Przewodnik konfiguracyjny Webex dla Cisco BroadWorks

Zwolnij 45.6

Wersja dokumentu 1

Spis treści

1 Podsumowanie zmian 1
1.1 Zmiany w wersji 45.6, czerwiec 2025 r. 1
1.2 Zmiany w wersji 45.5, maj 2025 r. 1
1.3 Zmiany w wersji 45.4, kwiecień 2025 1
1.4 Zmiany w wersji 45.3, marzec 2025 r. 1
1.5 Zmiany w wersji 45.2, luty 2025 r. 1
1.6 Zmiany w wydaniu 45.1, styczeń 2025 1
1.7 Zmiany w wydaniu 44.12, grudzień 2024 1
1.8 Zmiany w wersji 44.11, listopad 2024 r. 1
1.9 Zmiany w wersji 44.10, październik 2024 r. 2
1.10 Zmiany w wersji 44.9, wrzesień 2024 r. 2
1.11 Zmiany w wydaniu 44.8, sierpień 2024 r. 2
1.12 Zmiany w wydaniu 44.7, lipiec 2024 r. 2
1.13 Zmiany w wersji 44.6, czerwiec 2024 r. 2
1.14 Zmiany w wersji 44.5, maj 2024 r. 2
1.15 Zmiany w wersji 44.4, kwiecień 2024 r. 2
1.16 Zmiany w wersji 44.3, marzec 2024 r. 2
1.17 Zmiany w wersji 44.2, luty 2024 r. 3
1.18 Zmiany w wersji 44.1, styczeń 2024 r. 3
2 Zmiany w plikach konfiguracyjnych 4
2.1 Zmiany w plikach konfiguracyjnych dla wydania 45.6 4
2.2 Zmiany w plikach konfiguracyjnych dla wydania 45.5 4
2.3 Zmiany w plikach konfiguracyjnych dla wydania 45.4 5
2.4 Zmiany w plikach konfiguracyjnych dla wydania 45.3 5
2.5 Zmiany w plikach konfiguracyjnych dla wydania 45.2 5
2.6 Zmiany w plikach konfiguracyjnych dla wydania 45.1 5
2.7 Zmiany w plikach konfiguracyjnych dla wydania 44.12 5
2.8 Zmiany w plikach konfiguracyjnych dla wydania 44.11 5
2.9 Zmiany w plikach konfiguracyjnych dla wydania 44.10 6
2.10 Zmiany w plikach konfiguracyjnych dla wydania 44.9 6
2.11 Zmiany w plikach konfiguracyjnych dla wydania 44.8 6
2.12 Zmiany w plikach konfiguracyjnych dla wydania 44.7 6
2.13 Zmiany w plikach konfiguracyjnych dla wydania 44.6 6
2.14 Zmiany w plikach konfiguracyjnych dla wydania 44.5 7
2.15 Zmiany w plikach konfiguracyjnych dla wydania 44.4 7
2.16 Zmiany w plikach konfiguracyjnych dla wydania 44.3 7
2.17 Zmiany w plikach konfiguracyjnych dla wydania 44.2 8
2.18 Zmiany w plikach konfiguracyjnych dla wydania 44.1 10

Informacje poufne firmy Cisco

3 Wprowadzenie ... 11
4 Instalacja ... 12
4.1 Zlokalizowane pobieranie klienta ... 12
4.2 Klient dla systemu Android ... 12
4.3 Klient iOS ... 12
4.4 Klient komputerowy ... 12
5 Zarządzanie urządzeniami ... 13
5.1 Tagi zarządzania urządzeniami ... 13
5.2 Częściowe ulepszenia dopasowania dla wyboru typu urządzenia ... 14
5.3 Konfiguracja klienta ... 15
5.4 Wdrażanie config-wxt.xml ... 15
5.5 Plik konfiguracyjny (config-wxt.xml) ... 15
5.6 Domyślne znaczniki systemowe ... 16
5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks ... 16
6 Tagi niestandardowe ... 19
6.1 Cechy wspólne ... 32
6.1.1 Ustawienia serwera SIP ... 32
6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie rzeczywistym ... 35
6.1.3 Nagłówki SIP 3GPP dla SRTP ... 37
6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP ... 38
6.1.5 Konfigurowalny limit czasu otwierania gniazda SIP ... 40
6.1.6 Wykrywanie dynamicznego serwera proxy SIP ... 41
6.1.7 Preferowane użycie portu dla SIP ... 46
6.1.8 Przełączanie awaryjne i powrót do pracy po awarii SIP ... 46
6.1.9 SIP SUBSKRYBUJ I ZAREJESTRUJ SIĘ Odśwież i SUBSKRYBUJ Spróbuj ponownie ... 51
6.1.10 Użyj identyfikatorów URI P-Associated-URI w REGISTER ... 52
6.1.11 Nagłówek SIP P-Early Media (PEM) ... 53
6.1.12 Obsługa AKTUALIZACJI SIP ... 53
6.1.13 Poprzedni wpis FIR INFORMACJI SIP ... 54
6.1.14 Zarządzanie portem SIP na potrzeby przesyłania NAT ... 54
6.1.15 Identyfikator sesji SIP ... 55
6.1.16 Działanie odrzucania połączeń przychodzących ... 56
6.1.17 Zakres portów protokołu transportu w czasie rzeczywistym ... 56
6.1.18 Obsługa ICE (tylko Webex Calling) ... 57
6.1.19 MUX RTCP ... 57
6.1.20 Przekaż ... 58
6.1.21 Połączenia konferencyjne n-Way i uczestnicy ... 59
6.1.22 Przełączenie połączenia ... 60
6.1.23 Zadzwoń do parku/odzyskaj ... 60
6.1.24 Statystyki połączeń ... 61

Informacje poufne firmy Cisco

6.1.25 Automatyczne odzyskiwanie połączeń / bezproblemowe przekazywanie połączeń 62
6.1.26 Nagrywanie połączeń 62
6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej 63
6.1.28 Transkrypcja poczty głosowej dla usługi Webex Calling 65
6.1.29 Ustawienia połączeń 66
6.1.30 Portal ustawień i ustawienia połączeń sieciowych 68
6.1.31 Logowanie/wylogowanie do centrum połączeń / kolejki połączeń 72
6.1.32 Źródło i ścieżki XSI 72
6.1.33 Kanał zdarzeń XSI 73
6.1.34 Konfiguracja kodeka 74
6.1.35 Wybieranie SIP-URI 76
6.1.36 Historia połączeń na wszystkich urządzeniach 77
6.1.37 Wyłącz połączenia wideo 77
6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji u dostawcy usługi E911 78
6.1.39 PAI jako tożsamość 79
6.1.40 Wyłącz udostępnianie ekranu 80
6.1.41 Wskazanie połączeń spamowych 80
6.1.42 Usuwanie szumów i rozszerzenie przepustowości dla połączeń PSTN/komórkowych 80
6.1.43 Oznaczenie QoS DSCP 81
6.1.44 Profil podstawowy 82
6.1.45 Lista zablokowanych (tylko Webex Calling) 83
6.1.46 Adaptacja i wdrażanie odporności mediów (MARI) 84
6.1.47 Połączenia równoczesne z tym samym użytkownikiem 86
6.1.48 RTCP-XR 87
6.1.49 Informacje o przekierowywaniu połączeń 87
6.1.50 ID dzwoniącego 88
6.1.51 Wielowierszowe 91
6.1.52 Rozszerzona autoryzacja SIP 92
6.1.53 Asystent osobisty (obecność poza biurem) 93
6.2 Funkcje tylko pulpitu 95
6.2.1 Wymuszone wylogowanie 95
6.2.2 Odbiór połączenia 96
6.2.3 Pomoc techniczna dla szefa (kierownik-asystent) 96
6.2.4 Eskaluj połączenia SIP do spotkania (tylko Webex Calling) 97
6.2.5 Połączenia Desk Phone Control — automatyczne odbieranie 97
6.2.6 Automatyczne odbieranie z powiadomieniem tonalnym 98
6.2.7 Sterowanie telefonem stacjonarnym – Sterowanie w trakcie połączenia – Konferencja 98
6.2.8 Powiadomienia przejmowania połączeń 99
6.2.9 Pakiet zdarzeń zdalnego sterowania 101
6.2.10 Brama utrzymania (tylko Webex Calling) 102
6.2.11 Pakiet zdarzeń zdalnego sterowania wyciszeniem (tylko Webex Calling) 102

Informacje poufne firmy Cisco

6.2.12 Przenieś połączenie ... 103
6.3 Funkcje dostępne tylko na urządzeniach mobilnych ... 105
6.3.1 Połączenia alarmowe ... 105
6.3.2 Powiadomienia wypychane dotyczące połączeń ... 106
6.3.3 Pojedyncze alerty ... 109
6.3.4 Kliknij, aby zadzwonić (oddzwoń) ... 109
6.3.5 Obsługa MNO ... 110
6.3.6 Identyfikator dzwoniącego w połączeniu przychodzącym ... 115
7 Wczesne funkcje wersji próbnej (BETA) ... 117
8 Mapowanie znaczników niestandardowych między Webex dla Cisco BroadWorks i UC-One ... 118
9 Załącznik A: Szyfry TLS ... 126
10 Załącznik B: Skrypt dostarczania tagów DM ... 127
10.1 Pulpit ... 128
10.2 Mobilna ... 130
10.3 Tablet ... 133
10.4 Znaczniki systemowe ... 136
11 Akronimy i skróty ... 138

Informacje poufne firmy Cisco

1 Podsumowanie zmian

W tej sekcji opisano zmiany w tym dokumencie dla każdego wydania i wersji dokumentu.

1.1 Zmiany w wersji 45.6, czerwiec 2025 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.2 Zmiany w wersji 45.5, maj 2025 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Usunięto sekcję Wybór CLID agenta kolejki połączeń — przestarzały przez *6.1.50.1 Identyfikator dzwoniącego w połączeniach wychodzących*.
- Usunięto przestarzałe znaczniki i atrybuty.

1.3 Zmiany w wersji 45.4, kwiecień 2025

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Przeniesiono sekcję *6.1.34.1 Kodek AI* — poza wersją BETA.
- Dodano sekcję *6.1.51 Wielowierszowe* — połączono sekcje w wersji BETA aplikacji klasycznej i mobilnej.
- Przeniesiono sekcję *6.1.52 Rozszerzona autoryzacja SIP* — brak wersji BETA.
- Przeniesiona sekcja *6.1.53 Asystent osobisty (obecność poza* biurem) jako wspólna dla komputerów stacjonarnych i mobilnych

1.4 Zmiany w wersji 45.3, marzec 2025 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.5 Zmiany w wersji 45.2, luty 2025 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Dodano sekcję *Rozszerzona autoryzacja SIP**Error! Reference source not found.*** w wersji BETA.

1.6 Zmiany w wydaniu 45.1, styczeń 2025

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Przeniesiono sekcję *Asystent osobisty (obecność poza* biurem) z wersji BETA.
- Przeniesiono sekcję *6.3.2.3 Tryb dostarczania (tylko Webex Calling)* z wersji BETA.

1.7 Zmiany w wydaniu 44.12, grudzień 2024

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.8 Zmiany w wersji 44.11, listopad 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

Informacje poufne firmy Cisco

- Dodano sekcję *Telefon komórkowy (tylko Webex Calling)* w wersji BETA.

1.9 Zmiany w wersji 44.10, październik 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Dodano sekcję *Asystent osobisty (obecność poza biurem)* w wersji BETA***Error! Reference source not found.***.
- Dodano sekcję *Tryb dostarczania (tylko Webex Calling)* w wersji BETA.

1.10 Zmiany w wersji 44.9, wrzesień 2024 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.11 Zmiany w wydaniu 44.8, sierpień 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Zaktualizowano sekcję *6.1.34 Konfiguracja kodeka* – dodano wyjaśnienia dotyczące sygnałów DTMF i obsługiwanych mechanizmów dostarczania.

1.12 Zmiany w wydaniu 44.7, lipiec 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Dodano sekcję *Kodek AI* w wersji BETA.
- Zaktualizowano sekcję *6.1.44 Profil podstawowy* — usunięto szczegóły dotyczące zachowania aplikacji Webex od wersji 43.2.

1.13 Zmiany w wersji 44.6, czerwiec 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Zaktualizowano sekcję *6.3.6. Identyfikator dzwoniącego* w połączeniu przychodzącym – dodano więcej szczegółów na temat natywnego środowiska i sposobu działania funkcji.

1.14 Zmiany w wersji 44.5, maj 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Zaktualizowano sekcję *6.1.18 Obsługa ICE (tylko Webex Calling)* — dodano obsługę protokołu IPv6 przez NAT64.
- Zaktualizowano sekcję *6.1.50 ID dzwoniącego* — dodano podsekcję *6.1.50.2 Nazwa zdalnego identyfikatora dzwoniącego*.

1.15 Zmiany w wersji 44.4, kwiecień 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Zaktualizowano sekcję *6.1.50.1 Identyfikator dzwoniącego w połączeniach wychodzących*.
- Zaktualizowano sekcję *Zmiany w plikach konfiguracyjnych dla wydania 44.3* – dodano szczegóły dotyczące bieżących aktualizacji w wersji 44.3.

Informacje poufne firmy Cisco

1.16 Zmiany w wersji 44.3, marzec 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Zaktualizowano sekcję *6.3.6. Identyfikator dzwoniącego w połączeniu przychodzącym*
    - Przeniesiono sekcję *6.1.50.1 Identyfikator dzwoniącego w połączeniach wychodzących* jako wspólny dla komputerów stacjonarnych i mobilnych i zaktualizowano go o więcej szczegółów.
- Zaktualizowano sekcję *6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP* – dodano szczegóły dotyczące konfigurowalnych utrzymywań połączeń przy użyciu niestandardowych tagów.

1.17 Zmiany w wersji 44.2, luty 2024 r.

Niniejsza wersja dokumentu zawiera następujące zmiany:

- Dodano sekcję *6.3.6 Identyfikator dzwoniącego w* połączeniu przychodzącym
- Zaktualizowano sekcję *6.2.8 Powiadomienia przejmowania połączeń*
    - Dodano podsekcję *6.2.8.1 Pole sygnalizacji aktywności* linii - przeniesiono do niej szczegóły dotyczące BLF.
    - Dodano podsekcję *6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)*.
- Dodano sekcję *6.1.49 Informacje o przekierowywaniu połączeń*.
- Zaktualizowano sekcję *6.1.8.3 Wymuś wersję IP* – dodano szczegóły dotyczące nowego trybu *nat64* .
- Zaktualizowano sekcję *6.1.42 Usuwanie szumów i rozszerzenie przepustowości dla połączeń PSTN/komórkowych* – dodano szczegóły dotyczące nowego wsparcia rozszerzenia pasma i aktualizacji usuwania szumów. Sekcja *Ulepszenia mowy w połączeniach PSTN* została usunięta z wersji BETA.

1.18 Zmiany w wersji 44.1, styczeń 2024 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

Informacje poufne firmy Cisco

2 Zmiany w plikach konfiguracyjnych

2.1 Zmiany w plikach konfiguracyjnych dla wydania 45.6

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.2 Zmiany w plikach konfiguracyjnych dla wydania 45.5

Usunięto następujące sekcje/znaczniki:

- [D/M]
  - Nieaktualne w wersji 42.12
  - Zastąpione dla każdej linii w obszarze
- [D]
  - Zastąpione symbolem dla każdej linii w protokołach>
- [D/M]
  - Nieaktualne w wersji 43.11
  - Zastąpione w
- [D/M] <service-uri>
  - Nieaktualne w wersji 42.12
  - Zastąpione znakiem . dla każdej linii w obszarze
- [D/M] <usuwanie hałasu>
  - Nieaktualne w wersji 43.12
  - Zastąpione przez
- [D/M] <numer centrum>
  - Nieaktualne w wersji 42.12
  - Zastąpione dla każdej linii w obszarze
- [D]
  - Nieaktualne w wersji 44.3
  - Zastąpione

Usunięto następujące atrybuty:

- [D/M] atrybut url w
- [D/M] Atrybut z włączoną funkcją elementów graficznych w obszarze

Następujące %TAG%s zostały usunięte:

- [D] %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%

Informacje poufne firmy Cisco

2.3 Zmiany w plikach konfiguracyjnych dla wydania 45.4

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.4 Zmiany w plikach konfiguracyjnych dla wydania 45.3

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.5 Zmiany w plikach konfiguracyjnych dla wydania 45.2

- [Funkcja BETA] Dodano tag w sekcji .

```
<config>
<protocols>
  <sip>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Dodano %TAG% następujące informacje:

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.6 Zmiany w plikach konfiguracyjnych dla wydania 45.1

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.7 Zmiany w plikach konfiguracyjnych dla wydania 44.12

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.8 Zmiany w plikach konfiguracyjnych dla wydania 44.11

- [funkcja BETA] [Tylko telefon komórkowy] [Tylko połączenie Webex]Dodano atrybut obsługujący wiele linii w tag .

  Dodano sekcje i dla linii drugorzędnych w sekcji .

```
<config>
<protocols><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
   <personal>
      <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
   </personal>
   <line lineType="%BW-MEMBERTYPE-1%">
      …
   </line>
   <line lineType="%BW-MEMBERTYPE-2%">
      …
   </line>
   …
   <line lineType="%BW-MEMBERTYPE-10%">
      …
   </line>
</lines>
```


Informacje poufne firmy Cisco

2.9 Zmiany w plikach konfiguracyjnych dla wydania 44.10

- [Funkcja BETA] Dodano tag w sekcji .

```
<config>
<services>
   <personal-assistant enabled="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

- [Funkcja BETA] [Tylko telefon komórkowy] [Tylko aplikacja Webex Calling]Dodano atrybut trybu dostarczania w tag .

```
<config>
<services>
   <push-notifications-for-calls enabled="true" connect-sip-on-
accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%" ring-timeout-
seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%" delivery-
mode="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

Dodano %TAG%s:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.10 Zmiany w plikach konfiguracyjnych dla wydania 44.9

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.11 Zmiany w plikach konfiguracyjnych dla wydania 44.8

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

2.12 Zmiany w plikach konfiguracyjnych dla wydania 44.7

- [Funkcja BETA]
  Dodano kodek SI (xCodec) w sekcji .<audio>

```
<config>
<services><calls>
  <audio>
    <codecs>
      <codec name="opus" priority="1" payload=""/>
      <codec name="xCodec" mode="HP" priority=".99" payload=""/>
      <codec name="xCodec" mode="ULP" priority=".98" payload=""/>
      <codec name="G722" priority=".9" payload=""/>
      <codec name="PCMU" priority=".8" payload=""/>
      <codec name="PCMA" priority=".7" payload=""/>
      <codec name="G729" priority=".5" payload="" vad=""/>
      <codec name="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="telephone-event" payload="101" in-band="false"/>
```

2.13 Zmiany w plikach konfiguracyjnych dla wydania 44.6

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

Informacje poufne firmy Cisco

2.14 Zmiany w plikach konfiguracyjnych dla wydania 44.5

- [Tylko Webex Calling] Dodano atrybut enable-ipv6-support do tagu .

```
<config>
<protocols><rtp>
  <ice enabled="%ENABLE_RTP_ICE_WXT%"
       enable-ipv6-support="%ENABLE_RTP_ICE_IPV6_WXT%"
       mode="%RTP_ICE_MODE_WXT%"
       service-uri="%RTP_ICE_SERVICE_URI_WXT%"
       port="%RTP_ICE_PORT_WXT%"/>
```

- Znacznik został dodany w sekcji z jako podtagiem.

```
<config>
<services><calls>
   <caller-id>
      <remote-name>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Dodano %TAG%s:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.15 Zmiany w plikach konfiguracyjnych dla wydania 44.4

- [Tylko komputer] [Tylko aplikacja Webex Calling] Dodano tagi , i w sekcji .

```
<config>
<services><calls>
  <caller-id>
    <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <additional-numbers
enabled="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </outgoing-calls>
```

2.16 Zmiany w plikach konfiguracyjnych dla wydania 44.3

- [Tylko komputer] [Tylko Webex Calling] Dodano w nowej sekcji z jako podtagiem.

```
<config>
<services><calls>
  <caller-id>
    <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
    </outgoing-calls>
```


Informacje poufne firmy Cisco

- Dodano znaczniki niestandardowe (%UDP_KEEPALIVE_ENABLED_WXT%, %TCP_KEEPALIVE_ENABLED_WXT% i %TLS_KEEPALIVE_ENABLED_WXT%) w celu zastąpienia zapisanej na twardo wartości włączonej utrzymywania aktywności dla każdego transportu w ramach .

```
<config>
<protocols><sip>
<transports>
  <udp>
    <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
      …
  </udp>
  <tcp>
    <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
      …
  </tcp>
  <tls>
    <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
      …
  </tls>
```

Dodano %TAG%s:

- %UDP_KEEPALIVE_ENABLED_WXT%
- %TCP_KEEPALIVE_ENABLED_WXT%
- %TLS_KEEPALIVE_ENABLED_WXT%

2.17 Zmiany w plikach konfiguracyjnych dla wydania 44.2

- [Tylko telefon komórkowy] Dodano sekcję w sekcji .
  Dodano podznaczniki i z nowym znacznikiem dla obu tych elementów.

```
<config>
<services><calls>
  <caller-id>
    <incoming-calls>
      <append-number
enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
    </incoming-calls>
    <missed-calls>
      <append-number
enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
    </missed-calls>
```

- [Tylko telefon komórkowy] [Tylko aplikacja Webex Calling] Dodano w nowej sekcji .

```
<config>
<services><calls>
  <caller-id>
    <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <additional-numbers
enabled="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
```


Informacje poufne firmy Cisco

```
    </outgoing-calls>
```

- Dodano tag w sekcji .

```
<config>
<services><calls>
  <call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

- [Tylko komputer] [Tylko aplikacja Webex Calling] Dodano w sekcji z i jako podtagami.
  Dodano również znacznik pod każdym znacznikiem w sekcji .

```
<config>
<services><calls>
  <group-call-pickup-notifications enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
    <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
    <max-timeout value="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
  </group-call-pickup-notifications>
  …
<protocols><sip>
  <lines>
    <line>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
      ...
    </line>
    <line>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>
      ...
    </line>
    …
```

Dodano %TAG%s:

- %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%
- %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%
- %ENABLE_GCP_NOTIFICATIONS_WXT%
- %ENABLE_GCP_DISPLAY_CALLER_WXT%
- %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%
- %BWGROUP-CALL-PICKUP-BOOL-n%

Następujące znaczniki %TAG% zostały wycofane:

- %ENABLE_NOISE_REMOVAL_WXT%

Informacje poufne firmy Cisco

2.18 Zmiany w plikach konfiguracyjnych dla wydania 44.1

W tej wersji nie było żadnych aktualizacji plików konfiguracyjnych.

Informacje poufne firmy Cisco

3 Wprowadzenie

Celem tego dokumentu jest przedstawienie opisu konfiguracji klienta Webex dla Cisco BroadWorks.

Plik konfiguracyjny *config-wxt.xml* jest dostarczany w dwóch wersjach – jednej dla urządzeń przenośnych (Android i iOS) i jednej dla komputerów stacjonarnych (Windows i MacOS).

Klienci są konfigurowani przy użyciu konfiguracji, która nie jest widoczna dla użytkownika końcowego. Plik *config-wxt.xml* zawiera informacje specyficzne dla serwera, takie jak adresy i porty serwera oraz opcje runtime dla samego klienta (np. opcje widoczne na ekranie *Ustawienia*).

Pliki konfiguracyjne są odczytywane przez klienta podczas jego uruchamiania, po pobraniu z Zarządzania urządzeniami. Informacje z plików konfiguracyjnych są przechowywane w postaci zaszyfrowanej, dzięki czemu są niewidoczne i niedostępne dla użytkownika końcowego.

UWAGA: Właściwości XML nie mogą zawierać spacji (na przykład <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"/> instead of <transfer-call enabled = "%ENABLE_TRANSFER_CALLS_WXT%"/>).

Informacje poufne firmy Cisco

4 Instalacja

Klientów Webex for Cisco BroadWorks można zainstalować z następujących źródeł:

https://www.webex.com/webexfromserviceproviders-downloads.html

4.1 Zlokalizowane pobieranie klienta

Następujące zlokalizowane wersje klientów Webex for Cisco BroadWorks można pobrać w następujący sposób:

https://www.webex.com/ko/webexfromserviceproviders-downloads.html
https://www.webex.com/fr/webexfromserviceproviders-downloads.html
https://www.webex.com/pt/webexfromserviceproviders-downloads.html
https://www.webex.com/zh-tw/webexfromserviceproviders-downloads.html
https://www.webex.com/zh-cn/webexfromserviceproviders-downloads.html
https://www.webex.com/ja/webexfromserviceproviders-downloads.html
https://www.webex.com/es/webexfromserviceproviders-downloads.html
https://www.webex.com/de/webexfromserviceproviders-downloads.html
https://www.webex.com/it/webexfromserviceproviders-downloads.html

4.2 Klient dla systemu Android

Klient Android jest instalowany jako aplikacja (pakiet aplikacji Android [APK]), która przechowuje ustawienia- i dane związane z konfiguracją w swoim prywatnym obszarze.

Istnieje kontrola wersji oparta na procedurach Google Play. Wyświetlane jest standardowe powiadomienie Google Play (tzn. system Android automatycznie wskaże, że dostępna jest nowa wersja oprogramowania).

Po pobraniu nowej wersji stare oprogramowanie zostaje nadpisane. Dane użytkownika są jednak domyślnie zachowywane.

Należy pamiętać, że użytkownik nie musi wybierać żadnych opcji instalacji ani odinstalowywania.

4.3 Klient iOS

Klient systemu iOS jest instalowany jako aplikacja, która przechowuje dane związane z ustawieniami w "piaskownicy", a dane pliku konfiguracyjnego są przechowywane w formie zaszyfrowanej.

Istnieje kontrola wersji w oparciu o procedury Apple App Store. Ikona App Store jest podświetlona, aby poinformować, że dostępna jest nowa wersja oprogramowania.

Po pobraniu nowej wersji stare oprogramowanie zostaje nadpisane. Dane użytkownika są jednak domyślnie zachowywane.

Należy pamiętać, że użytkownik nie musi wybierać żadnych opcji instalacji ani odinstalowywania.

4.4 Klient komputerowy

Informacje o instalacji i kontroli wersji klienta komputerowego (Windows i MacOS) można znaleźć na stronie: https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade.

Informacje poufne firmy Cisco

5 Zarządzanie urządzeniami

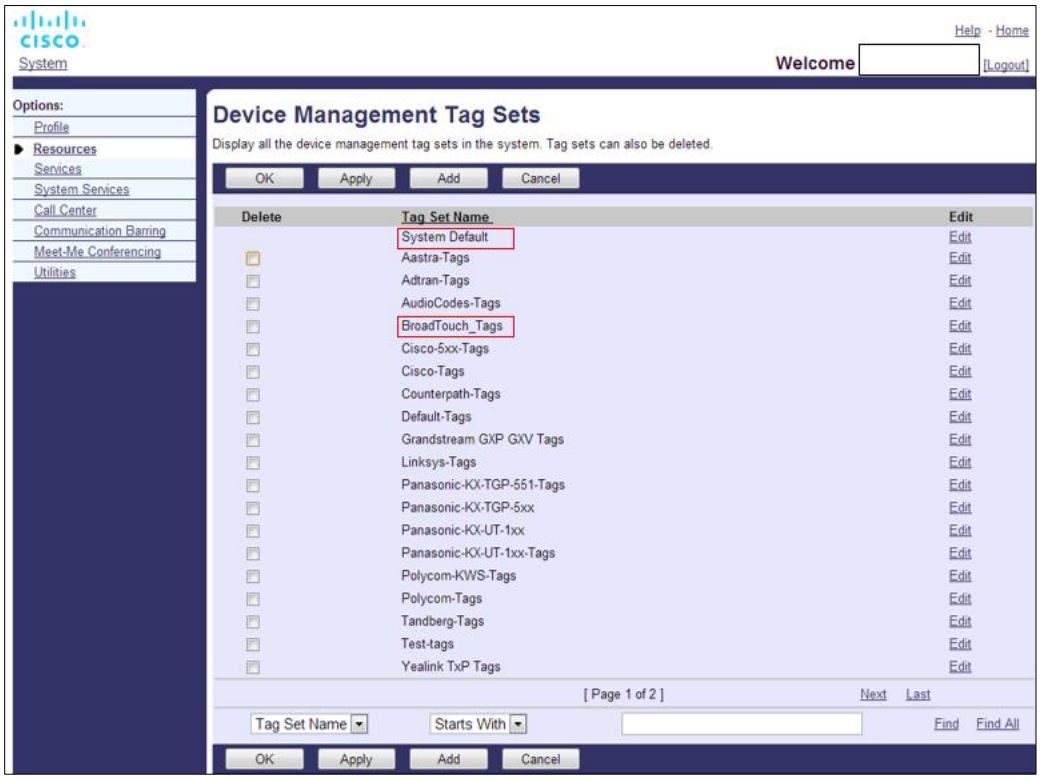
5.1 Tagi zarządzania urządzeniami

Webex dla Cisco BroadWorks używa *zestawów znaczników zarządzania urządzeniami* przedstawionych na poniższym rysunku. *Domyślne ustawienia systemu* i zestawy tagów niestandardowych są wymagane do skonfigurowania określonych ustawień urządzenia/klienta. Ten zestaw tagów zapewnia elastyczność w zarządzaniu ustawieniami łączności sieciowej/usługowej klienta, a także kontrolę aktywacji funkcji.

Ten zestaw niestandardowych tagów jest dostarczany przez administratora systemu za pomocą opcji *System → Zasoby → Zestawy tagów zarządzania urządzeniami* . Administrator musi dodać nowe zestawy tagów:

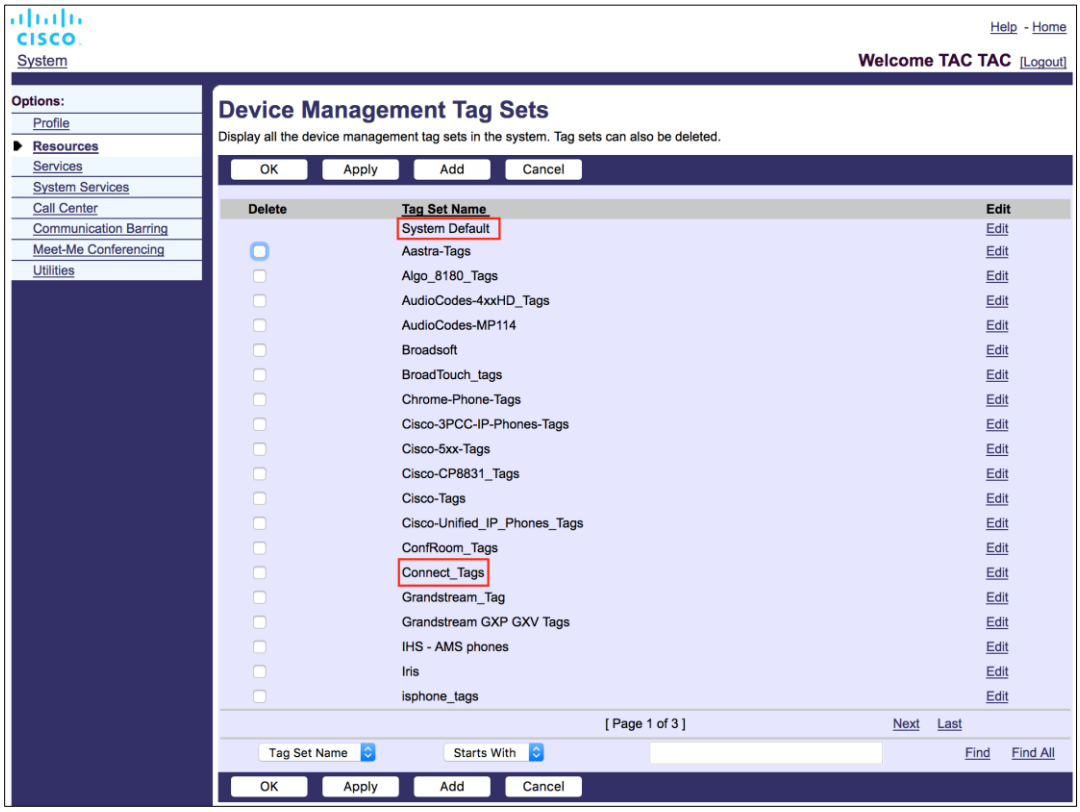
- Komórkowy: Połącz_Tagi
- Tabletka: PodłączTablet_Tags
- Pulpit: Tagi BroadTouch

Utwórz każdy indywidualny tag i ustaw jego wartość. Odnośniki do sekcji zawierają szczegółowe opisy każdego tagu. Znaczniki niestandardowe są podzielone na grupy na podstawie funkcjonalności i omówione w dalszej części dokumentu.



Rysunek 1 Zestawy tagów zarządzania urządzeniami stacjonarnymi

Informacje poufne firmy Cisco



Rysunek 2 Zestawy znaczników zarządzania urządzeniami przenośnymi

5.2 Częściowe ulepszenia dopasowania dla wyboru typu urządzenia

Aby zapewnić większą elastyczność przy wyborze pakietów funkcjonalności dla grup użytkowników lub poszczególnych użytkowników, typ profilu urządzenia wybierany jest na podstawie (pierwszego) częściowego dopasowania. Dzięki temu klienci mogą korzystać z różnych typów urządzeń.

Ogólna procedura zarządzania urządzeniami określa, że serwer aplikacji Cisco BroadWorks udostępnia typ profilu urządzenia. Nazywa się „Business Communicator – PC” dla komputerów stacjonarnych, „Connect – Mobile” dla urządzeń mobilnych i „Connect – Tablet” dla tabletów. Można utworzyć profil urządzenia i przypisać go użytkownikowi. Następnie serwer aplikacji tworzy plik konfiguracyjny i zapisuje go na serwerze profili.

Po zalogowaniu klient sprawdza listę przypisanych urządzeń za pomocą Xsi i wyszukuje odpowiedni profil typu urządzenia. Klient wybiera pierwszy profil, którego nazwa zaczyna się od nazwy odpowiadającego mu typu urządzenia. Następnie dane konfiguracji profilu urządzenia (plik konfiguracyjny) skojarzone z tym profilem urządzenia służą do włączania i wyłączania różnych funkcji.

Umożliwia to wykorzystanie tego samego pliku wykonywalnego klienta z różnymi typami profili urządzeń, dzięki czemu dostawca usług może zmieniać pakiety funkcji dla poszczególnych użytkowników lub grup użytkowników, po prostu zmieniając typ profilu urządzenia w DM dla użytkownika lub grupy użytkowników.

Informacje poufne firmy Cisco

Na przykład dostawca usług może mieć dowolną liczbę typów profili urządzeń opartych na rolach użytkowników, takich jak „Business Communicator – PC Basic”, „Business Communicator – PC Executive” lub „Business Communicator – PC Assistant”, i zmieniać funkcjonalność dostępną dla poszczególnych użytkowników, zmieniając dla nich typ profilu urządzenia.

Należy pamiętać, że w otrzymanej liście urządzeń XML nie oczekuje się występowania wielu pasujących typów profili urządzeń, lecz tylko jeden.

5.3 Konfiguracja klienta

Wersja klienta Webex for Cisco BroadWorks używa pliku *config-wxt.xml* do skonfigurowania funkcji połączeń. Istnieje osobna procedura konfiguracji dla Webex, która nie jest omówiona w tym dokumencie.

5.4 Wdrażanie config-wxt.xml

Dodaj odpowiedni *plik config-wxt.xml* do profili urządzeń Connect – Mobile, Connect – Tablet i Business Communicator – PC. Webex dla Cisco BroadWorks korzysta z tych samych profili urządzeń, co UC-One, dzięki czemu ułatwia wdrażanie.

UWAGA 1: Plik konfiguracyjny musi istnieć dla każdego profilu urządzenia.

UWAGA 2: Zdecydowanie ZALECAMY aktualizację szablonów za pomocą najnowszej wersji aplikacji Webex

5.5 Plik konfiguracyjny (config-wxt.xml)

Do odróżnienia nowego wdrożenia konfiguracji Webex dla Cisco BroadWorks od starszych klientów są używane nowe znaczniki niestandardowe z sufiksem **_WXT** . Nadal istnieje jednak kilka (systemowych) tagów, które są udostępniane między UC-One i Webex.

Niektóre z niestandardowych znaczników systemu Cisco BroadWorks są również używane w pliku konfiguracyjnym *config-wxt.xml* . Aby uzyskać więcej informacji na temat każdego z następujących tagów, zobacz *5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks*.

- %BWNETWORK-CONFERENCE-SIPURI-n%
- %BWVOICE-PORTAL-NUMBER-n%
- %BWLINEPORT-n%
- %BWAUTHUSER-n%
- %BWAUTHPASSWORD-n%
- %BWE164-n%
- %BWHOST-n%
- %BWNAME-n%
- %BWEXTENSION-n%
- %BWAPPEARANCE-LABEL-n%

Informacje poufne firmy Cisco

- %BWDISPLAYNAMELINEPORT%
- %BWLINEPORT-PRIMARY%
- %BWE911-PRIMARY-HELDURL%
- %BWE911-CUSTOMERID%
- %BWE911-SECRETKEY%
- %BWE911-EMERGENCY-NUMBER-LIST%
- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (tylko w usłudze Webex Calling)

5.6 Domyślne znaczniki systemowe

Jako administrator systemu możesz uzyskać dostęp do domyślnych tagów systemowych za pomocą opcji *System → Zasoby → Zestawy tagów zarządzania urządzeniami* . Poniższe domyślne tagi systemowe muszą zostać skonfigurowane podczas instalacji pakietu połączeń VoIP.

Znacznik	Opis
%SBC_ADDRESS_WXT%	Należy go skonfigurować jako w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP kontrolera granicznego sesji (SBC) wdrożonego w sieci. Przykład: sbc.yourdomain.com
%SBC_PORT_WXT%	Jeżeli SBC_ADDRESS_WXT jest adresem IP, to ten parametr należy ustawić na port SBC. Jeśli SBC_ADDRESS_WXT jest nazwą FQDN, można pozostawić ją nieustawioną. Przykład: 5075

5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks

Oprócz domyślnych znaczników systemowych i niestandardowych, które należy zdefiniować, istnieją zazwyczaj używane znaczniki systemowe Cisco BroadWorks, które są częścią zalecanego pliku archiwum typu urządzenia (DTAF). Tagi te są wymienione w tej sekcji. W zależności od zainstalowanego pakietu rozwiązań, nie wszystkie tagi systemowe są używane.

Znacznik	Opis
%BWNETWORK-CONFERENCE-SIPURI-n%	Jest to identyfikator URI serwera używany do włączania konferencji N-Way.
%BWVOICE-PORTAL-NUMBER-n%	Numer ten jest wykorzystywany do obsługi poczty głosowej. Klient wybiera ten numer podczas pobierania poczty głosowej.
%BWLINEPORT-n%	Nazwa użytkownika SIP używana w sygnalizacji SIP, na przykład podczas rejestracji.

Informacje poufne firmy Cisco

Znacznik	Opis
%BWHOST-n%	Jest to część domeny udostępnionego portu liniowego dla urządzenia przypisanego użytkownikowi. Jest on pobierany z profilu użytkownika. Zwykle używany jako domena SIP.
%BWAUTHUSER-n%	To jest nazwa użytkownika służąca do uwierzytelniania. Jeśli subskrybentowi przypisano uwierzytelnianie, jest to podany identyfikator użytkownika na stronie Uwierzytelnianie, niezależnie od wybranego trybu uwierzytelniania typu urządzenia. Nazwa użytkownika SIP, zazwyczaj używana w sygnalizacji 401 i 407. Może różnić się od domyślnej nazwy użytkownika SIP.
%BWAUTHPASSWORD-n%	To jest hasło uwierzytelniania użytkownika. Jeśli subskrybentowi przypisano uwierzytelnianie, jest to hasło udostępnione na stronie Uwierzytelnianie, niezależnie od wartości wybranego trybu uwierzytelniania typu urządzenia. Hasło protokołu SIP używane w sygnalizacji protokołu SIP.
%BWE164-n%	Ten tag zawiera numer telefonu użytkownika w formacie międzynarodowym.
%BWNAME-n%	Jest to imię i nazwisko subskrybenta podane w profilu użytkownika. Imię i nazwisko należy połączyć ze sobą. W przypadku konfiguracji wielowierszowej, jeśli nie skonfigurowano żadnej etykiety wiersza i nie jest ona pusta, używana jako nazwa wyświetlana dla wiersza w selektorze wiersza.
%BWEXTENSION-n%	Numer wewnętrzny subskrybenta jest pobierany z numeru wewnętrznego podanego w profilu użytkownika. Jeśli nie przydzielono numeru wewnętrznego, znacznik jest zastępowany numerem telefonu abonenta (DN).
%BWAPPEARANCE-LABEL-n%	Oto skonfigurowana etykieta linii. Używane jako nazwa wiersza, jeżeli nie jest puste.
%BWDISPLAYNAMELINEPORT%	Jest to linia/port pierwszej linii prywatnej, w odróżnieniu od linii współdzielonej (wygląd połączenia współdzielonego). Jest to port linii obsługiwany na urządzeniu przypisanym do użytkownika. Zostanie on pobrany z profilu użytkownika. Służy do identyfikacji głównej linii użytkownika.
%BWLINEPORT-PRIMARY%	Port linii podstawowej jest obsługiwany przez urządzenie przypisane do użytkownika. Ten znacznik nie obejmuje części domeny udostępnionego portu liniowego. Jest on pobierany z profilu użytkownika.
%BWE911-PRIMARY-HELDURL%	Określa adres URL platformy lokalizacji awaryjnej RedSky obsługującej protokół HELD.

Informacje poufne firmy Cisco

Znacznik	Opis
%BWE911-CUSTOMERID%	Identyfikator klienta (HeldOrgId, CompanyID) użyty w żądaniu HTTPS RedSky.
%BWE911-SECRETKEY%	Sekret uwierzytelniania żądania HTTPS RedSky.
%BWE911-EMERGENCY-NUMBER-LIST%	Lista numerów alarmowych obsługiwanych przez RedSky. Aby używać tego znacznika, do zestawu znaczników używanego przez typ urządzenia należy dodać niestandardowy znacznik %RESERVEDBW911-EMERGENCY-NUMBER-LIST% reserved. Tag „reserved" musi zawierać numery alarmowe zdefiniowane w BroadWorks w AS_CLI/System/CallP/CallTypes > w formacie rozdzielonym przecinkami, np. 911, 0911, 933. **UWAGA:** Klient Webex nie obsługuje symboli wieloznacznych w numerach alarmowych; dlatego do niestandardowego znacznika „zarezerwowane" należy dodać tylko dokładne numery alarmowe. Poniższy przykład pokazuje, w jaki sposób funkcja znaczników zarezerwowanych ma być używana: 1) Natywny znacznik %BWE911-EMERGENCY-NUMBER-LIST% został dodany do pliku szablonu urządzenia 2) Zarezerwowany niestandardowy znacznik %RESERVEDBW911-EMERGENCY-NUMBER-LIST% zostaje dodany do zestawu znaczników używanego przez urządzenie o wartości 911, 0911, 933 3) Po odtworzeniu pliku lokalny znacznik %RESERVEDBW911-EMERGENCY-NUMBER-LIST% zostanie rozwiązany na 911, 0911, 933
%BW-MEMBERTYPE-n%	To jest typ dla każdej linii. Może to być „Profil wirtualny", „Użytkownik" lub „Miejsce".
%BWUSEREXTID-n%	To jest zewnętrzny identyfikator dla danej linii (tylko Webex Calling)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Podaje informacje, czy odpowiednia linia ma skonfigurowaną grupę przejmowania połączeń. (tylko Webex Calling)

Informacje poufne firmy Cisco

6 Tagi niestandardowe

W tej sekcji opisano tagi niestandardowe używane w Webex dla Cisco BroadWorks. Zawiera listę wszystkich niestandardowych tagów używanych na platformach stacjonarnych i mobilnych/tabletach.

Należy jednak pamiętać, że niektóre ustawienia opisane w tej sekcji są obsługiwane tylko w konkretnej wersji klienta. Aby sprawdzić, czy dane ustawienie nie ma zastosowania do starszej wersji klienta, zapoznaj się z odpowiednim przewodnikiem konfiguracji właściwym dla danej wersji.

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_REJECT_WITH_486_WXT%	T	T	true	*6.1.16 Działanie odrzucania połączeń przychodzących*
%REJECT_WITH_XSI_MODE_WXT%	N	T	spadek_fałsz	*6.3.2 Powiadomienia wypychane dotyczące połączeń*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	T	zajęty	*6.3.2 Powiadomienia wypychane dotyczące połączeń*
%ENABLE_TRANSFER_CALLS_WXT%	T	T	false	*6.1.20 Przekaż*
%ENABLE_CONFERENCE_CALLS_WXT%	T	T	false	*6.1.21 Połączenia konferencyjne n-Way i uczestnicy*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	T	T	false	*6.1.21 Połączenia konferencyjne n-Way i uczestnicy*
%MAX_CONF_PARTIES_WXT%	T	T	10	*6.1.21 Połączenia konferencyjne n-Way i uczestnicy*
%ENABLE_CALL_STATISTICS_WXT%	T	T	false	*6.1.24 Statystyki połączeń*
%ENABLE_CALL_PULL_WXT%	T	T	false	*6.1.22 Przełączenie połączenia*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	T	false	*6.3.2 Powiadomienia wypychane dotyczące połączeń*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	T	T	false	*6.1.28 Transkrypcja poczty głosowej dla usługi Webex* Calling
%ENABLE_MWI_WXT%	T	T	false	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%MWI_MODE_WXT%	T	T	puste	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej*
%ENABLE_VOICE_MAIL_WXT%	T	T	false	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej*
%ENABLE_VISUAL_VOICE_MAIL_WXT%	T	T	false	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej*
%ENABLE_FORCED_LOGOUT_WXT%	T	N	false	*6.2.1 Wymuszone* wylogowanie
%FORCED_LOGOUT_APPID_WXT%	T	N	puste	*6.2.1 Wymuszone* wylogowanie
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	T	T	false	*6.1.29.1 Przekazywanie połączeń zawsze*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	T	T	true	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	T	T	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_EMERGENCY_DIALING_WXT%	N	T	false	*6.3.1 Połączenia alarmowe*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	T	911, 112	*6.3.1 Połączenia alarmowe*
%ENABLE_USE_RPORT_WXT%	T	T	false	*6.1.14 Zarządzanie portem SIP na potrzeby przesyłania* NAT
%RPORT_USE_LOCAL_PORT_WXT%	T	T	false	*6.1.14 Zarządzanie portem SIP na potrzeby przesyłania* NAT
%USE_TLS_WXT%	T	T	false	*6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie rzeczywistym*
%SBC_ADDRESS_WXT%	T	T	puste	*5.6 Domyślne znaczniki systemowe*
%SBC_PORT_WXT%	T	T	5060	*5.6 Domyślne znaczniki systemowe*
%USE_PROXY_DISCOVERY_WXT%	T	T	false	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%USE_TCP_FROM_DNS_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%USE_UDP_FROM_DNS_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%USE_TLS_FROM_DNS_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%DOMAIN_OVERRIDE_WXT%	T	T	puste	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Y (tylko system Windows)	N	false	*6.1.6 Wykrywanie dynamicznego serwera proxy SIP*
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	T	T	5000	*6.1.5 Konfigurowalny limit czasu otwierania gniazda SIP*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	T	T	10000	*6.1.5 Konfigurowalny limit czasu otwierania gniazda SIP*
%SOURCE_PORT_WXT%	T	T	5060	*6.1.7 Preferowane użycie portu dla SIP*
%SIP_FAILBACK_ENABLED_WXT%	T	N	true	*6.1.8.2 Powrót SIP*
%SIP_FAILBACK_TIMEOUT_WXT%	T	N	900	*6.1.8.2 Powrót SIP*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	T	N	false	*6.1.8.2 Powrót SIP*
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	T	T	dns	*6.1.8.3. Wymuś wersję IP*
%USE_ALTERNATIVE_IDENTITIES_WXT%	T	T	false	*6.1.10 Użyj identyfikatorów URI P-Associated-URI* w REGISTER
%TCP_SIZE_THRESHOLD_WXT%	T	T	18000	*6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP*
%SIP_REFRESH_ON_TTL_WXT%	T	N	false	*6.1.8.4 Zarządzanie TTL DNS*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	T	T	false	*6.1.12 Obsługa AKTUALIZACJI SIP*
%ENABLE_PEM_SUPPORT_WXT%	T	T	false	*6.1.11 Nagłówek SIP P-Early Media (PEM)*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_SIP_SESSION_ID_WXT%	T	T	false	*6.1.15 Identyfikator sesji SIP*
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	T	T	false	*6.1.13 Poprzedni wpis FIR INFORMACJI SIP*
%SRTP_ENABLED_WXT%	T	T	false	*6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie rzeczywistym*
%SRTP_MODE_WXT%	T	T	false	*6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie rzeczywistym*
%ENABLE_REKEYING_WXT%	T	T	true	*6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie rzeczywistym*
%RTP_AUDIO_PORT_RANGE_START_WXT%	T	T	8000	*6.1.17 Zakres portów protokołu transportu w czasie rzeczywistym*
%RTP_AUDIO_PORT_RANGE_END_WXT%	T	T	8099	*6.1.17 Zakres portów protokołu transportu w czasie rzeczywistym*
%RTP_VIDEO_PORT_RANGE_START_WXT%	T	T	8100	*6.1.17 Zakres portów protokołu transportu w czasie rzeczywistym*
%RTP_VIDEO_PORT_RANGE_END_WXT%	T	T	8199	*6.1.17 Zakres portów protokołu transportu w czasie rzeczywistym*
%ENABLE_RTCP_MUX_WXT%	T	T	true	*6.1.19 MUX RTCP*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	T	T	true	*6.1.33 Kanał zdarzeń XSI*
%CHANNEL_HEARTBEAT_WXT%	T	T	10000	*6.1.33 Kanał zdarzeń XSI*
%XSI_ROOT_WXT%	T	T	pusty (używa oryginalnego adresu URL)	*6.1.32 Źródło i ścieżki XSI*
%XSI_ACTIONS_PATH_WXT%	T	T	/com.broadsoft.xsi-actions/	*6.1.32 Źródło i ścieżki XSI*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%XSI_EVENTS_PATH_WXT%	T	T	/com.broadsoft.xsi-events/	*6.1.32 Źródło i ścieżki XSI*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	T	T	false	*6.1.25 Automatyczne odzyskiwanie połączeń / bezproblemowe przekazywanie* połączeń
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	T	tylko cs	*6.3.1 Połączenia alarmowe*
%ENABLE_CALL_PICKUP_BLIND_WXT%	T	N	false	*6.2.2 Odbiór połączenia*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	T	N	false	*6.2.2 Odbiór połączenia*
%WEB_CALL_SETTINGS_URL_WXT%	T	T	puste	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%USER_PORTAL_SETTINGS_URL_WXT%	T	T	puste	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%ENABLE_CALL_CENTER_WXT%	T	T	false	*6.1.31 Logowanie/wylogowanie do centrum połączeń / kolejki* połączeń
%WEB_CALL_SETTINGS_TARGET_WXT%	T	T	zewnętrzny	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i ustawienia połączeń sieciowych*
%USE_MEDIASEC_WXT%	T	T	false	*6.1.3 Nagłówki SIP 3GPP dla SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	T	false	*6.3.4 Kliknij, aby zadzwonić (oddzwoń)*
%DIALING_CALL_BACK_TIMER_WXT%	N	T	10	*6.3.4 Kliknij, aby zadzwonić (oddzwoń)*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	T	N	false	*6.2.3 Pomoc techniczna dla szefa (*kierownik-asystent)
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	T	35	*6.3.2 Powiadomienia wypychane dotyczące połączeń*
%ENABLE_CALL_RECORDING_WXT%	T	T	false	*6.1.26 Nagrywanie połączeń*
%ENABLE_SINGLE_ALERTING_WXT%	N	T	false	*6.3.3 Pojedyncze alerty*
%ENABLE_CALL_PARK_WXT%	T	T	false	*6.1.23 Zadzwoń do parku*/odzyskaj
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	T	T	10	*6.1.23 Zadzwoń do parku*/odzyskaj
%ENABLE_RTP_ICE_WXT%	T	T	false	*6.1.18 Obsługa ICE (tylko Webex Calling)*
%RTP_ICE_MODE_WXT%	T	T	ogłuszenie lodem	*6.1.18 Obsługa ICE (tylko Webex Calling)*
%RTP_ICE_SERVICE_URI_WXT%	T	T	puste	*6.1.18 Obsługa ICE (tylko Webex Calling)*
%RTP_ICE_PORT_WXT%	T	T	3478	*6.1.18 Obsługa ICE (tylko Webex Calling)*
%ENABLE_RTP_ICE_IPV6_WXT%	T	T	false	*6.1.18 Obsługa ICE (tylko Webex Calling)*
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	T	N	false	*6.1.8.4 Zarządzanie TTL DNS*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	T	N	false	*6.2.4 Eskaluj połączenia SIP do spotkania*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	T	N	false	*6.2.5 Połączenia Desk Phone Control — automatyczne odbieranie*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_DIALING_VOIP_WXT%	N	T	true	*6.3.5 Obsługa MNO Zadzwoń za pomocą natywnego dialera*
%ENABLE_DIALING_NATIVE_WXT%	N	T	false	*6.3.5 Obsługa MNO Zadzwoń za pomocą natywnego dialera*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	T	T	true	*6.1.35 Wybieranie SIP-URI*
%ENABLE_SIP_VIDEOCALLS_WXT%	T	T	true	*6.1.37 Wyłącz połączenia wideo*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	T	T	true	*6.1.37 Wyłącz połączenia wideo*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	T	T	Pulpit - prawda Mobilny, Tablet - fałsz	*6.1.37 Wyłącz połączenia wideo*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	T	T	false	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji u dostawcy usługi E911*
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	T	T	0	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji u dostawcy usługi E911*
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	T	T	-1	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji u dostawcy usługi E911*
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	T	T	raz_na_logowanie	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji u dostawcy usługi E911*
%ENABLE_AUTO_ANSWER_WXT%	T	N	false	*6.2.6 Automatyczne odbieranie z powiadomieniem tonalnym*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	T	T	false	*6.1.41 Wskazanie połączeń spamowych*
%ENABLE_NOISE_REMOVAL_WXT%	T	T	false	*6.1.42 Usuwanie szumów i rozszerzenie przepustowości dla połączeń PSTN/komórkowych*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_AUDIO_MARI_FEC_WXT%	T	T	false	*6.1.46.2 Korekcja błędów przekierowywania (FEC) i retransmisji pakietów (RTX)*
%ENABLE_AUDIO_MARI_RTX_WXT%	T	T	false	*6.1.46.2 Korekcja błędów przekierowywania (FEC) i retransmisji pakietów (RTX)*
%ENABLE_VIDEO_MARI_FEC_WXT%	T	T	false	*6.1.46.2 Korekcja błędów przekierowywania (FEC) i retransmisji pakietów (RTX)*
%ENABLE_VIDEO_MARI_RTX_WXT%	T	T	false	*6.1.46.2 Korekcja błędów przekierowywania (FEC) i retransmisji pakietów (RTX)*
%ENABLE_CALL_BLOCK_WXT%	T	T	false	*6.1.45 Lista zablokowanych (tylko Webex Calling)*
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	T	true	*6.3.5.6 Mobilność MNO — widget w trakcie połączenia*
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	T	true	*6.3.5.6 Mobilność MNO — widget w trakcie połączenia*
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	T	true	*6.3.5.6 Mobilność MNO — widget w trakcie połączenia*
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	T	T	false	*6.1.47 Połączenia równoczesne z tym samym użytkownikiem*
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	T	N	false	*6.2.11 Pakiet zdarzeń zdalnego sterowania wyciszeniem (tylko Webex Calling)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	T	T	true	*6.1.29.2 Przekierowywanie połączeń do poczty głosowej*
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	T	T	true	*6.1.8.1 Przełączenie awaryjne SIP*
%ENABLE_CALL_MOVE_HERE_WXT%	T	N	false	*6.2.12 Przenieś połączenie*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	T	T	false	*6.1.42 Usuwanie szumów i rozszerzenie przepustowości dla połączeń PSTN/komórkowych*

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	T	puste	*6.3.5.1 Zadzwoń za pomocą natywnego dialera*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	T	T	false	*6.1.20 Przekaż*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	T	T	true	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	T	false	*6.3.6 Identyfikator dzwoniącego w połączeniu przychodzącym*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	T	false	*6.3.6 Identyfikator dzwoniącego w połączeniu przychodzącym*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	T	false	*6.1.50 ID dzwoniącego* *Identyfikator dzwoniącego w połączeniach wychodzących*
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	T	false	*6.1.50 ID dzwoniącego* *Identyfikator dzwoniącego w połączeniach wychodzących*
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	T	false	*6.1.50 ID dzwoniącego* *Identyfikator dzwoniącego w połączeniach wychodzących*
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	T	false	*6.1.50 ID dzwoniącego* *Identyfikator dzwoniącego w połączeniach wychodzących*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	T	false	*6.1.50 ID dzwoniącego* *Identyfikator dzwoniącego w połączeniach wychodzących*
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	T	T	false	*6.1.49 Informacje o przekierowywaniu połączeń*
%ENABLE_BUSY_LAMP_FIELD_WXT%	T	N	false	*6.2.8.1 Pole sygnalizacji aktywności* linii
%ENABLE_BLF_DISPLAY_CALLER_WXT%	T	N	true	*6.2.8.1 Pole sygnalizacji aktywności* linii

Informacje poufne firmy Cisco

Znacznik	Używany na pulpicie	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%BLF_NOTIFICATION_DELAY_TIME_WXT%	T	N	0	*6.2.8.1 Pole sygnalizacji aktywności* linii
%ENABLE_GCP_NOTIFICATIONS_WXT%	T	N	false	*6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	T	N	false	*6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	T	N	120	*6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)*
%UDP_KEEPALIVE_ENABLED_WXT%	T	T	true	*6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP*
%TCP_KEEPALIVE_ENABLED_WXT%	T	T	false	*6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP*
%TLS_KEEPALIVE_ENABLED_WXT%	T	T	false	*6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP*
%ENABLE_MULTI_LINE_WXT%	T	T	false	*6.1.51 Wielowierszowe*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	T	false	*6.2.4 Eskalacja połączeń SIP do spotkania (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	T	false	*6.3.5.3 Tożsamość linii połączeń wychodzących (CLID) — podwójna* tożsamość
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	T	false	*6.3.5.36.3.5.3 Tożsamość linii wywołującej wychodzącej (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	T	T	rozwiązane	*6.1.50.2 Nazwa zdalnego identyfikatora dzwoniącego*
%PERSONAL_ASSISTANT_ENABLED_WXT%	T	T	false	*6.1.53 Asystent osobisty (obecność poza biurem)**Error! Reference source not found.***
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	T	n/s	***Error! Reference source not found.*** *Tryb dostarczania (tylko Webex Calling)*
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	T	T	false	*6.1.52 **Error! Reference source not found.**.*

Informacje poufne firmy Cisco

Aby uzyskać więcej informacji na temat mapowania znaczników niestandardowych używanych w Webex dla Cisco BroadWorks do tych używanych przez UC-One, zobacz sekcję *8 Mapowanie znaczników niestandardowych między Webex dla Cisco BroadWorks i UC-One*.

Informacje poufne firmy Cisco

6.1 Cechy wspólne

6.1.1 Ustawienia serwera SIP

Klient jest powszechnie skonfigurowany do korzystania z sieci SIP, co odbywa się poprzez modyfikowanie pliku *config-wxt.xml* . Zazwyczaj należy zmienić następujące parametry:

- Domena SIP. Jest on używany jako część domeny własnego URI SIP (własny URI SIP jest czasami nazywany portem liniowym) ogólnie w nagłówkach SIP i w połączeniach zdalnych (XSI). Część użytkownika własnego identyfikatora URI SIP pochodzi z konfiguracji poświadczeń SIP (parametr w sekcji).
- Adres URI serwera SIP lub adres IP serwera proxy SIP w przypadku niepowodzenia rozwiązywania nazw DNS. Należy pamiętać, że aby użyć protokołu TLS, adresy IP nie mogą być używane w parametrach proxy, ponieważ weryfikacja certyfikatu TLS zakończy się niepowodzeniem. Aby uzyskać więcej informacji na temat portu proxy, zobacz znacznik DM %SOURCE_PORT_WXT%. Należy pamiętać, że funkcja zarządzania DNS TTL nie może być używana, jeśli w parametrze adresu proxy używany jest adres IP. Z tych powodów generalnie nie zaleca się używania adresu IP w tym polu.

Można również zmienić inne parametry, aby włączyć różne funkcje połączeń. Jednakże poprzednie ustawienia umożliwiają podstawową funkcjonalność dla następujących elementów:

- Rejestracja w sieci SIP.
- Wykonywanie połączeń audio i wideo.
- Wykonywanie wykrywania serwerów proxy opartego na DNS, co pozwala na korzystanie z wielu serwerów proxy.

Po włączeniu rejestracji SIP włączenie usługi SIP SUBSCRIBE dla MWI musi zostać wykonane za pomocą oddzielnych parametrów konfiguracyjnych. Aby uzyskać więcej informacji na temat poczty głosowej, zobacz sekcję *6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej*.

Należy pamiętać, że podstawowa konfiguracja protokołu SIP jest zawsze wymagana dla usługi MWI, nawet gdy połączenia SIP są wyłączone. MWI opiera się na SIP NOTIFY.

Konfiguracja serwerów SIP przebiega według następującego podstawowego schematu:

- Adres proxy zawiera identyfikator URI serwera SIP.
- Można zdefiniować tylko jeden serwer proxy.
- Funkcja wykrywania serwerów proxy DNS obsługuje wiele serwerów proxy, które wymagają prawidłowej konfiguracji DNS.

Ponadto timery SIP są dostępne w pliku konfiguracyjnym (nie zaleca się ich modyfikowania).

```
<config>
<protocols>
<sip>
    <timers>
        <T1>500</T1>
        <T2>4000</T2>
        <T4>5000</T4>
   </timers>
```


Informacje poufne firmy Cisco

- T1 – czas opóźnienia w ruchu powrotnym w sieci (w milisekundach).
- T2 – maksymalny czas w milisekundach przed ponownym przesłaniem żądań niezaproszeń i odpowiedzi z zaproszeniami.
- T4 – maksymalny czas, w milisekundach, w jakim wiadomość pozostaje w sieci.

Każdy wiersz ma własne parametry, takie jak numer poczty głosowej, adres URI konferencji i domena, a także dane uwierzytelniania SIP. W razie potrzeby można skonfigurować oddzielne dane uwierzytelniające dla sygnalizacji 401 i 407.

Poniższy przykład i tabela zawierają informacje na temat najczęściej używanych tagów DM w konfiguracji SIP.

```
<config>
<protocols><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
       <line>
              <label>%BWAPPEARANCE-LABEL-1%</label>
              <name>%BWNAME-1%</name>
              <phone-number>%BWE164-1%</phone-number>
              <extension>%BWEXTENSION-1%</extension>
              <external-id>%BWUSEREXTID-1%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-1%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
1%</conference-service-uri>
              <domain>%BWHOST-1%</domain>
              <credentials>
                     <username>%BWLINEPORT-1%</username>
                     <password>%BWAUTHPASSWORD-1%</password>
                     <auth>
                            <auth401>
                                   <default>
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </default>
                                   <realm id="%BWHOST-1%">
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </realm>
                            </auth401>
                            <auth407>
                                   <default>
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </default>
                                   <realm id="%BWHOST-1%">
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </realm>
                            </auth407>
                     </auth>
              </credentials>
       </line>
       …
</lines>
<proxy address="%SBC_ADDRESS_WXT%" port="%SBC_PORT_WXT%" />
<preferred-port>%SOURCE_PORT_WXT%</preferred-port>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%BWLINEPORT-n%	puste	struna	Zazwyczaj nazwa użytkownika SIP. Aby uzyskać więcej informacji, patrz punkt *5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks*. Przykład: Jan Nowak
%BWAUTHPASSWORD-n%	puste	struna	Zwykle hasło SIP. Aby uzyskać więcej informacji, patrz punkt *5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks*. Przykład: tajnehasło
%BWE164-n%	puste	numer telefonu	Domyślny numer telefonu użytkownika w formacie międzynarodowym. Aby uzyskać więcej informacji, patrz punkt *5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks*. Przykład: 12345678
%SBC_ADDRESS_WXT%	puste	struna	Aby uzyskać więcej informacji, patrz punkt *5.6 Domyślne znaczniki systemowe*. Przykład: sbcexample.domain.com
%SBC_PORT_WXT%	5060	liczba	Aby uzyskać więcej informacji, patrz punkt*5.6 Domyślne znaczniki systemowe*. Przykład: 5060
%BWHOST-n%	puste	struna	Zwykle używany jako domena SIP. Aby uzyskać więcej informacji, patrz punkt *5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks*. Przykład: exampledomain.com
%SOURCE_PORT_WXT%	5060	liczba	Zwykle używany dla parametru *preferred-port* . Aby uzyskać więcej informacji, zobacz sekcję *6.1.7 Preferowane użycie portu dla SIP*. Przykład: 5061
%BWUSEREXTID-n%	puste	struna	(tylko Webex Calling) Przechowuje zewnętrzny identyfikator linii Aby uzyskać więcej informacji, sprawdź *6.1.51 Wielowierszowe*. Przykład: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

UWAGA: Zdecydowanie zaleca się, aby port SIP był inny niż 5060 (na przykład 5075) ze względu na znane problemy z używaniem standardowego portu SIP (5060) z urządzeniami mobilnymi.

Informacje poufne firmy Cisco

6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie rzeczywistym

Klienta można skonfigurować tak, aby korzystał z sygnalizacji SIP przez TLS i protokołu SRTP (Secure Real-time Transport Protocol) do szyfrowania multimediów. Funkcje te muszą jednak zostać włączone w konfiguracji, jak pokazano w poniższym przykładzie. Należy również pamiętać, że jeśli używane jest dynamiczne wykrywanie proxy SIP, priorytety DNS SRV zastępują parametry statyczne, takie jak ten (%USE_TLS_WXT%), a transport inny niż TLS jest używany, jeśli ma wyższy priorytet w usłudze DNS SRV. Aby uzyskać więcej informacji na temat dynamicznego wykrywania serwerów proxy SIP, zobacz sekcję *6.1.6 Wykrywanie dynamicznego serwera proxy SIP.*

Jeśli dynamiczne wykrywanie serwerów proxy nie jest używane, włączenie protokołu TLS dla protokołu SIP powoduje jego użycie.

Aby uzyskać szczegółowe informacje na temat zaleceń dotyczących portów SIP i protokołów transportowych, gdy w sieci są używane SIP ALG, zobacz *Webex dla Cisco BroadWorks Solution Guide*.

Należy pamiętać, że użyty certyfikat musi być ważny. Ponadto łańcuch certyfikatów musi być nienaruszony, aby certyfikat pośredni także był powiązany. Zaleca się zastosowanie powszechnie używanego certyfikatu, który jest domyślnie zainstalowany na urządzeniach. Możliwe jest również dodawanie certyfikatów lokalnie na komputerze stacjonarnym, ręcznie lub za pomocą zbiorczego provisionowania, choć zazwyczaj nie jest to praktykowane.

Aby włączyć protokół SRTP do szyfrowania multimediów, należy wykonać osobne ustawienie.

Oprócz protokołu RTP ruch RTCP można zabezpieczyć przy użyciu tych samych mechanizmów co RTP, stosując powyższą konfigurację.

Informacje na temat szyfrów SIP/TLS znajdują się w *Załącznik A: Szyfry TLS.*

Protokół SRTP służy do zapewnienia bezpieczeństwa strumienia multimedialnego w trzech różnych aspektach:

- Poufność (dane są szyfrowane)
- Uwierzytelnianie (zapewnienie tożsamości drugiej strony lub stron)
- Integralność (środki zapobiegające na przykład atakom typu replay)

Aktualna wersja infrastruktury multimedialnej obsługuje tryb licznika AES 128 w celu zapewnienia ochrony oraz kod uwierzytelniania HMAC-SHA-1 (Hash Message Authentication Code). Rozmiar klucza głównego wynosi 16 bajtów, a rozmiar klucza głównego — 14 bajtów.

Infrastruktura multimedialna obsługuje zarówno pełne (80-bitowe), jak i krótkie (32-bitowe) znaczniki uwierzytelniania. Klient wymienia klucze wewnątrz protokołu SDP w ramach sygnalizacji SIP, obie strony połączenia wysyłają drugiej stronie używany przez siebie klucz.

Protokół SRTP można włączyć, korzystając z konfiguracji pokazanej w poniższym przykładzie. Obecna implementacja wykorzystuje wyłącznie bezpieczny profil RTP SDP i obsługuje wieloliniowy protokół SDP dla wpisów profilu audiowizualnego (AVP) i bezpiecznego profilu audiowizualnego (SAVP). Implementację protokołu SRTP przetestowano pomyślnie w standardowej konfiguracji wdrożeniowej z różnymi kontrolerami SBC. Testowanie interoperacyjności (IoT) z punktami końcowymi obsługującymi szyfrowanie wyłącznie przy użyciu profilu AVP nie jest obsługiwane.

Informacje poufne firmy Cisco

Wdrożono procedury SDP wieloliniowe związane z SRTP, dzięki czemu zawsze używa się wielu m-linii. Dla AVP i SAVP stosuje się oddzielne linie m.

Należy jednak pamiętać, że należy poświęcić szczególną uwagę konfiguracji SBC, a w szczególności upewnić się, że linia przychodząca „m=" powiązana z RTP/SAVP w SDP nie zostanie usunięta, ponieważ w niektórych przypadkach połączenia SRTP mogą zostać zablokowane.

Możliwych jest jednak kilka różnych konfiguracji sieciowych. W niektórych wdrożeniach kontroler SBC nie bierze udziału w ruchu multimedialnym, podczas gdy w innych wdrożeniach każdy odcinek transmisji danych RTP klienta w kierunku kontrolera SBC jest oddzielnie szyfrowany i negocjowany za pośrednictwem kontrolera SBC. W niektórych wdrożeniach SBC nie obsługuje wielu linii SDP.

SBC może również modyfikować kolejność linii m SDP podczas zestawiania połączenia, ustawiając linię m AVP (nieszyfrowaną) lub SAVP (szyfrowaną) jako pierwszą. W związku z tym klienci wybierający pierwszą działającą linię m muszą wybierać między ruchem szyfrowanym a nieszyfrowanym. Różne opcje konfiguracji SRTP są następujące:

- Obowiązkowe – podczas nawiązywania połączenia początkowy protokół SDP obejmuje tylko linię m SAVP podczas oferowania, a klient akceptuje tylko linię m SAVP w protokole SDP podczas odbierania połączenia, dlatego możliwe są tylko połączenia SRTP.
- Preferowane – podczas nawiązywania połączenia początkowy SDP obejmuje zarówno linie m AVP, jak i SAVP, ale SAVP jest oferowany jako pierwszy, co wskazuje kolejność preferencji. Podczas odbierania połączenia klient wybiera opcję SAVP, jeśli jest dostępna, nawet jeśli nie jest to pierwsza linia m (zgodnie ze specyfikacją SIP kolejność linii m nie ulega zmianie podczas odbierania połączenia).
- Opcjonalnie — podczas konfiguracji połączenia początkowy protokół SDP obejmuje zarówno linie m-SAVP, jak i AVP, ale AVP najpierw wskazuje kolejność preferencji. Odbierając połączenie, klient wybiera pierwszą linię m, AVP lub SAVP.
- SRTP nie jest włączone – podczas oferowania w początkowym SDP nie ma linii m SAVP. Podczas odbierania połączeń SAVP nie jest akceptowane, dlatego możliwe są jedynie połączenia RTP.
- Transport – Automatyczny wybór trybu SRTP na podstawie protokołu transportowego. Jeżeli używany jest protokół TLS, włączony jest obowiązkowy tryb SRTP. Jeżeli używany jest protokół TCP lub UDP, protokół SRTP nie jest wykorzystywany.

Protokół SRTP i RTP jest symetryczny w obu kierunkach połączenia, co oznacza, że profile wysyłania i odbierania są takie same.

```
<config>
<protocols><sip>
<secure>%USE_TLS_WXT%</secure>
```

```
<config>
<protocols><rtp>
<secure enabled="%SRTP_ENABLED_WXT%" mode="%SRTP_MODE_WXT%" rekey-
always="%ENABLE_REKEYING_WXT%"/>
```


Informacje poufne firmy Cisco

Protokół Secure Real-Time Control Protocol (SRTCP) jest również używany, jeżeli włączony jest SRTP.

W niektórych wdrożeniach ponowne wprowadzanie kluczy SRTP nie jest obsługiwane. W związku z tym istnieje parametr konfiguracyjny umożliwiający włączenie/wyłączenie ponownego wprowadzania danych SRTP. Jednakże nowe klucze są zawsze brane pod uwagę po otrzymaniu ich w zaktualizowanym SDP zgodnie z rfc3264. Konfigurowalność dotyczy wyłącznie wysyłania nowych kluczy.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%USE_TLS_WXT%	false	prawda, fałsz	Gdy ustawione jest na „fałsz”, protokół SIP TLS jest wyłączony. W przypadku ustawienia wartości „true” protokół SIP TLS jest aktywowany. Należy pamiętać, że jeśli używany jest parametr *6.1.6 Wykrywanie dynamicznego serwera proxy* SIP , ten parametr jest ignorowany.
%SRTP_ENABLED_WXT%	false	prawda, fałsz	W przypadku ustawienia wartości „false” protokół SRTP jest dezaktywowany. Po ustawieniu wartości „true” protokół SRTP jest aktywowany.
%SRTP_MODE_WXT%	opcjonalne	obowiązkowy, preferowany, opcjonalny, transport	Definiuje, jak preferowany jest protokół SRTP podczas nawiązywania połączenia. Wartością domyślną jest „opcjonalny”.
%ENABLE_REKEYING_WXT%	true	prawda, fałsz	Włącza ponowne kodowanie SIP (SDP) dla SRTP.

UWAGA: Jeśli obsługa ICE jest włączona (patrz *6.1.18 Obsługa ICE (tylko* Webex Calling)), zawsze będzie przeprowadzane ponowne wprowadzenie (%ENABLE_REKEYING_WXT% wartość z konfiguracji jest ignorowana).

6.1.3 Nagłówki SIP 3GPP dla SRTP

Nowsze specyfikacje 3GPP wymagają dodatkowych nagłówków SIP, aby można było korzystać z protokołu SRTP (Secure Real-time Transport Protocol). Aby uzyskać więcej informacji, zapoznaj się z dokumentem *3GPP TS 24.229* , a także z poniższymi informacjami:

https://tools.ietf.org/html/draft-dawes-dispatch-mediasec-parameter-07

Nagłówki wymagane przez tę specyfikację mogą zakłócić działanie wywołań SIP w przypadku wdrożeń, w których specyfikacja ta nie jest stosowana. W związku z tym zaleca się korzystanie z tych nagłówków jedynie w środowiskach, w których są one obsługiwane po stronie serwera.

Informacje poufne firmy Cisco

Można konfigurować jedynie włączenie używania nagłówków. Nie ma możliwości dalszej konfiguracji poszczególnych nagłówków. Wszystkie nagłówki są albo włączone albo wyłączone.

```
<config>
<protocols><sip>
<use-mediasec enabled="%USE_MEDIASEC_WXT%"/>
```

Poniższy tag kontroluje tę możliwość.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%USE_MEDIASEC_WXT%	false	prawda, fałsz	Włącza nagłówki SIP 3GPP dla negocjacji SRTP.

6.1.4 Wymuś użycie i utrzymanie protokołów TCP, TLS lub UDP

W kliencie Webex for Cisco BroadWorks można skonfigurować używanie protokołu TCP, TLS lub UDP zarówno do sygnalizacji SIP, jak i RTP. Należy pamiętać, że domyślnym protokołem klienta jest TCP. Należy również pamiętać, że bez funkcji TCP keepalive połączenia SIP TCP są zamykane po pewnym okresie bezczynności.

Poniższy przykład ilustruje ten węzeł konfiguracji.

```
<config>
<protocols><sip>
<transports>
   <tcp-size-threshold>%TCP_SIZE_THRESHOLD_WXT%</tcp-size-threshold>
```

Poniższy tag kontroluje, czy klient używa protokołu TCP czy UDP.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości (w bajtach)	Opis
%TCP_SIZE_THRESHOLD_WXT%	0	0	Wymusza użycie protokołu TCP. Decyzja o tym, czy klient będzie korzystał z protokołu TCP czy UDP, należy do dostawcy usługi; zaleca się jednak używanie protokołu TCP z wartością domyślną „0”.
	0	1 - 99,000	Wymusza użycie protokołu UDP, jeżeli rozmiar wiadomości jest mniejszy od wartości określonej tutaj. Domyślnie używany jest protokół TCP, jeśli rozmiar wiadomości jest większy od ustawionej wartości. Aby używać protokołu UDP, zaleca się domyślnie ustawienie 1500.
	0	100000	Wymusza użycie protokołu UDP.

Ten sam węzeł konfiguracji ma również parametry keepalive dla UDP, TCP i TLS, przedstawione w poniższym przykładzie.

```
<config>
```


Informacje poufne firmy Cisco

```
<protocols><sip>
<transports>
        …
        <udp>
                <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
                        <timeout>20</timeout>
                        <payload>crlf</payload>
                </keepalive>
        </udp>
        <tcp>
                <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
                        <timeout>0</timeout>
                        <payload></payload>
                </keepalive>
        </tcp>
        <tls>
                <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
                        <timeout>0</timeout>
                        <payload></payload>
                </keepalive>
        </tls>
</transports>
```

Możliwe parametry to:

- Włączanie utrzymywania aktywności protokołu TCP lub TLS, możliwe wartości: prawda/fałsz, wartością domyślną jest „fałsz”, jeśli węzeł jest brakujący. Należy pamiętać, że gdy ta funkcja jest włączona, pakiety keepalive protokołu TCP są wysyłane nawet wtedy, gdy do protokołu SIP używany jest transport UDP.
- Włączanie utrzymywania aktywności UDP, możliwe wartości — prawda/fałsz, wartość domyślna to „prawda”, jeśli brakuje węzła. Należy pamiętać, że po włączeniu tej funkcji utrzymywanie aktywności UDP jest wysyłane nawet wtedy, gdy dla protokołu SIP jest używany transport TCP. Ponadto, nawet jeśli do SIP używany jest protokół TCP, klient akceptuje również ruch przez UDP zgodnie z *RFC 3261*.
- Limit czasu określa maksymalny czas braku aktywności w sekundach, po którym zostanie wysłana wiadomość keepalive. Brak wartości oznacza, że funkcja keepalive jest wyłączona dla protokołu.
- Ładunek dla wiadomości keepalive, możliwe wartości (brak wartości oznacza, że keepalive jest wyłączone dla protokołu):
  - Crlf
  - Null (nie należy używać)
  - Ciąg niestandardowy (**nie należy używać**)

Keepalives można wykorzystać do celów przechodzenia NAT, aby utrzymać powiązania NAT otwarte, przy niewielkim zwiększeniu ruchu.

Informacje poufne firmy Cisco

Adres IP i port serwera dla funkcji keepalive są ustalane przy użyciu standardowych procedur wykrywania serwera proxy SIP. Należy pamiętać, że porty SIP i wybór protokołu transportowego uzyskany za pośrednictwem dynamicznego wykrywania serwerów proxy SIP zastępują jakąkolwiek statyczną konfigurację portu lub transportu. Aby uzyskać więcej informacji na temat dynamicznego wykrywania serwerów proxy, zobacz *6.1.6 Wykrywanie dynamicznego serwera proxy SIP.*

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%UDP_KEEPALIVE_ENABLED_WXT%	true	prawda, fałsz	Określa, czy pakiety keep-alive powinny być wysyłane dla transportu UDP.
%TCP_KEEPALIVE_ENABLED_WXT%	false	prawda, fałsz	Kontroluje, czy pakiety utrzymywania aktywności mają być wysyłane dla transportu TCP.
%TLS_KEEPALIVE_ENABLED_WXT%	false	prawda, fałsz	Kontroluje, czy pakiety utrzymywania aktywności mają być wysyłane dla transportu TLS.

6.1.5 Konfigurowalny limit czasu otwierania gniazda SIP

Wcześniej limit czasu otwarcia gniazda SIP był na stałe ustawiony na 5 sekund dla protokołu TCP i 10 sekund dla protokołu TLS. Limity czasu można teraz konfigurować.

```
<config>
    <protocols>
        <sip>
            <transports>
                <udp>
                    …
                </udp>
                <tcp>
                    …
                    <connect-
timeout>%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </tcp>
                <tls>
                    <connect-
timeout>%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </tcp>
            </transports>
```

Poniższe tagi kontrolują limit czasu połączenia gniazda (w milisekundach).

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	- limit czasu w milisekundach	Limit czasu połączenia gniazda, gdy używany jest transport TCP.

Informacje poufne firmy Cisco

%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	- limit czasu w milisekundach	Upłynął limit czasu połączenia gniazda, gdy jest używany transport TLS.

6.1.6 Wykrywanie dynamicznego serwera proxy SIP

Aby włączyć funkcję dynamicznego wykrywania serwerów proxy SIP, zapoznaj się z poniższym przykładem.

```
<config>
<protocols><sip>
<proxy-discovery enabled="%USE_PROXY_DISCOVERY_WXT%” tcp=”%USE_TCP_FROM_DNS_WXT%"
udp="%USE_UDP_FROM_DNS_WXT%" tls="%USE_TLS_FROM_DNS_WXT%">
    <record-name>%SBC_ADDRESS_WXT%</record-name>
     <domain-override>%DOMAIN_OVERRIDE_WXT%</domain-override>
</proxy-discovery>
```

Możliwe jest kontrolowanie, które wpisy protokołów transportowych z DNS SRV będą używane, gdy dostępnych jest ich wiele, zgodnie z procedurami opisanymi w tej sekcji.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%USE_PROXY_DISCOVERY_WXT%	false	prawda, fałsz	Umożliwia dynamiczne wykrywanie serwerów proxy SIP dla połączeń audio i wideo. Zalecana wartość to „prawda”.
%SBC_ADDRESS_WXT%	puste	Struna	Ten znacznik Cisco BroadWorks jest zazwyczaj używany jako parametr nazwy rekordu. Powinien to być prawidłowy adres URL – nie adres IP. Aby uzyskać więcej informacji, patrz punkt *5.6 Domyślne znaczniki systemowe*. Przykład: sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	puste	Struna	Ten niestandardowy znacznik jest używany do zastąpienia domeny. Aby uzyskać więcej informacji, patrz poniższa sekcja. Przykład: other.domain.com
%USE_TCP_FROM_DNS_WXT%	true	prawda, fałsz	Jeżeli wartość tego parametru wynosi „fałsz”, wówczas wyniki DNS SRV dla tego protokołu transportowego (TCP) są odrzucane. Jeśli „prawda”, wówczas używane są wyniki z DNS SRV dla tego protokołu transportowego (TCP). W zależności od priorytetów SRV, może zostać wybrany inny transport.
%USE_UDP_FROM_DNS_WXT%	true	prawda, fałsz	Jeśli wartość tego parametru ma wartość „false”, wyniki DNS SRV dla tego protokołu transportowego (UDP) zostaną odrzucone. Jeśli wartość „true” (prawda), wówczas są używane wyniki z DNS SRV dla tego protokołu transportowego (UDP). W zależności od priorytetów SRV, może zostać wybrany inny transport.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%USE_TLS_FROM_DNS_WXT%	true	prawda, fałsz	Jeśli wartość tego parametru jest „fałsz”, wyniki DNS SRV dla tego protokołu transportowego (TLS) zostaną odrzucone. Jeśli wartość „true” (prawda), wówczas są używane wyniki z DNS dla tego protokołu transportowego (TLS). W zależności od priorytetów SRV, może zostać wybrany inny transport.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	prawda, fałsz	true	Włącza/wyłącza usługę kopii zapasowej DNS. Jeżeli opcja jest włączona, dla adresu proxy SIP wykonywane jest rozpoznawanie A/AAAA. Jest ona brana pod uwagę tylko wtedy, gdy włączone jest wykrywanie usług SRV/NAPTR.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	prawda, fałsz	true	Jeśli ustawiono na „true” i wyszukiwanie usługi NAPTR nie powiedzie się lub nie zwróci żadnych wyników, wówczas dla skonfigurowanego hosta zostanie przeprowadzone wyszukiwanie usługi SRV. Jeżeli ustawione na „fałsz”, wówczas nie zostanie przeprowadzone żadne wykrywanie SRV.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	prawda, fałsz	false	Pozwala na ominięcie pamięci podręcznej DNS systemu operacyjnego.

Usługa DNS umożliwia klientowi uzyskanie adresu IP, portu i protokołu transportowego dla serwera proxy SIP zgodnie z normą RFC 3263.

Obsługiwane są zapytania DNS SRV, Naming Authority Pointer (NAPTR) i A-record. Podczas logowania należy wykonać 3-etapowy proces, który wygląda następująco:

1. Wykonaj zapytanie NAPTR przy użyciu powyższego pola , aby uzyskać identyfikatory URI serwera z protokołami transportowymi, jeśli istnieją. Wartość parametru powinna być pełna domena do rozpoznania przez serwer DNS, ale nie może być adresem IP.
2. Rozwiąż elementy znalezione w zapytaniu NAPTR przy użyciu zapytania SRV w celu uzyskania końcowego identyfikatora URI i portu serwera. Część domeny używana w zapytaniu SRV jest pobierana z wyniku zapytania NAPTR w celu znalezienia końcowego identyfikatora URI serwera (i portu). Port otrzymany z zapytania DNS SRV jest używany, gdy wpisy DNS SRV są dostępne. Należy pamiętać, że port, tylko z pliku konfiguracyjnego, dotyczy statycznego serwera proxy w pliku konfiguracyjnym, a nie adresów URI rozwiązanych przy użyciu SRV. Zobacz poniższe przykłady użycia różnych nazw rekordów.

Informacje poufne firmy Cisco

Jeśli nie znaleziono rekordu NAPTR, klient próbuje wykonać zapytanie SRV o nazwie rekordu pobranej z parametru , chyba że istnieje parametr , w którym to przypadku jest używany i automatycznie próbuje znaleźć oddzielne wpisy dla protokołów TCP, UDP i TLS (_sip_protocol [UDP, TCP lub TLS]). Należy pamiętać, że protokół SCTP (Stream Control Transmission Protocol) nie jest obsługiwany. Jeśli zapytania SRV nie przyniosą żadnych wyników, wykrywanie serwera proxy kończy się niepowodzeniem, a użytkownikowi końcowemu wyświetlany jest błąd informujący, że połączenia nie są dostępne. W tym przypadku nie ma rejestracji SIP. Jednak nawet jeśli wszystkie zapytania SRV kończą się niepowodzeniem lub jeśli odebrane serwery nie działają, klient nadal sprawdza, czy skonfigurowany statyczny serwer proxy działa, tylko z zapytaniami A do identyfikatora URI określonego w polu , aby sprawdzić, czy otrzymano adres IP, który zapewnia działającą rejestrację SIP. Port i transport w tym ostatnim przypadku pochodzą z parametrów tcp-threshold i .

3. Rozwiąż znalezione identyfikatory URI przy użyciu zapytania A-record. Otrzymane ostateczne adresy IP są sprawdzane w kolejności ich otrzymania, aby uzyskać działające połączenie z serwerem proxy SIP. Kolejność ta może zostać określona przez dostawcę usługi w systemie DNS. Wybierany jest pierwszy identyfikator URI serwera proxy SIP, dla którego wyszukiwanie rekordu A zakończyło się powodzeniem, i jest on używany do momentu, aż przestanie działać lub klient się wyloguje. Na etapie zapytania A używany jest tylko jeden adres IP na raz, nawet jeśli otrzymano ich wiele. Jednakże wszystkie wpisy SRV zostają rozwiązane do momentu wylogowania lub utraty połączenia z siecią.

Ważne uwagi

UWAGA 1: Jeśli odkrycie serwera proxy DNS skutkuje wyborem protokołu transportowego w kroku SRV poprzez otrzymanie działającego identyfikatora URI serwera proxy SIP dla protokołu transportowego, zastępuje on parametr *tcp-threshold* , który zwykle jest używany do wybierania protokołu UDP lub TCP w pliku konfiguracyjnym. To samo dotyczy konfiguracji SIP/TLS. W zależności od priorytetu w DNS używany jest protokół TCP lub UDP.

UWAGA 2: Elementy otrzymane za pośrednictwem protokołu SRV mają priorytet nad statycznym serwerem proxy w pliku konfiguracyjnym. Kolejność NAPTR nie jest brana pod uwagę, liczy się tylko priorytet SRV. Gdy SRV wygeneruje kilka przedmiotów o tym samym protokole transportu, priorytecie i wadze, każdy z otrzymanych przedmiotów zostanie wybrany losowo. W tej wersji nie są obsługiwane wagi NAPTR, ale wagi SRV są obsługiwane. Najpierw brany jest pod uwagę priorytet SRV, a w przypadku elementów o równym priorytecie, brany jest pod uwagę ciężar, aby określić prawdopodobieństwo, że dany serwer zostanie wypróbowany jako następny.

UWAGA 3: Opcjonalny *parametr domain-override* umożliwia rozpoznanie nazwy rekordu A innej niż ta podana w parametrze konfiguracji domeny SIP za pomocą SRV, gdy pominięto wyniki NAPTR. Zobacz poniższe przykłady użycia parametru *domain-override* .

UWAGA 4: Klient wykorzystuje podstawowe funkcje systemu operacyjnego do operacji DNS, a odpowiedzi DNS są zazwyczaj buforowane w celu przestrzegania czasu życia odpowiedzi DNS.

UWAGA 5: Typ DNS (usługa) dla rekordów NAPTR musi być zgodny z procedurami *RFC 3263*, w przeciwnym razie rozpoznawanie nazw DNS może się nie powieść. Na przykład, wymagane jest użycie SIPS+D2T w przypadku SIP przez TLS.

UWAGA 6: Klient obsługuje tylko niektóre prefiksy dla usług NAPTR. Poniżej znajduje się lista obsługiwanych prefiksów:

SIP+D2U -> _sip._udp

Informacje poufne firmy Cisco

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

Jeśli odpowiedź NAPTR zawiera rekord z prefiksem, który nie pasuje do typu usługi, to rekord ten jest ignorowany.

Przykład 1: Korzystanie z wykrywania serwera proxy DNS bez parametru konfiguracji nadpisywania domeny

Poniżej przedstawiono przykład konfiguracji wykorzystującej wykrywanie serwerów proxy SIP, gdy używany jest tylko protokół SIP przez TCP, a zapytanie NAPTR w kroku 1 zwraca wyniki.

```
<config>
<protocols><sip>
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true" >
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domain>sip-domain.com</domain>
```

Powoduje to wykonanie następujących kroków na poziomie protokołu.

```
1. zapytanie NAPTR dla record-domain.com, odpowiedź:
record-domain.com.
28591 W NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.
2. Zapytanie SRV dla _sip._tcp.test.sip.record-domain.com (otrzymane w zapytaniu
NAPTR), odpowiedź
_sip._tcp.test.sip.record-domain.com. 28635 W REKORDZIE SRV
10 10 5061 test.sipgeo.record-domain.com.
3. Zapytanie typu A-record dla test.sipgeo.record-domain.com, odpowiedź:
test.sipgeo.record-domain.com. 16 W Wersji 1.2.3.4
```

W rezultacie rejestracja SIP odbywa się poprzez protokół TCP z wykorzystaniem portu 5061 (otrzymanego w kroku SRV) i w kierunku adresu IP 1.2.3.4.

Przykład 2: **Używanie parametru domain-override w pliku konfiguracyjnym**

Poniżej przedstawiono drugi przykład konfiguracji wykorzystującej wykrywanie serwera proxy SIP, w której domena SIP różni się od domeny serwera proxy i używany jest tylko protokół SIP przez UDP, a zapytanie NAPTR nie zwraca wyników.

```
<config>
<protocols><sip
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true">
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domain>sip-domain.com</domain>
```

Powoduje to wykonanie następujących czynności na poziomie protokołu.

```
1. Zapytanie NAPTR dla record-domain.com, brak odpowiedzi.
```


Informacje poufne firmy Cisco

```
2. Zapytanie SRV dla _sip._tcp.override-domain.com (z pliku konfiguracyjnego),
odpowiedź
_sip._tcp.override-domain.com. 28635 W REKORDZIE SRV
10 10 5061 test.override-domain.com.
3. Zapytanie rekordu A dla test.override-domain.com, odpowiedź:
test.sipgeooverride-domain.com. 16 W Wersji 4.3.2.1
```

W rezultacie rejestracja SIP odbywa się przez protokół UDP z użyciem portu 5061 (odbieranego w kroku SRV) i w kierunku adresu IP 4.3.2.1.

Przykład 3: **Korzystanie z priorytetów SRV**

Poniżej przedstawiono kolejny przykład konfiguracji wykorzystującej wykrywanie proxy protokołu SIP, w przypadku gdy używany jest tylko protokół SIP przez TCP, a zapytanie NAPTR w kroku 1 zwraca wyniki, ale odebrano kilka rekordów NAPTR i SRV o różnych priorytetach. W tym przypadku w tym zdarzeniu wydania liczy się tylko priorytet SRV, chociaż otrzymano również kilka rekordów NAPTR o różnych priorytetach.

```
<config>
<protocols><sip>
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true">
   <record-name>record-domain.com</record-name>
    <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domain>sip-domain.com</domain>
```

Powoduje to wykonanie następujących czynności na poziomie protokołu.

```
1. zapytanie NAPTR dla record-domain.com, odpowiedź:
record-domain.com.
28591 W NAPTR 100 10 "S" "SIPS+D2T" "" _sip._tcp.test.sip.record-domain.com.
28591 W NAPTR 120 10 "S" "SIPS+D2U" "" _sip._udp.test.sip.record-domain.com.

2. Zapytanie SRV dla _sip._tcp.test.sip.record-domain.com (otrzymane w zapytaniu
NAPTR), odpowiedź
_sip._tcp.test.sip.record-domain.com. 28635 W REKORDZIE SRV
10 10 5061 test.sipgeo.record-domain.com.

Zapytanie SRV dla _sip._udp.test.sip.record-domain.com (otrzymane w zapytaniu
NAPTR), odpowiedź
_sip._udp.test.sip.record-domain.com. 28635 W REKORDZIE SRV
20 10 5062 test.sipgeo.record-domain.com.

3. Zapytanie typu A-record dla test.sipgeo.record-domain.com, odpowiedź:
test.sipgeo.record-domain.com. 16 W Wersji 1.2.3.4
```

W rezultacie rejestracja SIP odbywa się przez protokół TCP z użyciem portu 5061 (odbieranego w kroku SRV) i w kierunku adresu IP 1.2.3.4, który obsługuje protokoły UDP i TCP.

Przykład 4: Korzystanie z wykrywania serwerów proxy DNS z NAPTR, gdy usługa nie jest zgodna z typem usługi

Poniższy przykład konfiguracji wykorzystującej wykrywanie proxy protokołu SIP, gdy jest używany protokół SIP przez TCP i TLS, a zapytanie NAPTR w kroku 1 zwraca wyniki.

```
<config>
```


Informacje poufne firmy Cisco

```
<protocols><sip>
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true" tcp="true" udp="false" tls="true">
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domain>sip-domain.com</domain>
```

Powoduje to wykonanie następujących kroków na poziomie protokołu.

```
1. zapytanie NAPTR dla record-domain.com, odpowiedź:
record-domain.com.
28591 W NAPTR 100 10 "S" "SIPS+D2T" "" _sip._tls.test.sip.record-domain.com.
28591 W NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.

2. Dla pierwszego rekordu mamy typ usługi „SIPS+D2T”, a prefiks to „sip._tls.”.
Ponieważ ten prefiks nie odpowiada typie usługi (zob. uwaga 6 powyżej), będzie
ignorowany.

3. Zapytanie SRV dla _sip._tcp.test.sip.record-domain.com (otrzymane w zapytaniu
NAPTR), odpowiedź
_sip._tcp.test.sip.record-domain.com. 28635 W REKORDZIE SRV
10 10 5061 test.sipgeo.record-domain.com.

3. Zapytanie typu A-record dla test.sipgeo.record-domain.com, odpowiedź:
test.sipgeo.record-domain.com. 16 W Wersji 1.2.3.4
```

W rezultacie rejestracja SIP odbywa się poprzez protokół TCP z wykorzystaniem portu 5061 (otrzymanego w kroku SRV) i w kierunku adresu IP 1.2.3.4.

6.1.7 Preferowane użycie portu dla SIP

Zdarzały się przypadki, że na tym samym komputerze co klient działał inny pakiet oprogramowania, zajmując domyślny port SIP. Aby skonfigurować klienta do używania innego portu dla protokołu SIP, można użyć parametru *preferred-port*. Klient próbuje użyć skonfigurowanej wartości portu określonej w parametrze *preferred-port*, ale jeśli jest ona zajęta, klient stopniowo próbuje używać wartości portów powyżej skonfigurowanej wartości. Na przykład, jeśli wartość *preferred-port* wynosi „6000” i ten port jest zajęty, klient próbuje 6001, 6002, 6003 itd., aż znajdzie wolny port. Gdy zostanie znaleziony nieużywany port, jest on wykorzystywany do własnej komunikacji SIP.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SOURCE_PORT_WXT%	5060	liczba	Określa preferowany lokalny port SIP do komunikacji. Przykład: 5060

6.1.8 Przełączanie awaryjne i powrót do pracy po awarii SIP

Przełączenie awaryjne i failback w protokole SIP są zgodne z procedurami Cisco BroadWorks. W tym celu należy skonfigurować więcej niż jeden serwer proxy (zazwyczaj SBC).

Po stronie klienta serwer proxy powinien być rozpoznawany jako wiele adresów IP. Można to osiągnąć poprzez:

Informacje poufne firmy Cisco

- Włączono funkcję SIP Proxy Discovery, a serwer DNS ma rekordy NAPTR i/lub SRV dla nazwy FQDN SBC (patrz sekcja *6.1.6 Wykrywanie dynamicznego serwera proxy SIP*), LUB
- Adres serwera proxy SIP jest podawany w postaci nazwy FQDN i jest rozwiązywany na wiele adresów IP (patrz sekcja *6.1.1 Ustawienia serwera SIP*).

Pamięć podręczna DNS systemu operacyjnego służy do unikania zbędnego ruchu DNS. Nie ma zakodowanego na stałe limitu maksymalnej liczby adresów IP na liście.

Jeśli podczas logowania zostanie rozwiązanych wiele adresów IP, zostaną one uporządkowane według priorytetu. Klient zaczyna używać pierwszego dostępnego adresu IP.

6.1.8.1 Przełączenie awaryjne SIP

Przełączenie awaryjne SIP może zostać wywołane przez błąd gniazda, błąd przekroczenia limitu czasu żądania lub ostateczną odpowiedź błędu z serwera w następujący sposób:

- Błąd gniazda – jeśli gniazdo pomiędzy klientem a serwerem ulegnie uszkodzeniu lub zostanie zamknięte, jak np. w przypadku utraty połączenia sieciowego, klient natychmiast zareaguje i uruchomi przełączenie awaryjne.
- Limit czasu (na przykład, gdy SBC się zawiesza) – na podstawie SIP T1:
  - SIP INVITE – jeśli żądanie INVITE przekroczy limit czasu, klient rejestruje się na kolejnym dostępnym kontrolerze SBC (adresie IP) i ponawia próbę wysłania żądania INVITE.
  - Kolejne żądanie SIP – klient próbuje zarejestrować się na kolejnym dostępnym kontrolerze SBC (adresie IP).
- Otrzymano ostateczną odpowiedź o błędzie z serwera:
  - Następujące błędy SIP wysyłane przez serwer do SIP REGISTER powodują przełączenie awaryjne:
    - 5xx
    - 6xx
  - Następujące odpowiedzi SIP *4xx* na SIP REGISTER <u>nie</u> powodują przełączenia awaryjnego:
    - 401 Brak uprawnień
    - 403 Zakazane
    - 404 Nie znaleziono
    - 407 Wymagane uwierzytelnienie proxy
    - 423 Zbyt krótki odstęp czasu
  - Co więcej, odpowiedzi na błędy *4xx* w odpowiedzi na SIP INVITE nie powodują przełączenia awaryjnego, natomiast *5xx* i *6xx* już tak.

Informacje poufne firmy Cisco

Gdy nastąpi przełączenie awaryjne, klient wybiera kolejny dostępny adres IP z listy. Timer SIP T1 określa, jak długo serwer proxy na liście jest wypróbowywany przed przejściem do następnego. Zazwyczaj używana jest wartość 32 sekund (64*T1). Jeżeli wszystkie adresy IP nie powiodą się, klient wyświetli błąd interfejsu użytkownika dla łączności SIP. Jeżeli w momencie wystąpienia przełączenia awaryjnego trwa połączenie VoIP, zostanie ono zakończone.

Logika przełączania awaryjnego SIP opiera się na kilku parametrach konfiguracyjnych:

- Timery SIP Failover – timery SIP T1, T2 i T4 są widoczne w pliku konfiguracyjnym, ale nie zaleca się ich modyfikowania.

```
<config><protocols><sip>
<timers>
    <T1>500</T1>
    <T2>4000</T2>
    <T4>5000</T4>
</timers>
```

  - T1 – czas opóźnienia w ruchu powrotnym w sieci (w milisekundach).
  - T2 – maksymalny czas w milisekundach przed ponownym przesłaniem żądań niezaproszeń i odpowiedzi z zaproszeniami.
  - T4 – maksymalny czas, w milisekundach, w jakim wiadomość pozostaje w sieci.
- Adres proxy SIP i wykrywanie proxy SIP
  - Zobacz sekcję *6.1.1 Ustawienia serwera SIP*.
  - Patrz sekcja *6.1.6 Wykrywanie dynamicznego serwera proxy SIP*.
- Zarejestruj konfigurację failover (patrz poniżej)

W przypadku przełączenia awaryjnego aplikacja Webex wysyła SIP REGISTER z dwoma nagłówkami Contact — jednym dla starej sesji i drugim z informacjami o nowym urządzeniu. Nagłówek kontaktu dla starej sesji jest dołączony w celu powiadomienia kontrolera SBC o konieczności wyczyszczenia danych. Nagłówek ten zawiera expires=0 i q=0.5.

Nagłówek Contact z nowymi informacjami o urządzeniu ma również wartość q, która jest odczytywana ze znacznika . Znacznik służy do wskazywania preferencji lub priorytetu określonego adresu kontaktu. Skala waha się od 0 do 1,0, gdzie 1,0 oznacza najwyższą preferencję, a 0 najniższą. Ten tag nie posiada niestandardowego tagu kontrolującego jego wartość — jest on na stałe zakodowany na 1.0. Wartość tę można dostosować ręcznie, jeśli kontroler SBC użyty we wdrożeniu ma odwrotną logikę i traktuje q=0,0 jako maksymalny priorytet.

Począwszy od wersji 42.11, w szablonie konfiguracji wprowadzona jest nowa sekcja . Dodano nowy konfigurowalny parametr do sprawdzania, czy aplikacja wyśle nagłówek Contact w celu wyczyszczenia informacji o starym urządzeniu. Niektóre kontrolery SBC czyszczą starą sesję natychmiast po rozłączeniu gniazda, więc nagłówek Contact dla starej sesji nie jest potrzebny. Domyślnie logika czyszczenia rejestracji jest włączona.

Dla zachowania spójności znacznik jest również przenoszony w tej samej sekcji .

Przykład:

Informacje poufne firmy Cisco

```
<config>
<protocols><sip>
   <q-value>1.0</q-value> <!-- DEPRECATED -->
   <register-failover>
      <registration-
cleanup>%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%</registration-cleanup>
      <q-value>1.0</q-value>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	true	prawda, fałsz	Kontroluje czyszczenie starych informacji o urządzeniu w przypadku awarii protokołu SIP.

6.1.8.2 Powrót SIP

Jeśli klient jest połączony z serwerem proxy, który nie ma priorytetu pierwszego, próbuje nawiązać połączenie z adresem IP o najwyższym priorytecie. Czas powrotu po awarii zależy od konfiguracji zarządzania wartością TTL usługi DNS (patrz sekcja *6.1.8.4 Zarządzanie TTL DNS*). Jeśli w momencie osiągnięcia limitu czasu powrotu po awarii trwa połączenie, klient czeka, aż wszystkie połączenia zostaną zakończone i uruchamia procedurę powrotu po awarii. Należy pamiętać, że dotyczy to tylko klientów stacjonarnych, ponieważ połączenie SIP jest aktywne wyłącznie podczas rozmowy na urządzeniu mobilnym.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SIP_FAILBACK_ENABLED_WXT%	true	prawda, fałsz	Włącza/wyłącza funkcję powrotu po awarii protokołu SIP.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Ponad 60	Limit czasu powrotu protokołu SIP w sekundach.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	prawda, fałsz	Dodaje losowy okres [0-10]% powrotu do stanu początkowego SIP.

6.1.8.3 Wymuś wersję IP

Klient Webex można skonfigurować, jak uporządkować listę rozwiązanych hostów za pośrednictwem DNS, a następnie wykonywać ich iterację w przypadku przełączenia awaryjnego SIP. We wszystkich trybach priorytet i waga są respektowane.

Obsługiwane konfiguracje to:

- dns - używa wszystkich adresów zwróconych przez zapytania DNS
- ipv4 — odfiltrowuje adresy IPv6
- ipv6 — odfiltrowuje adresy IPv4
- prefer-ipv4 — zamawia adresy IPv4 przed IPv6 (wersja 42.9)
- prefer-ipv6 — zamawia adresy IPv6 przed IPv4 (wersja 42.9)

Informacje poufne firmy Cisco

- nat64 – ignoruje adresy IPv6, zamawia adresy IPv4 (wersja 44.2)

Zaleca się używanie wartości domyślnej (dns), chyba że konfiguracja środowiska/sieci wymaga innego trybu.

W konfiguracji „dns” adresy IPv4 są traktowane priorytetowo względem adresów IPv6 dla danego hosta. Jeśli istnieją dwa hosty z adresami IPv4 i IPv6, kolejność będzie: IPv4 (host1), IPv6 (host1), IPv4 (host2), IPv6 (host2).

W trybie „preferowany adres IPv4” adresy IPv4 są zamawiane przed adresami IPv6 (kolejność w grupach IPv4 i IPv6 pozostaje)

Przykład: IPv4 (host1), IPv4 (host2), IPv6 (host1), IPv6 (host2).

W trybie „prefer-ipv6” kolejność jest odwrotna - adresy IPv6 są umieszczane przed adresami IPv4

Przykład: IPv6 (host1), IPv6 (host2), IPv4 (host1), IPv4 (host2).

W trybie „nat64” — adresy IPv6 są ignorowane — akceptowane jest kolejność adresów IPv4. Wykryto prefiks IPv6. Dla każdego adresu IPv4 tworzona jest kombinacja z każdym prefiksem i/lub sufiksem Pref64.

Przykład: Pref64(1)::IPv4(host1), Pref64(2)::IPv4(host1)::Suff64(2), IPv4(host1)::Suff64(3), Pref64(1)::IPv4(host2), Pref64(2)::IPv4(host2)::Suff64(2), IPv4(host2)::Suff64(3).

```
<config>
<protocols><sip><transports>
<enforce-ip-version>%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%</enforce-ip-version>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	dns	ipv4 ipv6 dns preferuj-ipv4 preferuj-ipv6 nat64	Kontroluje kolejność adresów IPv4/IPv6 używanych przez klienta Webex do połączenia sesji SIP.

6.1.8.4 Zarządzanie TTL DNS

Dodano osobny parametr konfiguracji służący do zarządzania sposobem ponownego rozwiązywania nazw DNS po wygaśnięciu czasu życia rekordu DNS aktualnie używanego serwera. Parametr w poniższej tabeli, gdy jest włączony, zmusza klienta do ponownego wykonania operacji DNS po wygaśnięciu czasu życia rekordu DNS SRV lub rekordu A aktualnie używanego serwera.

Informacje poufne firmy Cisco

Po ponownym wykonaniu rozwiązania DNS ten parametr wymusza również na kliencie ponowne połączenie się z serwerem o najwyższym priorytecie, jeśli jest on inny niż serwer aktualnie używany, nawet w przypadku, gdy bieżące połączenie działa w pełni. Ponowne połączenie zostanie jednak nawiązane dopiero po zakończeniu trwających połączeń.

Jeżeli wartości TTL dla serwerów A i rekordów SRV są różne, wybierana jest mniejsza wartość.

Gdy ten parametr jest wyłączony, operacje DNS nie są ponawiane po upływie czasu TTL, lecz co 15 minut.

Ten parametr działa tylko dla protokołu SIP.

Należy pamiętać, że funkcja zarządzania DNS TTL nie może być używana, jeśli w parametrze adresu proxy używany jest adres IP.

> **UWAGA**: Jest to funkcja dostępna wyłącznie na komputerach stacjonarnych, gdyż użytkownicy urządzeń mobilnych korzystają z połączenia SIP tylko podczas połączeń.

```
<config>
<protocols><sip>
<refresh-on-ttl enabled="%SIP_REFRESH_ON_TTL_WXT%"
  use-random-factor="%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SIP_REFRESH_ON_TTL_WXT%	false	fałsz, prawda	Gdy ustawione na „fałsz”, zarządzanie DNS TTL jest wyłączone dla protokołu SIP. Jeśli jest ustawiona wartość „true”, zarządzanie TTL DNS jest włączone dla SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	false	fałsz, prawda	Jeśli włączone, dodaje losowy okres pomiędzy 0-10% do DNS TTL.

> **UWAGA**: Zdecydowanie zaleca się włączenie losowego współczynnika TTL DNS w celu zapobiegania wzrostom liczby żądań kierowanych do serwera DNS i potencjalnym wzrostom liczby prób ponownego połączenia z serwerem aplikacji.

6.1.9 SIP SUBSKRYBUJ I ZAREJESTRUJ SIĘ Odśwież i SUBSKRYBUJ Spróbuj ponownie

Komunikator obsługuje konfigurację interwałów odświeżania dla funkcji SIP SUBSCRIBE i REGISTER. W przypadku SIP SUBSCRIBE istnieje osobny parametr określający interwał odświeżania (w sekundach) oraz czas oczekiwania klienta przed ponowieniem próby SIP SUBSCRIBE w przypadku wystąpienia błędów (w sekundach). Zalecana maksymalna wartość parametru *subscription-retry-interval* wynosi 2000000 sekund, natomiast każda wartość ujemna, 0 lub pusta spowoduje użycie wartości 1800 sekund. Każda ujemna wartość w polu Odświeżanie subskrypcji pomija nagłówek *Expires* i w ten sposób tworzy jednorazowy SUBSCRIBE.

Informacje poufne firmy Cisco

Proponowany przez klienta licznik odświeżania rejestru SIP można skonfigurować w ciągu sekund, ale zgodnie ze specyfikacjami SIP, serwer może nadpisać tę wartość. Obecnie klient zapamiętuje wartość proponowaną przez serwer przy kolejnych odświeżeniach, zamiast zawsze używać skonfigurowanej wartości.

Na koniec można również skonfigurować wartość wygasającą dla sesji SIP (dla SIP INVITE i SUBSCRIBE) (w sekundach).

```
<config>
<protocols><sip>
<subscription-refresh-interval>10800</subscription-refresh-interval>
<subscription-retry-interval>60</subscription-retry-interval>
<registration-refresh-interval>300</registration-refresh-interval>
<session>
       <expires-value>3600</expires-value>
</session>
```

6.1.10 Użyj identyfikatorów URI P-Associated-URI w REGISTER

Następujący parametr jest używany podczas rejestrowania i obsługi powiązanej odpowiedzi *200 OK* .

Jeżeli parametr zostanie ustawiony na „false”, klient nie użyje *P-Associated-URI* i zamiast tego użyje tożsamości ze swojego własnego SIP URI.

```
<config>
<protocols><sip>
<use-alternative-identities>%USE_ALTERNATIVE_IDENTITIES_WXT%</use-alternative-
identities>
```

Jeżeli parametr jest ustawiony na „true”, wówczas klient pobiera własną tożsamość z ostatniego nagłówka
P-Associated-URI dla wszystkich wychodzących żądań SIP (INVITE, SUBSCRIBE, CANCEL, INFO i REFER) z odpowiedzi *200 OK* w REGISTER. Ponadto te adresy URI nie są wyświetlane jako kontakty na liście kontaktów.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	prawda, fałsz	Umożliwia korzystanie z alternatywnych tożsamości w SIP REGISTER. Jeżeli ustawione na „prawda”, klient pobiera swoją tożsamość z ostatniego nagłówka *P-Associated-URI* dla wychodzących żądań SIP. Jeśli ustawione na „fałsz”, wówczas tożsamość użytkownika dla wychodzących żądań SIP jest pobierana z jego własnego identyfikatora URI SIP.

Informacje poufne firmy Cisco

6.1.11 Nagłówek SIP P-Early Media (PEM)

Nagłówek SIP *P-Early Media* (PEM) można wykorzystać na przykład w środowiskach IMS wewnątrz domeny zaufania, aby umożliwić sieci autoryzację wielu dialogów wczesnych mediów SIP, na przykład w przypadkach, gdy inna sieć zezwala na wszystkie wczesne media.

Parametr konfiguracyjny umożliwia reklamowanie obsługi PEM w sygnalizacji SIP. Rzeczywista wczesna logika obsługi nośników jest taka sama w przypadku zarówno plików PEM, jak i nie-PEM i opiera się na obsługiwanych wartościach nagłówka PEM.

```
<config>
<protocols><sip>
<support-p-early-media>%ENABLE_PEM_SUPPORT_WXT%</support-p-early-media>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_PEM_SUPPORT_WXT%	false	prawda, fałsz	Ustaw na „true”, aby włączyć obsługę PEM reklamowanego przez klienta w sygnalizacji SIP. Ustaw wartość „false” (fałsz), aby wyłączyć obsługę reklam PEM klienta w sygnalizacji w protokole SIP.

6.1.12 Obsługa AKTUALIZACJI SIP

Na przykład w niektórych wdrożeniach IMS potrzebna jest funkcja SIP UPDATE zamiast alternatywnej funkcji re-INVITE. Umożliwia klientowi aktualizację parametrów sesji, takich jak zestaw strumieni multimedialnych i ich kodeki, ale nie ma wpływu na stan dialogu SIP.

Typowe przypadki użycia dotyczą wczesnych mediów, gdzie na przykład stosuje się jednocześnie sygnał wywołania i sygnał ostrzegawczy.

Usługa SIP UPDATE jest obecnie obsługiwana tylko w przypadkach użycia przed dialogiem (wczesne media), a nie w trakcie aktywnego dialogu, na przykład w przypadku wstrzymania/wznowienia połączenia, gdy nadal używane jest polecenie re-INVITE.

W tej wersji nie jest możliwe dodawanie obrazu do dźwięku za pomocą SIP UPDATE (zmiana nośnika). Ponadto klient nie obsługuje pełnego przepływu długich połączeń IMS z rezerwacją zasobów.

```
<config>
<protocols><sip>
<support-update enabled="%ENABLE_SIP_UPDATE_SUPPORT_WXT%"/>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	prawda, fałsz	Gdy ustawione jest na „fałsz”, obsługa aktualizacji SIP jest wyłączona. W przypadku ustawienia wartości „true” obsługa aktualizacji SIP jest włączona.

6.1.13 Poprzedni wpis FIR INFORMACJI SIP

Ten klient obsługuje starszy sposób żądania klatek kluczowych wideo za pośrednictwem żądania sterowania multimediami SIP INFO. Jest to konieczne, gdyż niektóre urządzenia mają problemy z odpowiedzią na protokół RTCP-FB FIR, a czasami protokół RTCP nie dociera do zdalnego punktu końcowego, co może prowadzić do braku obrazu lub do transmisji jednokierunkowej. Aby uzyskać więcej informacji, patrz dokument *RFC 5168*.

```
<config>
<protocols><sip>
<force-sip-info-fir enabled="%ENABLE_FORCE_SIP_INFO_FIR_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false	prawda, fałsz	W przypadku ustawienia wartości „false” obsługa FIR INFO protokołu SIP jest wyłączona. Jeśli jest ustawiona wartość „true”, obsługa FIR INFO protokołu SIP jest włączona.

6.1.14 Zarządzanie portem SIP na potrzeby przesyłania NAT

Klienta można skonfigurować tak, aby używał mechanizmu SIP rport do przeglądania NAT. Należy pamiętać, że zazwyczaj nie może to być jedyne rozwiązanie w przypadku przechodzenia NAT; w tym celu używa się głównie protokołu SBC. Opis specyfikacji rport można znaleźć w dokumencie *RFC 3581*.

Aby uzyskać więcej informacji na temat zaleceń dotyczących portów SIP i protokołów transportowych, gdy w sieci są używane bramy SIP Application Layer Gateways (ALG), zobacz *Webex dla Cisco BroadWorks Solution Guide*.

Należy pamiętać, że ciąg „rport” jest zawsze obecny w wychodzących żądaniach SIP, niezależnie od konfiguracji. Parametr ten ma wpływ wyłącznie na wykorzystanie adresu IP i portu otrzymanych od serwera w nagłówkach SIP „received” i „rport”. Po włączeniu tej funkcji wartości z nagłówków „received” i „rport” są używane w nagłówku SIP Contact żądań SIP (nawet jeśli nagłówek „received” nie występuje w odpowiedzi REGISTER).

Parametr *Preferred-port* jest powiązany, ponieważ definiuje port używany w nagłówku SIP Contact. Aby uzyskać więcej informacji na temat przydzielania portów SIP, zobacz *6.1.7 Preferowane użycie portu dla SIP*.

Informacje poufne firmy Cisco

Istnieje oddzielny parametr konfiguracji *use-local-port* , który wymusza ustawienie lokalnego portu gniazda klienta w nagłówku *Contact* . Jest to używane w przypadku niektórych kontrolerów SBC, które wykrywają, że klient ma prawdziwy adres IP (na podstawie nagłówka *Contact*), a kontroler SBC próbuje nawiązać oddzielne gniazdo dla klienta w celu obsługi jego żądań. W większości przypadków zapora sieciowa znajduje się pomiędzy kontrolerem SBC a klientem i blokuje połączenia przychodzące do klienta.

> **UWAGA**: W środowiskach protokołu IPv6 wszystkie adresy są prawdziwe, a serwer SBC próbuje nawiązać połączenie z adresem klienta nasłuchującego (z nagłówka *Contact*).

```
<config>
<protocols><sip>
<use-rport enabled="%ENABLE_USE_RPORT_WXT%" use-local-
port="%RPORT_USE_LOCAL_PORT_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_USE_RPORT_WXT%	false	prawda, fałsz	Włącza raportowanie połączeń audio i wideo.
%RPORT_USE_LOCAL_PORT_WXT%	false	prawda, fałsz	Określa, czy lokalny port gniazda klienta ma zostać dodany do nagłówka SIP *Contact* .

6.1.15 Identyfikator sesji SIP

Po włączeniu tej opcji, podczas pierwszej rejestracji generowany jest lokalny identyfikator sesji. Identyfikator sesji jest używany przez cały czas trwania połączenia/sesji dla danego urządzenia, dla wszystkich dialogów poza połączeniem, REJESTRACJI, SUBSKRYPCJI, POWIADOMIENIA itd. Do momentu utraty powiązania używany jest ten sam identyfikator sesji. W przypadku utraty powiązania rejestracyjnego (wyszukiwanie DNS, resetowanie połączenia, resetowanie telefonu itd.) generowany jest nowy lokalny identyfikator sesji.

Wartość identyfikatora sesji można wykorzystać do znalezienia pełnego zestawu okien dialogowych powiązanych z danym urządzeniem.

```
<config>
<protocols><sip>
<sip-sessionid enabled="%ENABLE_SIP_SESSION_ID_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SIP_SESSION_ID_WXT%	false	prawda, fałsz	Kontroluje wykorzystanie identyfikatora sesji SIP.

Informacje poufne firmy Cisco

6.1.16 Działanie odrzucania połączeń przychodzących

Klient oferuje możliwość odrzucania połączeń za pomocą *486* lub *603*.

Należy pamiętać, że jeśli klient jest skonfigurowany do odrzucania połączeń za pomocą *603 Odrzuć*, wówczas usługi Przekierowywanie połączeń w przypadku zajętości i Przekierowywanie połączeń w przypadku braku odpowiedzi mogą nie działać zgodnie z oczekiwaniami.

```
<config>
<services><calls>
<reject-with-486 enabled="%ENABLE_REJECT_WITH_486_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_REJECT_WITH_486_WXT%	true	prawda, fałsz	Kontroluje kod błędu SIP i powód odrzucania przychodzących połączeń SIP. Jeśli włączone, używane jest ustawienie *486 Tymczasowo niedostępny* . W przeciwnym wypadku używany jest *603 Decline* .

6.1.17 Zakres portów protokołu transportu w czasie rzeczywistym

Klienta można skonfigurować tak, aby używał określonego zakresu portów dla strumieni protokołu RTP (Real-Time Transport Protocol), co dotyczy również protokołu SRTP. Konfigurację tę wykonuje się poprzez ustawienie wartości granicznych zakresu portów dla strumieni audio i wideo za pomocą tagów pokazanych w poniższym przykładzie.

```
<config>
<protocols><rtp>
<preferred-audio-port-start>%RTP_AUDIO_PORT_RANGE_START_WXT%</preferred-audio-port-
start>
<preferred-audio-port-end>%RTP_AUDIO_PORT_RANGE_END_WXT%</preferred-audio-port-end>
<preferred-video-port-start>%RTP_VIDEO_PORT_RANGE_START_WXT%</preferred-video-port-
start>
<preferred-video-port-end>%RTP_VIDEO_PORT_RANGE_END_WXT%</preferred-video-port-end>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	liczba	Początek zakresu portu audio.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	liczba	Koniec zakresu portów audio.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	liczba	Początek zakresu portów wideo.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	liczba	Koniec zakresu portów wideo.

Informacje poufne firmy Cisco

UWAGA: Zakresy portów należy ustawić tak, aby nigdy się nie nakładały.

6.1.18 Obsługa ICE (tylko Webex Calling)

Klient obsługuje negocjacje w protokole ICE (Interactive Connectivity Establishment), co umożliwia optymalizację ścieżki multimedialnej między punktami końcowymi (w trybie peer-to-peer). Ma to na celu skrócenie opóźnień w przesyłaniu danych, ograniczenie utraty pakietów i obniżenie kosztów operacyjnych wdrażania aplikacji.

Należy pamiętać, że obecna implementacja obsługuje serwer STUN, natomiast TURN nie jest obsługiwany.

Gdy włączona jest obsługa ICE, ponowne wprowadzanie klucza dla protokołu SRTP będzie zawsze wykonywane (patrz sekcja *6.1.2 SIP przez TLS i bezpieczny protokół transportu w czasie* rzeczywistym).

Począwszy od wersji 44.5 aplikacja Webex dodaje obsługę funkcji ICE przez IPv6 przy użyciu NAT64.

```
<config>
<protocols><rtp>
   <ice enabled="%ENABLE_RTP_ICE_WXT%"
        enable-ipv6-support="%ENABLE_RTP_ICE_IPV6_WXT%"
        mode="%RTP_ICE_MODE_WXT%"
        service-uri="%RTP_ICE_SERVICE_URI_WXT%"
        port="%RTP_ICE_PORT_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_RTP_ICE_WXT%	false	prawda, fałsz	Włącz / wyłącz obsługę ICE.
%RTP_ICE_MODE_WXT%	ogłuszenie lodem	ogłuszenie lodem	Tryb obsługi ICE. Obecnie jedyną obsługiwaną wartością jest „icestun”.
%RTP_ICE_SERVICE_URI_WXT%	(puste)	prawidłowy URI serwera STUN lub (pusty)	Adres URI serwera STUN.
%RTP_ICE_PORT_WXT%	3478	Numer (0-65535)	port serwera STUN.
%ENABLE_RTP_ICE_IPV6_WXT%	false	prawda, fałsz	Włącza obsługę funkcji ICE przez protokół IPv6.

6.1.19 MUX RTCP

RTCP MUX jest konfigurowalny. Funkcja ta powoduje, że klient używa tego samego portu dla protokołów RTP i RTCP. Na poziomie sygnalizacji SIP/SDP linia a=rtcp-mux jest dodawana do SDP. Ponadto możliwe są różne tryby:

Informacje poufne firmy Cisco

- Tryb zgodności wstecznej (czyli linia a=rtcp-mux nie pojawia się w SDP)
- Tryb multipleksowania (linia a=rtcp-mux pojawi się dwukrotnie w SDP): raz w sekcji m=audio i drugi raz w sekcji m=video)

Obraz i dźwięk nie korzystają z tego samego portu.

```
<config>
<protocols><rtp>
<mux enabled="%ENABLE_RTCP_MUX_WXT%"/>
```

Należy pamiętać, że RTCP MUX nie może być używany z połączeniami SRTP.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_RTCP_MUX_WXT%	true	prawda, fałsz	Aby włączyć RTPC MUX, ustaw na „true”. Aby wyłączyć RTCP MUX, ustaw na „false”.

6.1.20 Przekaż

Klient Webex for Cisco BroadWorks obsługuje przekazywanie połączeń nadzorowane (konsultacyjne), półkonsultacyjne i Bezpośrednie (ślepe).

Półkonsultacyjne przekierowanie połączenia pozwala dzwoniącemu na dokończenie przekierowania zanim połączenie zostanie odebrane przez zdalnego odbiorcę. Przycisk półkonsultacyjnego ukończenia połączenia staje się dostępny dla osoby dzwoniącej dopiero po rozpoczęciu dzwonienia po stronie odbiorcy i otrzymaniu przez osobę dzwoniącą odpowiedniego powiadomienia SIP (*180 Ringing*). Funkcja transferu w ciemno w interfejsie użytkownika nosi nazwę „Transfer Now”.

> **UWAGA**: Dzwonek *180 SIP* może nie być wyzwalany w niektórych środowiskach, w niektórych numerach ani w niektórych scenariuszach komunikacji między serwerami.

Wersja 43.9 aplikacji Webex wprowadza przekazywanie do innego autonomicznego trwającego połączenia tego samego typu. Połączenia zakończone w aplikacji Webex mogą być przekazywane do innych połączeń zakończonych w lokalnym punkcie końcowym. Połączenia zakończone na urządzeniu zdalnym mogą zostać przekierowane do połączeń zakończonych na zdalnym punkcie końcowym. Ta funkcja nie posiada opcji konfiguracyjnych.

Począwszy od wersji 43.12 aplikacja Webex dodaje opcję konfiguracji, która pozwala kontrolować, czy bieżące połączenie powinno zostać automatycznie wstrzymane po wybraniu elementu menu Przekaż. To zachowanie jest kontrolowane przez nowy atrybut *auto-hold* . Domyślnie funkcja automatycznego wstrzymania jest wyłączona.

```
<config>
<services><calls>
   <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"
                  xsi-enabled="%ENABLE_XSI_TRANSFER_CALLS_WXT%"
                  type="%TRANSFER_CALL_TYPE_WXT%"
                  auto-hold="%ENABLE_TRANSFER_AUTO_HOLD_WXT%"/>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_TRANSFER_CALLS_WXT%	false	prawda, fałsz	Po ustawieniu na „prawda” przekazywanie połączeń jest włączone. Ustawienie wartości „false” (fałsz) powoduje, że przekazywanie połączeń jest wyłączone.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false	prawda, fałsz	Włącza opcje transferu dla połączeń zdalnych (XSI) zakończonych w innej lokalizacji.
%TRANSFER_CALL_TYPE_WXT%	pełne	najpierw rozmowa, ślepy, pełny	Określa typy transferu dostępne dla użytkownika w konfiguracji BroadWorks.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	prawda, fałsz	Określa, czy aktywne połączenie ma zostać automatycznie wstrzymane, gdy użytkownik wybierze opcję Przekaż z menu ekranowego podczas połączenia.

6.1.21 Połączenia konferencyjne n-Way i uczestnicy

Poniższy niestandardowy znacznik może być używany do kontrolowania dostępności połączenia konferencyjnego Ad Hoc (N-Way) przez SIP w kliencie Webex for Cisco BroadWorks. Ponadto właściciel sieci N-way może zobaczyć pełną listę uczestników za pośrednictwem SIP SUBSCRIBE/NOTIFY i pakietu wydarzeń konferencyjnych. Klient właściciela dowiaduje się, do którego URI ma zostać wysłany komunikat SIP SUBSCRIBE, za pośrednictwem poprzedzającego nagłówka SIP *Contact* wiadomości *200 OK* wysłanej w odpowiedzi na INVITE do URI konferencji, podczas gdy dla uczestników te same informacje znajdują się w poprzedzającym komunikacie NOTIFY dotyczącym informacji o połączeniu.

Ustawienie systemu Cisco BroadWorks (*maxConferenceParties)* służy do ustawiania maksymalnej liczby uczestników konferencji. Dla danego połączenia wskazuje liczbę aktywnych jednoczesnych stron, które użytkownik może mieć lub dodać za pomocą opcji sterowania „Dodaj uczestników” w trakcie połączenia lub funkcji połączeń Cisco BroadWorks N-way.

Informacje te pobierane są z serwera aplikacji (AS) przy użyciu następującego polecenia interfejsu wiersza poleceń (CLI).

```
AS_CLI/SubscriberMgmt/Policy/CallProcessing/Conferencing> uzyskaj

Przykład danych wyjściowych:
maxConferenceParties = 6
conferenceURI =
```

Po uzyskaniu wartości *maxConferenceParties* (która ma zakres od 4 do 15) należy odpowiednio ustawić znacznik %MAX_CONF_PARTIES_WXT%.

```
<config>
<services><calls>
<conference enabled=”%ENABLE_CONFERENCE_CALLS_WXT%”>
   <service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-1%</service-uri>
```


Informacje poufne firmy Cisco

```
    <subscribe-conference-info enabled="%ENABLE_NWAY_PARTICIPANT_LIST_WXT%"/>
        <max-nway-participants>%MAX_CONF_PARTIES_WXT%</max-nway-participants>
</conference>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CONFERENCE_CALLS_WXT%	false	prawda, fałsz	Określa, czy opcja Konferencja powinna być włączona dla użytkownika.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	false	prawda, fałsz	Ustaw na „true", aby włączyć listę właścicieli-uczestników N-way. Ustaw wartość „false" (fałsz), aby wyłączyć listę uczestników właściciela w obie strony.
%MAX_CONF_PARTIES_WXT%	10	Liczba pomiędzy 4 a 15 (puste)	Określa maksymalną liczbę uczestników N-way, wymuszoną przez klienta, na przykład 10. Po stronie serwera obowiązują pewne ograniczenia. Pusta wartość wyłącza wymuszanie limitu uczestników N-way po stronie klienta.

6.1.22 Przełączenie połączenia

Funkcję Pull połączenia można włączyć za pomocą jednego parametru konfiguracyjnego, jak pokazano w poniższym przykładzie.

```
<config>
<services><calls>
<call-pull enabled="%ENABLE_CALL_PULL_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_PULL_WXT%	false	prawda, fałsz	Włącza funkcję Call Pull.

6.1.23 Zadzwoń do parku/odzyskaj

Funkcja grupowego parkowania połączeń umożliwia przekierowanie trwających połączeń VoIP na serwer parkowania połączeń, dzięki czemu osoba dzwoniąca może zająć się czymś innym i zostać odebrana przez tego samego lub innego użytkownika. Trwające połączenie zostanie zaparkowane pod pierwszym dostępnym numerem wewnętrznym w ramach Grupy Parkowania Połączeń.

Informacje poufne firmy Cisco

Ponowne odtworzenie połączenia może zostać wykonane przez użytkownika poprzez zaparkowanie połączenia w oknie dialogowym na konfigurowalną liczbę sekund bezpośrednio po zaparkowaniu połączenia. Albo zaparkowane połączenie może zostać odebrane przez użytkownika lub inną osobę poprzez wybranie opcji odebrania połączenia i wprowadzenie numeru lub numeru wewnętrznego.

```
<config>
<services><calls>
<call-park enabled="%ENABLE_CALL_PARK_WXT%"
timer="%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_PARK_WXT%	false	prawda, fałsz	Włącza parkowanie/przywracanie połączeń.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Liczba od 5 do 30	Określa liczbę sekund, przez które okno dialogowe informujące o pomyślnym zaparkowaniu połączenia będzie widoczne dla użytkownika, zanim zostanie automatycznie zamknięte.

6.1.24 Statystyki połączeń

Raportowanie statystyk zakończenia połączenia w komunikacie BYE protokołu SIP (Session Initiation Protocol) umożliwia wysyłanie statystyk połączenia do zdalnego użytkownika po zakończeniu połączenia. Statystyki połączeń są wysyłane jako nowy nagłówek w wiadomości SIP BYE lub w odpowiedniej odpowiedzi *200 OK* na wiadomość BYE. Statystyki obejmują wysłane lub odebrane pakiety protokołu RTP (Real-time Transport Protocol), całkowitą liczbę wysłanych lub odebranych bajtów, całkowitą liczbę utraconych pakietów, opóźnienie, opóźnienie w obie strony i czas trwania połączenia.

```
<config>
<services><calls>
<call-statistics enabled="%ENABLE_CALL_STATISTICS_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_STATISTICS_WXT%	false	prawda, fałsz	Ustaw na „prawda”, aby włączyć przechwytywanie metryk połączeń. Ustaw wartość „false” (fałsz), aby wyłączyć przechwytywanie metryk połączeń.

Informacje poufne firmy Cisco

6.1.25 Automatyczne odzyskiwanie połączeń / bezproblemowe przekazywanie połączeń

Klient ma możliwość automatycznego odzyskiwania połączeń podczas przełączania sieci, gdy użytkownik prowadzi rozmowę VoIP. Automatyczne odzyskiwanie połączeń działa w obu kierunkach – dane komórkowe-WiFi i Wi-Fi-dane komórkowe, a także podczas przełączania się między sieciami Wi-Fi. Następuje próba nawiązania połączenia w ciągu jednej minuty, po czym połączenie zostaje przerwane. Jeśli trwa więcej niż jedno połączenie VoIP, odzyskiwane jest tylko połączenie aktywne.

Podczas przejścia z sieci komórkowej na sieć Wi-Fi klient będzie kontynuował rozmowy VoIP, korzystając z sieci komórkowej, aż do jej zakończenia lub utraty połączenia z siecią komórkową.

```
<config>
<services><calls>
<auto-recovery enabled="%ENABLE_CALLS_AUTO_RECOVERY_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false	prawda, fałsz	Kontroluje, czy mechanizm automatycznego odzyskiwania powinien być włączony dla użytkownika.

6.1.26 Nagrywanie połączeń

Funkcja nagrywania rozmów jest obsługiwana przez klienta i zależy od dostępności tej funkcji po stronie serwera, a także opcji konfiguracji. Funkcja zależy od włączonego kanału zdarzeń XSI (patrz sekcja *6.1.33 Kanał zdarzeń XSI*) i serwera aplikacji (AS) skonfigurowanego do wysyłania nagłówka *X-BroadWorks-Correlation-Info* (zobacz *Webex for Cisco BroadWorks Solution Guide*).

Jeśli ta funkcja jest wyłączona, użytkownik nie ma dostępu do żadnych przycisków ani opcji nagrywania. Należy pamiętać, że nagrywanie rozmów odbywa się na podstawie użytkownika, a nie połączenia – oznacza to, że jeśli jeden z uczestników rozmowy obsługuje nagrywanie rozmów, rozmowa może zostać nagrana.

Jeśli funkcja nagrywania rozmów jest włączona, zawsze pojawia się wizualny wskaźnik informujący o nagrywaniu rozmowy. Cisco BroadWorks obsługuje następujące tryby nagrywania połączeń:

Zawsze

- Nagrywanie rozmów rozpocznie się automatycznie po nawiązaniu połączenia.
- Użytkownik **NIE** może zatrzymać/wstrzymać nagrywanie rozmowy.

Zawsze z obsługą wstrzymywania/wznawiania

- Nagrywanie połączeń zostanie rozpoczęte automatycznie podczas nawiązywania połączenia, ale użytkownik będzie mógł je wstrzymać i wznowić.
- Możliwe interakcje z użytkownikami:
  - Nagrywanie w toku – **Wstrzymaj** Akcja nagrywania.

Informacje poufne firmy Cisco

- Nagrywanie jest wstrzymane — czynność **Wznów** nagrywanie.

Na żądanie

- Po nawiązaniu połączenia na serwerze rozpoczyna się nagrywanie rozmowy.
- Jeżeli użytkownik naciśnie opcję Rozpocznij nagrywanie podczas połączenia, nagranie rozmowy zostanie zapisane i połączenie będzie utrzymywane od momentu jego rozpoczęcia. W przeciwnym wypadku, jeśli użytkownik nie zainicjuje nagrywania, nagranie rozmowy zostanie usunięte z serwera.
- Możliwe interakcje z użytkownikami:
  - Nagrywanie jeszcze się nie rozpoczęło – akcja **Rozpocznij** nagrywanie.
  - Nagrywanie w toku – **Wstrzymaj** Akcja nagrywania.
  - Nagrywanie jest wstrzymane — czynność **Wznów** nagrywanie.

Na żądanie z uruchomieniem inicjowanym przez użytkownika

- Użytkownik może rozpocząć, zatrzymać, wstrzymać i wznowić nagrywanie rozmów w dowolnym momencie, wielokrotnie w trakcie trwania połączenia.
- Dla każdego uruchomienia nagrywania rozmów będą wykonywane oddzielne nagrania.
- Możliwe interakcje z użytkownikami:
  - Nagrywanie jeszcze się nie rozpoczęło – akcja **Rozpocznij** nagrywanie.
  - Trwa nagrywanie — czynność **Zatrzymaj** i **Wstrzymaj** nagrywanie.
  - Nagrywanie jest wstrzymane — czynność **Zatrzymaj** i **Wznów** nagrywanie.

Tryb nagrywania rozmów przypisany użytkownikowi można wybrać w Control Hub.

```
<config>
<services><calls>
<record enabled="%ENABLE_CALL_RECORDING_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_RECORDING_WXT%	false	prawda, fałsz	Włącza kontrolę nagrywania rozmów.

6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej

Następujące tagi niestandardowe mogą być używane do kontrolowania dostępności poczty głosowej i wizualnej poczty głosowej Cisco BroadWorks w kliencie Webex for Cisco BroadWorks. Należy pamiętać, że znacznik systemowy Cisco BroadWorks (%BWVOICE-PORTAL-NUMBER-1%) jest używany z pocztą głosową.

Informacje poufne firmy Cisco

Poczta głosowa Visual Voicemail (VVM) obsługiwana jest wyłącznie w przypadku dźwięku. Obsługiwane formaty to wav, ulaw i mov zawierające wideo H264 (odtwarzane wyłącznie jako dźwięk). Umożliwia użytkownikom przeglądanie przychodzących wiadomości głosowych w formie listy i odtwarzanie pojedynczych elementów. Funkcja ta opiera się na Xsi, ale powiadomienia o nowej poczcie głosowej są przesyłane przez protokół SIP. Dlatego też, aby powiadomienia działały, należy włączyć protokół SIP. Ponadto konfiguracja SIP SUBSCRIBE dla Message Waiting Indicator (MWI) jest wymagana, aby powiadomienia mogły być odbierane, a MWI musi być włączone, aby usługa Visual Voicemail działała. Aby uzyskać więcej informacji na temat konfiguracji protokołu SIP, zobacz sekcję *6.1.1 Ustawienia serwera SIP*.

Wymagania dotyczące wersji i poprawek dla wizualnej poczty głosowej Cisco BroadWorks można znaleźć w
Przewodniku po rozwiązaniach Webex dla Cisco BroadWorks.

Pocztę głosową wizualną należy włączyć osobno w konfiguracji.

Aby korzystać z poczty głosowej Visual Voicemail, w portalu CommPilot wymagane są następujące ustawienia:

- Wiadomości głosowe włączone
- Włączona opcja „Gdy wiadomość dotrze, użyj ujednoliconej obsługi wiadomości”
- Włączona opcja „Użyj wskaźnika oczekującej wiadomości telefonicznej”

Brak przypisanej usługi wizualnej poczty głosowej po stronie Cisco BroadWorks dla użytkownika automatycznie wyłącza konfigurację tej usługi.

Należy pamiętać, że wyłączenie rejestracji SIP powoduje również wyłączenie MWI dla nowych wiadomości głosowych. Więcej informacji na temat włączania MWI znajdziesz w poniższej tabeli.

Aby wyświetlić informacje o wiadomościach poczty głosowej w interfejsie użytkownika, klient musi otrzymywać powiadomienia SIP MWI z serwera (czyli pakiety zdarzeń poczty głosowej). Opcje subskrypcji znajdziesz w tabeli poniżej. Należy również pamiętać, że MWI jest wymagane do działania powiadomień Visual Voicemail.

Należy pamiętać, że jeśli subskrypcja pakietu zdarzeń poczty głosowej SIP się nie powiedzie, klient będzie ponawiał próby, zgodnie ze skonfigurowaną procedurą. Aby uzyskać więcej informacji na temat konfiguracji ponawiania próby SIP SUBSCRIBE, zobacz sekcję *6.1.9 SIP SUBSKRYBUJ I ZAREJESTRUJ SIĘ Odśwież i SUBSKRYBUJ Spróbuj* ponownie.

```
<config>
<services><calls>
<mwi enabled="%ENABLE_MWI_WXT%" type="%MWI_MODE_WXT%"/>
<voice-mail enabled="%ENABLE_VOICE_MAIL_WXT%" visual-
voicemail="%ENABLE_VISUAL_VOICE_MAIL_WXT%">
   <center-number>%BWVOICE-PORTAL-NUMBER-1%</center-number>
</voice-mail>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_VOICE_MAIL_WXT%	false	prawda, fałsz	Ustaw na „true”, aby włączyć obsługę poczty głosowej. Ustaw wartość „false” (fałsz), aby wyłączyć obsługę poczty głosowej.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	prawda, fałsz	Ustawienie wartości „false” (fałsz) powoduje wyłączenie funkcji VVM. Po ustawieniu wartości „true” funkcja VVM jest włączona. Należy pamiętać, że opcja poczty głosowej enabled=false przed faktycznym atrybutem VVM jest nadal używana w celu zapewnienia wstecznej kompatybilności.
%BWVOICE-PORTAL-NUMBER-1%	puste	liczba	Klient dzwoni do tego numeru zazwyczaj określonego przy użyciu istniejącego znacznika systemowego Cisco BroadWorks podczas wybierania poczty głosowej.
%ENABLE_MWI_WXT%	false	prawda, fałsz	Ustaw na „true”, aby włączyć MWI. Ustaw na „fałsz”, aby wyłączyć MWI.
%MWI_MODE_WXT%	puste	dorozumiany, jawny	Ustaw na „jawny”, aby wysłać SIP SUBSCRIBE dla pakietu zdarzeń MWI, gdy MWI jest włączone. Używanie „niejawne” nie wysyła SIP SUBSCRIBE dla pakietu zdarzeń MWI, gdy MWI jest włączone. Jeśli pozostawisz puste, MWI zostanie wyłączone.

6.1.28 Transkrypcja poczty głosowej dla usługi Webex Calling

Dzięki tej funkcji wiadomości poczty głosowej są konwertowane na tekst i wyświetlane w wizualnym widoku wiadomości poczty głosowej w aplikacji klasycznej i mobilnej Webex Calling.

Funkcja powinna być włączona dla użytkownika tylko wtedy, gdy:

1. Aplikacja działa we wdrożeniu usługi Webex Calling.
2. Funkcja wizualnej poczty głosowej jest włączona dla użytkownika.
3. Funkcja ta jest włączona w konfiguracji (włączony atrybut w tagu powinien być ustawiony na „true”).

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	false	prawda, fałsz	[Tylko Webex Calling] Kontroluje dostępność transkrypcji poczty głosowej tylko wtedy, gdy jest włączona wizualna poczta głosowa.

Informacje poufne firmy Cisco

6.1.29 Ustawienia połączeń

6.1.29.1 Przekazywanie połączeń zawsze

Poniższy niestandardowy znacznik może być użyty do kontrolowania dostępności usługi Cisco BroadWorks Always Przekierowywanie połączeń w kliencie Webex for Cisco BroadWorks.

```
<config>
<services><supplementary-services>
<call-forwarding-always enabled="%ENABLE_CALL_FORWARDING_ALWAYS_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	prawda, fałsz	Kontroluje dostępność usługi Zawsze przekierowuj połączenia. Domyślnie ta funkcja jest wyłączona.

UWAGA: Przekierowywanie wszystkich połączeń i przekierowanie połączeń do poczty głosowej (*6.1.29.2 Przekierowywanie połączeń do poczty głosowej*) mogą być używane razem do wyświetlania lub ukrywania ustawienia „Przekierowanie połączeń" w aplikacjach Webex. Gdy oba znaczniki są wyłączone, ustawienie „Przekierowanie połączeń" w aplikacjach Webex jest ukryte.

6.1.29.2 Przekierowywanie połączeń do poczty głosowej

Począwszy od wersji 43.9, aplikacja Webex udostępnia opcję kontrolowania dostępności przekierowywania do poczty głosowej. Domyślnie ta funkcja jest włączona, a poniższą opcję konfiguracji można wyłączyć.

```
<config>
<services>
   <voice-mail>
      <forwarding enabled="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	true	prawda, fałsz	Kontroluje dostępność przekierowania do poczty głosowej. Domyślnie ta funkcja jest włączona.

UWAGA 1: Funkcja ta zależy od przypisania użytkownikowi jednej z usług „Użytkownik wiadomości głosowych" lub „Wsparcie poczty głosowej stron trzecich".

Informacje poufne firmy Cisco

UWAGA 2: Przekierowywanie połączeń do poczty głosowej i przekierowywanie połączeń zawsze (*6.1.29.1 Przekazywanie połączeń zawsze*) mogą być używane razem do wyświetlania lub ukrywania ustawienia „Przekierowywanie połączeń” w aplikacjach Webex. Gdy oba znaczniki są wyłączone, ustawienie „Przekierowanie połączeń” w aplikacjach Webex jest ukryte.

6.1.29.3 BroadWorks Anywhere (zasięg pod jednym numerem)

Następujące tagi niestandardowe kontrolują dostępność portalu BroadWorks Anywhere i jego ustawień w kliencie Webex for Cisco BroadWorks. Należy pamiętać, że nazwa tej funkcji w kliencie to *Zarządzaj moimi numerami*.

```
<config>
<services><supplementary-services>
<broadworks-anywhere enabled="%ENABLE_BROADWORKS_ANYWHERE_WXT%">
       <description enabled="%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%"/>
       <alert-all-locations
enabled="%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%"
default="%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%"/>
       <call-control enabled="%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%"
default="%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%"/>
       <diversion-inhibitor
enabled="%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%"
default="%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%"/>
       <answer-confirmation
enabled="%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%"
default="%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%"/>
</broadworks-anywhere>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_BROADWORKS_ANYWHERE_WXT%	false	prawda, fałsz	Włącza BroadWorks Anywhere (BWA) na poziomie konfiguracji.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	true	prawda, fałsz	Określa, czy opis lokalizacji BWA powinien być dostępny dla użytkownika.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	prawda, fałsz	Ustaw na „prawda”, aby usługa BWA udostępniała użytkownikowi alerty dotyczące wszystkich lokalizacji. Ustaw wartość „false” (fałsz), aby ustawienie powiadamiania wszystkich lokalizacji dla usługi BWA było niedostępne dla użytkownika.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	false	prawda, fałsz	Kontroluje, czy aplikacja powinna włączyć stan Alert dla wszystkich lokalizacji przy dodawaniu drugiej lub każdej kolejnej nowej lokalizacji BWA.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	prawda, fałsz	Określa, czy sterowanie połączeniami w lokalizacji narzędzia BWA powinno być dostępne dla użytkownika.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	false	prawda, fałsz	Kontroluje domyślny stan Kontroli połączeń dla lokalizacji BWA.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	prawda, fałsz	Określa, czy inhibitor przekierowania lokalizacji BWA powinien być dostępny dla użytkownika.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	prawda, fałsz	Kontroluje domyślny stan inhibitora przekierowania lokalizacji BWA.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false	prawda, fałsz	Określa, czy dla użytkownika powinno być dostępne potwierdzenie odpowiedzi lokalizacji narzędzia BWA.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	false	prawda, fałsz	Kontroluje domyślny stan potwierdzenia odpowiedzi w lokalizacji BWA.

6.1.30 Portal ustawień i ustawienia połączeń sieciowych

Klient Webex for Cisco BroadWorks zapewnia dostęp do portalu ustawień (Self Care), w którym użytkownik może skonfigurować niektóre ustawienia aplikacji i usługi.

Ponadto klient oferuje możliwość korzystania z widoku internetowego ustawień połączeń (CSWV). Dzięki temu użytkownik ma większą kontrolę nad ustawieniami połączeń na serwerze. Za pomocą oddzielnych tagów można kontrolować, czy konkretne usługi mają być widoczne w internetowych ustawieniach połączeń.

> **UWAGA**: Zaleca się ukrycie ustawień, które są już widoczne w aplikacji, takich jak Call Center (patrz sekcja *6.1.31 Logowanie/wylogowanie do centrum połączeń / kolejki* połączeń) i BroadWorks Anywhere (patrz sekcja *6.1.29.3 BroadWorks Anywhere*). Usługę Remote Office również zaleca się ukryć, ponieważ została ona zastąpiona przez usługę BroadWorks Anywhere.

Poniższy niestandardowy tag można wykorzystać do skonfigurowania adresu URL dla portalu ustawień (Self Care lub CSWV). Jeśli tag jest pusty, link do portalu ustawień nie będzie widoczny dla użytkownika w aplikacji.

```
<config>
<services>
<web-call-settings target="%WEB_CALL_SETTINGS_TARGET_WXT%"
 <url>%WEB_CALL_SETTINGS_URL_WXT%</url>
<branding-enabled="%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%">
  <service-settings>
   <service name="Call Forwarding Always"
visible="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <service name="Call Forwarding Busy"
visible="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <service name="Call Forwarding Not Reachable"
visible="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
```


Informacje poufne firmy Cisco

```
   <service name="Call Forwarding No Answer"
visible="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <service name="Do Not Disturb" visible="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
   <service name="Anonymous Call Rejection"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="Simultaneous Ring Personal"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <service name="Sequential Ring"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <service name="Automatic Callback"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <service name="Call Waiting" visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Calling Line ID Delivery Blocking"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <service name="Personal Assistant"
visible="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
   <service name="Call Center - Standard"
visible="%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%"/>
   <service name="BroadWorks Anywhere"
visible="%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%"/>
   <service name="BroadWorks Mobility"
visible="%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <service name="Remote Office" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Voice Messaging User"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
</web-call-settings>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%WEB_CALL_SETTINGS_TARGET_WXT%	zewnętrzny	zewnętrzny, csw	Kontroluje tryb portalu administracyjnego. Ustaw na „zewnętrzny", aby otworzyć skonfigurowany adres URL portalu ustawień w zewnętrznej przeglądarce. Ustaw opcję „csw", aby otworzyć portal CSW w osadzonej przeglądarce, korzystając z sekcji dodatkowych parametrów , aby utworzyć żądanie POST.
%WEB_CALL_SETTINGS_URL_WXT%	puste	Ciąg URL	Adres URL portalu ustawień. Przykład: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Zawsze przekierowuj połączenia ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Nie przeszkadzać (DND) powinna być widoczna dla użytkownika w ustawieniach WWW.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja odrzucania połączeń anonimowych (ACR) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	true	prawda, fałsz	Kontroluje, czy opcja Przekierowywanie połączeń zajętych (CFB) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	true	prawda, fałsz	Kontroluje, czy opcja Przekierowywanie połączeń nieosiągalnych (CFNR) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	true	prawda, fałsz	Kontroluje, czy opcja przekierowania połączeń w przypadku nieodebrania (CFNA) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Simultaneous Ring Personal (SIMRING) powinna być widoczna dla użytkownika w ustawieniach WWW.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja sekwencyjnego wywoływania połączeń (SEQRING) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja zdalnego biura (RO) powinna być widoczna dla użytkownika w ustawieniach WWW.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja automatycznego wywołania zwrotnego (ACB) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	true	prawda, fałsz	Kontroluje, czy opcja Call Waiting (CW) powinna być widoczna dla użytkownika w ustawieniach WWW.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja blokowania dostarczania identyfikatora linii wywołującej (CLIDB) powinna być widoczna dla użytkownika w ustawieniach WWW.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Asystent osobisty (PA) powinna być widoczna dla użytkownika w ustawieniach sieciowych.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja BroadWorks Anywhere (BWA) powinna być widoczna dla użytkownika w ustawieniach sieci WWW.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Centrum połączeń powinna być widoczna dla użytkownika w ustawieniach WWW.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	true	prawda, fałsz	Kontroluje, czy opcja BroadWorks Mobility (BWM) powinna być widoczna dla użytkownika w ustawieniach WWW. Obecnie zalecana wartość to „false" z powodu problemów ze współpracą między Webex for Cisco BroadWorks i BroadWorks Mobility.
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja zarządzania głosami (VM) powinna być widoczna dla użytkownika w ustawieniach WWW.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false	prawda, fałsz	Kontroluje, czy używać nowego brandingu Call Settings WebView. Włącz, jeśli wersja CSWV po stronie serwera to 1.8.6 lub nowsza. W przeciwnym wypadku podawaj nieprawdę.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcje wiadomości e-mail/poczty głosowej są widoczne w ustawieniach internetowych.
%USER_PORTAL_SETTINGS_URL_WXT%	puste	Ciąg URL	Określa adres URL portalu ustawień użytkownika. Aby włączyć tę funkcję i wyświetlić przycisk Dostęp do portalu użytkownika w interfejsie użytkownika, ten niestandardowy tag nie może być pusty. Na przykład: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	zewnętrzny	zewnętrzny, wewnętrzny	Określa, czy adres URL ma zostać otwarty w przeglądarce osadzonej czy zewnętrznej.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false	prawda, fałsz	Dotyczy tylko sytuacji, gdy skonfigurowano wbudowaną przeglądarkę (USER_PORTAL_SETTINGS_TARGET_WXT=internal). Po włączeniu tej opcji używane jest żądanie HTTP POST, a krótkotrwały token BroadWorks dodawany jest jako część BODY. Po wyłączeniu tej opcji adres URL jest otwierany za pomocą protokołu HTTP GET.

UWAGA 1: Adres URL WebView ustawień połączeń powinien zawsze mieć na końcu skonfigurowany znak „/". Na przykład: http(s)://<XSP-FQDN>/<CSW-Context-Path>/

UWAGA 2: Minimalna obsługiwana wersja aplikacji Call Settings WebView to 1.7.5.

Informacje poufne firmy Cisco

Aby uzyskać informacje na temat instalacji na oprogramowaniu Cisco BroadWorks w wersji 21.0, zobacz dodatkowe kroki opisane w *Przewodniku po rozwiązaniach Webex For Cisco BroadWorks*.

6.1.31 Logowanie/wylogowanie do centrum połączeń / kolejki połączeń

Aplikacja Webex zapewnia dostęp do ustawień agenta Call Center (kolejka połączeń). Jeśli użytkownik ma dostęp do Call Center, ta funkcja umożliwia mu zalogowanie się do Call Center i przeglądanie dostępnych kolejek połączeń, a także dołączanie do kolejek i ich opuszczanie, a także ustawianie statusu automatycznej dystrybucji połączeń (ACD).

Począwszy od wersji klasycznej 42.8 i mobilnej 42.12, agent Call Center (kolejka połączeń) nie jest już oparty na widoku internetowym ustawień połączeń (patrz sekcja *6.1.30 Portal ustawień i ustawienia połączeń sieciowych*). Konfiguracja agenta Call Center (kolejka połączeń) jest dostępna za pomocą stopki pulpitu i ustawień aplikacji mobilnej Webex.

```
<config>
<services>
<call-center-agent enabled="%ENABLE_CALL_CENTER_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_CENTER_WXT%	false	prawda, fałsz	Umożliwia obsługę Call Center.

6.1.32 Źródło i ścieżki XSI

Klient Webex for Cisco BroadWorks używa następujących tagów do sterowania ścieżką katalogu głównego, działań i wydarzeń XSI, jeśli muszą być skonfigurowane tak, aby różnić się od tagów używanych do logowania.

Głównym powodem zmiany XSI Root jest potrzeba wdrożenia równoważenia obciążenia na poziomie konfiguracji, choć zaleca się korzystanie z równoważenia obciążenia na poziomie warstwy HTTP.

Ścieżki zdarzeń i akcji są zazwyczaj zmieniane ze względu na wymagania dotyczące marki, aby usunąć odniesienie do domeny *com.broadsoft* ze ścieżek URL żądań HTTP XSI wykonywanych przez klienta.

```
<config>
<protocols><xsi>
        <paths>
                <root>%XSI_ROOT_WXT%</root>
                <actions>%XSI_ACTIONS_PATH_WXT%</actions>
                <events>%XSI_EVENTS_PATH_WXT%</events>
        </paths>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%XSI_ROOT_WXT%	Nadal używa oryginalnej konfiguracji do pobierania.	Ciąg URL	Korzeń XSI dla wszystkich operacji XSI. Przykład: https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	struna	Określa ścieżkę akcji XSI. Powinien zaczynać się i kończyć znakiem „/” i zawierać wyłącznie kontekst akcji. Przykład: /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	struna	Określa ścieżkę zdarzeń XSI. Powinna zaczynać się i kończyć znakiem „/” i zawierać tylko kontekst zdarzenia. Przykład: /com.domain.xsi-events/

6.1.33 Kanał zdarzeń XSI

Kanał zdarzeń XSI jest używany do różnych usług, takich jak:

- Elementy sterujące XSI w trakcie połączenia
- Powiadomienia o stanie ustawień połączeń
- Nagrywanie połączeń

Heartbeat zdarzeń XSI służy do utrzymywania kanału zdarzeń XSI otwartym. Interwał heartbeat można określić przy użyciu następującego parametru.

```
<config>
<protocols><xsi>
<event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
    <heartbeatInterval> %CHANNEL_HEARTBEAT_WXT%</heartbeatInterval>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_XSI_EVENT_CHANNEL_WXT%	true	prawda, fałsz	Kontroluje, czy kanał zdarzeń XSI jest włączony. Należy ustawić wartość „true”, aby na przykład otrzymywać informacje o zdarzeniach związanych z usługą kontroli połączenia. Zalecana wartość to „prawda”.
%CHANNEL_HEARTBEAT_WXT%	10000	liczba	To jest puls kanału zdarzeń XSI (w milisekundach). Wartość domyślna to „10000”.

Informacje poufne firmy Cisco

6.1.34 Konfiguracja kodeka

Webex for Cisco BroadWorks udostępnia szereg kodeków audio i wideo. Odpowiednie listy kodeków znajdują się w katalogu *config/services/calls/* w sekcjach *audio/codecs* i *video/codecs* . Priorytet każdego kodeka można zmienić za pomocą *atrybutu XML priorytet*, który jest wartością z zakresu od 0,0 (najniższa) do 1,0 (najwyższa).

Aplikacja Webex oficjalnie obsługuje następujące kodeki:

- Dźwięk
  - Opus
  - G.722
  - G.729
  - PMU (G.711U)
  - PCMA (G.711A)
  - iLBC
  - Kodek AI
- Wideo
  - H.264

Informacje poufne firmy Cisco

```
<config>
<services><calls>
  <audio>
    <codecs>
      <codec name="opus" priority="1" payload=""/>
      <codec name="xCodec" mode="HP" priority=".99" payload=""/>
      <codec name="xCodec" mode="ULP" priority=".98" payload=""/>
      <codec name="G722" priority=".9" payload=""/>
      <codec name="PCMU" priority=".8" payload=""/>
      <codec name="PCMA" priority=".7" payload=""/>
      <codec name="G729" priority=".5" payload="" vad=""/>
      <codec name="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="telephone-event" payload="101" in-band="false"/>
    …
  <video>
    <codecs>
      <codec name=”H264” payload=”109” resolution=”CIF” framerate=”25”
bitrate=”768000” priority=”1.0”>
        <packet-mode>0</packet-mode>
```

Klient obsługuje kodek wideo H.264. Atrybut rozdzielczości wideo można wykorzystać do ustawienia jednej z następujących dostępnych wartości: Obsługiwane formaty: SUBQCIF, QCIF, CIF, 4CIF, VGA i HD.

Jeżeli w konfiguracji nie wprowadzono szybkości transmisji, używane są domyślne wartości szybkości transmisji. Domyślne wartości szybkości transmisji dla danej rozdzielczości i liczby klatek na sekundę podano w poniższej tabeli.

Rozdzielczość	Rozmiar wideo *	FPS (ramki na sekundę)	Domyślne wartości szybkości transmisji bitów dla każdej rozdzielczości i liczby klatek na sekundę (FPS)
PODWYŻSZONE	128 x 96	15	128000
QCIF	176 x 144	30	192000
CIF	352 x 288	15	384000
CIF	352 x 288	30	768000
VGA	640 x 460	15	2000000
4CIF	704 x 576	25	2000000
HD	960 x 720	30	2000000

***** Maksymalna reklamowana rozdzielczość wideo. Rzeczywista rozdzielczość wideo podczas połączenia między dwoma klientami Webex dla Cisco BroadWorks zależy od możliwości obu klientów — będzie ona niższa z tych dwóch klientów i będzie taka sama dla obu klientów.

Rozdzielczość wideo dla połączenia wideo jest negocjowana podczas konfigurowania sesji i zależy od możliwości obu punktów końcowych. Rozdzielczość połączeń wideo jest taka sama na obu punktach końcowych. Oznacza to, że jeśli punkty końcowe Webex dla Cisco BroadWorks mają różne możliwości (a zatem obsługują różne rozdzielczości), niższa rozdzielczość jest negocjowana dla połączenia. Rozdzielczość obrazu może ulec zmianie w trakcie połączenia, jeżeli warunki sieciowe się pogorszą. W tym przypadku dwa mobilne punkty końcowe mogą używać różnych rozdzielczości wideo.

Informacje poufne firmy Cisco

Tryb pakietowania można skonfigurować jako SingleNAL (0) lub Non-interleaved (1). Szablon domyślnie używa SingleNAL (0).

Obsługiwana jest również konfiguracja zdarzeń telefonicznych, pojedynczych lub wielokrotnych. Podczas negocjacji kodeków klient wysyła wszystkie skonfigurowane kodeki, łącznie ze zdarzeniem telefonicznym. Po wybraniu kodeka audio wyszukiwane jest zdarzenie telefoniczne w ofercie. Jeżeli oferta zawiera zdarzenie telefoniczne z częstotliwością próbkowania wynegocjowanego kodeka audio, to to zdarzenie telefoniczne jest wybierane. W przeciwnym wypadku używane jest pierwsze zdarzenie telefoniczne na liście.

Jeżeli wynegocjowano co najmniej jedno zdarzenie telefoniczne, sygnały DTMF (dual-tone multi-frequency) są wysyłane jako pakiety RTP, wykorzystując odpowiedni typ danych. Jeśli nie przeprowadzono żadnych negocjacji zdarzeń telefonicznych, sygnały DTMF są wysyłane jako pakiety RTP zawierające typ danych negocjowanego kodeka audio. Mechanizm braku przepustowości dostarczania kodów DTMF nie jest obsługiwany przez aplikację Webex.

Przykład skonfigurowanych kodeków:

```
<codec name="telephone-event" payload="100" in-band="false" />
<codec name="telephone-event" payload="101" clockrate="48000" in-band="false" />
```

Jeżeli zostanie wynegocjowany kodek audio o częstotliwości próbkowania 48 kbps, używane jest zdarzenie telefoniczne z ładunkiem 101.

6.1.34.1 Kodek AI

Począwszy od wersji 44.8 aplikacja Webex wprowadza obsługę nowego kodeka audio — Kodek AI (xCodec). Ten kodek audio jest używany w przypadku niesprzyjających warunków sieciowych w celu uzyskania lepszej jakości połączeń. Silnik multimediów Webex w aplikacji Webex sprawdza możliwości urządzenia, śledzi jakość multimediów, a kodek SI może być używany, jeśli jest obsługiwany i włączony za pomocą pliku konfiguracyjnego.

Kodek AI działa tylko w połączeniu z kodekiem Opus. Oznacza to, że zarówno Opus jak i kodek AI powinny zostać ogłoszone i wynegocjowane przez obie strony podczas negocjacji SDP.

6.1.35 Wybieranie SIP-URI

Obecnie wybieranie numerów SIP-URI za pośrednictwem BroadWorks nie jest dostępne. Domyślnie wszystkie połączenia SIP-URI są kierowane przez Locus, co jest znane również jako „połączenia bezpłatne”. W niektórych środowiskach nie jest to pożądane i takie połączenia należy blokować.

> **UWAGA**: Dotyczy to wyłącznie sytuacji, gdy wywoływanie Locus jest wyłączone. Tylko w tym przypadku blokada wybierania numeru SIP URI będzie działać.

Poniższa konfiguracja udostępnia taką opcję.

```
<config>
    <services>
        <calls>
            <sip-uri-dialing enable-locus-
calling="%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%"/>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	true	prawda, fałsz	Kontroluje, czy SIP-URI ma być kierowany przez Locus (prawda), czy blokowany (fałsz).

6.1.36 Historia połączeń na wszystkich urządzeniach

Klient umożliwia zapisywanie i pobieranie historii połączeń z serwera zamiast przechowywania jej lokalnie. Dzięki temu historia połączeń jest ujednolicona na wszystkich urządzeniach.

UWAGA: Ujednolicona historia połączeń powinna być włączona jednocześnie po stronie klienta i serwera, aby uniknąć braku historii połączeń lub duplikacji rekordów.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	prawda, fałsz	Określa, czy aplikacja powinna używać ujednoliconej historii połączeń, czy też historii po stronie klienta (lokalnej).

6.1.37 Wyłącz połączenia wideo

W wersji 41.9 dodano możliwość wyłączania połączeń wideo. Dostępne są oddzielne opcje konfiguracji umożliwiające sterowanie tą funkcją w przypadku połączeń VoIP obsługiwanych przez BroadWorks i Locus (bezpłatnie).

Gdy funkcja jest włączona i tag funkcji jest ustawiony na „fałsz”:

- użytkownik nie zobaczy ustawienia „Akceptuj połączenia przychodzące z włączonym wideo”
- wszystkie przychodzące połączenia wideo, jeśli zostaną zaakceptowane, będą połączeniami audio
- użytkownik nie będzie mógł eskalować połączenia do rozmowy wideo, a eskalacje wideo będą automatycznie odrzucane

Po włączeniu połączeń wideo dodawana jest nowa właściwość konfiguracji kontrolująca wartość domyślną ustawienia „Akceptuj połączenia przychodzące z włączonym wideo”. Domyślnie ta funkcja jest WŁĄCZONA na komputerach stacjonarnych i WYŁĄCZONA na urządzeniach mobilnych i tabletach.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SIP_VIDEOCALLS_WXT%	true	prawda, fałsz	Kontroluje dostępność połączeń wideo SIP poprzez BroadWorks.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_LOCUS_VIDEO CALLS_WXT%	true	prawda, fałsz	Kontroluje dostępność połączeń wideo Locus (bezpłatnych).
%VIDEOCALLS_ANSWER_ WITH_VIDEO_ON_DEFAULT _WXT%	Pulpit - prawda Telefon komórkowy / tablet - fałsz	prawda, fałsz	Steruje domyślną wartością ustawienia „Akceptuj połączenia przychodzące z włączonym wideo”.

6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji u dostawcy usługi E911

Klient komputerowy i tabletu Webex obsługuje raportowanie lokalizacji E911 przy użyciu usług RedSky, Intrado lub Bandwidth jako dostawca połączeń alarmowych E911 dla wdrożenia Webex dla BroadWorks. Dostawca usługi E911 zapewnia obsługę lokalizacji dla każdego urządzenia (dla aplikacji komputerowych i tabletów Webex oraz urządzeń MPP obsługujących technologię HELD) oraz sieć, która przekierowuje połączenia alarmowe do punktów przyjmowania zgłoszeń o wypadkach (PSAP) w Stanach Zjednoczonych, terytoriach zależnych Stanów Zjednoczonych (Guam, Portoryko i Wyspy Dziewicze) oraz tylko w Kanadzie. Usługa jest włączana na podstawie lokalizacji.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%EMERGENCY_DIALING_ ENABLE_REDSKY_WXT%	false	prawda, fałsz	Włącza platformę lokalizacji połączeń alarmowych dostawcy usługi E911.
%BWE911-PRIMARY-HELDURL%	puste	struna	Określa adres URL platformy lokalizacji awaryjnej dostawcy usługi E911 obsługującej protokół HELD.
%BWE911-CUSTOMERID%	puste	struna	Identyfikator klienta (HeldOrgId, CompanyID) używany w żądaniu HTTPS dostawcy usługi E911.
%BWE911-SECRETKEY%	puste	struna	Klucz tajny umożliwiający uwierzytelnienie żądania HTTPS dostawcy usługi E911.
%BWE911-EMERGENCY-NUMBER-LIST%	puste	Ciąg CSV	Lista numerów alarmowych obsługiwanych przez dostawcę usługi E911.
%EMERGENCY_REDSKY_ USER_REMINDER_TIMEO UT_WXT%	0 (użytkownik nie będzie ponownie monitowany)	numer [0 - 43200]	Limit czasu (w minutach), który zostanie użyty do przypomnienia użytkownikowi o aktualizacji lokalizacji połączenia alarmowego, jeśli bieżąca lokalizacja nie została wprowadzona lub jest nieprawidłowa. Sugerowana wartość, jeśli zdecydujesz się włączyć: 1440 (jeden dzień).

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (użytkownik może zawsze anulować dialog)	liczba [-1 - 100]	Czasy, w których użytkownik może zamknąć okno dialogowe lokalizacji, zanim lokalizacja stanie się obowiązkowa (tzn. nie może zamknąć okna lokalizacji). Możliwe wartości: ▪ N = -1 (użytkownik może zawsze anulować okno dialogowe) ▪ N = 0 (użytkownik nie ma możliwości anulowania dialogu – zawsze wymagana lokalizacja) ▪ N > 0 (użytkownik może anulować dialog N razy, zanim stanie się on obowiązkowy)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	agresywny, raz_na_logowanie	raz_na_logowanie	Definiuje zachowanie monitowania o lokalizację E911. Wartość „aggressive" spowoduje wyświetlenie użytkownikowi okna dialogowego przy każdej zmianie sieci na nieznaną lokalizację, podczas gdy wartość „once_per_login" spowoduje wyświetlenie okna dialogowego tylko raz, zapobiegając dalszemu wyświetlaniu okienek i rozpraszaniu uwagi użytkownika.

UWAGA 1: Znaczniki BWE911-*** to „Dynamiczne znaczniki wbudowane systemu". Aby uzyskać więcej informacji, zobacz punkt *5.7 Tagi systemu dynamicznego wbudowanego Cisco BroadWorks*.

UWAGA 2: Jeśli połączenia VOIP są wyłączone, jedyną znaczącą wartością sekwencji wybierania alarmowego (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) jest tylko cs.

6.1.39 PAI jako tożsamość

W przypadku **połączeń przychodzących** ten nowy parametr kontroluje priorytet nagłówków SIP From i P-Asserted-Identity (PAI) oraz to, co powinno być używane jako identyfikator linii wywołującej. Jeśli w przychodzącym zaproszeniu SIP INVITE znajduje się nagłówek X-BroadWorks-Remote-Party-Info, jest on używany z priorytetem względem nagłówków SIP From i PAI. Jeśli w przychodzącym żądaniu SIP INVITE nie ma nagłówka X-BroadWorks-Remote-Party-Info, ten nowy parametr określa, czy nagłówek SIP From ma priorytet nad nagłówkiem PAI, czy odwrotnie.

Jeśli włączony atrybut tagu jest ustawiony na „true", nagłówek PAI jest używany z pierwszeństwem przed nagłówkiem From. Tożsamość osoby dzwoniącej służy do nawiązania kontaktu i przedstawienia go użytkownikowi.

W przypadku **połączeń wychodzących** ta logika nie jest stosowana. W odpowiedziach 18X, 200 OK, odebrana jest tożsamość połączonej linii, więc aplikacja Webex zawsze używa nagłówka SIP PAI z priorytetem.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	prawda, fałsz	Kontroluje, czy tożsamość dzwoniącego, przedstawiona użytkownikowi, ma zostać pobrana z nagłówka SIP From lub SIP P-Asserted-Identity. Ustaw na „true”, aby używać nagłówka PAI z priorytetem.

6.1.40 Wyłącz udostępnianie ekranu

Wersja 42.5 dodaje możliwość kontrolowania dostępności udostępniania ekranu. Gdy udostępnianie ekranu jest wyłączone:

- użytkownik nie zobaczy opcji inicjowania udostępniania ekranu podczas rozmów 1 na 1
- przychodzące prośby o udostępnienie ekranu są odrzucane, a użytkownik zobaczy komunikat informacyjny

Domyślnie ta funkcja jest włączona.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SCREEN_SHARE_WXT%	true	prawda, fałsz	Określa, czy udostępnianie ekranu powinno być włączone dla użytkownika.

6.1.41 Wskazanie połączeń spamowych

Gdy przełącznik funkcji (dla każdego typu wdrożenia) jest włączony, a funkcja jest włączona w pliku konfiguracyjnym, aplikacja Webex przetwarza nowy parametr wskazujący stan weryfikacji połączenia spamowego, jeśli został on odebrany jako część rekordów powiadomienia wypychanego lub historii połączeń.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	prawda, fałsz	Kontroluje dostępność informacji o połączeniach spamowych na ekranie połączenia przychodzącego i historii połączeń tylko dla usługi Webex Calling.

6.1.42 Usuwanie szumów i rozszerzenie przepustowości dla połączeń PSTN/komórkowych

Usuwanie hałasu zapewnia użytkownikom dzwoniącym lepszy komfort nawiązywania połączeń, gdy rozmawiają oni z użytkownikami spoza usługi Webex w sieci PSTN lub na urządzeniach przenośnych. Od wersji 43.12 usuwanie szumów jest domyślnie włączone.

Informacje poufne firmy Cisco

Wersja 44.2 aplikacji Webex wprowadza nowe ulepszenia AI mowy nośników audio dla wąskopasmowych połączeń PSTN.

- Dodano nowy algorytm rozszerzenia pasma w celu poprawy jakości dźwięku poprzez rozszerzenie pasma wąskopasmowego PSTN i usunięcie szumów. Rozszerzone pasmo zwiększy zrozumiałość i zmniejszy zmęczenie słuchu.
- Istniejący algorytm usuwania szumów został udoskonalony, dzięki czemu usunięto ograniczenia dotyczące muzyki podczas oczekiwania i innych dźwięków (np. sygnałów dźwiękowych).
- Po włączeniu tej funkcji użytkownicy widzą wskaźnik „Inteligentne audio – zewnętrzne" i mogą sterować ulepszeniami Speech AI dla przychodzących multimediów audio.

Domyślnie te ulepszenia mowy są włączone i aktywne. Użytkownik może kontrolować stan początkowy za pomocą inteligentnych ustawień audio w Preferencjach audio.

```
<config>
   <services>
      <calls>
         <speech-enhancements enabled="%ENABLE_SPEECH_ENHANCEMENTS_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	false	prawda, fałsz	Włącza ulepszenia mowy dla mediów zewnętrznych (przychodzących).

UWAGA: Usuwanie hałasu jest teraz częścią dodatkowych ulepszeń mowy, a znacznik został wycofany przez nowy znacznik . Niestandardowy znacznik Usuwanie hałasu %ENABLE_NOISE_REMOVAL_WXT% jest również przestarzały.

6.1.43 Oznaczenie QoS DSCP

Oznaczanie QoS DSCP jest obsługiwane w przypadku pakietów RTP multimediów połączeń aplikacji Webex (audio i wideo). DSCP określa klasyfikację ruchu dla danych sieciowych. Można go wykorzystać do określenia, który ruch sieciowy wymaga większej przepustowości, ma wyższy priorytet i jest bardziej narażony na utratę pakietów.

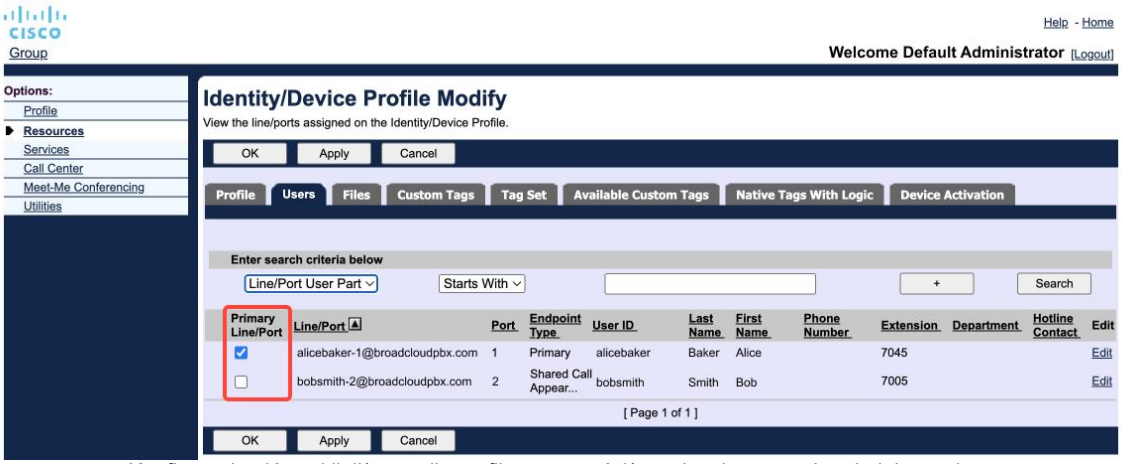
UWAGA: Ostatnie wersje systemu operacyjnego Microsoft Windows nie zezwalają aplikacjom na bezpośrednie ustawianie protokołu DSCP lub UP w pakietach wychodzących, a zamiast tego wymagały wdrożenia obiektów zasad grupy (GPO) w celu zdefiniowania zasad zaznaczania DSCP na podstawie zakresów portów UDP.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_AUDIO_QOS_WXT%	true	prawda, fałsz	Włącza QoS dla połączeń audio.
%AUDIO_QOS_VALUE_WXT%	46	0-63	Określa wartość QoS dla wybranego typu QoS dla połączeń audio. Uwaga: Wartość domyślna jest używana, jeśli nie podano żadnej wartości lub wartość nie mogła zostać pomyślnie przeanalizowana.
%ENABLE_VIDEO_QOS_WXT%	true	prawda, fałsz	Włącza QoS dla połączeń wideo
%VIDEO_QOS_VALUE_WXT%	34	0-63	Określa wartość QoS dla wybranego typu QoS dla połączeń wideo. Uwaga: Wartość domyślna jest używana, jeśli nie podano żadnej wartości lub wartość nie mogła zostać pomyślnie przeanalizowana.

6.1.44 Profil podstawowy

Dzięki integracji linii wspólnych (*6.1.51.1 Pulpit — wygląd linii wspólnej***Error! Reference source not found.**), jeśli linia użytkownika jest udostępniana innemu użytkownikowi, może zostać skonfigurowanych wiele profili tego samego typu. Aby wybrać odpowiedni profil do zalogowania się do usług telefonicznych, oprogramowanie Cisco BroadWorks zostało ulepszone w celu wskazania, czy użytkownik jest właścicielem urządzenia, tj. ma przypisaną linię/port dla urządzenia. Aby uzyskać więcej informacji na temat aktualizacji Cisco BroadWorks, sprawdź Flaga właściciela na liście urządzeń w celu obsługi linii wspólnych klienta Webex.



Konfiguracja głównej linii/portu dla profilu tożsamości/urządzenia w portalu administracyjnym

Informacje poufne firmy Cisco

Począwszy od wersji 43.2, dodano nową opcję konfiguracji (*device-owner-restriction*), aby określić, czy należy zastosować ograniczenie profilu podstawowego. Można z niego skorzystać, aby umożliwić aplikacji Webex korzystanie z innego niż podstawowy profilu linii/portu do logowania się do usług telefonicznych. Ta opcja konfiguracji jest stosowana do wszystkich konfiguracji, niezależnie od liczby profili skonfigurowanych dla użytkownika (**Jeśli ograniczenie własności urządzenia jest włączone i nie ma urządzenia z linią główną/portem dla odpowiedniej platformy, usługi telefoniczne nie zostaną nawiązane**).

To samo ograniczenie dotyczy urządzeń, z którymi użytkownik może sparować w aplikacji klasycznej Webex. Użytkownik może wyświetlać i parować tylko z urządzeniami, których jest właścicielem. Zapobiega to parowaniu z urządzeniami innego użytkownika, do których przypisano linię współdzieloną lub wirtualną. Wartość tego samego parametru konfiguracyjnego dotyczy również tego ograniczenia.

```
<config>
<services><calls>
<device-owner-restriction enabled="%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	true	prawda, fałsz	Steruje ograniczeniami właściciela urządzenia – czy usługi telefoniczne powinny używać głównego profilu dla danego urządzenia

UWAGA: Zaleca się włączenie ograniczenia właściciela. Jeśli ta opcja jest wyłączona, usługi telefoniczne będą używać pierwszego znalezionego profilu do logowania. Mogą wystąpić pewne problemy, jeśli dla użytkownika tego samego typu skonfigurowano wiele profili.

6.1.45 Lista zablokowanych (tylko Webex Calling)

Począwszy od wersji 43.5 aplikacja Webex wprowadza listę zablokowanych numerów telefonów zdefiniowanych przez użytkownika. Jeśli ta funkcja jest włączona, użytkownik może określić, że połączenia przychodzące z konkretnych numerów mają być blokowane po stronie serwera i nie będą dostarczane na żadne urządzenie użytkownika. Użytkownik może zobaczyć zablokowane połączenia w historii połączeń.

Użytkownik może skonfigurować listę blokowanych numerów z dwóch miejsc – w Preferencjach połączeń i Historii połączeń. W Preferencjach użytkownik może zobaczyć listę zablokowanych numerów i ją edytować. W historii połączeń użytkownik może przeglądać zapisy historii połączeń zablokowanych na liście blokowanych użytkowników. Te rekordy mają oznaczenie Zablokowane, jeśli numer znajduje się na liście zablokowanych numerów zdefiniowanej przez użytkownika. Użytkownik będzie miał możliwość bezpośredniego odblokowania numeru dla danego rekordu. Dostępna jest również opcja blokowania.

Zasady dotyczące numerów dodawanych do listy bloków zdefiniowanych przez użytkownika:

Format liczb

Informacje poufne firmy Cisco

- Zablokowanie z preferencji połączeń zastosuj ograniczenie formatu E.164 lokalnie w aplikacji Webex
- Blokowanie z historii połączeń jest dozwolone dla wszystkich rekordów usługi Webex Calling
- Cisco BroadWorks może zezwalać lub odrzucać żądania dotyczące nowych numerów dodanych do listy zablokowanych na podstawie formatu numerów

Numery wewnętrzne – połączenia przychodzące z numerów wewnętrznych będą dostarczane do użytkownika, nawet jeśli znajdują się one na liście blokowanych numerów zdefiniowanej przez użytkownika

Lista zablokowanych zdefiniowana przez użytkownika jest skonfigurowana w Cisco BroadWorks i stosowana do wszystkich urządzeń WxC dla użytkownika. Ta funkcja działa wspólnie z listą zablokowanych zdefiniowaną przez administratora, która nie jest konfigurowalna przez użytkownika i może być kontrolowana tylko przez administratorów za pośrednictwem Control Hub. BRAK zapisów historii połączeń dla połączeń przychodzących zablokowanych na liście blokowanych przez administratora.

Lista blokad zdefiniowana przez użytkownika jest stosowana po zastosowaniu zasad STIR/SHAKEN, listy blokad zdefiniowanej przez administratora i zasad odrzucania anonimowych połączeń.

```
<config>
<services><calls>
<call-block enabled="%ENABLE_CALL_BLOCK_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_BLOCK_WXT%	true	prawda, fałsz	Włącza zdefiniowaną przez użytkownika listę bloków Ustaw na „prawda”, aby zobaczyć listę blokowanych w Preferencjach połączeń i Historii połączeń

UWAGA: Ta funkcja zależy od przypisania do użytkownika usługi Cisco BroadWorks Call Block.

6.1.46 Adaptacja i wdrażanie odporności mediów (MARI)

6.1.46.1 Adaptacja tempa

Aplikacja Webex zintegrowała już techniki adaptacyjnej jakości multimediów, aby mieć pewność, że utrata pakietów wideo nie ma wpływu na dźwięk, oraz aby wideo mogło wykorzystać dostosowanie szybkości wideo do zarządzania przepustowością używaną w okresach dużego obciążenia.

Informacje poufne firmy Cisco

Adaptacja szybkości transmisji lub dynamiczne dostosowywanie szybkości transmisji danych dopasowuje szybkość połączenia do zmiennej dostępnej przepustowości, zmniejszając lub zwiększając szybkość transmisji danych wideo na podstawie stanu utraty pakietów. Punkt końcowy zmniejszy szybkość transmisji, gdy otrzyma od odbiornika komunikaty informujące o utracie pakietów; po zmniejszeniu się utraty pakietów nastąpi zwiększenie szybkości transmisji.

Nie ma konfigurowalnych ustawień kontrolujących wykorzystanie mechanizmu dostosowywania szybkości transmisji.

6.1.46.2 Korekcja błędów przekierowywania (FEC) i retransmisji pakietów (RTX)

Począwszy od wersji 43.4, aplikacja Webex dodaje do mechanizmu adaptacji multimediów obsługę korekcji błędów przekierowywania (FEC) i retransmisji pakietów (RTX) zarówno dla multimediów audio, jak i wideo.

FEC zapewnia redundancję przesyłanych informacji dzięki zastosowaniu ustalonego algorytmu. Dzięki redundancji odbiorca jest w stanie wykryć i skorygować ograniczoną liczbę błędów, bez konieczności proszenia nadawcy o dodatkowe dane. FEC umożliwia odbiornikowi korygowanie błędów bez konieczności korzystania z kanału zwrotnego (takiego jak RTCP) w celu żądania retransmisji danych, ale ta zaleta wiąże się z koniecznością zapewnienia większej przepustowości kanału przekazującego (więcej wysyłanych pakietów).

Punkty końcowe nie używają FEC przy przepustowościach mniejszych niż 768 kbps. Ponadto, aby można było wprowadzić FEC, musi wystąpić utrata pakietów na poziomie co najmniej 1,5%. Punkty końcowe zwykle monitorują skuteczność FEC i jeśli FEC nie jest wydajny, nie jest stosowany.

Kodowanie FEC zużywa więcej pasma niż retransmisja, ale ma mniejsze opóźnienie. RTX stosuje się, gdy dopuszczalne są niewielkie opóźnienia i występują ograniczenia przepustowości. W przypadku dużego opóźnienia i wystarczającej przepustowości preferowane jest FEC.

Aplikacja Webex dynamicznie wybiera protokół RTX lub FEC w zależności od wynegocjowanej przepustowości i tolerancji opóźnień dla danego strumienia multimediów. FEC skutkuje większym wykorzystaniem przepustowości ze względu na redundantne dane wideo, ale nie wprowadza dodatkowego opóźnienia w odzyskiwaniu utraconych pakietów. Natomiast RTX nie przyczynia się do większego wykorzystania przepustowości, ponieważ pakiety RTP są retransmitowane tylko wtedy, gdy odbiornik wskazuje utratę pakietów w kanale zwrotnym RTCP. RTX wprowadza opóźnienie odzyskiwania pakietów ze względu na czas potrzebny na dotarcie pakietu RTCP od nadawcy do odbiorcy oraz na dotarcie retransmitowanego pakietu od nadawcy do odbiorcy.

Aby włączyć RTX, konieczne jest włączenie FEC.

```
<config><services><calls>
<audio>
       <audio-quality-enhancements>
              <mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <payload>111</payload>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <m>8</m>
                            <multi_ssrc>1</multi_ssrc>
                            <non_seq>1</non_seq>
                            <feedback>0</feedback>
```


Informacje poufne firmy Cisco

```
                        <order>FEC_SRTP</order>
                    </fec>
                    <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                        <mari-rtx>90000</mari-rtx>
                        <payload>112</payload>
                        <time>180</time>
                        <data-flow>1</data-flow>
                        <order>RTX_SRTP</order>
                    </rtx>
                </mari>
...
<video>
        <video-quality-enhancements>
                <mari>
                    <fec enabled="%ENABLE_VIDEO_MARI_FEC_WXT%">
                        <x-ulpfecuc>8000</x-ulpfecuc>
                        <payload>111</payload>
                        <max_esel>1400</max_esel>
                        <max_n>255</max_n>
                        <m>8</m>
                        <multi_ssrc>1</multi_ssrc>
                        <non_seq>1</non_seq>
                        <feedback>0</feedback>
                        <order>FEC_SRTP</order>
                    </fec>
                    <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                        <mari-rtx>90000</mari-rtx>
                        <payload>112</payload>
                        <time>180</time>
                        <data-flow>1</data-flow>
                        <order>RTX_SRTP</order>
                    </rtx>
                </mari>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_AUDIO_MARI_FEC_WXT%	false	prawda, fałsz	Włącza funkcję FEC dla połączeń audio
%ENABLE_AUDIO_MARI_RTX_WXT%	false	prawda, fałsz	Włącza RTX dla połączeń audio (wymaga włączonego audio FEC)
%ENABLE_VIDEO_MARI_FEC_WXT%	false	prawda, fałsz	Włącza FEC dla połączeń wideo
%ENABLE_VIDEO_MARI_RTX_WXT%	false	prawda, fałsz	Włącza protokół RTX dla połączeń wideo (wymaga włączonego mechanizmu FEC wideo)

6.1.47 Połączenia równoczesne z tym samym użytkownikiem

Dodano obsługę jednoczesnych połączeń z tym samym użytkownikiem na jednym urządzeniu.

Informacje poufne firmy Cisco

Funkcja ta jest przydatna w przypadku niektórych wdrożeń, w których prezentowana tożsamość połączenia nie jest taka sama, jak tożsamość nawiązana. Prowadzi to do braku możliwości zainicjowania transferu powrotnego do pierwotnej strony. Włączając tę funkcję, użytkownik będzie mógł obsługiwać wiele jednoczesnych połączeń z tym samym rozmówcą.

```
<config>
   <services>
      <calls>
         <simultaneous-calls-with-same-user
enabled="%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false	prawda, fałsz	Określa, czy aplikacja Webex może mieć tylko jedno lub wiele połączeń WxC z tym samym użytkownikiem.

6.1.48 RTCP-XR

Począwszy od wersji 43.8, aplikacja Webex dodaje negocjacje dotyczące wymiany pakietów RTCP-XR podczas połączenia. Negocjacje odbywają się w trakcie ustanawiania sesji SIP INVITE. Jeśli oba punkty końcowe obsługują pakiety RTCP-XR, silnik multimedialny Webex rozpocznie wymianę tych pakietów i włączy mechanizm adaptacyjnej jakości połączeń. Ta funkcja jest włączona domyślnie.

Dodatkowo tylko w przypadku usługi Webex Calling te dodatkowe metryki będą wysyłane za pośrednictwem protokołu SIP BYE i w ten sposób ujawniane w Control Hub.

```
<config>
<protocols><sip>
   <rtcp-xr>
      <negotiation enabled="%ENABLE_RTCP_XR_NEGOTIATION_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	true	prawda, fałsz	Umożliwia negocjację protokołu RTCP-XR i wymianę pakietów w celu zapewnienia lepszej jakości połączeń. Domyślnie włączone.

6.1.49 Informacje o przekierowywaniu połączeń

Wersja 44.2 aplikacji Webex wprowadza konfigurowalną opcję kontrolowania widoczności informacji o przekierowywaniu i przekierowywaniu połączeń na ekranach związanych z połączeniami i w historii połączeń.

Informacje poufne firmy Cisco

```
<config>
<services><calls>
<call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	true	prawda, fałsz	Kontroluje widoczność informacji o przekierowaniu i przekierowaniu połączeń. Ustaw na „prawda”, aby zobaczyć informacje na ekranach związanych z połączeniami i historią połączeń.

6.1.50 ID dzwoniącego

6.1.50.1 Identyfikator dzwoniącego w połączeniach wychodzących

Aplikacje mobilne Webex (wersja 44.2) i Desktop (wersja 44.3) wprowadzają użytkownikowi nową możliwość wybierania preferowanego zewnętrznego identyfikatora dzwoniącego dla połączeń wychodzących. Lista dostępnych opcji obejmuje:

- Linia bezpośrednia (domyślna)
- Numer lokalizacji
- Niestandardowy numer z tej samej organizacji
- Kolejki połączeń, do których należy użytkownik, co umożliwia agentom korzystanie z jego numeru identyfikacyjnego dzwoniącego
    - Jeśli skonfigurowano dowolne opcje programu, będą one dostępne do wyboru
- Grupy poszukiwania, do których należy użytkownik, umożliwiająca agentom korzystanie z numeru identyfikatora dzwoniącego
- Ukryj identyfikator dzwoniącego

Uwagi:

- Lista opcji zależy od linii:
    - Linia podstawowa – pełen zestaw opcji
    - Linie współdzielone – niedostępne
    - Linie wirtualne – tylko opcje kolejki połączeń
- Jeżeli wybrana już tożsamość nie jest już dostępna, używany jest domyślny identyfikator dzwoniącego użytkownika
- Połączenia alarmowe zawsze należy wykonywać na numer alarmowy użytkownika
- Cofa znacznik <outgoing-calls> w sekcji <services><call-center-agent>

Informacje poufne firmy Cisco

Listę dostępnych opcji można skonfigurować poprzez portal administracyjny. Istnieją również oddzielne niestandardowe tagi DMS, które określają dostępność tych ulepszeń w aplikacji Webex.

```
<config>
<services><calls>
   <caller-id>
      <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
         <additional-numbers enabled="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
         <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
         <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
         <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
      </outgoing-calls>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	prawda, fałsz	Umożliwia wybór numeru identyfikacyjnego linii wywołującej dla połączeń wychodzących.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	false	prawda, fałsz	Kontroluje dostępność dodatkowych numerów skonfigurowanych dla użytkownika.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	false	prawda, fałsz	Kontroluje dostępność numerów centrum telefonicznego (Call Center) skonfigurowanych dla użytkownika.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	prawda, fałsz	Kontroluje dostępność numerów grupy poszukiwania skonfigurowanych dla użytkownika.
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	prawda, fałsz	Umożliwia blokowanie dostarczania identyfikatora rozmówcy jako wybór dla połączeń wychodzących.

UWAGA: Aplikacja klasyczna w wersji 44.3 obsługuje tylko Call Center CLID, a w wersji 44.4 dodano obsługę pozostałych opcji.

6.1.50.2 Nazwa zdalnego identyfikatora dzwoniącego

Podczas odbierania/inicjowania połączenia Cisco BroadWorks wysyła nazwę wyświetlaną zdalnego rozmówcy w INVITE protokołu SIP. Jest ona domyślnie używana przez aplikację Webex. W tym samym czasie aplikacja Webex rozpoczyna rozwiązywanie kontaktów z kilku źródeł, o następującym priorytecie:

- Wspólna tożsamość (CI)
- Usługa kontaktowa (kontakty niestandardowe)
- Kontakty programu Outlook (komputer)
- Lokalna książka adresowa (mobilna)

Informacje poufne firmy Cisco

W przypadku pomyślnego nawiązania kontaktu z dowolnym źródłem wyszukiwania wyświetlana nazwa strony zdalnej zostanie zaktualizowana. Ponadto, jeśli kontakt zostanie znaleziony w usłudze CI, sesja połączenia jest połączona z usługami tego samego użytkownika w chmurze Webex, zapewniając opcję wyświetlania awatara i obecności zdalnego rozmówcy, korzystania z czatu, udostępniania ekranu, opcji eskalacji do spotkania w chmurze Webex itp.

Wersja 44.5 aplikacji Webex dodaje konfigurowalną opcję ignorowania rozdzielczości kontaktu i zawsze zachowywania nazwy wyświetlanej Cisco BroadWorks dla połączeń z obszarami roboczymi lub urządzeniami RoomOS używanymi dla połączeń Cisco BroadWorks 1:1.

```
<config>
<services><calls>
   <caller-id>
      <remote-name>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	rozwiązanie	rozwiązany, łyk	Kontroluje nazwę wyświetlaną strony zdalnej dla obszarów roboczych i urządzeń RoomOS. Użyj „sip”, aby zignorować rozwiązanie kontaktu i użyć nazwy wyświetlanej otrzymanej w sesji SIP INVITE.

Informacje poufne firmy Cisco

6.1.51 Wielowierszowe

Użytkownik Webex może mieć linię podstawową i maksymalnie 9 linii pomocniczych. Linie dodatkowe mogą być udostępniane lub wirtualne (tylko Webex Calling).

Aplikacja Webex pobiera konfigurację linii za pomocą pliku konfiguracyjnego DMS, który jest pobierany po zalogowaniu się i co 12-godzinnego czasu. W przypadku wykrycia aktualizacji konfiguracji linii użytkownik jest proszony o ponowne uruchomienie aplikacji w celu zastosowania zmian. Ponowne zalogowanie użytkownika spowoduje natychmiastowe wykrycie i zastosowanie wszelkich aktualizacji konfiguracji linii.

Poniżej przedstawiono sekcję szablonu konfiguracji DMS dotyczącą obsługi wielu linii zarówno dla komputerów stacjonarnych, jak i mobilnych.

```
<config>
<protocols>
   <sip>
       <lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
          <personal>
             <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
          </personal>
          <line lineType="%BW-MEMBERTYPE-1%">
             <external-id>%BWUSEREXTID-1%</external-id>
             ...
          </line>
          <line lineType="%BW-MEMBERTYPE-2%">
             <external-id>%BWUSEREXTID-2%</external-id>
             ...
          </line>
          ...
          <line lineType="%BW-MEMBERTYPE-10%">
             <external-id>%BWUSEREXTID-10%</external-id>
             ...
          </line>
```

Aby sterować funkcją obsługi wielu linii, użyj dedykowanego znacznika niestandardowego.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_MULTI_LINE_WXT%	false	prawda, fałsz	Włącza obsługę wielu linii (jeśli skonfigurowano). Jeśli wyłączone (ustawione na „false”), aplikacja użyje tylko pierwszego skonfigurowanego wiersza.

UWAGA 1: Funkcja obsługi szefa-administratora (kierownik-asystent) jest niedostępna w połączeniu z konfiguracją wieloliniową.

UWAGA 2: Dodatkowe wymagania dotyczące oprogramowania BroadWorks można znaleźć w podręczniku Webex-for-Cisco-BroadWorks-Solution-Guide „Wygląd linii wspólnej”.

Informacje poufne firmy Cisco

6.1.51.1 Pulpit — wygląd linii wspólnej

Począwszy od wersji 42.12, aplikacja Webex dodaje obsługę linii wspólnych. Administrator powinien skonfigurować wyświetlanie połączeń współdzielonych dla każdej linii współdzielonej.

W wersji 43.12 aplikacja Webex została ulepszona, aby umożliwić przenoszenie (lokalne wznawianie) wstrzymanego połączenia na linii wspólnej lub wirtualnej, obsługiwanego przez innego użytkownika lub przez tego samego użytkownika na innym urządzeniu. Aby uzyskać więcej informacji, zobacz *6.2.12 Przenieś połączenie*.

6.1.51.2 Komputer — linie wirtualne (tylko Webex Calling)

Tylko w przypadku wdrożenia usługi Webex Calling aplikacja Webex obsługuje konfigurację wielu linii przy użyciu linii wirtualnych. Funkcjonalnie konfiguracja z liniami wirtualnymi jest zgodna z wieloma liniami korzystającymi z linii wspólnych — z możliwością przeglądania linii wirtualnych skonfigurowanych dla użytkownika i używania ich do połączeń przychodzących i wychodzących.

Wersja 43.4 rozszerza obsługę linii wirtualnych, dodając funkcje Grupowe parkowanie połączeń i Odzyskiwanie parkowania połączeń.

W wersji 43.12 aplikacja Webex została ulepszona, aby umożliwić przenoszenie (lokalne wznawianie) wstrzymanego połączenia na linii wspólnej lub wirtualnej, obsługiwanego przez innego użytkownika lub przez tego samego użytkownika na innym urządzeniu. Aby uzyskać więcej informacji, zobacz *6.2.12 Przenieś połączenie*.

6.1.51.3 Telefon komórkowy (tylko Webex Calling)

Tylko w przypadku wdrożenia usługi Webex Calling w wersji 45.4 dodano obsługę wielu linii (wspólnych i wirtualnych) w wersji mobilnej aplikacji Webex. Przypisanie linii dotyczy zarówno aplikacji klasycznej, jak i mobilnej.

Ze względu na specyfikę platformy mobilnej użytkownik może wykonywać do dwóch połączeń jednocześnie na dowolnej linii.

> **UWAGA 1**: Jeśli włączona jest funkcja dzwonienia za pomocą natywnego dialera (zobacz *6.3.5.1 Zadzwoń za pomocą natywnego dialera*), obsługa wielu linii jest wyłączona.
>
> **UWAGA 2**: Wersja na tablety nie obsługuje wielu linii.

6.1.52 Rozszerzona autoryzacja SIP

Wersja 45.4 aplikacji Webex udostępnia konfigurowalną opcję optymalizacji komunikacji SIP, udostępniając autoryzację między wszystkimi sesjami SIP. Aplikacja zapisze autoryzację i użyje jej ponownie, dopóki nie będzie nadal ważna.

Ta funkcja przyspiesza komunikację SIP między serwerem a aplikacją Webex, skraca ruch, skraca czas połączenia i poprawia ogólną wydajność aplikacji Webex.

```
<config>
<protocols>
  <sip>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	prawda, fałsz	Jeśli jest ustawiona wartość „true”, ulepszenie autoryzacji SIP jest włączone.

UWAGA 1: Niektóre kontrolki SBC mogą wymagać nowej autoryzacji SIP w każdej sesji, dlatego należy używać tej funkcji zgodnie ze specyfikacją wdrożenia.

UWAGA 2: Nawet jeśli ta funkcja jest włączona, jeśli aplikacja Webex otrzyma komunikat 401 Brak autoryzacji, nowa autoryzacja zostanie użyta w następnym żądaniu SIP.

6.1.53 Asystent osobisty (obecność poza biurem)

W wersji 44.11 aplikacja mobilna Webex oraz wersji 45.3, aplikacja klasyczna Webex, dodano integrację z usługą Cisco BroadWorks Personal Assistant (PA). Działa w połączeniu z obecnością użytkownika na zewnątrz i wymaga synchronizacji stanu PA z obecnością w chmurze Webex.

Usługa PA daje użytkownikowi możliwość poinformowania dzwoniących o przyczynie niedostępności abonenta, opcjonalnie podając informacje o tym, kiedy abonent powróci i czy jest dostępny operator, który może obsłużyć połączenie.

Jeśli włączony jest system nagłośnienia, opcja obecności „Nieobecny” będzie dostępna dla użytkownika. Można go użyć do skonfigurowania PA po stronie Cisco BroadWorks. Po włączeniu tej funkcji użytkownicy zobaczą status „Nieobecny” w połączeniu ze statusem PA i skonfigurowanym czasem trwania.

Użytkownik może skonfigurować jedynie ręczną konfigurację PA. Jeśli wystąpią jakiekolwiek harmonogramy mające wpływ na usługę PA, obecność zostanie zaktualizowana za pomocą synchronizacji statusu asystenta osobistego. Jednak aplikacja Webex nie ujawnia konfiguracji harmonogramów i harmonogramów mających wpływ na agencję płatniczą.

```
<config>
<services>
  <personal-assistant enabled="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	prawda, fałsz	Określa, czy funkcja obecności „Nieobecny” jest dostępna dla użytkownika.

UWAGA 1: Ta funkcja wymaga włączenia synchronizacji statusu asystenta osobistego w Centrum partnerskim.

Informacje poufne firmy Cisco

UWAGA 2: Trasowanie połączeń Asystenta osobistego nie będzie działać, gdy są aktywne usługi Nie przeszkadzać, Zawsze przekierowywanie połączeń lub Selektywne przekierowywanie połączeń.

UWAGA 3: Ręczne stany Nie przeszkadzać i Zajęty mają wyższy priorytet w porównaniu ze stanami Nieobecny. Jeśli instrukcja obsługi aktywuje jeden z tych statusów obecności, włączenie Asystenta osobistego nie spowoduje zmiany statusu obecności na Nieobecny.

Informacje poufne firmy Cisco

6.2 Funkcje tylko pulpitu

6.2.1 Wymuszone wylogowanie

Ta funkcja umożliwia Cisco BroadWorks śledzenie online wystąpień klientów tego samego typu urządzenia i zezwolenie na jednoczesne wyświetlanie tylko jednego z nich w trybie online. Gdy usługa Cisco BroadWorks powiadomi klienta o wylogowaniu, połączenie SIP zostaje przerwane, a klient informuje, że połączenie nie jest nawiązane.

Funkcja ta jest potrzebna w niektórych wdrożeniach, w których podobni klienci mogą być w tym samym czasie online, co może powodować skutki uboczne. Przykładem jest użytkownik posiadający komputer stacjonarny w pracy i w domu, gdzie połączenia przychodzące będą odbierane tylko przez jednego z klientów, w zależności od tego, która rejestracja SIP jest aktywna.

Wymuszone wylogowanie jest oparte na protokole SIP, klient wysyła polecenie SIP SUBSCRIBE do pakietu zdarzeń *call-info* ze specjalną wartością *appid-value* w nagłówku *From* , niezależnie od wartości parametru *bsoft-call-info*. Kiedy Cisco BroadWorks wykryje wiele wystąpień klientów online z tym samym *appid*, wysyła specjalny komunikat SIP NOTIFY do starszego wystąpienia klienta, powodując jego wylogowanie. Na przykład klienci komputerów stacjonarnych mieliby identyczną wartość *appid-value* , chociaż nie ma żadnych ograniczeń co do używania tego identyfikatora po stronie klienta. *appid-value* jest konfigurowana przez dostawcę usługi.

Należy pamiętać, że aby skorzystać z funkcji wymuszonego wylogowania, należy włączyć subskrypcję SIP *Call-Info* .

Aby uzyskać informacje na temat poprawek i wydań Cisco BroadWorks potrzebnych do tej funkcji, zobacz sekcję dotyczącą wymagań oprogramowania Cisco BroadWorks w *Przewodniku po rozwiązaniach Webex for Cisco BroadWorks*.

Szczegóły konfiguracji można znaleźć w poniższym przykładzie (SIP to jedyny obsługiwany protokół sterowania w tej wersji).

```
<config>
<services>
<forced-logout enabled="%ENABLE_FORCED_LOGOUT_WXT%" control-protocol="SIP"
appid="%FORCED_LOGOUT_APPID_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_FORCED_LOGOUT_WXT%	false	prawda, fałsz	Włącza wymuszone wylogowanie.
%FORCED_LOGOUT_APPID_WXT%	puste	struna	Identyfikator aplikacji używany po stronie serwera w celu korelacji. Może to być dowolny ciąg znaków. Przykład: „123abc”

Informacje poufne firmy Cisco

6.2.2 Odbiór połączenia

Przejmowanie połączeń to usługa dla wielu użytkowników umożliwiająca wybranym użytkownikom odbieranie połączeń na dowolnym dzwoniącym numerze z ich grupy przechwytywania połączeń. Grupę przechwytywania połączeń definiuje administrator. Jest to podzbiór użytkowników w grupie, którzy mogą odbierać połączenia innych osób.

Obsługiwane są następujące przypadki odbioru:

- Odbieranie połączeń w ciemno
- Przejmowanie połączeń kierowanych (umożliwiające użytkownikowi odebranie połączenia kierowanego do innego telefonu z jego grupy poprzez wybranie odpowiedniego kodu dostępu do funkcji, a następnie podanie numeru wewnętrznego dzwoniącego telefonu).

```
<config>
<services><calls>
<call-pickup blind="%ENABLE_CALL_PICKUP_BLIND_WXT%"
directed="%ENABLE_CALL_PICKUP_DIRECTED_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	prawda, fałsz	Ustaw na „true”, aby włączyć funkcję odbierania połączeń w ciemno.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	prawda, fałsz	Ustaw wartość „true” (prawda), aby włączyć przejmowanie połączeń kierowanych.

6.2.3 Pomoc techniczna dla szefa (kierownik-asystent)

Funkcja Boss-Admin, znana jako funkcja Kierownik-Asystent w Cisco BroadWorks, umożliwia asystentowi działanie w imieniu kierownika w celu wyświetlania, odbierania i nawiązywania połączeń jako „kierownik”. Jeden asystent może mieć wielu kierowników i możliwe jest:

- Wybierz żądaną rolę podczas wykonywania połączenia.
- Odbierz połączenie przychodzące w imieniu dyrektora i przekaż je do niego. Oprócz tego dostępne są wszystkie standardowe opcje zarządzania połączeniami.
- Sprawdź, czy połączenie przychodzące jest faktycznie przeznaczone dla osoby zarządzającej.

Kierownik i kierownik-asystent to dwie powiązane ze sobą usługi Cisco BroadWorks, które razem zapewniają następującą funkcjonalność:

- Użytkownik usługi Executive może zdefiniować grupę asystentów, którzy będą zarządzać jego połączeniami. Asystentów należy wybrać spośród użytkowników z tej samej grupy lub przedsiębiorstwa, którym przypisano usługę Asystent Kierownika.
- Użytkownik usługi Executive-Assistant może odbierać i inicjować połączenia w imieniu swoich przełożonych.

Informacje poufne firmy Cisco

- Zarówno kadra kierownicza, jak i ich asystenci mogą określić, które połączenia mają być przekierowywane do asystentów, w jaki sposób asystenci mają być powiadamiani o połączeniach przychodzących oraz które z połączeń przekierowywanych do asystentów mają być przedstawiane kadrze kierowniczej do sprawdzenia.

```
<config>
<services>
<executive-assistant enabled="%ENABLE_EXECUTIVE_ASSISTANT_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	prawda, fałsz	Ustaw na „true”, aby włączyć funkcję Boss-Admin.

UWAGA: Funkcja wsparcia Boss-Admin (Executive-Assistant) nie jest dostępna w połączeniu z Shared-Lines.

6.2.4 Eskaluj połączenia SIP do spotkania (tylko Webex Calling)

Klient udostępnia funkcję eskalacji trwającego połączenia SIP do spotkania za pośrednictwem usługi Webex Calling. Dzięki wykorzystaniu tej funkcjonalności zamiast standardowej konferencji ad-hoc, użytkownik będzie mógł korzystać zarówno z funkcji wideo, jak i udostępniania ekranu podczas spotkania.

```
<config>
<services><calls>
       <escalate-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	prawda, fałsz	Ustaw wartość „true” (prawda), aby włączyć opcję menu Eskaluj do spotkania Webex.

6.2.5 Połączenia Desk Phone Control — automatyczne odbieranie

Funkcja automatycznej odpowiedzi umożliwia użytkownikowi korzystanie z funkcji Desk Phone Control (DPC) do obsługi połączeń wychodzących na komputerze klienckim w celu zarządzania telefonami MPP bez konieczności dotykania ekranu.

Wybrany telefon MPP będzie obsługiwał dźwięk i obraz podczas wychodzącego połączenia DPC.

Funkcja automatycznej odpowiedzi może działać zarówno na urządzeniach podstawowych, jak i dodatkowych. Jeśli użytkownik ma zarejestrowany więcej niż jeden telefon stacjonarny, który można sparować, automatycznie odbierze połączenie tylko wybrane/sparowane urządzenie.

Informacje poufne firmy Cisco

```
<config>
<services><calls>
<deskphone-control auto-answer="%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	true	prawda, fałsz	Po ustawieniu na „prawda” włącza funkcję automatycznego odbierania połączeń za pomocą telefonu stacjonarnego.

UWAGA: Funkcja automatycznego odbierania połączeń nie będzie miała wpływu na połączenia przychodzące w trybie DPC. Telefon stacjonarny będzie dzwonił w przypadku połączeń przychodzących.

6.2.6 Automatyczne odbieranie z powiadomieniem tonalnym

Funkcja ta umożliwia automatyczną obsługę połączeń przychodzących na urządzeniach lokalnych, jeśli jest to wskazane w żądaniu połączenia przychodzącego.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_AUTO_ANSWER_WXT%	false	prawda, fałsz	Po ustawieniu na „true” włącza się automatyczna obsługa połączeń przychodzących, jeśli zostanie to zażądane przez zaplecze.

6.2.7 Sterowanie telefonem stacjonarnym – Sterowanie w trakcie połączenia – Konferencja

Ta funkcja umożliwia korzystanie z opcji konferencji i scalania dla połączeń zdalnych (XSI), zakończonych w innej lokalizacji.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	prawda, fałsz	Wartość „true” (prawda) powoduje włączenie opcji konferencji i scalania dla połączeń zdalnych (XSI), zakończonych w innej lokalizacji.

Informacje poufne firmy Cisco

6.2.8 Powiadomienia przejmowania połączeń

Powiadomienia o przejęciu połączenia umożliwiają użytkownikowi uzyskanie informacji o połączeniu przychodzącym do użytkownika, którego skonfigurował do monitorowania. Powiadomienia o przejęciu połączeń można otrzymywać dla list obserwacyjnych skonfigurowanych za pośrednictwem grupy Call Pickup i usług Busy Lamp Field.

Powiadomienia o przejęciu połączenia są przydatne, gdy monitorowani użytkownicy nie znajdują się blisko siebie i nie mogą usłyszeć dzwonka telefonu swojego współpracownika.

6.2.8.1 Pole sygnalizacji aktywności linii

Aplikacja komputerowa Webex wyświetla powiadomienie, jeśli członek na liście obserwowanych pól sygnalizacji aktywności linii (SZL) ma połączenie przychodzące w stanie alertu. Powiadomienie zawiera informacje o osobie dzwoniącej i użytkowniku, który odebrał połączenie przychodzące, z możliwością odebrania połączenia, wyciszenia lub zignorowania powiadomienia. Odebranie połączenia przychodzącego przez użytkownika powoduje zainicjowanie bezpośredniego przejęcia połączenia.

Począwszy od wersji 43.4, lista użytkowników monitorowanych z funkcją SZL jest dostępna w oknie wielu połączeń (MCW) for Calling (dostępne tylko dla systemu Windows). Integracja listy BLF w MCW obejmuje:

Monitoruj połączenia przychodzące i odbieraj połączenia lub ignorowaj powiadomienia.

Zobacz pełną listę użytkowników BLF.

Monitoruj obecność użytkowników — rozszerzona obecność jest dostępna tylko dla użytkowników z uprawnieniami do usługi Webex Cloud. Podstawowa (telefoniczna) obecność dostępna jest wyłącznie dla użytkowników BroadWorks.

Rozpocznij rozmowę z użytkownikiem BLF.

Rozpocznij czat z użytkownikiem SZL — dostępne tylko dla użytkowników z uprawnieniem Webex Cloud.

Dodaj użytkownika SZL jako kontakt.

```
<config>
  <services>
    <calls>
      <busy-lamp-field enabled="%ENABLE_BUSY_LAMP_FIELD_WXT%">
        <display-caller enabled="%ENABLE_BLF_DISPLAY_CALLER_WXT%"/>
        <notification-delay time="%BLF_NOTIFICATION_DELAY_TIME_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	prawda, fałsz	Włącza monitorowanie pola zajętości i powiadamianie innych użytkowników dzwonkiem, dając im możliwość odbierania połączeń.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	true	prawda, fałsz	Włącza wyświetlanie nazwy/numeru dzwoniącego w powiadomieniu o połączeniu.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Określa, o ile sekund powiadomienie o dzwonku ma być opóźnione przed wyświetleniem go użytkownikowi.

UWAGA: Funkcja ta jest zależna od usługi bezpośredniego odbierania połączeń.

6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)

Począwszy od wersji 44.2 aplikacja Webex dodaje obsługę powiadomień Group Call Pickup (GCP) dla wdrożenia usługi Webex Calling. Umożliwia użytkownikom otrzymywanie powiadomień o połączeniach przychodzących od dowolnego użytkownika monitorowanego za pośrednictwem grupy Odbieranie połączeń.

W przypadku połączenia przychodzącego do użytkownika należącego do grupy przechwytywania połączeń, odbiorca połączenia ma możliwość odebrania połączenia. Opóźnienie powiadomienia GCP można skonfigurować za pomocą Control Hub. Jeśli odbiorca nie przetworzy połączenia w skonfigurowanym czasie, do grupy wysyłane jest powiadomienie GCP.

W przypadku wielu połączeń w ramach tej samej grupy przejęcia połączeń, są one przetwarzane sekwencyjnie, na podstawie czasu ich odebrania. Powiadomienie o najstarszym połączeniu jest wysyłane do grupy jako pierwsze, a po jego przetworzeniu do grupy wysyłane jest kolejne powiadomienie.

Powiadomienia mogą być wyłącznie dźwiękowe, wyłącznie wizualne lub dźwiękowo-wizualne, w zależności od konfiguracji w portalu administracyjnym Control Hub. Jeśli pojawi się wizualne powiadomienie GCP, użytkownik może odebrać połączenie, korzystając z funkcji odbioru połączenia. Jeśli skonfigurowano powiadomienie tylko audio, użytkownik nie zobaczy wizualnego powiadomienia o połączeniu przychodzącym, usłyszy określony dzwonek i może odebrać połączenie z menu Przejmowanie połączeń dostępnego w aplikacji Webex lub ręcznie wybierając kod FAC (*98) i numer wewnętrzny.

Użytkownik może wyciszyć powiadomienie GCP w ustawieniach aplikacji. To ustawienie dotyczy wszystkich powiadomień o przejęciu połączenia (BLF i GCP). Domyślnie powiadomienia są wyciszone.

Funkcja ta działa w przypadku linii podstawowych oraz linii współdzielonych i wirtualnych przypisanych użytkownikowi.

Informacje poufne firmy Cisco

```
<config>
<services><calls>
    <group-call-pickup-notifications enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
        <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
        <max-timeout value="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
    </group-call-pickup-notifications>
...
<protocols><sip>
    <lines>
        <line>
            <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
            ...
        </line>
        <line>
            <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>
            ...
        </line>
        ...
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	prawda, fałsz	Włącza powiadomienia o odbiorze połączeń grupowych
%ENABLE_GCP_DISPLAY_CALLER_WXT%	true	prawda, fałsz	Włącza wyświetlanie nazwy/numeru wyświetlanego dzwoniącego w powiadomieniu dzwoniącego
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5-120	Określa maksymalny czas, przez jaki powiadomienie GCP jest dostępne dla użytkownika
%BWGROUP-CALL-PICKUP-BOOL-n%	false	prawda, fałsz	Wskazuje, czy odpowiednia linia ma skonfigurowaną grupę odbioru połączeń

UWAGA 1: To jest funkcja dostępna tylko w usłudze Webex Calling.

UWAGA 2: Funkcja ta zależy od grupy Przejmowanie połączeń skonfigurowanej dla użytkownika.

6.2.9 Pakiet zdarzeń zdalnego sterowania

W przypadku klientów typu Click to Dial, takich jak cienki klient pracownika recepcji BroadWorks i integrator Go, w którym aplikacja Webex jest urządzeniem wywołującym, podczas odbierania połączenia lub wstrzymywania/wznawiania aplikacji Webex honoruje teraz pakiet zdarzeń zdalnego sterowania.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false	prawda, fałsz	Gdy ustawione na „true”, określa, że pilot zdalnego sterowania powinien być włączony dla użytkownika.

6.2.10 Brama utrzymania (tylko Webex Calling)

Począwszy od wersji 43.2 aplikacja Webex dodaje obsługę trybu połączenia utrzymania. Jeśli ta funkcja jest włączona i nie ma połączenia z usługą Webex Cloud, aplikacja Webex może być uruchomiona w trybie utrzymania. W tym trybie użytkownik ma dostęp do ograniczonej funkcjonalności połączeń.

Klient wdraża lokalną bramę przetrwania.

```
<config>
<protocols>
<sip>
<survivability-gateway enabled="%ENABLE_SURVIVABILITY_GATEWAY_WXT%" fallback-
time="%SURVIVABILITY_FALLBACK_TIME_WXT%">%BWSURVIVABILITYGATEWAY%</survivability-
gateway>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	prawda, fałsz	Włącza obsługę trybu przetrwania.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Określa czas powrotu (bramka umożliwiająca przetrwanie w SSE)

UWAGA: Funkcja ta zapewnia pewność migracji z rozwiązań lokalnych do rozwiązań w chmurze.

6.2.11 Pakiet zdarzeń zdalnego sterowania wyciszeniem (tylko Webex Calling)

Począwszy od wersji 43.9 aplikacja Webex dodaje obsługę zdalnego sterowania wyciszeniem strumienia multimediów audio. Umożliwia to wyciszenie lub wyłączenie wyciszenia trwającego połączenia z innej lokalizacji, takiej jak cienki klient pracownika recepcji BroadWorks, gdzie aplikacja Webex jest urządzeniem wywołującym.

Funkcja ta jest zależna od nowego pakietu informacyjnego SIP *x-cisco-mute-status* . Jeśli podczas ustanawiania sesji SIP INVITE zostanie odebrany nagłówek *Recv-Info:x-cisco-mute-status* , a następnie za każdym razem, gdy jest aktualizacja (lokalna lub zdalna) stanu wyciszenia sesji połączenia audio, aplikacja Webex będzie odsyłać informacje SIP z *Info-Package:x-cisco-mute-status;muted=true* (lub *muted=false*), gdzie parametr wyciszony reprezentuje zaktualizowany stan strumienia multimediów audio.

Informacje poufne firmy Cisco

Wyciszenie i włączenie dźwięku można uruchomić lokalnie lub zdalnie. Zdalna aktualizacja wyzwala komunikat SIP NOTIFY z *wydarzeniem: wyciszenie* (lub *wyłączenie wyciszenia*), aby wysłać je do aplikacji Webex z serwera aplikacji. Aplikacja Webex honoruje żądanie zdalne, a po aktualizacji stanu strumienia multimediów audio wysyła z powrotem komunikat SIP NOTIFY z opcją *Info-Package:x-cisco-mute-status;muted=true* (lub *muted=false*).

```
<config>
<services>
   <calls>
       <remote-mute-control enabled="%ENABLE_REMOTE_MUTE_CONTROL_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false	prawda, fałsz	Po ustawieniu wartości „true” użytkownik ma włączoną zdalną kontrolę wyciszenia połączeń.

6.2.12 Przenieś połączenie

Aplikacja Webex zapewnia monitorowanie połączeń i kontrolę połączeń VoIP zakończonych w innej lokalizacji. Obecnie ta opcja jest dostępna tylko na głównej linii użytkownika.

Począwszy od wersji 43.12 aplikacja Webex jest ulepszona, aby wyświetlała połączenia zakończone w innej lokalizacji, również dla linii wspólnych i wirtualnych. Takie połączenia są widoczne w obszarze trwających połączeń wyłącznie w celach informacyjnych i bez możliwości ich kontrolowania. Tylko jeśli takie połączenie zostanie wstrzymane, użytkownik będzie mógł przenieść je na urządzenie lokalne, wybierając je, i wznowić je z ekranu połączenia. Mechanizm ten jest przydatny, jeśli połączenie zostało obsłużone przez tego samego użytkownika w innej lokalizacji lub przez innego użytkownika korzystającego z tej samej linii.

Zauważ, że aplikacja Webex nie może przenieść wstrzymanego połączenia na sparowane urządzenie. Jeśli użytkownik jest sparowany z urządzeniem, musi się najpierw rozłączyć, aby móc lokalnie wznowić zawieszone połączenie.

Monitorowanie połączeń na liniach współdzielonych i wirtualnych zależy od pakietu zdarzeń informacji o połączeniach SIP.

Monitorowanie połączeń na linii głównej użytkownika jest uzależnione od zdarzeń XSI (pakiet zdarzeń zaawansowanych połączeń) i przeniesienie połączenia na urządzenie lokalne nie jest możliwe w przypadku tych połączeń. W przypadku tego typu połączeń użytkownik może skorzystać z funkcji Call Pull (*6.1.22 Przełączenie połączenia*). Funkcja „pull call” działa tylko w przypadku ostatnich aktywnych połączeń użytkownika, natomiast mechanizm dla linii współdzielonych i wirtualnych działa w przypadku wszystkich połączeń użytkownika, które są wstrzymane.

- Przypadek użycia 1:
    a. Alicja przypisał linię Boba do profili telefonu stacjonarnego i telefonu stacjonarnego.

Informacje poufne firmy Cisco

b. Alicja rozmawia z Charliem przez telefon stacjonarny – Alicja może zobaczyć trwającą rozmowę w aplikacji na komputerze.

c. Alicja wstrzymuje połączenie z telefonu stacjonarnego. Połączenie może zostać wznowione przez Alicję z aplikacji komputerowej.

- Przypadek użycia 2:

  a. Alicja przypisał linię Boba do profili telefonu stacjonarnego i telefonu stacjonarnego.

  b. Bob ma połączenie z Charlie – Alice może zobaczyć trwające połączenie w aplikacji klasycznej.

  c. Bob zawiesza połączenie z Charliem – Alicja może wznowić rozmowę z Charliem z aplikacji na komputerze.

- Przypadek użycia 3:

  a. Alicja przypisał linię Boba do profili telefonu stacjonarnego i telefonu stacjonarnego.

  b. Alice jest sparowana ze swoim telefonem stacjonarnym za pomocą aplikacji na komputerze.

  c. Bob ma połączenie z Charlie – Alice może zobaczyć trwające połączenie w aplikacji klasycznej.

  d. Bob zawiesza połączenie z Charllem – Alice nie może wznowić połączenia z Charllem z aplikacji klasycznej.

  e. Alicja rozłącza aplikację komputerową z telefonem stacjonarnym – Alicja może wznowić rozmowę z Charliem z aplikacji komputerowej.

```
<config>
<services><calls>
    <call-move>
         <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALL_MOVE_HERE_WXT%	false	prawda, fałsz	Włącza przenoszenie połączeń na urządzeniu lokalnym. Używane do przytrzymywania/wznawiania w różnych lokalizacjach/dla różnych użytkowników w przypadku użycia wielowierszowego.

Informacje poufne firmy Cisco

6.3 Funkcje dostępne tylko na urządzeniach mobilnych

6.3.1 Połączenia alarmowe

Webex dla Cisco BroadWorks obsługuje natywne połączenia alarmowe.

Po włączeniu tej funkcji, podczas nawiązywania połączenia wychodzącego VoIP, aplikacja analizuje wybierany numer i porównuje go z listą skonfigurowanych numerów alarmowych. Jeżeli numer zostanie zidentyfikowany jako alarmowy, aplikacja wykona skonfigurowaną metodę wybierania numeru. Można go skonfigurować za pomocą znacznika *dial-sequence* .

Obsługiwane tryby to:

- tylko cs — klient nawiązuje połączenia alarmowe tylko przez sieć komórkową, jeśli sieć jest dostępna.
- cs-first – Po zainicjowaniu połączenia alarmowego klient sprawdza typ sieci, do której podłączone jest bieżące urządzenie. Jeżeli sieć komórkowa jest dostępna, klient nawiązuje połączenie za pośrednictwem sieci komórkowej. Jeżeli sieć komórkowa nie jest dostępna, ale dostępna jest sieć komórkowa danych/WiFi, klient nawiązuje połączenie za pośrednictwem sieci komórkowej danych/WiFi jako połączenie VoIP. Ponadto jeśli połączenie alarmowe jest nawiązywane za pośrednictwem sieci komórkowej, klient sugeruje użytkownikowi ponowne uruchomienie połączenia alarmowego jako VoIP.
- Tylko voip — klient nawiązuje połączenia alarmowe jako VoIP tylko wtedy, gdy dostępne są dane komórkowe/sieć Wi-Fi.
- cs-voip – Klient analizuje, czy urządzenie może zainicjować je jako natywne połączenie z komutacją obwodów (CS) (bez brania pod uwagę dostępności sieci CS). Jeżeli urządzenie może nawiązać połączenie natywne, numer alarmowy jest wybierany jako połączenie alarmowe CS. W przeciwnym razie połączenie będzie wybierane jako VoIP.

UWAGA: Jeśli połączenia VOIP są wyłączone, jedyną znaczącą wartością sekwencji wybierania alarmowego (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) jest tylko cs.

Podczas logowania użytkownikowi wyświetla się komunikat informujący o wyłączeniu odpowiedzialności za połączenia alarmowe. Nie można tego kontrolować poprzez opcje konfiguracji.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_EMERGENCY_DIALING_WXT%	false	prawda, fałsz	Ustaw na „prawda”, aby włączyć wykrywanie połączeń alarmowych. Wartość domyślna jest pusta.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	tylko cs	Tylko cs-tylko, cs-najpierw, tylko voip-tylko, cs-voip	Steruje trybem sekwencji wybierania numeru dla połączeń alarmowych.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	Lista CSV	Lista numerów alarmowych w formacie CSV. Przykład: 911,112

6.3.2 Powiadomienia wypychane dotyczące połączeń

Gdy odbierane jest połączenie przychodzące, klient mobilny otrzymuje najpierw powiadomienie push (PN). Istnieje parametr konfiguracyjny, który można wykorzystać do kontrolowania, kiedy ma zostać nawiązana sesja SIP REGISTER:

1. Po otrzymaniu powiadomienia push LUB
2. Gdy połączenie zostanie odebrane przez użytkownika.

Zalecane jest drugie podejście. Jednak w porównaniu do pierwszego przypadku, dodaje to pewne opóźnienie przed nawiązaniem połączenia.

Zgodnie z wymaganiami systemu iOS 13, PN VoIP powinny być używane tylko dla połączeń przychodzących. Pozostałe zdarzenia związane z połączeniami powinny używać zwykłych PN.

Aby spełnić ten wymóg, wprowadzono nowy interfejs API rejestracji PN, co wymaga zastosowania odpowiedniej poprawki na serwerze aplikacji. Jeśli zaplecze nie jest skonfigurowane do obsługi systemów iOS 13, parametr konfiguracyjny może być użyty do wymuszania korzystania ze starszych powiadomień push, w których wszystkie zdarzenia związane z połączeniami są dostarczane za pośrednictwem systemów PN systemu VoIP.

Powiadomienie push jest wysyłane przez serwer aplikacji (AS), gdy połączenie zostanie odebrane przez odbiorcę w innej lokalizacji, zamknięte przez osobę dzwoniącą lub na przykład przekierowane do poczty głosowej. W systemie iOS 13 ten typ powiadomień wypychanych jest teraz regularny i zawiera pewne ograniczenia. Wiadomość może zostać opóźniona przez usługę Apple Push Notification Service (APNS) lub w ogóle nie zostać dostarczona. Aby poradzić sobie z brakującymi lub opóźnionymi aktualizacjami połączeń PN, dodano konfigurowalny limit czasu dzwonienia, który pozwala kontrolować maksymalny czas dzwonienia. W przypadku osiągnięcia maksymalnego czasu dzwonienia dzwonienie zostaje przerwane dla odbiorcy, a połączenie traktowane jest jako nieodebrane. Po stronie osoby dzwoniącej połączenie może pozostać w stanie dzwonienia, dopóki nie zostanie wykonana zasada „brak odpowiedzi” skonfigurowana na serwerze aplikacji (AS).

Aby zachować spójność działania aplikacji, konfigurowalny zegar dzwonka ma zastosowanie zarówno w systemach Android, jak i iOS.

Informacje poufne firmy Cisco

Dodano osobną opcję konfiguracji umożliwiającą określenie zachowania w przypadku odrzucenia połączenia, gdy połączenie przychodzące zostanie odebrane w formie powiadomienia push. Klient można skonfigurować tak, aby ignorował połączenie lub odpowiadał na serwer za pośrednictwem Xsi z odrzuceniem ustawionym na „true” (prawda) lub „false” (fałsz). W takim przypadku zostaną zastosowane przypisane usługi przetwarzania połączeń Cisco BroadWorks. Jeżeli skonfigurowano opcję „decline_false”, połączenie będzie kontynuowane, dopóki nadawca nie przerwie połączenia lub nie upłynie czas oczekiwania na odpowiedź, a następnie zostaną uruchomione powiązane usługi obsługi połączeń. Jeżeli skonfigurowano opcję „decline_true”, powód odrzucenia określa przetwarzanie połączenia. Jeżeli powód odrzucenia zostanie ustawiony na „zajęty”, serwer natychmiast wymusza obsługę zajętości. Jeśli skonfigurowano opcję „temp_unavailable”, stosowana jest usługa obsługi sytuacji czasowej niedostępności.

```
<config>
<services>
    <push-notifications-for-calls enabled="true"
    connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
    ring-timeout-seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"/>
    <calls>
        <reject-with-xsi mode="%REJECT_WITH_XSI_MODE_WXT%"
        declineReason="%REJECT_WITH_XSI_DECLINE_REASON_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	prawda, fałsz	Kontroluje, kiedy zostanie nawiązana sesja SIP REGSITER – po otrzymaniu powiadomienia push o połączeniu przychodzącym lub po jego odebraniu.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Kontroluje maksymalny czas dzwonienia dla połączeń przychodzących przez PN. Jeżeli w określonym czasie nie zostanie odebrany żaden numer CallUpd PN, połączenie zostanie uznane za nieodebrane.
%REJECT_WITH_XSI_MODE_WXT%	odrzuć_false	zignoruj, odrzuć_prawdę, odrzuć_fałsz	Określa sposób odrzucania połączeń.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	zajęty	zajęty, temp_niedostępny	Określa powód odrzucenia połączenia, jeżeli tryb odrzucenia jest ustawiony na „decline_true”.

6.3.2.1 MWI

Po włączeniu funkcji MWI klient mobilny Webex subskrybuje powiadomienie push MWI w celu otrzymywania aktualizacji z pocztą głosową użytkownika i powiadamiania go.

Aby ograniczyć liczbę powiadomień i uniknąć niepotrzebnego rozpraszania uwagi, w niektórych przypadkach powiadomienia push MWI są wyłączane. Na przykład gdy użytkownik nasłuchuje wiadomości poczty głosowej lub oznacza je jako przeczytane w kliencie mobilnym Webex (liczba nieprzeczytanych wiadomości maleje). Nie ma konfigurowalnej opcji pozwalającej to kontrolować.

Informacje poufne firmy Cisco

Aby uzyskać więcej informacji o MWI, sprawdź sekcję *6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik wiadomości oczekującej*.

6.3.2.2 Rozprysk pierścieniowy

Usługi BroadWorks (np. DND) mogą wysyłać przypomnienia o dzwonku w przypadku przekierowania połączeń przychodzących. Klient mobilny Webex można skonfigurować w taki sposób, aby włączyć powiadomienia wypychane dzwonkiem i prezentować je użytkownikowi, gdy są wyzwalane przez BroadWorks.

```
config>
<services>
<ring-splash enabled="%ENABLE_RING_SPLASH_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_RING_SPLASH_WXT%	false	prawda, fałsz	Włącza Ring Splash w konfiguracji BroadWorks.

6.3.2.3 Tryb dostarczania (tylko Webex Calling)

Aplikacja Webex korzysta z serwera powiadomień push (NPS) do dostarczania powiadomień push dotyczących połączeń do APNS/FCM. Wersja 45.2 aplikacji Webex obsługuje teraz trzy różne tryby dostarczania, aby skonfigurować sposób dostarczania powiadomień push związanych z połączeniami do APNS/FCM:

- nps - obecny mechanizm, wykorzystujący NPS
- chmura — ulepszony mechanizm, przy użyciu mikrousługi Cisco Webex Cloud
- zewnętrzny - mechanizm wykorzystujący system zewnętrzny. Wymaga integracji systemu innej firmy z silnikiem Cisco WebHooks

```
<config>
<services><calls>
<push-notifications-for-calls enabled="true"
      connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
      ring-timeout-seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"
      delivery-mode="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	n/s	nps, chmura, zewnętrzny	Określa tryb dostarczania powiadomień push dotyczących połączeń.

Informacje poufne firmy Cisco

6.3.3 Pojedyncze alerty

Funkcja Mobile Single Alert jest przeznaczona do wdrożeń obejmujących konwergencję sieci stacjonarnych i mobilnych (FMC) / operatorów sieci komórkowych (MNO) wykorzystujących usługę BroadWorks Mobility. Bez niego po zalogowaniu się do klienta Webex i odebraniu połączenia przychodzącego użytkownik otrzyma jednocześnie dwa połączenia — połączenie natywne i połączenie VoIP (Push Notification). Po włączeniu tej funkcji aplikacja wyłączy powiadomienia o mobilności dotyczące lokalizacji BroadWorks Mobility użytkownika podczas logowania i włączy powiadomienia podczas wylogowywania. Ważnym warunkiem korzystania z tej funkcji jest przypisanie użytkownikowi usługi BroadWorks Mobility i skonfigurowanie dokładnie jednej lokalizacji.

```
<config>
<services><calls>
<single-alerting enabled="%ENABLE_SINGLE_ALERTING_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_SINGLE_ALERTING_WXT%	false	prawda, fałsz	Ustaw na „prawda”, aby włączyć pojedyncze alerty.

6.3.4 Kliknij, aby zadzwonić (oddzwoń)

Usługa Click to Dial (kliknij, aby wybrać numer) umożliwia użytkownikowi końcowemu wykonanie połączenia na osobistym telefonie komórkowym z komutacją obwodów i podanie firmowego numeru kierunkowego jako identyfikatora linii wywołującej.

Klient mobilny Webex obsługuje połączenia typu kliknij, aby wybrać (oddzwonić) przy użyciu usługi BroadWorks Anywhere. Lokalizacje BroadWorks Anywhere w aplikacji Webex są nazywane lokalizacjami zasięgu pojedynczego numeru (SNR).

Po włączeniu tej funkcji użytkownicy mogą wybrać lokalizację SNR z menu parowania urządzeń. Po sparowaniu z lokalizacją SNR wszystkie połączenia wychodzące będą inicjowane za pomocą połączeń typu Kliknij, aby wybrać numer (Oddzwoń). Aby zapobiec podwójnym alertom, powiadomienia push dotyczące połączeń przychodzących są wyłączone.

Gdy użytkownik zainicjuje połączenie „Kliknij, aby wybrać numer”, zobaczy ekran połączenia wychodzącego z informacją, że może spodziewać się połączenia przychodzącego w wybranej lokalizacji SNR. Ekran ten zamyka się automatycznie zgodnie z konfigurowalnym timerem.

Po rozłączeniu się z lokalizacją SNR aplikacja rejestruje się ponownie w celu otrzymywania powiadomień push o połączeniach przychodzących.

```
<config>
<services>
  <dialing>
    <call-back enabled="%ENABLE_DIALING_CALL_BACK_WXT%"
timer="%DIALING_CALL_BACK_TIMER_WXT%"/>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_DIALING_CALL_BACK_WXT%	false	prawda, fałsz	Ustaw na „true”, aby włączyć funkcję „Kliknij, aby wybrać numer (oddzwonić).
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Kontroluje liczbę sekund, po których ekran Oddzwaniania zostanie automatycznie zamknięty.

6.3.5 Obsługa MNO

6.3.5.1 Zadzwoń za pomocą natywnego dialera

Funkcja ta dodaje obsługę wdrożeń u operatorów sieci komórkowych (MNO) wykorzystujących usługę BroadWorks Mobility (BWM). Zakłada się, że użytkownikowi przypisana jest usługa BroadWorks Mobility i że skonfigurowano co najmniej jedną lokalizację.

Możliwość inicjowania połączeń przez użytkownika za pomocą natywnego dialera jest kontrolowana przez tag konfiguracji **natywnej** . Jeżeli ta opcja jest włączona, aplikacja uruchomi natywny dialer i nawiąże połączenie. Ponadto dostępność połączeń VoIP jest kontrolowana przez znacznik **voip** – w zależności od wymagań wdrożenia połączenia VoIP mogą być włączane lub wyłączane.

Jeśli włączone są VoIP i połączenia natywne, użytkownik będzie mógł wybrać, z której opcji chce skorzystać.

Znacznik określa, czy użytkownicy mogą wybrać sposób nawiązywania/odbierania połączeń przychodzących i wychodzących. Wymaga włączenia zarówno połączeń natywnych, jak i połączeń VoIP.

Począwszy od wersji 43.12, rozszerzona jest natywna konfiguracja wybierania, zapewniając możliwość wstępnego wstawiania niestandardowego prefiksu do numeru połączenia wychodzącego. Dotyczy to połączeń komórkowych inicjowanych z aplikacji Webex tylko wtedy, gdy wybrany numer rozpoczyna się kodem FAC.

Ta funkcja jest przydatna dla klientów korzystających z wdrożeń MNO, w których połączenia zamiast przekierowywać do zintegrowanego serwera aplikacji Cisco BroadWorks, kody FAC mogą być obsługiwane przez zaplecze Telecom. Nowy znacznik zostanie dodany w sekcji i mogą go użyć do rozwiązania tego problemu przez telekomunikacje.

```
<config>
<services>
  <dialing>
    <voip enabled="%ENABLE_DIALING_VOIP_WXT%"/>
    <native enabled="%ENABLE_DIALING_NATIVE_WXT%" enable-bwks-mobility-
dependency="%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%">
      <fac-prefix value="%DIALING_NATIVE_FAC_PREFIX_WXT%"/>
    </native>
    <dialing-mode enabled="%ENABLE_DIALING_MODE_WXT%" default="%DIALING_MODE_DEFAULT_WXT%"/>
```


Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_DIALING_VOIP_WXT%	true	prawda, fałsz	Ustaw na „true”, aby włączyć opcję połączeń VoIP.
%ENABLE_DIALING_NATIVE_WXT%	false	prawda, fałsz	Ustaw wartość „true” (prawda), aby włączyć opcję połączeń macierzystych.
%ENABLE_DIALING_MODE_WXT%	false	prawda, fałsz	Umożliwia użytkownikowi wybór trybu wykonywania połączeń za pomocą Ustawień połączeń w Preferencjach.
%DIALING_MODE_DEFAULT_WXT%	voip	voip, natywny	Określa wybrany domyślny tryb wywoływania.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false	prawda, fałsz	Określa, czy dostępność połączeń natywnych powinna zależeć od przypisania usługi BroadWorks Mobility i lokalizacji mobilności skonfigurowanej dla użytkownika.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*puste*	struna	Określa prefiks, który należy dodać na początku, jeśli połączenie wychodzące na numer rozpoczynający się od kodu FAC jest inicjowane jako połączenie komórkowe. Domyślnie prefiks FAC nie jest zdefiniowany i tag jest pusty.

UWAGA 1: Co najmniej jedna z funkcji połączeń **VoIP** i **natywnych** powinna być włączona.

UWAGA 2: Jeśli w sieciach MNO włączone jest tylko wywołanie **natywne** , zaleca się wyłączenie pojedynczego alertu, aby zapobiec wyłączeniu alertów BWM przez klienta.

UWAGA 3: Jeśli włączone są zarówno połączenia **natywne** , jak i **VoIP** , w przypadku wdrożeń MNO zaleca się włączenie pojedynczego alertu, aby zapobiec podwójnym alertom.

6.3.5.2 Elementy sterujące w trakcie połączenia

Ta funkcja umożliwia klientowi mobilnemu Webex sterowanie za pośrednictwem natywnych połączeń XSI na urządzeniu przenośnym, które są zakotwiczone w Cisco BroadWorks. Sterowanie połączeniami XSI jest dostępne tylko wtedy, gdy:

- Usługa BroadWorks Mobility (BWM) jest przypisana do użytkownika,
- Skonfigurowano tylko jedną tożsamość mobilną BMW,
- Tryb połączeń natywnych jest wybierany przez użytkownika (więcej informacji można znaleźć w sekcji *6.3.5.1 Zadzwoń za pomocą natywnego* dialera*),*
- Istnieje połączenie zakotwiczone w BroadWorks, przechodzące przez serwis BMW,
- Trwa połączenie komórkowe na urządzeniu mobilnym.

Informacje poufne firmy Cisco

Wersja 43.10 dodaje lepszą obsługę przekazywania konsultacyjnego, tworząc powiązanie między dwoma połączeniami komórkowymi przedstawionymi w aplikacji Webex i udostępniając użytkownikowi opcję ukończenia przekazywania. Ponadto, jeśli użytkownik realizuje dwa niezależne połączenia komórkowe na tym samym urządzeniu, menu transferu zostaje rozszerzone o możliwość przekierowania jednego połączenia do drugiego, nawet jeśli nie utworzono między nimi żadnego powiązania.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_XSI_CALL_CONTROL_WXT%	false	prawda, fałsz	Włącza kontrolę połączeń XSI dla środowiska MNO.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	Dostęp MNO	Dostęp_MNO, Sieć_MNO	Kontroluje typ wdrożenia XSI MNO używany przez aplikację. Możliwe wartości to: ▪ MNO_Access – pokazuje wszystkie zdalne wywołania (XSI) z typami urządzeń zdefiniowanymi w węźle poniżej. ▪ MNO_Network – pokazuje wszystkie połączenia zdalne (XSI).
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	struna	Nazwy typów urządzeń, które powinny zostać użyte w typie wdrożenia MNO_Access.
%ENABLE_XSI_HOLD_CALLS_WXT%	true	prawda, fałsz	Określa, czy akcja Wstrzymaj połączenie powinna być dostępna dla użytkownika w przypadku połączeń komórkowych XSI.

6.3.5.3 Tożsamość linii połączeń wychodzących (CLID) — podwójna tożsamość

W wersji mobilnej 42.12 aplikacja Webex umożliwia użytkownikom wybranie tożsamości linii połączeń (CLID) przedstawianej stronie zdalnej po zainicjowaniu połączenia wychodzącego.

Jeśli użytkownik ma skonfigurowaną usługę Cisco BroadWorks Mobility, typową konfigurację dla wdrożeń operatora sieci komórkowej (MNO) i włączona jest usługa połączeń natywnych, użytkownik może wybrać tożsamość, która ma być prezentowana dzwoniącym osobom. Użytkownik może wybrać swoją tożsamość biznesową lub osobistą. Dostępna jest również opcja ukrycia własnej tożsamości i wyświetlania rozmowy jako anonimowej.

W przypadku połączeń VoIP użytkownik ma również możliwość kontrolowania swojego CLID. W tym przypadku jedyną dostępną opcją jest kontrola nad tym, czy ukryć swoją tożsamość, czy nie.

Zarządzanie personami i blokowanie CLID są kontrolowane poprzez oddzielne opcje konfiguracji.

```
<config>
```


Informacje poufne firmy Cisco

```
<services>
<dialing>
   <calling-line-id-delivery-blocking
enabled="%ENABLE_CLID_DELIVERY_BLOCKING_WXT%"/>
   <mobility-persona-management
enabled="%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	false	prawda, fałsz	Włącza blokowanie dostarczania identyfikatora abonenta dzwoniącego. Dotyczy wszystkich typów połączeń wychodzących danego użytkownika.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	false	prawda, fałsz	Umożliwia zarządzanie osobiste połączeniami natywnymi, gdy typ wdrożenia jest skonfigurowany jako MNO_Access lub MNO_Network. (Do połączeń natywnych używany jest BroadWorks Mobility, a wszystkie połączenia natywne są zakotwiczone w BroadWorks)

6.3.5.4 Powiadomienie o połączeniach natywnych

W przypadku użytkowników wdrożonych z MNO ta funkcja dodaje baner powiadomień dla połączeń macierzystych, który można sterować za pomocą aplikacji Webex. To powiadomienie jest oparte na powiadomieniu wypychanym wysyłanym przez serwer aplikacji po nawiązaniu połączenia.

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	true	prawda, fałsz	Włącza subskrypcję powiadomienia push MOBILE_CALL_INFO.

6.3.5.5 Przenieś połączenie natywne do spotkania konwergentnego

W przypadku użytkowników wdrożonych z MNO ta funkcja umożliwia eskalację natywnego połączenia głosowego do spotkania dla obu stron połączenia 1:1 (nawet jeśli druga strona nie jest użytkownikiem Webex). Jeśli użytkownik zdalny jest użytkownikiem Webex, po zakończeniu spotkania strony będą miały możliwość:

- Inicjuj usługę Webex w ramach czatu spotkania
- Dodaj wideo (pamiętaj, że dźwięk będzie kontynuowany w wywołaniu natywnym)
- Udostępnij ekran / treść

Informacje poufne firmy Cisco

- Nagrywanie spotkań Trigger

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	prawda, fałsz	Włącza funkcję Power Up (akcje Zaproś i Spotkaj, Spotkanie wideo).

6.3.5.6 Mobilność MNO — widget w trakcie połączenia

Wersja 43.7 aplikacji Android Webex (mobilna i tablet) oficjalnie wprowadza nowy widget sterowania połączeniami (bańka), zapewniający dodatkowe sterowanie połączeniami dla połączeń natywnych zakotwiczonych w Cisco BroadWorks przy użyciu usługi Mobility. Widżet będzie wyświetlany na górze natywnego interfejsu użytkownika i umożliwi użytkownikowi wykonywanie następujących czynności:

- Wstrzymanie/Wznowienie
- Przekazanie bez konsultacji/bez konsultacji — umieszcza użytkownika w oknie dialogowym przenoszenia w aplikacji Webex.
- Complete Transfer – umożliwia ukończenie transferu konsultacyjnego (wydanie 43.10)
- Spotkanie wideo — przenosi uczestników do spotkania Webex.
- Zakończ połączenie

```
<config>
<services><calls>
       <hold xsi-enabled="%ENABLE_XSI_HOLD_CALLS_WXT%" widget-
enabled="%ENABLE_WIDGET_HOLD_CALLS_WXT%"/>
       <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%" xsi-
enabled="%ENABLE_XSI_TRANSFER_CALLS_WXT%" widget-
enabled="%ENABLE_WIDGET_TRANSFER_CALLS_WXT%" type="%TRANSFER_CALL_TYPE_WXT%"/>
       <escalate-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%" widget-
enabled="%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_WIDGET_HOLD_CALLS_WXT%	true	prawda, fałsz	Steruje dostępnością akcji Wstrzymaj w widżecie połączeń.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	true	prawda, fałsz	Kontroluje dostępność czynności Przekaż i Zakończ przekazywanie w widżecie połączenia.

Informacje poufne firmy Cisco

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	true	prawda, fałsz	Kontroluje dostępność czynności Spotkanie wideo w widżecie połączenia.

6.3.6 Identyfikator dzwoniącego w połączeniu przychodzącym

Wersja 44.2 dodaje możliwość kontrolowania informacji kontaktowych prezentowanych użytkownikowi na podstawie nazwy i numeru. Dodano dwie opcje konfiguracji umożliwiające kontrolowanie informacji prezentowanych użytkownikowi na ekranie połączenia przychodzącego, w powiadomieniach o połączeniach przychodzących oraz w powiadomieniach o nieodebranych połączeniach.

6.3.6.1 Ekran połączenia przychodzącego

Istnieją różnice platformowe między systemami Android i iOS, jeśli chodzi o wyświetlanie danych na ekranie połączenia przychodzącego. Wyświetlanie informacji o połączeniach przychodzących wygląda następująco:

Android — na ekranie połączenia przychodzącego znajdują się dwa oddzielne pola zawierające zarówno nazwę, jak i numer

iOS — istnieje tylko jedno pole, w którym wyświetlana jest nazwa lub numer — jeśli są dostępne, nazwa ma priorytet

Nowa opcja konfiguracji połączeń przychodzących może zostać użyta, aby upewnić się, że aplikacja Webex na ekranie połączenia będzie wyświetlana numer obok nazwy (format: *Nazwa (Numer)*). Zachowanie aplikacji Webex dla systemu Android nie ma wpływu.

6.3.6.2 Powiadomienie o połączeniu przychodzącym

W niektórych przypadkach połączenie przychodzące jest wyświetlane użytkownikowi w formie powiadomienia. Ze względu na ograniczoną ilość miejsca numer ten nie zawsze jest tam wyświetlany.

Nowa opcja konfiguracji połączeń przychodzących kontroluje również informacje wyświetlane w powiadomieniach o połączeniach przychodzących. Jeśli ta opcja jest włączona, a zarówno nazwa, jak i numer są dostępne, aplikacja Webex doda numer obok nazwy (format: *Nazwa (Numer)*). To zachowanie aplikacji Webex ma zastosowanie zarówno w systemach Android, jak i iOS.

Informacje poufne firmy Cisco

6.3.6.3 Powiadomienie o nieodebranym połączeniu

Dodano dodatkowy parametr konfiguracji dla powiadomień o nieodebranych połączeniach. Można go używać do kontrolowania informacji o zdalnym użytkowniku, podobnie jak w przypadku powiadomień o połączeniach przychodzących. Umożliwia on dołączenie numeru do wyświetlanej nazwy zdalnego użytkownika i wyświetlanie go w powiadomieniu o nieodebranym połączeniu. To zachowanie aplikacji Webex ma zastosowanie zarówno w systemach Android, jak i iOS.

```
<config>
<services><calls>
   <caller-id>
      <incoming-calls>
         <append-number enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
      </incoming-calls>
      <missed-calls>
         <append-number enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
      </missed-calls>
```

Znacznik	Domyślnie, jeśli pominięto	Obsługiwane wartości	Opis
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false	prawda, fałsz	Określa, czy numer powinien być dołączany do nazwy na ekranie połączenia przychodzącego (tylko w systemie iOS) oraz w powiadomieniach.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	false	prawda, fałsz	Określa, czy numer powinien zostać dołączony do nazwy w powiadomieniu o nieodebranym połączeniu.

UWAGA: Jeśli numer zostanie dostarczony jako nazwa wyświetlana lub nazwa wyświetlana kończy się cyframi, aplikacja Webex uniknie powielania i wyświetli numer tylko raz.

Informacje poufne firmy Cisco

7 Wczesne funkcje wersji próbnej (BETA)

W WERSJI BETA najnowszej wersji nie ma żadnych funkcji.

Informacje poufne firmy Cisco

8 Mapowanie znaczników niestandardowych między Webex dla Cisco BroadWorks i UC-One

W poniższej tabeli wymieniono tagi niestandardowe Webex dla Cisco BroadWorks, zgodne z ich starszymi tagami niestandardowymi dla UC-One.

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	nd.	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	nd.	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	nd.	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	nd.
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	nd.
%ENABLE_CALL_STATISTICS_WXT%	nd.	nd.
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N/A	%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%MWI_MODE_WXT%	%DESKTOP_MWI_MODE%	%MWI_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	N/A	nd.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	nd.
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	nd.
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	nd.
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	nd.	nd.
%ENABLE_BROADWORKS_ANYWHERE_WXT%	nd.	nd.

Informacje poufne firmy Cisco

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	nd.	nd.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	nd.	nd.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	nd.	nd.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	nd.	nd.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	nd.	nd.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	nd.	nd.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	nd.	nd.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	nd.	nd.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	nd.	nd.
%ENABLE_EMERGENCY_DIALING_WXT%	nd.	nd.
%EMERGENCY_DIALING_NUMBERS_WXT%	nd.	nd.
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	nd.	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	nd.
%SBC_ADDRESS_WXT%	%SBC_ADDRESS%	%SBC_ADDRESS%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILE%
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	nd.
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	nd.

Informacje poufne firmy Cisco

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%USE_TLS_FROM_DNS_WXT%	%USE_TLS_FROM_DNS%	nd.
%DOMAIN_OVERRIDE_WXT%	%DOMAIN_OVERRIDE%	%DOMAIN_OVERRIDE%
%SOURCE_PORT_WXT%	%SOURCE_PORT%	%SOURCE_PORT%
%USE_ALTERNATIVE_IDENTITIES_WXT%	%USE_ALTERNATIVE_IDENTITIES%	nd.
%TCP_SIZE_THRESHOLD_WXT%	%TCP_SIZE_THRESHOLD%	nd.
%SIP_REFRESH_ON_TTL_WXT%	%SIP_REFRESH_ON_TTL%	nd.
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	%ENABLE_SIP_UPDATE_SUPPORT_MOBILE%
%ENABLE_PEM_SUPPORT_WXT%	%ENABLE_PEM_SUPPORT_DESKTOP%	nd.
%ENABLE_SIP_SESSION_ID_WXT%	nd.	nd.
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	nd.	nd.
%SRTP_ENABLED_WXT%	%USE_SRTP%	%SRTP_ENABLED_MOBILE%
%SRTP_MODE_WXT%	%SRTP_PREFERENCE%	%SRTP_MODE_MOBILE%
%ENABLE_REKEYING_WXT%	%ENABLE_RE_KEYING_DESKTOP%	%ENABLE_RE-KEYING_MOBILE%
%RTP_AUDIO_PORT_RANGE_START_WXT%	%RTP_AUDIO_PORT_RANGE_START%	%RTP_AUDIO_PORT_RANGE_START%
%RTP_AUDIO_PORT_RANGE_END_WXT%	%RTP_AUDIO_PORT_RANGE_END%	%RTP_AUDIO_PORT_RANGE_END%
%RTP_VIDEO_PORT_RANGE_START_WXT%	%RTP_VIDEO_PORT_RANGE_START%	%RTP_VIDEO_PORT_RANGE_START%
%RTP_VIDEO_PORT_RANGE_END_WXT%	%RTP_VIDEO_PORT_RANGE_END%	%RTP_VIDEO_PORT_RANGE_END%
%ENABLE_RTCP_MUX_WXT%	%ENABLE_RTCP_MUX%	%ENABLE_RTCP_MUX%
%ENABLE_XSI_EVENT_CHANNEL_WXT%	%ENABLE_XSI_EVENT_CHANNEL%	nd.
%CHANNEL_HEARTBEAT_WXT%	%CHANNEL_HEARTBEAT%	%CHANNEL_HEARTBEAT_MOBILE%
%XSI_ROOT_WXT%	%XSI_ROOT%	%XSI_ROOT%
%XSI_ACTIONS_PATH_WXT%	nd.	%XSI_ACTIONS_PATH_MOBILE%
%XSI_EVENTS_PATH_WXT%	nd.	%XSI_EVENTS_PATH_MOBILE%

Informacje poufne firmy Cisco

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%ENABLE_CALLS_AUTO_ RECOVERY_WXT%	nd.	%ENABLE_CALLS_AUTO_ RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_ SEQUENCE_WXT%	nd.	%EMERGENCY_CALL_DIAL_ SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLI ND_WXT%	nd.	nd.
%ENABLE_CALL_PICKUP_ DIRECTED_WXT%	nd.	nd.
%WEB_CALL_SETTINGS_URL _WXT%	nd.	%WEB_CALL_SETTINGS_URL %
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP %
%ENABLE_CALL_CENTER_ WXT%	%ENABLE_CALL_CENTER_ DESKTOP%"	nd.
%WEB_CALL_SETTINGS_TAR GET_WXT%	nd.	nd.
%WEB_CALL_SETTINGS_CFA _ VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_CFA _VISIBLE%
%WEB_CALL_SETTINGS_DN D_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_DN D_VISIBLE%
%WEB_CALL_SETTINGS_AC R_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_AC R_VISIBLE%
%WEB_CALL_SETTINGS_CFB _VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_CFB _VISIBLE%
%WEB_CALL_SETTINGS_CFN R_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_CFN R_VISIBLE%
%WEB_CALL_SETTINGS_CFN A_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_CFN A_VISIBLE%
%WEB_CALL_SETTINGS_SIM RING_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_SIM RING_VISIBLE%
%WEB_CALL_SETTINGS_ SEQRING_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_SE QRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_ VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_RO_ VISIBLE%
%WEB_CALL_SETTINGS_ACB _VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_ACB _VISIBLE%
%WEB_CALL_SETTINGS_CW _VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_CW _VISIBLE%
%WEB_CALL_SETTINGS_CLI DB_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_CLI DB_VISIBLE%
%WEB_CALL_SETTINGS_PA_ VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_PA_ VISIBLE%

Informacje poufne firmy Cisco

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_BWA_VISIBLE%
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	nd.	%WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE%
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_BWM_VISIBLE%
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	nd.	%WEB_CALL_SETTINGS_VM_VISIBLE%
%ENABLE_DIALING_CALL_BACK_WXT%	nd.	nd.
%DIALING_CALL_BACK_TIMER_WXT%	nd.	nd.
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	nd.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	nd.	%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_MOBILE%
%ENABLE_CALL_RECORDING_WXT%	%ENABLE_CALL_RECORDING_DESKTOP%	%CALL_RECORDING_MOBILE%
%ENABLE_SINGLE_ALERTING_WXT%	nd.	%ENABLE_SINGLE_ALERTING%
%ENABLE_CALL_PARK_WXT%	%ENABLE_CALL_PARK_DESKTOP%	nd.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	nd.	nd.
%ENABLE_RTP_ICE_WXT%	nd.	nd.
%RTP_ICE_MODE_WXT%	nd.	nd.
%RTP_ICE_SERVICE_URI_WXT%	nd.	nd.
%RTP_ICE_PORT_WXT%	nd.	nd.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	nd.	nd.
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	nd.	nd.
%ENABLE_DIALING_VOIP_WXT%	nd.	nd.
%ENABLE_DIALING_NATIVE_WXT%	nd.	nd.
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	nd.	nd.
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	nd.	nd.

Informacje poufne firmy Cisco

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	nd.	nd.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	nd.	nd.
%USER_PORTAL_SETTINGS_URL_WXT%	nd.	nd.
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	nd.	nd.
%ENABLE_AUDIO_MARI_FEC_WXT%	nd.	nd.
%ENABLE_AUDIO_MARI_RTX_WXT%	nd.	nd.
%ENABLE_VIDEO_MARI_FEC_WXT%	nd.	nd.
%ENABLE_VIDEO_MARI_RTX_WXT%	nd.	nd.
%ENABLE_CALL_BLOCK_WXT%	nd.	nd.
%ENABLE_WIDGET_HOLD_CALLS_WXT%	nd.	nd.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	nd.	nd.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	nd.	nd.
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	nd.	nd.
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	nd.	nd.
%ENABLE_CALL_MOVE_HERE_WXT%	nd.	nd.
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	nd.	nd.
%DIALING_NATIVE_FAC_PREFIX_WXT%	nd.	nd.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	nd.	nd.
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	nd.	nd.
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	nd.	nd.

Informacje poufne firmy Cisco

Znacznik Webex dla Cisco BroadWorks	Tag starszej wersji pulpitu	Etykieta Mobile Legacy
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	nd.	nd.
%ENABLE_CLID_OUTGOING_CALLS_WXT%	nd.	nd.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	nd.	nd.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	nd.	nd.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	nd.	nd.
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	nd.	nd.
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	nd.	nd.
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	nd.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	nd.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	nd.	nd.
%ENABLE_GCP_NOTIFICATIONS_WXT%	nd.	nd.
%ENABLE_GCP_DISPLAY_CALLER_WXT%	nd.	nd.
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	nd.	nd.
%UDP_KEEPALIVE_ENABLED_WXT%	nd.	nd.
%TCP_KEEPALIVE_ENABLED_WXT%	nd.	nd.
%TLS_KEEPALIVE_ENABLED_WXT%	nd.	nd.
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	nd.	nd.
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	nd.	nd.

Informacje poufne firmy Cisco

UWAGA: N/A oznacza, że w UC-One nie było odpowiedniego niestandardowego znacznika kontrolującego tę funkcję. Posiadanie nd. dla starszych tagów zarówno pulpitu, jak i urządzeń przenośnych wskazuje, że znacznik Webex dla Cisco BroadWorks jest nowy i steruje nowymi funkcjami lub istniejącymi funkcjami, które nie były kontrolowane za pomocą niestandardowego znacznika w UC-One.

Informacje poufne firmy Cisco

9 Załącznik A: Szyfry TLS

Klient Webex for BroadWorks używa protokołu CiscoSSL, który bazuje na protokole OpenSSL z dodatkowym zabezpieczeniem.

Informacje poufne firmy Cisco

10 Załącznik B: Skrypt dostarczania tagów DM

Liczba niestandardowych tagów DM zwiększała się z każdą wersją, ponieważ wielu klientów preferowało tagi dla nowych parametrów konfiguracji. Aby ułatwić tworzenie mechanizmów dostarczania niestandardowych tagów DM, ta sekcja zawiera skrypt, który można uruchomić po stronie serwera aplikacji (AS) w celu przypisania wartości do niestandardowych tagów DM. Ten skrypt jest przeznaczony w szczególności do nowych wdrożeń, w których zamierza się używać większości niestandardowych tagów DM.

Należy pamiętać, że ten skrypt jest prawidłowy tylko w przypadku nowych wdrożeń, w których tworzone są niestandardowe tagi DM. Aby zmodyfikować istniejące niestandardowe tagi DM, polecenie w poniższym skrypcie należy zmienić z „add” na „set”.

Szablon skryptu zawierający tylko kilka niestandardowych tagów (podczas rzeczywistego wdrożenia konieczne byłoby utworzenie większej listy niestandardowych tagów). Należy pamiętać, że poniższy przykład dotyczy wersji mobilnej. W przypadku komputerów stacjonarnych należy używać zestawu tagów BroadTouch_tags zamiast Connect_Tags. W przypadku tabletu należy użyć zestawu tagów ConnectTablet_Tags zamiast Connect_Tags.

```
%% ********************************** Connect_Tags - read file **********************************
%%
%% Instructions:
%% -------------------
%% - This read file can be used to create, add and set Webex for BroadWorks
%% client custom tags
%% - Use %% to comment out any steps not required based on deployment specific
%% service requirements:
%% Step 1 -- for new deployments only, create initial tag set label
%% Step 2 -- add a new custom tag (an entry is required for each new tag)
%% Step 3 -- set value for an existing custom tag (entry required for each applicable tag)
%% Step 4 -- display and visually verify tag settings
%%
%% - Edit, modify file as needed respecting command syntax. Save file (e.g. WxT_Tags.txt)
%% - SFTP read file to AS under directory /tmp
%% - Login to AS, bwcli (login as admin)
%% - Execute the following command from bwcli: AS_CLI> r /tmp/ WxT_Tags.txt
%% - Verify results
%%
%% ----------------------------------------------------------------------------------------------------------------
%% Step 1: Create Connect tag set label - Connect_Tags
%% ----------------------------------------------------------------------------------------------------------------
quit all;System;DeviceTagSet
add Connect_Tags
%% ----------------------------------------------------------------------------------------------------------------
%% Step 2: Add WxT for BWKS custom tags
%% EXAMPLE – for all mobile tags see the list below-----------------------------------------------------
quit all;System;DeviceTagSet;Tags
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% true
%% ----------------------------------------------------------------------------------------------------------------
%% Step 3: Set Connect custom tags (if tag already exists)
%% EXAMPLE – for all mobile tags see the list below
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------------------------------------------------------------------------------------------------------------
%% Step 4: Verify custom tags have been correctly defined and set
%% ----------------------------------------------------------------------------------------------------------------
```


Informacje poufne firmy Cisco

```
quit all;System;DeviceTagSet;Tags
get tagSetName Connect_Tags
quit all
```

Poniżej znajduje się lista wszystkich znaczników niestandardowych używanych przez Webex dla Cisco BroadWorks, z wartościami przykładowymi (domyślnymi lub zalecanymi). Należy pamiętać, że niektóre tagi wymagają wartości specyficznych dla danego wdrożenia (np. adresy serwerów). Dlatego te znaczniki dodaje się na końcu skryptu, ale pozostawia się je puste. Aby je określić, należy dodać dodatkowe polecenia set.

10.1 Pulpit

```
add tagSetName BroadTouch_tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_WXT% true
add tagSetName BroadTouch_tags %BLF_NOTIFICATION_DELAY_TIME_WXT% 0
add tagSetName BroadTouch_tags %ENABLE_REMOTE_CONTROL_EVENTS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName BroadTouch_tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName BroadTouch_tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName BroadTouch_tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PULL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MWI_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
false
add tagSetName BroadTouch_tags %ENABLE_USE_RPORT_WXT% false
add tagSetName BroadTouch_tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName BroadTouch_tags %USE_TLS_WXT% false
add tagSetName BroadTouch_tags %SBC_PORT_WXT% 5075
add tagSetName BroadTouch_tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName BroadTouch_tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName BroadTouch_tags %SOURCE_PORT_WXT% 5060
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
```


Informacje poufne firmy Cisco

```
add tagSetName BroadTouch_tags %SIP_FAILBACK_ENABLED_WXT% true
add tagSetName BroadTouch_tags %SIP_FAILBACK_TIMEOUT_WXT% 900
add tagSetName BroadTouch_tags %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName BroadTouch_tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_WXT% false
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName BroadTouch_tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName BroadTouch_tags %SRTP_ENABLED_WXT% false
add tagSetName BroadTouch_tags %SRTP_MODE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REKEYING_WXT% true
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName BroadTouch_tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName BroadTouch_tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName BroadTouch_tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName BroadTouch_tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName BroadTouch_tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName BroadTouch_tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName BroadTouch_tags %USE_MEDIASEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_URL_WXT%
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_BLIND_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_DIRECTED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% true
add tagSetName BroadTouch_tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
```


Informacje poufne firmy Cisco

```
add tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PARK_WXT% false
add tagSetName BroadTouch_tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
add tagSetName BroadTouch_tags %RTP_ICE_PORT_WXT% 3478
add tagSetName BroadTouch_tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName BroadTouch_tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID_WXT% true
add tagSetName BroadTouch_tags %XSI_ROOT_WXT% true
add tagSetName BroadTouch_tags %SBC_ADDRESS_WXT% true
add tagSetName BroadTouch_tags %SBC_PORT_WXT% true
add tagSetName BroadTouch_tags %MWI_MODE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName BroadTouch_tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUTO_ANSWER_WXT% false
add tagSetName BroadTouch_tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName BroadTouch_tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName BroadTouch_tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName BroadTouch_tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName BroadTouch_tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REMOTE_MUTE_CONTROL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName BroadTouch_tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_MOVE_HERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_NOTIFICATIONS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_DISPLAY_CALLER_WXT% false
add tagSetName BroadTouch_tags %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% 120
add tagSetName BroadTouch_tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName BroadTouch_tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName BroadTouch_tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```

10.2 Mobilna

```
add tagSetName Connect_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
```


Informacje poufne firmy Cisco

```
add tagSetName Connect_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName Connect_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName Connect_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName Connect_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName Connect_Tags %ENABLE_MWI_WXT% false
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName Connect_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName Connect_Tags %USE_TLS_WXT% false
add tagSetName Connect_Tags %SBC_PORT_WXT% 5075
add tagSetName Connect_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName Connect_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName Connect_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName Connect_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName Connect_Tags %SOURCE_PORT_WXT% 5060
add tagSetName Connect_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName Connect_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName Connect_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName Connect_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName Connect_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName Connect_Tags %SRTP_ENABLED_WXT% false
add tagSetName Connect_Tags %SRTP_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_REKEYING_WXT% true
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName Connect_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName Connect_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName Connect_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName Connect_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName Connect_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName Connect_Tags %USE_MEDIASEC_WXT% false
add tagSetName Connect_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName Connect_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
```


Informacje poufne firmy Cisco

```
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName Connect_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName Connect_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName Connect_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName Connect_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName Connect_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName Connect_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName Connect_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName Connect_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName Connect_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName Connect_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName Connect_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName Connect_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName Connect_Tags %XSI_ROOT_WXT% true
add tagSetName Connect_Tags %SBC_ADDRESS_WXT% true
add tagSetName Connect_Tags %SBC_PORT_WXT% true
add tagSetName Connect_Tags %MWI_MODE_WXT% true
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName Connect_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
```


Informacje poufne firmy Cisco

```
add tagSetName Connect_Tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName Connect_Tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% false
add tagSetName Connect_Tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT% once_per_login
add tagSetName Connect_Tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_DELIVERY_BLOCKING_WXT% false
add tagSetName Connect_Tags %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT% false
add tagSetName Connect_Tags %ENABLE_RING_SPLASH_WXT% false
add tagSetName Connect_Tags %ENABLE_PN_MOBILE_CALL_INFO_WXT% true
add tagSetName Connect_Tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName Connect_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName Connect_Tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName Connect_Tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName Connect_Tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName Connect_Tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName Connect_Tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName Connect_Tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName Connect_Tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName Connect_Tags %ENABLE_WIDGET_HOLD_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_WIDGET_TRANSFER_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% true
add tagSetName Connect_Tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName Connect_Tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName Connect_Tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName Connect_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName Connect_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName Connect_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName Connect_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName Connect_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName Connect_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName Connect_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName Connect_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName Connect_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```

10.3 Tablet

```
add tagSetName ConnectTablet_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName ConnectTablet_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
```


Informacje poufne firmy Cisco

```
add tagSetName ConnectTablet_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_MWI_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%
false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName ConnectTablet_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName ConnectTablet_Tags %USE_TLS_WXT% false
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% 5075
add tagSetName ConnectTablet_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName ConnectTablet_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName ConnectTablet_Tags %SOURCE_PORT_WXT% 5060
add tagSetName ConnectTablet_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName ConnectTablet_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName ConnectTablet_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_REKEYING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName ConnectTablet_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName ConnectTablet_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName ConnectTablet_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName ConnectTablet_Tags %USE_MEDIASEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
```


Informacje poufne firmy Cisco

```
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName ConnectTablet_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName ConnectTablet_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName ConnectTablet_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName ConnectTablet_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName ConnectTablet_Tags %XSI_ROOT_WXT% true
add tagSetName ConnectTablet_Tags %SBC_ADDRESS_WXT% true
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% true
add tagSetName ConnectTablet_Tags %MWI_MODE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
```


Informacje poufne firmy Cisco

```
add tagSetName ConnectTablet_Tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName ConnectTablet_Tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName ConnectTablet_Tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RING_SPLASH_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PN_MOBILE_CALL_INFO_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName ConnectTablet_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName ConnectTablet_Tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName ConnectTablet_Tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_TRANSFER_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName ConnectTablet_Tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName ConnectTablet_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName ConnectTablet_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName ConnectTablet_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```

10.4 Znaczniki systemowe

Poniżej znajduje się lista tagów systemowych używanych przez Webex dla BroadWorks.

```
%BWNETWORK-CONFERENCE-SIPURI-n%
%BWVOICE-PORTAL-NUMBER-n%
%BWLINEPORT-n%
%BWHOST-n%
%BWAUTHUSER-n%
%BWAUTHPASSWORD-n%
%BWE164-n%
%BWNAME-n%
%BWEXTENSION-n%
```


Informacje poufne firmy Cisco

%BWAPPEARANCE-LABEL-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMARY%
%BWE911-PRIMARY-HELDURL%
%BWE911-CUSTOMERID%
%BWE911-SECRETKEY%
%BWE911-EMERGENCY-NUMBER-LIST%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%

Informacje poufne firmy Cisco

11 Akronimy i skróty

W tej sekcji wymieniono akronimy i skróty używane w niniejszym dokumencie. Akronimy i skróty podano w kolejności alfabetycznej wraz z ich znaczeniem.

ACB	Automatyczne połączenie zwrotne
ACD	Automatyczna dystrybucja połączeń
ACR	Odrzucanie połączeń anonimowych
AES	Zaawansowany standard szyfrowania
ALG	Brama warstwy aplikacji
API	Interfejs programowania aplikacji
APK	Pakiet aplikacji
APNS	Usługa powiadomień push Apple
ARS	Automatyczny wybór szybkości transmisji danych
AS	Serwer aplikacji (Cisco BroadWorks)
AVP	Profil wizualny audio
BW	BroadWorks
BWA	BroadWorks Anywhere
BWKS	BroadWorks
BWM	BroadWorks Mobility
BYOD	Przynieś własne urządzenie
CC	Centrum połączeń
CFB	Przekazywanie połączeń Zajęte
CFNA	Przekazywanie połączeń Bez odpowiedzi
CFNR	Niedostępne przekierowywanie połączeń
CIF	Wspólny format pośredni
CLI	Interfejs wiersza poleceń
CLID	Tożsamość linii wywołującej
CLIDB	Blokowanie dostarczania identyfikatora linii wywołującej
CRLF	Podawanie na linii powrotnej wózka
CS	Przełącznik
CSWV	Widok sieci WWW Ustawienia połączeń
CW	Połączenia oczekujące
DB	Baza danych
DM	Zarządzanie urządzeniami
DND	Nie przeszkadzać
DNS	System nazw domen

Informacje poufne firmy Cisco

DPC	Sterowanie telefonem stacjonarnym
DTAF	Typ urządzenia Plik archiwum
ECACS	Usługa zmiany adresu połączeń alarmowych
FMC	Konwergencja stacjonarna-mobilna
FQDN	W pełni kwalifikowana nazwa domeny
HMAC	Kod uwierzytelniania wiadomości skrótu
ICE	Ustanowienie interaktywnych połączeń sieciowych
iLBC	kodek internetowy o niskiej szybkości transmisji danych
IM	Wiadomości błyskawiczne
IM&P	Wiadomości błyskawiczne i informacje o obecności
IOT	Testy współdziałania
IP	Protokół internetowy
JID	Identyfikator Jabber
M/O	Obowiązkowe/opcjonalne
MNO	Operator sieci komórkowej
MTU	Maksymalna jednostka transmisyjna
MUC	Czat dla wielu użytkowników
MWI	Wskaźnik oczekującej wiadomości
NAL	Warstwa abstrakcji sieci
NAPTR	Wskaźnik uprawnień nadawania nazw
NAT	Translacja adresów sieciowych
OTT	Na górze
PA	Asystent osobisty
PAI	Tożsamość potwierdzona przez P
PEM	P-Early Media
PLI	Wskazanie utraty obrazu
PLMN	Publiczna lądowa sieć komórkowa
PN	Powiadomienie wypychane
QCIF	Czwarty wspólny format pośredni
QoS	Jakość usług
RO	Zdalne biuro
RTCP	Protokół sterowania w czasie rzeczywistym
RTP	Protokół czasu rzeczywistego
SaaS	Oprogramowanie jako usługa
SAN	Nazwa alternatywna podmiotu
SASL	Proste uwierzytelnianie i warstwa zabezpieczeń

Informacje poufne firmy Cisco

SAVP	Bezpieczny profil audio i wideo
SBC	Kontroler graniczny sesji
SCA	Wygląd połączenia udostępnionego
SCF	Funkcja ciągłości sesji
SCTP	Protokół transmisji sterowania strumieniem
SDP	Protokół definicji sesji
SEQRING	Sekwencyjne wywoływanie połączeń
SIMRING	Jednoczesne wywoływanie połączeń
SIP	Protokół inicjowania sesji
SNR	Stosunek sygnału do szumu
SNR	Zasięg pojedynczego numeru
SRTCP	Protokół bezpiecznej kontroli w czasie rzeczywistym
SRTP	Bezpieczny protokół transportu w czasie rzeczywistym
SSL	Warstwa bezpiecznych gniazd
STUN	Narzędzia przechodzenia sesji dla usługi NAT
SUBQCIF	Podkwartał CIF
TCP	Protokół sterowania transmisją
TLS	Zabezpieczenia warstwy transportowej
TTL	Czas żyć
TURN	Przechodzenie przy użyciu usługi NAT przekazywania
UDP	Protokół danych użytkownika
UI	Interfejs użytkownika
UMS	Serwer wiadomości (Cisco BroadWorks)
URI	Jednolity identyfikator zasobu
UVS	Serwer wideo (Cisco BroadWorks)
VGA	Video Graphics Array
VoIP	Głos przez IP (VoIP)
VVM	Wizualna poczta głosowa
WXT	Webex
XMPP	Rozszerzalny protokół przesyłania wiadomości i obecności
XR	Raport rozszerzony
Xsp	Platforma usług rozszerzonych
Xsi	Interfejs usług rozszerzonych

Informacje poufne firmy Cisco