyczny adres IP, nie trzeba 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:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Krok 4 Sprawdź pola Adres IP, Maska podsieci i Router domyślny.

Jeśli telefon ma przypisany statyczny adres IP, należy ręcznie wprowadzić ustawienia tych opcji.

Krok 5 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:

https://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

Metody dodawania telefonów, na stronie 62
Cisco Unified Communications Manager — Dokumentacja, na stronie 14

Sprawdzanie ustawień DNS

Procedura

Krok 1 Naciśnij przycisk **Ustawienia** w telefonie.

Krok 2 Wybierz kolejno **Ustawienia admin.** > **Konfiguracja sieci Ethernet** > **Konfiguracja protokołu IPv4**

Krok 3 Sprawdź, czy pole Serwer DNS 1 zawiera poprawną wartość.

Krok 4 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 (domyślnie), Domyślne, Telefonia, SIP, UI, Sieć, Multimedia, Uaktualnienie, Akcesorium, Bezpieczeństwo, Energywise, MobileRemoteAccess (Przenośny zdalny dostęp)
- Zdalny dziennik — wartości: Wyłącz (domyślne), Włącz
- Serwer rejestrowania IPv6 lub Serwer rejestrowania — adres IP (adres IPv4 lub IPv6)

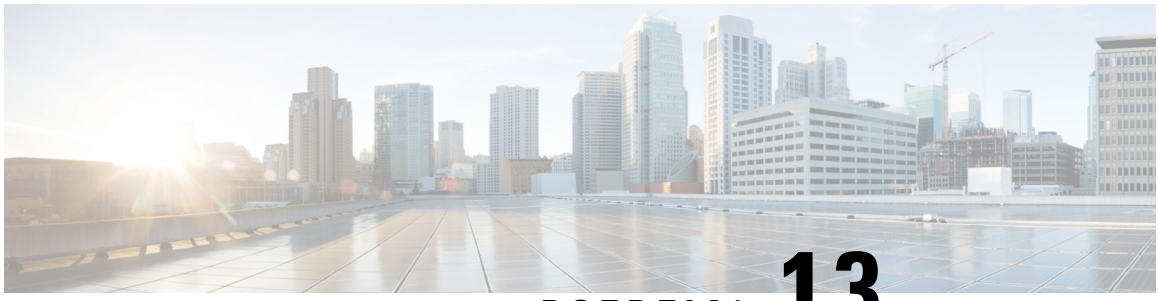
Uwaga Gdy nie będzie można uzyskać dostępu do Serwera rejestrowania, telefon zatrzyma wysyłanie komunikatów debugowania.

- 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

- Ponowne uruchamianie lub resetowanie telefonu konferencyjnego, na stronie 179
- Monitorowanie jakości dźwięku, na stronie 181
- Czyszczenie telefonu IP Cisco, na stronie 182

Ponowne uruchamianie lub resetowanie telefonu konferencyjnego

Resetowanie podstawowe umożliwia przywrócenie poprawnego działania telefonu w przypadku błędu. Można też przywrócić ustawienia domyślne konfiguracji i zabezpieczeń.

Ponowne uruchamianie telefonu konferencyjnego

Podczas ponownego uruchomienia telefonu zostaną utracone wszystkie zmiany ustawień użytkownika i sieci, które nie zostały zapisane w pamięci flash.

Procedura

Naciśnij kolejno **Ustawienia** > **Ustawienia admin.** > **Resetuj ustawienia** > **Resetuj urządzenie**.

Tematy pokrewne

Wprowadzanie tekstu za pomocą telefonu i poruszanie się po jego menu, na stronie 43

Resetowanie ustawień telefonu konferencyjnego za pomocą menu telefonu

Procedura

Krok 1 Naciśnij przycisk **Ustawienia**.

Krok 2 Wybierz kolejno **Ustawienia admin.** > **Resetuj ustawienia**.

Krok 3 Wybierz typ resetowania.

- **Wszystko —** przywraca ustawienia fabryczne.
- **Resetuj urządzenie —** resetuje urządzenie. Aktualne ustawienia nie zostaną zmienione.
- **Sieć —** resetuje konfigurację sieci do ustawień domyślnych.
- **Tryb usługi —** powoduje wyczyszczenie bieżącego trybu usługi, dezaktywowanie sieci VPN i ponowne uruchomienie telefonu.
- **Zabezpieczenia —** resetuje konfigurację zabezpieczeń do ustawień domyślnych. Ta opcja usuwa plik CTL.

Krok 4 Naciśnij **Resetuj** lub **Anuluj**.

Tematy pokrewne

Wprowadzanie tekstu za pomocą telefonu i poruszanie się po jego menu, na stronie 43

Przywracanie ustawień fabrycznych telefonu konferencyjnego za pomocą klawiatury numerycznej

Zresetowanie telefonu za pomocą klawiatury numerycznej powoduje przywrócenie w telefonie ustawień fabrycznych.

Procedura

Krok 1 Odłącz zasilanie telefonu:

- W przypadku zasilania PoE odłącz kabel sieci LAN.
- W przypadku korzystania z zasilacza odłącz go.

Krok 2 Odczekaj 5 sekund.

Krok 3 Naciśnij i przytrzymaj klawisz # i ponownie włącz zasilanie telefonu.

Krok 4 Podczas uruchamiania telefonu zaświeci się pasek LED. Gdy pasek LED włączy się, naciśnij kolejno klawisze **123456789*0#**.

Po naciśnięciu powyższych klawiszy telefon rozpocznie procedurę przywracania fabrycznych ustawień domyślnych.

Jeśli pomylisz kolejność klawiszy, telefon uruchomi się w zwykły sposób.

Przestroga Nie należy wyłączać zasilania telefonu, dopóki nie zakończy procedury przywracania fabrycznych ustawień domyślnych i nie pojawi się jego ekran główny.

Tematy pokrewne

Wprowadzanie tekstu za pomocą telefonu i poruszanie się po jego menu, na stronie 43

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 31: 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.	• Szumy lub zniekształcenia dźwięku, takie jak echo lub zmiany poziomu. • Połączenia z wieloma etapami kodowania i dekodowania, takie jak połączenia z telefonami komórkowymi lub telefonami na kartę. • Problemy akustyczne powodowane przez telefon głośnomówiący, telefon komórkowy w trybie głośnomówiącym albo bezprzewodowy zestaw słuchawkowy. Sprawdź liczniki pakietów wysłanych (TxCnt) i pakietów odebranych (RxCnt), aby sprawdzić przepływ pakietów z dźwiękiem.

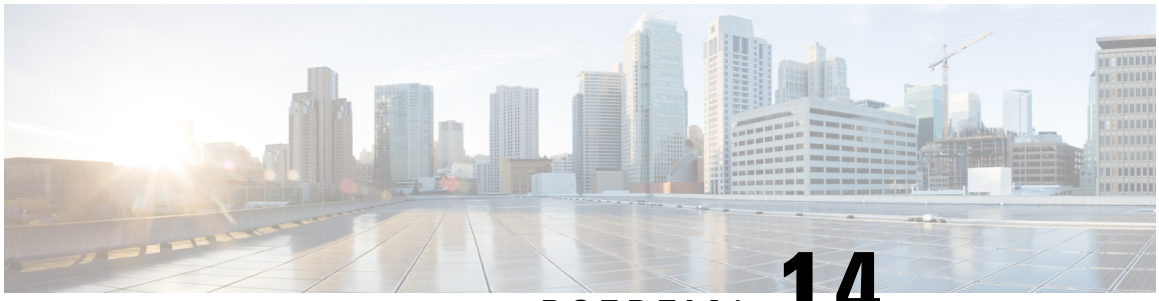
Zmiana metryki	Warunek
Znaczne obniżenie wyników MOS LQK	Problemy z działaniem sieci polegające na utracie pakietów lub dużych wahaniach opóźnień: • Średni spadek MOS LQK może wskazywać na powszechne i jednolite problemy. • Pojedyncze spadki MOS LQK mogą wskazywać na nagłe i krótkotrwałe problemy. Sprawdź, czy współczynnik ukrywania i sekundy ukrywania wskazują na utratę pakietów i wahania opóźnień.
Znaczny wzrost wyników MOS LQK	• Sprawdź, czy telefon nie używa innego kodeka niż powinien (RxType i TxType). • Sprawdź, czy po uaktualnieniu oprogramowania sprzętowego zmieniła się wersja MOS LQK.

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 183
- Obsługa zapisu połączeń międzynarodowych w dzienniku, na stronie 183
- Ograniczenia językowe, na stronie 184

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 14

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 (Chiny)
- 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**.