Przewodnik konfiguracji Webex dla Cisco BroadWorks

Wersja 45.4

Wersja dokumentu 1

Spis treści

1 Podsumowanie zmian 1
1.1 Zmiany w wersji 45.4, kwiecień 2025 r. 1
1.2 Zmiany w wersji 45.3, marzec 2025 r. 1
1.3 Zmiany w wersji 45.2, luty 2025 r. 1
1.4 Zmiany w wersji 45.1, styczeń 2025 r. 1
1.5 Zmiany w wersji 44.12 z grudnia 2024 r. 1
1.6 Zmiany w wersji 44.11, listopad 2024 r. 1
1.7 Zmiany w wersji 44.10, październik 2024 r. 1
1.8 Zmiany w wersji 44.9, wrzesień 2024 r. 2
1.9 Zmiany w wersji 44.8, sierpień 2024 r. 2
1.10 Zmiany w wersji 44.7, lipiec 2024 r. 2
1.11 Zmiany w wersji 44.6, czerwiec 2024 r. 2
1.12 Zmiany w wersji 44.5, maj 2024 r. 2
1.13 Zmiany w wersji 44.4, kwiecień 2024 r. 2
1.14 Zmiany w wersji 44.3, marzec 2024 r. 2
1.15 Zmiany w wersji 44.2, luty 2024 r. 3
1.16 Zmiany w wersji 44.1 ze stycznia 2024 r. 3
2 Zmiany dotyczące plików konfiguracyjnych 4
2.1 Zmiany w plikach konfiguracyjnych dla wersji 45.4 4
2.2 Zmiany w plikach konfiguracyjnych dla wersji 45.3 4
2.3 Zmiany w plikach konfiguracyjnych dla wersji 45.2 4
2.4 Zmiany w plikach konfiguracyjnych dla wersji 45.1 4
2.5 Zmiany w plikach konfiguracyjnych dla wersji 44.12 4
2.6 Zmiany w plikach konfiguracyjnych dla wersji 44.11 4
2.7 Zmiany w plikach konfiguracyjnych dla wersji 44.10 5
2.8 Zmiany w plikach konfiguracyjnych dla wersji 44.9 5
2.9 Zmiany w plikach konfiguracyjnych dla wersji 44.8 5
2.10 Zmiany dotyczące plików konfiguracyjnych dla wersji 44.7 5
2.11 Zmiany dotyczące plików konfiguracyjnych dla wersji 44.6 5
2.12 Zmiany w plikach konfiguracyjnych dla wersji 44.5 6
2.13 Zmiany w plikach konfiguracyjnych dla wersji 44.4 6
2.14 Zmiany w plikach konfiguracyjnych dla wersji 44.3 6
2.15 Zmiany w plikach konfiguracyjnych dla wersji 44.2 7
2.16 Zmiany dotyczące plików konfiguracyjnych dla wersji 44.1 9
3 Wprowadzenie 10
4 Instalacja 11
4.1 Pobieranie zlokalizowanego klienta 11
4.2 Klient systemu Android 11
4.3 Klient iOS 11

Poufne informacje Cisco

4.4 Klient stacjonarny ... 11
5 Zarządzanie urządzeniami ... 12
5.1 Tagi zarządzania urządzeniami ... 12
5.2 Ulepszenia dopasowania częściowego przy wyborze typu urządzenia ... 13
5.3 Konfiguracja klienta ... 14
5.4 Rozmieszczenie config-wxt.xml ... 14
5.5 Plik konfiguracyjny (config-wxt.xml) ... 14
5.6 Domyślne znaczniki systemowe ... 15
5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks ... 15
6 Tagi niestandardowe ... 18
6.1 Cechy wspólne ... 31
6.1.1 Ustawienia serwera SIP ... 31
6.1.2 SIP Over TLS i bezpieczny protokół transportu w czasie rzeczywistym ... 34
6.1.3 Nagłówki SIP 3GPP dla SRTP ... 36
6.1.4 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania aktywności ... 37
6.1.5 Konfigurowalny limit czasu otwarcia gniazda SIP ... 39
6.1.6 Wykrywanie dynamicznych serwerów proxy SIP ... 40
6.1.7 Preferowane użycie portu dla SIP ... 45
6.1.8 Przełączanie awaryjne SIP i powrót po awarii ... 46
6.1.9 SIP SUBCSRIBE i REGISTER Odśwież i SUBSKRYBUJ Ponów próbę ... 51
6.1.10 Użyj P-Associated-URI w REGISTER ... 52
6.1.11 Nagłówek SIP P-Early Media (PEM) ... 52
6.1.12 Obsługa aktualizacji SIP ... 53
6.1.13 Starsze informacje o SIP FIR ... 53
6.1.14 Zarządzanie portami SIP dla przechodzenia translacji adresów sieciowych ... 54
6.1.15 SIP Session ID (Identyfikator sesji SIP) ... 55
6.1.16 Odrzucanie połączeń przychodzących ... 55
6.1.17 Zakres portów protokołu transportowego w czasie rzeczywistym ... 56
6.1.18 Obsługa ICE(tylko Webex Calling) ... 56
6.1.19 RTCP MUX ... 57
6.1.20 Przenoszenie ... 58
6.1.21 N-Way połączenia konferencyjne i uczestnicy ... 59
6.1.22 Ściąganie połączeń ... 60
6.1.23 Wywołanie Parkuj/Odzyskaj ... 60
6.1.24 Statystyki połączeń ... 61
6.1.25 Automatyczne przywracanie połączeń/bezproblemowe przekazywanie połączeń ... 61
6.1.26 Nagrywanie rozmów ... 62
6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik oczekujących wiadomości ... 63
6.1.28 Transkrypcja poczty głosowej dla Webex Calling ... 65
6.1.29 Ustawienia połączeń ... 65
6.1.30 Portal ustawień i internetowe ustawienia połączeń ... 68

Poufne informacje Cisco

6.1.31 Call Center / Logowanie / Wylogowanie z kolejki połączeń ... 72
6.1.32 Katalog główny XSI i ścieżki ... 72
6.1.33 Kanał zdarzeń XSI ... 73
6.1.34 Konfiguracja kodeka ... 74
6.1.35 Wybieranie numerów SIP-URI ... 76
6.1.36 Historia połączeń na wszystkich urządzeniach ... 77
6.1.37 Wyłączanie połączeń wideo ... 77
6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji przez dostawcę E911 ... 78
6.1.39 PAI jako tożsamość ... 80
6.1.40 Wyłącz współdzielenie ekranu ... 80
6.1.41 Wskazanie połączenia spamowego ... 81
6.1.42 Usuwanie szumów i zwiększanie przepustowości dla połączeń PSTN/komórkowych 81
6.1.43 Oznaczenie DSCP QoS ... 82
6.1.44 Profil podstawowy ... 83
6.1.45 Lista zablokowanych (tylko Webex Calling) ... 84
6.1.46 Adaptacja do mediów i wdrażanie odporności (MARI) ... 85
6.1.47 Jednoczesne połączenia z tym samym użytkownikiem ... 87
6.1.48 RTCP-XR ... 88
6.1.49 Informacje o przekierowywaniu połączeń ... 88
6.1.50 ID abonenta dzwoniącego ... 89
6.1.51 Obsługa wielu linii ... 92
6.1.52 Rozszerzona autoryzacja SIP ... 93
6.1.53 Osobisty asystent (obecność poza domem) ... 94
6.2 Funkcje tylko dla komputerów stacjonarnych ... 96
6.2.1 Wymuszone wylogowanie ... 96
6.2.2 Przejmowanie połączeń ... 97
6.2.3 Wsparcie Boss-Admin (Executive-Assistant) ... 97
6.2.4 Eskaluj połączenia SIP do Meeting (tylko Webex Calling) ... 98
6.2.5 Sterowanie telefonem biurkowym — automatyczne odbieranie ... 98
6.2.6 Automatyczne odbieranie z powiadomieniem tonowym ... 99
6.2.7 Sterowanie telefonem biurkowym — elementy sterujące w trakcie połączenia — konferencja ... 99
6.2.8 Powiadomienia o przejmowaniu połączeń ... 100
6.2.9 Pakiet zdarzeń zdalnego sterowania ... 102
6.2.10 Wybór identyfikatora CLID agenta kolejki połączeń ... 103
6.2.11 Survivability Gateway (tylko Webex Calling) ... 103
6.2.12 Pakiet zdarzeń zdalnego wyciszenia (tylko Webex Calling) ... 104
6.2.13 Przenoszenie połączenia ... 105
6.3 Funkcje dostępne tylko dla urządzeń przenośnych ... 107
6.3.1 Połączenia alarmowe ... 107
6.3.2 Powiadomienia push o połączeniach ... 108
6.3.3 Alert pojedynczy ... 111

Poufne informacje Cisco

6.3.4 Kliknij, aby zadzwonić (Oddzwoń) ... 111
6.3.5 Obsługa MNO ... 112
6.3.6 Identyfikator rozmówcy przychodzącego ... 117
7 Funkcje BETA (Early Field Trial) ... 119
8 Mapowanie tagów niestandardowych między Webex dla Cisco BroadWorks i UC-One ... 120
9 Dodatek A: Szyfry TLS ... 128
10 Dodatek B: Skrypt inicjowania obsługi tagów DM ... 129
10.1 Pulpit ... 130
10.2 Komórkowy ... 133
10.3 Tablet ... 135
10.4 Tagi systemowe ... 138
11 Akronimy i skróty ... 140

Poufne informacje Cisco

1 Podsumowanie zmian

W tej sekcji opisano zmiany wprowadzone w tym dokumencie dla każdej wersji i wersji dokumentu.

1.1 Zmiany w wersji 45.4, kwiecień 2025 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Przeniesiona sekcja *6.1.34.1 Kodek AI* – poza wersją BETA.
- Dodano sekcję *6.1.51 Obsługa* wielu linii – połączono sekcje BETA tylko na komputery stacjonarne i mobilne.
- Przeniesiona sekcja *6.1.52 Rozszerzona autoryzacja SIP* – poza wersją BETA.
- Przeniesiono sekcję *6.1.53 Osobisty asystent (obecność poza* domem) jako typową dla komputerów i urządzeń mobilnych

1.2 Zmiany w wersji 45.3, marzec 2025 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.3 Zmiany w wersji 45.2, luty 2025 r.

Ta wersja dokumentu zawiera następujące zmiany:

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

1.4 Zmiany w wersji 45.1, styczeń 2025 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Przeniesiono sekcję *Osobisty asystent (obecność poza* domem) z wersji BETA.
- Przeniesiono sekcję *6.3.2.3 Sposób dostawy (tylko Webex Calling)* z wersji BETA.

1.5 Zmiany w wersji 44.12 z grudnia 2024 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.6 Zmiany w wersji 44.11, listopad 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

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

1.7 Zmiany w wersji 44.10, październik 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Dodano sekcję *Osobisty asystent (obecność poza* domem) w wersji BETA***Error! Reference source not found.***.
- Dodano sekcję *Sposób dostawy (tylko Webex Calling)* w wersji BETA.

Poufne informacje Cisco

1.8 Zmiany w wersji 44.9, wrzesień 2024 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

1.9 Zmiany w wersji 44.8, sierpień 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Zaktualizowana sekcja *6.1.34 Konfiguracja kodeka* – dodano wyjaśnienia dotyczące DTMF i obsługiwanych mechanizmów realizacji.

1.10 Zmiany w wersji 44.7, lipiec 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

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

1.11 Zmiany w wersji 44.6, czerwiec 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Zaktualizowana sekcja *6.3.6. Identyfikator rozmówcy przychodzącego* - Dodano więcej szczegółów na temat natywnego doświadczenia i sposobu działania tej funkcji.

1.12 Zmiany w wersji 44.5, maj 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Zaktualizowana sekcja *6.1.18 Obsługa ICE(tylko Webex Calling)* – dodano obsługę IPv6 przez NAT64.
- Zaktualizowana sekcja *6.1.50 ID abonenta* dzwoniącego - dodano podsekcję *6.1.50.2 Nazwa identyfikatora zdalnego rozmówcy*.

1.13 Zmiany w wersji 44.4, kwiecień 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Zaktualizowana sekcja *6.1.50.1 Identyfikator rozmówcy wychodzącego*.
- Zaktualizowana sekcja *Zmiany w plikach konfiguracyjnych dla wersji 44.3* – dodano szczegóły dotyczące aktualizacji w wersji 44.3.

1.14 Zmiany w wersji 44.3, marzec 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Zaktualizowana sekcja *6.3.6. Identyfikator rozmówcy przychodzącego*
    - Przeniesiono sekcję *6.1.50.1 Identyfikator rozmówcy wychodzącego* jako typową dla komputerów i urządzeń mobilnych i zaktualizowano ją o więcej szczegółów.
- Zaktualizowana sekcja *6.1.4 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania* aktywności – dodano szczegóły dotyczące konfigurowalnych pamiątek za pomocą niestandardowych tagów.

Poufne informacje Cisco

1.15 Zmiany w wersji 44.2, luty 2024 r.

Ta wersja dokumentu zawiera następujące zmiany:

- Dodano sekcję *6.3.6 Identyfikator rozmówcy przychodzącego*
- Zaktualizowana sekcja *6.2.8 Powiadomienia o przejmowaniu* połączeń
  - Dodano podsekcję *6.2.8.1 Pole sygnalizacji aktywności* linii - przeniesiono w niej BLF szczegóły.
  - Dodano podsekcję *6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)*.
- Dodano sekcję *6.1.49 Informacje o przekierowywaniu* połączeń.
- Zaktualizowana sekcja *6.1.8.3 Wymuszanie wersji IP* – dodano szczegóły dla nowego *trybu nat64* .
- Zaktualizowana sekcja *6.1.42 Usuwanie szumów i zwiększanie przepustowości dla połączeń PSTN/komórkowych* - dodano szczegóły dotyczące nowej obsługi rozszerzenia przepustowości i aktualizacji usuwania szumów. Sekcja *Ulepszenia mowy dla połączeń* PSTN została usunięta z wersji beta.

1.16 Zmiany w wersji 44.1 ze stycznia 2024 r.

W tym wydaniu nie wprowadzono żadnych zmian w tym dokumencie.

Poufne informacje Cisco

2 Zmiany dotyczące plików konfiguracyjnych

2.1 Zmiany w plikach konfiguracyjnych dla wersji 45.4

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

2.2 Zmiany w plikach konfiguracyjnych dla wersji 45.3

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

2.3 Zmiany w plikach konfiguracyjnych dla wersji 45.2

- [Funkcja BETA]
  Dodano znacznik <enhanced-authorization> w sekcji <protocols><sip>.

```
<config>
<protokoły>
  <łyk>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Dodano następujący %TAG%:

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.4 Zmiany w plikach konfiguracyjnych dla wersji 45.1

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

2.5 Zmiany w plikach konfiguracyjnych dla wersji 44.12

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

2.6 Zmiany w plikach konfiguracyjnych dla wersji 44.11

- [Funkcja BETA] [Tylko dla urządzeń przenośnych] [Tylko Webex Calling]
  Dodano atrybut multi-line enabled w tagu <protocols><sip><lines>.
  Dodano sekcje <osobiste> i <wiersz> dla linii pomocniczych w sekcji <protokoły><sip><linie>.

```
<config>
<protokoły><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
   <osobiste>
      <port-linii>%BWDISPLAYNAMELINEPORT%</port-linii>
   </osobiste>
   <line lineType="%BW-MEMBERTYPE-1%">
      …
   </linia>
   <line lineType="%BW-MEMBERTYPE-2%">
      …
   </linia>
   …
   <line lineType="%BW-MEMBERTYPE-10%">
      …
   </linia>
</linie>
```


Poufne informacje Cisco

2.7 Zmiany w plikach konfiguracyjnych dla wersji 44.10

- [Funkcja BETA]
  Dodano znacznik <asystent-osobisty> w sekcji <usługi>.

```
<config>
<usługi>
   <Asystent-osobisty włączony="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

- [Funkcja BETA] [Tylko dla urządzeń przenośnych] [Tylko Webex Calling]
  Dodano atrybut delivery-mode pod tagiem <services><push-notifications-for-calls>.

```
<config>
<usługi>
   <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 następujący %TAG%s:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.8 Zmiany w plikach konfiguracyjnych dla wersji 44.9

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

2.9 Zmiany w plikach konfiguracyjnych dla wersji 44.8

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

2.10 Zmiany dotyczące plików konfiguracyjnych dla wersji 44.7

- [Funkcja BETA]
  Dodano kodek AI (xCodec) w sekcji <usługi><połączenia><audio><kodeki>.

```
<config>
<usługi><połączenia>
  <audio>
    <kodeki>
      <nazwa kodeka="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=""/>
      <nazwa kodeka="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="phone-event" payload="101" in-band="false"/>
```

2.11 Zmiany dotyczące plików konfiguracyjnych dla wersji 44.6

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

Poufne informacje Cisco

2.12 Zmiany w plikach konfiguracyjnych dla wersji 44.5

- [Tylko Webex Calling]
  Dodano atrybut enable-ipv6-support do znacznika <protocols><rtp><ice>.

```
<config>
<protokoły><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 <zdalna-nazwa> został dodany w sekcji <services><calls><caller-id> z <machine> jako podznacznikiem.

```
<config>
<usługi><połączenia>
   <identyfikator dzwoniącego>
      <nazwa-zdalna>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Dodano następujący %TAG%s:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.13 Zmiany w plikach konfiguracyjnych dla wersji 44.4

- [Tylko komputery stacjonarne] [Tylko Webex Calling]
  Dodano tagi <numery-dodatkowe>, <grupa-wyszukiwania> i <blokowanie-dostarczania> w sekcji <identyfikator-dzwoniącego><połączenia wychodzące>.

```
<config>
<usługi><połączenia>
  <identyfikator dzwoniącego>
    <Połączenia wychodzące włączone="%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%"/>
    </połączenia wychodzące>
```

2.14 Zmiany w plikach konfiguracyjnych dla wersji 44.3

- [Tylko komputery stacjonarne] [Tylko Webex Calling]
  Dodano <połączenia wychodzące> w nowej sekcji <identyfikator-dzwoniącego> z podtagiem <call-center>.

```
<config>
<usługi><połączenia>
  <identyfikator dzwoniącego>
    <Połączenia wychodzące włączone="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
    </połączenia wychodzące>
```


Poufne informacje Cisco

- Dodano niestandardowe tagi (%UDP_KEEPALIVE_ENABLED_WXT%, %TCP_KEEPALIVE_ENABLED_WXT% i %TLS_KEEPALIVE_ENABLED_WXT%) zastępujące zakodowaną na stałe wartość włączoną dla każdego transportu w ramach <protocols><sip><transports>.

```
<config>
<protokoły><sip>
<transporty>
  <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 następujący %TAG%s:

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

2.15 Zmiany w plikach konfiguracyjnych dla wersji 44.2

- [Tylko dla urządzeń przenośnych]
  Dodano sekcję <identyfikator-dzwoniącego> w sekcji <services><calls>. Dodano podtagi <połączenie przychodzące> i <nieodebrane połączenie> z nowym podtagiem <numer-dołączenia> dla obu.

```
<config>
<usługi><połączenia>
  <identyfikator dzwoniącego>
    <połączenia przychodzące>
      <append-number
enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
    </połączenia przychodzące>
    <Nieodebrane połączenia>
      <append-number
enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
    </nieodebrane połączenia>
```

- [Tylko dla urządzeń przenośnych] [Tylko Webex Calling]
  Dodano <połączenia wychodzące> w nowej sekcji <identyfikator-dzwoniącego>.

```
<config>
<usługi><połączenia>
  <identyfikator dzwoniącego>
    <Połączenia wychodzące włączone="%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%"/>
```


Poufne informacje Cisco

```
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </połączenia wychodzące>
```

- Dodano znacznik <call-forwarding-info> w sekcji <services><calls>.

```
<config>
<usługi><połączenia>
  <call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

- [Tylko komputery stacjonarne] [Tylko Webex Calling]
  Dodano sekcję <grupa-powiadomienia-o przejęciu-połączeniach> w sekcji <usługi><połączenia>, z <display-caller> i <max-timeout> jako tagami podrzędnymi. Dodano także znacznik <group-call-pickup> pod każdym znacznikiem <line> w sekcji <protocols><sip><lines>.

```
<config>
<usługi><połączenia>
  <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%"/>
  </grupowe powiadomienia o odebraniu połączenia>
  …
<protokoły><sip>
  <linie>
    <linia>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
      ...
    </linia>
    <linia>
      <grupowe-przejmowanie-połączeń>%BWGROUP-CALL-PICKUP-BOOL-2%</group-
call-pickup>
      ...
    </linia>
    …
```

Dodano następujący %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%

Poufne informacje Cisco

Następujący %TAG% został wycofany:

- %ENABLE_NOISE_REMOVAL_WXT%

2.16 Zmiany dotyczące plików konfiguracyjnych dla wersji 44.1

W plikach konfiguracyjnych dla tej wersji nie było żadnych aktualizacji.

Poufne informacje Cisco

3 Wprowadzenie

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

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

Klienci są konfigurowani za pomocą konfiguracji, która nie jest widoczna dla użytkownika końcowego. config-wxt.xml zawiera informacje specyficzne dla serwera, takie jak adresy i porty serwera oraz opcje środowiska wykonawczego dla samego klienta (na przykład opcje widoczne na *ekranie Ustawienia*).

Pliki konfiguracyjne są odczytywane przez klienta w momencie jego uruchomienia, po pobraniu ich z Zarządzanie urządzeniami. Informacje z plików konfiguracyjnych są przechowywane w postaci zaszyfrowanej, co czyni je niewidocznymi i niedostępnymi dla użytkownika końcowego.

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

Poufne informacje Cisco

4 Instalacja

Webex klientów Cisco BroadWorks można zainstalować z następujących elementów:

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

4.1 Pobieranie zlokalizowanego klienta

Następujące zlokalizowane wersje Webex dla klientów 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 systemu Android

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

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

Po pobraniu nowej wersji stare oprogramowanie jest zastępowane; Jednak dane użytkownika są zachowywane domyślnie.

Należy pamiętać, że użytkownik nie musi wybierać żadnych opcji instalacji lub dezinstalacji.

4.3 Klient iOS

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

Istnieje kontrola wersji oparta na procedurach Apple App Store. Ikona App Store jest podświetlona, aby wskazać, że dostępna jest nowa wersja oprogramowania.

Po pobraniu nowej wersji stare oprogramowanie jest zastępowane; Jednak dane użytkownika są zachowywane domyślnie.

Należy pamiętać, że użytkownik nie musi wybierać żadnych opcji instalacji lub dezinstalacji.

4.4 Klient stacjonarny

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

Poufne informacje Cisco

5 Zarządzanie urządzeniami

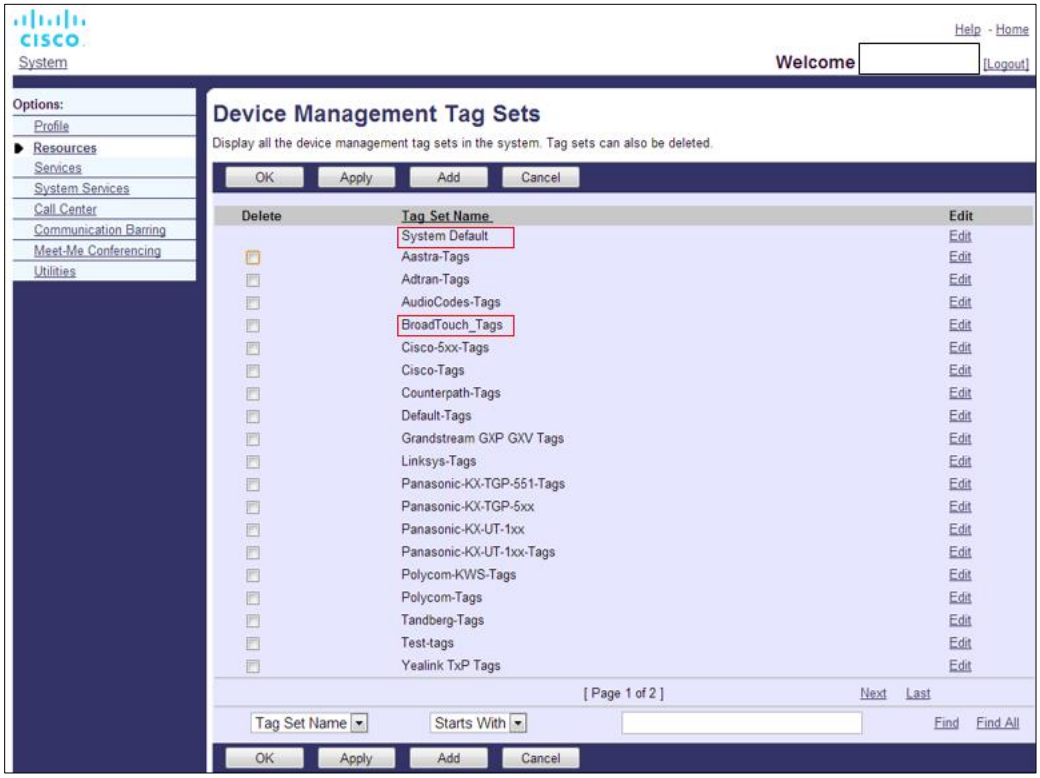
5.1 Tagi zarządzania urządzeniami

Webex Cisco BroadWorks korzysta *zZestawy tagów* zarządzania urządzeniami pokazano na poniższym rysunku. Domyślne ustawienia systemowe i niestandardowe są wymagane do obsługi określonych ustawień urządzenia/klienta. Ten zestaw tagów zapewnia elastyczność w zarządzaniu ustawieniami łączności sieci/usługi klienta, a także kontrolkami aktywacji funkcji.

Ten niestandardowy zestaw tagów jest udostępniany przez administratora systemu za pomocą *opcji System → Resources*→ Device Management Tag Sets (Zestawy tagów *zarządzania systememZasobyurządzenie*). Administrator musi dodać nowe zestawy znaczników:

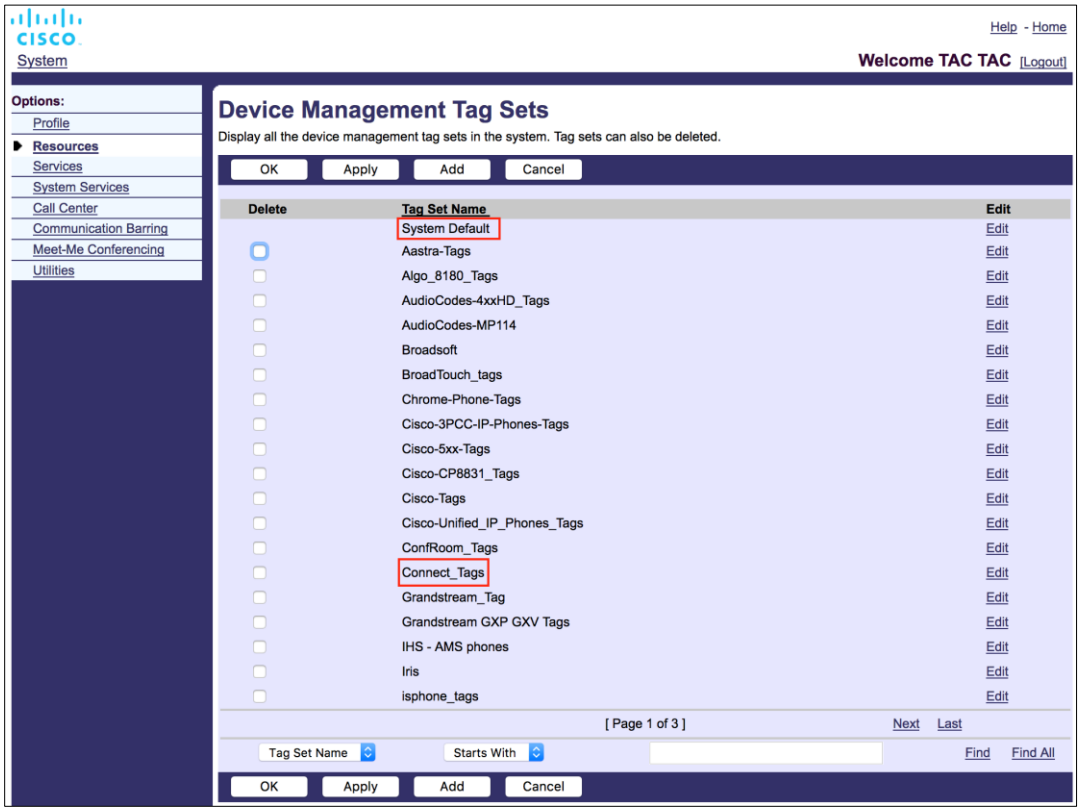
- Telefon komórkowy: Connect_Tags
- Tabletka: ConnectTablet_Tags
- Pulpit: BroadTouch_Tags

Utwórz każdy tag i ustaw jego wartość. Odwołania do sekcji zawierają szczegółowe opisy poszczególnych tagów. Tagi niestandardowe są podzielone na grupy w zależności od funkcji i omówione w dalszej części tego dokumentu.



Zestawy 1 tagów zarządzania urządzeniami stacjonarnymi

Poufne informacje Cisco



Rysunek 2 Zestawy tagów zarządzania urządzeniami mobilnymi

5.2 Ulepszenia dopasowania częściowego przy wyborze typu urządzenia

Aby zapewnić większą elastyczność przy wyborze pakietów funkcji dla grup użytkowników lub poszczególnych użytkowników, typ profilu urządzenia jest wybierany 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. Nosi nazwę "Business Communicator – PC" dla komputerów stacjonarnych, "Connect - Mobile" dla urządzeń przenośnych i "Connect - Tablet" dla tabletów. Profil urządzenia można utworzyć i przypisać do użytkownika. Następnie serwer aplikacji tworzy plik konfiguracyjny i zapisuje go na serwerze profili.

Podczas logowania klient wysyła zapytanie do przypisanej listy urządzeń za pośrednictwem Xsi i wyszukuje odpowiedni profil typu urządzenia. Klient wybiera pierwszy profil, który zaczyna się od odpowiedniej nazwy typu urządzenia. Następnie dane konfiguracyjne profilu urządzenia (plik konfiguracyjny) skojarzony z tym profilem urządzenia są używane do włączania i wyłączania różnych funkcji.

Dzięki temu ten sam plik wykonywalny klienta może być używany z różnymi typami profili urządzeń, dzięki czemu usługodawca może zmieniać pakiety funkcji dla poszczególnych użytkowników lub grup użytkowników, po prostu zmieniając typ profilu urządzenia w DM dla użytkownika lub grupy użytkowników.

Poufne informacje Cisco

Na przykład usługodawca może mieć dowolną liczbę typów profili urządzeń na podstawie ról użytkowników, takich jak "Business Communicator – PC Basic", "Business Communicator – PC Executive" lub "Business Communicator – PC Assistant" i zmieniać funkcje dostępne dla poszczególnych użytkowników, zmieniając dla nich typ profilu urządzenia.

Należy pamiętać, że nie oczekuje się, że na liście odebranych urządzeń znajdzie się wiele pasujących typów profilów urządzeń, XML ale tylko jeden.

5.3 Konfiguracja klienta

Wersja Webex klienta Cisco BroadWorks wykorzystuje *plik config-wxt.xml* do konfiguracji funkcji wywoływania. Istnieje osobna procedura konfiguracji dla Webex, która nie została omówiona w tym dokumencie.

5.4 Rozmieszczenie config-wxt.xml

Dodaj odpowiedni *plik config-wxt.xml* do profili urządzeń "Connect – Mobile", "Connect – Tablet" i "Business Communicator – PC". Webex dla Cisco BroadWorks używa tych samych profili urządzeń co UC-One, aby ułatwić wdrażanie.

UWAGA 1: Dla każdego profilu urządzenia musi istnieć plik konfiguracyjny.

UWAGA 2: WYSOCE ZALECA się, aby szablony były aktualizowane o najnowszą wersję aplikacji Webex

5.5 Plik konfiguracyjny (config-wxt.xml)

Nowe tagi niestandardowe z **sufiksem_WXT** służą do odróżniania nowego Webex wdrażania konfiguracji Cisco BroadWorks od starszych klientów. Jednak nadal istnieją pewne tagi (systemowe), które są współużytkowane między UC-One i Webex.

Niektóre niestandardowe tagi systemu Cisco BroadWorks są również używane w pliku konfiguracyjnym *config-wxt.xml* . Aby uzyskać więcej informacji na temat każdego z poniższych tagów, zobacz sekcję *5.7 Dynamiczne wbudowane znaczniki systemowe* Cisco BroadWorks.

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

Poufne informacje Cisco

- %BWLINEPORT-PRIMARY%
- %BWE911-GŁÓWNY-HELDURL%
- %BWE911-CUSTOMERID%
- %BWE911-SECRETKEY%
- %BWE911-LISTA-NUMERÓW-ALARMOWYCH%
- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (tylko Webex Calling)

5.6 Domyślne znaczniki systemowe

Administrator systemu może uzyskać dostęp do domyślnych tagów systemowych za pomocą *opcji System*→ Resources → Device Management Tag Sets (Zestawy tagów *zarządzania* systemem). Podczas instalowania pakietu VoIP Calling należy udostępnić następujące domyślne tagi systemowe.

Znacznik	Opis
%SBC_ADDRESS_WXT%	Należy ją 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%	Jeśli SBC_ADDRESS_WXT jest adresem IP, ten parametr powinien być ustawiony na port SBC. Jeśli SBC_ADDRESS_WXT jest nazwą FQDN, można ją pozostawić nieustawioną. Przykład: 5075

5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks

Oprócz domyślnych tagów systemowych i tagów niestandardowych, które muszą zostać zdefiniowane, istnieją znaczniki systemowe Cisco BroadWorks, które są zwykle używane i stanowią część zalecanego pliku archiwum typu urządzenia (DTAF). Tagi te są wymienione w tej sekcji. W zależności od zainstalowanego pakietu rozwiązania nie wszystkie tagi systemowe są używane.

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

Poufne informacje Cisco

Znacznik	Opis
%BWHOST-n%	Jest to część domeny aprowizowanego portu linii dla urządzenia przypisanego do użytkownika. Jest on pobierany z profilu użytkownika. Zazwyczaj używany jako domena SIP.
%BWAUTHUSER-n%	Jest to nazwa użytkownika uwierzytelniania. Jeśli subskrybentowi przypisano uwierzytelnianie, jest to udostępniony identyfikator użytkownika na stronie Uwierzytelnianie, niezależnie od wybranego trybu uwierzytelniania danego typu urządzenia. Nazwa użytkownika SIP, zwykle używana w sygnalizacji 401 i 407. Może różnić się od domyślnej nazwy użytkownika SIP.
%BWAUTHPASSWORD-n%	Jest to hasło uwierzytelniające użytkownika. Jeśli subskrybentowi przypisano uwierzytelnianie, jest to hasło inicjowane na stronie Uwierzytelnianie, niezależnie od wybranej wartości trybu uwierzytelniania typu urządzenia. Hasło SIP używane w sygnalizacji SIP.
%BWE164-n%	Ten tag zawiera numer telefonu użytkownika w formacie międzynarodowym.
%BWNAME-n%	Jest to imię i nazwisko subskrybenta w profilu użytkownika. Imię i nazwisko są ze sobą połączone. W przypadku konfiguracji wielowierszowej, jeśli nie skonfigurowano etykiety linii i jeśli nie jest pusta, należy użyć jako nazwy wyświetlanej linii w selektorze linii.
%BWEXTENSION-n%	Numer wewnętrzny subskrybenta jest pobierany z rozszerzenia udostępnionego w profilu użytkownika. Jeśli numer wewnętrzny nie został podany, tag zostanie zastąpiony numerem telefonu abonenta.
%BWAPPEARANCE-LABEL-n%	Jest to skonfigurowana etykieta linii. Używana jako nazwa wiersza, jeśli nie jest pusta.
%BWDISPLAYNAMELINEPORT%	Jest to linia/port pierwszej linii prywatnej, w przeciwieństwie do linii wspólnej (Shared Call Appearance). Jest to port linii obsługiwany w urządzeniu przypisanym do użytkownika. Jest on pobierany z profilu użytkownika. Służy do identyfikacji linii podstawowej użytkownika.
%BWLINEPORT-PRIMARY%	Port linii podstawowej jest obsługiwany na urządzeniu przypisanym do użytkownika. Ten tag nie obejmuje części domeny aprowizowanego portu linii. Jest on pobierany z profilu użytkownika.
%BWE911-GŁÓWNY-HELDURL%	Określa adres URL platformy lokalizacji alarmowej RedSky obsługującej protokół HELD.
%BWE911-CUSTOMERID%	Identyfikator klienta (HeldOrgId, CompanyID) używany dla żądania HTTPS RedSky.

Poufne informacje Cisco

Znacznik	Opis
%BWE911-SECRETKEY%	Klucz tajny uwierzytelniania żądania HTTPS RedSky.
%BWE911-LISTA-NUMERÓW-ALARMOWYCH%	Lista numerów alarmowych obsługiwanych przez RedSky. Aby użyć tego tagu, do zestawu tagów używanego przez typ urządzenia należy dodać zastrzeżony tag niestandardowy %RESERVEDBW911-EMERGENCY-NUMBER-LIST%. Znacznik "reserved" musi zawierać numery alarmowe zdefiniowane w BroadWorks w > AS_CLI/System/CallP/CallTypes, w formacie oddzielonym przecinkami, takim jak 911, 0911, 933. **UWAGA:** Klient Webex nie obsługuje symboli wieloznacznych w numerach alarmowych, dlatego do tagu niestandardowego "zarezerwowane" należy dodawać tylko dokładne numery alarmowe. Poniższy przykład ilustruje sposób wykorzystania funkcji tagu zastrzeżonego: 1) Do pliku szablonu urządzenia dodawany jest natywny znacznik %BWE911-EMERGENCY-NUMBER-LIST% 2) Zarezerwowany tag niestandardowy %RESERVEDBW911-EMERGENCY-NUMBER-LIST% jest dodawany do zestawu tagów używanego przez urządzenie o wartościach 911, 0911, 933 3) Po przebudowaniu pliku natywny tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% jest rozpoznawany jako 911, 0911, 933
%BW-MEMBERTYPE-n%	Jest to typ dla każdego wiersza. Może to być "Profil wirtualny", "Użytkownik" lub "Miejsce".
%BWUSEREXTID-n%	Jest to identyfikator zewnętrzny danego wiersza (tylko Webex Calling)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Zawiera informacje, czy dla odpowiedniej linii skonfigurowano grupę przejmowania połączeń. (Webex tylko połączenia)

Poufne informacje Cisco

6 Tagi niestandardowe

W tej sekcji opisano tagi niestandardowe używane w Webex w programie Cisco BroadWorks. Zawiera listę wszystkich niestandardowych tagów używanych zarówno dla komputerów stacjonarnych, jak i mobilnych / tabletów.

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

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_REJECT_WITH_486_WXT%	T	T	true	*6.1.16 Odrzucanie połączeń przychodzących*
%REJECT_WITH_XSI_MODE_WXT%	N	T	decline_false	*6.3.2 Powiadomienia push o połączeniach*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	T	zajęte	*6.3.2 Powiadomienia push o połączeniach*
%ENABLE_TRANSFER_CALLS_WXT%	T	T	false	*6.1.20 Przenoszenie*
%ENABLE_CONFERENCE_CALLS_WXT%	T	T	false	*6.1.21 N-Way połączenia konferencyjne i uczestnicy*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	T	T	false	*6.1.21 N-Way połączenia konferencyjne i uczestnicy*
%MAX_CONF_PARTIES_WXT%	T	T	10	*6.1.21 N-Way połączenia konferencyjne i uczestnicy*
%ENABLE_CALL_STATISTICS_WXT%	T	T	false	*6.1.24 Statystyki połączeń*
%ENABLE_CALL_PULL_WXT%	T	T	false	*6.1.22 Ściąganie połączeń*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	T	false	*6.3.2 Powiadomienia push o połączeniach*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	T	T	false	*6.1.28 Transkrypcja poczty głosowej dla Webex* Calling
%ENABLE_MWI_WXT%	T	T	false	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik* oczekujących wiadomości

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%MWI_MODE_WXT%	T	T	pusty	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik* oczekujących wiadomości
%ENABLE_VOICE_MAIL_WXT%	T	T	false	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik* oczekujących wiadomości
%ENABLE_VISUAL_VOICE_MAIL_WXT%	T	T	false	*6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik* oczekujących wiadomości
%ENABLE_FORCED_LOGOUT_WXT%	T	N	false	*6.2.1* *Wymuszone* wylogowanie
%FORCED_LOGOUT_APPID_WXT%	T	N	pusty	*6.2.1* *Wymuszone* wylogowanie
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	T	T	false	*6.1.29.1 Przekierowywanie 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*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	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 portami SIP dla przechodzenia translacji* adresów sieciowych
%RPORT_USE_LOCAL_PORT_WXT%	T	T	false	*6.1.14 Zarządzanie portami SIP dla przechodzenia translacji* adresów sieciowych
%USE_TLS_WXT%	T	T	false	*6.1.2 SIP Over TLS i bezpieczny protokół transportu w* czasie rzeczywistym
%SBC_ADDRESS_WXT%	T	T	pusty	*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 dynamicznych serwerów proxy* SIP
%USE_TCP_FROM_DNS_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP
%USE_UDP_FROM_DNS_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP
%USE_TLS_FROM_DNS_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP
%DOMAIN_OVERRIDE_WXT%	T	T	pusty	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	T	T	true	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Y (tylko Windows)	N	false	*6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	T	T	5000	*6.1.5 Konfigurowalny limit czasu otwarcia gniazda SIP*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	T	T	10000	*6.1.5 Konfigurowalny limit czasu otwarcia 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 protokołu* SIP po awarii
%SIP_FAILBACK_TIMEOUT_WXT%	T	N	900	*6.1.8.2 Powrót protokołu* SIP po awarii
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	T	N	false	*6.1.8.2 Powrót protokołu* SIP po awarii
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	T	T	Dns	*6.1.8.3. Wymuszanie wersji IP*
%USE_ALTERNATIVE_IDENTITIES_WXT%	T	T	false	*6.1.10 Użyj P-Associated-URI w REGISTER*
%TCP_SIZE_THRESHOLD_WXT%	T	T	18000	*6.1.4 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania* aktywności
%SIP_REFRESH_ON_TTL_WXT%	T	N	false	*6.1.8.4 Zarządzanie czasem wygaśnięcia* 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)*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_SIP_SESSION_ID_WXT%	T	T	false	*6.1.15 SIP Session ID* (Identyfikator sesji SIP)
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	T	T	false	*6.1.13 Starsze informacje o SIP* FIR
%SRTP_ENABLED_WXT%	T	T	false	*6.1.2 SIP Over TLS i bezpieczny protokół transportu w* czasie rzeczywistym
%SRTP_MODE_WXT%	T	T	false	*6.1.2 SIP Over TLS i bezpieczny protokół transportu w* czasie rzeczywistym
%ENABLE_REKEYING_WXT%	T	T	true	*6.1.2 SIP Over TLS i bezpieczny protokół transportu w* czasie rzeczywistym
%RTP_AUDIO_PORT_RANGE_START_WXT%	T	T	8000	*6.1.17 Zakres portów protokołu transportowego w* czasie rzeczywistym
%RTP_AUDIO_PORT_RANGE_END_WXT%	T	T	8099	*6.1.17 Zakres portów protokołu transportowego w* czasie rzeczywistym
%RTP_VIDEO_PORT_RANGE_START_WXT%	T	T	8100	*6.1.17 Zakres portów protokołu transportowego w* czasie rzeczywistym
%RTP_VIDEO_PORT_RANGE_END_WXT%	T	T	8199	*6.1.17 Zakres portów protokołu transportowego w* czasie rzeczywistym
%ENABLE_RTCP_MUX_WXT%	T	T	true	*6.1.19 RTCP MUX*
%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 Katalog główny XSI i* ścieżki
%XSI_ACTIONS_PATH_WXT%	T	T	/com.broadsoft.xsi-actions/	*6.1.32 Katalog główny XSI i* ścieżki

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%XSI_EVENTS_PATH_WXT%	T	T	/com.broadsoft.xsi-events/	*6.1.32 Katalog główny XSI i* ścieżki
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	T	T	false	*6.1.25 Automatyczne przywracanie 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 Przejmowanie połączeń*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	T	N	false	*6.2.2 Przejmowanie połączeń*
%WEB_CALL_SETTINGS_URL_WXT%	T	T	pusty	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%USER_PORTAL_SETTINGS_URL_WXT%	T	T	pusty	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%ENABLE_CALL_CENTER_WXT%	T	T	false	*6.1.31 Call Center / Logowanie / Wylogowanie z* kolejki połączeń
%WEB_CALL_SETTINGS_TARGET_WXT%	T	T	zewnętrzny	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	T	T	true	*6.1.30 Portal ustawień i internetowe ustawienia połączeń*
%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)*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	T	N	false	*6.2.3 Wsparcie Boss-Admin (Executive-Assistant)*
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	T	35	*6.3.2 Powiadomienia push o połączeniach*
%ENABLE_CALL_RECORDING_WXT%	T	T	false	*6.1.26 Nagrywanie rozmów*
%ENABLE_SINGLE_ALERTING_WXT%	N	T	false	*6.3.3 Alert pojedynczy*
%ENABLE_CALL_PARK_WXT%	T	T	false	*6.1.23 Wywołanie Parkuj/Odzyskaj*
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	T	T	10	*6.1.23 Wywołanie Parkuj/Odzyskaj*
%ENABLE_RTP_ICE_WXT%	T	T	false	*6.1.18 Obsługa ICE(tylko Webex Calling)*
%RTP_ICE_MODE_WXT%	T	T	icestun	*6.1.18 Obsługa ICE(tylko Webex Calling)*
%RTP_ICE_SERVICE_URI_WXT%	T	T	pusty	*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 czasem wygaśnięcia* DNS
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	T	N	false	*6.2.4 Eskaluj połączenia SIP do Meeting*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	T	N	false	*6.2.5 Sterowanie telefonem biurkowym — automatyczne odbieranie*
%ENABLE_DIALING_VOIP_WXT%	N	T	true	*6.3.5 Obsługa MNO* *Nawiązywanie połączeń przy użyciu* natywnego programu wybierającego

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_DIALING_NATIVE_WXT%	N	T	false	*6.3.5 Obsługa MNO Nawiązywanie połączeń przy użyciu* natywnego programu wybierającego
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	T	T	true	*6.1.35 Wybieranie numerów* SIP-URI
%ENABLE_SIP_VIDEOCALLS_WXT%	T	T	true	*6.1.37 Wyłączanie połączeń wideo*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	T	T	true	*6.1.37 Wyłączanie połączeń wideo*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	T	T	Pulpit - prawda Telefon komórkowy, Tablet - fałsz	*6.1.37 Wyłączanie połączeń wideo*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	T	T	false	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji przez dostawcę E911*
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	T	T	0	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji przez dostawcę E911*
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	T	T	-1	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji przez dostawcę E911*
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	T	T	once_per_login	*6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji przez dostawcę E911*
%ENABLE_AUTO_ANSWER_WXT%	T	N	false	*6.2.6 Automatyczne odbieranie z powiadomieniem tonowym*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	T	T	false	*6.1.41 Wskazanie połączenia spamowego*
%ENABLE_NOISE_REMOVAL_WXT%	T	T	false	*6.1.42 Usuwanie szumów i zwiększanie przepustowości dla połączeń PSTN/komórkowych*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_AUDIO_MARI_FEC_WXT%	T	T	false	*6.1.46.2 Forward Error Correction (FEC) i Packets Retransmission (RTX)*
%ENABLE_AUDIO_MARI_RTX_WXT%	T	T	false	*6.1.46.2 Forward Error Correction (FEC) i Packets Retransmission (RTX)*
%ENABLE_VIDEO_MARI_FEC_WXT%	T	T	false	*6.1.46.2 Forward Error Correction (FEC) i Packets Retransmission (RTX)*
%ENABLE_VIDEO_MARI_RTX_WXT%	T	T	false	*6.1.46.2 Forward Error Correction (FEC) i Packets Retransmission (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 - widżet In-call*
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	T	true	*6.3.5.6 Mobilność MNO - widżet In-call*
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	T	true	*6.3.5.6 Mobilność MNO - widżet In-call*
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	T	T	false	*6.1.47 Jednoczesne połączenia z tym samym* użytkownikiem
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	T	N	false	*6.2.12 Pakiet zdarzeń zdalnego wyciszenia (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 Przełączanie awaryjne* SIP
%ENABLE_CALL_MOVE_HERE_WXT%	T	N	false	*6.2.13 Przenoszenie połączenia*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	T	T	false	*6.1.42 Usuwanie szumów i zwiększanie przepustowości dla połączeń PSTN/komórkowych*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	T	pusty	*6.3.5.1 Nawiązywanie połączeń przy użyciu* natywnego programu wybierającego
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	T	T	false	*6.1.20 Przenoszenie*
%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 rozmówcy przychodzącego*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	T	false	*6.3.6 Identyfikator rozmówcy przychodzącego*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	T	false	*6.1.50 ID abonenta* dzwoniącego *Identyfikator rozmówcy wychodzącego*
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	T	false	*6.1.50 ID abonenta* dzwoniącego *Identyfikator rozmówcy wychodzącego*
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	T	false	*6.1.50 ID abonenta* dzwoniącego *Identyfikator rozmówcy wychodzącego*
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	T	false	*6.1.50 ID abonenta* dzwoniącego *Identyfikator rozmówcy wychodzącego*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	T	false	*6.1.50 ID abonenta* dzwoniącego *Identyfikator rozmówcy wychodzącego*
%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

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	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 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania* aktywności
%TCP_KEEPALIVE_ENABLED_WXT%	T	T	false	*6.1.4 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania* aktywności
%TLS_KEEPALIVE_ENABLED_WXT%	T	T	false	*6.1.4 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania* aktywności
%ENABLE_MULTI_LINE_WXT%	T	T	false	*6.1.51 Obsługa* wielu linii
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	T	false	*6.2.4 Eskalacja połączeń SIP na spotkanie (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	T	false	*6.3.5.3 Tożsamość wychodzącej linii telefonicznej (CLID) – podwójna persona*
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	T	false	*6.3.5.3 Tożsamość wychodzącej linii wywołującej (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	T	T	Rozwiązane	*6.1.50.2 Nazwa identyfikatora zdalnego rozmówcy*
%PERSONAL_ASSISTANT_ENABLED_WXT%	T	T	false	*6.1.53 Osobisty asystent (obecność poza* domem)***Error! Reference source not found.***
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	T	NPS	***Error! Reference source not found.*** *Sposób dostawy (tylko Webex Calling)*

Poufne informacje Cisco

Znacznik	Używane w komputerach stacjonarnych	Używany w telefonie komórkowym/tablecie	Wartość domyślna	Sekcja
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	T	T	false	*6.1.52* ***Error! Reference source not found.***

Więcej informacji na temat mapowania tagów niestandardowych używanych w Webex dla Cisco BroadWorks na tagi używane przez UC-One można znaleźć w sekcji *8 Mapowanie tagów niestandardowych między Webex dla Cisco BroadWorks i UC-One*.

Poufne informacje Cisco

6.1 Cechy wspólne

6.1.1 Ustawienia serwera SIP

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

- Domena SIP. Jest on używany jako domenowa część własnego URI SIP (własna URI SIP jest czasami nazywana portem liniowym) ogólnie w nagłówkach SIP i w połączeniach zdalnych (XSI). Część użytkownika własnego URI SIP pochodzi z konfiguracji poświadczeń SIP (parametr <nazwa_użytkownika> w sekcji <poświadczenia>).
- Serwer SIP URI lub adres IP serwera proxy SIP, jeśli DNS rozpoznanie nie powiedzie się. Należy zauważyć, że aby użyć TLS, nie można użyć adresów IP w parametrze proxy, ponieważ sprawdzanie poprawności certyfikatu TLS zakończy się niepowodzeniem. Aby uzyskać więcej informacji na temat portu proxy, zobacz tag DM %SOURCE_PORT_WXT%. Należy zauważyć, że funkcji zarządzania DNS TTL nie można użyć, gdy w parametrze adresu serwera proxy jest używany adres IP. Ogólnie rzecz biorąc, z tych powodów nie zaleca się używania adresu IP w tym polu.

Inne parametry można również zmienić, aby włączyć różne funkcje połączeń. Jednak poprzednie ustawienia włączają podstawowe funkcje dla następujących elementów:

- Rejestracja w sieci SIP.
- Nawiązywanie połączeń audio lub wideo.
- Wykrywanie serwerów proxy w oparciu o DNS, które umożliwia korzystanie z kilku serwerów proxy.

Po włączeniu rejestracji SIP, włączenie SIP SUBSCRIBE dla MWI musi nastąpić za pomocą oddzielnych parametrów konfiguracyjnych. Więcej informacji na temat poczty głosowej można znaleźć w sekcji *6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik* oczekujących wiadomości.

Należy pamiętać, że podstawowa konfiguracja SIP jest zawsze potrzebna do MWI nawet wtedy, gdy połączenia SIP są wyłączone. MWI opiera się na SIP NOTIFY.

Konfiguracja serwerów SIP przebiega według następującego podstawowego schematu:

- Adres proxy zawiera URI serwera SIP.
- Można zdefiniować tylko jeden serwer proxy.
- Odnajdowanie serwera proxy DNS zapewnia obsługę wielu serwerów proxy, które wymagają odpowiedniej konfiguracji DNS.

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

```
<config>
<protokoły>
<łyk>
   <timery>
      <T1>500</T1>
      <T2>4000</T2>
      <T4>5000</T4>
   </timery>
```


Poufne informacje Cisco

- T1 – czas w milisekundach opóźnienia podróży w obie strony sieci.
- T2 – maksymalny czas (w milisekundach) przed ponownym przesłaniem żądań niezaproszonych i odpowiedzi na zaproszenia.
- T4 – maksymalny czas, w milisekundach, aby wiadomość pozostawała w sieci.

Każda linia ma własne parametry, takie jak numer poczty głosowej, URI konferencji i domena, a także poświadczenia uwierzytelniania SIP. W razie potrzeby można skonfigurować oddzielne poświadczenia dla sygnalizacji 401 i 407.

Poniższy przykład i tabela zawierają informacje o najbardziej typowych tagach DM używanych do konfiguracji SIP.

```
<config>
<protokoły><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
       <linia>
              <label>%BWAPPEARANCE-LABEL-1%</label>
              <nazwa>%nazwa-BW-1%</nazwa>
              <numer>%BWE164-1%</numer>
              <rozszerzenie>%BWEXTENSION-1%</rozszerzenie>
              <identyfikator-zewnętrzny>%BWUSEREXTID-1%</identyfikator-zewnętrzny>
              <numer-poczty głosowej>%BWNUMER-PORTALU-GŁOSOWEGO-1%</numer-poczty
głosowej>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
1%</conference-service-uri>
              <domena>%BWHOST-1%</domena>
              <poświadczenia>
                     <nazwa_użytkownika>%BWLINEPORT-1%</nazwa_użytkownika>
                     <password>%BWAUTHPASSWORD-1%</password>
                     <auth>
                            <auth401>
                                   <domyślnie>
                                          <nazwa_użytkownika>%BWAUTHUSER-
1%</nazwa_użytkownika>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </domyślnie>
                                   <realm id="%BWHOST-1%">
                                          <nazwa_użytkownika>%BWAUTHUSER-
1%</nazwa_użytkownika>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </królestwo>
                            </auth401>
                            <auth407>
                                   <domyślnie>
                                          <nazwa_użytkownika>%BWAUTHUSER-
1%</nazwa_użytkownika>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </domyślnie>
                                   <realm id="%BWHOST-1%">
                                          <nazwa_użytkownika>%BWAUTHUSER-
1%</nazwa_użytkownika>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </królestwo>
                            </auth407>
                     </auth>
              </referencje>
       </linia>
```


Poufne informacje Cisco

```
        …
</linie>
<adres proxy="%SBC_ADDRESS_WXT%" port="%SBC_PORT_WXT%" />
<preferowany-port>%SOURCE_PORT_WXT%</preferowany-port>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%BWLINEPORT-n%	pusty	łańcuch	Zazwyczaj nazwa użytkownika SIP. Aby uzyskać więcej informacji, zobacz sekcję *5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks*. Przykład: jankowalski
%BWAUTHPASSWORD-n%	pusty	łańcuch	Zazwyczaj hasło SIP. Aby uzyskać więcej informacji, zobacz sekcję *5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks*. przykład: secretpassword
%BWE164-n%	pusty	numer	Domyślny numer telefonu użytkownika w formacie międzynarodowym. Aby uzyskać więcej informacji, zobacz sekcję *5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks*. Przykład: 12345678
%SBC_ADDRESS_WXT%	pusty	łańcuch	Aby uzyskać więcej informacji, zobacz sekcję *5.6 Domyślne znaczniki systemowe*. Przykład: sbcexample.domain.com
%SBC_PORT_WXT%	5060	numer	Aby uzyskać więcej informacji, zobacz sekcję *5.6 Domyślne znaczniki systemowe*. Przykład: 5060
%BWHOST-n%	pusty	łańcuch	Zazwyczaj używany jako domena SIP. Aby uzyskać więcej informacji, zobacz sekcję *5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks*. Przykład: exampledomain.com
%SOURCE_PORT_WXT%	5060	numer	Zazwyczaj używany dla parametru preferowanego *portu* . Aby uzyskać więcej informacji, zobacz sekcję *6.1.7 Preferowane użycie portu dla* SIP. Przykład: 5061
%BWUSEREXTID-n%	pusty	łańcuch	(Tylko Webex Calling) Przechowuje zewnętrzny identyfikator linii Aby uzyskać więcej informacji, sprawdź *6.1.51 Obsługa* wielu linii. Przykład: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

Poufne informacje Cisco

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

6.1.2 SIP Over TLS i bezpieczny protokół transportu w czasie rzeczywistym

Klienta można skonfigurować do korzystania z sygnalizacji SIP przez TLS i bezpiecznego protokołu transportu w czasie rzeczywistym (SRTP) do szyfrowania mediów. Te funkcje muszą być jednak włączone w konfiguracji, jak pokazano w poniższym przykładzie. Należy również zauważyć, że gdy jest używane dynamiczne odnajdowanie serwera 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 DNS SRV. Więcej informacji na temat dynamicznego wykrywania serwerów proxy SIP można znaleźć w sekcji *6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP.

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

Szczegółowe informacje na temat zaleceń dotyczących portu SIP i protokołu transportowego, gdy w sieci są używane grupy SIP ALG, można znaleźć w *Webex przewodniku po rozwiązaniach* Cisco BroadWorks.

Należy pamiętać, że użyty certyfikat musi być ważny. Ponadto łańcuch certyfikatów musi być nienaruszony, aby certyfikat pośredni był również połączony. Zaleca się stosowanie powszechnie używanego certyfikatu, aby był już domyślnie obecny na urządzeniach. Możliwe jest również dodawanie certyfikatów lokalnie na komputerze stacjonarnym ręcznie lub przy użyciu aprowizacji zbiorczej, chociaż zazwyczaj nie jest to wykonywane.

Aby włączyć powiązany SRTP szyfrowania multimediów, istnieje osobne ustawienie.

Oprócz RTP, ruch RTCP może być zabezpieczony tymi samymi mechanizmami, co RTP przy użyciu poprzedniej konfiguracji.

Dla szyfrów SIP/TLS, patrz *Dodatek A: Szyfry TLS.*

SRTP służy do zapewnienia bezpieczeństwa strumienia multimediów w trzech różnych aspektach:

- Poufność (dane są szyfrowane)
- Uwierzytelnianie (zapewnienie tożsamości drugiej strony lub stron)
- Integralność (środki przeciwdziałające na przykład atakom powtórkowym)

Bieżąca wersja struktury nośników obsługuje tryb licznika AES 128 dla ochrony i Hash Message Authentication Code (HMAC)-SHA-1 dla uwierzytelniania. Rozmiar klucza głównego wynosi 16 bajtów, a sól główna 14 bajtów.

Media Framework obsługuje zarówno pełny (80-bitowy), jak i krótki (32-bitowy) tag uwierzytelniania. Klient wymienia klucze wewnątrz SDP w ramach sygnalizacji SIP, obie strony połączenia wysyłają używany klucz na drugą stronę.

Poufne informacje Cisco

SRTP można włączyć przy użyciu konfiguracji pokazanej w poniższym przykładzie. Bieżąca implementacja używa tylko bezpiecznego profilu RTP SDP i obsługuje wielowierszowe wpisy SDP dla profili audiowizualnych (AVP) i bezpiecznych profili audiowizualnych (SAVP). Implementacja SRTP została pomyślnie przetestowana w zwykłej konfiguracji wdrażania z różnymi kontrolerami SBC. Testowanie interoperacyjności (IOT) z punktami końcowymi, które obsługują tylko szyfrowanie przy użyciu profilu AVP, nie jest obsługiwane.

Wieloliniowe procedury SDP związane z SRTP są zaimplementowane, dzięki czemu zawsze używanych jest wiele linii m. Stosowane są oddzielne linie m dla AVP i SAVC.

Należy jednak zwrócić szczególną uwagę na konfigurację kontrolera SBC; w szczególności zapewnienie, że przychodząca linia "m=", powiązana z RTP/SAVP w SDP, nie zostanie usunięta, ponieważ w niektórych przypadkach połączenia SRTP mogą zostać zablokowane.

Możliwe jest jednak kilka różnych konfiguracji sieci, w niektórych wdrożeniach kontroler SBC nie jest zaangażowany w ruch nośników, podczas gdy w innych wdrożeniach każdy klient RTP składnik nośnika w kierunku kontrolera SBC jest oddzielnie szyfrowany i negocjowany za pośrednictwem kontrolera SBC. W niektórych wdrożeniach kontroler SBC nie zezwala na wiele linii SDP.

Kontroler SBC może również modyfikować kolejność linii m SDP podczas konfiguracji połączenia, umieszczając na pierwszym miejscu linię m AVP (nieszyfrowaną) lub SAVP (szyfrowaną). Dlatego klienci, którzy wybierają pierwszą działającą linię m, preferują ruch zaszyfrowany lub niezaszyfrowany. Dostępne są następujące opcje konfiguracji SRTP:

- Obowiązkowe – podczas konfiguracji połączenia początkowy SDP obejmuje tylko linię m SAVP podczas oferowania, a klient akceptuje tylko linię m SAVP w SDP podczas odbierania, dlatego możliwe są tylko połączenia SRTP.
- Preferowane – podczas konfiguracji połączenia początkowy SDP zawiera zarówno linie m AVP, jak i SAPP, ale SAVP jest pierwszy przy oferowaniu, wskazując preferowaną kolejność. Odpowiadając, klient wybiera SAPP, jeśli jest dostępny, nawet jeśli nie jest to pierwsza linia m (zgodnie ze specyfikacją SIP kolejność linii m nie jest zmieniana podczas odpowiadania).
- Opcjonalnie – podczas konfiguracji połączenia początkowy SDP zawiera zarówno linie m SAPP, jak i AVP podczas oferowania, ale AVP najpierw wskazuje preferowaną kolejność. Odpowiadając, klient wybiera pierwszą linię m, AVP lub SAVP.
- SRTP włączone — w początkowym SDP nie ma linii m SAVP podczas oferowania. Podczas odbierania SAVP nie jest akceptowany, dlatego możliwe są tylko RTP połączenia.
- Transport — automatycznie wybiera tryb SRTP na podstawie protokołu transportowego. Jeśli TLS jest używany, obowiązkowy tryb SRTP jest włączony. Jeśli używany jest TCP lub UDP, nie jest używany żaden SRTP.

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

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

```
<config>
<protokoły><rtp>
```


Poufne informacje Cisco

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

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

W niektórych wdrożeniach ponowne wprowadzanie klucza dla SRTP nie jest obsługiwane. W związku z tym istnieje parametr konfiguracyjny umożliwiający włączanie/wyłączanie SRTP ponowne tworzenie klucza. Jednak nowe klucze są zawsze brane pod uwagę po otrzymaniu w zaktualizowanym SDP zgodnie z rfc3264. Możliwość konfiguracji dotyczy tylko wysyłania nowych kluczy.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%USE_TLS_WXT%	false	prawda, fałsz	Po ustawieniu wartości "false" TLS SIP jest dezaktywowany. Po ustawieniu wartości "true" aktywowany jest TLS SIP. Należy pamiętać, że jeśli *6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP jest używany, ten parametr jest ignorowany.
%SRTP_ENABLED_WXT%	false	prawda, fałsz	Po ustawieniu wartości "false" SRTP jest dezaktywowany. Po ustawieniu wartości "true" aktywowana jest SRTP.
%SRTP_MODE_WXT%	fakultatywny	obowiązkowe, preferowane, fakultatywne, transport	Określa preferowany SRTP podczas konfiguracji połączenia. Wartość domyślna to "optional".
%ENABLE_REKEYING_WXT%	true	prawda, fałsz	Umożliwia ponowne wprowadzanie kluczy SIP (SDP) dla SRTP.

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

6.1.3 Nagłówki SIP 3GPP dla SRTP

Nowsze specyfikacje 3GPP wymagają dodatkowych nagłówków SIP do korzystania z protokołu Secure Real-time Transport Protocol (SRTP). Aby uzyskać więcej informacji, zobacz *3GPP TS 24.229* , a także następujące:

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

Poufne informacje Cisco

Nagłówki wymagane przez tę specyfikację mogą przerwać wywołania SIP we wdrożeniach, w których ta specyfikacja nie jest używana. Dlatego zaleca się, aby te nagłówki były używane tylko w środowiskach, w których są obsługiwane po stronie serwera.

Można konfigurować tylko możliwość korzystania z nagłówków. Nie ma dalszych możliwości konfiguracji dla poszczególnych nagłówków. Wszystkie nagłówki są włączone lub wyłączone.

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

Poniższy tag steruje tą możliwością.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%USE_MEDIASEC_WXT%	false	Prawda, fałsz	Włącza nagłówki SIP 3GPP do negocjacji SRTP.

6.1.4 Wymuszanie TCP, TLS lub UDP użytkowania i utrzymywania aktywności

Webex klienta Cisco BroadWorks można skonfigurować tak, aby używał TCP, TLS lub UDP zarówno dla sygnalizacji SIP, jak i nośników RTP. Należy zauważyć, że klient domyślnie TCP. Należy również pamiętać, że bez TCP utrzymaniu aktywności połączenia TCP SIP są zamykane po pewnym okresie nieaktywności.

Poniższy przykład przedstawia ten węzeł konfiguracji.

```
<config>
<protokoły><sip>
<transporty>
   <tcp-size-threshold>%TCP_SIZE_THRESHOLD_WXT%</tcp-size-threshold>
```

Poniższy tag określa, czy klient używa TCP, czy UDP.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości (bajty)	Opis
%TCP_SIZE_THRESHOLD_WXT%	0	0	Siły TCP do użycia. Decyzja o użyciu TCP lub UDP dla klienta należy do usługodawcy, jednak zaleca się użycie TCP o wartości domyślnej "0".
	0	1 - 99,000	Wymusza użycie UDP, gdy rozmiar wiadomości jest niższy od podanej tutaj wartości. Domyślnie TCP, gdy rozmiar wiadomości jest większy niż ustawiona wartość. Aby użyć UDP, domyślnym zaleceniem jest 1500.
	0	100000	Siły UDP do użycia.

Poufne informacje Cisco

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

```
<config>
<protokoły><sip>
<transporty>
        …
        <udp>
                <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
                        <limit czasu>20</limit czasu>
                        <ładunek>crlf</ładunek>
                </utrzymaj przy życiu>
        </udp>
        <tcp>
                <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
                        <limit czasu>0</limit czasu>
                        <ładowność></ładunek>
                </utrzymaj przy życiu>
        </tcp>
        <tls>
                <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
                        <limit czasu>0</limit czasu>
                        <ładowność></ładunek>
                </utrzymaj przy życiu>
        </tls>
</transporty>
```

Możliwe parametry to:

- Włączenie TCP lub TLS utrzymywania aktywności, możliwe wartości - prawda/fałsz, domyślnie "false", jeśli brakuje węzła. Należy pamiętać, że gdy ta funkcja jest włączona, wysyłane są TCP zachowania, nawet jeśli transport UDP jest używany do obsługi protokołu SIP.
- Włączenie UDP utrzymywania aktywnych, możliwych wartości - prawda/fałsz, domyślnie "true", jeśli brakuje węzła. Należy pamiętać, że gdy ta funkcja jest włączona, wysyłane są UDP zachowania, nawet jeśli transport TCP jest używany do protokołu SIP. Ponadto, nawet jeśli TCP jest używany dla SIP, klient akceptuje również ruch przez UDP zgodnie z *RFC 3261*.
- Limit czasu określa maksymalny czas braku aktywności w sekundach, po którym wysyłana jest wiadomość o utrzymaniu aktywności. Brak wartości oznacza, że utrzymywanie aktywności jest wyłączone dla protokołu.
- Ładunek dla komunikatów keepalive, możliwe wartości (brak wartości oznacza, że funkcja keepalive jest wyłączona dla protokołu):
  - Crlf
  - Null (nie należy używać)
  - Ciąg niestandardowy (**nie należy go używać**)

Keepalives mogą być używane do celów przechodzenia przez NAT, aby utrzymać wiązania NAT otwarte przy niewielkim dodatkowym ruchu.

Poufne informacje Cisco

Adres IP serwera i port dla utrzymania aktywności są określane przy użyciu normalnych procedur wykrywania serwera proxy SIP. Należy pamiętać, że porty SIP i wybór protokołu transportowego uzyskany za pośrednictwem dynamicznego wykrywania serwera proxy SIP zastępują wszelkie statyczne porty lub konfiguracje transportu. Więcej informacji na temat dynamicznego odnajdowania serwerów proxy można znaleźć w sekcji *6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%UDP_KEEPALIVE_ENABLED_WXT%	true	prawda, fałsz	Kontroluje, czy pakiety utrzymujące się przy życiu powinny być wysyłane do transportu UDP.
%TCP_KEEPALIVE_ENABLED_WXT%	false	prawda, fałsz	Kontroluje, czy pakiety utrzymujące się przy życiu powinny być wysyłane do transportu TCP.
%TLS_KEEPALIVE_ENABLED_WXT%	false	prawda, fałsz	Kontroluje, czy pakiety utrzymywane przy życiu powinny być wysyłane do transportu TLS.

6.1.5 Konfigurowalny limit czasu otwarcia gniazda SIP

Wcześniej limit czasu otwarcia gniazda SIP był zakodowany na stałe do 5 sekund dla TCP i 10 sekund dla TLS. Te limity czasu można teraz konfigurować.

```
<config>
    <protokoły>
        <łyk>
            <transporty>
                <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>
            </transporty>
```

Poniższe znaczniki określają limit czasu połączenia gniazda (w milisekundach).

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<liczba całkowita> — limit czasu w milisekundach	Limit czasu połączenia gniazda, gdy używany jest transport TCP.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	<liczba całkowita> — limit czasu w milisekundach	Limit czasu połączenia gniazda, gdy używany jest transport TLS.

6.1.6 Wykrywanie dynamicznych serwerów proxy SIP

Aby włączyć funkcję dynamicznego wykrywania serwera proxy SIP, zobacz poniższy przykład.

```
<config>
<protokoły><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%">
    <nazwa-rekordu>%SBC_ADDRESS_WXT%</nazwa-rekordu>
    <domain-override>%DOMAIN_OVERRIDE_WXT%</domain-override>
</proxy-discovery>
```

Można kontrolować, które wpisy protokołów transportowych z DNS SRV są używane, gdy wiele z nich jest dostępnych, postępując zgodnie z procedurami podanymi w tej sekcji.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%USE_PROXY_DISCOVERY_WXT%	false	Prawda, fałsz	Umożliwia dynamiczne wykrywanie serwerów proxy SIP dla połączeń audio i wideo. Zalecana wartość to "true".
%SBC_ADDRESS_WXT%	pusty	Ciąg	Ten tag Cisco BroadWorks jest zwykle używany jako parametr record-name. Powinien to być prawidłowy adres URL – nie powinien to być adres IP. Aby uzyskać więcej informacji, zobacz sekcję *5.6 Domyślne znaczniki systemowe*. Przykład: sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	pusty	Ciąg	Ten tag niestandardowy jest używany do zastępowania domeny. Więcej informacji można znaleźć w poniższej sekcji. Przykład: other.domain.com

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%USE_TCP_FROM_DNS_WXT%	true	Prawda, fałsz	Jeśli ta wartość parametru to "false", DNS wyników SRV dla tego protokołu transportowego (TCP) są odrzucane. Jeśli wartość "true", używane są wyniki z DNS SRV dla tego protokołu transportowego (TCP). W zależności od priorytetów SRV nadal może zostać wybrany inny transport.
%USE_UDP_FROM_DNS_WXT%	true	Prawda, fałsz	Jeśli wartość parametru to "false", DNS wyników SRV dla tego protokołu transportowego (UDP) są odrzucane. Jeśli wartość "true", używane są wyniki z DNS SRV dla tego protokołu transportowego (UDP). W zależności od priorytetów SRV nadal może zostać wybrany inny transport.
%USE_TLS_FROM_DNS_WXT%	true	Prawda, fałsz	Jeśli ta wartość parametru to "false", DNS wyników SRV dla tego protokołu transportowego (TLS) są odrzucane. Jeśli "true", używane są wyniki z DNS dla tego protokołu transportowego (TLS). W zależności od priorytetów SRV nadal może zostać wybrany inny transport.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	Prawda, fałsz	true	Włącza/wyłącza usługę tworzenia kopii zapasowych DNS. Jeśli ta opcja jest włączona, rozpoznawanie A/AAAA jest wykonywane dla adresu proxy SIP. Jest ona brana pod uwagę tylko wtedy, gdy włączone jest odnajdowanie usługi SRV/NAPTR.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	Prawda, fałsz	true	Jeśli ustawiona jest wartość "true", a odnajdowanie usługi NAPTR nie powiedzie się lub nie zwróci żadnych wyników, dla skonfigurowanego hosta zostanie przeprowadzone odnajdowanie usługi SRV. Jeśli ustawiona jest wartość "false", wykrywanie SRV nie jest wykonywane.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Prawda, fałsz	false	Umożliwia obejście pamięci podręcznej systemu operacyjnego DNS.

DNS umożliwia klientowi uzyskanie adresu IP, portu i protokołu transportowego dla serwera proxy SIP zgodnie ze specyfikacją RFC 3263.

DNS SRV, Obsługiwane są zapytania wskaźnika organu nazewnictwa (NAPTR) i rekordów A. Podczas logowania przepływ w 3 krokach wygląda następująco:

1. Wykonaj zapytanie NAPTR, używając *pola* <record-name> powyżej, aby uzyskać identyfikatory URI serwera z protokołami transportowymi, jeśli istnieją. Wartość *parametru<record-name>* powinna być pełną domeną, którą DNS rozpoznać, i nie może być adresem IP.

Poufne informacje Cisco

2. Rozwiąż elementy znalezione w zapytaniu NAPTR przy użyciu zapytania SRV, aby uzyskać ostateczny URI i port serwera. Część domeny używana w zapytaniu SRV jest pobierana z wyniku zapytania NAPTR w celu znalezienia ostatecznego URI (i portu) serwera. Port odebrany z DNS kwerendy SRV jest używany, gdy dostępne są DNS wpisy SRV. Należy zauważyć, że port, tylko z pliku konfiguracyjnego, dotyczy statycznego serwera proxy w pliku konfiguracyjnym, a nie identyfikatorów URI rozpoznawanych przy użyciu protokołu SRV. Zobacz poniższe przykłady użycia różnych nazw rekordów.

   Jeśli numer NAPTR nie zostanie znaleziony, klient próbuje utworzyć zapytanie SRV z nazwą rekordu pobraną z <*domain*> parametr, chyba że *występuje parametr<domain-override>* parametr, w którym to przypadku *użyto parametru<domain-override>* i automatycznie próbuje znaleźć osobne wpisy dla TCP, UDP i TLS (*_sip_protocol* [UDP, TCP lub TLS]). Należy zauważyć, że protokół SCTP (Stream Control Transmission Protocol) nie jest obsługiwany. Jeśli zapytania SRV nie przynoszą żadnych wyników, odnajdowanie serwera proxy kończy się niepowodzeniem, a użytkownikowi końcowemu jest wyświetlany komunikat o błędzie wskazujący, że połączenia są niedostępne. W takim przypadku nie ma rejestracji SIP. Jednak nawet jeśli wszystkie zapytania SRV zakończą się niepowodzeniem lub jeśli odebrane tam serwery nie działają, klient nadal sprawdza, czy skonfigurowany statyczny serwer proxy działa, tylko za pomocą zapytań A do URI określonego w <adres proxy> aby sprawdzić, czy daje IP adres, który zapewnia działającą rejestrację SIP. Port i transport w tym ostatnim przypadku pochodzą z *parametrów progowych* TCP i < *bezpiecznych*> .

3. Rozpoznawanie znalezionych identyfikatorów URI przy użyciu zapytania rekordu A. Odebrane końcowe adresy IP są wypróbowywane w kolejności, w jakiej zostały odebrane, aby uzyskać działające połączenie z serwerem proxy SIP. Kolejność ta może być zdefiniowana przez usługodawcę w DNS. Pierwszy URI proxy SIP z pomyślnym wyszukiwaniem rekordu A jest wybierany i używany do momentu, gdy przestanie działać lub klient się wyloguje. W kroku Zapytanie A używany jest tylko jeden adres IP naraz, nawet jeśli odebrano ich wiele. Jednak wszystkie wpisy SRV są usuwane do momentu wylogowania lub utraty sieci.

Ważne uwagi

UWAGA 1: Jeśli wykrycie serwera proxy DNS powoduje wybór protokołu transportowego w kroku SRV poprzez odebranie działającego URI proxy SIP dla protokołu transportowego, zastępuje *parametr progu* tcp zwykle używany do wybierania UDP lub TCP w pliku konfiguracyjnym. To samo dotyczy konfiguracji SIP/TLS. TCP lub UDP jest używany w zależności od priorytetu w DNS.

UWAGA 2: Elementy odebrane za pośrednictwem SRV mają wyższy priorytet niż statyczny serwer proxy w pliku konfiguracyjnym. Porządek NAPTR nie jest analizowany; Liczy się tylko priorytet SRV. Jeśli wynikiem SRV jest kilka pozycji o jednakowym protokole transportowym, priorytecie i wadze, każdy otrzymany jest wybierany losowo. Wagi NAPTR nie są obsługiwane w tej wersji, ale są obsługiwane wzorce SRV. Priorytet SRV jest analizowany w pierwszej kolejności, a w przypadku elementów o równym priorytecie sprawdzana jest waga, aby określić prawdopodobieństwo, że dany serwer zostanie wypróbowany w następnej kolejności.

UWAGA 3: Opcjonalny *parametr zastąpienia* domeny umożliwia rozpoznawanie nazwy rekordu A innej niż ta w parametrze konfiguracji domeny SIP za pomocą protokołu SRV, jeśli wyniki NAPTR zostaną pominięte. Zobacz poniższe przykłady użycia parametru *domain-override* .

UWAGA 4: Klient używa prymitywów systemu operacyjnego do DNS operacji i zazwyczaj odpowiedzi DNS są buforowane w celu honorowania czasu wygaśnięcia odpowiedzi DNS.

Poufne informacje Cisco

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 dla SIP over TLS.

UWAGA 6: Klient obsługuje tylko niektóre prefiksy dla usług NAPTR. Poniżej wymieniono obsługiwane prefiksy:

SIP+D2U -> _sip._udp

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, ten rekord jest ignorowany.

Przykład 1: Używanie DNS odnajdowania serwera proxy bez parametru konfiguracyjnego zastąpienia domeny

Poniżej przedstawiono przykład konfiguracji używającej odnajdowania serwera proxy SIP, gdy używany jest tylko protokół SIP over TCP, a zapytanie NAPTR w kroku 1 zwraca wyniki.

```
<config>
<protokoły><sip>
<adres proxy="domain.com" port="5060"/>
<proxy-discovery enabled="true" >
    <nazwa-rekordu>record-domain.com</nazwa-rekordu>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domena>sip-domain.com</domena>
```

Powoduje to następujące kroki 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 (odebrane w zapytaniu
NAPTR), odpowiedź
_sip._tcp.test.sip.record-domain.com. 28635 W SRV
10 10 5061 test.sipgeo.record-domain.com.
3. Zapytanie o rekord A dla test.sipgeo.record-domain.com, odpowiedź:
test.sipgeo.record-domain.com. 16 W A 1.2.3.4
```

W efekcie rejestracja SIP odbywa się przez TCP przy użyciu portu 5061 (odebranego w kroku SRV) oraz w kierunku adresu IP 1.2.3.4.

Przykład 2: **Użycie parametru zastąpienia domeny w pliku konfiguracyjnym**

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

```
<config>
<protokoły><sip
<adres proxy = "domain.com" port = "5060"/>
```


Poufne informacje Cisco

```
<proxy-discovery enabled="true">
    <nazwa-rekordu>record-domain.com</nazwa-rekordu>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domena>sip-domain.com</domena>
```

Powoduje to następujące kroki na poziomie protokołu.

```
1. Zapytanie NAPTR dla record-domain.com, brak odpowiedzi.
2. Zapytanie SRV dla _sip._tcp.override-domain.com (z pliku konfiguracyjnego),
odpowiedź
_sip._tcp.override-domain.com. 28635 W SRV
10 10 5061 test.override-domain.com.
3. Zapytanie o rekord A dla test.override-domain.com, odpowiedź:
test.sipgeooverride-domain.com. 16 W A 4.3.2.1
```

W efekcie rejestracja SIP odbywa się przez UDP przy użyciu portu 5061 (odebranego w kroku SRV) oraz w kierunku adresu IP 4.3.2.1.

Przykład 3: **Korzystanie z priorytetów SRV**

Poniżej przedstawiono kolejny przykład konfiguracji używającej odnajdowania serwera proxy SIP, gdy używany jest tylko protokół SIP over TCP, a zapytanie NAPTR w kroku 1 zwraca wyniki, ale odbieranych jest kilka rekordów NAPTR i SRV o różnych priorytetach. W tym przypadku w tym zdarzeniu wydania liczy się tylko priorytet SRV, chociaż odbieranych jest również kilka rekordów NAPTR o różnych priorytetach.

```
<config>
<protokoły><sip>
<adres proxy = "domain.com" port = "5060"/>
<proxy-discovery enabled="true">
    <nazwa-rekordu>record-domain.com</nazwa-rekordu>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domena>sip-domain.com</domena>
```

Powoduje to następujące kroki 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 (odebrane w zapytaniu
NAPTR), odpowiedź
_sip._tcp.test.sip.record-domain.com. 28635 W SRV
10 10 5061 test.sipgeo.record-domain.com.

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

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


Poufne informacje Cisco

W rezultacie rejestracja SIP odbywa się przez TCP przy użyciu portu 5061 (odebranego w kroku SRV) i w kierunku adresu IP 1.2.3.4, który obsługiwałby zarówno UDP, jak i TCP.

Przykład 4: Używanie odnajdowania serwera proxy DNS z NAPTR, gdy usługa nie jest zgodna z typem usługi

Poniżej przedstawiono przykład konfiguracji używającej wykrywania serwera proxy SIP, gdy używany jest protokół SIP przez TCP i TLS, a zapytanie NAPTR w kroku 1 zwraca wyniki.

```
<config>
<protokoły><sip>
<adres proxy = "domain.com" port = "5060"/>
<proxy-discovery enabled="true" tcp="true" udp="false" tls="true">
    <nazwa-rekordu>record-domain.com</nazwa-rekordu>
     <override-domain>override-domain.com</domain-override>
</proxy-discovery>
<domena>sip-domain.com</domena>
```

Powoduje to następujące kroki 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 typowi usługi (patrz uwaga 6 powyżej),
zostanie zignorowany.

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

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

W rezultacie rejestracja SIP odbywa się przez TCP przy użyciu portu 5061 (odebranego w kroku SRV) i w kierunku adresu IP 1.2.3.4.

6.1.7 Preferowane użycie portu dla SIP

W niektórych przypadkach inny pakiet oprogramowania był uruchomiony na tym samym komputerze co klient, zajmując domyślny port SIP. Aby skonfigurować klienta do korzystania z innego portu dla SIP, można użyć parametru *preferred-port* . Klient próbuje użyć skonfigurowanej wartości portu określonej w parametrze *preferowanego portu* , ale jeśli jest ona zajęta, klient stopniowo próbuje użyć wartości portów przekraczających skonfigurowaną wartość. Na przykład, jeśli preferowany *port* ma wartość "6000" i ten port jest zajęty, klient próbuje użyć 6001, 6002, 6003 itd., aż znajdzie nieużywany port. Po znalezieniu nieużywanego portu używa go do własnej komunikacji SIP.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SOURCE_PORT_WXT%	5060	numer	Określa preferowany lokalny port SIP do komunikacji. Przykład: 5060

6.1.8 Przełączanie awaryjne SIP i powrót po awarii

Przełączanie awaryjne SIP i powrót po awarii są zgodne z procedurami Cisco BroadWorks. W tym celu musi być skonfigurowany więcej niż jeden serwer proxy (zazwyczaj kontroler SBC).

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

- Włączona jest funkcja wykrywania serwerów proxy SIP, a serwer DNS posiada rekordy NAPTR i/lub SRV dla nazwy FQDN kontrolera SBC (patrz sekcja *6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP), LUB
- Adres serwera proxy SIP jest podawany jako nazwa FQDN i jest rozpoznawany jako wiele adresów IP (patrz sekcja *6.1.1 Ustawienia serwera SIP*).

System operacyjny DNS pamięć podręczna służy do unikania niepotrzebnego ruchu DNS. Nie ma
ustalonego limitu maksymalnej liczby adresów IP na liście.

Jeśli podczas logowania rozpoznano wiele adresów IP, są one uporządkowane według priorytetu. Klient zaczyna korzystać z pierwszego dostępnego adresu IP.

6.1.8.1 Przełączanie awaryjne SIP

Przełączanie awaryjne SIP może zostać wywołane przez błąd gniazda, błąd limitu czasu żądania lub ostateczną odpowiedź serwera na błąd w następujący sposób:

- Błąd gniazda – jeśli gniazdo między klientem a serwerem zostanie zerwane lub zamknięte, jak w przypadku utraty łączności sieciowej, klient reaguje natychmiast i uruchamia przełączanie awaryjne.
- Limit czasu (na przykład przy zawieszeniu kontrolera SBC) – na podstawie protokołu SIP T1:
  - SIP INVITE — jeśli upłynie limit czasu żądania INVITE klient rejestruje się w następnym dostępnym kontrolerze SBC (IP) i ponawia próbę wysłania zaproszenia.
  - Kolejne żądanie SIP – klient próbuje zarejestrować się do następnego dostępnego SBC (IP).
- Ostateczna odpowiedź na błąd otrzymana z serwera:
  - Następujące odpowiedzi serwera na błędy protokołu SIP skierowane do rejestru SIP powodują przełączenie awaryjne:
    - 5xx
    - 6xx

Poufne informacje Cisco

- Następujące odpowiedzi SIP *4xx* na SIP REGISTER nie powodują przełączenia awaryjnego:
  - 401 Brak autoryzacji
  - 403 Zabronione
  - 404 Nie znaleziono
  - 407 Wymagane uwierzytelnianie serwera proxy.
  - 423 interwał za krótki
- Co więcej, *odpowiedzi 4xx* na błędy SIP INVITE nie powodują przełączania awaryjnego, ale *5xx* i *6xx* tak.

Po wyzwoleniu trybu failover klient pobiera z listy następny dostępny adres IP. Timer SIP T1 określa, jak długo serwer proxy na liście jest wypróbowywany przed przejściem do następnego, zwykle używana jest wartość 32 sekund (64*T1). Jeśli wszystkie adresy IP nie powiedzie się, klient wyświetli błąd interfejsu użytkownika dla łączności SIP. Jeśli połączenie VoIP jest w trakcie przełączania awaryjnego, połączenie zostanie zakończone.

Logika pracy awaryjnej SIP opiera się na kilku parametrach konfiguracyjnych:

- Zegary awaryjne SIP — czasomierze SIP T1, T2 i T4 są widoczne w pliku konfiguracyjnym, ale nie zaleca się ich modyfikowania.

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

  - T1 – czas w milisekundach opóźnienia podróży w obie strony sieci.
  - T2 – maksymalny czas (w milisekundach) przed ponownym przesłaniem żądań niezaproszonych i odpowiedzi na zaproszenia.
  - T4 – maksymalny czas, w milisekundach, aby wiadomość pozostawała w sieci.
- Adres proxy SIP i wykrywanie serwera proxy SIP
  - Patrz sekcja *6.1.1 Ustawienia serwera SIP*.
  - Patrz sekcja *6.1.6 Wykrywanie dynamicznych serwerów proxy* SIP.
- Zarejestruj konfigurację awaryjną (patrz poniżej)

W przypadku awarii aplikacja Webex wysyła SIP REGISTER z dwoma nagłówkami kontaktu - jednym dla starej sesji i drugim z informacjami o nowym urządzeniu. Nagłówek kontaktu dla starej sesji jest dołączony, aby powiadomić kontroler SBC o konieczności oczyszczenia danych. Ten nagłówek zawiera expires=0 i q=0.5.

Poufne informacje Cisco

Nagłówek Kontakt z informacjami o nowym urządzeniu również ma wartość q, która jest odczytywana ze *znacznika<q-value>* . Wartość *<q-value>* tag służy do wskazania preferencji lub priorytetu określonego adresu kontaktowego. Zakres waha się od 0 do 1,0, przy czym 1,0 oznacza najwyższą preferencję, a 0 najniższą. Ten tag nie ma niestandardowego tagu do kontrolowania wartości - jest zakodowany na stałe do 1.0. Wartość można dostosować ręcznie, jeśli kontroler SBC użyty we wdrożeniu ma odwrotną logikę i traktuje q = 0,0 z maksymalnym priorytetem.

Począwszy od wersji 42.11, w szablonie konfiguracyjnym wprowadzono nową *sekcję <register-failover>* . Dodano nowy konfigurowalny parametr *<registration-cleanup>* w celu określenia, czy aplikacja wyśle nagłówek Kontakt, aby wyczyścić stare informacje o urządzeniu, czy nie. Niektóre kontrolery SBC czyszczą starą sesję natychmiast po rozłączeniu gniazda, więc istnienie nagłówka kontaktu dla starej sesji nie jest potrzebne. Domyślnie logika czyszczenia rejestracji jest włączona.

Dla zachowania spójności znacznik *<q-value>* jest również przenoszony do tej samej *sekcji <register-failover>* .

Przykład:

```
<config>
<protokoły><sip>
   <wartość q>1,0</wartość-q> <!-- PRZESTARZAŁE -->
   <register-failover>
      <registration-
cleanup>%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%</registration-cleanup>
      <wartość q>1,0</wartość q>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	true	prawda, fałsz	Kontroluje czyszczenie starych informacji o urządzeniu w przypadku awarii SIP.

6.1.8.2 Powrót protokołu SIP po awarii

Jeśli klient jest połączony z serwerem proxy, który nie jest pierwszy pod względem priorytetu, próbuje ponownie połączyć się z IP o najwyższym priorytecie. Czas powrotu po awarii zależy od DNS konfiguracji zarządzania czasem wygaśnięcia (patrz sekcja *6.1.8.4 Zarządzanie czasem wygaśnięcia* DNS). Jeśli połączenie jest w toku po osiągnięciu licznika czasu powrotu po awarii, 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 tylko podczas połączenia na telefonie komórkowym.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_FAILBACK_ENABLED_WXT%	true	prawda, fałsz	Włącza/wyłącza powrót protokołu SIP po awarii.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_FAILBACK_TIMEOUT_WXT%	900	Ponad 60	Limit czasu powrotu protokołu SIP po awarii w sekundach.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	prawda, fałsz	Dodaje losowy okres [0-10]% błędu awaryjnego SIP.

6.1.8.3 Wymuszanie wersji IP

Webex klienta można skonfigurować w taki sposób, aby uporządkować listę rozpoznanych hostów za pośrednictwem DNS, a następnie iterować przez nie w przypadku przełączenia awaryjnego SIP. We wszystkich trybach przestrzegany jest priorytet i waga.

Obsługiwane konfiguracje to:

- DNS — używa wszystkich adresów zwracanych przez zapytania DNS
- ipv4 - odfiltrowuje adresy IPv6
- IPv6 — odfiltrowywanie adresów IPv4
- prefer-IPv4 – kolejność adresów IPv4 przed IPv6 (wersja 42.9)
- prefer-IPv6 – porządkuje adresy IPv6 przed IPv4 (wersja 42.9)
- nat64 – ignoruje adresy IPv6, porządkuje adresy IPv4 (wersja 44.2)

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

W konfiguracji "dns" adresy IPv4 są traktowane priorytetowo w stosunku do adresów IPv6 dla danego hosta. Jeśli istnieją dwa hosty z adresami IPv4 i IPv6, kolejność będzie następująca: IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

W trybie "prefer-IPv4" adresy IPv4 są uporządkowane przed adresami IPv6 (pozostaje kolejność w grupach IPv4 i IPv6)

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, kolejność IPv4 jest przestrzegana. Prefiksy IPv6 zostaną wykryte. 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>
<protokoły><sip><transporty>
<enforce-ip-version>%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%</enforce-ip-version>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	Dns	protokół IPv4 IPv6 Dns prefer-IPv4 prefer-IPv6 nat64	Kontroluje kolejność adresów IPv4/IPv6 używanych przez klienta Webex do łączenia się z sesją SIP.

6.1.8.4 Zarządzanie czasem wygaśnięcia DNS

Dodano osobny parametr konfiguracyjny służący do zarządzania sposobem DNS rozpoznawania nazw po wygaśnięciu czasu wygaśnięcia rekordu DNS aktualnie używanego serwera. Jeśli parametr w poniższej tabeli jest włączony, wymusza na kliencie ponowienie DNS operacji po wygaśnięciu czasu wygaśnięcia rekordu SRV lub A DNS aktualnie używanego serwera.

Po ponownym zakończeniu rozpoznawania nazw DNS ten parametr wymusza również na kliencie ponowne nawiązanie połączenia z odebranym serwerem o najwyższym priorytecie, jeśli jest on inny niż aktualnie używany serwer, nawet jeśli bieżące połączenie działa w pełni. Jednak ponowne połączenie odbywa się dopiero po zakończeniu trwających połączeń.

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

Gdy ten parametr jest wyłączony, DNS operacje nie są powtarzane po wygaśnięciu czasu wygaśnięcia czasu wygaśnięcia, ale co 15 minut.

Ten parametr działa tylko dla SIP.

Należy zauważyć, że funkcji zarządzania DNS TTL nie można użyć, gdy w parametrze adresu serwera proxy jest używany adres IP.

> **UWAGA**: Jest to funkcja dostępna tylko dla komputerów stacjonarnych, ponieważ klienci mobilni mają połączenie SIP tylko podczas połączenia.

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


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_REFRESH_ON_TTL_WXT%	false	fałsz, prawda	Gdy DNS ustawieniu wartości "false", zarządzanie czasem wygaśnięcia jest wyłączone dla SIP. Po ustawieniu na "true" DNS zarządzanie czasem wygaśnięcia jest włączone dla SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	false	fałsz, prawda	Jeśli ta opcja jest włączona, dodaje losowy okres od 0 do 10% do DNS czasu wygaśnięcia.

UWAGA: Zdecydowanie zaleca się włączenie współczynnika losowego DNS TTL, aby zapobiec gwałtownemu wzrostowi liczby żądań kierowanych do DNS i potencjalnym skokom liczby prób ponownego nawiązania połączenia z serwerem aplikacji.

6.1.9 SIP SUBCSRIBE i REGISTER Odśwież i SUBSKRYBUJ Ponów próbę

Program Communicator obsługuje konfigurowanie interwałów odświeżania dla protokołów SIP SUBSCRIBE i REGISTER. W przypadku SIP SUBSCRIBE istnieje osobny parametr dla interwału odświeżania (w sekundach) i czasu oczekiwania przez klienta na ponowienie próby SIP SUBSCRIBE w przypadku wystąpienia błędów (w sekundach). Zalecana maksymalna wartość interwału ponawiania prób subskrypcji wynosi 2000000 sekundy, podczas gdy każda wartość ujemna, 0 lub pusta powoduje użycie 1800 sekund. Każda wartość ujemna *w przypadku odświeżania subskrypcji pomija nagłówek Wygasa* i w ten sposób tworzy jednorazową wartość SUBSCRIBE.

Zaproponowany przez klienta zegar odświeżania SIP REGISTER można skonfigurować w kilka sekund, ale zgodnie ze specyfikacją SIP serwer może nadpisać tę wartość. Obecnie klient zapamiętuje wartość zaproponowaną przez serwer dla kolejnych odświeżeń, zamiast zawsze używać skonfigurowanej wartości.

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

```
<config>
<protokoły><sip>
<subscription-refresh-interval>10800</subscription-refresh-interval>
<interwał ponawiania prób subskrypcji>60</interwał ponawiania prób subskrypcji>
<registration-refresh-interval>300</registration-refresh-interval>
<sesja>
       <expires-value>3600</expires-value>
</sesja>
```


Poufne informacje Cisco

6.1.10 Użyj P-Associated-URI w REGISTER

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

Jeśli parametr jest ustawiony na "false", klient nie używa identyfikatora *P-Associated-URI* i zamiast tego używa tożsamości z własnego URI SIP.

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

Jeśli parametr ma wartość "true", 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 identyfikatory URI nie są wyświetlane jako kontakty na liście kontaktów.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	prawda, fałsz	Umożliwia korzystanie z alternatywnych tożsamości w SIP REGISTER. W przypadku ustawienia "true" klient pobiera własną tożsamość z ostatniego *nagłówka P-Associated-URI dla wychodzących żądań SIP* . W przypadku ustawienia "false" jego własna tożsamość wychodzących żądań SIP jest pobierana z jego własnych URI SIP.

6.1.11 Nagłówek SIP P-Early Media (PEM)

Nagłówek SIP *P-Early Media* (PEM) może być używany na przykład w środowiskach IMS wewnątrz domeny zaufania, aby umożliwić sieci autoryzację wielu dialogowych wczesnych nośników SIP, na przykład w przypadkach, gdy inna sieć zezwala na wszystkie wczesne media.

Parametr konfiguracyjny umożliwia anonsowanie obsługi PEM w sygnalizacji SIP. Rzeczywista logika obsługi nośników na początku jest taka sama zarówno dla przypadków PEM, jak i innych niż PEM, działając na podstawie obsługiwanych wartości nagłówków PEM.

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

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_PEM_SUPPORT_WXT%	false	Prawda, fałsz	Ustaw wartość "true", aby umożliwić obsługę PEM reklamowania klienta w sygnalizacji SIP. Ustaw wartość "false", aby wyłączyć obsługę PEM reklamowania klienta w sygnalizacji SIP.

Poufne informacje Cisco

6.1.12 Obsługa aktualizacji SIP

SIP UPDATE jest potrzebny, na przykład, w niektórych wdrożeniach IMS, zamiast alternatywnego ponownego zaproszenia. Umożliwia klientowi aktualizację parametrów sesji, takich jak zestaw strumieni multimedialnych i ich kodeków, ale nie ma wpływu na stan okna dialogowego SIP.

Typowe przypadki użycia są związane z wczesnymi mediami, gdy na przykład używają sygnału dzwonka i alertu wstępnego jednocześnie.

SIP UPDATE jest obecnie obsługiwany tylko wtedy, gdy jest odbierany w przypadkach użycia przed dialogiem (wczesne media), a nie podczas aktywnego okna dialogowego, na przykład w przypadku zawieszania/wznawiania połączenia, gdy funkcja re-INVITE jest nadal używana.

W tej wersji nie można dodawać wideo do audio 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%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	prawda, fałsz	Po ustawieniu na "false" obsługa SIP UPDATE jest wyłączona. Po ustawieniu na "true" włączona jest obsługa SIP UPDATE.

6.1.13 Starsze informacje o SIP FIR

Ten klient obsługuje starszy sposób żądania klatek kluczowych wideo za pośrednictwem żądania sterowania multimediami SIP INFO. Jest to konieczne, ponieważ niektóre urządzenia mają problemy z reagowaniem na RTCP-FB FIR i czasami RTCP nie docierają do zdalnego punktu końcowego, co może prowadzić do braku wideo lub jednokierunkowego wideo. Aby uzyskać więcej informacji, zobacz *RFC 5168*.

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


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false	Prawda, fałsz	Po ustawieniu na "false" obsługa SIP INFO FIR jest wyłączona. Po ustawieniu na "true" włączona jest obsługa SIP INFO FIR.

6.1.14 Zarządzanie portami SIP dla przechodzenia translacji adresów sieciowych

Klienta można skonfigurować tak, aby używał mechanizmu rport SIP do przechodzenia przez translację adresów sieciowych. Należy pamiętać, że zazwyczaj nie może to być jedyne rozwiązanie do przechodzenia translacji adresów sieciowych, a SBC jest używany głównie do tego celu. Opis specyfikacji portu można znaleźć *w dokumencie RFC 3581*.

Więcej informacji na temat zaleceń dotyczących portów SIP i protokołów transportowych, gdy w sieci są używane bramy warstwy aplikacji SIP (ALG), zobacz *Webex przewodnika po rozwiązaniach* Cisco BroadWorks.

Należy zauważyć, że ciąg "rport" jest zawsze obecny w wychodzących żądaniach SIP, niezależnie od konfiguracji. Ten parametr wpływa tylko na użycie adresu IP i portu odebranego z serwera w nagłówkach SIP "received" i "rport". Gdy funkcja jest włączona, wartości z nagłówków "received" i "rport" są używane w nagłówku SIP Contact żądań SIP (nawet jeśli w odpowiedzi REGISTER brakuje nagłówka "received").

Parametr *Preferred-port* jest powiązany w tym, że inaczej definiuje port używany w nagłówku kontaktu SIP. Więcej informacji na temat przydzielania portów SIP można znaleźć w sekcji *6.1.7 Preferowane użycie portu dla* SIP.

Istnieje osobny parametr *konfiguracyjny use-local-port* , który wymusza ustawienie lokalnego portu gniazda klienta w nagłówku *Kontakt* . Jest to używane w przypadku niektórych kontrolerów SBC, które wykrywają, że klient ma rzeczywisty IP (z nagłówka Kontakt *),* a kontroler SBC próbuje ustanowić osobne gniazdo dla swoich żądań. W większości przypadków między kontrolerem SBC a klientem znajduje się zapora, która odmawia połączeń przychodzących do klienta.

> **UWAGA:** W środowiskach IPv6 wszystkie adresy są rzeczywiste i kontroler SBC próbuje nawiązać połączenie z adresem klienta nasłuchującego (z *nagłówka Kontakt*).

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


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_USE_RPORT_WXT%	false	prawda, fałsz	Włącza port dla połączeń audio i wideo.
%RPORT_USE_LOCAL_PORT_WXT%	false	prawda, fałsz	Określa, czy lokalny port gniazda klienta ma zostać dodany w nagłówku Kontakt *SIP* .

6.1.15 SIP Session ID (Identyfikator sesji SIP)

Po włączeniu tej opcji podczas początkowej rejestracji generowany jest lokalny identyfikator sesji. Identyfikator sesji jest używany przez cały okres istnienia połączenia/sesji dla tego urządzenia, dla wszystkich okien dialogowych poza połączeniem, ZAREJESTRUJ, SUBSKRYBUJ, POWIADAMIAJ i tak dalej. Ten sam identyfikator sesji jest używany do momentu utraty powiązania. W przypadku utraty powiązania rejestracji (wyszukiwanie DNS, zresetowanie połączenia, zresetowanie telefonu itd.) generowany jest nowy lokalny identyfikator sesji.

Wartość identyfikatora sesji może służyć do znajdowania pełnego zestawu okien dialogowych powiązanych z tym urządzeniem.

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

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SIP_SESSION_ID_WXT%	false	Prawda, fałsz	Kontroluje użycie identyfikatora sesji SIP.

6.1.16 Odrzucanie połączeń przychodzących

Klient oferuje możliwość odrzucenia połączenia z *numerem 486* lub *603*.

Należy zauważyć, że jeśli klient jest skonfigurowany do odrzucania połączenia z *opcją Odrzuć* 603, usługi Przekierowywanie połączeń zajęte i Przekierowywanie połączeń bez odpowiedzi mogą nie działać zgodnie z oczekiwaniami.

```
<config>
<usługi><połączenia>
<reject-with-486 enabled="%ENABLE_REJECT_WITH_486_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_REJECT_WITH_486_WXT%	true	prawda, fałsz	Kontroluje kod błędu SIP i przyczynę używaną do odrzucania przychodzących połączeń SIP. Jeśli ta opcja jest włączona,486 *Tymczasowo niedostępny* . W przeciwnym razie *używany jest 603 Decline* .

6.1.17 Zakres portów protokołu transportowego w czasie rzeczywistym

Klienta można skonfigurować tak, aby używał zdefiniowanego zakresu portów dla strumieni protokołu RTP (Real-Time Transport Protocol), co ma również zastosowanie do SRTP. Ta konfiguracja odbywa się przez ustawienie wartości granicznych zakresu portów dla strumieni audio i wideo za pomocą tagów pokazanych w poniższym przykładzie.

```
<config>
<protokoły><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	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	numer	Początek zakresu portów audio.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	numer	Koniec zakresu portów audio.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	numer	Początek zakresu portów wideo.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	numer	Koniec zakresu portów wideo.

UWAGA: Zakresy portów powinny być ustawione tak, aby nigdy się nie nakładały.

6.1.18 Obsługa ICE(tylko Webex Calling)

Klient obsługuje negocjacje Interactive Connectivity Establishment (ICE), które umożliwiają optymalizację ścieżki nośników między punktami końcowymi (w trybie peer-to-peer). Ma to na celu zmniejszenie opóźnień danych, zmniejszenie utraty pakietów i zmniejszenie kosztów operacyjnych wdrażania aplikacji.

Poufne informacje Cisco

Zauważ, że bieżąca implementacja obsługuje serwer STUN, podczas gdy TURN nie jest obsługiwana.

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

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

```
<config>
<protokoły><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	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_RTP_ICE_WXT%	false	prawda, fałsz	Włącz / wyłącz obsługę ICE.
%RTP_ICE_MODE_WXT%	icestun	icestun	Tryb obsługi ICE. Obecnie jedyną obsługiwaną wartością jest "icestun".
%RTP_ICE_SERVICE_URI_WXT%	(puste)	prawidłowy serwer STUN URI lub (pusty)	Serwer STUN URI.
%RTP_ICE_PORT_WXT%	3478	Numer (0-65535)	Port serwera STUN.
%ENABLE_RTP_ICE_IPV6_WXT%	false	prawda, fałsz	Włącza ICE przez IPv6.

6.1.19 RTCP MUX

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

- Tryb zgodności z poprzednimi wersjami (tzn. 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 po raz drugi w sekcji m=video)

Obraz i dźwięk nie używają tego samego portu.

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

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

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	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 Przenoszenie

Webex klienta Cisco BroadWorks obsługuje przekazywanie połączeń nadzorowanych (konsultacyjnych), półkonsultacyjnych i bezpośrednich (ślepych).

Pół-konsultacyjne przekazywanie połączeń umożliwia dzwoniącemu zakończenie transferu, zanim połączenie zostanie odebrane przez zdalnego rozmówcę. Przycisk zakończenia półkonsultacyjnego jest włączony dla dzwoniącego dopiero po rozpoczęciu dzwonienia po stronie dzwoniącego i otrzymaniu odpowiedniego powiadomienia SIP (*180 dzwonków*) po stronie dzwoniącego. Przeniesienie w ciemno nosi nazwę "Przenieś teraz" w interfejsie użytkownika.

> **UWAGA**: Dzwonienie *SIP* 180 może nie być wyzwalane w niektórych środowiskach, dla niektórych numerów lub w niektórych scenariuszach komunikacji między serwerami.

Wersja 43.9 aplikacji Webex wprowadza przekazywanie do innego samodzielnego trwającego połączenia tego samego typu. Połączenia zakończone w aplikacji Webex można przekierowywać do innych połączeń zakończonych w lokalnym punkcie końcowym. Połączenia zakończone na urządzeniu zdalnym można przenosić na połączenia zakończone na zdalnym punkcie końcowym. Ta funkcja nie ma konfigurowalnych opcji.

Począwszy od wersji 43.12, aplikacja Webex dodaje opcję konfiguracji, aby określić, czy bieżące połączenie ma być automatycznie wstrzymywane po wybraniu pozycji menu Przekaż. To zachowanie jest kontrolowane przez nowy *atrybut auto-hold* . Domyślnie automatyczne wstrzymywanie jest wyłączone.

```
<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%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_TRANSFER_CALLS_WXT%	false	prawda, fałsz	Po ustawieniu wartości "true" przekazywanie połączeń jest włączone. Po ustawieniu wartości "false" przekazywanie połączeń jest wyłączone.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false	prawda, fałsz	Włącza opcje transferu dla połączeń zdalnych (XSI) zakończonych w innej lokalizacji.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%TRANSFER_CALL_TYPE_WXT%	pełny	najpierw mów, niewidomy, pełny	Określa typy transferu dostępne dla użytkownika w konfiguracji BroadWorks.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	prawda, fałsz	Określa, czy aktywne połączenie zostanie automatycznie zawieszone, gdy użytkownik wybierze opcję Przekaż z menu ekranu w trakcie połączenia.

6.1.21 N-Way połączenia konferencyjne i uczestnicy

Za pomocą poniższego tagu niestandardowego można kontrolować dostępność połączenia konferencyjnego Ad Hoc (N-Way) za pośrednictwem protokołu SIP w Webex klienta Cisco BroadWorks. Ponadto właściciel N-way może zobaczyć pełną listę uczestników za pośrednictwem SIP SUBSCRIBE / NOTIFY i pakietu wydarzeń konferencyjnych. Klient właściciela dowiaduje się, URI wysłać SIP SUBSCRIBE za pośrednictwem poprzedzającego nagłówka *kontaktu* SIP *wiadomości 200 OK* wysłanej w odpowiedzi na INVITE do URI konferencji, podczas gdy dla uczestników ta sama informacja znajduje się w poprzedzającej rozmowie NOTIFY.

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

Te informacje są pobierane z serwera aplikacji (AS) przy użyciu następującego polecenia interfejsu wiersza polecenia (CLI).

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

Przykładowe dane wyjściowe:
maxConferenceParty = 6
conferenceURI =
```

Po uzyskaniu wartości *maxConferenceParties* (która ma zakres od 4 do 15), tag %MAX_CONF_PARTIES_WXT% powinien zostać odpowiednio ustawiony.

```
<config>
<usługi><połączenia>
<konferencja włączona="%ENABLE_CONFERENCE_CALLS_WXT%">
    <service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-1%</service-uri>
    <subscribe-conference-info enabled="%ENABLE_NWAY_PARTICIPANT_LIST_WXT%"/>
        <max-nway-participants>%MAX_CONF_PARTIES_WXT%</max-nway-participants>
</konferencja>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	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 wartość "true", aby włączyć N-way owner participant list. Ustaw wartość "false", aby wyłączyć N-way owner participant list.
%MAX_CONF_PARTIES_WXT%	10	Liczba od 4 do 15 (puste)	Określa maksymalną liczbę uczestników N-way, wymuszoną przez klienta, na przykład 10. Strona serwera ma swoje ograniczenia. Pusta wartość wyłącza wymuszanie po stronie klienta limitu uczestników N-way.

6.1.22 Ściąganie połączeń

Funkcję ściągania połączenia można włączyć przy użyciu jednego parametru konfiguracji, jak pokazano w poniższym przykładzie.

```
<config>
<usługi><połączenia>
<call-pull enabled="%ENABLE_CALL_PULL_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_PULL_WXT%	false	Prawda, fałsz	Włącza ściąganie połączeń.

6.1.23 Wywołanie Parkuj/Odzyskaj

Funkcja grupowego parkowania połączeń umożliwia przekazywanie trwających połączeń VoIP do serwera parkowania połączeń, co pozwala dzwoniącemu zrobić coś innego i pobrać je przez tego samego użytkownika lub innego użytkownika. Trwające połączenie zostanie zaparkowane przy pierwszym dostępnym numerze wewnętrznym w ramach Call Park Group.

Pobieranie połączenia może być wykonywane przez użytkownika parkującego połączenie w oknie dialogowym przez konfigurowalną liczbę sekund bezpośrednio po zaparkowaniu połączenia. Zaparkowane połączenie może też zostać odebrane przez użytkownika lub innego użytkownika, wybierając opcję pobierania połączenia i wprowadzając numer lub numer wewnętrzny.

```
<config>
<usługi><połączenia>
<call-park enabled="%ENABLE_CALL_PARK_WXT%"
timer="%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_PARK_WXT%	false	Prawda, fałsz	Umożliwia parkowanie/odbieranie połączeń.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Liczba od 5 do 30	Określa liczbę sekund, przez które pomyślne okno dialogowe Zaparkowane połączenie jest widoczne dla użytkownika, zanim zostanie automatycznie zamknięte.

6.1.24 Statystyki połączeń

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

```
<config>
<usługi><połączenia>
<Statystyka połączeń włączona="%ENABLE_CALL_STATISTICS_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_STATISTICS_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby umożliwić przechwytywanie metryk połączeń. Ustaw wartość "false", aby wyłączyć przechwytywanie metryk połączeń.

6.1.25 Automatyczne przywracanie połączeń/bezproblemowe przekazywanie połączeń

Klient obsługuje automatyczne odzyskiwanie połączenia przy przełączaniu sieci, podczas gdy użytkownik ma trwające połączenie VoIP. Automatyczne odzyskiwanie połączenia działa w obu kierunkach - Cellular Data-to-WiFi i WiFi-to-Cellular Data, a także podczas przełączania między sieciami WiFi. Próbuje się odzyskać połączenie w ciągu jednej minuty, a następnie zostaje zatrzymane. Jeśli trwa więcej niż jedno VoIP połączenia, odzyskiwane jest tylko aktywne.

W przypadku przejścia z danych komórkowych na sieć Wi-Fi klient będzie kontynuował trwające połączenia VoIP danych komórkowych do momentu zakończenia transmisji danych lub utraty sieci komórkowej.

```
<config>
<usługi><połączenia>
```


Poufne informacje Cisco

```
<automatyczne odzyskiwanie włączone="%ENABLE_CALLS_AUTO_RECOVERY_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false	prawda, fałsz	Określa, czy mechanizm automatycznego odzyskiwania powinien być włączony dla użytkownika.

6.1.26 Nagrywanie rozmów

Funkcja nagrywania rozmów jest obsługiwana przez klienta i zależy od dostępności 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 SIP X-BroadWorks-Correlation-Info* (patrz Webex *przewodnika po rozwiązaniach* Cisco BroadWorks).

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

Jeśli funkcja nagrywania rozmów jest włączona, zawsze pojawia się wizualne wskazanie, kiedy połączenie jest nagrywane. Następujące tryby nagrywania rozmów są obsługiwane przez Cisco BroadWorks:

Zawsze

- Nagrywanie rozmów zostanie uruchomione automatycznie podczas nawiązywania połączenia.
- Użytkownik NIE **jest** w stanie zatrzymać/wstrzymać nagrywania rozmowy.

Zawsze z obsługą pauzy/wznawiania

- Nagrywanie połączeń rozpocznie się automatycznie podczas nawiązywania połączenia, ale użytkownik będzie mógł wstrzymać i wznowić połączenie.
- Możliwe interakcje użytkownika:
  - Nagrywanie jest w toku – **Wstrzymaj** nagrywanie.
  - Nagrywanie jest wstrzymane – **wznów** nagrywanie.

Na żądanie

- Po nawiązaniu połączenia rozpocznie się nagrywanie rozmowy na serwerze.
- Jeśli użytkownik naciśnie opcję Rozpocznij nagrywanie podczas połączenia, nagranie rozmowy zostanie zapisane i połączenie nie zostanie uruchomione. W przeciwnym razie, jeśli użytkownik nie rozpocznie nagrywania, nagranie rozmowy zostanie usunięte z serwera.
- Możliwe interakcje użytkownika:

Poufne informacje Cisco

- Nagrywanie jeszcze się nie rozpoczęło –Rozpocznij nagrywanie.
- Nagrywanie jest w toku – **Wstrzymaj** nagrywanie.
- Nagrywanie jest wstrzymane – **wznów** nagrywanie.

Na żądanie po zainicjowaniu przez użytkownika

- Użytkownik może rozpoczynać, zatrzymywać, wstrzymywać i wznawiać nagrywanie połączenia w dowolnym momencie, kilka razy w trakcie połączenia.
- Dla każdego uruchomienia nagrywania rozmów będą dostępne osobne nagrania rozmów.
- Możliwe interakcje użytkownika:
  - Nagrywanie jeszcze się nie rozpoczęło –Rozpocznij nagrywanie.
  - Trwa nagrywanie — **zatrzymaj** i **wstrzymaj** nagrywanie.
  - Nagrywanie jest wstrzymane – **zatrzymaj** i **wznów** nagrywanie.

Tryb nagrywania połączeń przypisany do użytkownika można wybrać z Centrum sterowania.

```
<config>
<usługi><połączenia>
<rekord włączony="%ENABLE_CALL_RECORDING_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_RECORDING_WXT%	false	prawda, fałsz	Włącza elementy sterujące nagrywaniem rozmów.

6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik oczekujących wiadomości

Za pomocą poniższych tagów niestandardowych można kontrolować dostępność poczty głosowej i wizualnej poczty głosowej Cisco BroadWorks w Webex klienta Cisco BroadWorks. Należy zauważyć, że tag systemowy Cisco BroadWorks (%BWVOICE-PORTAL-NUMBER-1%) jest używany z pocztą głosową.

Wizualna poczta głosowa (VVM) jest obsługiwana tylko dla dźwięku. Obsługiwane formaty to wav, ulaw i mov zawierające wideo H264 (odtwarzane tylko jako dźwięk). Umożliwia użytkownikom przeglądanie przychodzących wiadomości głosowych w widoku listy i odtwarzanie poszczególnych elementów. Ta funkcja jest oparta na Xsi, ale powiadomienia o nowej poczcie głosowej są dostarczane przez SIP; W związku z tym protokół SIP musi być włączony, aby powiadomienia działały. Ponadto do nadejścia powiadomień wymagana jest konfiguracja SIP SUBSCRIBE for Message Waiting Indicator (MWI), a MWI musi być włączona, aby wizualna poczta głosowa działała. Więcej informacji na temat konfiguracji protokołu SIP można znaleźć w sekcji *6.1.1 Ustawienia serwera SIP*.

Wymagania dotyczące wydania i poprawek dla wizualnej poczty głosowej w programie Cisco BroadWorks można znaleźć w
Webex Przewodniku po rozwiązaniu Cisco BroadWorks.

Poufne informacje Cisco

Wizualna poczta głosowa musi być włączona osobno w konfiguracji.

Do korzystania z wizualnej poczty głosowej w portalu CommPilot wymagane są następujące ustawienia:

- Wiadomości głosowe włączone
- Włączona opcja "Po nadejściu wiadomości użyj usługi Unified Messaging"
- Włączona opcja "Użyj wskaźnika wiadomości oczekujących na telefon"

Brak przypisania usługi wizualnej poczty głosowej po stronie Cisco BroadWorks dla użytkownika powoduje automatyczne wyłączenie konfiguracji usługi.

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

Aby informacje o wiadomościach poczty głosowej były wyświetlane w interfejsie użytkownika, klient musi otrzymywać powiadomienia MWI SIP z serwera (czyli pakiet zdarzeń poczty głosowej). W poniższej tabeli przedstawiono opcje subskrypcji. Należy również pamiętać, że MWI jest potrzebne do działania powiadomień wizualnej poczty głosowej.

Należy zauważyć, że jeśli subskrypcja SIP pakietu zdarzeń poczty głosowej nie powiedzie się, klient będzie kontynuował ponowienie próby, jeśli zostanie to skonfigurowane. Więcej informacji na temat konfiguracji ponownych prób SIP SUBSCRIBE można znaleźć w sekcji *6.1.9 SIP SUBCSRIBE i REGISTER Odśwież i SUBSKRYBUJ Ponów* próbę.

```
<config>
<usługi><połączenia>
<mwi enabled="%ENABLE_MWI_WXT%" type="%MWI_MODE_WXT%"/>
<voice-mail enabled="%ENABLE_VOICE_MAIL_WXT%" visual-
voicemail="%ENABLE_VISUAL_VOICE_MAIL_WXT%">
    <numer_centralny>%BWNUMER-PORTALU-GŁOSOWEGO-1%</numer-centrum>
</poczta głosowa>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_VOICE_MAIL_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć obsługę poczty głosowej. Ustaw wartość "false", aby wyłączyć obsługę poczty głosowej.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	prawda, fałsz	Po ustawieniu wartości "false" maszyna wirtualna jest wyłączona. Po ustawieniu wartości "true" maszyna wirtualna jest włączona. Należy zauważyć, że poczta głosowa enabled=false, zanim rzeczywisty atrybut VVM będzie nadal używany w celu zapewnienia zgodności z poprzednimi wersjami.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%BWVOICE-PORTAL-NUMBER-1%	pusty	numer	Klient dzwoni pod ten numer, zwykle określony przy użyciu istniejącego tagu systemowego Cisco BroadWorks podczas wybierania poczty głosowej.
%ENABLE_MWI_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć MWI. Ustaw na "false", aby wyłączyć MWI.
%MWI_MODE_WXT%	pusty	niejawne, jawne	Ustaw na "explicit", aby wysyłać SIP SUBSCRIBE dla pakietu zdarzeń MWI, gdy MWI jest włączona. Użycie opcji "implicit" nie powoduje wysłania pakietu zdarzeń SIP SUBSCRIBE dla MWI, gdy jest włączona MWI. Jeśli pozostanie pusta, MWI zostanie wyłączona.

6.1.28 Transkrypcja poczty głosowej dla Webex Calling

Dzięki tej funkcji wiadomości poczty głosowej są konwertowane na tekst i wyświetlane w widoku wizualnych wiadomości poczty głosowej w aplikacjach komputerowych i mobilnych Webex Calling.

Funkcja powinna być włączona dla użytkownika tylko wtedy, gdy:

1. Aplikacja jest uruchomiona w Webex Calling wdrożeniu.
2. Funkcja wizualnej poczty głosowej jest włączona dla użytkownika.
3. Funkcja jest włączona w config (atrybut enabled w tagu <services><voice-mail><transcription> powinien mieć wartość "true").

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

6.1.29 Ustawienia połączeń

6.1.29.1 Przekierowywanie połączeń zawsze

Za pomocą poniższego tagu niestandardowego można kontrolować dostępność usługi Always przekierowywania połączeń Cisco BroadWorks w Webex klienta Cisco BroadWorks.

```
<config>
<usługi><usługi uzupełniające>
```


Poufne informacje Cisco

```
<przekazywanie połączeń-zawsze włączone="%ENABLE_CALL_FORWARDING_ALWAYS_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	prawda, fałsz	Kontroluje dostępność usługi Zawsze przekierowywanie połączeń. Domyślnie ta funkcja jest wyłączona.

UWAGA: Funkcje Przekierowywanie połączeń zawsze i przekierowywanie połączeń do poczty głosowej (*6.1.29.2 Przekierowywanie połączeń do poczty* głosowej) mogą być używane razem do wyświetlania lub ukrywania ustawienia "Przekierowywanie połączeń" w Webex aplikacjach. Gdy oba tagi są wyłączone, ustawienie "Przekazywanie połączeń" w aplikacjach Webex jest ukryte.

6.1.29.2 Przekierowywanie połączeń do poczty głosowej

Począwszy od wersji 43.9, aplikacja Webex oferuje opcję kontrolowania dostępności przekazywania do poczty głosowej. Domyślnie funkcja jest włączona i można ją wyłączyć za pomocą następującej opcji konfiguracji.

```
<config>
<usługi>
   <poczta głosowa>
      <przekazywanie włączone="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	true	prawda, fałsz	Kontroluje dostępność funkcji przekazywania do poczty głosowej. Domyślnie funkcja ta jest włączona.

UWAGA 1: Ta funkcja zależy od jednej z usług "Użytkownik wiadomości głosowych" lub "Obsługa poczty głosowej innej firmy", która ma zostać przypisana do użytkownika.

UWAGA 2: Przekierowywanie połączeń do poczty głosowej i Przekierowywanie połączeń zawsze (*6.1.29.1 Przekierowywanie połączeń zawsze*) może być używane razem do wyświetlania lub ukrywania ustawienia "Przekazywanie połączeń" w Webex aplikacjach. Gdy oba tagi są wyłączone, ustawienie "Przekazywanie połączeń" w aplikacjach Webex jest ukryte.

Poufne informacje Cisco

6.1.29.3 BroadWorks Anywhere (Single Number Reach)

Następujące tagi niestandardowe sterują dostępnością usługi BroadWorks Anywhere i dostępnością jej ustawień w Webex klienta Cisco BroadWorks. Pamiętaj, że nazwa tej funkcji wewnątrz klienta 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	Domyślne, jeśli zostało pominięte	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 ma być dostępny dla użytkownika.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby udostępnić użytkownikowi opcję Alert All Locations dla usługi BWA. Ustaw wartość "false", aby opcja Alert All Locations dla usługi BWA była niedostępna dla użytkownika.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	false	prawda, fałsz	Określa, czy aplikacja powinna włączać stan Alert All Locations (Alert All Locations) podczas dodawania drugiej lub każdej kolejnej nowej lokalizacji BWA.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	prawda, fałsz	Określa, czy sterowanie połączeniami w lokalizacji BWA ma być dostępne dla użytkownika.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	false	prawda, fałsz	Kontroluje domyślny stan sterowania połączeniami dla lokalizacji BWA.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	prawda, fałsz	Kontroluje, czy inhibitor zmiany kierunku lokalizacji BWA powinien być dostępny dla użytkownika.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	prawda, fałsz	Steruje domyślnym stanem inhibitora dywersji lokalizacji BWA.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false	prawda, fałsz	Określa, czy potwierdzenie odpowiedzi lokalizacji BWA powinno być dostępne dla użytkownika.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	false	prawda, fałsz	Steruje domyślnym stanem potwierdzenia odpowiedzi lokalizacji BWA.

6.1.30 Portal ustawień i internetowe ustawienia połączeń

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

Ponadto klient udostępnia opcję użycia widoku internetowego ustawień połączeń (CSWV). Dzięki temu użytkownik może kontrolować więcej ustawień połączeń opartych na serwerze. Za pomocą oddzielnych tagów można kontrolować, czy określone usługi powinny być widoczne w ustawieniach połączeń internetowych.

> **UWAGA:** Zaleca się ukrycie ustawień, które są już widoczne w aplikacji, takich jak Call Center (patrz sekcja *6.1.31 Call Center / Logowanie / Wylogowanie z* kolejki połączeń) i BroadWorks Anywhere (patrz sekcja *6.1.29.3 BroadWorks Anywhere*). Usługa Remote Office powinna być również ukryta, ponieważ została zastąpiona przez usługę BroadWorks Anywhere.

Do skonfigurowania adresu URL portalu ustawień (Self Care lub CSWV) można użyć następującego tagu niestandardowego. Jeśli tag jest pusty, łącze do portalu ustawień nie jest widoczne dla użytkownika w aplikacji.

```
<config>
<usługi>
<web-call-settings target="%WEB_CALL_SETTINGS_TARGET_WXT%"
 <url>%WEB_CALL_SETTINGS_URL_WXT%</url>
<branding-enabled="%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%">
  <ustawienia usługi>
   <nazwa usługi="Zawsze przekierowywanie połączeń"
visible="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <nazwa usługi="Przekierowywanie połączeń zajęte"
visible="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <nazwa usługi="Przekierowywanie połączeń jest nieosiągalne"
visible="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
   <nazwa usługi="Przekierowywanie połączeń bez odpowiedzi"
visible="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <service name="Nie przeszkadzać" visible="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
   <nazwa usługi="Odrzucenie połączenia anonimowego"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="Simultaneous Ring Personal"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
```


Poufne informacje Cisco

```
   <service name="Sequential Ring"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <service name="Automatyczne wywołanie zwrotne"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <nazwa usługi="Połączenie oczekujące"
visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Calling Line ID Delivery Blocking"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <nazwa usługi="Asystent osobisty" 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%"/>
   <nazwa usługi="BroadWorks Mobility"
visible="%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <nazwa usługi="Zdalne biuro" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Użytkownik wiadomości głosowych"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
</ustawienia połączeń internetowych>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%WEB_CALL_SETTINGS_TARGET_WXT%	zewnętrzny	zewnętrzne, CSW	Kontroluje tryb portalu administracyjnego. Ustaw wartość "external", aby otworzyć skonfigurowany adres URL portalu ustawień w przeglądarce zewnętrznej. Ustaw wartość "csw", aby otworzyć portal CSW we wbudowanej przeglądarce przy użyciu sekcji dodatkowych parametrów <services><web-call-settings> z żądania POST.
%WEB_CALL_SETTINGS_URL_WXT%	pusty	Ciąg adresu URL	Adres URL portalu ustawień. Przykład: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Zawsze przekierowywanie połączeń ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Nie przeszkadzać (DND) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Anonimowe odrzucanie połączeń (ACR, Anonymous Call Rejection) ma być widoczna dla użytkownika w ustawieniach sieci Web.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Przekierowywanie połączeń zajęte (CFB, Call Forwarding Busy – CFB) ma być widoczna dla użytkownika w ustawieniach sieci Web.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Przekierowywanie połączeń nieosiągalne (CFNR) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja CFNA (Call Forwarding No Answer) ma być widoczna dla użytkownika w ustawieniach sieci Web.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Simultaneous Ring Personal (SIMRING) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Dzwonek sekwencyjny (SEQRING) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Biuro zdalne (RO) ma być widoczna dla użytkownika w ustawieniach sieci Web.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja automatycznego wywołania zwrotnego (ACB, Automatic Callback) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Połączenie oczekujące (CW) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Calling Line ID Delivery Blocking (CLIDB) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Asystent osobisty (PA) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja BroadWorks Anywhere (BWA) ma być widoczna dla użytkownika w ustawieniach sieci Web.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Call Center ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja BroadWorks Mobility (BWM) ma być widoczna dla użytkownika w ustawieniach internetowych. Obecnie zalecana wartość to "false" z powodu problemów ze współdziałaniem między Webex dla Cisco BroadWorks i BroadWorks Mobility.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcja Zarządzanie głosem (VM) ma być widoczna dla użytkownika w ustawieniach internetowych.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false	prawda, fałsz	Określa, czy mają być używane nowe ustawienia połączeń WebView znakowanie. Włącz, jeśli wersja CSWV po stronie serwera to 1.8.6 lub nowsza. W przeciwnym razie zachowaj fałsz.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	true	prawda, fałsz	Określa, czy opcje wiadomości e-mail/poczty głosowej mają być widoczne w ustawieniach internetowych.
%USER_PORTAL_SETTINGS_URL_WXT%	pusty	Ciąg adresu URL	Określa adres URL portalu ustawień użytkownika. Aby włączyć tę funkcję i zaprezentować przycisk Access User Portal w interfejsie użytkownika, ten tag niestandardowy nie powinien być pusty. Na przykład: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	zewnętrzny	Zewnętrzne, wewnętrzne	Określa, czy adres URL powinien być otwierany w przeglądarce osadzonej czy zewnętrznej.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false	Prawda, fałsz	Ma zastosowanie tylko wtedy, gdy skonfigurowana jest wbudowana przeglądarka (USER_PORTAL_SETTINGS_TARGET_WXT=wewnętrzna). Po włączeniu tej opcji używane jest żądanie HTTP POST, a krótkotrwały token BroadWorks jest dodawany jako część BODY. Po wyłączeniu adres URL jest otwierany za pomocą protokołu HTTP GET.

UWAGA 1: Adres URL ustawień połączeń WebView powinien zawsze mieć skonfigurowany końcowy znak "/". Na przykład: https://<XSP-FQDN>/<CSW-Context-Path>/

UWAGA 2: Minimalna obsługiwana wersja aplikacji Ustawienia połączeń WebView to 1.7.5.

W przypadku instalacji programu Cisco BroadWorks w wersji 21.0 zapoznaj się z dodatkowymi krokami opisanymi w *Webex Podręczniku rozwiązania Cisco BroadWorks*.

Poufne informacje Cisco

6.1.31 Call Center / Logowanie / Wylogowanie z kolejki połączeń

Aplikacja Webex zapewnia dostęp do ustawień agenta Call Center (kolejki połączeń). Jeśli użytkownik jest obsługiwany przez biuro obsługi, ta funkcja umożliwia mu zalogowanie się do biura obsługi i przeglądanie dostępnych kolejek połączeń, a także dołączanie/odłączanie kolejek i ustawianie stanu automatycznej dystrybucji połączeń (ACD).

Począwszy od wersji Desktop 42.8 i Mobile w wersji 42.12, agent Call Center (kolejka połączeń) nie jest już oparty na widoku sieci Web ustawień połączeń (patrz sekcja *6.1.30 Portal ustawień i internetowe ustawienia połączeń*). Konfiguracja agenta Call Center (kolejki połączeń) jest dostępna poprzez stopkę pulpitu i Ustawienia aplikacji Mobile Webex.

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

Znacznik	Domyśln e, jeśli zostało pominięt e	Obsługiwa ne wartości	Opis
%ENABLE_CALL_CENTER_WXT%	false	prawda, fałsz	Włącza obsługę Call Center.

6.1.32 Katalog główny XSI i ścieżki

Webex klienta Cisco BroadWorks używa następujących znaczników do sterowania ścieżką katalogu głównego, akcji i zdarzeń XSI, jeśli muszą one różnić się od tych używanych do logowania.

Głównym powodem zmiany katalogu głównego XSI jest zaimplementowanie równoważenia obciążenia na poziomie konfiguracji, chociaż zaleca się stosowanie równoważenia obciążenia w warstwie HTTP.

Ścieżki zdarzeń i akcji są zazwyczaj zmieniane ze względu na wymagania dotyczące znakowania w celu usunięcia *odwołania do domeny com.broadsoft* ze ścieżek adresów URL żądań XSI HTTP wykonywanych przez klienta.

```
<config>
<protokoły><xsi>
       <ścieżki>
              <root>%XSI_ROOT_WXT%</root>
              <akcje>%XSI_ACTIONS_PATH_WXT%</akcje>
              <events>%XSI_EVENTS_PATH_WXT%</events>
       </ścieżki>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%XSI_ROOT_WXT%	Nadal używa oryginalnego używanego do pobierania konfiguracji.	Ciąg adresu URL	Katalog główny XSI dla wszystkich operacji XSI. Przykład: https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	łańcuch	Określa ścieżkę Akcje XSI. Powinien zaczynać się i kończyć znakiem "/" i zawierać tylko kontekst akcji. Przykład: /com.domena.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	łańcuch	Określa ścieżkę zdarzeń XSI. Powinien zaczynać się i kończyć znakiem "/" i zawierać tylko kontekst zdarzeń. Przykład: /com.domena.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 rozmów

Puls zdarzeń XSI jest używany do utrzymywania otwartego kanału zdarzeń XSI, a interwał pulsu można określić za pomocą następującego parametru.

```
<config>
<protokoły><xsi>
<event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
    <interwał uderzeń serca> %CHANNEL_HEARTBEAT_WXT%</interwał pulsu>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_XSI_EVENT_CHANNEL_WXT%	true	prawda, fałsz	Określa, czy kanał zdarzeń XSI jest włączony. Powinna być ustawiona na wartość "true", aby odbierać na przykład zdarzenia związane z usługą sterowania w trakcie połączenia. Zalecana wartość to "true".
%CHANNEL_HEARTBEAT_WXT%	10000	numer	Jest to puls kanału zdarzenia XSI (w milisekundach). Wartość domyślna to "10000".

Poufne informacje Cisco

6.1.34 Konfiguracja kodeka

Webex dla Cisco BroadWorks oferuje wiele kodeków audio i wideo. Odpowiednie listy kodeków znajdują się w sekcjach *config/services/calls/* w sekcjach *audio/kodeki* i *video/kodeki* . Priorytet każdego kodeka można zmienić za pomocą *priorytetu* atrybutu XML, który jest wartością z przedziału od 0,0 (najniższy) do 1,0 (najwyższy).

Aplikacja Webex oficjalnie obsługuje następujące kodeki:

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

Poufne informacje Cisco

```
<config>
<usługi><połączenia>
  <audio>
    <kodeki>
      <nazwa kodeka="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=""/>
      <nazwa kodeka="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="phone-event" payload="101" in-band="false"/>
    …
  <wideo>
    <kodeki>
      <codec name="H264" payload="109" resolution="CIF" framerate="25"
bitrate="768000" priority="1.0">
        <tryb pakietowy>0</tryb pakietowy>
```

Klient obsługuje kodek wideo H.264. Za pomocą atrybutu Video resolution [Rozdzielczość wideo] można ustawić jedną z następujących dostępnych wartości: SUBQCIF, QCIF, CIF, 4CIF, VGA i HD.

Jeśli w konfiguracji nie zostanie wprowadzona szybkość transmisji bitów, zostaną użyte domyślne wartości szybkości transmisji bitów. W poniższej tabeli podano domyślne wartości szybkości transmisji bitów dla rozdzielczości i liczby klatek na sekundę.

Rozwiązanie	Rozmiar wideo *	FPS (klatki na sekundę)	Domyślne wartości szybkości transmisji bitów na rozdzielczość i liczbę klatek na sekundę
SUBQCIF	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 filmu. Rzeczywista rozdzielczość wideo podczas połączenia między dwoma Webex dla klientów Cisco BroadWorks zależy od możliwości obu klientów – będzie niższa z nich i będzie taka sama na obu klientach.

Rozdzielczość wideo dla połączenia wideo jest negocjowana podczas konfigurowania sesji i zależy od możliwości dwóch punktów końcowych. Rozdzielczość połączenia wideo jest taka sama na obu punktach końcowych. Oznacza to, że jeśli Webex dla punktów końcowych Cisco BroadWorks mają różne możliwości (i dlatego obsługują różne rozdzielczości), wówczas niższa rozdzielczość jest negocjowana dla połączenia. Rozdzielczość wideo może ulec zmianie podczas połączenia, jeśli warunki sieciowe ulegną pogorszeniu. W takim przypadku dwa mobilne punkty końcowe mogą używać różnych rozdzielczości wideo.

Poufne informacje Cisco

Tryb pakietyzacji można skonfigurować jako SingleNAL (0) lub Non-interleaved (1). Szablon domyślnie używa SingleNAL (<packet-mode>0</packet-mode>).

Obsługiwana jest również konfiguracja zdarzeń telefonicznych, pojedyncza lub wielokrotna. Podczas negocjacji kodeka klient wysyła wszystkie skonfigurowane kodeki, w tym zdarzenie telefoniczne. Po wybraniu kodeka audio wyszukuje zdarzenie telefoniczne w ofercie. Jeśli oferta zawiera zdarzenie telefoniczne z częstotliwością próbkowania negocjowanego kodeka audio, wybierane jest to zdarzenie telefoniczne. W przeciwnym razie zostanie użyte pierwsze zdarzenie telefoniczne na liście.

Jeśli wynegocjowano co najmniej jedno zdarzenie telefoniczne, dwutonowe wieloczęstotliwościowe (DTMF) są wysyłane jako pakiety RTP przy użyciu odpowiedniego typu ładunku. A jeśli w ogóle nie negocjowano żadnych zdarzeń telefonicznych, DTMF są wysyłane jako pakiety RTP z typem ładunku negocjowanego kodeka audio. Pozapasmowy mechanizm dostarczania DTMF nie jest obsługiwany przez aplikację Webex.

Przykładowe skonfigurowane kodeki:

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

Jeśli negocjowany jest kodek audio z częstotliwością próbkowania 48 kb/s, 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 - AI Codec (xCodec). Ten kodek audio jest używany w niekorzystnych warunkach sieciowych w celu uzyskania lepszej jakości połączeń. Webex Media Engine w aplikacji Webex sprawdza możliwości urządzenia, śledzi jakość multimediów, a kodek AI 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 AI Codec powinny być reklamowane i negocjowane przez obie strony podczas negocjacji SDP.

6.1.35 Wybieranie numerów SIP-URI

Obecnie wybieranie numerów SIP-URI za pośrednictwem BroadWorks jest niedostępne i domyślnie wszystkie połączenia SIP-URI są przekierowywane przez Locus, znany również jako "Free Calling". W niektórych środowiskach nie jest to pożądane i takie połączenia powinny być blokowane.

UWAGA: Ma to zastosowanie tylko wtedy, gdy połączenie Locus jest wyłączone. Tylko w takim przypadku SIP URI blokowanie wybierania będzie działać.

Ta opcja jest dostępna w poniższej konfiguracji.

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


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	true	prawda, fałsz	Określa, czy identyfikator SIP-URI ma być przekierowywany przez identyfikator Locus (prawda), czy blokowany (fałsz).

6.1.36 Historia połączeń na wszystkich urządzeniach

Klient zapewnia możliwość przechowywania i pobierania historii połączeń z serwera zamiast przechowywania jej lokalnie. W ten sposób historia połączeń jest ujednolicona na wszystkich urządzeniach.

UWAGA: Ujednolicona historia połączeń powinna być włączona w tym samym czasie po stronie klienta i serwera, aby uniknąć utraty historii połączeń lub zduplikowanych rekordów.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	prawda, fałsz	Określa, czy aplikacja ma używać ujednoliconej historii połączeń, czy po stronie klienta (lokalnej).

6.1.37 Wyłączanie połączeń wideo

W wersji 41.9 dodano możliwość wyłączenia połączeń wideo. Istnieją oddzielne opcje konfiguracji do sterowania tą funkcją dla połączeń VoIP wspieranych przez BroadWorks i Locus (bezpłatnych).

Gdy funkcja jest włączona, a znacznik funkcji ma wartość "false":

- Użytkownik nie będzie widział ustawienia "Akceptuj połączenia przychodzące z włączonym filmem wideo"
- Wszystkie przychodzące połączenia wideo, jeśli zostaną zaakceptowane, będą połączeniami audio
- Użytkownik nie będzie mógł eskalować połączenia do wideo, a eskalacje wideo zostaną automatycznie odrzucone

Gdy połączenia wideo są włączone, dodawana jest nowa właściwość konfiguracji, aby kontrolować domyślną wartość ustawienia "Akceptuj połączenia przychodzące z włączonym wideo". Domyślnie ta funkcja jest włączona dla komputerów i wyłączona dla telefonów komórkowych i tabletów.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SIP_VIDEOCALLS_WXT%	true	prawda, fałsz	Kontroluje dostępność połączeń wideo SIP za pośrednictwem BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	true	prawda, fałsz	Kontroluje dostępność (bezpłatnych) połączeń wideo Locus.
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Pulpit - prawda Telefon komórkowy / Tablet - fałsz	Prawda, fałsz	Określa domyślną wartość ustawienia "Akceptuj połączenia przychodzące z włączonym wideo".

6.1.38 Połączenia alarmowe (911) — raportowanie lokalizacji przez dostawcę E911

Klient Webex komputerów stacjonarnych i tabletów obsługuje raportowanie lokalizacji E911 przy użyciu RedSky, Intrado lub Bandwidth jako dostawca połączeń alarmowych E911 dla Webex wdrożenia BroadWorks. Dostawca E911 zapewnia obsługę lokalizacji poszczególnych urządzeń (dla Webex aplikacji stacjonarnych i tabletów oraz urządzeń MPP z obsługą HELD) oraz sieć, która kieruje połączenia alarmowe do punktów przyjmowania zgłoszeń o wypadkach (PSAP) w Stanach Zjednoczonych, ich terytoriach (Guam, Puerto Rico i Wyspy Dziewicze) i Kanadzie. Usługa jest włączana dla poszczególnych lokalizacji.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	false	Prawda, fałsz	Włącza platformę lokalizacji alarmowej dostawcy E911.
%BWE911-GŁÓWNY-HELDURL%	pusty	łańcuch	Określa adres URL platformy lokalizacji alarmowej dostawcy E911 obsługującej protokół HELD.
%BWE911-CUSTOMERID%	pusty	łańcuch	Identyfikator klienta (HeldOrgId, CompanyID) używany dla żądania HTTPS dostawcy E911.
%BWE911-SECRETKEY%	pusty	łańcuch	Klucz tajny uwierzytelniania żądania HTTPS dostawcy E911.
%BWE911-LISTA-NUMERÓW-ALARMOWYCH%	pusty	CSV ciąg	Lista numerów alarmowych obsługiwanych przez dostawcę E911.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (monit użytkownika nie zostanie ponownie wyświetlony)	Numer [0 - 43200]	Limit czasu w minutach, który będzie używany do przypomnienia użytkownikowi o aktualizacji lokalizacji alarmowej, jeśli bieżąca lokalizacja nie zostanie wprowadzona lub jest nieprawidłowa. Sugerowana wartość, jeśli zdecydujesz się włączyć: 1440 (jeden dzień).
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (użytkownik może zawsze anulować okno dialogowe)	Numer [-1 - 100]	Czas, w którym 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 może anulować okna dialogowego - zawsze obowiązkowa lokalizacja) ▪ N > 0 (użytkownik może anulować okno dialogowe N razy, zanim stanie się obowiązkowe)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	agresywny, once_per_login	once_per_login	Definiuje zachowanie monitowania o lokalizację E911. Wartość "agresywna" pokaże użytkownikowi okno dialogowe przy każdej zmianie sieciowej w nieznanej lokalizacji, podczas gdy wartość "once_per_login" pokaże okno dialogowe tylko raz, zapobiegając dalszemu wyskakującemu okienku i rozpraszaniu uwagi użytkownika.

UWAGA 1: Znaczniki BWE911-*** to "Dynamiczne wbudowane znaczniki systemowe". Aby uzyskać więcej informacji, zobacz sekcję *5.7 Dynamiczne wbudowane znaczniki systemowe Cisco BroadWorks*.

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

Poufne informacje Cisco

6.1.39 PAI jako tożsamość

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

Jeśli atrybut enabled tagu <use-pai-as-calling-identity> ma wartość "true", nagłówek PAI jest używany z priorytetem przed nagłówkiem Od. Ta tożsamość strony wywołującej służy do rozpoznawania kontaktu i prezentowania go użytkownikowi.

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

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	prawda, fałsz	Określa, czy tożsamość wywołująca prezentowana użytkownikowi ma być pobierana z nagłówków SIP From czy SIP P-Asserted-Identity. Ustaw wartość "true", aby używać nagłówka PAI z priorytetem.

6.1.40 Wyłącz współdzielenie ekranu

Wersja 42.5 dodaje możliwość kontrolowania dostępności współdzielenia ekranu. Gdy współdzielenie ekranu jest wyłączone:

- Użytkownik nie będzie widział możliwości zainicjowania współdzielenia ekranu w przypadku połączeń 1-1
- Przychodzące żądania współdzielenia ekranu są odrzucane, a użytkownik widzi komunikat informacyjny

Domyślnie ta funkcja jest włączona.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SCREEN_SHARE_WXT%	true	prawda, fałsz	Określa, czy użytkownik powinien włączyć udostępnianie ekranu.

Poufne informacje Cisco

6.1.41 Wskazanie połączenia spamowego

Gdy przełącznik funkcji (według typu wdrożenia) jest włączony, a funkcja jest włączona w pliku konfiguracyjnym, aplikacja Webex przetwarza nowy parametr wskazujący stan weryfikacji połączenia spamowego, jeśli są one odbierane w ramach powiadomień push o nowym połączeniu lub rekordów historii połączeń.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	prawda, fałsz	Kontroluje dostępność wskazań spamu na ekranie połączeń przychodzących i historii połączeń tylko dla Webex Calling.

6.1.42 Usuwanie szumów i zwiększanie przepustowości dla połączeń PSTN/komórkowych

Usuwanie szumów zapewnia lepszą obsługę połączeń użytkownikom dzwoniącym, gdy rozmawiają z użytkownikami spoza Webex w sieci PSTN lub urządzeniach mobilnych. W wersji 43.12 usuwanie szumów jest domyślnie włączone.

W wersji 44.2 aplikacji Webex wprowadzono nowe ulepszenia przychodzących multimediów audio Speech AI dla wąskopasmowych połączeń PSTN.

- Dodano nowy algorytm rozszerzenia pasma w celu poprawy jakości dźwięku poprzez rozszerzenie pasma wąskopasmowego widma PSTN i usunięcie szumów. Zwiększona przepustowość zwiększy zrozumiałość i zmniejszy zmęczenie słuchaniem.
- Istniejący już algorytm usuwania szumów został ulepszony, usuwając ograniczenia dla muzyki przy zawieszeniu i innych dźwięków audio (np. sygnałów dźwiękowych).
- Gdy ta funkcja jest włączona, użytkownicy widzą wskaźnik "Inteligentny dźwięk – zewnętrzny" i mogą kontrolować ulepszenia Speech AI dla przychodzących multimediów audio.

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

```
<config>
   <usługi>
      <połączenia>
         <Ulepszenia mowy włączone="%ENABLE_SPEECH_ENHANCEMENTS_WXT%"/>
```


Poufne informacje Cisco

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

UWAGA: Usuwanie szumów jest teraz częścią dodatkowych ulepszeń mowy, a znacznik <usuwanie szumów> został wycofany przez nowy znacznik <ulepszenia mowy>. Niestandardowy tag %ENABLE_NOISE_REMOVAL_WXT% usuwania szumów również jest przestarzały.

6.1.43 Oznaczenie DSCP QoS

Oznaczenie DSCP QoS jest obsługiwane przez aplikację Webex wywołującą media RTP pakiety (Audio i Video). DSCP określa klasyfikację ruchu dla danych sieciowych. Można to wykorzystać do określenia, który ruch sieciowy wymaga większej przepustowości, ma wyższy priorytet i jest bardziej prawdopodobne, że porzuci pakiety.

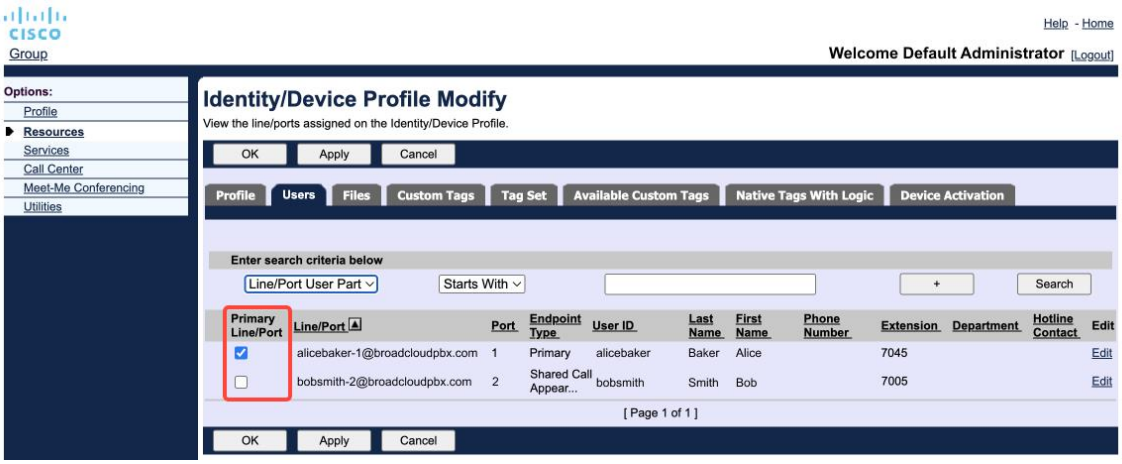
UWAGA: Najnowsze wersje systemu operacyjnego Microsoft Windows nie zezwalają aplikacjom na bezpośrednie konfigurowanie DSCP lub UP dla pakietów wychodzących, zamiast tego wymagają wdrożenia obiektów zasad grupy (GPO) w celu zdefiniowania DSCP oznaczania zasad na podstawie UDP zakresów portów.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_AUDIO_QOS_WXT%	true	Prawda, fałsz	Włącza funkcję 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 nie można pomyślnie przeanalizować wartości.
%ENABLE_VIDEO_QOS_WXT%	true	Prawda, fałsz	Włącza funkcję 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 nie można pomyślnie przeanalizować wartości.

Poufne informacje Cisco

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 współdzielona z innym użytkownikiem, może istnieć wiele profili tego samego typu skonfigurowanych dla użytkownika. Aby wybrać właściwy profil do logowania się w usługach telefonicznych, usługa Cisco BroadWorks została ulepszona w celu wskazania, czy użytkownik jest właścicielem urządzenia, tzn. przypisano mu linię podstawową/port dla urządzenia — aby uzyskać więcej informacji na temat aktualizacji Cisco BroadWorks, zaznacz pole wyboru Flaga właściciela na liście urządzeń, aby obsługiwać linie wspólne klienta Webex.



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

Począwszy od wersji 43.2, dodano nową opcję konfiguracji (*ograniczenie* właściciela urządzenia), aby kontrolować, czy należy zastosować ograniczenie profilu podstawowego. Można go użyć, aby umożliwić aplikacji Webex używanie profilu linii/portu innego niż podstawowy do logowania się do usług telefonicznych. Ta opcja konfiguracji jest stosowana dla wszystkich konfiguracji, niezależnie od liczby profili skonfigurowanych dla użytkownika (**jeśli ograniczenie własności urządzenia jest włączone i nie ma urządzenia z linią podstawową/portem dla odpowiedniej platformy, usługi telefoniczne nie będą się łączyć**).

To samo ograniczenie dotyczy urządzeń, które użytkownik może sparować w aplikacji Desktop Webex. Użytkownik może wyświetlać i parować tylko z urządzeniami, które posiada. Zapobiega to parowaniu z urządzeniami innego użytkownika, który ma przypisaną linię współdzieloną lub wirtualną. Wartość tego samego parametru konfiguracyjnego dotyczy również tego ograniczenia.

```
<config>
<usługi><połączenia>
<device-owner-restriction enabled="%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	true	prawda, fałsz	Kontroluje ograniczenie właściciela urządzenia — jeśli usługi telefoniczne mają korzystać z profilu głównego danego urządzenia

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

6.1.45 Lista zablokowanych (tylko Webex Calling)

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

Użytkownik może skonfigurować listę zablokowanych z dwóch miejsc - Preferencje połączeń i Historia połączeń. W Preferencjach użytkownik może zobaczyć listę blokowanych numerów i edytować ją. W historii połączeń użytkownik może zobaczyć rekordy historii połączeń dla połączeń zablokowanych przez zdefiniowaną przez użytkownika listę zablokowanych. Te rekordy mają wskazanie Zablokowane, jeśli numer znajduje się na liście zablokowanych zdefiniowanej przez użytkownika, a użytkownik będzie miał możliwość odblokowania numeru bezpośrednio dla danego rekordu. Dostępna jest również opcja bloku.

Reguły dotyczące numerów dodawanych do listy zablokowanych zdefiniowanej przez użytkownika:

- Format liczb
  - Blokowanie połączeń w preferencjach połączeń powoduje zastosowanie ograniczenia formatu E.164 lokalnie w aplikacji Webex
  - Blokowanie dostępu do historii połączeń jest dozwolone dla wszystkich rekordów Webex Calling
  - Firma Cisco BroadWorks może dopuszczać lub odrzucać żądania dotyczące nowych numerów dodanych do listy zablokowanych na podstawie formatu liczbowego
- Numery wewnętrzne - połączenia przychodzące z numerów wewnętrznych będą dostarczane do użytkownika, nawet jeśli znajdują się one na zdefiniowanej przez użytkownika liście zablokowanych

Poufne informacje Cisco

Lista zablokowanych zdefiniowana przez użytkownika jest konfigurowana w serwisie Cisco BroadWorks i stosowana do wszystkich urządzeń WxC dla użytkownika. Ta funkcja współpracuje z listą zablokowanych zdefiniowaną przez administratora, która nie jest konfigurowalna przez użytkownika i może być kontrolowana tylko przez administratorów za pośrednictwem Centrum sterowania. NIE ma rekordów historii połączeń dla połączeń przychodzących zablokowanych przez listę zablokowanych zdefiniowaną przez administratora.

Lista zablokowanych zdefiniowana przez użytkownika jest stosowana po STIR/SHAKEN, liście zablokowanych zdefiniowanej przez administratora i anonimowych zasadach odrzucania połączeń.

```
<config>
<usługi><połączenia>
<call-block enabled="%ENABLE_CALL_BLOCK_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_BLOCK_WXT%	true	prawda, fałsz	Włącza listę zablokowanych zdefiniowaną przez użytkownika Ustaw wartość "true", aby zobaczyć listę zablokowanych w preferencjach połączeń i historii połączeń

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

6.1.46 Adaptacja do mediów i wdrażanie odporności (MARI)

6.1.46.1 Dostosowanie stawek

Aplikacja Webex ma już zintegrowane techniki adaptacyjnej jakości mediów, aby zapewnić, że utrata pakietów wideo nie wpłynie na dźwięk i zapewnić, że wideo może wykorzystać adaptację szybkości wideo do zarządzania przepustowością wykorzystywaną w czasach przeciążenia.

Dostosowanie szybkości lub dynamiczne dostosowanie szybkości transmisji bitów dostosowuje szybkość wywołania do dostępnej zmiennej przepustowości, zmniejszając lub zwiększając szybkość transmisji bitów wideo w zależności od warunków utraty pakietów. Punkt końcowy zmniejszy szybkość transmisji bitów, gdy otrzyma komunikaty z odbiornika wskazujące na utratę pakietów; A gdy utrata pakietów zmniejszy się, nastąpi przyspieszenie szybkości transmisji bitów.

Nie ma konfigurowalnych ustawień kontrolujących wykorzystanie mechanizmu dostosowania stawek.

6.1.46.2 Forward Error Correction (FEC) i Packets Retransmission (RTX)

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

Poufne informacje Cisco

FEC zapewnia nadmiarowość przesyłanych informacji za pomocą wcześniej określonego algorytmu. Redundancja pozwala odbiorcy wykryć i skorygować ograniczoną liczbę błędów, bez konieczności proszenia nadawcy o dodatkowe dane. FEC daje odbiornikowi możliwość korygowania błędów bez konieczności korzystania z kanału zwrotnego (takiego jak RTCP) w celu żądania retransmisji danych, ale ta zaleta odbywa się kosztem stałej, wyższej szerokości kanału forward (więcej wysłanych pakietów).

Punkty końcowe nie używają FEC w przepustowości niższej niż 768 kb/s. Ponadto przed wprowadzeniem FEC musi nastąpić co najmniej 1,5% utraty pakietów. Punkty końcowe zazwyczaj monitorują skuteczność FEC, a jeśli FEC nie jest wydajny, nie jest używany.

FEC zużywa więcej pasma niż retransmisja, ale ma mniejsze opóźnienie. RTX jest używany, gdy dozwolone jest małe opóźnienie i istnieją ograniczenia przepustowości. W przypadku dużego opóźnienia i wystarczającej przepustowości preferowane jest FEC.

Aplikacja Webex dynamicznie wybiera RTX lub FEC w zależności od wynegocjowanego pasma i tolerancji opóźnienia dla danego strumienia mediów. FEC powoduje większe wykorzystanie przepustowości ze względu na nadmiarowe 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 wskaże utratę pakietów w kanale sprzężenia zwrotnego RTCP. RTX wprowadza opóźnienie odzyskiwania pakietów ze względu na czas potrzebny pakietowi RTCP dotarcie do odbiorcy od nadawcy i dotarcie retransmitowanego pakietu do odbiorcy od nadawcy.

FEC musi być włączony, aby włączyć RTX.

```
<config><services><calls>
<audio>
       <Ulepszenia jakości dźwięku>
              <mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <ładowność>111</ładunek>
                            <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>
                            <zamówienie>FEC_SRTP</porządek>
                     </fec>
                     <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
                            <ładowność>112</ładunek>
                            <czas>180</czas>
                            <przepływ danych>1</przepływ danych>
                            <zamówienie>RTX_SRTP</zamówienie>
                     </rtx>
              </mari>
...
<wideo>
       <Ulepszenia jakości wideo>
              <mari>
                     <fec enabled="%ENABLE_VIDEO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <ładowność>111</ładunek>
                            <max_esel>1400</max_esel>
```


Poufne informacje Cisco

```
                        <max_n>255</max_n>
                        <m>8</m>
                        <multi_ssrc>1</multi_ssrc>
                        <non_seq>1</non_seq>
                        <feedback>0</feedback>
                        <zamówienie>FEC_SRTP</porządek>
                </fec>
                <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                        <mari-rtx>90000</mari-rtx>
                        <ładowność>112</ładunek>
                        <czas>180</czas>
                        <przepływ danych>1</przepływ danych>
                        <zamówienie>RTX_SRTP</zamówienie>
                </rtx>
        </mari>
```

Znacznik	Domyśln e, jeśli zostało pominięt e	Obsługiwa ne wartości	Opis
%ENABLE_AUDIO_MARI_FEC_WXT%	false	prawda, fałsz	Włącza FEC dla połączeń audio
%ENABLE_AUDIO_MARI_RTX_WXT%	false	prawda, fałsz	Włącza RTX dla połączeń audio (wymaga włączonego FEC audio)
%ENABLE_VIDEO_MARI_FEC_WXT%	false	prawda, fałsz	Włącza FEC dla połączeń wideo
%ENABLE_VIDEO_MARI_RTX_WXT%	false	prawda, fałsz	Włącza RTX dla połączeń wideo (wymaga włączonego wideo FEC)

6.1.47 Jednoczesne połączenia z tym samym użytkownikiem

Dodanie obsługi jednoczesnych połączeń z tym samym użytkownikiem na jednym urządzeniu.

Ta funkcja jest przydatna w przypadku niektórych wdrożeń, w których tożsamość prezentowana połączenia nie jest taka sama jak tożsamość połączenia. Prowadzi to do braku możliwości zainicjowania nadzorowanego transferu z powrotem do pierwotnej strony. Włączając tę funkcję, użytkownik będzie mógł obsługiwać wiele jednoczesnych połączeń z tą samą stroną zdalną.

```
<config>
   <usługi>
      <połączenia>
         <jednoczesne-połączenia-z-tym samym-użytkownikiem
enabled="%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false	prawda, fałsz	Określa, czy aplikacja Webex może obsługiwać tylko jedno lub wiele połączeń WxC z tym samym użytkownikiem.

6.1.48 RTCP-XR

Począwszy od wersji 43.8, aplikacja Webex dodaje negocjację wymiany pakietów RTCP-XR podczas połączenia. Negocjacje odbywają się podczas ustanawiania sesji SIP INVITE Jeśli oba punkty końcowe obsługują pakiety RTCP-XR, Webex Media Engine rozpocznie wymianę tych pakietów i wspomoże mechanizm adaptacyjnej jakości połączeń. Ta funkcja jest domyślnie włączona.

Ponadto tylko w przypadku Webex Calling te dodatkowe metryki będą wysyłane przez SIP BYE i w ten sposób udostępniane w centrum sterowania.

```
<config>
<protokoły><sip>
   <rtcp-xr>
      <negocjacja włączona="%ENABLE_RTCP_XR_NEGOTIATION_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	true	prawda, fałsz	Umożliwia negocjację RTCP-XR i wymianę pakietów w celu uzyskania lepszej jakości połączeń. Domyślnie włączone.

6.1.49 Informacje o przekierowywaniu połączeń

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

```
<config>
<usługi><połączenia>
<call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	true	prawda, fałsz	Kontroluje widoczność informacji o przekierowaniu i przekierowaniu. Ustaw wartość "true", aby zobaczyć informacje na ekranach związanych z połączeniami i w historii połączeń.

6.1.50 ID abonenta dzwoniącego

6.1.50.1 Identyfikator rozmówcy wychodzącego

Aplikacje Webex Mobile (wersja 44.2) i Desktop (wersja 44.3) wprowadzają nową możliwość wyboru przez użytkownika preferowanego identyfikatora zewnętrznego rozmówcy dla połączeń wychodzących. Lista dostępnych opcji obejmuje:

- Linia bezpośrednia (domyślna)
- Numer lokalizacji
- Numer niestandardowy z tej samej organizacji
- Kolejki połączeń, do których należy użytkownik, co umożliwia agentom korzystanie z jego numeru identyfikacyjnego osoby dzwoniącej
- Grupy wyszukiwania, do których należy użytkownik, co umożliwia agentom korzystanie z ich numeru identyfikacyjnego osoby dzwoniącej
- Ukryj identyfikator rozmówcy

Notatki:

- Lista opcji zależy od linii:
  - Linia podstawowa – pełny zestaw opcji
  - Linie wspólne – niedostępne
  - Linie wirtualne — tylko opcje kolejki połączeń
- Jeśli wybrana już tożsamość nie jest już dostępna, używany jest domyślny identyfikator dzwoniącego użytkownika
- Połączenia alarmowe zawsze korzystają z numeru alarmowego użytkownika
- Usuwa tag <połączenia wychodzące> w sekcji <services><agent-call-center>

Listę dostępnych opcji można konfigurować w portalu administracyjnym. Istnieją również oddzielne niestandardowe tagi DMS, aby kontrolować dostępność tych ulepszeń w aplikacji Webex.

```
<config>
<usługi><połączenia>
   <identyfikator dzwoniącego>
      <Połączenia wychodzące włączone="%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%"/>
```


Poufne informacje Cisco

```
        <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </połączenia wychodzące>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	prawda, fałsz	Umożliwia wybór numeru identyfikatora 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 biura obsługi (DNIS) skonfigurowanych dla użytkownika.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	prawda, fałsz	Kontroluje dostępność numerów grup wyszukiwania skonfigurowanych dla użytkownika.
"%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	prawda, fałsz	Włącza blokowanie dostarczania identyfikatora dzwoniącego jako wybór dla połączeń wychodzących.

UWAGA: Aplikacja komputerowa w wersji 44.3 obsługuje tylko identyfikator CLID Call Center, a 44.4 dodaje obsługę pozostałych opcji.

6.1.50.2 Nazwa identyfikatora zdalnego rozmówcy

Po odebraniu/zainicjowaniu połączenia firma Cisco BroadWorks wysyła nazwę wyświetlaną strony zdalnej w zaproszeniu SIP. Jest on domyślnie używany przez aplikację Webex. Jednocześnie aplikacja Webex rozpoczyna rozpoznawanie kontaktów z kilku źródeł, z następującym priorytetem:

- Wspólna tożsamość (CI)
- Usługa kontaktów (kontakty niestandardowe)
- Kontakty programu Outlook (wersja klasyczna)
- Lokalna książka adresowa (wersja mobilna)

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

Poufne informacje Cisco

W wersji 44.5 aplikacji Webex dodano konfigurowalną opcję ignorowania rozpoznawania kontaktów i zawsze zachowywania nazwy wyświetlanej Cisco BroadWorks dla połączeń z obszarami roboczymi lub urządzeniami RoomOS używanymi do połączeń Cisco BroadWorks 1:1.

```
<config>
<usługi><połączenia>
   <identyfikator dzwoniącego>
      <nazwa-zdalna>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	Rozwiązane	rozwiązane, SIP	Kontroluje nazwę wyświetlaną strony zdalnej dla obszarów roboczych i urządzeń RoomOS. Użyj ciągu "sip", aby zignorować rozpoznawanie kontaktu i użyj nazwy wyświetlanej otrzymanej w sesji SIP REVIT.

Poufne informacje Cisco

6.1.51 Obsługa wielu linii

Użytkownik Webex może mieć linię podstawową i maksymalnie 9 linii pomocniczych. Linie pomocnicze mogą być współdzielone lub wirtualne (tylko połączenia Webex).

Webex aplikacja pobiera konfigurację linii za pośrednictwem pliku konfiguracyjnego DMS, który jest pobierany przy logowaniu i co 12 godzin. W przypadku wykrycia aktualizacji konfiguracji linii, użytkownik jest proszony o ponowne uruchomienie aplikacji w celu zastosowania zmian. Ponowne zalogowanie użytkownika natychmiast wykryje i zastosuje wszelkie aktualizacje konfiguracji linii.

Poniżej przedstawiono sekcję szablonu konfiguracyjnego DMS związaną z obsługą wielu linii zarówno dla komputerów stacjonarnych, jak i urządzeń mobilnych.

```
<config>
<protokoły>
   <łyk>
       <lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
          <osobiste>
             <port-linii>%BWDISPLAYNAMELINEPORT%</port-linii>
          </osobiste>
          <line lineType="%BW-MEMBERTYPE-1%">
             <identyfikator-zewnętrzny>%BWUSEREXTID-1%</identyfikator-zewnętrzny>
             ...
          </linia>
          <line lineType="%BW-MEMBERTYPE-2%">
             <external-id>%BWUSEREXTID-2%</external-id>
             ...
          </linia>
          ...
          <line lineType="%BW-MEMBERTYPE-10%">
             <identyfikator-zewnętrzny>%BWUSEREXTID-10%</identyfikator-zewnętrzny>
             ...
          </linia>
```

Aby kontrolować funkcję wielowierszową, użyj dedykowanego tagu niestandardowego.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_MULTI_LINE_WXT%	false	Prawda, fałsz	Umożliwia obsługę wielu linii (jeśli jest skonfigurowana). Jeśli opcja jest wyłączona (ustawiona na wartość "false"), aplikacja będzie używać tylko pierwszego skonfigurowanego wiersza.

UWAGA 1: Obsługa funkcji Boss-Admin (Executive-Assistant) nie jest dostępna w połączeniu z konfiguracją wieloliniową.

UWAGA 2: Dodatkowe wymagania dotyczące rozwiązań BroadWorks można znaleźć w części "Wygląd linii wspólnej" w przewodniku Webex-for-Cisco-BroadWorks-Solution-Guide.

Poufne informacje Cisco

6.1.51.1 Pulpit — wygląd linii wspólnej

Począwszy od wersji 42.12, Webex aplikacja dodaje obsługę linii wspólnych. Administrator powinien skonfigurować wspólne wystąpienia połączeń dla każdej linii wspólnej.

W wersji 43.12 aplikacja Webex została rozszerzona o możliwość przenoszenia (lokalnego wznawiania) zawieszonego połączenia na linii udostępnionej lub wirtualnej, obsługiwanego przez innego użytkownika lub przez tego samego użytkownika na innym urządzeniu. Aby uzyskać więcej informacji, sprawdź *6.2.13 Przenoszenie połączenia*.

6.1.51.2 Desktop — Virtual Lines (tylko Webex Calling)

Tylko w przypadku Webex Calling wdrożenia aplikacja Webex obsługuje konfigurację wielu linii przy użyciu linii wirtualnych. Funkcjonalnie konfiguracja z liniami wirtualnymi odpowiada wielolinii wykorzystującej linie wspólne – mając możliwość zobaczenia linii wirtualnych skonfigurowanych dla użytkownika i wykorzystania ich do połączeń przychodzących i wychodzących.

Wersja 43.4 rozszerza obsługę linii wirtualnych, dodając grupowe parkowanie połączeń i pobieranie parkowania połączeń.

W wersji 43.12 aplikacja Webex została rozszerzona o możliwość przenoszenia (lokalnego wznawiania) zawieszonego połączenia na linii udostępnionej lub wirtualnej, obsługiwanego przez innego użytkownika lub przez tego samego użytkownika na innym urządzeniu. Aby uzyskać więcej informacji, sprawdź *6.2.13 Przenoszenie połączenia*.

6.1.51.3 Telefon komórkowy (tylko Webex Calling)

Tylko w przypadku wdrożenia Webex Calling wersja 45.4 dodaje obsługę wielu linii (udostępnionej i wirtualnej) w wersji mobilnej aplikacji Webex. Przypisanie linii ma zastosowanie zarówno do aplikacji Webex na komputerach, jak i na urządzenia przenośne.

Ze względu na specyfikę platformy mobilnej, użytkownik może mieć do dwóch jednoczesnych połączeń jednocześnie na dowolnej linii.

> **UWAGA 1**: Jeśli włączona jest opcja Nawiązywanie połączeń za pomocą natywnego programu wybierającego (patrz *6.3.5.1 Nawiązywanie połączeń przy użyciu* natywnego programu wybierającego), funkcja obsługi wielu linii jest wyłączona.
>
> **UWAGA 2**: Tryb Multi-line dla wersji Tablet nie jest obsługiwany.

6.1.52 Rozszerzona autoryzacja SIP

Wersja 45.4 aplikacji Webex zapewnia konfigurowalną opcję optymalizacji komunikacji SIP poprzez współdzielenie autoryzacji między wszystkimi sesjami SIP. Aplikacja będzie przechowywać autoryzację i używać jej ponownie, dopóki nie będzie ważna.

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

Poufne informacje Cisco

```
<config>
<protokoły>
  <łyk>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	prawda, fałsz	Po ustawieniu wartości "true" włączone jest rozszerzenie autoryzacji SIP.

UWAGA 1: Niektóre kontrolery SBC mogą wymagać nowej autoryzacji SIP w każdej sesji, dlatego ta funkcja powinna być używana zgodnie ze specyfiką wdrożenia.

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

6.1.53 Osobisty asystent (obecność poza domem)

W wersji 44.11 aplikacja Mobile Webex i aplikacja Desktop Webex w wersji 45.3 zapewnia integrację z usługą Cisco BroadWorks Personal Assistant (PA). Działa w połączeniu z obecnością użytkownika poza domem i wymaga synchronizacji stanu PA z obecnością Webex Cloud.

Usługa PA udostępnia użytkownikowi opcję poinformowania dzwoniących o przyczynie niedostępności strony wywoływanej, opcjonalnie podając informacje o tym, kiedy strona wywoływana powróci i czy jest opiekun do obsługi połączenia.

Jeśli PA jest włączona, opcja Obecność poza domem będzie dostępna dla użytkownika. Można go użyć do skonfigurowania PA po stronie Cisco BroadWorks. Gdy funkcja jest aktywna, użytkownicy będą widzieć obecność użytkownika z dala w połączeniu ze statusem PA i skonfigurowanym czasem trwania.

Użytkownik może skonfigurować tylko ręczną konfigurację PA. Jeśli istnieją harmonogramy mające wpływ na usługę PA, obecność zostanie zaktualizowana za pomocą synchronizacji stanu asystenta osobistego. Jednak aplikacja Webex nie udostępnia konfiguracji harmonogramów i harmonogramów, które mają wpływ na PA.

```
<config>
<usługi>
  <Asystent-osobisty włączony="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	prawda, fałsz	Określa, czy funkcja Obecność poza domem jest dostępna dla użytkownika.

UWAGA 1: Ta funkcja wymaga włączenia synchronizacji stanu asystenta osobistego z poziomu Centrum partnerów.

UWAGA 2: Standardowe przekierowywanie połączeń asystenta osobistego nie będzie obowiązywać, gdy aktywne są usługi DND, Call Forwarding Always lub Call Forwarding Select.

UWAGA 3: Ręczne stany Nie przeszkadzać i Zajęty mają wyższy priorytet niż stany Z dala od komputera. Gdy użytkownik ręcznie aktywuje jeden z tych statusów obecności, włączenie Asystenta osobistego nie powoduje zmiany statusu obecności na Z dala od komputera.

Poufne informacje Cisco

6.2 Funkcje tylko dla komputerów stacjonarnych

6.2.1 Wymuszone wylogowanie

Ta funkcja umożliwia firmie Cisco BroadWorks śledzenie instancji klientów online z tym samym typem urządzenia i zezwalanie tylko jednemu z nich na połączenie z Internetem w danym momencie. Gdy firma Cisco BroadWorks powiadamia klienta o konieczności wylogowania, połączenie SIP zostaje zakończone, a klient wskazuje, że połączenie nie zostało połączone.

Ta funkcja jest potrzebna w niektórych wdrożeniach, w których podobni klienci mogą być w trybie online w tym samym czasie, co powoduje skutki uboczne. Jednym z przykładów jest użytkownik komputera stacjonarnego w pracy i w domu, gdzie połączenia przychodzące byłyby odbierane tylko przez jednego z klientów, w zależności od tego, która rejestracja SIP jest aktywna.

Wymuszone wylogowanie jest oparte na SIP, klient wysyła SIP SUBSCRIBE do *pakietu zdarzeń call-info* ze specjalną *wartością* appid w nagłówku *Od* , niezależnie od wartości parametru *bsoft-call-info* . Gdy firma Cisco BroadWorks wykryje wiele instancji klienta online przy użyciu tego samego *identyfikatora* aplikacji, wysyła specjalny komunikat SIP NOTIFY do starszej instancji klienta, powodując jej wylogowanie. Na przykład klienty stacjonarne będą miały identyczną *wartość* identyfikatora aplikacji, chociaż nie ma ograniczeń co do użycia tego identyfikatora po stronie klienta. Wartość *identyfikatora* aplikacji jest konfigurowana przez dostawcę usług.

Należy pamiętać, że aby można było korzystać z wymuszonego wylogowania, musi być włączona subskrypcja SIP *Call-Info* .

Informacje na temat poprawek i wydań Cisco BroadWorks wymaganych dla tej funkcji można znaleźć w sekcji poświęconej wymaganiom programowym Cisco BroadWorks w *podręczniku* Webex dotyczącym rozwiązania Cisco BroadWorks.

Szczegóły konfiguracji można znaleźć w poniższym przykładzie (SIP jest jedynym obsługiwanym protokołem sterującym w tej wersji).

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

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_FORCED_LOGOUT_WXT%	false	prawda, fałsz	Włącza wymuszone wylogowanie.
%FORCED_LOGOUT_APPID_WXT%	pusty	łańcuch	Appid używany po stronie serwera do korelacji. Może to być dowolny ciąg. Przykład: "123abc"

Poufne informacje Cisco

6.2.2 Przejmowanie połączeń

Przejmowanie połączeń to usługa dla wielu użytkowników, która umożliwia wybranym użytkownikom odbieranie dowolnej linii dzwonka w ramach grupy przejmowania połączeń. Grupa przejmowania połączeń jest definiowana przez administratora i jest podzbiorem użytkowników w grupie, którzy mogą odbierać nawzajem połączenia.

Obsługiwane są następujące przypadki odbioru:

- Przejmowanie połączeń w ciemno
- Kierowane przejmowanie połączeń (które umożliwia użytkownikowi odebranie połączenia skierowanego do innego telefonu w jego grupie poprzez wybranie odpowiedniego kodu dostępu do funkcji, a następnie numeru wewnętrznego dzwoniącego telefonu).

```
<config>
<usługi><połączenia>
<call-pickup blind="%ENABLE_CALL_PICKUP_BLIND_WXT%"
directed="%ENABLE_CALL_PICKUP_DIRECTED_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć przejmowanie połączeń w ciemno.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć funkcję Kierowane przejmowanie połączeń.

6.2.3 Wsparcie Boss-Admin (Executive-Assistant)

Funkcja Boss-Admin, znana w Cisco BroadWorks jako Executive-Assistant, umożliwia asystentowi działanie w imieniu kierownika w celu monitorowania, odbierania i wykonywania połączeń jako "kierownik". Jeden asystent może mieć wielu menedżerów i możliwe:

- Wybierz żądaną rolę podczas wykonywania połączenia.
- Odbierz połączenie przychodzące w imieniu kierownika, a następnie przekaż je do kierownictwa. Ponadto dostępne są wszystkie zwykłe opcje zarządzania połączeniami.
- Sprawdź, czy połączenie przychodzące jest w rzeczywistości przeznaczone dla kierownika.

Executive i Executive-Assistant to dwie powiązane ze sobą usługi Cisco BroadWorks, które łącznie zapewniają następujące funkcje:

- Użytkownik z usługą Kierownictwo może zdefiniować pulę asystentów, którzy zarządzają połączeniami. Asystenci muszą być wybrani spośród użytkowników w tej samej grupie lub przedsiębiorstwie, którzy mają przypisaną usługę Asystent wykonawczy.
- Użytkownik korzystający z usługi Asystent wykonawczy może odbierać i inicjować połączenia w imieniu swojego kierownictwa.

Poufne informacje Cisco

- Zarówno dyrektor wykonawczy, jak i jego asystenci mogą określić, które połączenia powinny być przekazywane asystentom, w jaki sposób asystenci powinni być powiadamiani o połączeniach przychodzących oraz które z połączeń przekazanych asystentom powinny być przedstawiane dyrektorowi do kontroli.

```
<config>
<usługi>
<Asystent-wykonawczy włączony="%ENABLE_EXECUTIVE_ASSISTANT_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć funkcję Boss-Admin.

UWAGA: Obsługa funkcji Boss-Admin (Executive-Assistant) nie jest dostępna w połączeniu z Shareed-Lines.

6.2.4 Eskaluj połączenia SIP do Meeting (tylko Webex Calling)

Klient udostępnia funkcję eskalacji trwającego połączenia SIP do spotkania za pośrednictwem Webex Calling. Korzystając z tej funkcjonalności zamiast standardowej konferencji ad-hoc, użytkownik będzie mógł korzystać z wideo, a także udostępniania ekranu podczas spotkania.

```
<config>
<usługi><połączenia>
       <escalate-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć opcję menu Eskaluj do Webex spotkania.

6.2.5 Sterowanie telefonem biurkowym — automatyczne odbieranie

Automatyczne odbieranie umożliwia użytkownikowi korzystanie z funkcji Desk Phone Control (DPC) dla połączeń wychodzących na kliencie w celu zarządzania telefonami MPP z zerową odpowiedzią dotykową.

Wybrany telefon MPP będzie przesyłał sygnał audio/wideo dla wychodzącego połączenia DPC.

Automatyczne odbieranie może działać na urządzeniach obsługiwanych jako podstawowe i inne niż główne. Jeśli użytkownik ma więcej niż jeden zarejestrowany telefon biurkowy, z którym można sparować, automatycznie odbiera tylko wybrane/sparowane urządzenie.

Poufne informacje Cisco

```
<config>
<usługi><połączenia>
<Deskphone-control auto-answer="%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	true	prawda, fałsz	Po ustawieniu wartości "true" włącza automatyczne odbieranie sterowania telefonem biurkowym.

UWAGA: Automatyczne odbieranie nie wpływa na połączenia przychodzące w trybie DPC, więc telefon stacjonarny dzwoni dla połączeń przychodzących.

6.2.6 Automatyczne odbieranie z powiadomieniem tonowym

Ta funkcja umożliwia obsługę automatycznego odbierania połączeń przychodzących dla urządzeń lokalnych, jeśli jest to wskazane w żądaniu połączenia przychodzącego.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_AUTO_ANSWER_WXT%	false	prawda, fałsz	Po ustawieniu na "true" włącza automatyczne odbieranie połączeń przychodzących, jeśli jest to wymagane z zaplecza.

6.2.7 Sterowanie telefonem biurkowym — elementy sterujące w trakcie połączenia — konferencja

Ta funkcja włącza opcje konferencji i scalania dla połączeń zdalnych (XSI), zakończonych w innej lokalizacji.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	prawda, fałsz	Po ustawieniu wartości "true" włącza opcje konferencji i scalania dla połączeń zdalnych (XSI) zakończonych w innej lokalizacji.

Poufne informacje Cisco

6.2.8 Powiadomienia o przejmowaniu połączeń

Powiadomienia o przejmowaniu połączeń umożliwiają użytkownikowi poznanie nadejścia połączenia przychodzącego do użytkownika, którego ma monitorować. Powiadomienia o przejmowaniu połączeń można odbierać dla list obserwowanych skonfigurowanych za pośrednictwem grupy Przejmowanie połączeń i usług polowych sygnalizacji zajętości lampki.

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

6.2.8.1 Pole sygnalizacji aktywności linii

Aplikacja Webex pulpitu wyświetla powiadomienie, jeśli członek na liście obserwowanych BLF (Busy Lamp Field) ma połączenie przychodzące w stanie alertu. Powiadomienie zawiera informacje o dzwoniącym i użytkowniku, który odebrał połączenie przychodzące, z opcjami odebrania połączenia, wyciszenia lub zignorowania powiadomienia. Odebranie połączenia przychodzącego przez użytkownika inicjuje kierowane przejmowanie połączenia.

Począwszy od wersji 43.4, lista użytkowników monitorowanych przez BLF jest dostępna w oknie Multi Call Window (MCW) dla połączeń (dostępne tylko dla systemu Windows). Integracja listy BLF w MCW obejmuje:

- Monitoruj połączenia przychodzące z opcją odebrania połączenia lub zignorowania alertu.
- Zobacz pełną listę użytkowników BLF.
- Monitoruj obecność użytkowników — rozbudowana obecność jest dostępna tylko dla użytkowników z uprawnieniami Webex Cloud. Podstawowa obecność (telefoniczna) jest dostępna tylko dla użytkowników BroadWorks.
- Rozpocznij połączenie z użytkownikiem BLF.
- Rozpocznij czat z użytkownikiem BLF — dostępny tylko dla użytkowników z uprawnieniami Webex Cloud.
- Dodaj użytkownika BLF jako kontakt.

```
<config>
  <usługi>
    <połączenia>
      <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	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	prawda, fałsz	Włącza monitorowanie pola sygnalizacji zajętości i powiadamianie o dzwonieniu dla innych użytkowników z możliwością odbierania połączeń.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	true	prawda, fałsz	Umożliwia wyświetlanie wyświetlanej nazwy/numeru dzwoniącego w powiadomieniu o dzwonieniu.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Określa, o ile sekund powiadomienie o dzwonieniu powinno być opóźnione, zanim zostanie wyświetlone użytkownikowi.

UWAGA: Ta funkcja zależy od usługi kierowanego przejmowania połączeń.

6.2.8.2 Grupa przejmowania połączeń (tylko Webex Calling)

Począwszy od wersji 44.2, Webex aplikacja dodaje obsługę powiadomień o przejmowaniu połączeń grupowych (GCP) dla wdrożenia Webex Calling. Umożliwia użytkownikom otrzymywanie powiadomień o połączeniach przychodzących dla dowolnego użytkownika monitorowanego przez grupę Przejmowanie połączeń.

W przypadku połączenia przychodzącego do użytkownika należącego do grupy przejmowania połączeń, osoba dzwoniąca ma szansę odebrać połączenie. Istnieje opóźnienie powiadomienia GCP, które można skonfigurować za pomocą centrum sterowania. Jeśli rozmówca nie przetworzy połączenia w skonfigurowanym czasie, do grupy zostanie wysłane powiadomienie GCP.

W przypadku wielu połączeń w ramach tej samej grupy przejmowania połączeń są one przetwarzane sekwencyjnie na podstawie czasu ich odebrania. Powiadomienie o najstarszym połączeniu jest początkowo dostarczane do grupy, a po przetworzeniu kolejne powiadomienie w kolejce jest dostarczane do grupy.

Powiadomienia mogą być tylko dźwiękowe, tylko wizualne lub dźwiękowo-wizualne w zależności od konfiguracji w portalu administracyjnym centrum sterowania. Jeśli istnieje wizualne powiadomienie GCP, użytkownik może odebrać połączenie za pomocą funkcji Przejmowanie połączeń. Jeśli skonfigurowane jest powiadomienie tylko dźwiękowe, użytkownik nie zobaczy wizualnego powiadomienia o połączeniu przychodzącym, usłyszy określony sygnał dzwonka i będzie mógł odebrać połączenie z menu przejmowania 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) i domyślnie powiadomienia są wyciszone.

Funkcja działa dla linii podstawowych oraz dla linii współdzielonych lub wirtualnych przypisanych do użytkownika.

Poufne informacje Cisco

```
<config>
<usługi><połączenia>
    <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%"/>
    </grupowe powiadomienia o odebraniu połączenia>
...
<protokoły><sip>
    <linie>
        <linia>
            <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
            ...
        </linia>
        <linia>
            <grupowe-przejmowanie-połączeń>%BWGROUP-CALL-PICKUP-BOOL-2%</group-
call-pickup>
            ...
        </linia>
        ...
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	prawda, fałsz	Włącza powiadomienia o przejmowaniu połączeń grupowych
%ENABLE_GCP_DISPLAY_CALLER_WXT%	true	prawda, fałsz	Umożliwia wyświetlanie wyświetlanej nazwy/numeru osoby dzwoniącej w powiadomieniu o dzwonieniu
%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 na odpowiedniej linii skonfigurowano grupę przejmowania połączeń

UWAGA 1: Jest to funkcja tylko dla Webex Calling.

UWAGA 2: Ta funkcja zależy od grupy przejmowania połączeń skonfigurowanej dla użytkownika.

6.2.9 Pakiet zdarzeń zdalnego sterowania

W przypadku klientów typu Kliknij, aby zadzwonić, takich jak cienki klient BroadWorks Receptionist i integrator Go, w których aplikacja Webex jest urządzeniem dzwoniącym, podczas odbierania połączenia lub obsługi, zawieszania/wznawiania aplikacja Webex honoruje teraz pakiet zdarzeń zdalnego sterowania.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false	Prawda, fałsz	Po ustawieniu wartości "true" określa, że użytkownik powinien mieć włączony pilot zdalnego sterowania.

6.2.10 Wybór identyfikatora CLID agenta kolejki połączeń

Gdy agenci dzwonią do swoich klientów, chcą, aby klienci widzieli odpowiedni identyfikator linii wywołującej (CLID), a nie ich osobisty / firmowy CLID. Na przykład, jeśli agentka Mary Smith jest dołączona do kolejki połączeń pomocy technicznej, to podczas dzwonienia do klientów Mary chce, aby klienci widzieli jej CLID jako pomoc techniczną, a nie Mary Smith.

Administratorzy w Control Hub lub CommPilot mogą określić dla kolejki połączeń jeden lub więcej numerów DNIS, które mają być używane dla wychodzącego CLID. Agenci mają wtedy możliwość wybrania jednego z numerów DNIS, który ma być używany jako ich CLID podczas wykonywania połączeń wychodzących. Aplikacja Webex umożliwia agentom wybór DNIS, który ma być używany jako ich CLID.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%	false	Prawda, fałsz	Włącza połączenia wychodzące (wybór CLID) w imieniu kolejki biura obsługi.

6.2.11 Survivability Gateway (tylko Webex Calling)

Począwszy od wersji 43.2, Webex aplikacja dodaje obsługę trybu wywołania Survivability. Jeśli funkcja jest włączona i nie ma łączności Webex z chmurą, aplikacja Webex może działać w trybie przetrwania. W tym trybie dostępna jest ograniczona funkcjonalność połączeń dla użytkownika.

Lokalna brama przeżywalności jest wdrażana przez klienta.

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


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	prawda, fałsz	Włącza obsługę trybu przeżywalności.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Określa czas awaryjny (brama przeżywalności do SSE)

UWAGA: Ta funkcja zapewnia pewność migracji z rozwiązań do połączeń lokalnych do rozwiązań do połączeń w chmurze.

6.2.12 Pakiet zdarzeń zdalnego wyciszenia (tylko Webex Calling)

Począwszy od wersji 43.9, aplikacja Webex dodaje obsługę zdalnego wyciszania połączeń strumienia multimediów audio. Umożliwia to wyciszenie/wyłączenie wyciszenia trwającego połączenia z innej lokalizacji, takiej jak cienki klient BroadWorks Receptionist, gdzie urządzeniem dzwoniącym jest aplikacja Webex.

Funkcja zależy od nowego pakietu informacyjnego SIP *x-cisco-mute-status* . *Jeśli nagłówek Recv-Info:x-cisco-mute-status* zostanie odebrany podczas ustanawiania sesji SIP INVITE połączenia, to za każdym razem, gdy następuje aktualizacja (lokalna lub zdalna) stanu wyciszenia sesji połączenia audio, aplikacja Webex odsyła SIP INFO z Info-Package *:x-cisco-mute-status; muted=true* (lub *muted=false*), gdzie parametr muted reprezentuje zaktualizowany stan strumienia multimediów audio.

Wyciszenie lub wyłączenie wyciszenia może być wyzwalane lokalnie lub z lokalizacji zdalnej. Zdalna aktualizacja wyzwala wyciszenie (lub wyłączenie wyciszenia) protokołu SIP NOTIFY ze *zdarzeniem: wyciszenie* (lub *wyłączenie wyciszenia*) do aplikacji Webex z serwera aplikacji. Aplikacja Webex honoruje zdalne żądanie i po aktualizacji stanu strumienia multimediów audio odsyła SIP NOTIFY z Info-Package *:x-cisco-mute-status; muted=true* (lub *muted=false*).

```
<config>
<usługi>
   <połączenia>
       <zdalne wyciszenie-enabled = "%ENABLE_REMOTE_MUTE_CONTROL_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false	Prawda, fałsz	Po ustawieniu wartości "true" zdalne wyciszanie połączeń jest włączone dla użytkownika.

Poufne informacje Cisco

6.2.13 Przenoszenie połączenia

Webex aplikacja zapewnia monitorowanie połączeń i sterowanie połączeniami VoIP zakończonymi w innej lokalizacji. Ta opcja jest obecnie dostępna tylko dla głównej linii użytkownika.

Począwszy od wersji 43.12, aplikacja Webex została rozszerzona o wyświetlanie połączeń zakończonych w innej lokalizacji, również dla linii współdzielonych i wirtualnych. Takie połączenia są widoczne w obszarze bieżących połączeń w celach informacyjnych i bez możliwości ich kontrolowania. Tylko wtedy, gdy takie połączenie zostanie zawieszone, użytkownik będzie mógł przenieść je na urządzenie lokalne, wybierając je i wznowić z ekranu połączenia. Ten mechanizm jest przydatny, jeśli połączenie zostało obsłużone przez tego samego użytkownika w innej lokalizacji lub przez innego użytkownika korzystającego z tej samej linii.

Pamiętaj, że aplikacja Webex nie może przenieść zawieszonego połączenia na sparowane urządzenie. Jeśli użytkownik jest sparowany z urządzeniem, musi najpierw się rozłączyć, a następnie wznowić zawieszone połączenie lokalnie.

Monitorowanie połączeń dla linii udostępnionej i wirtualnej zależy od pakietu zdarzeń SIP call-info.

Monitorowanie połączeń dla linii podstawowej użytkownika zależy od zdarzeń XSI (pakiet zdarzeń Advanced Call), a przenoszenie połączenia na urządzenie lokalne nie jest dostępne dla tych połączeń. W przypadku tego typu połączeń użytkownik może użyć funkcji ściągania połączeń (*6.1.22 Ściąganie połączeń*). Ściąganie połączeń działa tylko dla ostatnich aktywnych połączeń użytkownika, podczas gdy mechanizm dla linii współdzielonych i wirtualnych działa dla wszystkich połączeń użytkownika, które są zawieszone.

- Przypadek użycia 1:
    a. Alicja ma linię Roberta przypisaną do profili Komputer stacjonarny i Telefon biurkowy.
    b. Alicja rozmawia z Charliem przez telefon biurkowy — Alicja widzi trwające połączenie w aplikacji Komputer.
    c. Alicja zawiesza połączenie na telefonie biurkowym — połączenie może zostać wznowione przez Alicję z aplikacji Komputer.
- Przypadek użycia 2:
    a. Alicja ma linię Roberta przypisaną do profili Komputer stacjonarny i Telefon biurkowy.
    b. Bob ma rozmowę z Charliem — Alicja widzi trwające połączenie w aplikacji Komputer.
    c. Bob zawiesza połączenie z Charliem — Alicja może wznowić połączenie z Charliem w aplikacji Komputer.
- Przypadek użycia 3:
    a. Alicja ma linię Roberta przypisaną do profili Komputer stacjonarny i Telefon biurkowy.
    b. Alicja jest sparowana ze swoim telefonem biurkowym z aplikacji Komputer.
    c. Bob ma rozmowę z Charliem — Alicja widzi trwające połączenie w aplikacji Komputer.
    d. Bob zawiesza połączenie z Charliem — Alicja nie może wznowić połączenia z Charliem z aplikacji Komputer.

Poufne informacje Cisco

e. Alicja odłącza aplikację Komputer od telefonu stacjonarnego — Alicja może wznowić połączenie z Charliem z aplikacji Komputer.

```
<config>
<usługi><połączenia>
    <call-move>
         <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALL_MOVE_HERE_WXT%	false	Prawda, fałsz	Umożliwia przenoszenie połączeń na urządzeniu lokalnym. Służy do zawieszania/wznawiania między lokalizacjami/użytkownikami w przypadku użycia wielu linii.

Poufne informacje Cisco

6.3 Funkcje dostępne tylko dla urządzeń przenośnych

6.3.1 Połączenia alarmowe

Webex dla Cisco BroadWorks obsługuje natywne połączenia alarmowe.

Gdy funkcja jest włączona, podczas inicjowania wychodzącego połączenia VoIP aplikacja analizuje wybrany numer i porównuje go ze skonfigurowaną listą numerów alarmowych. Jeśli numer zostanie zidentyfikowany jako numer alarmowy, aplikacja wykona skonfigurowane zachowanie wybierania. Można go konfigurować za pomocą znacznika sekwencji *wybierania* .

Obsługiwane tryby to:

- cs-only — klient wykonuje połączenia alarmowe tylko za pośrednictwem sieci komórkowej, jeśli sieć jest dostępna.
- cs-first – Po zainicjowaniu połączenia alarmowego klient sprawdza typ sieci, do której podłączone jest bieżące urządzenie. Jeśli sieć komórkowa jest dostępna, klient nawiązuje połączenie za pośrednictwem sieci komórkowej. Jeśli sieć komórkowa jest niedostępna, ale dostępna jest sieć komórkowa danych/Wi-Fi, klient nawiązuje połączenie przez sieć komórkową danych/Wi-Fi jako połączenie VoIP. Ponadto, jeśli połączenie alarmowe jest nawiązywane za pośrednictwem sieci komórkowej, klient sugeruje użytkownikowi ponowienie połączenia alarmowego w VoIP.
- Tylko VoIP – klient wykonuje połączenia alarmowe tylko wtedy, VoIP gdy dostępna jest sieć danych komórkowych/Wi-Fi.
- cs-voip – Klient analizuje, czy urządzenie może zainicjować je jako natywne połączenie komutowane (CS) (bez brania pod uwagę, czy sieć CS jest dostępna, czy nie). Jeśli urządzenie może rozpocząć połączenie natywne, numer alarmowy jest wybierany jako połączenie CS dla połączeń alarmowych. W przeciwnym razie połączenie zostanie wybrane jako VoIP.

> **UWAGA**: Jeśli połączenia VOIP są wyłączone, jedyną znaczącą wartością dla sekwencji wybierania alarmowego (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) jest cs-only.

Podczas logowania użytkownikowi jest wyświetlany komunikat o wyłączeniu odpowiedzialności za połączenia alarmowe. Nie jest kontrolowany za pomocą opcji konfiguracji.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_EMERGENCY_DIALING_WXT%	false	prawda, fałsz	Ustaw wartość "true", aby włączyć wykrywanie połączeń alarmowych. Wartością domyślną jest puste pole.

Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	Tylko CS	cs-only,cs-first,voip-only,cs-voip	Steruje trybem wybierania numerów dla połączeń alarmowych.
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	Lista CSV	CSV listę numerów alarmowych. Przykład: 911,112

6.3.2 Powiadomienia push o połączeniach

Po odebraniu połączenia przychodzącego klient mobilny otrzymuje najpierw powiadomienie push (PN). Istnieje parametr konfiguracyjny, który może być użyty do kontrolowania, kiedy sesja SIP REGISTER ma zostać ustanowiona:

1. Po otrzymaniu powiadomienia push, LUB
2. Po zaakceptowaniu połączenia przez użytkownika.

Zalecane jest drugie podejście. Jednak w porównaniu z pierwszym przypadkiem dodaje pewne opóźnienie przed nawiązaniem połączenia.

Zgodnie z wymaganiami iOS 13, VoIP PN powinny być używane tylko dla połączeń przychodzących. Pozostałe zdarzenia związane z połączeniem powinny korzystać ze zwykłych PN.

Aby spełnić to wymaganie, wprowadzono nowy API rejestracji PN, który wymaga zastosowania odpowiedniej poprawki na serwerze aplikacji. Jeśli zaplecze nie jest skonfigurowane do obsługi iOS 13 PN, parametru konfiguracyjnego można użyć do wymuszenia użycia starszych powiadomień push, w których wszystkie zdarzenia związane z połączeniem są dostarczane za pośrednictwem VoIP PN.

Serwer aplikacji (AS) wysyła powiadomienie push, gdy dzwoniące połączenie zostanie zaakceptowane przez rozmówcę w innej lokalizacji, zamknięte przez dzwoniącego lub, na przykład, przekierowane do poczty głosowej. W systemie iOS 13 ten typ powiadomienia push jest teraz zwykły i ma pewne ograniczenia. Może być opóźniony przez usługę Apple Push Notification Service (APNS) lub nawet w ogóle nie dostarczony. Aby obsłużyć brakujące lub opóźnione PN aktualizacji połączeń, dodano konfigurowalny limit czasu dzwonienia w celu kontrolowania maksymalnego czasu dzwonienia. Jeśli zostanie osiągnięty maksymalny czas dzwonienia, dzwonienie dla dzwoniącego zostanie zatrzymane, a połączenie będzie traktowane jako nieodebrane. Po stronie wywołującego połączenie może pozostać w stanie dzwonienia do momentu wykonania zasady braku odpowiedzi skonfigurowanej na serwerze aplikacji (AS).

Aby zachować spójność działania aplikacji, konfigurowalny zegar dzwonienia dotyczy zarówno systemu Android, jak i iOS.

Poufne informacje Cisco

Dodano oddzielną opcję konfiguracji, aby określić zachowanie odrzucania połączenia, gdy połączenie przychodzące jest odbierane jako powiadomienie push. Klienta można skonfigurować tak, aby ignorował połączenie lub odpowiadał serwerowi przez Xsi z opcją odrzucenia ustawioną na "true" lub "false", w którym to przypadku zostaną zastosowane przypisane usługi przetwarzania wywołań Cisco BroadWorks. Jeśli skonfigurowano "decline_false", połączenie będzie nadal dzwonić do momentu porzucenia połączenia przez inicjatora lub wygaśnięcia licznika czasu braku odpowiedzi i rozpoczęcia powiązanych usług przetwarzania połączeń. Jeśli skonfigurowano "decline_true", przyczyna odrzucenia określa przetwarzanie połączenia. Jeśli przyczyna odrzucenia jest ustawiona na "zajęty", serwer natychmiast wymusza zajętą usługę leczenia. Jeśli skonfigurowano "temp_unavailable", stosowana jest tymczasowa niedostępna usługa leczenia.

```
<config>
<usługi>
    <powiadomienia push dla-połączeń enabled="true"
    connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
    ring-timeout-seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"/>
    <połączenia>
        <reject-with-xsi mode="%REJECT_WITH_XSI_MODE_WXT%"
        declineReason="%REJECT_WITH_XSI_DECLINE_REASON_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	prawda, fałsz	Kontroluje, kiedy sesja SIP REGSITER jest ustanawiana – po otrzymaniu powiadomienia Push o połączeniu przychodzącym lub po jego zaakceptowaniu.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Określa maksymalny czas dzwonienia połączenia przychodzącego dla połączeń odebranych przez PN. Jeśli w podanym terminie nie zostanie odebrany żaden CallUpd PN, połączenie będzie traktowane jako nieodebrane.
%REJECT_WITH_XSI_MODE_WXT%	decline_fałsz	ignoruj, decline_true, decline_false	Określa zachowanie podczas odrzucania połączeń.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	zajęte	zajęty, temp_unavailable	Określa przyczynę odrzucenia połączenia, jeśli tryb odrzucenia jest ustawiony na "decline_true".

6.3.2.1 MWI

Po włączeniu funkcji MWI klient Webex mobilnego subskrybuje MWI powiadomienie push, aby otrzymywać aktualizacje pocztą głosową użytkownika i powiadamiać go.

Aby zmniejszyć liczbę powiadomień i uniknąć niepotrzebnego rozpraszania uwagi, MWI powiadomienia push są w niektórych przypadkach pomijane. Na przykład, gdy użytkownik słucha wiadomości poczty głosowej lub oznacza je jako przeczytane z poziomu klienta Webex mobilnego (zmniejsza się liczba nieprzeczytanych). Nie ma konfigurowalnej opcji, aby to kontrolować.

Poufne informacje Cisco

Aby uzyskać więcej informacji na temat MWI, sprawdź sekcję *6.1.27 Poczta głosowa, wizualna poczta głosowa, wskaźnik* oczekujących wiadomości.

6.3.2.2 Pierścień Splash

Usługi BroadWorks (takie jak DND) mogą wysyłać przypomnienia o dzwonku, gdy przychodzące jest przekierowywane. Klienta Webex Mobile można skonfigurować tak, aby włączał powiadomienia Ring Splash Push i prezentował je użytkownikowi, gdy są wyzwalane przez BroadWorks.

```
konfiguracja>
<usługi>
<ring-splash enabled="%ENABLE_RING_SPLASH_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_RING_SPLASH_WXT%	false	prawda, fałsz	Włącza Ring Splash w konfiguracji BroadWorks.

6.3.2.3 Sposób dostawy (tylko Webex Calling)

Aplikacja Webex wykorzystuje serwer NPS (Notification Push Server) do dostarczania powiadomień push dla połączeń APNS/FCM. Wersja 45.2 aplikacji Webex obsługuje teraz trzy różne tryby dostarczania w celu skonfigurowania sposobu dostarczania powiadomień push związanych z połączeniami do APNS/FCM:

- nps - mechanizm prądowy, wykorzystujący NPS
- chmura - ulepszony mechanizm, wykorzystujący mikroserwis Cisco Webex Cloud
- Zewnętrzny - mechanizm wykorzystujący system innej firmy. Wymaga to integracji systemu innej firmy z mechanizmem Cisco WebHooks

```
<config>
<usługi><połączenia>
<powiadomienia push dla-połączeń 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	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	NPS	NPS, chmura, zewnętrzny	Określa sposób dostarczania powiadomień push dla połączeń.

Poufne informacje Cisco

6.3.3 Alert pojedynczy

Funkcja Mobile Single Alert jest przeznaczona dla wdrożeń konwergencji stacjonarnej i komórkowej (FMC) / operatora sieci komórkowej (MNO) wykorzystujących usługę BroadWorks Mobility. Bez niego, po zalogowaniu się do klienta Webex i odebraniu połączenia przychodzącego, użytkownik otrzyma jednocześnie dwa połączenia – natywne i połączenie Push Notification (VoIP). Gdy funkcja jest włączona, aplikacja wyłączy alerty Mobility w lokalizacji BroadWorks Mobility użytkownika podczas logowania i włączy alerty podczas wylogowywania. Ważnym warunkiem wstępnym korzystania z tej funkcji jest przypisanie użytkownikowi usługi BroadWorks Mobility i skonfigurowanie dokładnie jednej lokalizacji.

```
<config>
<usługi><połączenia>
<single-alerting enabled="%ENABLE_SINGLE_ALERTING_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_SINGLE_ALERTING_WXT%	false	Prawda, fałsz	Ustaw wartość "true", aby włączyć alerty pojedyncze.

6.3.4 Kliknij, aby zadzwonić (Oddzwoń)

Wychodzące połączenie "Kliknij, aby wybrać" zapewnia, że użytkownik końcowy może nawiązać połączenie ze swoim osobistym telefonem komórkowym z komutacją obwodu i podać swoją służbową nazwę wyróżniającą jako identyfikator linii wywołującej.

Klient Mobile Webex obsługuje połączenia typu Kliknij, aby wybrać (Oddzwoń) przy użyciu usługi BroadWorks Anywhere. Lokalizacje BroadWorks Anywhere w aplikacji Webex nazywane są lokalizacjami Single Number Reach (SNR).

Gdy funkcja jest włączona, użytkownicy mogą wybrać lokalizację SNR z menu parowania urządzeń. Po sparowaniu z SNR lokalizacją wszystkie połączenia wychodzące są inicjowane za pomocą funkcji Kliknij, aby wybrać numer (Oddzwoń). Aby zapobiec podwójnemu alarmowaniu, powiadomienia push dla połączeń przychodzących są wyłączone.

Gdy użytkownik zainicjuje połączenie "Kliknij, aby wybrać", zobaczy ekran połączenia wychodzącego z informacją, że może oczekiwać połączenia przychodzącego w wybranej lokalizacji SNR. Ten ekran jest zamykany automatycznie na podstawie konfigurowalnego timera.

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

```
<config>
<usługi>
  <wybieranie numeru>
    <call-back enabled="%ENABLE_DIALING_CALL_BACK_WXT%"
timer="%DIALING_CALL_BACK_TIMER_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_DIALING_CALL_BACK_WXT%	false	Prawda, fałsz	Ustaw wartość "true", aby włączyć połączenia typu Kliknij, aby zadzwonić.
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Określa liczbę sekund przed automatycznym zamknięciem ekranu Oddzwoń.

6.3.5 Obsługa MNO

6.3.5.1 Nawiązywanie połączeń przy użyciu natywnego programu wybierającego

Ta funkcja dodaje obsługę wdrożeń operatora sieci komórkowej (MNO) wykorzystujących usługę BroadWorks Mobility (BWM). Zakłada się, że użytkownik ma przypisaną usługę BroadWorks Mobility i skonfigurowano co najmniej jedną lokalizację.

Możliwość inicjowania połączeń przez użytkownika za pośrednictwem natywnego programu wybierającego jest kontrolowana przez natywny **tag konfiguracyjny** . Jeśli ta opcja jest włączona, aplikacja uruchomi natywny dialer i wykona połączenie. Ponadto dostępność połączeń VoIP jest kontrolowana przez **tag voip** – w zależności od wymagań wdrożenia, VoIP połączenia mogą być włączone lub wyłączone.

Jeśli VoIP i Połączenia natywne są włączone, użytkownik będzie mógł wybrać opcję, której użyć.

Tag <tryb wybierania numeru> określa, czy użytkownicy mogą wybrać sposób rozpoczynania/odbierania połączeń przychodzących i wychodzących. Wymaga włączenia zarówno połączenia natywnego, jak i VoIP.

Począwszy od wersji 43.12 rozszerzono macierzystą konfigurację wybierania, umożliwiając wstępne przypisanie niestandardowego prefiksu do numeru połączenia wychodzącego. Dotyczy to połączeń komórkowych inicjowanych z aplikacji Webex tylko wtedy, gdy wybrany numer zaczyna się od kodu FAC.

Ta funkcja jest przydatna dla klientów korzystających z wdrożeń MNO, w których połączenia zamiast być przekierowywane do zintegrowanego serwera aplikacji Cisco BroadWorks, kody FAC mogą być obsługiwane przez zaplecze telekomunikacyjne. Nowy tag <fac-prefix> został dodany w sekcji <wybieranie><natywny> i telekomy mogą go użyć do rozwiązania tego problemu.

```
<config>
<usługi>
  <wybieranie numeru>
    <VoIP Enabled="%ENABLE_DIALING_VOIP_WXT%"/>
    <natywne włączone="%ENABLE_DIALING_NATIVE_WXT%" enable-bwks-mobility-
dependency="%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%">
      <fac-prefix value="%DIALING_NATIVE_FAC_PREFIX_WXT%"/>
    </rodzimy>
    <dialing-mode enabled="%ENABLE_DIALING_MODE_WXT%" default="%DIALING_MODE_DEFAULT_WXT%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_DIALING_VOIP_WXT%	true	prawda, fałsz	Ustaw na "true", aby włączyć opcję połączenia VoIP.
%ENABLE_DIALING_NATIVE_WXT%	false	prawda, fałsz	Ustaw na "true", aby włączyć opcję połączenia natywnego.
%ENABLE_DIALING_MODE_WXT%	false	Prawda, fałsz	Włącza wybór trybu połączenia przez użytkownika za pośrednictwem ustawień połączeń w Preferencjach.
%DIALING_MODE_DEFAULT_WXT%	VoIP	VoIP, natywna	Określa wybrany domyślny tryb połączeń.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false	prawda, fałsz	Określa, czy dostępność połączeń macierzystych powinna zależeć od przypisania usługi BroadWorks Mobility i lokalizacji przenośności skonfigurowanej dla użytkownika.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*pusty*	łańcuch	Określa prefiks, który powinien być poprzedzony, jeśli połączenie wychodzące na numer rozpoczynający się od kodu FAC jest inicjowane jako połączenie komórkowe. Domyślnie nie jest zdefiniowany żaden prefiks FAC, a znacznik jest pusty.

UWAGA 1: Powinno być włączone co najmniej jedno z połączeń **VoIP** i **natywnych** .

UWAGA 2: Jeśli włączone jest tylko **wywołanie natywne** , we wdrożeniach MNO zaleca się wyłączenie alertów jednokrotnych, aby uniemożliwić klientowi wyłączenie alertów BWM.

UWAGA 3: Jeśli włączone są zarówno połączenia natywne **, jak** i **połączenia VoIP** , we wdrożeniach MNO zaleca się włączenie pojedynczego alertu, aby zapobiec podwójnemu alarmowaniu.

6.3.5.2 Elementy sterujące w trakcie połączenia

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

- Usługa BroadWorks Mobility (BWM) jest przypisana do użytkownika,
- Skonfigurowano tylko jedną tożsamość mobilną BMW,
- Tryb wywołania natywnego jest wybierany przez użytkownika (więcej informacji w sekcji *6.3.5.1 Nawiązywanie połączeń przy użyciu* natywnego programu wybierającego *sprawdź),*
- Istnieje połączenie zakotwiczone w BroadWorks, przechodzące przez serwis BMW,

Poufne informacje Cisco

- Na urządzeniu przenośnym trwa połączenie komórkowe.

Wersja 43.10 dodaje lepszą obsługę przekazywania konsultacyjnego, tworząc powiązanie między dwoma połączeniami komórkowymi prezentowanymi w aplikacji Webex i udostępniając użytkownikowi opcję ukończenia transferu. Ponadto, jeśli użytkownik ma dwa niezależne połączenia komórkowe na tym samym urządzeniu, menu przesyłania jest rozszerzone, aby umożliwić przesyłanie jednego do drugiego, nawet jeśli nie ma między nimi powiązania.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_XSI_CALL_CONTROL_WXT%	false	prawda, fałsz	Włącza sterowanie połączeniami XSI dla środowiska MNO.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Kontroluje typ wdrożenia XSI MNO używany przez aplikację. Możliwe wartości to: ▪ MNO_Access – pokazuje wszystkie połączenia zdalne (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%	“”	łańcuch	Nazwy typów urządzeń, które powinny być używane w MNO_Access typu wdrożenia.
%ENABLE_XSI_HOLD_CALLS_WXT%	true	Prawda, fałsz	Określa, czy akcja Wstrzymanie połączenia ma być dostępna dla użytkownika dla połączeń komórkowych XSI.

6.3.5.3 Tożsamość wychodzącej linii telefonicznej (CLID) – podwójna persona

W wersji Mobile 42.12 aplikacja Webex umożliwia użytkownikom wybranie tożsamości linii wywołującej (CLID) prezentowanej stronie zdalnej po zainicjowaniu połączenia wychodzącego.

Jeśli użytkownik ma skonfigurowaną funkcję Cisco BroadWorks Mobility, typową konfigurację wdrożeń operatora sieci komórkowej (MNO) i włączono funkcję Połączenia natywne, użytkownik może wybrać tożsamość, która ma być prezentowana osobom, do których dzwoni. Użytkownik może wybrać swoją tożsamość biznesową lub osobistą. Istnieje również opcja ukrycia własnej tożsamości i połączenia przedstawianego jako anonimowe.

W przypadku połączeń VoIP użytkownik ma również możliwość kontrolowania swojego CLID. Dostępną opcją w tym przypadku jest tylko kontrolowanie, czy ukryć swoją tożsamość, czy nie.

Poufne informacje Cisco

Zarządzanie minimotywami i blokowanie CLID są kontrolowane za pomocą oddzielnych opcji konfiguracji.

```
<config>
<usługi>
<wybieranie numeru>
   <calling-line-id-delivery-blocking
enabled="%ENABLE_CLID_DELIVERY_BLOCKING_WXT%"/>
   <mobility-persona-management
enabled="%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%"/>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	false	Prawda, fałsz	Włącza blokowanie dostarczania identyfikatora linii wywołującej. Dotyczy to wszystkich typów połączeń wychodzących dla użytkownika.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	false	Prawda, fałsz	Umożliwia osobiste zarządzanie połączeniami natywnymi, gdy typ wdrożenia został skonfigurowany jako MNO_Access lub MNO_Network. (BroadWorks Mobility jest używany dla połączeń natywnych, a wszystkie połączenia natywne są zakotwiczone w BroadWorks)

6.3.5.4 Powiadomienia o połączeniach natywnych

W przypadku użytkowników wdrożonych z MNO ta funkcja dodaje baner powiadomień dla połączeń natywnych, które można kontrolować za pomocą aplikacji Webex. To powiadomienie opiera się na powiadomieniu push wysyłanym przez serwer aplikacji po nawiązaniu połączenia.

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	true	prawda, fałsz	Włącza subskrypcję MOBILE_CALL_INFO powiadomień push.

6.3.5.5 Przenoszenie połączenia natywnego na spotkanie konwergentne

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, podczas spotkania strony będą miały możliwość:

Poufne informacje Cisco

- Inicjowanie Webex w rozmowie na czacie na spotkaniu
- Dodaj wideo (zwróć uwagę, że dźwięk będzie kontynuowany w połączeniu natywnym)
- Udostępnij ekran / zawartość
- Nagrywanie spotkań wyzwalających

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	prawda, fałsz	Włącza Power Up (Invite and Meet, Video Meet).

6.3.5.6 Mobilność MNO - widżet In-call

W wersji 43.7 aplikacji Android Webex (Mobile and Tablet) oficjalnie wprowadzono nowy widżet sterowania połączeniami (bubble), zapewniający dodatkową kontrolę połączeń natywnych zakotwiczonych w Cisco BroadWorks, przy użyciu usługi Mobility. Widżet zostanie wyświetlony na górze natywnego interfejsu użytkownika i umożliwi użytkownikowi następujące działania:

- Zawieś/Wznów
- Blind/Consultative Transfer – umieszcza użytkownika w oknie dialogowym transferu w aplikacji Webex.
- Kompletny transfer — opcja dokończenia transferu konsultacyjnego (wersja 43.10)
- Spotkanie wideo – przenosi strony do Webex spotkania.
- Zakończ połączenie

```
<config>
<usługi><połączenia>
       <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%"/>
```


Poufne informacje Cisco

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_WIDGET_HOLD_CALLS_WXT%	true	Prawda, fałsz	Określa dostępność operacji Zawieś w widżecie połączenia.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	true	Prawda, fałsz	Określa dostępność akcji Przekaż i Zakończ przekazanie w widżecie połączenia.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	true	Prawda, fałsz	Kontroluje dostępność akcji Spotkanie wideo w widżecie Połączenie.

6.3.6 Identyfikator rozmówcy przychodzącego

W wersji 44.2 dodano możliwość kontrolowania informacji kontaktowych prezentowanych użytkownikowi na podstawie nazwy i numeru. Dodano dwie opcje konfiguracji w celu kontrolowania informacji prezentowanych użytkownikowi na ekranie połączenia przychodzącego i powiadomień o połączeniach przychodzących oraz powiadomień o nieodebranych połączeniach.

6.3.6.1 Ekran połączenia przychodzącego

Istnieją różnice między platformami Android i iOS, jeśli chodzi o wyświetlanie danych na ekranie połączenia przychodzącego. Natywne środowisko wyświetlania informacji o połączeniu przychodzącym jest następujące:

Android - na ekranie połączenia przychodzącego znajdują się dwa oddzielne pola, w których wyświetlane są zarówno nazwa, jak i numer

iOS - jest tylko jedno pole do wyświetlania nazwy lub numeru - jeśli oba są dostępne, nazwa ma priorytet

Nowa opcja konfiguracji połączeń przychodzących może być użyta, aby upewnić się, że aplikacja iOS Webex wyświetli numer na ekranie połączenia obok nazwy (format: *Nazwa (numer)*). Nie ma to wpływu na zachowanie aplikacji Android Webex.

6.3.6.2 Powiadomienie o połączeniu przychodzącym

W niektórych przypadkach połączenie przychodzące jest prezentowane użytkownikowi jako powiadomienie. Ze względu na ograniczoną przestrzeń numer nie zawsze jest tam wyświetlany.

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

Poufne informacje Cisco

6.3.6.3 Powiadomienie o nieodebranym połączeniu

Dodano dodatkowy parametr konfiguracyjny dla powiadomień o nieodebranych połączeniach. Może być używany do kontrolowania informacji o zdalnej stronie, podobnie jak powiadomienia o połączeniach przychodzących, umożliwiając dołączenie numeru do nazwy wyświetlanej zdalnego użytkownika i przedstawienie go w powiadomieniu o nieodebranym połączeniu. To zachowanie aplikacji Webex ma zastosowanie zarówno do systemu Android, jak i iOS.

```
<config>
<usługi><połączenia>
   <identyfikator dzwoniącego>
      <połączenia przychodzące>
         <append-number enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
      </połączenia przychodzące>
      <Nieodebrane połączenia>
         <append-number enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
      </nieodebrane połączenia>
```

Znacznik	Domyślne, jeśli zostało pominięte	Obsługiwane wartości	Opis
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false	prawda, fałsz	Określa, czy numer ma być dołączany do nazwy na ekranie połączenia przychodzącego (tylko iOS) i powiadomieniach.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	false	prawda, fałsz	Określa, czy numer ma być dołączany do nazwy w powiadomieniu o nieodebranym połączeniu.

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

Poufne informacje Cisco

7 Funkcje BETA (Early Field Trial)

W wersji BETA nie ma żadnych funkcji w najnowszej wersji.

Poufne informacje Cisco

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

W poniższej tabeli wymieniono Webex tagów niestandardowych Cisco BroadWorks, pasujące do starszych tagów niestandardowych dla UC-One.

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	N/D	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N/D	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	N/D	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	N/D
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	N/D
%ENABLE_CALL_STATISTICS_WXT%	N/D	N/D
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N/D	%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/D	N/D
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	N/D
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	N/D
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	N/D
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	N/D	N/D
%ENABLE_BROADWORKS_ANYWHERE_WXT%	N/D	N/D

Poufne informacje Cisco

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	N/D	N/D
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	N/D	N/D
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	N/D	N/D
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	N/D	N/D
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	N/D	N/D
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	N/D	N/D
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	N/D	N/D
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	N/D	N/D
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	N/D	N/D
%ENABLE_EMERGENCY_DIALING_WXT%	N/D	N/D
%EMERGENCY_DIALING_NUMBERS_WXT%	N/D	N/D
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	N/D	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	N/D
%SBC_ADDRESS_WXT%	%SBC_ADDRESS%	%SBC_ADDRESS%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILNY%
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	N/D
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	N/D

Poufne informacje Cisco

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%USE_TLS_FROM_DNS_WXT%	%USE_TLS_FROM_DNS%	N/D
%DOMAIN_OVERRIDE_WXT%	%DOMAIN_OVERRIDE%	%DOMAIN_OVERRIDE%
%SOURCE_PORT_WXT%	%SOURCE_PORT%	%SOURCE_PORT%
%USE_ALTERNATIVE_IDENTITIES_WXT%	%USE_ALTERNATIVE_IDENTITIES%	N/D
%TCP_SIZE_THRESHOLD_WXT%	%TCP_SIZE_THRESHOLD%	N/D
%SIP_REFRESH_ON_TTL_WXT%	%SIP_REFRESH_ON_TTL%	N/D
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	%ENABLE_SIP_UPDATE_SUPPORT_MOBILE%
%ENABLE_PEM_SUPPORT_WXT%	%ENABLE_PEM_SUPPORT_DESKTOP%	N/D
%ENABLE_SIP_SESSION_ID_WXT%	N/D	N/D
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	N/D	N/D
%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%	N/D
%CHANNEL_HEARTBEAT_WXT%	%CHANNEL_HEARTBEAT%	%CHANNEL_HEARTBEAT_MOBILNY%
%XSI_ROOT_WXT%	%XSI_ROOT%	%XSI_ROOT%
%XSI_ACTIONS_PATH_WXT%	N/D	%XSI_ACTIONS_PATH_MOBILE%
%XSI_EVENTS_PATH_WXT%	N/D	%XSI_EVENTS_PATH_MOBILE%

Poufne informacje Cisco

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	N/D	%ENABLE_CALLS_AUTO_RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N/D	%EMERGENCY_CALL_DIAL_SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLIND_WXT%	N/D	N/D
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	N/D	N/D
%WEB_CALL_SETTINGS_URL_WXT%	N/D	%WEB_CALL_SETTINGS_URL%
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP%
%ENABLE_CALL_CENTER_WXT%	%ENABLE_CALL_CENTER_DESKTOP%"	N/D
%WEB_CALL_SETTINGS_TARGET_WXT%	N/D	N/D
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_CFA_VISIBLE%
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_DND_VISIBLE%
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_ACR_VISIBLE%
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_CFB_VISIBLE%
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_CFNR_VISIBLE%
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_CFNA_VISIBLE%
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_SIMRING_VISIBLE%
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_SEQRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_RO_VISIBLE%
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_ACB_VISIBLE%
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_CW_VISIBLE%
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_CLIDB_VISIBLE%
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_PA_VISIBLE%

Poufne informacje Cisco

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_BWA_VISIBLE%
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	N/D	%WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE%
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_BWM_VISIBLE%
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	N/D	%WEB_CALL_SETTINGS_VM_VISIBLE%
%ENABLE_DIALING_CALL_BACK_WXT%	N/D	N/D
%DIALING_CALL_BACK_TIMER_WXT%	N/D	N/D
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	N/D
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N/D	%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_MOBILE%
%ENABLE_CALL_RECORDING_WXT%	%ENABLE_CALL_RECORDING_DESKTOP%	%CALL_RECORDING_MOBILE%
%ENABLE_SINGLE_ALERTING_WXT%	N/D	%ENABLE_SINGLE_ALERTING%
%ENABLE_CALL_PARK_WXT%	%ENABLE_CALL_PARK_DESKTOP%	N/D
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	N/D	N/D
%ENABLE_RTP_ICE_WXT%	N/D	N/D
%RTP_ICE_MODE_WXT%	N/D	N/D
%RTP_ICE_SERVICE_URI_WXT%	N/D	N/D
%RTP_ICE_PORT_WXT%	N/D	N/D
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	N/D	N/D
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/D	N/D
%ENABLE_DIALING_VOIP_WXT%	N/D	N/D
%ENABLE_DIALING_NATIVE_WXT%	N/D	N/D
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	N/D	N/D
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	N/D	N/D

Poufne informacje Cisco

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	N/D	N/D
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	N/D	N/D
%USER_PORTAL_SETTINGS_URL_WXT%	N/D	N/D
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	N/D	N/D
%ENABLE_AUDIO_MARI_FEC_WXT%	N/D	N/D
%ENABLE_AUDIO_MARI_RTX_WXT%	N/D	N/D
%ENABLE_VIDEO_MARI_FEC_WXT%	N/D	N/D
%ENABLE_VIDEO_MARI_RTX_WXT%	N/D	N/D
%ENABLE_CALL_BLOCK_WXT%	N/D	N/D
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N/D	N/D
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N/D	N/D
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/D	N/D
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	N/D	N/D
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	N/D	N/D
%ENABLE_CALL_MOVE_HERE_WXT%	N/D	N/D
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	N/D	N/D
%DIALING_NATIVE_FAC_PREFIX_WXT%	N/D	N/D
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	N/D	N/D
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	N/D	N/D
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N/D	N/D

Poufne informacje Cisco

Webex dla Tag Cisco BroadWorks	Starszy tag pulpitu	Starszy tag urządzenia mobilnego
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N/D	N/D
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N/D	N/D
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N/D	N/D
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N/D	N/D
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N/D	N/D
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N/D	N/D
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	N/D	N/D
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	N/D
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	N/D
%BLF_NOTIFICATION_DELAY_TIME_WXT%	N/D	N/D
%ENABLE_GCP_NOTIFICATIONS_WXT%	N/D	N/D
%ENABLE_GCP_DISPLAY_CALLER_WXT%	N/D	N/D
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	N/D	N/D
%UDP_KEEPALIVE_ENABLED_WXT%	N/D	N/D
%TCP_KEEPALIVE_ENABLED_WXT%	N/D	N/D
%TLS_KEEPALIVE_ENABLED_WXT%	N/D	N/D
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N/D	N/D
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	N/D	N/D

Poufne informacje Cisco

UWAGA: Nie dotyczy oznacza, że nie było odpowiedniego tagu niestandardowego sterującego tą funkcją w UC-One. Brak dotyczy zarówno dla klasycznych, jak i mobilnych tagów Legacy oznacza, że Webex tagu Cisco BroadWorks jest nowy i kontroluje nową funkcjonalność lub istniejącą funkcję, która nie była kontrolowana za pomocą tagu niestandardowego w UC-One.

Poufne informacje Cisco

9 Dodatek A: Szyfry TLS

Webex klienta BroadWorks korzysta z protokołu CiscoSSL, który jest oparty na OpenSSL z dodatkowym wzmocnieniem zabezpieczeń.

Poufne informacje Cisco

10 Dodatek B: Skrypt inicjowania obsługi tagów DM

Liczba niestandardowych tagów DM wzrasta z każdym wydaniem, ponieważ wielu klientów preferuje tagi dla nowych parametrów konfiguracyjnych. Aby ułatwić obsługę administracyjną tych 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 szczególnie dla nowych wdrożeń, w których przeznaczona jest większość niestandardowych tagów DM.

Należy pamiętać, że ten skrypt jest odpowiedni tylko dla nowych wdrożeń, w których są tworzone niestandardowe tagi DM. Aby zmodyfikować istniejące niestandardowe znaczniki DM, polecenie w poniższym skrypcie musi zostać zmienione z "add" na "set".

Szablon skryptu z ustawionymi tylko kilkoma tagami niestandardowymi (w rzeczywistym wdrożeniu konieczne byłoby wypełnienie większej listy tagów niestandardowych). Pamiętaj, że poniższy przykład dotyczy urządzeń mobilnych. Na komputerze użyj zestawu znaczników BroadTouch_tags zamiast Connect_Tags. W przypadku tabletu użyj zestawu tagów ConnectTablet_Tags zamiast Connect_Tags.

```
%% ********************************* Connect_Tags - odczyt ********************************* pliku
%%
%% Instrukcje:
%% -------------------
%% - Ten plik odczytu może być używany do tworzenia, dodawania i ustawiania Webex dla
BroadWorks
%% niestandardowe tagi klienta
%% - Użyj %%, aby skomentować wszelkie kroki, które nie są wymagane ze względu na konkretne
wdrożenie
%% Wymagania serwisowe:
%% Krok 1 -- tylko w przypadku nowych wdrożeń utwórz etykietę początkowego zestawu tagów
%% Krok 2 -- dodaj nowy tag niestandardowy (wpis jest wymagany dla każdego nowego tagu)
%% Krok 3 -- ustaw wartość dla istniejącego tagu niestandardowego (wpis wymagany dla każdego
odpowiedniego tagu)
%% Krok 4 -- wyświetlanie i wizualna weryfikacja ustawień tagów
%%
%% - Edytuj, modyfikuj plik zgodnie z potrzebami z uwzględnieniem składni poleceń. Zapisz plik (np.
WxT_Tags.txt)
%% - SFTP odczyt pliku do AS w katalogu /tmp
%% - Zaloguj się do AS, bwcli (zaloguj się jako admin)
%% - Wykonaj następujące polecenie z bwcli: AS_CLI> r /tmp/ WxT_Tags.txt
%% - Sprawdź wyniki
%%
%% ----------------------------------------------------------------------------------------------------------
%% Krok 1: Utwórz etykietę zestawu tagów Connect - Connect_Tags
%% ----------------------------------------------------------------------------------------------------------
rzucić wszystko; System; DeviceTagSet
Dodaj Connect_Tags
%% ----------------------------------------------------------------------------------------------------------
%% Krok 2: Dodaj WxT dla niestandardowych tagów BWKS
%% PRZYKŁAD – dla wszystkich tagów mobilnych zobacz poniższą listę-----------------------------------
-----------------
rzucić wszystko; System; DeviceTagSet; Tagi
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% true
%% ----------------------------------------------------------------------------------------------------------
%% Krok 3: Ustaw niestandardowe tagi Connect (jeśli tag już istnieje)
%% PRZYKŁAD – dla wszystkich tagów mobilnych zobacz poniższą listę
```


Poufne informacje Cisco

```
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------------------------------------------------------------------------------------------------------------
%% Krok 4: Sprawdź, czy niestandardowe tagi zostały poprawnie zdefiniowane i ustawione
%% ----------------------------------------------------------------------------------------------------------------
rzucić wszystko; System; DeviceTagSet; Tagi
get tagSetName Connect_Tags
Zamknij wszystko
```

Poniżej wymieniono wszystkie tagi niestandardowe używane przez Webex dla Cisco BroadWorks, na przykład wartości (domyślne lub zalecane). Należy zauważyć, że niektóre tagi wymagają wartości specyficznych dla danego wdrożenia (np. adresy serwerów). Dlatego znaczniki te są dodawane na końcu skryptu, ale pozostawione puste, i należy dodać dodatkowe polecenia zestawu, aby je określić.

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% pełny
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
```


Poufne informacje Cisco

```
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
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
```


Poufne informacje Cisco

```
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
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_CALL_CENTER_AGENT_OUTGOING_CALLS_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% rozwiązany
add tagSetName BroadTouch_tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```


Poufne informacje Cisco

10.2 Komórkowy

```
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
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
```


Poufne informacje Cisco

```
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
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% zajęty
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
```


Poufne informacje Cisco

```
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
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% rozwiązany
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% pełny
add tagSetName ConnectTablet_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
```


Poufne informacje Cisco

```
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
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
```


Poufne informacje Cisco

```
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
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% zajęty
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
```


Poufne informacje Cisco

```
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
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% rozwiązany
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 Tagi systemowe

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

```
%BWNETWORK-KONFERENCJA-SIPURI-n%
%BWVOICE-PORTAL-NUMBER-n%
%BWLINEPORT-n%
%BWHOST-n%
%BWAUTHUSER-n%
```


Poufne informacje Cisco

%BWAUTHPASSWORD-n%
%BWE164-n%
%BWNAME-n%
%BWEXTENSION-n%
%BWAPPEARANCE-LABEL-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMARY%
%BWE911-GŁÓWNY-HELDURL%
%BWE911-CUSTOMERID%
%BWE911-SECRETKEY%
%BWE911-LISTA-NUMERÓW-ALARMOWYCH%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%

Poufne informacje Cisco

11 Akronimy i skróty

W tej sekcji wymieniono akronimy i skróty występujące w tym dokumencie. Akronimy i skróty są wymienione w kolejności alfabetycznej wraz z ich znaczeniem.

ACB	Automatyczne oddzwanianie
ACD	Automatyczna dystrybucja połączeń
Protokół ACR	Anonimowe odrzucanie połączeń
AES	Zaawansowany standard szyfrowania (ang. Advanced Encryption Standard)
ALG	Brama warstwy aplikacji
API	Interfejs programowania aplikacji
APK	Pakiet aplikacji
APNS	Usługa powiadomień push firmy Apple
ARS	Automatyczny wybór szybkości transmisji bitów
GDY	Serwer aplikacji (Cisco BroadWorks)
AVP	Profil audiowizualny
BW	BroadWorks
BWA	BroadWorks w dowolnym miejscu
BWKS	BroadWorks
BWM	Mobilność BroadWorks
BYOD	Przynieś własne urządzenie
CC	Call center
CFB	Przekierowywanie połączeń zajęte
Życiorys	Przekierowywanie połączeń Brak odpowiedzi
CFNR	Przekierowywanie połączeń jest nieosiągalne
CIF	Wspólny format pośredni
CLI	Interfejs wiersza poleceń
CLID	Tożsamość linii wywołującej
CLIDB	Blokowanie dostarczania identyfikatora linii wywołującej
CRLF	Posuw linii powrotnej karetki
CS	Przełączanie obwodów
CSWV	Widok sieci Web ustawień połączeń
CW	Połączenie oczekujące
DB	Baza danych
DECYMETR	Zarządzanie urządzeniami
NPrzszk	Nie przeszkadzać
DNS	DNS (system nazw domenowych)

Poufne informacje Cisco

DPC	Sterowanie telefonem biurkowym
DTAF	Plik archiwum typu urządzenia
ECACS	Usługa zmiany adresu połączenia alarmowego
FMC	Konwergencja telefonii stacjonarnej i komórkowej
FQDN	W pełni kwalifikowana nazwa domeny
HMAC	Kod uwierzytelniania wiadomości skrótu
ICE	Ustanowienie interaktywnej łączności
iLBC	Internetowy kodek Low Bitrate Codec
IM	Wiadomości błyskawiczne
IM&P	Wiadomości błyskawiczne i obecność
IOT	Testowanie interoperacyjności
IP	Protokół IP
JID	Identyfikator Jabbera
M/O	Obowiązkowe/opcjonalne
MNO	Operator sieci komórkowej
MTU	Maksymalna jednostka transmisyjna
MUC	Czat dla wielu użytkowników
MWI	Wskaźnik wiadomości oczekującej
NAL	Warstwa abstrakcji sieci
NAPTR	Wskaźnik organu nazewnictwa
NAT	Translacja adresów sieciowych
OTT	Przesada
TATUŚ	Osobisty asystent
PAI	P-Asserted-Identity
PEM	P-Early Media
PLI	Wskaźnik utraty obrazu
PLMN	Publiczna lądowa sieć komórkowa
PN	Powiadomienia push
QCIF	Kwartalny wspólny format pośredni
QoS	Quality of Service
RO	Zdalne biuro
RTCP	Protokół sterowania w czasie rzeczywistym
RTP	Real Time Protocol
SaaS	Oprogramowanie jako usługa
SAN	Alternatywna nazwa podmiotu
SASL	Proste uwierzytelnianie i warstwa bezpieczeństwa

Poufne informacje Cisco

SAVP	Bezpieczny profil audio i wideo
SBC	Kontroler brzegowy sesji
SCA	Wygląd połączenia udostępnionego
SCF	Funkcja ciągłości sesji
SCTP	Protokół transmisji sterowania strumieniem
SDP	Protokół definicji sesji
SEQRING	Pierścień sekwencyjny
SIMRING	Jednoczesny dzwonek
SIP	Session Initiation Protocol, protokół SIP
SNR	Stosunek sygnału do szumu
SNR	Single Number Reach
Protokół SRTCP	Bezpieczny protokół sterowania w czasie rzeczywistym
SRTP	Bezpieczny protokół transportu w czasie rzeczywistym
SSL	Bezpieczna warstwa gniazd
STUN	Narzędzia do przechodzenia sesji dla translatora adresów sieciowych
SUBQCIF	Sub kwartał CIF
TCP	TCP
TLS	Transport Layer Security
TTL	Czas na życie
TURN	Przechodzenie przy użyciu translacji adresów sieciowych przekaźnika
UDP	Protokół UDP (User Datagram Protocol)
IU	Interfejs użytkownika
UMS	Serwer wiadomości (Cisco BroadWorks)
URI	Identyfikator URI (Uniform Resource Identifier)
UVS	Serwer wideo (Cisco BroadWorks)
VGA	Tablica grafiki wideo
VoIP	Lektor Over IP
VVM	Wizualna poczta głosowa
WXT	Webex
XMPP	Extensible Messaging and Presence Protocol
XR	Raport rozszerzony
Xsp	Platforma usług Xtended
Xsi	Interfejs usług Xtended

Poufne informacje Cisco