# Webex für Cisco Broadworks – Konfigurationsleitfaden

Freigeben 44.7

Dokumentversion 1

## Inhaltsverzeichnis


**1 Zusammenfassung der Änderungen ..... 1**
1.1 Änderungen für Version 44.7, Juli 2024 ..... 1
1.2 Änderungen für Version 44.6, Juni 2024 ..... 1
1.3 Änderungen für Version 44.5, Mai 2024 ..... 1
1.4 Änderungen für Version 44.4, April 2024 ..... 1
1.5 Änderungen für Version 44.3, März 2024 ..... 1
1.6 Änderungen für Version 44.2, Februar 2024 ..... 1
1.7 Änderungen für Version 43.1, Januar 2024 ..... 2
1.8 Änderungen für Version 43.12, Dezember 2023 ..... 2
1.9 Änderungen für Version 43.11, November 2023 ..... 2
1.10 Änderungen für Version 43.10, Oktober 2023 ..... 2
1.11 Änderungen für Version 43.9, September 2023 ..... 3
1.12 Änderungen für Version 43.8, August 2023 ..... 3
1.13 Änderungen für Version 43.7, Juli 2023 ..... 3
1.14 Änderungen für Version 43.6, Juni 2023 ..... 3
1.15 Änderungen für Version 43.5, Mai 2023 ..... 3
1.16 Änderungen für Version 43.4, April 2023 ..... 3
1.17 Änderungen für Version 43.3, März 2023 ..... 4
1.18 Änderungen für Version 43.2, Februar 2023 ..... 4
1.19 Änderungen für Version 43.1, Januar 2023 ..... 4
**2 Änderungen für Konfigurationsdateien ..... 5**
2.1 Änderungen für Konfigurationsdateien für Version 44.7 ..... 5
2.2 Änderungen für Konfigurationsdateien für Version 44.6 ..... 5
2.3 Änderungen für Konfigurationsdateien für Version 44.5 ..... 5
2.4 Änderungen für Konfigurationsdateien für Version 44.4 ..... 6
2.5 Änderungen für Konfigurationsdateien für Version 44.3 ..... 6
2.6 Änderungen für Konfigurationsdateien in Version 44.2 ..... 7
2.7 Änderungen für Konfigurationsdateien für Version 44.1 ..... 8
2.8 Änderungen für Konfigurationsdateien für Version 43. 1 2 ..... 8
2.9 Änderungen für Konfigurationsdateien für Version 43. 1 1 ..... 10
2.10 Änderungen für Konfigurationsdateien für Version 43. 10 ..... 10
2.11 Änderungen für Konfigurationsdateien in Version 43.9 ..... 10
2.12 Änderungen für Konfigurationsdateien in Version 43.8 ..... 11
2.13 Änderungen für Konfigurationsdateien in Version 43.7 ..... 11
2.14 Änderungen für Konfigurationsdateien in Version 43. 6 ..... 11
2.15 Änderungen für Konfigurationsdateien in Version 43.5 ..... 11
2.16 Änderungen für Konfigurationsdateien in Version 43.4 ..... 12
2.17 Änderungen für Konfigurationsdateien in Version 43.3 ..... 13
2.18 Änderungen für Konfigurationsdateien in Version 43.2 ..... 13





Cisco – vertraulich

2.19 Änderungen für Konfigurationsdateien in Version 43.1 ... 14
**3 Einführung ... 15**
**4 Installation ... 16**
4.1 Lokalisierter Client-Download ... 16
4.2 Android-Client ... 16
4.3 iOS-Client ... 16
4.4 Desktop-Client ... 16
**5 Geräteverwaltung ... 18**
5.1 Gerätemanagement-Tags ... 18
5.2 Teilweise Match-Verbesserungen für die Auswahl des Gerätetyps ... 19
5.3 Client-Konfiguration ... 20
5.4 Bereitstellung von config-wxt.xml ... 20
5.5 Konfigurationsdatei (config-wxt.xml) ... 20
5.6 Systemstandard-Tags ... 21
5.7 Dynamische, integrierte System-Tags in Cisco BroadWorks ... 21
**6 Benutzerdefinierte Tags ... 24**
6.1 Allgemeine Funktionen ... 36
6.1.1 SIP-Servereinstellungen ... 36
6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll ... 39
6.1.3 3GPP SIP-Header für SRTP ... 41
6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen ... 42
6.1.5 Konfigurierbarer Zeitüberschreitung beim Öffnen der SIP-Steckdose ... 44
6.1.6 Dynamische SIP-Proxyerkennung ... 45
6.1.7 Bevorzugte Portnutzung für SIP ... 51
6.1.8 SIP Failover und Failback ... 51
6.1.9 SIP SUBCSRIBE und REGISTRIEREN Aktualisieren und SUBSCRIBE Wiederholen ... 56
6.1.10 P-zugeordnete URIs in REGISTER verwenden ... 57
6.1.11 SIP P-Early Media (PEM)-Header ... 57
6.1.12 Unterstützung für SIP-UPDATE ... 58
6.1.13 Ältere SIP-INFO-FIR ... 59
6.1.14 SIP rport Management für NAT Traversal ... 59
6.1.15 SIP-Sitzungs-ID ... 60
6.1.16 Ablehnungsverhalten eingehender Anrufe ... 60
6.1.17 Portbereich des Transportprotokolls in Echtzeit ... 61
6.1.18 ICE-Unterstützung (nur Webex Calling) ... 62
6.1.19 RTCP-MUX ... 62
6.1.20 Transfer ... 63
6.1.21 N-Wege-Konferenzanrufe und Teilnehmer ... 64
6.1.22 Anrufübergabe ... 65
6.1.23 Anruf parken/abrufen ... 65



Cisco – vertraulich

6.1.24 Anrufstatistik ... 66
6.1.25 Automatische Anrufwiederherstellung / Nahtlose Anrufübergabe ... 67
6.1.26 Anrufaufzeichnung ... 67
6.1.27 Voicemail , Visuelle Voicemail, Briefkastenlampe ... 68
6.1.28 Voicemail-Transkription für Webex Calling ... 70
6.1.29 Anrufeinstellungen ... 71
6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen ... 73
6.1.31 Anmeldung/Abmeldung bei Callcenter/Anrufwarteschlange ... 77
6.1.32 XSI-Wurzel und -Pfade ... 78
6.1.33 XSI-Ereigniskanal ... 79
6.1.34 Codec-Konfiguration ... 79
6.1.35 SIP-URI-Wahl ... 82
6.1.36 Anrufprotokoll auf allen Geräten ... 82
6.1.37 Videoanrufe deaktivieren ... 83
6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter ... 84
6.1.39 PAI als Identität ... 85
6.1.40 Bildschirmfreigabe deaktivieren ... 86
6.1.41 Anzeige von Spam-Anrufen ... 86
6.1.42 Geräuschunterdrückung und Bandbreitenerweiterung für PSTN/Mobile-Anrufe ... 86
6.1.43 QoS DSCP-Markierung ... 87
6.1.44 Primäres Profil ... 88
6.1.45 Sperrliste (nur Webex Calling) ... 89
6.1.46 Medienanpassung und Resilienzimplementierung (MARI) ... 90
6.1.47 Gleichzeitige Anrufe mit demselben Benutzer ... 92
6.1.48 RTCP-XR ... 93
6.1.49 Informationen zur Anrufweiterleitung ... 93
6.1.50 Anrufer-ID ... 94
6.2 Nur Desktop-Funktionen ... 97
6.2.1 Erzwungene Abmeldung ... 97
6.2.2 Anrufübernahme ... 98
6.2.3 Unterstützung von Chef-Administratoren (Führungskraft-Assistent) ... 98
6.2.4 Eskalieren von SIP-Anrufen an Meeting (nur Webex Calling) ... 99
6.2.5 Anrufe über das Tischtelefon steuern – Automatische Anrufannahme ... 99
6.2.6 Automatische Anrufannahme mit Tonbenachrichtigung ... 100
6.2.7 Steuerung des Tischtelefons – Steuerung mittlerer Anrufe – Konferenz ... 100
6.2.8 Benachrichtigungen zur Anrufübernahme ... 101
6.2.9 Remote-Event-Paket ... 103
6.2.10 CLID-Auswahl des Agenten für Anrufwarteschlange ... 104
6.2.11 Survivability Gateway (nur Webex Calling) ... 104
6.2.12 Mehrere Leitungen – Darstellung gemeinsam genutzter Leitungen ... 105
6.2.13 Mehrere Leitungen – Virtuelle Leitungen (nur Webex Calling) ... 106
6.2.14 Remote-Stummschaltungssteuerungs-Event-Paket (nur Webex Calling) ... 106



Cisco – vertraulich

6.2.15 Anruf verschieben ..... 107
6.3 Funktionen nur für Mobilgeräte ..... 109
6.3.1 Notrufe ..... 109
6.3.2 Push-Benachrichtigungen für Anrufe ..... 110
6.3.3 Einzelne Benachrichtigung ..... 112
6.3.4 Zum Wählen klicken (Rückruf ) ..... 113
6.3.5 MNO-Unterstützung ..... 113
6.3.6 Anrufer-ID für eingehenden Anruf ..... 119
**7 Funktionen für Early Field Trial (BETA) ..... 121**
7.1 KI-Codec ..... 121
**8 Benutzerdefinierte Tags-Zuordnung zwischen Webex für Cisco BroadWorks und UC-One ..... 122**
**9 Anhang A: TLS-Schlüssel ..... 129**
**10 Anhang B: Skript für die Bereitstellung des DM-Tags ..... 130**
10.1 Desktop ..... 131
10.2 Mobil ..... 134
10.3 Tablet ..... 137
10.4 Systemkennzeichnungen ..... 140
**11 Abkürzungen und Abkürzungen ..... 141**



Cisco – vertraulich

# 1 Zusammenfassung der Änderungen

Dieser Abschnitt beschreibt die Änderungen an diesem Dokument für jede Version und Dokumentversion.

## 1.1 Änderungen für Version 44.7, Juli 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *KI-Codec* in BETA hinzugefügt.
- Abschnitt *6.1.44 Primary Profile* – Details zum Verhalten der Webex-App wurden von vornherein in Version 43.2 entfernt.

## 1.2 Änderungen für Version 44.6, Juni 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.3.6. Anrufer-ID für eingehenden* Anruf – weitere Details zur nativen Erfahrung und zum Funktionieren der Funktion hinzugefügt

## 1.3 Änderungen für Version 44.5, Mai 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.18ICE-Unterstützung (nur Webex Calling)*– IPv6-Unterstützung über NAT64 hinzugefügt.
- Aktualisierter Abschnitt *6.1.50Anrufer-ID* – Unterabschnitt hinzugefügt *6.1.50.2Name der Remote-Anrufer-ID*.

## 1.4 Änderungen für Version 44.4, April 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.50.1Ausgehende Anrufer-ID (nur Webex Calling)*.
- Aktualisierter Abschnitt *Änderungen für Konfigurationsdateien für Version 44.3* – Details zu den Keepalive-Aktualisierungen in 44.3.

## 1.5 Änderungen für Version 44.3, März 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.3.6. Anrufer-ID für eingehenden* Anruf
  - Der Abschnitt *6.1.50.1Ausgehende Anrufer-ID (nur Webex Calling)* wurde wie üblich für Desktop und Mobilgeräte verschoben und mit weiteren Details aktualisiert.
- Aktualisierter Abschnitt *6.1.4TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen* – Details zu den konfigurierbaren Keepalives mit benutzerdefinierten Tags hinzugefügt.

## 1.6 Änderungen für Version 44.2, Februar 2024

Diese Version des Dokuments enthält die folgenden Änderungen:



Cisco – vertraulich

- Abschnitt *6.3.6Anrufer-ID für eingehenden* Anruf mit Unterabschnitten hinzugefügt:
  - 6.3.6.1 ID des eingehenden Anrufers
  - 6.3.6.2 Ausgehende Anrufer-ID (nur Webex Calling)
- Aktualisierter Abschnitt *6.2.8 Benachrichtigungen zur Anrufübernahme*
  - Unterabschnitt *6.2.8.1Besetztlampenfeld* wurde hinzugefügt – BLF-Angaben wurden darin verschoben.
  - Unterabschnitt *6.2.8.2Anrufübernahmegruppe (nur Webex Calling)* hinzugefügt.
- Abschnitt *6.1.49Informationen zur Anrufweiterleitung* hinzugefügt.
- Aktualisierter Abschnitt *6.1.8.3IP-Version erzwingen* – Details für den neuen *nat64 - Modus* hinzugefügt.
- Aktualisierter Abschnitt *6.1.42Geräuschunterdrückung und Bandbreitenerweiterung für PSTN/Mobile-Anrufe* – Details für die Unterstützung der neuen Bandbreitenerweiterung und die Aktualisierungen zur Geräuschunterdrückung hinzugefügt. Abschnitt *Sprachverbesserungen für PSTN-Anrufe* wurde aus BETA entfernt.

## 1.7 Änderungen für Version 43.1, Januar 2024

An diesem Dokument für diese Version wurden keine Änderungen vorgenommen.

## 1.8 Änderungen für Version 43.12, Dezember 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.1SIP-Servereinstellungen* – Das Beispiel wurde aktualisiert (Domäne und externe ID pro Leitung hinzugefügt).
- Abschnitt *6.2.15 hinzugefügt Anruf verschieben*.
- Aktualisierter Abschnitt *6.3.5.1Anruf mit nativem Wählprogramm* – Details zur konfigurierbaren Präfixunterstützung für ausgehende Mobilfunkanrufe hinzugefügt.
- Aktualisierter Abschnitt *6.1.20Transfer* – Details zur neuen Option für das automatische Halten hinzugefügt.
- Abschnitt *6.1.48RTCP-XR* hinzugefügt.
- Abschnitt *Sprachverbesserungen für PSTN-Anrufe* in BETA hinzugefügt.

## 1.9 Änderungen für Version 43.11, November 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.8.1SIP-Failover* – Details zur Bereinigung der Registrierung und Aktualisierungen des q-Werts hinzugefügt.

## 1.10 Änderungen für Version 43.10, Oktober 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.29.2 Rufumleitung an Voicemail* aus BETA verschoben.



Cisco – vertraulich

- Aktualisierter Abschnitt *6.3.5.2Anrufsteuerungen*– Details zur Weiterleitung mit Rücksprache und Weiterleitung an einen anderen laufenden Anruf hinzugefügt.
- Aktualisierter Abschnitt *6.3.5.6MNO-Mobilität – Widget in Anrufen* – Details zur vollständigen Übergabe hinzugefügt.

## 1.11 Änderungen für Version 43.9, September 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.47Gleichzeitige Anrufe mit demselben Benutzer* aus BETA verschoben.
- Aktualisierter Abschnitt *6.1.20Transfer* – Details zur Übergabe an einen laufenden Anruf hinzugefügt.
- Abschnitt hinzugefügt *6.2.14*
- *Remote-Stummschaltungssteuerungs-Event-Paket (nur Webex Calling)*.
- Abschnitt *Rufumleitung an Voicemail* in BETA hinzugefügt.

## 1.12 Änderungen für Version 43.8, August 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *Gleichzeitige Anrufe mit demselben Benutzer* in BETA hinzugefügt.

## 1.13 Änderungen für Version 43.7, Juli 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.3.5.6MNO-Mobilität – Widget in Anrufen* aus BETA verschoben .

## 1.14 Änderungen für Version 43.6, Juni 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.46Medienanpassung und Resilienzimplementierung (MARI)* aus BETA verschoben .
- Abschnitt *MNO-Mobilität – Widget in Anrufen* in BETA hinzugefügt.
- Aktualisierter Abschnitt *5.4Bereitstellung von config-wxt.xml* – Empfehlung hinzugefügt, um die Konfigurationsvorlage mit der neuesten Version der Webex-Anwendung auf dem neuesten Stand zu halten.

## 1.15 Änderungen für Version 43.5, Mai 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.45Sperrliste (nur Webex Calling)* hinzugefügt.
- Aktualisierter Abschnitt *6.1.44 Primäres Profil* .

## 1.16 Änderungen für Version 43.4, April 2023

Diese Version des Dokuments enthält die folgenden Änderungen:



Cisco – vertraulich

- Aktualisierter Abschnitt *6.2.8Benachrichtigungen zur Anrufübernahme*. Benachrichtigungen zur Anrufübernahme
- Abschnitt *6.2.13Mehrere Leitungen – Virtuelle Leitungen (nur Webex* Calling) hinzugefügt.
- Abschnitt *Medienanpassung und Resilienzimplementierung (MARI)* in BETA .

## 1.17 Änderungen für Version 43.3, März 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.44 Primäres Profil  hinzugefügt.*
- Aktualisierter Abschnitt *6.2.12*
- *Mehrere Leitungen –* Darstellung gemeinsam genutzter Leitungen.

## 1.18 Änderungen für Version 43.2, Februar 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.2.12*
- *Mehrere Leitungen –* Darstellung gemeinsam genutzter Leitungen.
- Hinzugefügt *6.2.11Survivability Gateway (nur Webex Calling)*.
- Aktualisierter Abschnitt *6.1.4TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen*.

## 1.19 Änderungen für Version 43.1, Januar 2023

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.2.12*
- *Mehrere Leitungen –* Darstellung gemeinsam genutzter Leitungen.



Cisco – vertraulich

# 2 Änderungen für Konfigurationsdateien

## 2.1 Änderungen für Konfigurationsdateien für Version 44.7

- [BETA-Funktion] AI-Codec (xCodec) im Abschnitt hinzugefügt <services><calls><audio><codecs>.

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

## 2.2 Änderungen für Konfigurationsdateien für Version 44.6

In den Konfigurationsdateien für diese Version gab es keine Aktualisierungen.

## 2.3 Änderungen für Konfigurationsdateien für Version 44.5

- [Nur Webex Calling]
  Attribut „enable-ipv6-support“ zum Tag <protocols><rtp><ice> hinzugefügt.

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

- Das Tag <remote-name> wurde im Abschnitt <services><calls><caller-id> mit <machine> als Untertag hinzugefügt.

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

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%



Cisco – vertraulich

## 2.4 Änderungen für Konfigurationsdateien für Version 44.4

- [Nur Desktop] [Nur Webex Calling]
  Tags <additional-numbers>, <Sammelanschluss> und < clid-delivery-blocking> im Abschnitt <caller-id><outgoing-calls> hinzugefügt.

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

## 2.5 Änderungen für Konfigurationsdateien für Version 44.3

- [Nur Desktop] [Nur Webex Calling]
  <ausgehend-Anrufe> wurde im neuen Abschnitt <caller-id> hinzugefügt, mit < call-center> als Untertag.

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

- Benutzerdefinierte Tags (%UDP_KEEPALIVE_ENABLED_WXT%,%TCP_KEEPALIVE_ENABLED_WXT% hinzugefügt und %TLS_KEEPALIVE_ENABLED_WXT%) den hartcodierten Keep-Alive-Aktivierungswert für jeden Transport unter <protocols><sip><transports> ersetzt.

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

Die folgenden %TAG%s wurden hinzugefügt:



Cisco – vertraulich

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

## 2.6 Änderungen für Konfigurationsdateien in Version 44.2

- [Nur für Mobilgeräte]
  Abschnitt <caller-id> unter <services><calls> hinzugefügt. Die Untertagungen <eingehender Anruf> und <Anruf in Abwesenheit> wurden hinzugefügt, mit dem neuen Untertag <hinzugefügte Nummer> für beide.

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

- [Nur für Mobilgeräte] [Nur für Webex Calling]
  <ausgehend-Anrufe> wurde im neuen Abschnitt <caller-id> hinzugefügt.

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

- Tag <call-forwarding-info> im Abschnitt <services><calls> hinzugefügt.

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

- [Nur Desktop] [Nur Webex Calling]
  Abschnitt <group-call-pickup-notifications> unter <services><calls> hinzugefügt, mit <display-caller> und <max-timeout> als Untertags. Außerdem <group-call-pickup> Tag unter jedem <line> Tag im <protocols><sip><lines> Abschnitt hinzugefügt.

```
<config>
<services><calls>
  <group-call-pickup-notifications
enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
    <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
    <max-timeout value="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
  </group-call-pickup-notifications>
  …
```



Cisco – vertraulich

```
<protocols><sip>
  <lines>
    <line>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
      ...
    </line>
    <line>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>
      ...
    </line>
    …
```

Die folgenden %TAG%s wurden hinzugefügt:

- %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%

Die folgenden %TAG% wurden eingestellt:

- %ENABLE_NOISE_REMOVAL_WXT%

## 2.7 Änderungen für Konfigurationsdateien für Version 44.1

In den Konfigurationsdateien für diese Version gab es keine Aktualisierungen.

## 2.8 Änderungen für Konfigurationsdateien für Version 43. 1 2

- <domain>-Tag für jeden <line>-Abschnitt unter <config><protocols><sip>< lines >hinzugefügt.

```
<config>
<protocols><sip>
    <lines>
        <line>
            <domain>%BWHOST-1%</domain>
            ...
        </line>
        <line>
```



Cisco – vertraulich

```
            <domain>%BWHOST-2%</domain>
            ...
        </line>
        ...
```

- [Nur Desktop]
  Abschnitt <call-move> mit <move-here> Tag unter Abschnitt <config><services><calls> hinzugefügt.

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

- Tag <speech-enhements> unter Abschnitt <config><services><calls> hinzugefügt.

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

- [Nur für Mobilgeräte]
  <fac-prefix> Tag im Abschnitt <config><services><dialing><native> hinzugefügt.

```
<config>
<services>
  <dialing>
    <native enabled="%ENABLE_DIALING_NATIVE_WXT%" enable-bwks-mobility-
dependency="%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%">
      <fac-prefix value="%DIALING_NATIVE_FAC_PREFIX_WXT%"/>
```

- Attribut für automatische Halten im Tag <config><services><calls><transfer-call> hinzugefügt.

```
<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%"/>
```

- Abschnitt <rtcp-xr> unter <config><protocols><sip> hinzugefügt.

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

Die folgenden %TAG%s wurden hinzugefügt:

- %BWHOST-n%
- %ENABLE_CALL_MOVE_HERE_WXT%
- %ENABLE_SPEECH_ENHANCEMENTS_WXT%
- %DIALING_NATIVE_FAC_PREFIX_WXT%
- %ENABLE_TRANSFER_AUTO_HOLD_WXT%
- %ENABLE_RTCP_XR_NEGOTIATION_WXT%



Cisco – vertraulich

## 2.9 Änderungen für Konfigurationsdateien für Version 43. 1 1

- Neuer Abschnitt <register-failover> mit <registration-cleanup> als Untertag unter Abschnitt <config><protocols><sip> hinzugefügt. Das <q-value>-Tag wurde unter das <register-failover>-Tag verschoben.

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

Das folgende %TAG% wurde hinzugefügt:

- %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%

## 2.10 Änderungen für Konfigurationsdateien für Version 43. 10

In den Konfigurationsdateien für diese Version gab es keine Aktualisierungen.

## 2.11 Änderungen für Konfigurationsdateien in Version 43.9

- Hat das Tag <multiple-calls-per-user> im Abschnitt <config><services><calls> in < simultaneous-calls-with-same-user> umbenannt.

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

- Neues Tag <remote-mute-control> im Abschnitt <config><services><calls> hinzugefügt.

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

- Neues Tag <forwarding> im Abschnitt <config><services><voice-mail> hinzugefügt.

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

Das folgende %TAG% wurde aktualisiert:

- %ENABLE_MULTIPLE_CALLS_PER_USER_WXT% was renamed to %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_REMOTE_MUTE_CONTROL_WXT%
- %ENABLE_VOICE_MAIL_FORWARDING_WXT%



Cisco – vertraulich

## 2.12 Änderungen für Konfigurationsdateien in Version 43.8

- Neues Tag <multiple-calls-per-user> im Abschnitt <config><services><calls> hinzugefügt.

```
<config>
<services><calls>
<multiple-calls-per-user enabled="%ENABLE_MULTIPLE_CALLS_PER_USER_WXT%"/>
```

Das folgende %TAG% wurde hinzugefügt:

- %ENABLE_MULTIPLE_CALLS_PER_USER_WXT%

## 2.13 Änderungen für Konfigurationsdateien in Version 43.7

In den Konfigurationsdateien für diese Version gab es keine Aktualisierungen.

## 2.14 Änderungen für Konfigurationsdateien in Version 43. 6

- [Nur für Mobilgeräte]
  Neue Attribute in den Tags <Halten>, <Anruf übertragen> und <Eskalation zu Webex-Meeting> unter Abschnitt <config><services><calls> hinzugefügt

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

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_WIDGET_HOLD_CALLS_WXT%
- %ENABLE_WIDGET_TRANSFER_CALLS_WXT%
- %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%

## 2.15 Änderungen für Konfigurationsdateien in Version 43.5

- [Nur Webex Calling]
  <call block>-Tag im Abschnitt <config><services><calls> hinzugefügt

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

Das folgende %TAG% wurde hinzugefügt:

- %ENABLE_CALL_BLOCK_WXT%



Cisco – vertraulich

## 2.16 Änderungen für Konfigurationsdateien in Version 43.4

- [Nur Webex Calling]
  Für jedes hinzugefügte *Attribut lineType* <line>-Tag. Außerdem <external-id> Tag unter jedem <line> Tag hinzugefügt.

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

- Abschnitt <Audio-Qualitätsverbesserungen> unter <Dienste><Anrufe><Audio> und <Video-Qualitätsverbesserungen> unter <Dienste><Anrufe><Video> hinzugefügt

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



Cisco – vertraulich

```
                                    <max_n>255</max_n>
                                    <m>8</m>
                                    <multi_ssrc>1</multi_ssrc>
                                    <non_seq>1</non_seq>
                                    <feedback>0</feedback>
                                    <order>FEC_SRTP</order>
                              </fec>
                              <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                                    <mari-rtx>90000</mari-rtx>
                                    <payload>112</payload>
                                    <time>180</time>
                                    <data-flow>1</data-flow>
                                    <order>RTX_SRTP</order>
                              </rtx>
                              </mari>
                </video-quality-enhancements>
```

- [Nur Desktop]
  Hardcodierter Wert für den Namen der ersten Zeile unter dem entsprechenden Abschnitt <line> unter <protocols><sip> entfernt.

```
<config>
<protocols><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
   …
   <line>
       <label>%BWAPPEARANCE-LABEL-1%</label>
       …
```

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_AUDIO_MARI_FEC_WXT%
- %ENABLE_AUDIO_MARI_RTX_WXT%
- %ENABLE_VIDEO_MARI_FEC_WXT%
- %ENABLE_VIDEO_MARI_RTX_WXT%

Die folgende Systemebene %TAG%s wurde hinzugefügt:

- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%

## 2.17 Änderungen für Konfigurationsdateien in Version 43.3

In den Konfigurationsdateien für diese Version gab es keine Aktualisierungen.

## 2.18 Änderungen für Konfigurationsdateien in Version 43.2

Tag <device-owner-restriction> unter Abschnitt <services><calls> hinzugefügt.

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



Cisco – vertraulich

Das folgende %TAG% wurde hinzugefügt:

- %ENABLE_DEVICE_OWNER_RESTRICTION_WXT%

## 2.19 Änderungen für Konfigurationsdateien in Version 43.1

In den Konfigurationsdateien für diese Version gab es keine Aktualisierungen.



Cisco – vertraulich

# 3 Einführung

Zweck dieses Dokuments ist eine Beschreibung der Konfiguration des Webex für Cisco BroadWorks-Clients.

Die Konfigurationsdatei *config-wxt.xml* wird in zwei Versionen bereitgestellt – eine für Mobilgeräte (Android und iOS) und eine für Desktops (Windows und MacOS).

Die Clients werden mit einer Konfiguration konfiguriert, die für den Endbenutzer nicht sichtbar ist. Die *Datei config-wxt.xml* bietet serverspezifische Informationen wie Serveradressen und Ports und Laufzeitoptionen für den Client selbst (z. B. Optionen, die im Bildschirm *Settings* sichtbar sind).

Die Konfigurationsdateien werden vom Client gelesen, wenn sie gestartet werden, nachdem sie aus der Geräteverwaltung abgerufen wurden. Die Informationen aus den Konfigurationsdateien werden verschlüsselt gespeichert, sodass sie für den Endbenutzer unsichtbar und unzugänglich sind.

**HINWEIS:** Die XML-Eigenschaften sollten keine Leerzeichen enthalten (z. B. <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"/> anstelle von <transfer-call enabled = "%ENABLE_TRANSFER_CALLS_WXT%"/>).



Cisco – vertraulich

# 4 Installation

Die Webex für Cisco BroadWorks-Clients können wie folgt installiert werden:

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

## 4.1 Lokalisierter Client-Download

Die folgenden lokalisierten Versionen der Webex für Cisco BroadWorks-Clients können wie folgt heruntergeladen werden:

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 Android-Client

Der Android-Client wird als Anwendung installiert (Android-Anwendungspaket [APK]), das die Einstellungen- und Konfigurationsdaten in seinem privaten Bereich speichert.

Es gibt Versionskontrolle basierend auf den Google Play-Verfahren. Es wird eine standardmäßige Google Play-Benachrichtigung bereitgestellt (d. h. Android zeigt automatisch an, dass eine neue Version der Software verfügbar ist).

Wenn die neue Version heruntergeladen wird, wird die alte Software überschrieben; Benutzerdaten werden jedoch standardmäßig beibehalten.

Beachten Sie, dass der Benutzer keine Optionen für die Installation oder Deinstallation auswählen muss.

## 4.3 iOS-Client

Der iOS-Client wird als Anwendung installiert, die die einstellungsbezogenen Daten in ihrer „Sandbox“ speichert und die Konfigurationsdateidaten verschlüsselt speichert.

Es gibt Versionskontrolle basierend auf den Apple App Store-Verfahren. Das App Store-Symbol wird hervorgehoben, um anzuzeigen, dass eine neue Version der Software verfügbar ist.

Wenn die neue Version heruntergeladen wird, wird die alte Software überschrieben; Benutzerdaten werden jedoch standardmäßig beibehalten.

Beachten Sie, dass der Benutzer keine Optionen für die Installation oder Deinstallation auswählen muss.

## 4.4 Desktop-Client

Informationen zur Installation und Versionskontrolle des Desktop-Clients (Windows und MacOS) finden Sie auf der folgenden Seite: https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade .



Cisco – vertraulich

Cisco – vertraulich

# 5 Geräteverwaltung

## 5.1 Gerätemanagement-Tags

Webex für Cisco BroadWorks verwendet die *Geräte-Management-Tag-Sets* wie in der folgenden Abbildung dargestellt. Die *Systemstandardeinstellungen* und benutzerdefinierte Tag-Sets sind erforderlich, um bestimmte Geräte-/Client-Einstellungen bereitzustellen. Dieser Tag-Satz bietet Flexibilität bei der Verwaltung der Netzwerk-/Dienstkonnektivitätseinstellungen des Clients sowie Funktionsaktivierungssteuerungen.

Dieser benutzerdefinierte Tag-Satz wird von einem Systemadministrator über die Option *System → Ressourcen → Geräte-Management-Tag-Sätze* bereitgestellt. Der Administrator muss neue Tag-Sets hinzufügen:

- Mobil: Connect_Tags
- Tablet: ConnectTablet_Tags
- Desktop: BroadTouch_Tags

Erstellen Sie jedes einzelne Tag und legen Sie seinen Wert fest. Sektionsreferenzen enthalten detaillierte Beschreibungen für jedes Tag. Die benutzerdefinierten Tags werden basierend auf der Funktionalität in Gruppen getrennt und später in diesem Dokument besprochen.

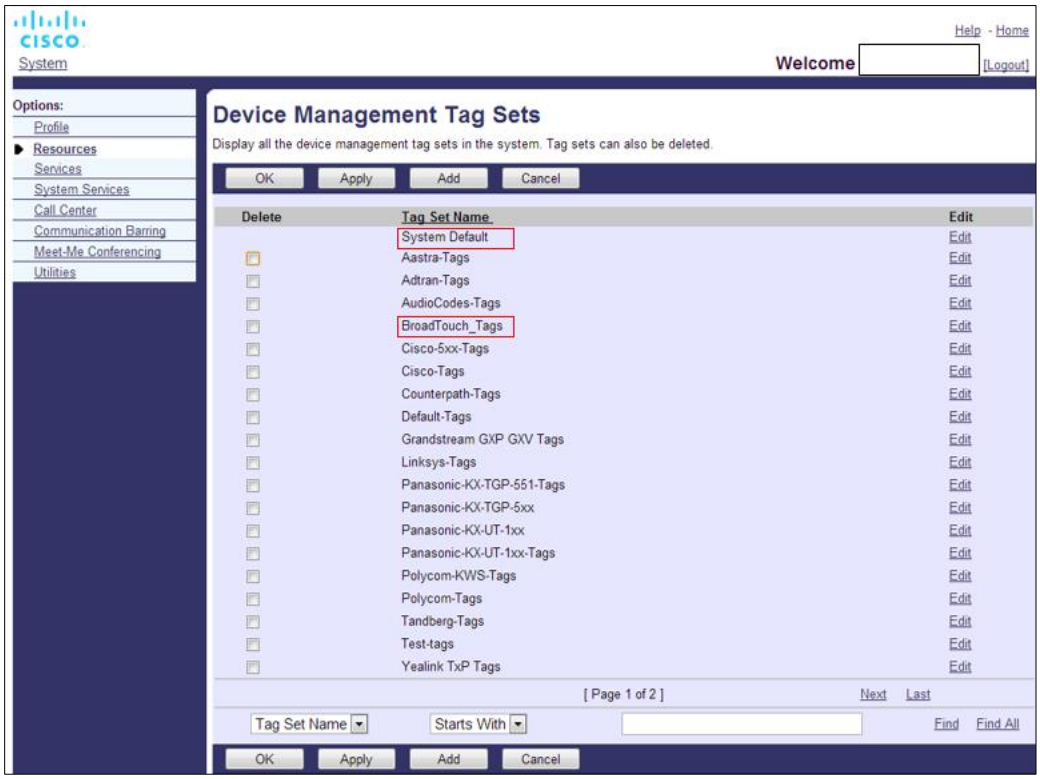



Abbildung 1 Desktop-Geräteverwaltungs-Tag-Sets



Cisco – vertraulich

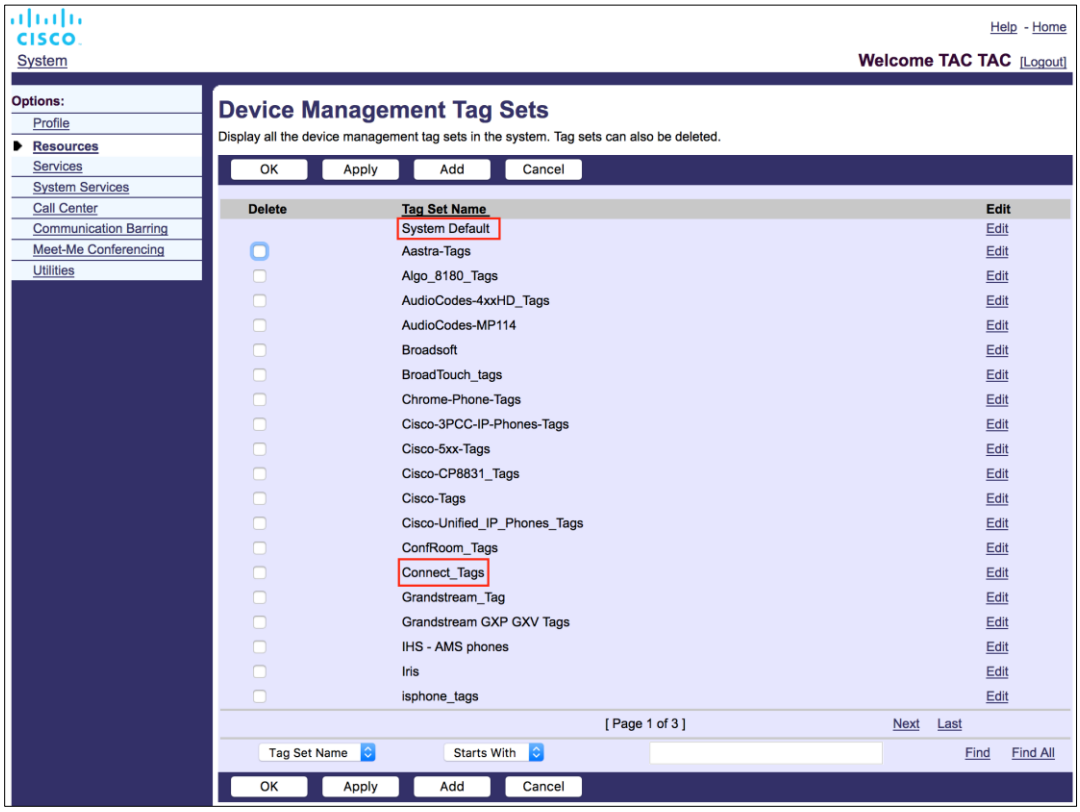



Abbildung 2: Tag-Sets für die Verwaltung mobiler Geräte

## 5.2 Teilweise Match-Verbesserungen für die Auswahl des Gerätetyps

Um eine größere Flexibilität bei der Auswahl von Funktionspaketen für Benutzergruppen oder einzelne Benutzer zu ermöglichen, wird der Geräteprofiltyp basierend auf einer (ersten) teilweisen Übereinstimmung ausgewählt. Auf diese Weise können Kunden verschiedene Gerätetypen verwenden.

Das allgemeine Verfahren für die Geräteverwaltung legt fest, dass der Cisco BroadWorks-Anwendungsserver einen Geräteprofiltyp bereitstellt. Er trägt den Namen „Business Communicator – PC“ für Desktop, „Connect – Mobile“ für Mobilgeräte und „Connect – Tablet“ für Tablets. Ein Geräteprofil kann erstellt und dem Benutzer zugewiesen werden. Der Anwendungsserver erstellt dann eine Konfigurationsdatei und speichert sie auf dem Profilserver.

Bei der Anmeldung fragt der Client über Xsi die zugewiesene Geräteliste ab und sucht nach dem entsprechenden Gerätetypprofil. Der Client wählt das erste Profil aus, das mit dem entsprechenden Gerätetypnamen beginnt. Anschließend werden die mit diesem Geräteprofil verknüpften Geräteprofilkonfigurationsdaten (Konfigurationsdatei) verwendet, um verschiedene Funktionen zu aktivieren und zu deaktivieren.

Dies ermöglicht die Verwendung derselben ausführbaren Client-Datei mit verschiedenen Geräteprofiltypen, sodass der Serviceanbieter Funktionspakete für einzelne Benutzer oder Benutzergruppen ändern kann, indem er einfach den Geräteprofiltyp in DM für einen Benutzer oder eine Benutzergruppe ändert.



Cisco – vertraulich

Beispielsweise könnte der Serviceanbieter eine beliebige Anzahl von Geräteprofiltypen basierend auf Benutzerrollen haben, z. B. „Business Communicator – PC Basic“, „Business Communicator – PC Executive“ oder „Business Communicator – PC Assistant“, und die für einzelne Benutzer verfügbare Funktionalität ändern, indem er den Geräteprofiltyp für sie ändert.

Beachten Sie, dass in der XML der empfangenen Geräteliste nicht mehrere übereinstimmende Geräteprofiltypen erwartet werden, sondern nur einer.

## 5.3 Client-Konfiguration

Die Webex für Cisco BroadWorks-Version des Clients verwendet die Datei *config-wxt.xml* für die Konfiguration der Anruffunktionen. Es gibt ein separates Konfigurationsverfahren für Webex, das in diesem Dokument nicht behandelt wird.

## 5.4 Bereitstellung von config-wxt.xml

Fügen Sie die entsprechende Datei *config-wxt.xml* zu den Geräteprofilen „Connect – Mobile“, „Connect – Tablet“ und „Business Communicator – PC“ hinzu. Webex für Cisco BroadWorks verwendet dieselben Geräteprofile wie UC-One, um die Bereitstellung zu vereinfachen.

**ANMERKUNG 1 <UNK>** : Für jedes Geräteprofil muss eine Konfigurationsdatei vorhanden sein.

**ANMERKUNG 2 <UNK>** : Es wird HIER EMPFOHLEN, die Vorlagen mit der neuesten Version der Webex-App auf dem neuesten Stand zu halten

## 5.5 Konfigurationsdatei (config-wxt.xml)

Neue benutzerdefinierte Tags mit dem Suffix **_WXT** werden verwendet, um die neue Webex-Konfigurationsbereitstellung für Cisco BroadWorks von älteren Clients zu unterscheiden. Es gibt jedoch immer noch einige (System-) Tags, die zwischen UC-One und Webex geteilt werden.

Einige der benutzerdefinierten Tags für das Cisco BroadWorks-System werden auch in der Konfigurationsdatei *config-wxt.xml* verwendet. Weitere Informationen zu den folgenden Tags finden Sie im Abschnitt *5.7Dynamische, integrierte System-Tags* in Cisco BroadWorks.

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



Cisco – vertraulich

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

## 5.6 Systemstandard-Tags

Als Systemadministrator können Sie über die Option *System → Ressourcen → Geräte-Management-Tag-Sets* auf die Systemstandard-Tags zugreifen. Die folgenden Systemstandard-Tags müssen bereitgestellt werden, wenn das VoIP Calling-Paket installiert ist.

| Tag | Beschreibung |
|---|---|
| %SBC_ADDRESS_WXT% | Dies sollte als vollqualifizierter Domänenname (FQDN) oder IP-Adresse des Session Border Controller (SBC) konfiguriert werden, der im Netzwerk bereitgestellt wird.<br>Beispiel: sbc.yourdomain.com |
| %SBC_PORT_WXT% | Wenn SBC_ADDRESS_WXT eine IP-Adresse ist, sollte dieser Parameter auf den SBC-Port festgelegt werden.<br>Wenn SBC_ADDRESS_WXT ein FQDN ist, kann er nicht festgelegt werden.<br>Beispiel: 5075 |

## 5.7 Dynamische, integrierte System-Tags in Cisco BroadWorks

Zusätzlich zu den Standard-System-Tags und den benutzerdefinierten Tags, die definiert werden müssen, gibt es vorhandene Cisco BroadWorks-System-Tags, die normalerweise verwendet werden und Teil der empfohlenen Gerätetyp-Archivdatei (DTAF) sind. Diese Tags sind in diesem Abschnitt aufgeführt. Abhängig vom installierten Lösungspaket werden nicht alle System-Tags verwendet.

| Tag | Beschreibung |
|---|---|
| %BWNETWORK-CONFERENCE-SIPURI-n% | Dies ist der Server-URI, der zum Aktivieren von N-Way-Konferenzen verwendet wird. |
| %BWVOICE-PORTAL-NUMBER-n% | Diese Nummer wird für Voicemail verwendet. Der Client wählt diese Nummer beim Abrufen der Voicemail. |
| %BWLINEPORT-n% | In der SIP-Signalisierung verwendeter SIP-Benutzername, z. B. bei der Registrierung. |



Cisco – vertraulich

| Tag | Beschreibung |
|---|---|
| %BWHOST-n% | Dies ist der Domänenteil des bereitgestellten Leitungsports für das dem Benutzer zugewiesene Gerät. Sie wird aus dem Profil des Benutzers abgerufen.<br><br>Wird normalerweise als SIP-Domäne verwendet. |
| %BWAUTHUSER-n% | Dies ist der Benutzername für die Authentifizierung. Wenn dem Subscriber die Authentifizierung zugewiesen wurde, handelt es sich hierbei um die bereitgestellte Benutzer-ID auf der Authentifizierungsseite, unabhängig vom ausgewählten Authentifizierungsmodus des Gerätetyps.<br><br>Der SIP-Benutzername, der normalerweise bei der 401- und 407-Signalisierung verwendet wird. Kann vom Standard-SIP-Benutzernamen abweichen. |
| %BWAUTHPASSWORD-n% | Dies ist das Authentifizierungspasswort des Benutzers. Wenn dem Subscriber die Authentifizierung zugewiesen wurde, ist dies das bereitgestellte Kennwort auf der Authentifizierungsseite, unabhängig vom ausgewählten Authentifizierungsmodus-Wert des Gerätetyps.<br><br>Das in der SIP-Signalisierung verwendete SIP-Kennwort. |
| %BWE164-n% | Dieses Tag enthält die Telefonnummer des Benutzers im internationalen Format. |
| %BWNAME-n% | Dies ist der Vorname und Nachname des Subscribers im Profil des Benutzers. Die Vor- und Nachnamen werden miteinander verkettet.<br><br>Wenn bei der Konfiguration mit mehreren Leitungen keine Leitungsbezeichnung konfiguriert ist und wenn diese nicht leer ist, wird sie als Anzeigename für die Leitung in der Leitungsauswahl verwendet. |
| %BWEXTENSION-n% | Die Durchwahl des Subscribers wird von der im Profil des Benutzers bereitgestellten Durchwahl abgerufen. Wenn eine Durchwahl nicht bereitgestellt wurde, wird das Tag durch die Telefonnummer (DN) des Subscribers ersetzt. |
| %BWAPPEARANCE-LABEL-n% | Dies ist die konfigurierte Leitungsbezeichnung. Wird als Leitungsname verwendet, wenn er nicht leer ist. |
| %BWDISPLAYNAMELINEPORT% | Dies ist die Leitung/der Port der ersten privaten Leitung im Gegensatz zu einer gemeinsam genutzten Leitung (Gemeinsame Leitungsdarstellung).<br><br>Dies ist der Leitungsport, der auf dem dem Benutzer zugewiesenen Gerät bereitgestellt wird. Dieser wird aus dem Profil des Benutzers abgerufen.<br><br>Wird verwendet, um die Hauptleitung des Benutzers zu identifizieren. |



Cisco – vertraulich

| Tag | Beschreibung |
|---|---|
| %BWLINEPORT-PRIMARY% | Der primäre Leitungsport wird auf dem Gerät bereitgestellt, das dem Benutzer zugewiesen ist. Dieses Tag umfasst nicht den Domänenteil des bereitgestellten Leitungsports. Sie wird aus dem Profil des Benutzers abgerufen. |
| %BWE911-PRIMARY-HELDURL% | Gibt die URL zur RedSky Emergency Location Platform an, die das HELD-Protokoll unterstützt. |
| %BWE911-CUSTOMERID% | Die für die RedSky-HTTPS-Anforderung verwendete Kunden-ID (HeldOrgId, CompanyID). |
| %BWE911-SECRETKEY% | Das Geheimnis zur Authentifizierung der RedSky HTTPS-Anforderung. |
| %BWE911-EMERGENCY-NUMBER-LIST% | Die Liste der von RedSky unterstützten Notrufnummern.<br>Um dieses Tag zu verwenden, muss das reservierte, benutzerdefinierte Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% zum vom Gerätetyp verwendeten Tag hinzugefügt werden. Das Tag „Reserviert“ muss die Notrufnummern enthalten, die in BroadWorks unter AS_CLI/System/CallP/CallTypes > in einem kommagetrennten Format definiert sind, z. B. 911, 0911, 933.<br>**HINWEIS:** Der Webex-Client unterstützt keine Platzhalter in Notrufnummern. Daher sollten dem benutzerdefinierten Tag „Reserviert“ nur exakte Notrufnummern hinzugefügt werden.<br>Das folgende Beispiel zeigt, wie die Funktion für reservierte Tags verwendet werden soll:<br>1) Das native Tag %BWE911-EMERGENCY-NUMBER-LIST% wird zur Vorlagendatei des Geräts hinzugefügt.<br>2) Das reservierte benutzerdefinierte Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% wird zum vom Gerät verwendeten Tag mit dem Wert 911, 0911, 933 hinzugefügt.<br>3) Wenn die Datei neu erstellt wird, wird das native Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% auf 911, 0911, 933 aufgelöst. |
| %BW-MEMBERTYPE-n% | Dies ist der Typ für jede Leitung. Es kann sich um ein „virtuelles Profil“, einen „Benutzer“ oder einen „Ort“ handeln. |
| %BWUSEREXTID-n% | Dies ist die externe ID für eine bestimmte Leitung (nur Webex Calling) |
| %BWGROUP-CALL-PICKUP-BOOL-n%" | Gibt Informationen an, ob für die entsprechende Leitung eine Anrufübernahmegruppe konfiguriert ist. (Nur Webex Calling) |



Cisco – vertraulich

# 6 Benutzerdefinierte Tags

In diesem Abschnitt werden die in Webex für Cisco BroadWorks verwendeten benutzerdefinierten Tags beschrieben. Es listet alle benutzerdefinierten Tags auf, die für Desktop- und Mobile/Tablet-Plattformen verwendet werden.

Beachten Sie jedoch, dass einige in diesem Abschnitt beschriebene Einstellungen nur für die spezifische Version des Clients unterstützt werden. Informationen dazu, ob eine Einstellung nicht auf eine ältere Client-Version zutrifft, finden Sie im entsprechenden Release-spezifischen Konfigurationsleitfaden.

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %ENABLE_REJECT_WITH_486_WXT% | J | J | wahr | *6.1.16 Ablehnungsverhalten eingehender Anrufe* |
| %REJECT_WITH_XSI_MODE_WXT% | N | J | ablehnen_false | *6.3.2 Push-Benachrichtigungen für Anrufe* |
| %REJECT_WITH_XSI_DECLINE_REASON_WXT% | N | J | beschäftigt | *6.3.2 Push-Benachrichtigungen für Anrufe* |
| %ENABLE_TRANSFER_CALLS_WXT% | J | J | Falsch | *6.1.20 Transfer* |
| %ENABLE_CONFERENCE_CALLS_WXT% | J | J | Falsch | *6.1.21 N-Wege-Konferenzanrufe und Teilnehmer* |
| %ENABLE_NWAY_PARTICIPANT_LIST_WXT% | J | J | Falsch | *6.1.21 N-Wege-Konferenzanrufe und Teilnehmer* |
| %MAX_CONF_PARTIES_WXT% | J | J | 10 | *6.1.21 N-Wege-Konferenzanrufe und Teilnehmer* |
| %ENABLE_CALL_STATISTICS_WXT% | J | J | Falsch | *6.1.24 Anrufstatistik* |
| %ENABLE_CALL_PULL_WXT% | J | J | Falsch | *6.1.22 Anrufübergabe* |
| %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% | N | J | Falsch | *6.3.2 Push-Benachrichtigungen für Anrufe* |
| %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% | J | J | Falsch | *6.1.28 Voicemail-Transkription für Webex Calling* |
| %ENABLE_MWI_WXT% | J | J | Falsch | *6.1.27 Voicemail , Visuelle Voicemail, Briefkastenlampe* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %MWI_MODE_WXT% | J | J | leer | *6.1.27 Voicemail , Visuelle Voicemail, Briefkastenlampe* |
| %ENABLE_VOICE_MAIL_WXT% | J | J | Falsch | *6.1.27 Voicemail , Visuelle Voicemail, Briefkastenlampe* |
| %ENABLE_VISUAL_VOICE_MAIL_WXT% | J | J | Falsch | *6.1.27 Voicemail , Visuelle Voicemail, Briefkastenlampe* |
| %ENABLE_FORCED_LOGOUT_WXT% | J | N | Falsch | *6.2.1 Erzwungene* Abmeldung |
| %FORCED_LOGOUT_APPID_WXT% | J | N | leer | *6.2.1 Erzwungene* Abmeldung |
| %ENABLE_CALL_FORWARDING_ALWAYS_WXT% | J | J | Falsch | *6.1.29.1 Immer Rufumleitung* |
| %ENABLE_BROADWORKS_ANYWHERE_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% | J | J | wahr | *6.1.29.3 BroadWorks Anywhere* |
| %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% | J | J | Falsch | *6.1.29.3 BroadWorks Anywhere* |
| %ENABLE_EMERGENCY_DIALING_WXT% | N | J | Falsch | *6.3.1 Notrufe* |
| %EMERGENCY_DIALING_NUMBERS_WXT% | N | J | 911 <UNK> , <UNK> 11 <UNK> <UNK> 2 | *6.3.1 Notrufe* |
| %ENABLE_USE_RPORT_WXT% | J | J | Falsch | *6.1.14 SIP rport Management für NAT Traversal* |
| %RPORT_USE_LOCAL_PORT_WXT% | J | J | Falsch | *6.1.14 SIP rport Management für NAT Traversal* |
| %USE_TLS_WXT% | J | J | Falsch | *6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll* |
| %SBC_ADDRESS_WXT% | J | J | leer | *5.6 Systemstandard-Tags* |
| %SBC_PORT_WXT% | J | J | 5060 | *5.6 Systemstandard-Tags* |
| %USE_PROXY_DISCOVERY_WXT% | J | J | Falsch | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %USE_TCP_FROM_DNS_WXT% | J | J | wahr | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %USE_UDP_FROM_DNS_WXT% | J | J | wahr | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %USE_TLS_FROM_DNS_WXT% | J | J | wahr | *6.1.6 Dynamische SIP-Proxyerkennung* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %DOMAIN_OVERRIDE_WXT% | J | J | leer | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% | J | J | wahr | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% | J | J | wahr | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% | Y (nur Windows) | N | Falsch | *6.1.6 Dynamische SIP-Proxyerkennung* |
| %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% | J | J | 5000 | *6.1.5 Konfigurierbarer Zeitüberschreitung beim Öffnen der SIP-Steckdose* |
| %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% | J | J | 10000 | *6.1.5 Konfigurierbarer Zeitüberschreitung beim Öffnen der SIP-Steckdose* |
| %SOURCE_PORT_WXT% | J | J | 5060 | *6.1.7 Bevorzugte Portnutzung für SIP* |
| %SIP_FAILBACK_ENABLED_WXT% | J | N | wahr | *6.1.8.2 SIP-Fehler* |
| %SIP_FAILBACK_TIMEOUT_WXT% | J | N | 900 | *6.1.8.2 SIP-Fehler* |
| %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% | J | N | Falsch | *6.1.8.2 SIP-Fehler* |
| %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% | J | J | dns | *6.1.8.3. IP-Version erzwingen* |
| %USE_ALTERNATIVE_IDENTITIES_WXT% | J | J | Falsch | *6.1.10 P-zugeordnete URIs in REGISTER* verwenden |
| %TCP_SIZE_THRESHOLD_WXT% | J | J | 18000 | *6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen* |
| %SIP_REFRESH_ON_TTL_WXT% | J | N | Falsch | *6.1.8.4 DNS TTL-Verwaltung* |
| %ENABLE_SIP_UPDATE_SUPPORT_WXT% | J | J | Falsch | *6.1.12 Unterstützung für SIP-UPDATE* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %ENABLE_PEM_SUPPORT_WXT% | J | J | Falsch | *6.1.11 SIP P-Early Media (PEM)-Header* |
| %ENABLE_SIP_SESSION_ID_WXT% | J | J | Falsch | *6.1.15 SIP-Sitzungs-ID* |
| %ENABLE_FORCE_SIP_INFO_FIR_WXT% | J | J | Falsch | *6.1.13 Ältere SIP-INFO-FIR* |
| %SRTP_ENABLED_WXT% | J | J | Falsch | *6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll* |
| %SRTP_MODE_WXT% | J | J | Falsch | *6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll* |
| %ENABLE_REKEYING_WXT% | J | J | wahr | *6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll* |
| %RTP_AUDIO_PORT_RANGE_START_WXT% | J | J | 8000 | *6.1.17 Portbereich des Transportprotokolls in Echtzeit* |
| %RTP_AUDIO_PORT_RANGE_END_WXT% | J | J | 8099 | *6.1.17 Portbereich des Transportprotokolls in Echtzeit* |
| %RTP_VIDEO_PORT_RANGE_START_WXT% | J | J | 8100 | *6.1.17 Portbereich des Transportprotokolls in Echtzeit* |
| %RTP_VIDEO_PORT_RANGE_END_WXT% | J | J | 8199 | *6.1.17 Portbereich des Transportprotokolls in Echtzeit* |
| %ENABLE_RTCP_MUX_WXT% | J | J | wahr | *6.1.19 RTCP-MUX* |
| %ENABLE_XSI_EVENT_CHANNEL_WXT% | J | J | wahr | *6.1.33 XSI-Ereigniskanal* |
| %CHANNEL_HEARTBEAT_WXT% | J | J | 10000 | *6.1.33 XSI-Ereigniskanal* |
| %XSI_ROOT_WXT% | J | J | leer (verwendet ursprüngliche URL) | *6.1.32 XSI-Wurzel und -Pfade* |
| %XSI_ACTIONS_PATH_WXT% | J | J | /com.broadsoft.xsi-actions/ | *6.1.32 XSI-Wurzel und -Pfade* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %XSI_EVENTS_PATH_WXT% | J | J | /com.broadsoft.xsi-events/ | *6.1.32 XSI-Wurzel und -Pfade* |
| %ENABLE_CALLS_AUTO_RECOVERY_WXT% | J | J | Falsch | *6.1.25 Automatische Anrufwiederherstellung / Nahtlose Anrufübergabe* |
| %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% | N | J | Nur-C | *6.3.1 Notrufe* |
| %ENABLE_CALL_PICKUP_BLIND_WXT% | J | N | Falsch | *6.2.2 Anrufübernahme* |
| %ENABLE_CALL_PICKUP_DIRECTED_WXT% | J | N | Falsch | *6.2.2 Anrufübernahme* |
| %WEB_CALL_SETTINGS_URL_WXT% | J | J | leer | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %USER_PORTAL_SETTINGS_URL_WXT% | J | J | leer | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %ENABLE_CALL_CENTER_WXT% | J | J | Falsch | *6.1.31 Anmeldung/Abmeldung bei Callcenter/Anrufwarteschlange* |
| %WEB_CALL_SETTINGS_TARGET_WXT% | J | J | extern | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% | J | J | wahr | *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen* |
| %USE_MEDIASEC_WXT% | J | J | Falsch | *6.1.3 3GPP SIP-Header für SRTP* |
| %ENABLE_DIALING_CALL_BACK_WXT% | N | J | Falsch | *6.3.4 Zum Wählen klicken (Rückruf )* |
| %DIALING_CALL_BACK_TIMER_WXT% | N | J | 10 | *6.3.4 Zum Wählen klicken (Rückruf )* |
| %ENABLE_EXECUTIVE_ASSISTANT_WXT% | J | N | Falsch | *6.2.3 Unterstützung von Chef-Administratoren (*Führungskraft-Assistent) |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% | N | J | 35 | *6.3.2 Push-Benachrichtigungen für Anrufe* |
| %ENABLE_CALL_RECORDING_WXT% | J | J | Falsch | *6.1.26 Anrufaufzeichnung* |
| %ENABLE_SINGLE_ALERTING_WXT% | N | J | Falsch | *6.3.3 Einzelne Benachrichtigung* |
| %ENABLE_CALL_PARK_WXT% | J | J | Falsch | *6.1.23 Anruf parken/abrufen* |
| %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% | J | J | 10 | *6.1.23 Anruf parken/abrufen* |
| %ENABLE_RTP_ICE_WXT% | J | J | Falsch | *6.1.18 ICE-Unterstützung (nur Webex Calling)* |
| %RTP_ICE_MODE_WXT% | J | J | icestun | *6.1.18 ICE-Unterstützung (nur Webex Calling)* |
| %RTP_ICE_SERVICE_URI_WXT% | J | J | leer | *6.1.18 ICE-Unterstützung (nur Webex Calling)* |
| %RTP_ICE_PORT_WXT% | J | J | 3478 | *6.1.18 ICE-Unterstützung (nur Webex Calling)* |
| %ENABLE_RTP_ICE_IPV6_WXT% | J | J | Falsch | *6.1.18 ICE-Unterstützung (nur Webex Calling)* |
| %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT% | J | N | Falsch | *6.1.8.4 DNS TTL-Verwaltung* |
| %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | J | N | Falsch | *6.2.4 Eskalieren von SIP-Anrufen an Meeting* |
| %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% | J | N | Falsch | *6.2.5 Anrufe über das Tischtelefon steuern – Automatische* Anrufannahme |
| %ENABLE_DIALING_VOIP_WXT% | N | J | wahr | *6.3.5 MNO-Unterstützung* *Anruf* mit nativem Wählprogramm |
| %ENABLE_DIALING_NATIVE_WXT% | N | J | Falsch | *6.3.5 MNO-Unterstützung* *Anruf* mit nativem Wählprogramm |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% | J | J | wahr | *6.1.35 SIP-URI-Wahl* |
| %ENABLE_SIP_VIDEOCALLS_WXT% | J | J | wahr | *6.1.37 Videoanrufe deaktivieren* |
| %ENABLE_LOCUS_VIDEOCALLS_WXT% | J | J | wahr | *6.1.37 Videoanrufe deaktivieren* |
| %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% | J | J | Desktop – wahr<br>Mobil, Tablet - falsch | *6.1.37 Videoanrufe deaktivieren* |
| %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% | J | J | Falsch | *6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter* |
| %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% | J | J | 0 | *6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter* |
| %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% | J | J | -1 | *6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter* |
| %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT% | J | J | einmal_pro_login | *6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter* |
| %ENABLE_AUTO_ANSWER_WXT% | J | N | Falsch | *6.2.6 Automatische Anrufannahme mit Tonbenachrichtigung* |
| %ENABLE_CALLS_SPAM_INDICATION_WXT% | J | J | Falsch | *6.1.41 Anzeige von Spam-Anrufen* |
| %ENABLE_NOISE_REMOVAL_WXT% | J | J | Falsch | *6.1.42 Geräuschunterdrückung und Bandbreitenerweiterung für PSTN/Mobile-Anrufe* |
| %ENABLE_AUDIO_MARI_FEC_WXT% | J | J | Falsch | *6.1.46.2 Forward Error Correction (FEC) und Packets Retransmission (RTX)* |
| %ENABLE_AUDIO_MARI_RTX_WXT% | J | J | Falsch | *6.1.46.2 Forward Error Correction (FEC) und Packets Retransmission (RTX)* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %ENABLE_VIDEO_MARI_FEC_WXT% | J | J | Falsch | *6.1.46.2 Forward Error Correction (FEC) und Packets Retransmission (RTX)* |
| %ENABLE_VIDEO_MARI_RTX_WXT% | J | J | Falsch | *6.1.46.2 Forward Error Correction (FEC) und Packets Retransmission (RTX)* |
| %ENABLE_CALL_BLOCK_WXT% | J | J | Falsch | *6.1.45 Sperrliste (nur Webex Calling)* |
| %ENABLE_WIDGET_HOLD_CALLS_WXT% | N | J | wahr | *6.3.5.6 MNO-Mobilität – Widget in Anrufen* |
| %ENABLE_WIDGET_TRANSFER_CALLS_WXT% | N | J | wahr | *6.3.5.6 MNO-Mobilität – Widget in Anrufen* |
| %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | N | J | wahr | *6.3.5.6 MNO-Mobilität – Widget in Anrufen* |
| %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% | J | J | Falsch | *6.1.47 Gleichzeitige Anrufe mit demselben Benutzer* |
| %ENABLE_REMOTE_MUTE_CONTROL_WXT% | J | N | Falsch | *6.2.14 Remote-Stummschaltungssteuerungs-Event-Paket (nur Webex Calling)* |
| %ENABLE_VOICE_MAIL_FORWARDING_WXT% | J | J | wahr | *6.1.29.2 Anrufweiterleitung an Voicemail* |
| %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% | J | J | wahr | *6.1.8.1 SIP-Failover* |
| %ENABLE_CALL_MOVE_HERE_WXT% | J | N | Falsch | *6.2.15 Anruf verschieben* |
| %ENABLE_SPEECH_ENHANCEMENTS_WXT% | J | J | Falsch | *6.1.42 Geräuschunterdrückung und Bandbreitenerweiterung für PSTN/Mobile-Anrufe* |
| %DIALING_NATIVE_FAC_PREFIX_WXT% | N | J | leer | *6.3.5.1 Anruf mit nativem Wählprogramm* |
| %ENABLE_TRANSFER_AUTO_HOLD_WXT% | J | J | Falsch | *6.1.20 Transfer* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %ENABLE_RTCP_XR_NEGOTIATION_WXT% | J | J | wahr | *6.1.48 RTCP-XR* |
| %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% | N | J | Falsch | *6.3.6 Anrufer-ID für eingehenden* Anruf |
| %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% | N | J | Falsch | *6.3.6 Anrufer-ID für eingehenden* Anruf |
| %ENABLE_CLID_OUTGOING_CALLS_WXT% | N | J | Falsch | *6.1.50 Anrufer-ID* *Ausgehende* Anrufer-ID (nur Webex Calling) |
| %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% | N | J | Falsch | *6.1.50 Anrufer-ID* *Ausgehende* Anrufer-ID (nur Webex Calling) |
| %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% | N | J | Falsch | *6.1.50 Anrufer-ID* *Ausgehende* Anrufer-ID (nur Webex Calling) |
| %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% | N | J | Falsch | *6.1.50 Anrufer-ID* *Ausgehende* Anrufer-ID (nur Webex Calling) |
| %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% | N | J | Falsch | *6.1.50 Anrufer-ID* *Ausgehende* Anrufer-ID (nur Webex Calling) |
| %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% | J | J | Falsch | *6.1.49 Informationen zur Anrufweiterleitung* |
| %ENABLE_BUSY_LAMP_FIELD_WXT% | J | N | Falsch | *6.2.8.1 Besetztlampenfeld* |
| %ENABLE_BLF_DISPLAY_CALLER_WXT% | J | N | wahr | *6.2.8.1 Besetztlampenfeld* |
| %BLF_NOTIFICATION_DELAY_TIME_WXT% | J | N | 0 | *6.2.8.1 Besetztlampenfeld* |
| %ENABLE_GCP_NOTIFICATIONS_WXT% | J | N | Falsch | *6.2.8.2 Anrufübernahmegruppe (nur Webex Calling)* |



Cisco – vertraulich

| Tag | Auf Desktop verwendet | In Mobilgeräten/Tablets verwendet | Standardwert | Abschnitt |
|---|---|---|---|---|
| %ENABLE_GCP_DISPLAY_CALLER_WXT% | J | N | Falsch | *6.2.8.2 Anrufübernahmegruppe (nur Webex Calling)* |
| %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% | J | N | 120 | *6.2.8.2 Anrufübernahmegruppe (nur Webex Calling)* |
| %UDP_KEEPALIVE_ENABLED_WXT% | J | J | wahr | *6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen* |
| %TCP_KEEPALIVE_ENABLED_WXT% | J | J | Falsch | *6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen* |
| %TLS_KEEPALIVE_ENABLED_WXT% | J | J | Falsch | *6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen* |
| %ENABLE_MULTI_LINE_WXT% | J | N | Falsch | *6.2.12 Mehrere Leitungen – Darstellung* gemeinsam genutzter Leitungen |
| %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | N | J | Falsch | *6.2.4 Eskalieren von SIP-Anrufen an Meetings (Webex Calling)* |
| %ENABLE_CLID_DELIVERY_BLOCKING_WXT% | N | J | Falsch | *6.3.5.3 Leitungsidentität (CLID) für ausgehende Anrufe – Dual Persona* |
| %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT% | N | J | Falsch | *6.3.5.3 Leitungsidentität für ausgehende Anrufe (CLID)* |
| %CLID_REMOTE_NAME_MACHINE_MODE_WXT% | J | J | gelöst | *6.1.50.2 Name der Remote-Anrufer-ID* |

Weitere Informationen zum Zuordnen der in Webex für Cisco BroadWorks verwendeten benutzerdefinierten Tags zu den von UC-One verwendeten Tags finden Sie im Abschnitt *8Benutzerdefinierte Tags-Zuordnung zwischen Webex für Cisco BroadWorks und UC-One*.



Cisco – vertraulich

## 6.1 Allgemeine Funktionen

### 6.1.1 SIP-Servereinstellungen

Der Client ist üblicherweise so konfiguriert, dass er ein SIP-Netzwerk verwendet, indem er die Datei *config-wxt.xml* ändert. In der Regel müssen die folgenden Parameter geändert werden:

- SIP-Domäne. Dies wird als Domänenteil des eigenen SIP-URI (der eigene SIP-URI wird manchmal auch Leitungsport genannt) im Allgemeinen in SIP-Headern und in Remote-Anrufen (XSI) verwendet. Der Benutzerteil des eigenen SIP-URI stammt aus der Konfiguration der SIP-Anmeldeinformationen (Parameter <Benutzername> unter <Anmeldeinformationen>).
- SIP-Server-URI oder IP-Adresse des SIP-Proxyservers, wenn die DNS-Auflösung fehlschlagen sollte. Beachten Sie, dass zur Verwendung von TLS keine IP-Adressen im Proxy-Parameter verwendet werden können, da die TLS-Zertifikatsprüfung fehlschlägt. Weitere Informationen zum Proxy-Port finden Sie im DM-Tag %SOURCE_PORT_WXT%. Beachten Sie, dass die DNS TTL-Verwaltungsfunktion nicht verwendet werden kann, wenn im Proxy-Adressparameter eine IP-Adresse verwendet wird. Generell wird aus diesen Gründen die Verwendung einer IP-Adresse in diesem Feld nicht empfohlen.

Es können auch andere Parameter geändert werden, um verschiedene Funktionen für Anrufe zu aktivieren. Die vorherigen Einstellungen ermöglichen jedoch grundlegende Funktionen für Folgendes:

- Registrierung im SIP-Netzwerk.
- Tätigen von Audio- oder Videoanrufen.
- Durchführen einer DNS-basierten Proxy-Erkennung, die die Verwendung mehrerer Proxys ermöglicht.

Sobald die SIP-Registrierung aktiviert ist, muss die Aktivierung von SIP-ABONNEMENT für MWI über separate Konfigurationsparameter erfolgen. Weitere Informationen zur Voicemail finden Sie im Abschnitt *6.1.27Voicemail , Visuelle Voicemail, Briefkastenlampe*.

Beachten Sie, dass die grundlegende SIP-Konfiguration für MWI immer erforderlich ist, auch wenn SIP-Anrufe deaktiviert sind. MWI basiert auf SIP NOTIFYs.

Die Einrichtung der SIP-Server folgt diesem grundlegenden Schema:

- Die Proxy-Adresse enthält den SIP-Server-URI.
- Es kann nur ein Proxy definiert werden.
- Die DNS-Proxy-Erkennung bietet Unterstützung für viele Proxys, die die ordnungsgemäße Einrichtung des DNS erfordern.

Darüber hinaus werden SIP-Timer in der Konfigurationsdatei offengelegt (es wird nicht empfohlen, sie zu ändern).

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



Cisco – vertraulich

```
        <T4>5000</T4>
    </timers>
```

- T1 – die Zeitspanne in Millisekunden für eine Netzwerk-Roundtrip-Verzögerung.
- T2 – die maximale Zeit in Millisekunden, bevor nicht eingeladene Anfragen und Antworten erneut gesendet werden.
- T4 – die maximale Zeit in Millisekunden, bis eine Nachricht im  Netzwerk verbleibt.

Jede Leitung hat eigene Parameter wie die Voicemail-Nummer, den Konferenz-URI und die Domäne sowie die SIP-Authentifizierungsanmeldeinformationen. Bei Bedarf können separate Anmeldeinformationen für die 401- und 407-Signalisierung konfiguriert werden.

Das folgende Beispiel und die folgende Tabelle enthalten Informationen zu den typischen DM-Tags, die für die SIP-Konfiguration verwendet werden.

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



Cisco – vertraulich

```
<proxy address="%SBC_ADDRESS_WXT%" port="%SBC_PORT_WXT%" />
<preferred-port>%SOURCE_PORT_WXT%</preferred-port>
```

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %BWLINEPORT-n% | leer | Zeichenfolge | Normalerweise SIP-Benutzername.<br>Weitere Informationen finden Sie im Abschnitt *5.7Dynamische, integrierte System-Tags in Cisco* BroadWorks.<br>Beispiel: johndoe |
| %BWAUTHPASSWORD-n% | leer | Zeichenfolge | Normalerweise SIP-Kennwort.<br>Weitere Informationen finden Sie im Abschnitt *5.7Dynamische, integrierte System-Tags in Cisco* BroadWorks.<br>Beispiel: Sekretpasswort |
| %BWE164-n% | leer | Telefonnummer | Standardtelefonnummer für den Benutzer im internationalen Format.<br>Weitere Informationen finden Sie im Abschnitt *5.7Dynamische, integrierte System-Tags in Cisco* BroadWorks.<br>Beispiel: 12345678 |
| %SBC_ADDRESS_WXT% | leer | Zeichenfolge | Weitere Informationen finden Sie im Abschnitt *5.6Systemstandard-Tags*.<br>Beispiel: sbcexample.domain.com |
| %SBC_PORT_WXT% | 5060 | Nummer | Weitere Informationen finden Sie im Abschnitt *5.6Systemstandard-Tags*.<br>Beispiel: 5060 |
| %BWHOST-n% | leer | Zeichenfolge | Wird normalerweise als SIP-Domäne verwendet.<br>Weitere Informationen finden Sie im Abschnitt *5.7Dynamische, integrierte System-Tags in Cisco* BroadWorks.<br>Beispiel: exampledomain.com |
| %SOURCE_PORT_WXT% | 5060 | Nummer | Wird normalerweise für den Parameter *preferred-port* verwendet.<br>Weitere Informationen finden Sie im Abschnitt *6.1.7Bevorzugte Portnutzung für SIP*.<br>Beispiel: 5061 |
| %BWUSEREXTID-n% | leer | Zeichenfolge | (Nur Webex Calling) Enthält die externe ID der Leitung<br>Weitere Informationen finden Sie unter *6.2.13Mehrere Leitungen – Virtuelle Leitungen (nur Webex* Calling).<br>Beispiel: 30f69bf7-710b-4cd0-ab4b-35ab393a1709 |



Cisco – vertraulich

**HINWEIS:** Es ist dringend ratsam, dass sich der SIP-Port von 5060 (z. B. 5075) unterscheidet, da bekannte Probleme mit der Verwendung des Standard-SIP-Ports (5060) mit Mobilgeräten aufgetreten sind.

### 6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll

Der Client kann so konfiguriert werden, dass die SIP-Signalisierung über TLS und SRTP (Secure Real-time Transport Protocol) für die Medienverschlüsselung verwendet wird. Diese Funktionen müssen jedoch in der Konfiguration aktiviert werden, wie im folgenden Beispiel gezeigt. Beachten Sie außerdem, dass bei Verwendung der dynamischen SIP-Proxy-Erkennung die DNS SRV-Prioritäten statische Parameter wie diesen (%USE_TLS_WXT%) überschreiben und der Nicht-TLS-Transport verwendet wird, wenn er eine höhere Priorität in DNS SRV hat. Weitere Informationen zur dynamischen SIP-Proxy-Erkennung finden Sie im Abschnitt *6.1.6Dynamische SIP-Proxyerkennung.*

Wenn keine dynamische Proxy-Erkennung verwendet wird, wird TLS für SIP verwendet.

Weitere Informationen zu SIP-Port- und Transportprotokollempfehlungen, wenn SIP-ALGs im Netzwerk verwendet werden, finden Sie im *Webex for Cisco BroadWorks Solution Guide* .

Beachten Sie, dass das verwendete Zertifikat gültig sein muss. Außerdem muss die Zertifikatskette intakt sein, damit auch das Zwischenzertifikat verknüpft ist. Es wird empfohlen, dass ein weit verbreitetes Zertifikat verwendet wird, sodass es standardmäßig bereits auf den Geräten vorhanden ist. Es ist auch möglich, Zertifikate lokal auf dem Desktop-Computer entweder manuell oder durch Massenbereitstellung hinzuzufügen, obwohl dies normalerweise nicht der Fall ist.

Um das zugehörige SRTP für die Medienverschlüsselung zu aktivieren, gibt es eine separate Einstellung.

Zusätzlich zu RTP kann der RTCP-Datenverkehr mit den gleichen Mechanismen wie RTP mithilfe der vorhergehenden Konfiguration gesichert werden.

Informationen zu SIP-/TLS-Chiffren finden Sie unter *Anhang A: TLS-Schlüssel.*

Das SRTP wird verwendet, um die Sicherheit des Medienstreams in drei verschiedenen Aspekten zu gewährleisten:

- Vertraulichkeit (Daten sind verschlüsselt)
- Authentifizierung (Zusicherung der Identität der anderen Partei oder Parteien)
- Integrität (Maßnahmen gegen z. B. Wiederholungsangriffe)

Die aktuelle Version des Medienrahmens unterstützt den AES 128-Counter-Modus für den Schutz und den Hash Message Authentication Code (HMAC)-SHA-1 für die Authentifizierung. Die Hauptschlüsselgröße ist 16 Bytes und das Hauptsalz ist 14 Bytes.

Das Medien-Framework unterstützt sowohl das vollständige (80-Bit) als auch das kurze (32-Bit) Authentifizierungs-Tag. Der Client tauscht die Schlüssel innerhalb des SDP als Teil der SIP-Signalisierung aus. Beide Seiten des Anrufs senden den von ihnen verwendeten Schlüssel an die andere Seite.



Cisco – vertraulich

SRTP kann mithilfe der im folgenden Beispiel gezeigten Konfiguration aktiviert werden. Die aktuelle Implementierung verwendet nur das sichere SDP-RTP-Profil und unterstützt Multiline-SDP für die Einträge Audio Visual Profile (AVP) und Secure Audio Visual Profile (SAVP). Die SRTP-Implementierung wurde in der üblichen Bereitstellungskonfiguration mit verschiedenen SBCs erfolgreich getestet. Interoperability Testing (IOT) mit Endpunkten, die nur die Verschlüsselung mit dem AVP-Profil unterstützen, wird nicht unterstützt.

SRTP-bezogene SDP-Prozeduren für mehrere Leitungen werden implementiert, sodass immer mehrere m-Leitungen verwendet werden. Es werden separate m-Linien für AVP und SAVP verwendet.

Beachten Sie jedoch, dass die SBC-Konfiguration sorgfältig geprüft werden muss; insbesondere muss sichergestellt werden, dass die eingehende „m=“-Leitung, die im SDP mit RTP/SAVP verknüpft ist, nicht entfernt wird, da SRTP-Anrufe in bestimmten Fällen blockiert werden können.

Mehrere verschiedene Netzwerkkonfigurationen sind jedoch möglich. In einigen Bereitstellungen ist der SBC nicht am Medienverkehr beteiligt, während in anderen Bereitstellungen jeder Client-RTP-Medienabschnitt zum SBC separat verschlüsselt und über den SBC ausgehandelt wird. In einigen Bereitstellungen lässt der SBC nicht mehrere SDP-Leitungen zu.

Der SBC kann auch die Reihenfolge der SDP-m-Leitungen bei der Anrufeinrichtung ändern, wobei AVP (unverschlüsselt) oder SAVP (verschlüsselt) m-Leitung an erster Stelle steht. Daher werden Clients, die die erste funktionierende m-Zeile auswählen, entweder verschlüsselten oder unverschlüsselten Datenverkehr bevorzugen. Die verschiedenen SRTP-Konfigurationsoptionen lauten wie folgt:

- Obligatorisch – Bei der Anrufeinrichtung umfasst das anfängliche SDP beim Annehmen nur die SAVP-m-Leitung und der Client akzeptiert beim Annehmen nur die SAVP-m-Leitung im SDP. Daher sind nur SRTP-Anrufe möglich.
- Bevorzugt – Bei der Anrufeinrichtung umfasst das anfängliche SDP sowohl die AVP- als auch die SAVP-m-Leitung, aber SAVP steht beim Angebot an erster Stelle und gibt die bevorzugte Reihenfolge an. Beim Annehmen wählt der Client SAVP aus, wenn verfügbar, auch wenn es sich nicht um die erste m-Leitung handelt (gemäß den SIP-Spezifikationen wird die Reihenfolge der m-Leitungen beim Annehmen nicht geändert).
- Optional – Bei der Anrufeinrichtung umfasst das anfängliche SDP sowohl die SAVP- als auch die AVP-m-Leitung, wenn es angeboten wird, aber AVP gibt zuerst die bevorzugte Reihenfolge an. Bei der Beantwortung wählt der Client die erste m-Leitung, AVP oder SAVP aus.
- SRTP nicht aktiviert – Im anfänglichen SDP ist keine SAVP-m-Leitung beim Anbieten vorhanden. Bei der Annahme wird SAVP nicht angenommen, daher sind nur RTP-Anrufe möglich.
- Transport – Wählen Sie automatisch den SRTP-Modus basierend auf dem Transportprotokoll aus. Wenn TLS verwendet wird, ist der obligatorische SRTP-Modus aktiviert. Wenn TCP oder UDP verwendet wird, wird kein SRTP verwendet.

SRTP im Vergleich zu RTP ist in beide Richtungen des Anrufs symmetrisch, d. h. die Sende- und Empfangsprofile sind gleich.

```
<config>
<protocols><sip>
```



Cisco – vertraulich

```
<secure>%USE_TLS_WXT%</secure>
```

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

Das Secure Real-Time Control Protocol (SRTCP) wird auch verwendet, wenn SRTP aktiviert ist.

In einigen Bereitstellungen wird eine erneute Eingabe für SRTP nicht unterstützt. Daher gibt es einen Konfigurationsparameter zum Aktivieren/Deaktivieren der SRTP-Neueingabe. Neue Schlüssel werden jedoch immer verwendet, wenn sie in einem aktualisierten SDP gemäß rfc3264 empfangen werden. Die Konfigurierbarkeit bezieht sich nur auf das Senden neuer Schlüssel.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USE_TLS_WXT% | Falsch | wahr, falsch | Wenn „false“ festgelegt ist, wird SIP TLS deaktiviert.<br>Wenn die Option auf „true“ festgelegt ist, wird SIP TLS aktiviert.<br>Beachten Sie, dass dieser Parameter ignoriert wird, wenn *6.1.6Dynamische SIP-Proxyerkennung* er verwendet wird. |
| %SRTP_ENABLED_WXT% | Falsch | wahr, falsch | Wenn „false“ festgelegt ist, wird SRTP deaktiviert.<br>Wenn „true“ festgelegt ist, wird SRTP aktiviert. |
| %SRTP_MODE_WXT% | optional | obligatorisch, bevorzugt, optional, Transport | Definiert, wie das bevorzugte SRTP bei der Anrufeinrichtung ist.<br>Der Standardwert ist „optional“. |
| %ENABLE_REKEYING_WXT% | wahr | wahr, falsch | Aktiviert die erneute SIP-Eingabe (SDP) für SRTP. |

**HINWEIS:** Wenn die ICE-Unterstützung aktiviert ist (siehe *6.1.18ICE-Unterstützung (nur Webex Calling)*), wird immer eine erneute Eingabe durchgeführt (%ENABLE_REKEYING_WXT%-Wert aus der Konfiguration wird ignoriert).

### 6.1.3 3GPP SIP-Header für SRTP

Neuere 3GPP-Spezifikationen erfordern zusätzliche SIP-Header für die Verwendung des Secure Real-time Transport Protocol (SRTP). Weitere Informationen finden Sie unter *3GPP TS 24.229* sowie unter:

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



Cisco – vertraulich

Die von dieser Spezifikation erforderlichen Header können SIP-Anrufe in Bereitstellungen unterbrechen, in denen diese Spezifikation nicht verwendet wird. Daher wird empfohlen, diese Header nur in Umgebungen zu verwenden, in denen sie von der Serverseite unterstützt werden.

Nur die Aktivierung der Verwendung der Header ist konfigurierbar. Für einzelne Header ist keine weitere Konfigurierbarkeit vorhanden. Alle Header sind entweder aktiviert oder deaktiviert.

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

Das folgende Tag steuert diese Funktion.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USE_MEDIASEC_WXT% | Falsch | wahr, falsch | Aktiviert 3GPP SIP-Header für die SRTP-Verhandlung. |

### 6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen

Der Webex for Cisco BroadWorks -Client kann so konfiguriert werden, dass er sowohl TCP, TLS als auch UDP für SIP-Signalisierung und RTP-Medien verwendet. Beachten Sie, dass der Client standardmäßig TCP verwendet. Beachten Sie außerdem, dass ohne TCP keepalive SIP TCP-Verbindungen nach einer Zeit der Inaktivität geschlossen werden.

Das folgende Beispiel zeigt diesen Konfigurationsknoten an.

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

Das folgende Tag steuert, ob der Client TCP oder UDP verwendet.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte (Bytes) | Beschreibung |
|---|---|---|---|
| %TCP_SIZE_THRESHOLD_WXT% | 0 | 0 | Zwingt die Verwendung von TCP. Die Entscheidung, TCP oder UDP für den Client zu verwenden, liegt beim Serviceanbieter. Es wird jedoch empfohlen, TCP mit dem Standardwert „0“ zu verwenden. |
| | 0 | 1 bis 99.000 | Erzwingt die Verwendung von UDP, wenn die Nachrichtengröße unter dem hier angegebenen Wert liegt.<br>Der Standardwert ist TCP, wenn die Nachrichtengröße größer als der festgelegte Wert ist. Um UDP zu verwenden, ist 1500 die Standardempfehlung. |



Cisco – vertraulich

| | | | |
|---|---|---|---|
| | 0 | 10.000 | Zwingt zur Verwendung von UDP. |

Der gleiche Konfigurationsknoten enthält auch Parameter für UDP, TCP und TLS Keepalive, wie im folgenden Beispiel dargestellt.

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

Folgende Parameter sind möglich:

- Aktivieren von TCP oder TLS keepalive, mögliche Werte – true/false, der Standardwert ist „false“, wenn der Knoten fehlt. Beachten Sie, dass bei Aktivierung dieser Funktion TCP-Keepalives gesendet werden, selbst wenn der UDP-Transport für SIP verwendet wird.
- Aktivieren von UDP keepalive, mögliche Werte – true/false, der Standardwert ist „true“, wenn der Knoten fehlt. Beachten Sie, dass UDP-Keepalives gesendet werden, wenn diese Funktion aktiviert ist, selbst wenn der TCP-Transport für SIP verwendet wird. Darüber hinaus akzeptiert der Client auch Datenverkehr über UDP, selbst wenn TCP für SIP verwendet wird, gemäß *RFC 3261*.
- Timeout gibt die maximale Zeit der Inaktivität in Sekunden an, nach der die keepalive-Nachricht gesendet wird. Kein Wert bedeutet, dass keepalive für das Protokoll deaktiviert ist.
- Nutzlast für die keepalive-Nachrichten, mögliche Werte (kein Wert bedeutet, dass keepalive für das Protokoll deaktiviert ist):
  - Absturz
  - Null (nicht zu verwenden)
  - Benutzerdefinierte Zeichenfolge ( **nicht zu verwenden** )

Die Keepalives können für NAT-Traversal-Zwecke verwendet werden, um NAT-Bindungen mit wenig zusätzlichem Datenverkehr offen zu halten.



Cisco – vertraulich

Die Server-IP-Adresse und der Port für Keepalives werden anhand der normalen Verfahren für die SIP-Proxy-Erkennung bestimmt. Beachten Sie, dass SIP-Ports und die Auswahl des Transportprotokolls, das über die dynamische SIP-Proxyerkennung abgerufen wird, jede statische Port- oder Transportkonfiguration überschreiben. Weitere Informationen zur dynamischen Proxyerkennung finden Sie im Abschnitt *6.1.6Dynamische SIP-Proxyerkennung.*

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %UDP_KEEPALIVE_ENABLED_WXT% | wahr | wahr, falsch | Steuert, ob die Keep-Alive-Pakete für den UDP-Transport gesendet werden sollen. |
| %TCP_KEEPALIVE_ENABLED_WXT% | Falsch | wahr, falsch | Steuert, ob die Keep-Alive-Pakete für den TCP-Transport gesendet werden sollen. |
| %TLS_KEEPALIVE_ENABLED_WXT% | Falsch | wahr, falsch | Steuert, ob die Keep-Alive-Pakete für den TLS-Transport gesendet werden sollen. |

### 6.1.5 Konfigurierbarer Zeitüberschreitung beim Öffnen der SIP-Steckdose

Bisher wurde die Zeitüberschreitung beim Öffnen eines SIP-Sockets für TCP auf 5 Sekunden und für TLS auf 10 Sekunden festcodiert. Diese Zeitüberschreitungen können jetzt konfiguriert werden.

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

Die folgenden Tags steuern die Zeitüberschreitung der Socket-Verbindung (in Millisekunden).



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% | 5000 | <integer> – Zeitüberschreitung in Millisekunden | Die Zeitüberschreitung der Socket-Verbindung, wenn der TCP-Transport verwendet wird. |
| %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% | 10000 | <integer> – Zeitüberschreitung in Millisekunden | Die Zeitüberschreitung für die Socket-Verbindung, wenn der TLS-Transport verwendet wird. |

### 6.1.6 Dynamische SIP-Proxyerkennung

Informationen zum Aktivieren der Funktion für die dynamische SIP-Proxyerkennung finden Sie im folgenden Beispiel.

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

Es ist möglich zu steuern, welche Transportprotokolleinträge von DNS SRV verwendet werden, wenn viele nach den in diesem Abschnitt angegebenen Verfahren verfügbar sind.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USE_PROXY_DISCOVERY_WXT% | Falsch | wahr, falsch | Aktiviert die dynamische SIP-Proxyerkennung für Audio- und Videoanrufe.<br>Der empfohlene Wert ist „true“. |
| %SBC_ADDRESS_WXT% | leer | String | Dieses Cisco BroadWorks-Tag wird normalerweise für den Parameter „Datensatzname“ verwendet. Es sollte eine gültige URL sein – keine IP-Adresse.<br>Weitere Informationen finden Sie im Abschnitt *5.6Systemstandard-Tags*.<br>Beispiel: sbc.domain.com |
| %DOMAIN_OVERRIDE_WXT% | leer | String | Dieses benutzerdefinierte Tag wird für die Domänenüberschreibung verwendet. Weitere Informationen finden Sie im folgenden Abschnitt.<br>Beispiel: Sonstige.Domäne.com |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USE_TCP_FROM_DNS_WXT% | wahr | wahr, falsch | Wenn dieser Parameterwert „false“ ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (TCP) verworfen.<br>Wenn „true“, werden die Ergebnisse von DNS SRV für dieses Transportprotokoll (TCP) verwendet. Abhängig von den SRV-Prioritäten kann noch ein anderer Transport gewählt werden. |
| %USE_UDP_FROM_DNS_WXT% | wahr | wahr, falsch | Wenn dieser Parameterwert „false“ ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (UDP) verworfen.<br>Wenn „true“, werden die Ergebnisse von DNS SRV für dieses Transportprotokoll (UDP) verwendet. Abhängig von den SRV-Prioritäten kann noch ein anderer Transport gewählt werden. |
| %USE_TLS_FROM_DNS_WXT% | wahr | wahr, falsch | Wenn dieser Parameterwert „false“ ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (TLS) verworfen.<br>Wenn „true“, werden die Ergebnisse von DNS für dieses Transportprotokoll (TLS) verwendet. Abhängig von den SRV-Prioritäten kann noch ein anderer Transport gewählt werden. |
| %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% | wahr, falsch | wahr | Aktiviert/deaktiviert den DNS-Sicherungsdienst. Wenn diese Option aktiviert ist, wird die A/AAAA-Auflösung für die SIP-Proxyadresse ausgeführt. Sie wird nur berücksichtigt, wenn die SRV/NAPTR-Diensterkennung aktiviert ist. |
| %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% | wahr, falsch | wahr | Wenn „true“ festgelegt ist und die NAPTR-Serviceerkennung fehlschlägt oder keine Ergebnisse zurückgibt, wird die SRV-Serviceerkennung für den konfigurierten Host durchgeführt. Wenn „false“ festgelegt ist, wird keine SRV-Erkennung durchgeführt. |
| %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% | wahr, falsch | Falsch | Ermöglicht die Umgehung des DNS-Cache des Betriebssystems. |

DNS ermöglicht dem Client, die IP-Adresse, den Port und das Transportprotokoll für den SIP-Proxy gemäß RFC 3263 abzurufen.

DNS SRV, Naming Authority Pointer (NAPTR) und A-Record-Abfragen werden unterstützt. Bei der Anmeldung erfolgt der 3-stufige Ablauf wie folgt:

1. Führen Sie eine NAPTR-Abfrage mit dem *<record-name>* Feld durch, um die Server-URIs mit den Transportprotokollen zu erhalten, falls vorhanden. Der Wert für den Parameter *<record-name>* sollte die vollständige Domäne sein, die DNS auflösen soll, und darf keine IP-Adresse sein.



Cisco – vertraulich

2. Beheben Sie die in der NAPTR-Abfrage gefundenen Elemente mithilfe einer SRV-Abfrage, um den endgültigen Server-URI und Port abzurufen. Der in der SRV-Abfrage verwendete Domänenteil wird aus dem Ergebnis der NAPTR-Abfrage entnommen, um den endgültigen Server-URI (und Port) zu finden. Der von der DNS SRV-Abfrage empfangene Port wird verwendet, wenn die DNS SRV-Einträge verfügbar sind. Beachten Sie, dass der Port nur aus der Konfigurationsdatei für den statischen Proxy in der Konfigurationsdatei gilt und nicht für die URIs, die mit SRV aufgelöst werden. Die Verwendung der verschiedenen Datensatznamen finden Sie in den folgenden Beispielen.

   Wenn kein NAPTR gefunden wird, versucht der Client eine SRV-Abfrage mit dem Datensatznamen, der vom Parameter *<domain>* genommen wurde, es sei denn, es ist *<domain-override>* Parameter vorhanden, in diesem Fall *<domain-override>* wird verwendet und versucht automatisch, separate Einträge für TCP, UDP und TLS zu finden (*_sip_protocol* [UDP, TCP oder TLS]). Beachten Sie, dass das Stream Control Transmission Protocol (SCTP) nicht unterstützt wird. Wenn SRV-Abfragen keine Ergebnisse liefern, schlägt die Proxy-Erkennung fehl, und dem Endbenutzer wird ein Fehler angezeigt, der angibt, dass Anrufe nicht verfügbar sind. In diesem Fall gibt es keine SIP-Registrierung. Selbst wenn alle SRV-Abfragen fehlschlagen oder die dort empfangenen Server nicht funktionieren, überprüft der Client als Fallback weiterhin, ob der konfigurierte statische Proxy funktioniert, nur mit A-Abfragen an den URI, der in <proxy address> angegeben ist, um zu sehen, ob er eine IP-Adresse bereitstellt, die eine funktionierende SIP-Registrierung bereitstellt. Port und Transport in diesem letzten Fall kommen von *tcp-threshold* und *<secure>* Parametern.

3. Beheben Sie gefundene URIs mit der A-Datensatzabfrage. Die empfangenen endgültigen IP-Adressen werden in der Reihenfolge versucht, in der sie empfangen werden, um eine funktionierende Verbindung zum SIP-Proxy zu erhalten. Diese Reihenfolge kann vom Serviceanbieter im DNS definiert werden. Der erste SIP-Proxy-URI mit erfolgreicher A-Eintrag-Suche wird ausgewählt und verwendet, bis er nicht mehr funktioniert oder sich der Client abmeldet. Bei der A-Abfrage wird immer nur eine IP-Adresse verwendet, auch wenn viele empfangen werden. Alle SRV-Einträge werden jedoch bis zum Abmelden oder Verlust des Netzwerks aufgelöst.

**Wichtige Hinweise**

**ANMERKUNG 1 <UNK>** : Wenn die DNS-Proxy-Erkennung zur Auswahl des Transportprotokolls im SRV-Schritt führt, indem sie einen funktionierenden SIP-Proxy-URI für ein Transportprotokoll erhält, überschreibt sie den Parameter *tcp-threshold* , der normalerweise verwendet wird, um UDP oder TCP in der Konfigurationsdatei auszuwählen. Dasselbe gilt auch für die Konfiguration von SIP/TLS. TCP oder UDP wird abhängig von der Priorität im DNS verwendet.

**ANMERKUNG 2 <UNK>** : Über SRV empfangene Elemente werden in der Konfigurationsdatei vor dem statischen Proxy priorisiert. Die NAPTR-Bestellung wird nicht geprüft; es zählt nur die SRV-Priorität. Wenn SRV mehrere Elemente mit dem gleichen Transportprotokoll, der gleichen Priorität und der gleichen Gewichtung ergibt, wird jeder empfangene nach dem Zufallsprinzip ausgewählt. NAPTR-Gewichte werden in dieser Version nicht unterstützt, aber SRV-Gewichte werden unterstützt. Die SRV-Priorität wird zuerst untersucht, und bei Elementen mit gleicher Priorität wird die Gewichtung untersucht, um die Wahrscheinlichkeit zu ermitteln, in der als Nächstes ein bestimmter Server versucht wird.

**ANMERKUNG 3 <UNK>** : Der optionale Parameter *Domänenüberschreibung* ermöglicht es, einen anderen A-Datensatznamen als den im SIP-Domänenkonfigurationsparameter mit SRV aufzulösen, wenn NAPTR-Ergebnisse ausgelassen werden. In den folgenden Beispielen wird die Verwendung des Parameters *domain-override* beschrieben.



Cisco – vertraulich

**ANMERKUNG 4 <UNK>** : Der Client verwendet Betriebssystem-Primitiven für DNS-Operationen und DNS-Antworten werden normalerweise zwischengespeichert, um die TTL der DNS-Antwort zu berücksichtigen.

**ANMERKUNG 5 <UNK>** : Der DNS-Typ (Dienst) für NAPTR-Datensätze muss die Verfahren *RFC* 3263 befolgen, andernfalls kann die DNS-Auflösung fehlschlagen. Beispielsweise muss SIPS+D2T für SIP über TLS verwendet werden.

**ANMERKUNG 6 <UNK>** : Der Client unterstützt nur bestimmte Präfixe für NAPTR-Dienste. Im Folgenden sind die unterstützten Präfixe aufgeführt:

SIP+D2U -> _sip._udp

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

Wenn die NAPTR-Antwort einen Datensatz mit Präfix enthält, der nicht mit dem Servicetyp übereinstimmt, wird dieser Datensatz ignoriert.

**Beispiel 1: DNS-Proxy-Erkennung ohne Konfigurationsparameter Domänenüberschreibung verwenden**

Das folgende Beispiel zeigt eine Konfiguration mit SIP-Proxy-Erkennung, wenn nur SIP über TCP verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse liefert.

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

Daraus ergeben sich die folgenden Schritte in der Protokollebene.

```
1. NAPTR-Abfrage für record-domain.com, Antwort:
record-domain.com .
28591 IN NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.
2. SRV-Abfrage für _sip._tcp.test.sip.record-domain.com (in der NAPTR-
Abfrage empfangen), Antwort
_sip._tcp.test.sip.record-domain.com. 28635 IN SRV
10 10 5061  test.sipgeo.record-domain.com .
3. A-Record-Abfrage für  test.sipgeo.record-domain.com , Antwort:
test.sipgeo.record-domain.com . 16 IN A 1.2.3.4
```

Infolgedessen erfolgt die SIP-Registrierung über TCP mit Port 5061 (erhalten im SRV-Schritt) und in Richtung IP-Adresse 1.2.3.4.



Cisco – vertraulich

**Beispiel 2: Parameter für Domänenüberschreibung in Konfigurationsdatei verwenden**

Das folgende zweite Beispiel einer Konfiguration mit SIP-Proxy-Erkennung, bei der die SIP-Domäne von der Proxy-Domäne abweicht und nur SIP über UDP verwendet wird und die NAPTR-Abfrage keine Ergebnisse liefert.

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

Daraus ergeben sich die folgenden Schritte auf Protokollebene.

```
1. NAPTR query for record-domain.com, no answer.
2. SRV query for _sip._tcp.override-domain.com (from configuration file),
answer
_sip._tcp.override-domain.com. 28635 IN SRV
10 10 5061 test.override-domain.com.
3. A-record query for test.override-domain.com, answer:
test.sipgeooverride-domain.com. 16 IN A 4.3.2.1
```

Infolgedessen erfolgt die SIP-Registrierung über UDP mit Port 5061 (erhalten im SRV-Schritt) und in Richtung IP-Adresse 4.3.2.1.

**Beispiel 3 : Verwenden von SRV-Prioritäten**

Das folgende Beispiel zeigt eine Konfiguration mithilfe der SIP-Proxy-Erkennung, wenn nur SIP über TCP verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse zurückgibt, aber mehrere NAPTR- und SRV-Datensätze mit unterschiedlichen Prioritäten empfangen werden. In diesem Fall spielt in diesem Release-Event nur die SRV-Priorität eine Rolle, obwohl auch mehrere NAPTR-Datensätze mit unterschiedlichen Prioritäten empfangen werden.

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

Daraus ergeben sich die folgenden Schritte auf Protokollebene.

```
1. NAPTR query for record-domain.com, answer:
record-domain.com.
28591 IN NAPTR 100 10 "S" "SIPS+D2T" "" _sip._tcp.test.sip.record-domain.com.
28591 IN NAPTR 120 10 "S" "SIPS+D2U" "" _sip._udp.test.sip.record-domain.com.

2. SRV query for _sip._tcp.test.sip.record-domain.com (received in the NAPTR
query), answer
_sip._tcp.test.sip.record-domain.com. 28635 IN SRV
```



Cisco – vertraulich

```
10 10 5061 test.sipgeo.record-domain.com.

SRV query for _sip._udp.test.sip.record-domain.com (received in the NAPTR
query), answer
_sip._udp.test.sip.record-domain.com. 28635 IN SRV
20 10 5062 test.sipgeo.record-domain.com.

3. A-record query for test.sipgeo.record-domain.com, answer:
test.sipgeo.record-domain.com. 16 IN A 1.2.3.4
```

Daher erfolgt die SIP-Registrierung über TCP mit Port 5061 (erhalten im SRV-Schritt) und in Richtung IP-Adresse 1.2.3.4, die sowohl UDP als auch TCP unterstützen würde.

**Beispiel 4: DNS-Proxy-Erkennung mit NAPTR verwenden, wenn der Dienst nicht mit dem Servicetyp übereinstimmt**

Das folgende Beispiel zeigt eine Konfiguration mithilfe der SIP-Proxy-Erkennung, wenn SIP über TCP und TLS verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse zurückgibt.

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

Daraus ergeben sich die folgenden Schritte in der Protokollebene.

```
1. NAPTR query for record-domain.com, answer:
record-domain.com.
28591 IN NAPTR 100 10 "S" "SIPS+D2T" "" _sip._tls.test.sip.record-
domain.com.
28591 IN NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.

2. For the first record we have service type "SIPS+D2T" and the prefix is
"sip._tls.". Since this prefix doesn't match the service type (see Note 6
above) it will be ignored.

3. SRV query for _sip._tcp.test.sip.record-domain.com (received in the NAPTR
query), answer
_sip._tcp.test.sip.record-domain.com. 28635 IN SRV
10 10 5061 test.sipgeo.record-domain.com.

3. A-record query for test.sipgeo.record-domain.com, answer:
test.sipgeo.record-domain.com. 16 IN A 1.2.3.4
```

Infolgedessen erfolgt die SIP-Registrierung über TCP mit Port 5061 (erhalten im SRV-Schritt) und in Richtung IP-Adresse 1.2.3.4.



Cisco – vertraulich

### 6.1.7 Bevorzugte Portnutzung für SIP

Es gab einige Fälle, in denen ein anderes Softwarepaket auf demselben Computer wie der Client ausgeführt wurde und den Standard-SIP-Port belegt. Um den Client so zu konfigurieren, dass er einen anderen Port für SIP verwendet, kann der Parameter preferred-port verwendet werden. Der Client versucht, den konfigurierten Portwert zu verwenden, der im Parameter *preferred-port* angegeben ist, aber wenn er genommen wird, versucht der Client inkrementell Portwerte oberhalb des konfigurierten Werts. Wenn der Wert des bevorzugten Ports beispielsweise „6000“ ist und dieser Port übernommen wird, versucht der Client 6001, 6002, 6003 usw., bis ein nicht verwendeter Port gefunden wird. Sobald ein nicht verwendeter Port gefunden wurde, verwendet er diesen für seine eigene SIP-Kommunikation.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SOURCE_PORT_WXT% | 5060 | Nummer | Gibt den bevorzugten lokalen SIP-Port für die Kommunikation an.<br>Beispiel: 5060 |

### 6.1.8 SIP Failover und Failback

SIP-Failover und -Failback müssen die Cisco BroadWorks-Verfahren befolgen. Dazu muss mehr als ein Proxy (normalerweise der SBC) konfiguriert sein.

Auf der Client-Seite sollte der Proxy auf mehrere IP-Adressen aufgelöst werden. Dies kann auf eine der folgenden Arten erreicht werden:

- Die SIP-Proxyerkennung ist aktiviert und der DNS-Server verfügt über NAPTR- und/oder SRV-Datensätze für den SBC-FQDN (siehe Abschnitt *6.1.6Dynamische SIP-Proxyerkennung*).
- Die SIP-Proxyadresse wird als FQDN bereitgestellt und auf mehrere IP-Adressen aufgelöst (siehe Abschnitt *6.1.1SIP-Servereinstellungen*).

Der DNS-Cache des Betriebssystems wird verwendet, um unnötigen DNS-Datenverkehr zu vermeiden. Es gibt kein
festcodiertes Limit für die maximale Anzahl von IP-Adressen in der Liste.

Wenn mehrere IP-Adressen aufgelöst werden, werden sie bei der Anmeldung nach Priorität geordnet. Der Client beginnt mit der ersten verfügbaren IP-Adresse.

#### 6.1.8.1 SIP-Failover

Ein SIP-Failover kann wie folgt durch einen Socket-Fehler, einen Anfrage-Timeout-Fehler oder eine definitive Fehlerantwort vom Server ausgelöst werden:

- Socket-Fehler: Wenn der Socket zwischen Client und Server defekt wird oder geschlossen wird, wie bei einem Netzwerkverbindungsverlust, reagiert der Client sofort und löst einen Failover aus.
- Zeitüberschreitung (z. B. wenn der SBC hängt) – basierend auf dem SIP T1:



Cisco – vertraulich

- SIP INVITE – Wenn die INVITE-Anforderung eine Zeitüberschreitung aufweist, registriert sich der Client beim nächsten verfügbaren SBC (IP) und versucht die INVITE erneut.
- Eine weitere SIP-Anforderung – der Client versucht, sich beim nächsten verfügbaren SBC (IP) zu registrieren.

- Definitive Fehlerantwort vom Server empfangen:
  - Die folgenden SIP-Fehlerantworten vom Server auf ein SIP REGISTER lösen ein Failover aus:
    - 5xx
    - 6xx
  - Die folgenden SIP *4xx* Antworten auf SIP REGISTER führen nicht zu Failover:
    - 401 nicht berechtigt
    - 403 Verboten
    - 404 nicht gefunden
    - 407 Proxy-Authentifizierung erforderlich
    - 423-Intervall zu kurz
  - Darüber hinaus *lösen* 4xx -Fehlerantworten auf SIP INVITE kein Failover aus, aber *5xx* und *6xx* tun dies.

Wenn ein Failover ausgelöst wird, übernimmt der Client die nächste verfügbare IP-Adresse aus der Liste. Der SIP T1-Timer definiert, wie lange ein Proxy in der Liste versucht wird, bevor er zum nächsten Proxy wechselt. Der Wert wird normalerweise 32 Sekunden verwendet (64*T1). Wenn alle IP-Adressen fehlschlagen, zeigt der Client einen Benutzeroberflächenfehler für die SIP-Konnektivität an. Wenn ein VoIP-Anruf während des Failovers ausgeführt wird, wird der Anruf beendet.

Die SIP-Failover-Logik basiert auf mehreren Konfigurationsparametern:

- SIP-Failover-Timer – Die SIP-Timer T1, T2 und T4 sind in der Konfigurationsdatei sichtbar, aber es wird nicht empfohlen, sie zu ändern.

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

  - T1 – die Zeitspanne in Millisekunden für eine Netzwerk-Roundtrip-Verzögerung.
  - T2 – die maximale Zeit in Millisekunden, bevor nicht eingeladene Anfragen und Antworten erneut gesendet werden.
  - T4 – Die maximale Zeit in Millisekunden, bis eine Nachricht im Netzwerk verbleibt.

- SIP-Proxyadresse und SIP-Proxyerkennung
  - Siehe Abschnitt *6.1.1SIP-Servereinstellungen*.



Cisco – vertraulich

- Siehe Abschnitt *6.1.6Dynamische SIP-Proxyerkennung*.

- Failover-Konfiguration registrieren (siehe unten)

Im Falle eines Failovers sendet die Webex-Anwendung SIP REGISTER mit zwei Kontakt-Headern – einen für die alte Sitzung und einen zweiten mit den neuen Geräteinformationen. Die Kontaktkopfzeile für die alte Sitzung enthält eine Benachrichtigung an den SBC, um die Daten zu bereinigen. Dieser Header umfasst expires=0 und q=0.5.

Der Kontakt-Header mit den neuen Geräteinformationen hat auch einen q-Wert, der aus dem <*q-value*> Tag gelesen wird. Der <*q-value*> Tag-Wert wird verwendet, um die Voreinstellung oder Priorität einer bestimmten Kontaktadresse anzugeben. Sie reicht von 0 bis 1,0, wobei 1,0 die höchste Präferenz und 0 die niedrigste ist. Dieses Tag hat kein benutzerdefiniertes Tag, um den Wert zu steuern - es ist auf 1.0 hardcodiert. Der Wert kann manuell angepasst werden, wenn der in der Bereitstellung verwendete SBC eine umgekehrte Logik aufweist und q=0.0 mit maximaler Priorität behandelt.

Ab Version 42.11 wird ein neuer <*register-failover*> Abschnitt in die Konfigurationsvorlage eingeführt. Es wird ein neuer konfigurierbarer Parameter <*Registration-Cleanup*> hinzugefügt, um zu steuern, ob die Anwendung den Kontakt-Header sendet, um die alten Geräteinformationen zu bereinigen, oder nicht. Einige SBCs bereinigen die alte Sitzung sofort beim Trennen des Sockets, sodass das Vorhandensein der Kontaktkopfzeile für die alte Sitzung nicht erforderlich ist. Standardmäßig ist die Registrierungsbereinigungslogik aktiviert.

Zur Konsistenz wird das <*q-value*> Tag auch unter denselben <*register-failover*> Abschnitt verschoben.

Beispiel:

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% | wahr | wahr, falsch | Steuert die Bereinigung der alten Geräteinformationen im Falle eines SIP-Failovers. |



Cisco – vertraulich

#### 6.1.8.2 SIP-Fehler

Wenn der Client mit einem Proxy verbunden ist, der nicht die erste Priorität hat, versucht er, die Verbindung zur IP mit der höchsten Priorität wiederherzustellen. Die Zeit für das Failback basiert auf der DNS TTL-Verwaltungskonfiguration (siehe Abschnitt *6.1.8.4DNS TTL-Verwaltung*). Wenn ein Anruf aktiv ist, wenn der Failback-Timer erreicht wird, wartet der Client, bis alle Anrufe abgeschlossen sind, und löst das Failback-Verfahren aus. Beachten Sie, dass dies nur für Desktop-Clients gilt, da die SIP-Verbindung nur während eines Anrufs auf einem Mobilgerät aktiv ist.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SIP_FAILBACK_ENABLED_WXT% | wahr | wahr, falsch | Aktiviert/deaktiviert das SIP-Failback. |
| %SIP_FAILBACK_TIMEOUT_WXT% | 900 | Über 60 | Die SIP-Failback-Zeitüberschreitung in Sekunden. |
| %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% | Falsch | wahr, falsch | Fügt eine zufällige Periode [0-10]% des SIP-Failbacks hinzu. |

#### 6.1.8.3 IP-Version erzwingen

Der Webex-Client kann konfiguriert werden, wie die Liste der aufgelösten Hosts über den DNS bestellt und im Falle eines SIP-Failovers dann über sie iteriert wird. In allen Modi wird die Priorität und das Gewicht respektiert.

Unterstützte Konfigurationen sind:

- dns – verwendet alle von den DNS-Abfragen zurückgegebenen Adressen
- ipv4 – filtert die IPv6-Adressen heraus
- ipv6 – filtert die IPv4-Adressen heraus
- prefer-ipv4 – bestellt die IPv4-Adressen vor dem IPv6 (Version 42.9)
- prefer-ipv6 – bestellt die IPv6-Adressen vor dem IPv4 (Version 42.9)
- nat64 – ignoriert die IPv6-Adressen, bestellt die IPv4-Adressen (Version 44.2)

Es wird empfohlen, den Standardwert (dns) zu verwenden, es sei denn, die Umgebung-/Netzwerkkonfiguration erfordert einen anderen Modus.

Mit „dns“-Konfiguration werden die IPv4-Adressen den IPv6-Adressen für den angegebenen Host vorgezogen. Wenn zwei Hosts mit IPv4- und IPv6-Adressen vorhanden sind, lautet die Reihenfolge IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

Im „prefer-ipv4“-Modus werden die IPv4-Adressen vor den IPv6-Adressen bestellt (die Reihenfolge innerhalb der IPv4- und IPv6-Gruppen bleibt bestehen)

*Beispiel:* IPv4(host1), IPv4(host2), IPv6(host1), IPv6(host2).



Cisco – vertraulich

Im Modus „prefer-ipv6“ ist die Reihenfolge umgekehrt – die IPv6-Adressen werden vor die IPv4-Adressen platziert.

*Beispiel:* IPv6(host1), IPv6(host2), IPv4(host1), IPv4(host2).

Im „nat64“-Modus – die IPv6-Adressen werden ignoriert, die IPv4-Reihenfolge wird eingehalten. Das IPv6-Präfix(e) wird bzw. werden erkannt. Für jede IPv4-Adresse wird eine Kombination mit jedem Pref64-Präfix und/oder Suffix erstellt.

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

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% | dns | ipv4<br>IPv6<br>dns<br>Bevorzugung-ipv4<br>Bevorzugung-ipv6<br>nat64 | Steuert die Reihenfolge der IPv4-/IPv6-Adressen, die vom Webex-Client zum Verbinden der SIP-Sitzung verwendet werden. |

#### 6.1.8.4 DNS TTL-Verwaltung

Es wurde ein separater Konfigurationsparameter hinzugefügt, mit dem die Wiederauflösung von DNS verwaltet werden kann, wenn die TTL des DNS-Datensatzes des aktuell verwendeten Servers abläuft. Wenn der Parameter in der folgenden Tabelle aktiviert ist, wird der Client gezwungen, DNS-Vorgänge erneut auszuführen, sobald die TTL des DNS SRV oder A-Datensatzes des aktuell verwendeten Servers abläuft.

Nachdem die DNS-Auflösung erneut hergestellt wurde, zwingt dieser Parameter den Client auch, sich erneut mit dem Server mit der höchsten Priorität zu verbinden, der empfangen wird, wenn er sich vom aktuell verwendeten Server unterscheidet, selbst wenn die aktuelle Verbindung vollständig funktioniert. Die erneute Verbindung wird jedoch erst nach Abschluss laufender Anrufe hergestellt.

Wenn sich die TTLs für Server-A- und SRV-Datensätze unterscheiden, wird der kleinere Wert ausgewählt.

Wenn dieser Parameter deaktiviert ist, werden DNS-Vorgänge nicht bei Ablauf von TTL, sondern alle 15 Minuten wiederholt.



Cisco – vertraulich

Dieser Parameter funktioniert nur für SIP.

Beachten Sie, dass die DNS TTL-Verwaltungsfunktion nicht verwendet werden kann, wenn im Proxy-Adressparameter eine IP-Adresse verwendet wird.

> **HINWEIS:** Dies ist eine reine Desktop-Funktion, da die mobilen Clients nur während eines Anrufs über eine SIP-Verbindung verfügen.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SIP_REFRESH_ON_TTL_WXT% | Falsch | falsch, wahr | Wenn „false“ festgelegt ist, ist die DNS-TTL-Verwaltung für SIP deaktiviert.<br>Wenn die Option auf „true“ festgelegt ist, ist die DNS TTL-Verwaltung für SIP aktiviert. |
| %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%" | Falsch | falsch, wahr | Wenn diese Option aktiviert ist, wird a zufälliger Zeitraum zwischen 0 und 10 % zur DNS-TTL hinzugefügt. |

> **HINWEIS:** Es wird dringend empfohlen, den DNS TTL-Zufallsfaktor zu aktivieren, um Spitzen von Anfragen an den DNS und potenzielle Spitzen von Wiederverbindungsversuchen an den Anwendungsserver zu verhindern.

### 6.1.9 SIP SUBCSRIBE und REGISTRIEREN Aktualisieren und SUBSCRIBE Wiederholen

Communicator unterstützt die Konfiguration der Aktualisierungsintervalle für das SIP-ABONNEMENT und die REGISTRIERUNG. Für SIP SUBSCRIBE gibt es einen separaten Parameter für das Aktualisierungsintervall (in Sekunden) und wie lange der Client wartet, bevor er SIP SUBSCRIBE erneut versucht, wenn Fehler auftreten (in Sekunden). Der empfohlene Höchstwert für das *Abonnement-Wiederholungsintervall* beträgt 2000000 Sekunden, während negative, 0 oder leere Werte in 1800 Sekunden verwendet werden. Jeder negative Wert für die Abonnement-Aktualisierung lässt den Header *Expires* aus und erstellt so ein einmaliges ABONNEMENT.

Der vom Client vorgeschlagene Aktualisierungs-Timer für die SIP-Registrierung kann in Sekunden konfiguriert werden, aber gemäß den SIP-Spezifikationen kann der Server den Wert überschreiben. Derzeit merkt sich der Client den vom Server vorgeschlagenen Wert für nachfolgende Aktualisierungen, anstatt immer den konfigurierten Wert zu verwenden.

Schließlich kann der Ablaufwert für SIP-Sitzungen (für SIP INVITE und SUBSCRIBE) auch konfiguriert werden (in Sekunden).



Cisco – vertraulich

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

### 6.1.10 P-zugeordnete URIs in REGISTER verwenden

Der folgende Parameter wird bei der Registrierung und Verarbeitung der zugehörigen *Antwort 200 OK* verwendet.

Wenn der Parameter auf „false“ festgelegt ist, verwendet der Client nicht den *P-Associated-URI* und verwendet stattdessen die Identität von seinem eigenen SIP-URI.

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

Wenn der Parameter auf „true“ gesetzt ist, dann nimmt der Client seine eigene Identität aus dem letzten *P-Associated-URI -Header* für alle ausgehenden SIP-Anfragen (INVITE, SUBSCRIBE, CANCEL, INFO und REFER) aus der *200 OK -Antwort* im REGISTER. Außerdem werden diese URIs nicht als Kontakte in der Kontaktliste angezeigt.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USE_ALTERNATIVE_IDENTITIES_WXT% | Falsch | wahr, falsch | Aktiviert die Verwendung alternativer Identitäten im SIP REGISTER.<br>Wenn „true“ festgelegt ist, übernimmt der Client seine eigene Identität aus dem letzten *P-Associated-URI -Header* für ausgehende SIP-Anfragen.<br>Wenn diese Option auf „false“ gesetzt ist, wird die eigene Identität für ausgehende SIP-Anfragen aus der eigenen SIP-URI übernommen. |

### 6.1.11 SIP P-Early Media (PEM)-Header

Der SIP *P-Early Media* (PEM)-Header kann beispielsweise in IMS-Umgebungen innerhalb einer Vertrauensdomäne verwendet werden, um dem Netzwerk zu ermöglichen, mehrere SIP-Early-Media-Dialoge zu autorisieren, z. B. in Fällen, in denen ein anderes Netzwerk alle Early Media zulässt.

Der Konfigurationsparameter aktiviert die Unterstützung von Werbe-PEM bei der SIP-Signalisierung. Die tatsächliche Logik für die Early-Media-Verarbeitung ist sowohl für PEM- als auch für Nicht-PEM-Fälle gleich und wird auf unterstützte PEM-Kopfzeilenwerte angewendet.



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_PEM_SUPPORT_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die PEM-Unterstützung für Client-Werbung in der SIP-Signalisierung zu aktivieren.<br>Legen Sie „false“ fest, um die Unterstützung von Client-Werbe-PEM in der SIP-Signalisierung zu deaktivieren. |

### 6.1.12 Unterstützung für SIP-UPDATE

SIP-UPDATE wird beispielsweise in einigen IMS-Bereitstellungen anstelle der alternativen erneuten EINLADUNG benötigt. Es ermöglicht einem Client, die Parameter einer Sitzung zu aktualisieren, z. B. den Satz der Medienstreams und ihrer Codecs, hat jedoch keine Auswirkungen auf den Status eines SIP-Dialogs.

Typische Anwendungsfälle stehen im Zusammenhang mit Early Media, wenn beispielsweise der Rückrufton und die Vorwarnung gleichzeitig verwendet werden.

SIP UPDATE wird derzeit nur unterstützt, wenn es in Anwendungsfällen vor dem Dialog (Early Media) empfangen wird, und nicht während des aktiven Dialogs, z. B. für Halten/Fortsetzen von Anrufen, bei denen re-INVITE weiterhin verwendet wird.

Es ist nicht möglich, mit SIP UPDATE (Medienänderung) in dieser Version Video zu Audio hinzuzufügen. Darüber hinaus unterstützt der Client keinen vollständigen IMS-Long-Call-Flow mit Ressourcenreservierung.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SIP_UPDATE_SUPPORT_WXT% | Falsch | wahr, falsch | Wenn „false“ festgelegt ist, ist die SIP-UPDATE-Unterstützung deaktiviert.<br>Wenn die Option auf „true“ festgelegt ist, ist die SIP-UPDATE-Unterstützung aktiviert. |



Cisco – vertraulich

### 6.1.13 Ältere SIP-INFO-FIR

Dieser Client unterstützt die ältere Methode zum Anfordern von Video-Keyframes über die SIP INFO-Mediensteuerungsanforderung. Dies ist erforderlich, da einige der Geräte Probleme damit haben, auf RTCP-FB-FIR zu reagieren, und RTCP gelegentlich nicht über einen Remote-Endpunkt geleitet wird, was zu keinem Video oder One-Way-Video führen kann. Weitere Informationen finden Sie unter *RFC 5168* .

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_FORCE_SIP_INFO_FIR_WXT% | Falsch | wahr, falsch | Wenn diese Option auf „false“ gesetzt ist, ist die SIP INFO FIR-Unterstützung deaktiviert.<br>Wenn diese Option auf „true“ gesetzt ist, ist die SIP INFO FIR-Unterstützung aktiviert. |

### 6.1.14 SIP rport Management für NAT Traversal

Der Client kann so konfiguriert werden, dass er den SIP-rport-Mechanismus für die NAT-Traversal verwendet. Beachten Sie, dass es in der Regel nicht die einzige Lösung für NAT-Traversal sein kann und SBC hauptsächlich für diesen Zweck verwendet wird. Eine Beschreibung der rport-Spezifikation finden Sie unter *RFC 3581* .

Weitere Informationen zu SIP-Port- und Transportprotokollempfehlungen, wenn SIP Application Layer Gateways (ALGs) im Netzwerk verwendet werden, finden Sie im *Webex for Cisco BroadWorks Solution Guide* .

Beachten Sie, dass die Zeichenfolge „rport“ unabhängig von der Konfiguration immer in ausgehenden SIP-Anfragen vorhanden ist. Der Parameter wirkt sich nur auf die Verwendung der IP-Adresse und des Ports aus, die vom Server in den Headern „received“ und „rport“ empfangen werden. Wenn die Funktion aktiviert ist, werden die Werte von „received“- und „rport“-Headern im SIP-Kontakt-Header von SIP-Anfragen verwendet (auch wenn der „received“-Header in der REGISTER-Antwort fehlt).

Der Parameter *Bevorzugter Port* bezieht sich darauf, dass er andernfalls den im SIP-Kontaktheader verwendeten Port definiert. Weitere Informationen zur SIP-Portzuweisung finden Sie im Abschnitt *6.1.7Bevorzugte Portnutzung für SIP*.

Es gibt einen separaten Konfigurationsparameter *use-local-port* , der die Einstellung des lokalen Ports des Client-Sockets im *Contact -Header* erzwingt. Dies wird für einige SBCs verwendet, die erkennen, dass der Client eine echte IP hat (aus dem *Contact -Header* ) und der SBC versucht, einen separaten Socket für den Client für seine Anforderungen zu erstellen. In den meisten Fällen befindet sich eine Firewall zwischen dem SBC und dem Client und verweigert die eingehenden Verbindungen zum Client.



Cisco – vertraulich

**HINWEIS:** In IPv6-Umgebungen sind alle Adressen real, und der SBC versucht, eine Verbindung zur Listening-Client-Adresse herzustellen (aus dem *Contact -Header* ).

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_USE_RPORT_WXT% | Falsch | wahr, falsch | Aktiviert den Rport für Audio- und Videoanrufe. |
| %RPORT_USE_LOCAL_PORT_WXT% | Falsch | wahr, falsch | Steuert, ob der lokale Port des Client-Sockets im SIP *Contact -Header* hinzugefügt werden soll. |

### 6.1.15 SIP-Sitzungs-ID

Wenn diese Option aktiviert ist, wird bei der erstmaligen Registrierung eine lokale Sitzungs-ID generiert. Die Sitzungs-ID wird für die Lebensdauer der Verbindung/Sitzung für dieses Gerät, für alle Dialogfelder außerhalb des Anrufs, REGISTRIEREN, ABONNIEREN, BENACHRICHTIGEN usw. verwendet. Dieselbe Sitzungs-ID wird verwendet, bis die Bindung getrennt wird. Wenn die Registrierungsbindung abgebrochen wird (DNS-Suche, Verbindungs-Reset, Telefon-Reset usw.), wird eine neue lokale Sitzungs-ID generiert.

Der Wert der Sitzungs-ID kann verwendet werden, um die vollständige Liste der mit diesem Gerät verknüpften Dialogfelder zu finden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SIP_SESSION_ID_WXT% | Falsch | wahr, falsch | Steuert die Verwendung der SIP-Sitzungs-ID. |

### 6.1.16 Ablehnungsverhalten eingehender Anrufe

Der Client bietet die Flexibilität, einen Anruf mit *486* oder *603 abzulehnen* .

Beachten Sie, dass die Dienste „Rufumleitung bei Besetzt“ und „Rufumleitung bei Nichtbeantwortung“ möglicherweise nicht wie erwartet funktionieren, wenn der Client so konfiguriert ist, dass ein Anruf mit *603 Ablehnen* abgelehnt wird.



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_REJECT_WITH_486_WXT% | wahr | wahr, falsch | Steuert den SIP-Fehlercode und den Grund für die Ablehnung eingehender SIP-Anrufe. Wenn diese Option aktiviert ist, *wird „486 vorübergehend nicht verfügbar“* verwendet. Andernfalls wird *603 Ablehnen* verwendet. |

### 6.1.17 Portbereich des Transportprotokolls in Echtzeit

Der Client kann so konfiguriert werden, dass er einen definierten Portbereich für RTP-Streams (Real-Time Transport Protocol) verwendet, der auch für SRTP gilt. Diese Konfiguration erfolgt, indem die Grenzwerte für den Portbereich für Audio- und Videostreams mit den im folgenden Beispiel gezeigten Tags festgelegt werden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %RTP_AUDIO_PORT_RANGE_START_WXT% | 8000 | Nummer | Start des Audioport-Bereichs. |
| %RTP_AUDIO_PORT_RANGE_END_WXT% | 8099 | Nummer | Ende des Audioport-Bereichs. |
| %RTP_VIDEO_PORT_RANGE_START_WXT% | 8100 | Nummer | Start des Video-Portbereichs. |
| %RTP_VIDEO_PORT_RANGE_END_WXT% | 8199 | Nummer | Ende des Video-Portbereichs. |

**HINWEIS:** Portbereiche sollten so festgelegt werden, dass sie sich nie überschneiden.



Cisco – vertraulich

### 6.1.18 ICE-Unterstützung (nur Webex Calling)

Der Client unterstützt die Aushandlung Interactive Connectivity Establishment ( ICE), die eine Medienpfadoptimierung zwischen Endpunkten ermöglicht (auf Peer-to-Peer-Weise). Dies geschieht, um die Latenz der Daten zu reduzieren, den Paketverlust zu reduzieren und die Betriebskosten der Bereitstellung der Anwendung zu reduzieren.

Beachten Sie, dass die aktuelle Implementierung STUN-Server unterstützt, während TURN nicht unterstützt wird.

Wenn die ICE-Unterstützung aktiviert ist, wird immer eine erneute Eingabe für SRTP durchgeführt (siehe Abschnitt *6.1.2SIP über TLS und sicheres Echtzeit-Transportprotokoll*).

Ab Version 44.5 unterstützt die Webex-App ICE über IPv6 mit NAT64.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_RTP_ICE_WXT% | Falsch | wahr, falsch | ICE-Unterstützung aktivieren/deaktivieren. |
| %RTP_ICE_MODE_WXT% | icestun | icestun | ICE-Unterstützungsmodus. Derzeit ist der einzige unterstützte Wert „icestun“. |
| %RTP_ICE_SERVICE_URI_WXT% | (leer) | gültiger STUN-Server-URI oder (leer) | STUN-Server-URI. |
| %RTP_ICE_PORT_WXT% | 3478 | Nummer ( 0 - 65535 ) | STUN-Serverport. |
| %ENABLE_RTP_ICE_IPV6_WXT% | Falsch | wahr, falsch | Aktiviert ICE über IPv6. |

### 6.1.19 RTCP-MUX

RTCP MUX ist konfigurierbar. Mit dieser Funktion verwendet der Client den gleichen Port für RTP und RTCP. Auf SIP-/SDP-Signalisierungsebene wird die Leitung a=rtcp-mux zum SDP hinzugefügt. Darüber hinaus sind verschiedene Modi möglich:

- Abwärtskompatibilitätsmodus (d. h. Zeile a=rtcp-mux wird nicht im SDP angezeigt)
- Multiplexmodus (die Zeile a=rtcp-mux wird im SDP zweimal angezeigt: einmal im Abschnitt m=Audio und ein zweites Mal im Abschnitt m=Video)

Video und Audio verwenden nicht den gleichen Port.

```
<config>
```



Cisco – vertraulich

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

Beachten Sie, dass RTCP MUX nicht mit SRTP-Anrufen verwendet werden kann.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_RTCP_MUX_WXT% | wahr | wahr, falsch | Um RTPC MUX zu aktivieren, legen Sie „true“ fest.<br>Um RTCP MUX zu deaktivieren, legen Sie „false“ fest. |

### 6.1.20 Transfer

Der Webex for Cisco BroadWorks-Client unterstützt betreute (beratende), semi-beratende und direkte (blinde) Anrufübergabe.

Mit der halbberatenden Anrufübergabe kann der Anrufer die Übergabe abschließen, bevor der Anruf von der anderen Person angenommen wird. Die halbberatende Abschlusstaste ist für den Anrufer erst aktiviert, nachdem auf der Anruferseite das Klingeln gestartet und die entsprechende SIP-Benachrichtigung ( *180 Klingeln*) auf der Anruferseite empfangen wurde. Die Übergabe ohne Rückfrage wird auf der Benutzeroberfläche als „Jetzt übergeben“ bezeichnet.

> **HINWEIS:** Das SIP *180 Klingeln* wird in einigen Umgebungen, bei einigen Nummern oder in einigen serverübergreifenden Kommunikationsszenarien möglicherweise nicht ausgelöst.

Version 43.9 der Webex-App führt die Übergabe an einen anderen eigenständigen laufenden Anruf desselben Typs ein. In der Webex-App beendete Anrufe können an andere Anrufe übertragen werden, die im lokalen Endpunkt beendet wurden. Und Anrufe, die auf einem Remote-Gerät beendet werden, können an Anrufe übergeben werden, die auf einem Remote-Endpunkt beendet werden. Diese Funktion verfügt nicht über konfigurierbare Optionen.

Ab Version 43.12 fügt die Webex-App eine Konfigurationsoption hinzu, mit der gesteuert werden kann, ob der aktuelle Anruf bei Auswahl des Menüelements „Übergabe“ automatisch gehalten werden soll. Dieses Verhalten wird durch das neue Attribut *auto-hold* gesteuert. Die automatische Halten-Funktion ist standardmäßig deaktiviert.

```
<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%"/>
```



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_TRANSFER_CALLS_WXT% | Falsch | wahr, falsch | Wenn „true“ festgelegt ist, ist die Anrufübergabe aktiviert.<br>Wenn „false“ festgelegt ist, ist die Anrufübergabe deaktiviert. |
| %ENABLE_XSI_TRANSFER_CALLS_WXT% | Falsch | wahr, falsch | Aktiviert Übertragungsoptionen für Remote-Anrufe (XSI), die an einem anderen Standort beendet wurden. |
| %TRANSFER_CALL_TYPE_WXT% | voll | talk-first, blind, voll | Gibt die für den Benutzer in der BroadWorks-Konfiguration verfügbaren Übergabetypen an. |
| %ENABLE_TRANSFER_AUTO_HOLD_WXT% | Falsch | wahr, falsch | Steuert, ob der aktive Anruf automatisch gehalten wird, wenn der Benutzer die Option „Übergabe“ aus dem Menü im Anruf auswählt. |

### 6.1.21 N-Wege-Konferenzanrufe und Teilnehmer

Das folgende benutzerdefinierte Tag kann verwendet werden, um die Verfügbarkeit des Ad-Hoc-Konferenzanrufs (N-Way) über SIP im Webex für Cisco BroadWorks-Client zu steuern. Darüber hinaus kann der N-Way-Besitzer die vollständige Liste der Teilnehmer über SIP SUBSCRIBE/NOTIFY und das Konferenzveranstaltungspaket anzeigen. Der Client des Besitzers lernt den URI, an den das SIP-ABONNEMENT über den vorangehenden SIP *Contact -Header* der *200 OK -Nachricht gesendet* wird, die als Antwort auf die INVITE-Nachricht an den Konferenz-URI gesendet wird, während für Teilnehmer dieselben Informationen in einer vorhergehenden Anrufinfo NOTIFY enthalten sind.

Die Cisco BroadWorks-Systemeinstellung ( *maxConferenceParties)* wird verwendet, um die maximale Anzahl von Konferenzparteien festzulegen. Für einen bestimmten Anruf gibt er die Anzahl aktiver gleichzeitiger Parteien an, die ein Benutzer über die Option „Teilnehmer hinzufügen“ zur Anrufsteuerung oder über die Cisco BroadWorks N-Way-Anruffunktion haben oder hinzufügen kann.

Diese Informationen werden über den Befehl Application Server (AS) über die Befehlszeilenschnittstelle (CLI) abgerufen.

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

Example output:
maxConferenceParties = 6
conferenceURI =
```

Nachdem Sie den Wert für *maxConferenceParties* erhalten haben (der einen Bereich von 4 bis 15 hat), sollte das Tag %MAX_CONF_PARTIES_WXT% entsprechend festgelegt werden.

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



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CONFERENCE_CALLS_WXT% | Falsch | wahr, falsch | Steuert, ob die Konferenzoption für den Benutzer aktiviert werden sollte. |
| %ENABLE_NWAY_PARTICIPANT_LIST_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die N-Wege-Eigentümer-Teilnehmerliste zu aktivieren.<br>Legen Sie „false“ fest, um die N-Wege-Eigentümer-Teilnehmerliste zu deaktivieren. |
| %MAX_CONF_PARTIES_WXT% | 10 | Nummer zwischen 4 und 15<br>(leer) | Gibt die maximale N-Wege-Teilnehmernummer an, die vom Client erzwungen wird, z. B. 10. Server-Seite hat ihre eigenen Grenzen.<br>Der leere Wert deaktiviert die clientseitige Durchsetzung der N-Wege-Teilnehmerbegrenzung. |

### 6.1.22 Anrufübergabe

Die Anrufabruffunktion kann mit einem einzigen Konfigurationsparameter aktiviert werden, wie im folgenden Beispiel gezeigt.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_PULL_WXT% | Falsch | wahr, falsch | Aktiviert die Anrufannahme. |

### 6.1.23 Anruf parken/abrufen

Mit der Funktion „Gruppenanruf parken“ können laufende VoIP-Anrufe an einen Server für geparkte Anrufe übergeben werden, sodass der Anrufer andere Aktionen ausführen und vom selben oder einem anderen Benutzer abgerufen werden kann. Ein laufender Anruf wird für den ersten verfügbaren Anschluss innerhalb der Gruppe zum Parken von Anrufen geparkt.



Cisco – vertraulich

Der Anrufabruf kann durchgeführt werden, indem der Benutzer den Anruf im Dialogfeld für eine konfigurierbare Anzahl von Sekunden direkt nach dem Parken des Anrufs parkt. Oder der geparkte Anruf kann durch den Benutzer oder einen anderen Benutzer abgerufen werden, indem Sie die Option „Anrufabruf“ auswählen und die Nummer oder den Anschluss eingeben.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_PARK_WXT% | Falsch | wahr, falsch | Aktiviert das Parken/Abrufen von Anrufen. |
| %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% | 10 | Nummer zwischen 5 und 30 | Gibt an, wie viele Sekunden das Dialogfeld „Geparkter Anruf“ für den Benutzer angezeigt wird, bevor es automatisch geschlossen wird. |

### 6.1.24 Anrufstatistik

Die Berichterstellung für End-of-Call-Statistiken in der SIP-BYE-Nachricht (Session Initiation Protocol) ermöglicht das Senden von Anrufstatistiken an ein Remote-Ende, wenn ein Anruf beendet wird. Die Anrufstatistiken werden als neuer Header in der SIP-BYE-Nachricht oder in der entsprechenden *200 OK -Antwort* auf die BYE-Nachricht gesendet. Die Statistiken umfassen gesendete oder empfangene RTP-Pakete (Real-time Transport Protocol), gesendete oder empfangene Bytes, Gesamtanzahl der verlorenen Pakete, verzögerter Jitter, Round-Trip-Verzögerung und Anrufdauer.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_STATISTICS_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die Erfassung von Anrufmetriken zu aktivieren.<br>Legen Sie „false“ fest, um die Erfassung von Anrufmetriken zu deaktivieren. |



Cisco – vertraulich

### 6.1.25 Automatische Anrufwiederherstellung / Nahtlose Anrufübergabe

Der Client unterstützt die automatische Wiederherstellung von Anrufen bei Netzwerkwechseln, während der Benutzer einen laufenden VoIP-Anruf führt. Die automatische Wiederherstellung von Anrufen funktioniert in beide Richtungen – Mobilfunkdaten und WLAN-Mobilfunkdaten sowie beim Wechsel zwischen WLAN-Netzwerken. Der Anruf wird innerhalb von einer Minute wiederhergestellt und anschließend beendet. Wenn mehrere VoIP-Anrufe aktiv sind, wird nur der aktive Anruf wiederhergestellt.

Beim Übergang von Mobilfunkdaten zu WLAN behält der Client die laufenden VoIP-Anrufe auf Mobilfunkdaten, bis sie beendet sind oder das Mobilfunknetz verloren geht.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALLS_AUTO_RECOVERY_WXT% | Falsch | wahr, falsch | Steuert, ob der automatische Wiederherstellungsmechanismus für den Benutzer aktiviert werden sollte. |

### 6.1.26 Anrufaufzeichnung

Die Anrufaufzeichnungsfunktion wird vom Client unterstützt und hängt von der serverseitigen Verfügbarkeit der Funktion sowie von der Konfigurationsoption ab. Die Funktion hängt vom aktivierten XSI-Ereigniskanal (siehe Abschnitt *6.1.33XSI-Ereigniskanal*) und vom Anwendungsserver (AS) ab, der so konfiguriert ist, dass *X-BroadWorks-Correlation-Info* SIP-Header gesendet wird (siehe *Webex for Cisco BroadWorks Solution Guide* ).

Wenn die Funktion deaktiviert ist, gibt es keine Aufzeichnungsschaltflächen und -optionen für den Benutzer. Beachten Sie, dass die Anrufaufzeichnung pro Benutzer und nicht pro Anruf erfolgt. Das bedeutet, dass der Anruf aufgezeichnet werden kann, wenn einer der Teilnehmer eines Anrufs die Anrufaufzeichnung unterstützt.

Wenn die Anrufaufzeichnungsfunktion aktiviert ist, wird immer ein visueller Hinweis angezeigt, wenn der Anruf aufgezeichnet wird. Die folgenden Anrufaufzeichnungsmodi werden von Cisco BroadWorks unterstützt:

**Immer**

- Die Anrufaufzeichnung wird bei der Einrichtung des Anrufs automatisch gestartet.
- Der Benutzer kann **die** Anrufaufzeichnung NICHT stoppen/anhalten.

**Unterstützung immer mit Pause/Wiederaufnahme**

- Die Anrufaufzeichnung wird bei der Einrichtung des Anrufs automatisch gestartet, aber der Benutzer kann den Anruf anhalten und fortsetzen.
- Mögliche Benutzerinteraktionen:



Cisco – vertraulich

- Aufzeichnung ist in Bearbeitung – **Aktion „** Aufzeichnung anhalten“.
- Aufzeichnung wird angehalten – Aktion **Aufzeichnung fortsetzen** .

**Auf Anfrage**

- Nachdem der Anruf eingerichtet wurde, wird die Anrufaufzeichnung auf dem Server gestartet.
- Wenn der Benutzer während des Anrufs die Option „Aufzeichnung starten“ drückt, wird die Anrufaufzeichnung gespeichert und der Anruf wird nicht gestartet. Andernfalls wird die Anrufaufzeichnung auf dem Server gelöscht, wenn vom Benutzer keine Startaufzeichnung gestartet wird.
- Mögliche Benutzerinteraktionen:
  - Es wurde noch keine Aufzeichnung gestartet – **Aktion „Aufzeichnung starten** “.
  - Aufzeichnung ist in Bearbeitung – **Aktion „** Aufzeichnung anhalten“.
  - Aufzeichnung wird angehalten – Aktion **Aufzeichnung fortsetzen** .

**Bei Bedarf mit vom Benutzer initiiertem Start**

- Der Benutzer kann die Anrufaufzeichnung jederzeit mehrmals während eines Anrufs starten, stoppen, anhalten und fortsetzen.
- Für jeden Start der Anrufaufzeichnung gibt es separate Anrufaufzeichnungen.
- Mögliche Benutzerinteraktionen:
  - Es wurde noch keine Aufzeichnung gestartet – **Aktion „Aufzeichnung starten** “.
  - Aufzeichnung läuft – Aktion **„Aufzeichnung beenden“** und „ **Pause“** .
  - Aufzeichnung wird angehalten – Aktion **Stop** und **Resume** Aufzeichnung.

Der dem Benutzer zugewiesene Anrufaufzeichnungsmodus kann über Control Hub ausgewählt werden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_RECORDING_WXT% | Falsch | wahr, falsch | Aktiviert Anrufaufzeichnungssteuerungen. |

### 6.1.27 Voicemail , Visuelle Voicemail, Briefkastenlampe

Die folgenden benutzerdefinierten Tags können verwendet werden, um die Verfügbarkeit von Cisco BroadWorks Voicemail und Visual Voicemail im Webex für Cisco BroadWorks-Client zu steuern. Beachten Sie, dass ein Cisco BroadWorks-System-Tag (%BWVOICE-PORTAL-NUMBER-1%) mit Voicemail verwendet wird.



Cisco – vertraulich

Visual Voicemail (VVM) wird nur für Audio unterstützt. Unterstützte Formate sind wav, ulaw und mov, die H264-Video enthalten (nur als Audio wiedergegeben). Es ermöglicht Benutzern, eingehende Voicemails in einer Listenansicht anzuzeigen, und einzelne Elemente können wiedergegeben werden. Diese Funktion basiert auf Xsi, aber Benachrichtigungen über neue Voicemails werden über SIP bereitgestellt. Daher muss SIP aktiviert sein, damit die Benachrichtigungen funktionieren. Darüber hinaus ist die Konfiguration von SIP SUBSCRIBE for Message Waiting Indicator (MWI) erforderlich, damit die Benachrichtigungen ankommen, und MWI muss aktiviert sein, damit die visuelle Voicemail funktioniert. Weitere Informationen zur SIP-Konfiguration finden Sie im Abschnitt *6.1.1SIP-Servereinstellungen*.

Informationen zu den Release- und Patch-Anforderungen für Cisco BroadWorks für Visual Voicemail finden Sie im
Lösungshandbuch *Webex für Cisco BroadWorks* .

Visual Voicemail muss in der Konfiguration separat aktiviert sein.

Die folgenden Einstellungen werden im CommPilot-Portal benötigt, um Visual Voicemail zu erhalten:

- Sprachnachrichten aktiviert
- Option „Wenn eine Nachricht eingeht, verwenden Sie Unified Messaging“ aktiviert
- Option „Anzeige für wartende Telefonnachrichten verwenden“ aktiviert

Wenn der Visual Voicemail-Dienst nicht auf Cisco BroadWorks-Seite für den Benutzer zugewiesen ist, wird die Konfiguration für den Dienst automatisch deaktiviert.

Beachten Sie, dass beim Deaktivieren der SIP-Registrierung auch MWI für neue Voicemails deaktiviert wird. Weitere Informationen zum Aktivieren von MWI finden Sie in der folgenden Tabelle.

Um Informationen zu Voicemail-Nachrichten auf der Benutzeroberfläche anzuzeigen, muss der Client SIP-MWI-Benachrichtigungen vom Server erhalten (d. h. das Voicemail-Ereignispaket). Informationen zu den Abonnementoptionen finden Sie in der folgenden Tabelle. Beachten Sie auch, dass MWI erforderlich ist, damit visuelle Voicemail-Benachrichtigungen funktionieren.

Wenn das SIP-Abonnement des Voicemail-Ereignispakets fehlschlägt, versucht der Client dies erneut, wenn er dafür konfiguriert ist. Weitere Informationen zur SIP-SUBSCRIBE-Wiederholungskonfiguration finden Sie im Abschnitt *6.1.9SIP SUBCSRIBE und REGISTRIEREN Aktualisieren und SUBSCRIBE Wiederholen.*

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



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_VOICE_MAIL_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die Voicemail-Unterstützung zu aktivieren.<br>Legen Sie „false“ fest, um die Voicemail-Unterstützung zu deaktivieren. |
| %ENABLE_VISUAL_VOICE_MAIL_WXT% | Falsch | wahr, falsch | Wenn „false“ festgelegt ist, ist VVM deaktiviert.<br>Wenn „true“ festgelegt ist, ist VVM aktiviert.<br>Beachten Sie, dass Voicemail=false aktiviert ist, bevor das tatsächliche VVM-Attribut weiterhin zur Abwärtskompatibilität verwendet wird. |
| %BWVOICE-PORTAL-NUMBER-1% | leer | Nummer | Der Client ruft diese Nummer an, die normalerweise mit einem vorhandenen Cisco BroadWorks-Systemtag beim Wählen der Voicemail angegeben wird. |
| %ENABLE_MWI_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um MWI zu aktivieren.<br>Legen Sie „false“ fest, um MWI zu deaktivieren. |
| %MWI_MODE_WXT% | leer | implizit, explizit | Legen Sie „explizit“ fest, um SIP-ABONNEMENT für MWI-Ereignispaket zu senden, wenn MWI aktiviert ist.<br>Die Verwendung von „implizit“ sendet kein SIP-ABONNEMENT für MWI-Ereignispaket, wenn MWI aktiviert ist.<br>Wenn das Feld leer gelassen wird, ist MWI deaktiviert. |

### 6.1.28 Voicemail-Transkription für Webex Calling

Mit dieser Funktion werden Voicemail-Nachrichten in Text umgewandelt und in der visuellen Voicemail-Nachrichtenansicht in den Webex Calling-Desktop- und mobilen Apps angezeigt.

Die Funktion sollte nur für Benutzer aktiviert werden, wenn:

1. Die App wird in der Webex Calling-Bereitstellung ausgeführt.
2. Die visuelle Voicemail-Funktion ist für den Benutzer aktiviert.
3. Die Funktion ist in der Konfiguration aktiviert (das Attribut "enabled" im Tag <services><voice-mail><transcription> sollte auf "true" gesetzt werden).



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% | Falsch | wahr, falsch | [Nur Webex Calling] Steuert die Verfügbarkeit der Voicemail-Transkription nur, wenn die visuelle Voicemail aktiviert ist. |

### 6.1.29 Anrufeinstellungen

#### 6.1.29.1 Immer Rufumleitung

Das folgende benutzerdefinierte Tag kann verwendet werden, um die Verfügbarkeit des Dienstes „Cisco BroadWorks-Rufumleitung immer“ im Webex für Cisco BroadWorks-Client zu steuern.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_FORWARDING_ALWAYS_WXT% | Falsch | wahr, falsch | Steuert die Verfügbarkeit des Dienstes „Rufumleitung immer“.<br>Die Funktion ist standardmäßig deaktiviert. |

**HINWEIS:** Die Funktion „Rufumleitung immer“ und „Rufumleitung an Voicemail“ (*6.1.29.2Anrufweiterleitung an Voicemail*) können zusammen verwendet werden, um die Einstellung „Rufumleitung“ in den Webex-Apps anzuzeigen oder auszublenden. Wenn beide Tags deaktiviert sind, wird die Einstellung „Rufumleitung“ in den Webex-Apps ausgeblendet.

#### 6.1.29.2 Anrufweiterleitung an Voicemail

Ab Version 43.9 bietet die Webex-App eine Option zum Steuern der Verfügbarkeit der Weiterleitung an Voicemail. Standardmäßig ist die Funktion aktiviert und kann mit der folgenden Konfigurationsoption deaktiviert werden.

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



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_VOICE_MAIL_FORWARDING_WXT% | wahr | wahr, falsch | Steuert die Verfügbarkeit der Weiterleitung an Voicemail.<br>Die Funktion ist standardmäßig aktiviert. |

**HINWEIS 1:** Diese Funktion hängt von einem der „Voice Messaging-Benutzer"- oder „Voice Mail Support von Drittanbietern"-Dienste ab, die dem Benutzer zugewiesen werden sollen.

**HINWEIS 2:** Anrufweiterleitung an Voicemail und Rufumleitung immer (*6.1.29.1Immer Rufumleitung*) können zusammen verwendet werden, um die Einstellung „Anrufweiterleitung" in den Webex-Apps anzuzeigen oder auszublenden. Wenn beide Tags deaktiviert sind, wird die Einstellung „Rufumleitung" in den Webex-Apps ausgeblendet.

### 6.1.29.3 BroadWorks Anywhere (Erreichbarkeit unter einer Rufnummer)

Die folgenden benutzerdefinierten Tags steuern die Verfügbarkeit von BroadWorks Anywhere und die Verfügbarkeit der Einstellungen im Webex für Cisco BroadWorks-Client. Beachten Sie, dass der Name dieser Funktion im Client „ *Meine Nummern verwalten" lautet*.

```
<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>
```

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_BROADWORKS_ANYWHERE_WXT% | Falsch | wahr, falsch | Aktiviert BroadWorks Anywhere (BWA) auf Konfigurationsebene. |
| %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% | wahr | wahr, falsch | Steuert, ob die Beschreibung des BWA-Standorts für den Benutzer verfügbar sein sollte. |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um Alle Standorte für den BWA-Dienst für den Benutzer verfügbar zu machen.<br>Legen Sie „false“ fest, um Alle Standorte darauf hinzuweisen, dass der BWA-Dienst für den Benutzer nicht verfügbar ist. |
| %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% | Falsch | wahr, falsch | Steuert, ob die Anwendung den Status „Alle Standorte warnen“ aktivieren soll, wenn ein zweiter oder jeder weitere neue BWA-Standort hinzugefügt wird. |
| %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% | Falsch | wahr, falsch | Steuert, ob die Anrufsteuerung des BWA-Standorts für den Benutzer verfügbar sein sollte. |
| %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% | Falsch | wahr, falsch | Steuert den Standardstatus der Anrufsteuerung für den BWA-Standort. |
| %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% | Falsch | wahr, falsch | Steuert, ob der Umleitungshemmer des BWA-Standorts für den Benutzer verfügbar sein sollte. |
| %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% | Falsch | wahr, falsch | Steuert den Standardstatus des Umleitungsinhibitors des BWA-Standorts. |
| %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% | Falsch | wahr, falsch | Steuert, ob die Antwortbestätigung des BWA-Standorts für den Benutzer verfügbar sein sollte. |
| %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% | Falsch | wahr, falsch | Steuert den Standardstatus der Antwortbestätigung des BWA-Standorts. |

### 6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen

Der Webex für Cisco BroadWorks-Client bietet Zugriff auf ein Einstellungsportal (Self-Service), in dem der Benutzer einige der Anwendungs- und Diensteinstellungen konfigurieren kann.

Darüber hinaus bietet der Client die Möglichkeit, stattdessen die Webansicht „Anrufeinstellungen“ (CSWV) zu verwenden. Dadurch kann der Benutzer mehr serverbasierte Anrufeinstellungen steuern. Separate Tags können verwendet werden, um zu steuern, ob bestimmte Dienste in den webbasierten Anrufeinstellungen sichtbar sein sollen.

> **HINWEIS:** Es empfiehlt sich, die Einstellungen auszublenden, die bereits in der Anwendung angezeigt werden, z. B. Callcenter (siehe Abschnitt *6.1.31Anmeldung/Abmeldung bei Callcenter/Anrufwarteschlange*) und BroadWorks Anywhere (siehe Abschnitt *6.1.29.3BroadWorks Anywhere* ). Der Remote Office-Dienst sollte ebenfalls ausgeblendet werden, da er durch den BroadWorks Anywhere-Dienst erfolgreich war.



Cisco – vertraulich

Das folgende benutzerdefinierte Tag kann verwendet werden, um die URL für das Einstellungsportal (Self-Service oder CSWV) zu konfigurieren. Wenn das Tag leer ist, wird der Link zum Einstellungsportal für den Benutzer in der Anwendung nicht angezeigt.

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



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %WEB_CALL_SETTINGS_TARGET_WXT% | extern | extern, csw | Steuert den Administratorportal-Modus.<br>Legen Sie „extern“ fest, um die konfigurierte Einstellungsportal-URL in einem externen Browser zu öffnen.<br>Legen Sie „csw“ fest, um das CSW-Portal in einem eingebetteten Browser zu öffnen. Verwenden Sie dazu den Abschnitt <services><web-call-settings>, um die POST-Anforderung zu erstellen. |
| %WEB_CALL_SETTINGS_URL_WXT% | leer | URL-Zeichenfolge | URL für das Einstellungsportal.<br>Beispiel: https://settings .webex.com |
| %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Rufumleitung immer“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. |
| %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Bitte nicht stören“ in den webbasierten Einstellungen für den Benutzer sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option zum Ablehnen anonymer Anrufe (Anonymous Call Rejection, ACR) für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die CFB-Option (Call Forwarding Busy) für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Rufumleitung nicht erreichbar“ für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Keine Antwort für Rufumleitung“ für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Persönliches Simultandolmetschen“ (SIMRING) für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option "Sequentieller Rufton (SEQRING)" für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. |
| %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option Remote Office (RO) für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option Automatischer Rückruf (ACB) für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Anklopfen“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. |
| %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Calling Line ID Delivery Blocking (CLIDB)-Option für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Persönlicher Assistent“ (PA) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. |
| %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die BroadWorks Anywhere (BWA)-Option für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte. |
| %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Call Center-Option für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. |
| %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option BroadWorks Mobility (BWM) für den Benutzer in den webbasierten Einstellungen sichtbar sein sollte.<br>Der empfohlene Wert ist derzeit aufgrund von Interoperabilitätsproblemen zwischen Webex für Cisco BroadWorks und BroadWorks Mobility „falsch“. |
| %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Option „Sprachverwaltung“ (VM) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. |
| %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% | Falsch | wahr, falsch | Steuert, ob das neue Branding für Anrufeinstellungen in WebView verwendet werden soll. Aktivieren Sie diese Option, wenn die serverseitige CSWV-Version 1.8.6 oder höher ist. Andernfalls halten Sie es falsch. |
| %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% | wahr | wahr, falsch | Steuert, ob die Optionen für E-Mail-/Voicemail-Nachrichten in den webbasierten Einstellungen angezeigt werden. |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USER_PORTAL_SETTINGS_URL_WXT% | leer | URL-Zeichenfolge | Gibt die URL für das Benutzereinstellungsportal an. Um die Funktion zu aktivieren und die Schaltfläche „Zugriffbenutzerportal“ in der Benutzeroberfläche anzuzeigen, sollte dieses benutzerdefinierte Tag nicht leer sein. Zum Beispiel: https://settings.webex.com. |
| %USER_PORTAL_SETTINGS_TARGET_WXT% | extern | extern, intern | Gibt an, ob die URL in einem eingebetteten oder externen Browser geöffnet werden soll. |
| %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% | Falsch | wahr, falsch | Gilt nur, wenn der eingebettete Browser konfiguriert ist (USER_PORTAL_SETTINGS_TARGET_WXT=intern). Wenn diese Option aktiviert ist, wird die HTTP POST-Anforderung verwendet und das BroadWorks-Kurzzeit-Token wird als Teil des BODYS hinzugefügt. Wenn diese Option deaktiviert ist, wird die URL mit HTTP GET geöffnet. |

**ANMERKUNG 1 <UNK>** : Die WebView-URL für Anrufeinstellungen sollte immer eine Nachspur „/“ konfiguriert haben. Zum Beispiel: http(s)://<XSP-FQDN>/<CSW-Context-Path>/

**ANMERKUNG 2 <UNK>** : Die unterstützte Mindestversion der WebView-Anwendung „Anrufeinstellungen“ ist 1.7.5.

Informationen zur Installation auf Cisco BroadWorks Version 21.0 finden Sie in den zusätzlichen Schritten, die im *Lösungshandbuch zu BroadWorks BroadWorks beschrieben sind*.

### 6.1.31 Anmeldung/Abmeldung bei Callcenter/Anrufwarteschlange

Die Webex-App bietet Zugriff auf die Agenteneinstellungen für das Callcenter (Anrufwarteschlange). Wenn ein Benutzer für Call Center bereitgestellt ist, ermöglicht diese Funktion dem Benutzer, sich bei einem Callcenter anzumelden und die verfügbaren Anrufwarteschlangen anzuzeigen sowie Warteschlangen beizutreten/aufzuheben und den Status der automatischen Anrufverteilung (ACD) festzulegen.

Ab Desktop Version 42.8 und Mobile Version 42.12 basiert der Call Center-Agent (Anrufwarteschlange) nicht mehr auf der Webansicht der Anrufeinstellungen (siehe Abschnitt *6.1.30Einstellungsportal und webbasierte Anrufeinstellungen*). Auf die Konfiguration des Call Center-Agenten (Anrufwarteschlange) kann über die Fußzeile des Desktops und die Einstellungen der mobilen Webex-App zugegriffen werden.

```
<config>
<services>
```



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_CENTER_WXT% | Falsch | wahr, falsch | Aktiviert die Call Center-Unterstützung. |

### 6.1.32 XSI-Wurzel und -Pfade

Der Webex für Cisco BroadWorks-Client verwendet die folgenden Tags, um den XSI-Stamm, Aktionen und Ereignispfad zu steuern, wenn sie so konfiguriert werden müssen, dass sie von den für die Anmeldung verwendeten Tags abweichen.

Der Hauptgrund für die Änderung des XSI-Stammes ist die Implementierung des Lastausgleichs auf Konfigurationsebene, obwohl es empfohlen wird, stattdessen den Lastausgleich auf der HTTP-Ebene zu verwenden.

Die Events- und Actions-Pfade werden normalerweise aufgrund von Branding-Anforderungen geändert, um die *Domänenreferenz com.broadsoft* aus den URL-Pfaden der XSI-HTTP-Anforderungen des Clients zu entfernen.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %XSI_ROOT_WXT% | Verwendet weiterhin das ursprüngliche für den Konfigurationsabruf. | URL-Zeichenfolge | Die XSI-Wurzel für alle XSI-Operationen.<br>Beispiel: https://domain .com/ |
| %XSI_ACTIONS_PATH_WXT% | /com.broadsoft.xsi-actions/ | Zeichenfolge | Gibt den Pfad für XSI-Aktionen an.<br>Sie sollte mit „/“ beginnen und enden und nur den Aktionskontext enthalten.<br>Beispiel: /com.domain.xsi-actions/ |
| %XSI_EVENTS_PATH_WXT% | /com.broadsoft.xsi-events/ | Zeichenfolge | Gibt den XSI Events-Pfad an.<br>Sie sollte mit „/“ beginnen und enden und nur den Ereigniskontext enthalten.<br>Beispiel: /com.domain.xsi-events/ |



Cisco – vertraulich

### 6.1.33 XSI-Ereigniskanal

Der XSI-Ereigniskanal wird für verschiedene Dienste verwendet, wie:

- XSI-Anrufsteuerungen
- Statusbenachrichtigungen zu Anrufeinstellungen
- Anrufaufzeichnung

XSI Events Heartbeat wird verwendet, um den XSI Event-Kanal offen zu halten, und das Heartbeat-Intervall kann mit dem folgenden Parameter angegeben werden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_XSI_EVENT_CHANNEL_WXT% | wahr | wahr, falsch | Steuert, ob der XSI-Ereigniskanal aktiviert ist. Es sollte auf „true“ festgelegt werden, um z. B. dienstbezogene Ereignisse während der Anrufsteuerung zu empfangen.<br>Der empfohlene Wert ist „true“. |
| %CHANNEL_HEARTBEAT_WXT% | 10000 | Nummer | Dies ist der XSI-Ereigniskanal-Heartbeat (in Millisekunden).<br>Der Standardwert ist „10000“. |

### 6.1.34 Codec-Konfiguration

Webex für Cisco BroadWorks bietet eine Vielzahl von Audio- und Video-Codecs. Die entsprechenden Codecs-Listen befinden sich unter *config/services/calls/* in den Abschnitten *audio/codecs* und *video/codecs* . Die Priorität der einzelnen Codec kann über das *XML-Attribut priority* , geändert werden, das einen Wert zwischen 0.0 (niedrigsten) und 1.0 (höchsten) darstellt.

Die Webex-App unterstützt offiziell die folgenden Codecs:

- Audio
  - Opus
  - G.722
  - G.729
  - PCMU (G.711U)
  - PCMA (G.711A)
  - iLBC
- Video



Cisco – vertraulich

- H.264



Cisco – vertraulich

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

Der Client unterstützt H.264 als Video-Codec. Mit dem Attribut „Videoauflösung“ können Sie einen der folgenden verfügbaren Werte festlegen: SUBQCIF, QCIF, CIF, 4CIF, VGA und HD.

Wenn die Bitrate nicht in der Konfiguration eingegeben wird, werden die Standardbitratenwerte verwendet. Die Standardbitratenwerte pro Auflösung und Bildrate sind in der folgenden Tabelle aufgeführt.

| Auflösung | Videogröße * | FPS (Rahmen pro Sekunde) | Standard-Bitratenwerte pro Auflösung und FPS |
|---|---|---|---|
| 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 |

***** Maximale angekündigte Videoauflösung. Die tatsächliche Videoauflösung während eines Anrufs zwischen zwei Webex für Cisco BroadWorks-Clients hängt von den Funktionen beider Clients ab – sie ist die niedrigere der beiden Clients und die gleiche für beide Clients.

Die Videoauflösung für einen Videoanruf wird während der Sitzungseinrichtung ausgehandelt und basiert auf den Funktionen der beiden Endpunkte. Die Videoanruf-Auflösung ist auf beiden Endpunkten gleich. Das heißt, wenn die Webex für Cisco BroadWorks-Endpunkte unterschiedliche Funktionen haben (und daher unterschiedliche Auflösungen unterstützen), wird die niedrigere Auflösung für den Anruf ausgehandelt. Die Videoauflösung kann sich während eines Anrufs ändern, wenn sich die Netzwerkbedingungen verschlechtern. In diesem Fall verwenden die beiden mobilen Endpunkte möglicherweise unterschiedliche Videoauflösungen.

Der Paketisierungsmodus kann so konfiguriert werden, dass er SingleNAL (0) oder Non-interleaved (1) ist. Die Vorlage verwendet standardmäßig SingleNAL (<Paketmodus>0</Paketmodus>).



Cisco – vertraulich

Die Konfiguration mehrerer Telefonereignisse wird ebenfalls unterstützt. Während der Codec-Verhandlung sendet der Client alle konfigurierten Codecs, einschließlich mehrerer Telefonereignisse. Nachdem der Audio-Codec ausgewählt wurde, sucht er nach Telefonereignissen im Angebot. Wenn das Angebot das Telefonereignis mit der Abtastrate des ausgehandelten Audio-Codecs enthält, wird dieses Telefonereignis ausgewählt. Andernfalls wird das erste Telefonereignis in der Liste verwendet. Gibt es überhaupt keine telefonischen Veranstaltungen im Angebot, kommen In-Band-Dual-Tone-Multi-Frequenzen (DTMFs) zum Einsatz.

Beispiel für konfigurierte Codecs:

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

Wenn ein Audio-Codec mit einer Abtastrate von 48 Kbit/s ausgehandelt wird, wird das Telefonereignis mit Nutzlast 101 verwendet.

### 6.1.35 SIP-URI-Wahl

Derzeit ist das SIP-URI-Wählen über BroadWorks nicht verfügbar und standardmäßig werden alle SIP-URI-Anrufe über Locus weitergeleitet, auch bekannt als „Free Calling“. In einigen Umgebungen ist dies nicht wünschenswert und solche Anrufe sollten blockiert werden.

**HINWEIS:** Dies gilt nur, wenn Locus Calling deaktiviert ist. Nur in diesem Fall funktioniert die Blockierung der SIP-URI-Wahl.

Die folgende Konfiguration bietet diese Option.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% | wahr | wahr, falsch | Steuert, ob der SIP-URI über Locus (true) geroutet oder blockiert (false) werden soll. |

### 6.1.36 Anrufprotokoll auf allen Geräten

Der Client bietet die Möglichkeit, das Anrufprotokoll vom Server zu speichern und abzurufen, anstatt es lokal zu speichern. Auf diese Weise wird das Anrufprotokoll auf allen Geräten vereinheitlicht.



Cisco – vertraulich

**HINWEIS:** Das einheitliche Anrufprotokoll sollte gleichzeitig auf Client- und Serverseite aktiviert sein, um fehlende Anrufprotokolle oder doppelte Datensätze zu vermeiden.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_UNIFIED_CALL_HISTORY_WXT% | Falsch | wahr, falsch | Steuert, ob die Anwendung ein einheitliches Anrufprotokoll oder ein clientseitiges (lokales) verwenden sollte. |

### 6.1.37 Videoanrufe deaktivieren

In Version 41.9 wurde die Möglichkeit zum Deaktivieren von Videoanrufen hinzugefügt. Es gibt separate Konfigurationsoptionen, um diese Funktion für BroadWorks-unterstützte und Locus (kostenlose) VoIP-Anrufe zu steuern.

Wenn die Funktion aktiviert und das Feature-Tag auf „false“ festgelegt ist:

- Der Benutzer sieht die Einstellung „Eingehende Anrufe mit eingeschaltetem Video annehmen“ nicht.
- Alle eingehenden Videoanrufe (falls angenommen) sind Audioanrufe
- der Benutzer einen Anruf nicht an ein Video eskalieren kann und Videoeskalationen automatisch abgelehnt werden

Wenn Videoanrufe aktiviert sind, wird eine neue Konfigurationseigenschaft hinzugefügt, um den Standardwert der Einstellung „Eingehende Anrufe mit eingeschaltetem Video annehmen“ zu steuern. Diese Funktion ist standardmäßig für den Desktop AKTIVIERT und für Mobilgeräte und Tablets DEAKTIVIERT.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SIP_VIDEOCALLS_WXT% | wahr | wahr, falsch | Steuert die Verfügbarkeit von SIP-Videoanrufen über BroadWorks. |
| %ENABLE_LOCUS_VIDEOCALLS_WXT% | wahr | wahr, falsch | Steuert die Verfügbarkeit von Locus-Videoanrufen (kostenlos). |
| %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% | Desktop – wahr<br>Mobil / Tablet - falsch | wahr, falsch | Steuert den Standardwert der Einstellung „Eingehende Anrufe mit eingeschaltetem Video annehmen“. |



Cisco – vertraulich

### 6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter

Der Desktop- und Tablet-Webex-Client unterstützt E911-Standortberichte mit RedSky, Intrado oder Bandbreite als E911-Notrufanbieter für die Webex for BroadWorks-Bereitstellung. Der E911-Anbieter bietet Standortunterstützung pro Gerät (für Webex-Desktop- und Tablet-Apps und HELD-fähige MPP-Geräte) und ein Netzwerk, das Notrufe nur an PSAPs (Public Safety Answering Points) in den USA, ihren Territorien (Guam, Puerto Rico und Jungferninseln) und Kanada weiterleitet. Der Dienst wird auf Standortbasis aktiviert.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% | Falsch | wahr, falsch | Aktiviert die Emergency Location Platform des E911-Anbieters. |
| %BWE911-PRIMARY-HELDURL% | leer | Zeichenfolge | Gibt die URL zur Emergency Location Platform des E911-Anbieters an, die das HELD-Protokoll unterstützt. |
| %BWE911-CUSTOMERID% | leer | Zeichenfolge | Die für die HTTPS-Anforderung des E911-Anbieters verwendete Kunden-ID (HeldOrgId, CompanyID). |
| %BWE911-SECRETKEY% | leer | Zeichenfolge | Das Geheimnis zur Authentifizierung der HTTPS-Anforderung des E911-Anbieters. |
| %BWE911-EMERGENCY-NUMBER-LIST% | leer | CSV-Zeichenfolge | Die Liste der Notrufnummern, die vom E911-Anbieter unterstützt werden. |
| %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% | 0 (Benutzer wird nicht erneut aufgefordert) | Nummer [0 - 43200] | Die Zeitüberschreitung in Minuten, die verwendet wird, um den Benutzer daran zu erinnern, den Notfallstandort zu aktualisieren, wenn der aktuelle Standort nicht eingegeben wurde oder ungültig ist.<br>Der vorgeschlagene Wert, wenn die Option aktiviert ist: 1440 (einen Tag). |
| %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% | -1 (der Benutzer kann den Dialog immer abbrechen) | Zahl [-1 - 100] | Die Zeiten, zu denen der Benutzer den Standortdialog schließen darf, bevor der Standort obligatorisch wird (d. h., er kann das Standortfenster nicht schließen).<br>Mögliche Werte:<br>▪ N = -1 (der Benutzer kann den Dialog immer abbrechen)<br>▪ N = 0 (Benutzer darf Dialogfeld nicht abbrechen – obligatorischer Standort immer)<br>▪ N > 0 (der Benutzer kann den Dialog N mal abbrechen, bevor er obligatorisch wird) |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT% | aggressiv, once_per_login | einmal_pro_login | Definiert das Aufforderungsverhalten des E911-Standorts. Der „aggressive“ Wert zeigt den Dialog für den Benutzer bei jeder Netzwerkänderung an einen unbekannten Ort an, während der Wert „once_per_login“ den Dialog nur einmal anzeigt, um weiteres Popup und Ablenkungen für den Benutzer zu verhindern. |

**ANMERKUNG 1 <UNK>** : BWE911-***-Tags sind „Dynamic Built-in System Tags“. Weitere Informationen finden Sie im Abschnitt *5.7Dynamische, integrierte System-Tags in Cisco* BroadWorks.

**ANMERKUNG 2 <UNK>** : Wenn VOIP-Anrufe deaktiviert sind, ist der einzige aussagekräftige Wert für die Notrufsequenz (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) „cs-only“.

### 6.1.39 PAI als Identität

Für **eingehende Anrufe** steuert dieser neue Parameter die Priorität der SIP-From- und P-Asserted-Identity (PAI)-Header und was als Anrufleitungs-Identität verwendet werden soll. Wenn ein X-BroadWorks-Remote-Party-Info-Header in der eingehenden SIP INVITE vorhanden ist, wird er mit Priorität vor den SIP From- und PAI-Headern verwendet. Wenn im eingehenden SIP INVITE kein X-BroadWorks-Remote-Party-Info-Header vorhanden ist, bestimmt dieser neue Parameter, ob der SIP-From-Header Vorrang vor dem PAI-Header hat oder umgekehrt.

Wenn das aktivierte Attribut des <use-pai-as-calling-identity>-Tags auf „true“ festgelegt ist, wird der PAI-Header mit Priorität vor dem From-Header verwendet. Diese Anrufer-Identität wird verwendet, um den Kontakt aufzulösen und dem Benutzer zu präsentieren.

Für **ausgehende Anrufe** wird diese Logik nicht angewendet. Bei 18X-200 OK-Antworten wird die Identität der verbundenen Leitung empfangen, sodass die Webex-Anwendung immer den SIP PAI-Header mit Priorität verwendet.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %USE_PAI_AS_CALLING_IDENTITY_WXT% | Falsch | wahr, falsch | Steuert, ob die dem Benutzer angezeigte Anrufidentität aus dem SIP-From- oder SIP-P-Asserted-Identity-Header übernommen werden sollte. Legen Sie „true“ fest, um den PAI-Header mit Priorität zu verwenden. |



Cisco – vertraulich

### 6.1.40 Bildschirmfreigabe deaktivieren

Version 42.5 bietet die Möglichkeit, die Verfügbarkeit der Bildschirmfreigabe zu steuern. Wenn die Bildschirmfreigabe deaktiviert ist:

- dem Benutzer wird die Option zum Initiieren der Bildschirmfreigabe in 1-1 Anrufen nicht angezeigt
- eingehende Teilen von Bildschirminhalten-Anforderungen werden abgelehnt, und dem Benutzer wird eine informative Nachricht angezeigt

Diese Funktion ist standardmäßig aktiviert.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SCREEN_SHARE_WXT% | wahr | wahr, falsch | Gibt an, ob die Bildschirmfreigabe für den Benutzer aktiviert werden soll. |

### 6.1.41 Anzeige von Spam-Anrufen

Wenn der Funktionsumschalter (pro Bereitstellungstyp) aktiviert ist und die Funktion in der Konfigurationsdatei aktiviert ist, verarbeitet die Webex-App den neuen Parameter, der den Status der Spam-Anrufverifizierung angibt, wenn diese als Teil der NewCall Push-Benachrichtigung oder des Anrufprotokolls empfangen werden.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALLS_SPAM_INDICATION_WXT% | Falsch | wahr, falsch | Steuert nur die Verfügbarkeit der Spam-Anrufanzeige im Bildschirm für eingehende Anrufe und im Anrufprotokoll für Webex Calling. |

### 6.1.42 Geräuschunterdrückung und Bandbreitenerweiterung für PSTN/Mobile-Anrufe

Die Geräuschunterdrückung bietet Anrufern ein besseres Anruferlebnis, wenn sie mit Nicht-Webex-Benutzern auf PSTN oder Mobilgeräten sprechen. Ab Version 43.12 ist die Geräuschunterdrückung standardmäßig aktiviert.

In Version 44.2 der Webex-App werden neue KI-Verbesserungen für die Audio-Medien-Sprache für Schmalband-PSTN-Anrufe eingeführt.

- Ein neuer Algorithmus zur Bandbreitenerweiterung wird hinzugefügt, um die Audioqualität zu verbessern, indem die Bandbreite des Schmalband-PSTN-Spektrums erweitert und das Rauschen entfernt wird. Die erweiterte Bandbreite verbessert die Verständlichkeit und verringert die Ermüdung beim Zuhören.



Cisco – vertraulich

- Der bereits vorhandene Geräuschunterdrückungsalgorithmus wurde verbessert, wodurch die Einschränkungen für die Warteschleifenmusik und andere Audiotöne (z. B. Piepsignale) beseitigt werden.
- Wenn diese Funktion aktiviert ist, sieht der Benutzer den Indikator „Intelligentes Audio – extern“ und kann die Sprach-KI-Verbesserungen für die eingehenden Audiomedien steuern.

Diese Sprachverbesserungen sind standardmäßig aktiviert und aktiviert. Der Benutzer kann den Anfangsstatus über die intelligenten Audioeinstellungen in den Audioeinstellungen steuern.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SPEECH_ENHANCEMENTS_WXT% | Falsch | wahr, falsch | Aktiviert die Sprachverbesserungen für externe (eingehende) Medien. |

**HINWEIS:** Die Rauschunterdrückung ist jetzt Teil der zusätzlichen Sprachverbesserungen, und das Tag <Geräuschunterdrückung> wurde durch das neue Tag <Sprachverbesserungen> eingestellt. Das benutzerdefinierte Tag % ENABLE_NOISE_REMOVAL_WXT% zur Rauschunterdrückung ist ebenfalls veraltet.

### 6.1.43 QoS DSCP-Markierung

Die QoS DSCP-Markierung wird mit den RTP-Paketen für Anrufmedien der Webex-App (Audio und Video) unterstützt. DSCP bestimmt die Datenverkehrsklassifizierung für Netzwerkdaten. Dies kann verwendet werden, um zu bestimmen, welcher Netzwerkverkehr eine höhere Bandbreite erfordert, eine höhere Priorität hat und Pakete wahrscheinlicher fallen lässt.

**HINWEIS:** Aktuelle Versionen des Microsoft Windows-Betriebssystems erlauben Anwendungen nicht, DSCP oder UP für ausgehende Pakete direkt festzulegen, sondern erfordern die Bereitstellung von Gruppenrichtlinienobjekten (GPO), um DSCP-Markierungsrichtlinien basierend auf UDP-Portbereichen zu definieren.

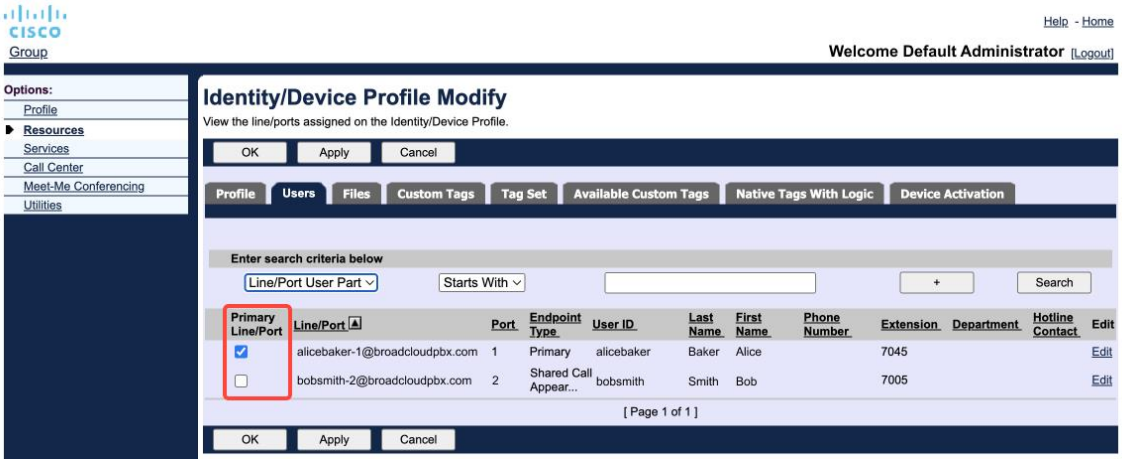


Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_AUDIO_QOS_WXT% | wahr | wahr, falsch | Aktiviert QoS für Audioanrufe. |
| %AUDIO_QOS_VALUE_WXT% | 46 | 0–63 | Gibt den QoS-Wert für den ausgewählten QoS-Typ für Audioanrufe an.<br>Hinweis: Der Standardwert wird verwendet, wenn kein Wert angegeben wurde oder der Wert nicht erfolgreich analysiert werden konnte. |
| %ENABLE_VIDEO_QOS_WXT% | wahr | wahr, falsch | Aktiviert QoS für Videoanrufe |
| %VIDEO_QOS_VALUE_WXT% | 34 | 0–63 | Gibt den QoS-Wert für den ausgewählten QoS-Typ für Videoanrufe an.<br>Hinweis: Der Standardwert wird verwendet, wenn kein Wert angegeben wurde oder der Wert nicht erfolgreich analysiert werden konnte. |

### 6.1.44 Primäres Profil

Mit der Integration der gemeinsam genutzten Leitungen (*6.2.12Mehrere Leitungen – Darstellung gemeinsam genutzter Leitungen*) kann es, wenn die Leitung des Benutzers mit einem anderen Benutzer geteilt wird, mehrere Profile desselben Typs geben, die für den Benutzer konfiguriert sind. Um das richtige Profil für die Anmeldung bei den Telefondiensten auszuwählen, wurde Cisco BroadWorks erweitert, um anzugeben, ob ein Benutzer ein Gerät besitzt, d. h., ihm wird die primäre Leitung/der primäre Port für ein Gerät zugewiesen. Weitere Informationen zum Cisco BroadWorks-Update finden Sie unter Eigentümermarkierung in der Geräteliste, um gemeinsam genutzte Webex-Client-Leitungen zu unterstützen .



Konfiguration der primären Leitung/des Ports für Identität/Geräteprofil im Administratorportal



Cisco – vertraulich

Ab Version 43.2 wird eine neue Konfigurationsoption ( *device-owner-restriction* ) hinzugefügt, um zu steuern, ob die primäre Profilbeschränkung angewendet werden soll. Sie kann verwendet werden, damit sich die Webex-Anwendung über ein nicht primäres Leitungs-/Portprofil bei den Telefondiensten anmelden kann. Diese Konfigurationsoption wird für alle Konfigurationen angewendet, unabhängig von der Anzahl der für den Benutzer konfigurierten Profile ( **Wenn die Gerätebesitzbeschränkung aktiviert ist und es kein Gerät mit primärer Leitung/Port für die entsprechende Plattform gibt, werden die Telefondienste keine Verbindung herstellen**).

Dieselbe Einschränkung gilt für die Geräte, mit denen der Benutzer in der Webex-Desktop-App koppeln kann. Der Benutzer kann nur Geräte sehen und koppeln, die er besitzt. Dies verhindert die Kopplung mit Geräten eines anderen Benutzers, der eine gemeinsam genutzte oder virtuelle Leitung zugewiesen hat. Der Wert desselben Konfigurationsparameters gilt auch für diese Einschränkung.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% | wahr | wahr, falsch | Steuert die Beschränkung des Geräteeigentümers – wenn die Telefondienste das primäre Profil für das jeweilige Gerät verwenden sollten |

**HINWEIS:** Es wird empfohlen, die Beschränkung des Besitzers zu aktivieren. Wenn diese Option deaktiviert ist, verwenden die Telefondienste das erste gefundene Profil für die Anmeldung, und einige Probleme können auftreten, wenn für den Benutzer desselben Typs mehrere Profile konfiguriert sind.

### 6.1.45 Sperrliste (nur Webex Calling)

Ab Version 43.5 führt die Webex-App eine benutzerdefinierte Sperrliste mit Telefonnummern ein. Wenn die Funktion aktiviert ist, kann der Benutzer eingehende Anrufe von bestimmten Nummern angeben, die serverseitig blockiert und auf keinem der Geräte des Benutzers zugestellt werden sollen. Benutzer können diese blockierten Anrufe im Anrufprotokoll anzeigen.

Der Benutzer kann die Sperrliste an zwei Orten konfigurieren: Anrufvoreinstellungen und Anrufprotokoll. In den Einstellungen kann der Benutzer die Liste der blockierten Nummern sehen und bearbeiten. Im Anrufprotokoll können Benutzer die Anrufprotokolldatensätze für die Anrufe anzeigen, die von der benutzerdefinierten Sperrliste blockiert werden. Diese Datensätze haben Blockiert, wenn sich die Nummer in der benutzerdefinierten Sperrliste befindet und der Benutzer die Möglichkeit hat, die Nummer direkt für einen bestimmten Datensatz zu entsperren. Die Option „Blockieren“ ist ebenfalls verfügbar.

Regeln für die Nummern, die der benutzerdefinierten Sperrliste hinzugefügt werden:

- Nummernformat



Cisco – vertraulich

- Das Blockieren der Anrufeinstellungen wendet lokal in der Webex-App Einschränkungen im E.164-Format an.
- Blockieren aus dem Anrufprotokoll ist für alle Webex Calling-Datensätze zulässig
- Cisco BroadWorks kann Anfragen für neue Nummern, die basierend auf dem Zahlenformat in der Sperrliste hinzugefügt werden, zulassen oder ablehnen

■ Interne Nummern – eingehende Anrufe von internen Nummern werden an den Benutzer weitergeleitet, auch wenn sie Teil der benutzerdefinierten Sperrliste sind

Die benutzerdefinierte Sperrliste wird in Cisco BroadWorks konfiguriert und auf alle WxC-Geräte für den Benutzer angewendet. Diese Funktion funktioniert mit der vom Administrator definierten Sperrliste, die vom Benutzer nicht konfiguriert werden kann und nur von den Administratoren über den Control Hub gesteuert werden kann. Es gibt KEINE Anrufprotokolldatensätze für eingehende Anrufe, die von der vom Administrator definierten Sperrliste blockiert werden.

Die benutzerdefinierte Sperrliste wird nach den Richtlinien STIR/SHAKEN, admin-definierte Sperrliste und anonyme Anrufablehnung angewendet.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_BLOCK_WXT% | wahr | wahr, falsch | Aktiviert die benutzerdefinierte Sperrliste<br>Auf „true“ festlegen, um die Sperrliste in den Anrufeinstellungen und im Anrufprotokoll anzuzeigen |

**HINWEIS:** Diese Funktion hängt davon ab, ob der Cisco BroadWorks-Anrufsperrdienst dem Benutzer zugewiesen wird.

### 6.1.46 Medienanpassung und Resilienzimplementierung (MARI)

#### 6.1.46.1 Anpassung der Rate

Die Webex-Anwendung hat bereits adaptive Techniken für die Medienqualität integriert, um sicherzustellen, dass Audio nicht von einem Videopaketverlust betroffen ist, und um sicherzustellen, dass Video die Anpassung der Videorate nutzen kann, um die Menge der während einer Überlastung verwendeten Bandbreite zu verwalten.

Anpassung der Rate oder Anpassungen der dynamischen Bitrate passen die Anrufübertragungsrate an die verfügbare variable Bandbreite an, wodurch die Video-Bitrate basierend auf der Paketverlustbedingung reduziert oder beschleunigt wird. Ein Endpunkt reduziert die Bitrate, wenn er Nachrichten vom Empfänger empfängt, die darauf hinweisen, dass ein Paketverlust vorliegt. Sobald sich der Paketverlust verringert hat, wird die Bitrate beschleunigt.



Cisco – vertraulich

Es gibt keine konfigurierbaren Einstellungen, um die Verwendung des Ratenanpassungsmechanismus zu steuern.

#### 6.1.46.2 Forward Error Correction (FEC) und Packets Retransmission (RTX)

Ab Version 43.4 unterstützt die Webex-App den Medienanpassungsmechanismus bei der Fehlerkorrektur bei der Weiterleitung (Forward Error Correction, FEC) und der Paketneuransmission (RTX) für Audio- und Videomedien.

FEC bietet Redundanz für die übermittelten Informationen unter Verwendung eines vorgegebenen Algorithmus. Die Redundanz ermöglicht es dem Empfänger, eine begrenzte Anzahl von Fehlern zu erkennen und zu korrigieren, ohne den Absender nach zusätzlichen Daten fragen zu müssen. FEC bietet dem Empfänger die Möglichkeit, Fehler zu korrigieren, ohne dass ein umgekehrter Kanal (z. B. RTCP) erforderlich ist, um eine erneute Übertragung von Daten anzufordern. Dieser Vorteil geht jedoch zu Lasten einer festen höheren Kanalbandbreite (mehr gesendete Pakete).

Die Endpunkte verwenden FEC nicht auf Bandbreiten unter 768 Kbit/s. Außerdem muss es mindestens 1,5 % Paketverlust geben, bevor FEC eingeführt wird. Endpunkte überwachen normalerweise die Wirksamkeit von FEC, und wenn FEC nicht effizient ist, wird es nicht verwendet.

FEC verbraucht mehr Bandbreite als die Wiederübertragung, hat aber weniger Verzögerung. RTX wird verwendet, wenn geringe Verzögerung zulässig ist und Bandbreitenbeschränkungen vorliegen. Bei großer Verzögerung und ausreichender Bandbreite ist FEC vorzuziehen.

Die Webex-App wählt je nach ausgehandelter Bandbreite und Verzögerungstoleranz für einen bestimmten Medienstrom dynamisch RTX oder FEC aus. FEC führt aufgrund redundanter Videodaten zu einer höheren Bandbreitennutzung, aber es verursacht keine zusätzliche Verzögerung bei der Wiederherstellung verlorener Pakete. RTX trägt nicht zu einer höheren Bandbreitennutzung bei, da die RTP-Pakete nur dann erneut übertragen werden, wenn der Empfänger den Paketverlust im RTCP-Feedback-Kanal anzeigt. RTX führt eine Verzögerung bei der Paketwiederherstellung ein, da das RTCP-Paket den Empfänger vom Absender erreicht und das erneut übertragene Paket den Empfänger vom Absender erreicht.

FEC muss aktiviert sein, damit RTX aktiviert ist.

```
<config><services><calls>
<audio>
       <audio-quality-enhancements>
              <mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                             <payload>111</payload>
                             <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <m>8</m>
                             <multi_ssrc>1</multi_ssrc>
                             <non_seq>1</non_seq>
                             <feedback>0</feedback>
                            <order>FEC_SRTP</order>
                     </fec>
                      <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
                             <payload>112</payload>
                             <time>180</time>
```



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_AUDIO_MARI_FEC_WXT% | Falsch | wahr, falsch | Aktiviert FEC für Audioanrufe |
| %ENABLE_AUDIO_MARI_RTX_WXT% | Falsch | wahr, falsch | Aktiviert RTX für Audioanrufe (erfordert aktivierten Audio-FEC) |
| %ENABLE_VIDEO_MARI_FEC_WXT% | Falsch | wahr, falsch | Aktiviert FEC für Videoanrufe |
| %ENABLE_VIDEO_MARI_RTX_WXT% | Falsch | wahr, falsch | Aktiviert RTX für Videoanrufe (erfordert aktivierte Video-FEC) |

### 6.1.47 Gleichzeitige Anrufe mit demselben Benutzer

Unterstützung für gleichzeitige Anrufe mit demselben Benutzer auf einem Gerät.

Diese Funktion ist für einige Bereitstellungen nützlich, bei denen die angezeigte Identität des Anrufs nicht mit der verbundenen Identität übereinstimmt. Dies führt zu der Unfähigkeit, eine betreute Übergabe an die ursprüngliche Partei einzuleiten. Wenn Sie diese Funktion aktivieren, kann der Benutzer mehrere gleichzeitige Anrufe mit demselben Remote-Teilnehmer bearbeiten.

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



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% | Falsch | wahr, falsch | Gibt an, ob die Webex-App nur einen oder mehrere WxC-Anrufe mit demselben Benutzer haben kann. |

### 6.1.48 RTCP-XR

Ab Version 43.8 fügt die Webex-App die Verhandlung für den RTCP-XR-Paketaustausch während eines Anrufs hinzu. Die Verhandlung findet während der Einrichtung der SIP INVITE-Sitzung statt. Wenn beide Endpunkte RTCP-XR-Pakete unterstützen, beginnt die Webex Media Engine mit dem Austausch dieser Pakete und unterstützt den adaptiven Anrufqualitätsmechanismus. Diese Funktion ist standardmäßig aktiviert.

Außerdem werden diese zusätzlichen Metriken nur für Webex Calling über das SIP BYE gesendet und auf diese Weise in Control Hub offengelegt.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_RTCP_XR_NEGOTIATION_WXT% | wahr | wahr, falsch | Ermöglicht die RTCP-XR-Verhandlung und den Paketaustausch für eine bessere Anrufqualität.<br>Standardmäßig aktiviert. |

### 6.1.49 Informationen zur Anrufweiterleitung

In Version 44.2 der Webex-App wird eine konfigurierbare Option eingeführt, mit der die Sichtbarkeit der Informationen zur Anrufweiterleitung und Umleitung in den anrufbezogenen Bildschirmen und im Anrufprotokoll gesteuert werden kann.

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



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% | wahr | wahr, falsch | Steuert die Sichtbarkeit der Informationen zur Anrufweiterleitung und Umleitung.<br>Legen Sie „true“ fest, um die Informationen in den anrufbezogenen Bildschirmen und im Anrufprotokoll anzuzeigen. |

**HINWEIS:** Diese Funktion erfordert, dass die Umleitungsinformationen (Umleitung oder Verlaufsinformationen) auf der Cisco BroadWorks-Seite aktiviert sind.

### 6.1.50 Anrufer-ID

#### 6.1.50.1 Ausgehende Anrufer-ID (nur Webex Calling)

Die Apps Webex Mobile (Version 44.2) und Desktop (Version 44.3) bieten dem Benutzer eine neue Möglichkeit, die bevorzugte externe Anrufer-ID für ausgehende Anrufe auszuwählen. Die Liste der verfügbaren Optionen umfasst:

- Direktdurchwahl (Standard)
- Standortnummer
- Benutzerdefinierte Nummer aus derselben Organisation
- Anrufwarteschlangen, zu denen der Benutzer gehört, sodass Agenten ihre Anrufer-ID-Nummer verwenden können
- Sammelanschlüsse, zu denen der Benutzer gehört, sodass Agenten ihre Anrufer-ID-Nummer verwenden können
- Anrufer-ID ausblenden

Notizen:

- Nur Webex Calling
- Die Liste der Optionen hängt von der Leitung ab:
  - Hauptleitung – vollständiger Satz von Optionen
  - Gemeinsam genutzte Leitungen – nicht verfügbar
  - Virtuelle Leitungen – nur Anrufwarteschlangenoptionen
- Wenn die bereits ausgewählte Identität nicht mehr verfügbar ist, wird die Standard-Anrufer-ID des Benutzers verwendet.
- Notrufe verwenden immer die Rückrufnummer für den Notfall des Benutzers
- <Tag für ausgehende Anrufe> unter Abschnitt <Dienste><Callcenter-Agent> veraltet



Cisco – vertraulich

Die Liste der verfügbaren Optionen kann über das Administratorportal konfiguriert werden. Es gibt auch separate DMS-benutzerdefinierte Tags, um die Verfügbarkeit dieser Verbesserungen in der Webex-App zu steuern.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CLID_OUTGOING_CALLS_WXT% | Falsch | wahr, falsch | Aktiviert die Auswahl der ID-Nummer der anrufenden Leitung für ausgehende Anrufe. |
| %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% | Falsch | wahr, falsch | Steuert die Verfügbarkeit der zusätzlichen Nummern, die für den Benutzer konfiguriert sind. |
| %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% | Falsch | wahr, falsch | Steuert die Verfügbarkeit der für den Benutzer konfigurierten DNIS-Nummern (Call Center). |
| %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% | Falsch | wahr, falsch | Steuert die Verfügbarkeit der für den Benutzer konfigurierten Sammelanschlussnummern. |
| "%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% | Falsch | wahr, falsch | Aktiviert die Anrufer-ID-Zustellungsblockierung als Auswahl für ausgehende Anrufe. |

**HINWEIS:** Die Desktop-App-Version 44.3 unterstützt nur Call Center CLID und 44.4 bietet zusätzliche Unterstützung für die restlichen Optionen.

#### 6.1.50.2 Name der Remote-Anrufer-ID

Beim Empfang/Initiieren eines Anrufs sendet Cisco BroadWorks den Anzeigenamen des Remoteteilnehmers in der SIP-EINLADUNG. Sie wird standardmäßig von der Webex-App verwendet. Gleichzeitig startet die Webex-App die Kontaktauflösung für mehrere Quellen mit der folgenden Priorität:

- Gemeinsame Identität (CI)
- Kontaktdienst (benutzerdefinierte Kontakte)
- Outlook-Kontakte (Desktop)
- Lokales Adressbuch (mobil)



Cisco – vertraulich

Im Falle einer erfolgreichen Kontaktauflösung gegen eine der Suchquellen wird der Anzeigename der Remoteteilnehmer aktualisiert. Wenn der Kontakt in CI gefunden wird, ist die Anrufsitzung mit den Webex Cloud-Diensten desselben Benutzers verknüpft und bietet die Option zum Anzeigen des Avatars und der Präsenz der Remoteteilnehmer, zum Chatten, zur Bildschirmfreigabe, zur Eskalation zu einem Webex Cloud-Meeting usw.

Version 44.5 der Webex-App fügt eine konfigurierbare Option hinzu, um die Kontaktauflösung zu ignorieren und immer den Cisco BroadWorks-Anzeigenamen für Anrufe mit Arbeitsbereichen oder RoomOS-Geräten beizubehalten, die für einen 1:1-Cisco BroadWorks-Anruf verwendet werden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %CLID_REMOTE_NAME_MACHINE_MODE_WXT% | gelöst | aufgelöst, sip | Steuert den Anzeigenamen des Remote-Teilnehmers für Arbeitsbereiche und RoomOS-Geräte. Verwenden Sie „sip“, um die Kontaktauflösung zu ignorieren und den Anzeigenamen zu verwenden, der in der SIP INVITE-Sitzung empfangen wurde. |



Cisco – vertraulich

## 6.2 Nur Desktop-Funktionen

### 6.2.1 Erzwungene Abmeldung

Mit dieser Funktion kann Cisco BroadWorks Online-Client-Instanzen mit demselben Gerätetyp verfolgen und nur eine davon kann gleichzeitig online sein. Wenn Cisco BroadWorks den Client benachrichtigt, sich abzumelden, wird die SIP-Verbindung beendet, und der Client zeigt an, dass der Anruf nicht verbunden ist.

Diese Funktion wird in einigen Bereitstellungen benötigt, in denen ähnliche Clients ansonsten gleichzeitig online sein können, was Nebenwirkungen verursacht. Ein Beispiel ist ein Benutzer mit einem Desktop-Computer am Arbeitsplatz und zu Hause, bei dem die eingehenden Anrufe nur von einem der Clients empfangen würden, je nachdem, welche SIP-Registrierung aktiv ist.

Das erzwungene Abmelden basiert auf SIP. Der Client sendet ein SIP-ABONNEMENT an das *call-info* Event-Paket mit einem speziellen *appid-Wert* im *From* Header, unabhängig vom *bsoft-call-info* -Parameterwert. Wenn Cisco BroadWorks mehrere Client-Instanzen online mit derselben *ID erkennt*, sendet es eine spezielle SIP NOTIFY an die ältere Client-Instanz, wodurch es sich abmeldet. Desktop-Clients hätten beispielsweise einen identischen *appid-Wert* , obwohl es keine Einschränkung hinsichtlich der Verwendung dieses Bezeichners auf der Client-Seite gibt. Der *appid-Wert* wird vom Serviceanbieter konfiguriert.

Beachten Sie, dass für die erzwungene Abmeldung das SIP *Call-Info -Abonnement* aktiviert sein muss.

Weitere Informationen zu den Cisco BroadWorks-Patches und -Versionen, die für diese Funktion erforderlich sind, finden Sie im Abschnitt zu den Cisco BroadWorks-Softwareanforderungen im *Lösungshandbuch für Webex für Cisco BroadWorks*.

Im folgenden Beispiel finden Sie Konfigurationsdetails (SIP ist das einzige unterstützte Steuerungsprotokoll in dieser Version).

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_FORCED_LOGOUT_WXT% | Falsch | wahr, falsch | Erzwungenes Abmelden. |
| %FORCED_LOGOUT_APPID_WXT% | leer | Zeichenfolge | Appid, das auf der Serverseite für die Korrelation verwendet wird. Dies kann eine beliebige Zeichenfolge sein.<br>Beispiel: „123abc“ |



Cisco – vertraulich

### 6.2.2 Anrufübernahme

Die Anrufübernahme ist ein Dienst für mehrere Benutzer, mit dem ausgewählte Benutzer jede klingelnde Leitung in ihrer Anrufübernahmegruppe annehmen können. Eine Anrufübernahmegruppe wird vom Administrator definiert und ist eine Teilmenge der Benutzer in der Gruppe, die die Anrufe der anderen annehmen können.

Die folgenden Anrufübernahmefälle werden unterstützt:

- Anrufübernahme ohne Rückfrage
- Gezielte Anrufübernahme (d. h. ein Benutzer kann einen Anruf annehmen, der an ein anderes Telefon in seiner Gruppe weitergeleitet wird, indem er den entsprechenden Funktionscode und anschließend die Durchwahl des klingelnden Telefons wählt).

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_PICKUP_BLIND_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die Anrufübernahme ohne Rückfrage zu aktivieren. |
| %ENABLE_CALL_PICKUP_DIRECTED_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die gezielte Anrufübernahme zu aktivieren. |

### 6.2.3 Unterstützung von Chef-Administratoren (Führungskraft-Assistent)

Der Boss-Admin, die Funktion „Führungskraft-Assistent“ in Cisco BroadWorks, ermöglicht es einem Assistenten, im Auftrag einer Führungskraft zu arbeiten, um Anrufe als „Führungskraft“ zu filtern, anzunehmen und zu tätigen. Ein Assistent kann viele Führungskräfte haben und es ist möglich:

- Wählen Sie die gewünschte Rolle aus, wenn Sie einen Anruf tätigen.
- Nehmen Sie einen eingehenden Anruf im Namen einer Führungskraft an und leiten Sie den Anruf an die Führungskraft weiter. Darüber hinaus sind alle üblichen Anrufverwaltungsoptionen verfügbar.
- Sehen Sie, dass ein eingehender Anruf tatsächlich für die Führungskraft bestimmt ist.

Executive und Executive-Assistant sind zwei miteinander verbundene Cisco BroadWorks-Dienste, die zusammen die folgenden Funktionen bereitstellen:

- Ein Benutzer mit dem Dienst „Führungskraft“ kann einen Pool von Assistenten definieren, die ihre Anrufe verwalten. Die Assistenten müssen unter den Benutzern in derselben Gruppe oder demselben Unternehmen ausgewählt werden, denen der Dienst „Führungskraft-Assistent“ zugewiesen ist.



Cisco – vertraulich

- Ein Benutzer mit dem Dienst Führungskraft-Assistent kann Anrufe im Namen seiner Führungskräfte annehmen und initiieren.
- Sowohl die Führungskraft als auch ihre Assistenten können festlegen, welche Anrufe an die Assistenten weitergeleitet werden sollen, wie Assistenten über eingehende Anrufe benachrichtigt werden sollen und welche der an die Assistenten weitergeleiteten Anrufe der Führungskraft zur Überprüfung vorgelegt werden sollen.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_EXECUTIVE_ASSISTANT_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die Boss-Admin-Funktion zu aktivieren. |

**HINWEIS:** Die Funktion Boss-Admin (Executive-Assistant) wird in Kombination mit Shared-Lines nicht unterstützt.

### 6.2.4 Eskalieren von SIP-Anrufen an Meeting (nur Webex Calling)

Der Client bietet die Funktion zum Eskalieren eines laufenden SIP-Anrufs zu einem Meeting über Webex Calling. Wenn der Benutzer diese Funktion anstelle einer Standard-Ad-hoc-Konferenz verwendet, kann er während des Meetings sowohl Video als auch Bildschirmfreigabe verwenden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die Menüoption „An Webex Meeting eskalieren“ zu aktivieren. |

### 6.2.5 Anrufe über das Tischtelefon steuern – Automatische Anrufannahme

Mit der automatischen Anrufannahme kann der Benutzer die Desk Phone Control (DPC) für ausgehende Anrufe auf dem Client verwenden, um MPP-Telefone mit Zero-Touch-Anrufannahme zu verwalten.

Das ausgewählte MPP-Telefon überträgt das Audio/Video für den ausgehenden DPC-Anruf.



Cisco – vertraulich

Die automatische Anrufannahme kann auf den primären und nicht primär bereitgestellten Geräten funktionieren. Wenn der Benutzer mehr als ein registriertes Tischtelefon hat, mit dem gekoppelt werden kann, muss nur das ausgewählte/gekoppelte Gerät die automatische Anrufannahme durchführen.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% | wahr | wahr, falsch | Wenn die Option auf „true“ festgelegt ist, wird die automatische Anrufannahme für die Steuerung des Tischtelefons aktiviert. |

**HINWEIS:** Die automatische Anrufannahme wirkt sich nicht auf eingehende Anrufe im DPC-Modus aus, sodass das Tischtelefon bei eingehenden Anrufen klingelt.

### 6.2.6 Automatische Anrufannahme mit Tonbenachrichtigung

Diese Funktion ermöglicht die automatische Unterstützung der Anrufannahme für lokale Geräte, wenn dies in der Anforderung für eingehende Anrufe angezeigt wird.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_AUTO_ANSWER_WXT% | Falsch | wahr, falsch | Wenn „true“ festgelegt ist, wird die automatische Anrufannahme aktiviert, wenn dies vom Backend angefordert wird. |

### 6.2.7 Steuerung des Tischtelefons – Steuerung mittlerer Anrufe – Konferenz

Diese Funktion aktiviert Konferenz- und Zusammenführungsoptionen für Remote-Anrufe (XSI), die an einem anderen Standort beendet werden.



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_XSI_CONFERENCE_CALLS_WXT% | Falsch | wahr, falsch | Wenn die Option auf „true“ festgelegt ist, werden die Konferenz- und Zusammenführungsoptionen für Remote-Anrufe (XSI) aktiviert, die an einem anderen Standort beendet werden. |

### 6.2.8 Benachrichtigungen zur Anrufübernahme

Benachrichtigungen zur Anrufübernahme ermöglichen es dem Benutzer zu erfahren, wann ein Anruf an einen Benutzer eingeht, den er für die Überwachung konfiguriert hat. Anrufübernahme-Benachrichtigungen können für Watchlisten empfangen werden, die über die Dienste Anrufübernahmegruppe und Besetztlampenfeld konfiguriert wurden.

Benachrichtigungen zur Anrufübernahme sind nützlich, wenn sich die überwachten Benutzer nicht physisch nahe beieinander befinden und das Klingeln des Telefons ihres Kollegen nicht hören können.

#### 6.2.8.1 Besetztlampenfeld

Die Desktop-Webex-Anwendung zeigt eine Benachrichtigung an, wenn ein Mitglied in seiner Besetztlampenfeld-Watchlist einen eingehenden Anruf im Benachrichtigungsstatus hat. Die Benachrichtigung enthält Informationen über den Anrufer und den Benutzer, der den eingehenden Anruf empfangen hat, mit den Optionen, um den Anruf anzunehmen, die Benachrichtigung stummzuschalten oder zu ignorieren. Durch die Annahme des eingehenden Anrufs durch den Benutzer wird eine gezielte Anrufübernahme eingeleitet.

Ab Version 43.4 ist die Liste der vom Besetztlampenfeld überwachten Benutzer im Fenster für mehrere Anrufe (MCW) für Anrufe verfügbar (nur für Windows verfügbar). Die Integration der Besetztlampenfeld-Liste in MCW umfasst Folgendes:

- Überwachen Sie die eingehenden Anrufe mit der Option, den Anruf anzunehmen oder die Warnung zu ignorieren.
- Sehen Sie sich die vollständige Liste der BLF-Benutzer an.
- Überwachen Sie die Präsenz der Benutzer – Rich Presence ist nur für Benutzer mit Webex Cloud-Berechtigung verfügbar. Die Standard-Präsenz (Telefonie) ist nur für BroadWorks-Benutzer verfügbar.
- Starten Sie einen Anruf mit einem BLF-Benutzer.
- Starten Sie einen Chat mit einem BLF-Benutzer – nur für Benutzer mit Webex Cloud-Berechtigung verfügbar.
- Fügen Sie einen BLF-Benutzer als Kontakt hinzu.

```
<config>
  <services>
    <calls>
      <busy-lamp-field enabled="%ENABLE_BUSY_LAMP_FIELD_WXT%">
```



Cisco – vertraulich

```
        <display-caller enabled="%ENABLE_BLF_DISPLAY_CALLER_WXT%"/>
        <notification-delay time="%BLF_NOTIFICATION_DELAY_TIME_WXT%"/>
```

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_BUSY_LAMP_FIELD_WXT% | Falsch | wahr, falsch | Aktiviert die Überwachung des Besetztlampenfelds und die Klingelbenachrichtigung für andere Benutzer, die Anrufe annehmen können. |
| %ENABLE_BLF_DISPLAY_CALLER_WXT% | wahr | wahr, falsch | Aktiviert die Anzeige des Anzeigenamens/der Nummer des Anrufers in der eingehenden Benachrichtigung. |
| %BLF_NOTIFICATION_DELAY_TIME_WXT% | 0 | 0–60 | Steuert, wie viele Sekunden die klingelnde Benachrichtigung verzögert werden sollte, bevor sie dem Benutzer angezeigt wird. |

**HINWEIS:** Diese Funktion hängt vom Dienst für die gezielte Anrufübernahme ab.

#### 6.2.8.2 Anrufübernahmegruppe (nur Webex Calling)

Ab Version 44.2 unterstützt die Webex-Anwendung GCP-Benachrichtigungen (Group Call Pickup) für die Webex Calling-Bereitstellung. Damit können Benutzer bei eingehenden Anrufen für alle über die Anrufannahmegruppe überwachten Benutzer benachrichtigt werden.

Im Falle eines eingehenden Anrufs für einen Benutzer, der Teil einer Anrufübernahmegruppe ist, erhält der Angerufene die Möglichkeit, den Anruf anzunehmen. Es gibt eine über Control Hub konfigurierbare GCP-Benachrichtigungsverzögerung. Wenn der Angerufene den Anruf nicht innerhalb der konfigurierten Zeit verarbeitet, wird eine GCP-Benachrichtigung an die Gruppe gesendet.

Bei mehreren Anrufen innerhalb derselben Anrufübernahmegruppe werden sie nacheinander basierend auf der Uhrzeit verarbeitet, zu der sie empfangen werden. Die Benachrichtigung über den ältesten Anruf wird zunächst an die Gruppe übergeben und nach der Verarbeitung wird die nächste Benachrichtigung in der Leitung an die Gruppe übergeben.

Abhängig von der Konfiguration im Control Hub-Administratorportal können Benachrichtigungen nur Audio, nur visuell oder nur Audio und visuell sein. Wenn eine visuelle GCP-Benachrichtigung vorhanden ist, kann der Benutzer den Anruf mit der Anrufübernahme-Funktion annehmen. Wenn die Nur-Audio-Benachrichtigung konfiguriert ist, sieht der Benutzer keine visuelle Benachrichtigung für den eingehenden Anruf, hört einen bestimmten Klingelton und kann den Anruf über das Menü „Anrufübernahme“ in der Webex-App oder durch manuelles Wählen des FAC-Codes (*98) und der Durchwahl annehmen.

Der Benutzer kann die GCP-Benachrichtigung über die Anwendungseinstellungen stummschalten. Diese Einstellung gilt für alle Benachrichtigungen zur Anrufübernahme (BLF und GCP) und standardmäßig sind Benachrichtigungen stummgeschaltet.

Die Funktion funktioniert für die primären Leitungen und für gemeinsam genutzte oder virtuelle Leitungen, die dem Benutzer zugewiesen sind.



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_GCP_NOTIFICATIONS_WXT% | Falsch | wahr, falsch | Aktiviert Benachrichtigungen für die Gruppenanrufübernahme |
| %ENABLE_GCP_DISPLAY_CALLER_WXT% | wahr | wahr, falsch | Ermöglicht die Anzeige des Anzeigenamens/der Nummer des Anrufers in der eingehenden Benachrichtigung. |
| %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% | 120 | 5–120 | Definiert die maximale Zeit, die eine GCP-Benachrichtigung für den Benutzer verfügbar ist |
| %BWGROUP-CALL-PICKUP-BOOL-n% | Falsch | wahr, falsch | Gibt an, ob für die entsprechende Leitung eine Anrufannahmegruppe konfiguriert ist |

**HINWEIS 1:** Dies ist nur eine Webex Calling-Funktion.

**HINWEIS 2:** Diese Funktion hängt davon ab, ob die Anrufübernahmegruppe für den Benutzer konfiguriert wird.

### 6.2.9 Remote-Event-Paket

Für Click-to-Dial-Clients wie den BroadWorks Receptionist Thin Client und Go-Integrator, bei dem die Webex-App das Anrufgerät ist, ehrt die Webex-App jetzt das Event-Paket für die Remotesteuerung, wenn sie einen Anruf erhält oder Halten/Fortsetzen verarbeitet.



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_REMOTE_CONTROL_EVENTS_WXT% | Falsch | wahr, falsch | Wenn „true“ festgelegt ist, muss die Remotesteuerung für den Benutzer aktiviert sein. |

### 6.2.10 CLID-Auswahl des Agenten für Anrufwarteschlange

Wenn Agenten Anrufe an ihre Kunden tätigen, möchten sie, dass den Kunden die entsprechende CLID (Calling Line ID) anstatt ihre persönliche CLID/Unternehmens-CLID angezeigt wird. Wenn z. B. die Agentin Mary Smith der Anrufwarteschlange des technischen Supports beigetreten ist, möchte Mary beim Anrufen von Kunden, dass die Kunden ihre CLID als technischen Support sehen, nicht Mary Smith.

Administratoren in Control Hub oder CommPilot können für eine Anrufwarteschlange eine oder mehrere DNIS-Nummern angeben, die für eine ausgehende CLID verwendet werden sollen. Agenten haben dann die Möglichkeit, eine der DNIS-Nummern auszuwählen, die als CLID für ausgehende Anrufe verwendet werden soll. Die Webex-App bietet Agenten die Möglichkeit, auszuwählen, welche DNIS als CLID verwendet werden sollen.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT% | Falsch | wahr, falsch | Aktiviert ausgehende Anrufe (CLID-Auswahl) im Namen der Callcenter-Warteschlange. |

### 6.2.11 Survivability Gateway (nur Webex Calling)

Ab Version 43.2 unterstützt die Webex-Anwendung den Survivability-Anrufmodus. Wenn die Funktion aktiviert ist und keine Webex Cloud-Konnektivität vorhanden ist, kann die Webex-Anwendung im Survivability-Modus ausgeführt werden. In diesem Modus ist die Anruffunktion für den Benutzer eingeschränkt.

Das lokale Survivability Gateway wird vom Kunden bereitgestellt.

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



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SURVIVABILITY_GATEWAY_WXT% | Falsch | wahr, falsch | Aktiviert die Unterstützung des Survivability-Modus. |
| %SURVIVABILITY_FALLBACK_TIME_WXT% | 30 | >=30 | Gibt die Fallback-Zeit (Survivability-Gateway zu SSE) an |

**HINWEIS:** Diese Funktion bietet Vertrauen in die Migration von lokalen zu Cloud-Anruflösungen.

### 6.2.12 Mehrere Leitungen – Darstellung gemeinsam genutzter Leitungen

Ab Version 42.12 unterstützt die Webex-Anwendung mehrere Leitungen. Ein Webex-Benutzer kann eine primäre Leitung haben und bis zu 9 Leitungen mit anderen Benutzern teilen.

Der Administrator sollte die Anzeige gemeinsam genutzter Anrufe für jede gemeinsam genutzte Leitung einrichten.

Der Webex-Client erkennt Leitungskonfigurationsaktualisierungen innerhalb von 12 Stunden und fordert den Benutzer auf, die Anwendung neu zu starten. Durch die erneute Anmeldung des Benutzers werden die Leitungsaktualisierungen sofort angewendet.

Ab Version 43.12 wurde die Webex-App erweitert, um das Verschieben (lokale Wiederaufnahme) eines gehaltenen Anrufs auf einer gemeinsam genutzten Leitung zu ermöglichen, der von einem anderen Benutzer oder demselben Benutzer auf einem anderen Gerät bearbeitet wird. Weitere Informationen finden Sie unter *6.2.15Anruf verschieben*.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_MULTI_LINE_WXT% | Falsch | wahr, falsch | Aktiviert die Unterstützung für mehrere Leitungen (sofern konfiguriert). Wenn diese Option deaktiviert ist (auf "false" gesetzt), wird nur die erste konfigurierte Leitung von der Anwendung verwendet. |

**ANMERKUNG 1 <UNK>** : Die Funktion Boss-Admin (Executive-Assistant) Unterstützung ist in Kombination mit Shared-Lines nicht verfügbar.

**ANMERKUNG 2 <UNK>** : Weitere BroadWorks-Anforderungen finden Sie unter „Darstellung einer gemeinsam genutzten Leitung“ im Webex-for-Cisco-BroadWorks-Solution-Guide.



Cisco – vertraulich

### 6.2.13 Mehrere Leitungen – Virtuelle Leitungen (nur Webex Calling)

Nur für die Webex Calling-Bereitstellung unterstützt die Webex-App die Konfiguration mehrerer Leitungen über virtuelle Leitungen. Die Konfiguration mit virtuellen Leitungen stimmt mit der Konfiguration mehrerer Leitungen über gemeinsam genutzte Leitungen überein und bietet die Möglichkeit, die für den Benutzer konfigurierten virtuellen Leitungen zu sehen und sie für eingehende und ausgehende Anrufe zu verwenden. Es können maximal 10 kombinierte virtuelle Leitungen und gemeinsam genutzte Leitungen konfiguriert werden.

Version 43.4 erweitert die Unterstützung für virtuelle Leitungen und fügt „Anruf parken“ und „Anruf parken abrufen“ hinzu.

Ab Version 43.12 wurde die Webex-App erweitert, um das Verschieben (lokale Wiederaufnahme) eines gehaltenen Anrufs auf einer virtuellen Leitung zu ermöglichen, der von einem anderen Benutzer oder demselben Benutzer auf einem anderen Gerät bearbeitet wird. Weitere Informationen finden Sie unter *6.2.15Anruf verschieben*.

Im Folgenden werden die Änderungen der Konfigurationsvorlage im Zusammenhang mit der Unterstützung für virtuelle Leitungen dargestellt.

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

### 6.2.14 Remote-Stummschaltungssteuerungs-Event-Paket (nur Webex Calling)

Ab Version 43.9 unterstützt die Webex-App die Remote-Stummschaltung von Anrufen über den Audio-Medienstrom. Auf diese Weise kann die Stummschaltung/Stummschaltung eines laufenden Anrufs von einem anderen Standort wie dem BroadWorks Receptionist Thin Client, bei dem die Webex-App das Anrufgerät ist, ausgelöst werden.

Die Funktion hängt vom neuen Informationspaket *„SIP x-cisco-mute-status “* ab. Wenn der Header *Recv-Info:x-cisco-mute-status* während der Einrichtung der Anruf-SIP INVITE-Sitzung empfangen wird und die Webex-App bei einer Aktualisierung (lokal oder remote) auf den Stummschaltungsstatus der Audio-Anrufsitzung SIP-INFO mit dem *Info-Paket:x-cisco-mute-status;muted=true* (oder *muted=false* ) zurücksendet, wobei der Parameter „Stummgeschaltet“ den aktualisierten Status des Audio-Medienstreams darstellt.



Cisco – vertraulich

Ein Stumm- oder Freischalten kann lokal oder von einem Remotestandort aus ausgelöst werden. Remote-Update löst SIP NOTIFY mit *Event aus: Stummschalten* (oder *Stummschaltung aufheben* ), um vom Anwendungsserver an die Webex-App gesendet zu werden. Die Webex-App berücksichtigt die Remote-Anforderung und sendet nach der Aktualisierung des Audio-Medien-Stream-Status eine SIP NOTIFY mit dem *Info-Paket:x-cisco-mute-status;muted=true* (oder *muted=false* ) zurück.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_REMOTE_MUTE_CONTROL_WXT% | Falsch | wahr, falsch | Wenn „true“ festgelegt ist, ist die Remote-Stummschaltung der Anrufsteuerung für den Benutzer aktiviert. |

### 6.2.15 Anruf verschieben

Die Webex-App bietet Anrufüberwachung und Anrufsteuerung für VoIP-Anrufe, die an einem anderen Standort beendet wurden. Dies ist derzeit nur für die Hauptleitung des Benutzers verfügbar.

Ab Version 43.12 zeigt die Webex-App nun auch für freigegebene und virtuelle Leitungen Anrufe an, die an einem anderen Standort beendet wurden. Solche Anrufe werden im Bereich „Aktive Anrufe“ zu Informationszwecken und ohne Option zur Steuerung angezeigt. Nur wenn ein solcher Anruf gehalten wird, kann der Benutzer ihn auf das lokale Gerät verschieben, indem er ihn auswählt und im Anrufbildschirm wieder aufnimmt. Dieser Mechanismus ist nützlich, wenn der Anruf vom gleichen Benutzer an einem anderen Standort oder von einem anderen Benutzer mit derselben Leitung bearbeitet wurde.

Beachten Sie, dass es nicht möglich ist, dass die Webex-App einen gehaltenen Anruf auf ein gekoppeltes Gerät verschiebt. Wenn der Benutzer mit einem Gerät gekoppelt ist, muss er zuerst die Verbindung trennen und kann dann den gehaltenen Anruf lokal fortsetzen.

Die Anrufüberwachung für gemeinsam genutzte und virtuelle Leitungen hängt vom Paket des SIP-Anrufinfo-Ereignisses ab.

Die Überwachung der Anrufe für die Hauptleitung des Benutzers hängt von den XSI-Ereignissen (Advanced Call-Ereignispaket) ab, und das Verschieben eines Anrufs auf das lokale Gerät ist für diese Anrufe nicht verfügbar. Für diesen Anruftyp kann der Benutzer die Funktion „Anrufannahme“ (*6.1.22Anrufübergabe*) verwenden. Das Ziehen von Anrufen funktioniert nur für die letzten aktiven Anrufe des Benutzers, während der Mechanismus für freigegebene und virtuelle Leitungen für alle Anrufe des Benutzers funktioniert, die gehalten werden.

1. Anwendungsfall 1:
    a. Alice hat Bobs Leitung für die Desktop- und Tischtelefonprofile zugewiesen.



Cisco – vertraulich

b. Alice hat einen Anruf mit Charlie über das Tischtelefon – Alice kann den laufenden Anruf in der Desktop-App sehen.

c. Alice hält den Anruf über das Tischtelefon – Alice kann den Anruf über die Desktop-App fortsetzen.

2. Anwendungsfall 2:

   a. Alice hat Bobs Leitung für die Desktop- und Tischtelefonprofile zugewiesen.

   b. Bob hat einen Anruf mit Charlie – Alice kann den laufenden Anruf in der Desktop-App sehen.

   c. Bob stellt den Anruf mit Charlie auf Eis – Alice kann den Anruf mit Charlie über die Desktop-App fortsetzen.

3. Anwendungsfall 3:

   a. Alice hat Bobs Leitung für die Desktop- und Tischtelefonprofile zugewiesen.

   b. Alice wird über die Desktop-App mit seinem Tischtelefon gekoppelt.

   c. Bob hat einen Anruf mit Charlie – Alice kann den laufenden Anruf in der Desktop-App sehen.

   d. Bob stellt den Anruf mit Charlie in die Warteschleife – Alice kann den Anruf mit Charlie nicht über die Desktop-App fortsetzen.

   e. Alice trennt die Desktop-App vom Tischtelefon – Alice kann den Anruf mit Charlie über die Desktop-App fortsetzen.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALL_MOVE_HERE_WXT% | Falsch | wahr, falsch | Aktiviert das Verschieben von Anrufen auf einem lokalen Gerät. Wird für Halten/Fortsetzen über Standorte/Benutzer hinweg im Anwendungsfall mit mehreren Leitungen verwendet. |



Cisco – vertraulich

## 6.3 Funktionen nur für Mobilgeräte

### 6.3.1 Notrufe

Webex für Cisco BroadWorks unterstützt native Notrufe.

Wenn die Funktion aktiviert ist, analysiert die Anwendung beim Initiieren eines ausgehenden VoIP-Anrufs die gewählte Nummer und vergleicht sie mit der Liste der konfigurierten Notrufnummern. Wenn die Nummer als Notrufnummer identifiziert wird, führt die Anwendung das konfigurierte Wählverhalten aus. Es kann mit dem *Tag „Wählsequenz“* konfiguriert werden.

Unterstützte Modi sind:

- *cs-only* – Der Client tätigt Notrufe nur über das Mobilfunknetz, wenn das Netzwerk verfügbar ist.
- *cs-first* – Nach dem Initiieren eines Notrufs überprüft der Client den Netzwerktyp, mit dem das aktuelle Gerät verbunden ist. Wenn das Mobilfunknetz verfügbar ist, tätigt der Client Anrufe über das Mobilfunknetz. Wenn das Mobilfunknetz nicht verfügbar ist, aber ein Mobilfunknetz/WLAN-Netzwerk verfügbar ist, tätigt der Client den Anruf über das Mobilfunknetz/WLAN-Netzwerk als VoIP-Anruf. Wenn der Notruf über das Mobilfunknetz getätigt wird, empfiehlt der Client dem Benutzer, den Notruf als VoIP zu wiederholen.
- *VoIP-only* – Der Client tätigt Notrufe nur als VoIP, wenn das Mobilfunknetz/WLAN-Netzwerk verfügbar ist.
- *cs-voip* – Der Kunde analysiert, ob das Gerät es als nativ schaltungsgesteuerten Anruf (CS) initiieren kann (ohne zu berücksichtigen, ob das CS-Netzwerk verfügbar ist oder nicht). Wenn das Gerät einen systemeigenen Anruf starten kann, wird die Notrufnummer als CS-Notruf gewählt. Andernfalls wird der Anruf als VoIP gewählt.

**HINWEIS:** Wenn VOIP-Anrufe deaktiviert sind, ist der einzige aussagekräftige Wert für die Notrufsequenz (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) „cs-only“.

Der Haftungsausschluss für Notrufe wird dem Benutzer bei der Anmeldung angezeigt. Sie wird nicht über die Konfigurationsoptionen gesteuert.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_EMERGENCY_DIALING_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die Erkennung von Notrufen zu aktivieren.<br>Der Standardwert ist leer. |
| %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% | Nur-C | Nur cs, cs-first, nur Voip, cs-voip | Steuert den Wählsequenzmodus für Notrufe. |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %EMERGENCY_DIALING_NUMBERS_WXT% | „ <UNK> 911 <UNK> ,11 <UNK> <UNK> 2 <UNK> “ | CSV-Liste | CSV-Liste der Notrufnummern.<br>Beispiel: 911,112 |

### 6.3.2 Push-Benachrichtigungen für Anrufe

Wenn ein eingehender Anruf empfangen wird, erhält der mobile Client zuerst eine Push-Benachrichtigung (PN). Es gibt einen Konfigurationsparameter, der verwendet werden kann, um zu steuern, wann die SIP REGISTER-Sitzung eingerichtet werden soll:

1. Wenn die Push-Benachrichtigung empfangen wird ODER
2. Wenn der Anruf vom Benutzer angenommen wird.

Der zweite Ansatz wird empfohlen. Im Vergleich zum ersten Fall führt dies jedoch zu einer gewissen Verzögerung, bevor der Anruf eingerichtet wird.

Gemäß den iOS 13-Anforderungen sollten die VoIP-PNs nur für eingehende Anrufe verwendet werden. Die restlichen anrufbezogenen Events sollten reguläre PNs verwenden.

Um diese Anforderung zu erfüllen, wird eine neue PN-Registrierungs-API eingeführt, und es muss ein entsprechender Patch auf den Anwendungsserver angewendet werden. Wenn das Backend nicht so konfiguriert ist, dass es die iOS 13 PNs unterstützt, kann der Konfigurationsparameter verwendet werden, um die Verwendung der älteren Push-Benachrichtigungen zu erzwingen, bei denen alle anrufbezogenen Ereignisse über VoIP-PNs bereitgestellt werden.

Es wird eine Push-Benachrichtigung vom Anwendungsserver (AS) gesendet, wenn ein eingehender Anruf von dem Angerufenen an einem anderen Standort angenommen, vom Anrufer geschlossen oder beispielsweise an die Voicemail weitergeleitet wird. Mit dem iOS 13 ist diese Art der Push-Benachrichtigung nun eine reguläre und es hat einige Einschränkungen. Sie kann durch den Apple Push Notification Service (APNS) verzögert oder gar nicht zugestellt werden. Um fehlende oder verzögerte Anruf-Update-PNs zu verarbeiten, wird eine konfigurierbare Zeitüberschreitung für das Klingeln hinzugefügt, um die maximale Klingelzeit zu steuern. Wenn die maximale Klingeldauer erreicht ist, wird das Klingeln für den Angerufenen gestoppt und der Anruf wird als verpasst behandelt. Auf der Seite des Anrufers kann der Anruf so lange klingeln, bis die auf dem Anwendungsserver (AS) konfigurierte Richtlinie für das Klingeln ohne Antwort ausgeführt wird.

Um das Anwendungsverhalten einheitlich zu halten, gilt der konfigurierbare Timer für Klingeltöne für Android und iOS.



Cisco – vertraulich

Eine separate Konfigurationsoption wird hinzugefügt, um das Verhalten zum Ablehnen von Anrufen festzulegen, wenn ein eingehender Anruf als Push-Benachrichtigung empfangen wird. Der Client kann so konfiguriert werden, dass er den Anruf ignoriert oder über Xsi auf den Server reagiert und die Option auf „true“ oder „false“ gesetzt wird. In diesem Fall werden die zugewiesenen Cisco BroadWorks-Anrufbehandlungsdienste angewendet. Wenn „decline_false“ konfiguriert ist, wird das Klingeln des Anrufs so lange fortgesetzt, bis der Anrufer den Anruf abbricht oder der Timer für die Nichtannahme abläuft und die zugehörigen Anrufbehandlungsdienste gestartet werden. Wenn „decline_true“ konfiguriert ist, gibt der Grund für das Ablehnen die Anrufverarbeitung an. Wenn der Ablehnungsgrund auf „Besetzt“ gesetzt ist, erzwingt der Server sofort den Besetztbehandlungsdienst. Wenn „temp_unavailable“ konfiguriert ist, wird der temporäre nicht verfügbare Behandlungsdienst angewendet.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% | Falsch | wahr, falsch | Steuert, wann die SIP REGSITER-Sitzung eingerichtet wird – beim Empfang einer Push-Benachrichtigung für eingehende Anrufe oder bei deren Annahme. |
| %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% | 35 | [0–180] | Steuert die maximale Klingelzeit für eingehende Anrufe, die über den PN empfangen werden. Wenn innerhalb des angegebenen Zeitraums kein CallUpd-PN empfangen wird, wird der Anruf als verpasst behandelt. |
| %REJECT_WITH_XSI_MODE_WXT% | decline_falsch | ignorieren, decline_true, decline_false | Gibt das Verhalten zum Ablehnen von Anrufen an. |
| %REJECT_WITH_XSI_DECLINE_REASON_WXT% | beschäftigt | Besetzt, temp_nicht verfügbar | Gibt den Grund für das Ablehnen des Anrufs an, wenn der Ablehnungsmodus auf „decline_true“ festgelegt ist. |

#### 6.3.2.1 MWI

Wenn die MWI-Funktion aktiviert ist, abonniert der Mobile Webex-Client die MWI-Push-Benachrichtigung, um Aktualisierungen mit der Voicemail des Benutzers zu erhalten und ihn zu benachrichtigen.

Um die Anzahl der Benachrichtigungen zu reduzieren und unnötige Ablenkungen zu vermeiden, werden die MWI-Push-Benachrichtigungen in einigen Fällen unterdrückt. Wenn der Benutzer beispielsweise die Voicemail-Nachrichten hört oder sie im mobilen Webex-Client als gelesen markiert (die ungelesene Nummer nimmt ab). Es gibt keine konfigurierbare Option, um dies zu steuern.



Cisco – vertraulich

Weitere Informationen zu MWI finden Sie im Abschnitt *6.1.27Voicemail , Visuelle Voicemail, Briefkastenlampe*.

#### 6.3.2.2 Hinweiston

BroadWorks-Dienste (wie DND) können Ruftonerinnerungen senden, wenn eingehende Anrufe umgeleitet werden. Der Webex Mobile-Client kann so konfiguriert werden, dass die Ring Splash Push-Benachrichtigungen aktiviert und dem Benutzer angezeigt werden, wenn sie von BroadWorks ausgelöst werden.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_RING_SPLASH_WXT% | Falsch | t rue , false | Aktiviert Ring Splash in der B road W orks config . |

### 6.3.3 Einzelne Benachrichtigung

Die Mobile Single Alert-Funktion ist für die Bereitstellung von Festnetz-Mobilfunk-Konvergenz (FMC)/Mobilfunknetzbetreiber (MNO) mithilfe des BroadWorks Mobility-Dienstes vorgesehen. Ohne sie erhält der Benutzer, wenn er beim Webex-Client angemeldet ist und einen eingehenden Anruf erhält, gleichzeitig zwei Anrufe – einen systemeigenen und einen Push-Benachrichtigung (VoIP)-Anruf. Wenn die Funktion aktiviert ist, deaktiviert die Anwendung die Mobilitätsbenachrichtigung am BroadWorks-Mobilitätsstandort des Benutzers, wenn Sie sich anmelden, und aktiviert die Benachrichtigung, wenn Sie sich abmelden. Eine wichtige Voraussetzung für die Verwendung dieser Funktion ist, dass dem Benutzer der BroadWorks-Mobilitätsdienst zugewiesen und genau ein Standort konfiguriert ist.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_SINGLE_ALERTING_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um Single Alerting zu aktivieren. |



Cisco – vertraulich

### 6.3.4 Zum Wählen klicken (Rückruf )

Das ausgehende Click-to-Dial stellt sicher, dass der Endbenutzer auf seinem persönlichen Circuit Switched-Mobiltelefon einen Anruf tätigen und seine geschäftliche Verzeichnisnummer als Anrufleitungs-ID bereitstellen kann.

Der Mobile Webex-Client unterstützt Click-to-Dial-Anrufe (Rückruf) mit dem BroadWorks Anywhere-Dienst. Die BroadWorks Anywhere-Standorte in der Webex-Anwendung werden als SNR-Standorte (Single Number Reach) bezeichnet.

Wenn die Funktion aktiviert ist, können Benutzer den SNR-Standort über das Menü Gerätekopplung auswählen. Wenn Sie mit dem SNR-Standort gekoppelt sind, werden alle ausgehenden Anrufe mit Click-to-Dial-Anrufen (Rückruf) initiiert. Um doppelte Benachrichtigungen zu verhindern, sind Push-Benachrichtigungen für eingehende Anrufe deaktiviert.

Wenn ein Benutzer einen Click-to-Dial-Anruf initiiert, wird der Bildschirm „Ausgehender Anruf“ mit Informationen angezeigt, um einen eingehenden Anruf am ausgewählten SNR-Standort zu erwarten. Dieser Bildschirm wird basierend auf dem konfigurierbaren Timer automatisch geschlossen.

Wenn Sie die Verbindung zu einem SNR-Standort trennen, registriert sich die Anwendung erneut für Push-Benachrichtigungen für eingehende Anrufe.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_DIALING_CALL_BACK_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um „Click to Dial“-Anrufe (Rückruf) zu aktivieren. |
| %DIALING_CALL_BACK_TIMER_WXT% | 10 | [3-20] | Steuert die Anzahl der Sekunden, bevor der Rückruf-Bildschirm automatisch geschlossen wird. |

### 6.3.5 MNO-Unterstützung

#### 6.3.5.1 Anruf mit nativem Wählprogramm

Diese Funktion bietet zusätzliche Unterstützung für MNO-Bereitstellungen (Mobile Network Operator), die den BWM-Dienst (BroadWorks Mobility) nutzen. Es wird davon ausgegangen, dass dem Benutzer der BroadWorks-Mobilitätsdienst zugewiesen und mindestens ein Standort konfiguriert ist.



Cisco – vertraulich

Die Möglichkeit des Benutzers, Anrufe über den nativen Dialer zu initiieren, wird durch das **native** Konfigurations-Tag „ “ gesteuert. Wenn diese Option aktiviert ist, startet die Anwendung das native Dialer und tätigt den Anruf. Darüber hinaus wird die Verfügbarkeit von VoIP-Anrufen durch das **VoIP-Tag** gesteuert – basierend auf den Bereitstellungsanforderungen können VoIP-Anrufe aktiviert oder deaktiviert werden.

Wenn VoIP und native Anrufe aktiviert sind, kann der Benutzer auswählen, welche Option verwendet werden soll.

Der <Dialing-Mode>-Tag steuert, ob Benutzer auswählen können, wie eingehende und ausgehende Anrufe gestartet/empfangen werden sollen. Erfordert, dass sowohl der native Anruf als auch VoIP-Anrufe aktiviert werden.

Ab Version 43. 12 wird die native Wählkonfiguration erweitert, sodass der ausgehenden Anrufnummer ein benutzerdefiniertes Präfix vorangestellt werden kann. Dies gilt nur für Mobilfunkanrufe, die über die Webex-App initiiert werden, wenn die gewählte Nummer mit einem FAC-Code beginnt.

Diese Funktion ist hilfreich für Kunden, die MNO-Bereitstellungen verwenden, bei denen Anrufe nicht an den integrierten Cisco BroadWorks-Anwendungsserver umgeleitet werden, sondern die FAC-Codes vom Telecom-Backend verarbeitet werden können. Das neue <fac-prefix>-Tag wird im Abschnitt <dialing><native> hinzugefügt und die Telekommunikation kann es verwenden, um dieses Problem zu beheben.

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_DIALING_VOIP_WXT% | wahr | wahr, falsch | Legen Sie „true“ fest, um die VoIP-Anrufoption zu aktivieren. |
| %ENABLE_DIALING_NATIVE_WXT% | Falsch | wahr, falsch | Legen Sie „true“ fest, um die native Anrufoption zu aktivieren. |
| %ENABLE_DIALING_MODE_WXT% | Falsch | wahr, falsch | Aktiviert die Auswahl des Wählmodus durch den Benutzer über die Anrufeinstellungen in den Einstellungen. |
| %DIALING_MODE_DEFAULT_WXT% | VoIP | voip, nativ | Gibt den Standard-Wählmodus an, der ausgewählt wurde, wenn der Wählmodus in den Einstellungen aktiviert ist. |
| %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% | Falsch | wahr, falsch | Steuert, ob die Verfügbarkeit nativer Anrufe von der BroadWorks Mobility-Dienstzuweisung und dem Mobilitätsstandort abhängen sollte, der für den Benutzer konfiguriert wird. |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %DIALING_NATIVE_FAC_PREFIX_WXT% | *leer* | Zeichenfolge | Gibt ein Präfix an, das vorangestellt werden soll, wenn ein ausgehender Anruf an eine Nummer, die mit einem FAC-Code beginnt, als zellulärer Anruf initiiert wird.<br>Standardmäßig ist kein FAC-Präfix definiert und das Tag ist leer. |

**ANMERKUNG 1 <UNK>** : Mindestens einer der Anrufe **voip** und **native** sollte aktiviert sein.

**ANMERKUNG 2 <UNK>** : Wenn nur der **native Anruf** aktiviert ist, wird in MNO-Bereitstellungen empfohlen, die Einzelbenachrichtigung zu deaktivieren, um zu verhindern, dass der Client die BWM-Benachrichtigung deaktiviert.

**ANMERKUNG 3 <UNK>** : Wenn sowohl **systemeigene Anrufe als** auch **VoIP-Anrufe** aktiviert sind, wird in MNO-Bereitstellungen empfohlen, die Einzelbenachrichtigung zu aktivieren, um doppelte Benachrichtigungen zu verhindern.

#### 6.3.5.2 Anrufsteuerungen

Mit dieser Funktion kann der Mobile Webex-Client über XSI-native Anrufe auf dem Mobilgerät steuern, die auf Cisco BroadWorks verankert sind. Die XSI-Anrufsteuerungen sind nur verfügbar, wenn:

- Der BroadWorks Mobility (BWM)-Dienst ist dem Benutzer zugewiesen,
- Es gibt nur eine einzige BMW Mobile Identity konfiguriert ,
- Der native Wählmodus wird vom Benutzer ausgewählt (für weitere Informationen siehe Abschnitt *6.3.5.1Anruf mit nativem Wählprogramm),*
- An BroadWorks ist ein Anruf verankert, der den BMW-Dienst durchläuft,
- Es gibt einen laufenden Mobilfunkanruf auf dem Mobilgerät.

Version 43.10 bietet eine bessere Handhabung der beratenden Übergabe, eine Verknüpfung zwischen den beiden in der Webex-App präsentierten Mobilfunkanrufen und eine Option für den Benutzer, um die Übergabe abzuschließen. Wenn ein Benutzer zwei unabhängige Mobilfunkanrufe auf demselben Gerät hat, wird das Übergabemenü erweitert, um die Weiterleitung von einem zu dem anderen zu ermöglichen, auch wenn keine Verknüpfung zwischen ihnen erstellt wurde.



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_XSI_CALL_CONTROL_WXT% | Falsch | wahr, falsch | Aktiviert die XSI-Anrufsteuerung für MNO-Umgebungen. |
| %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% | MNO_Zugriff | MNO_Access, MNO_Network | Steuert den von der Anwendung verwendeten XSI MNO-Bereitstellungstyp. Folgende Werte sind möglich:<br>▪ MNO_Access – zeigt alle Remote-Anrufe (XSI) mit den im Knoten unten definierten Gerätetypen an.<br>▪ MNO_Network – zeigt alle Remote-Anrufe (XSI) an. |
| %DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT% | “” | Zeichenfolge | Der Name des/der Gerätetyps, der/die im MNO_Access-Bereitstellungstyp verwendet werden soll/sollen. |
| %ENABLE_XSI_HOLD_CALLS_WXT% | wahr | wahr, falsch | Steuert, ob die Aktion „Anruf halten“ für den Benutzer für XSI-Mobilanrufe verfügbar sein sollte. |

#### 6.3.5.3 Leitungsidentität (CLID) für ausgehende Anrufe – Dual Persona

Mit der mobilen Version 42.12 ermöglicht die Webex-App Benutzern, ihre Calling Line Identity (CLID) auszuwählen, die dem Remote-Teilnehmer beim Initiieren eines ausgehenden Anrufs angezeigt wird.

Wenn der Benutzer mit Cisco BroadWorks Mobility konfiguriert ist, einer typischen Konfiguration für MNO-Bereitstellungen (Mobile Network Operator) und native Anrufe aktiviert sind, kann der Benutzer auswählen, welche Identität den angerufenen Personen angezeigt werden soll. Benutzer können ihre geschäftliche oder persönliche Identität auswählen. Es gibt auch eine Option zum Ausblenden der eigenen Identität und des Anrufs, der als Anonym angezeigt werden soll.

Bei VoIP-Anrufen hat der Benutzer auch die Möglichkeit, seine CLID zu steuern. Die verfügbare Option ist in diesem Fall nur zu steuern, ob seine Identität zu verbergen oder nicht.

Persona-Verwaltung und CLID-Blockierung werden durch separate Konfigurationsoptionen gesteuert.

```
<config>
<services>
<dialing>
   <calling-line-id-delivery-blocking
enabled="%ENABLE_CLID_DELIVERY_BLOCKING_WXT%"/>
```



Cisco – vertraulich

```
   <mobility-persona-management
enabled="%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%"/>
```

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CLID_DELIVERY_BLOCKING_WXT% | Falsch | wahr, falsch | Aktiviert das Blockieren der Anrufleitungs-ID-Zustellung. Sie gilt für alle ausgehenden Anruftypen für den Benutzer. |
| %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT% | Falsch | wahr, falsch | Aktiviert die persönliche Verwaltung für native Anrufe, wenn der Bereitstellungstyp als MNO_Access oder MNO_Network konfiguriert ist. (BroadWorks-Mobilität wird für die systemeigenen Anrufe verwendet, und alle systemeigenen Anrufe sind in BroadWorks verankert) |

#### 6.3.5.4 Benachrichtigung für native Anrufe

Für Benutzer, die mit MNO bereitgestellt werden, fügt diese Funktion ein Benachrichtigungsbanner für native Anrufe hinzu, das über die Webex-App gesteuert werden kann. Diese Benachrichtigung basiert auf einer Push-Benachrichtigung, die vom Anwendungsserver gesendet wird, sobald der Anruf eingerichtet wurde.

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_PN_MOBILE_CALL_INFO_WXT% | wahr | t rue , false | Aktiviert das Abonnement für die Push-Benachrichtigung MOBILE_CALL_INFO. |

#### 6.3.5.5 Nativer Anruf an konvertiertes Meeting verschieben

Bei Benutzern, die mit MNO bereitgestellt werden, ermöglicht diese Funktion die Eskalation eines nativen Sprachanrufs zu einem Meeting für beide Parteien eines 1:1-Anrufs (auch wenn die andere Partei kein Webex-Benutzer ist). Wenn der Remote-Benutzer ein Webex-Benutzer ist, haben die Teilnehmer einmal in einem Meeting die folgenden Möglichkeiten:

- Webex im Meeting-Chat initiieren
- Video hinzufügen (beachten Sie, dass die Audiowiedergabe im systemeigenen Anruf fortgesetzt wird)
- Bildschirm/Inhalt freigeben
- Meeting-Aufzeichnung auslösen



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | Falsch | wahr, falsch | Aktiviert das Einschalten (Einladen und Treffen, Videokonferenz-Aktionen). |

#### 6.3.5.6 MNO-Mobilität – Widget in Anrufen

Version 43.7 der Android Webex-App (Mobil und Tablet) führt offiziell ein neues Widget für die Anrufsteuerung (Bubble) ein, das zusätzliche Anrufsteuerung für native Anrufe bietet, die über den Mobilitätsdienst auf Cisco BroadWorks verankert sind. Das Widget wird oben auf der nativen Benutzeroberfläche angezeigt und ermöglicht dem Benutzer die folgenden Aktionen:

- Halten / Fortsetzen
- Übergabe ohne Rücksprache/Beratung – versetzt den Benutzer in das Dialogfeld „Übergabe“ in der Webex-App.
- Vollständige Übertragung – bietet die Möglichkeit, die beratende Übertragung abzuschließen (Version 43.10)
- Video-Meeting – Verschiebt die Parteien in ein Webex Meeting .
- Anruf beenden

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_WIDGET_HOLD_CALLS_WXT% | wahr | wahr, falsch | Steuert die Verfügbarkeit der Aktion „ Halten“ im Anruf-Widget. |
| %ENABLE_WIDGET_TRANSFER_CALLS_WXT% | wahr | wahr, falsch | Steuert die Verfügbarkeit der Aktionen „Übergabe “ und „Übergabe abschließen“ im Anruf-Widget. |



Cisco – vertraulich

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | wahr | wahr, falsch | Steuert die Verfügbarkeit der Aktion Video Meeting im Anruf-Widget. |

### 6.3.6 Anrufer-ID für eingehenden Anruf

Version 44.2 bietet die Möglichkeit, die Kontaktinformationen zu steuern, die dem Benutzer basierend auf dem Namen und der Nummer angezeigt werden. Es wurden zwei Konfigurationsoptionen hinzugefügt, um die Informationen zu steuern, die dem Benutzer im Bildschirm „Eingehender Anruf“ und in der Benachrichtigung über eingehende Anrufe sowie in den Benachrichtigungen über verpasste Anrufe angezeigt werden.

#### 6.3.6.1 Bildschirm „Eingehender Anruf“

Es gibt Plattformunterschiede zwischen Android und iOS, wenn es um die Anzeige von Daten im Bildschirm für eingehende Anrufe geht. Das native Erlebnis, das Informationen für eingehende Anrufe anzeigt, ist wie folgt:

- Android – im Bildschirm für eingehende Anrufe werden Name und Nummer in zwei separaten Feldern angezeigt
- iOS – es gibt nur ein Feld, in dem entweder der Name oder die Nummer angezeigt wird. Wenn beide verfügbar sind, hat der Name Priorität.

Mit der neuen Konfigurationsoption für eingehende Anrufe kann sichergestellt werden, dass die iOS Webex-App die Nummer im Anrufbildschirm neben dem Namen anzeigt (Format: *Name (Nummer)*). Das Verhalten der Android Webex-App ist nicht betroffen.

#### 6.3.6.2 Benachrichtigung bei eingehendem Anruf

In einigen Fällen wird der eingehende Anruf dem Benutzer als Benachrichtigung angezeigt. Aufgrund der begrenzten Platzverhältnisse wird die Nummer dort nicht immer angezeigt.

Die neue Konfigurationsoption für eingehende Anrufe steuert auch die Informationen, die in den Benachrichtigungen für eingehende Anrufe angezeigt werden. Wenn diese Option aktiviert ist und sowohl der Name als auch die Nummer verfügbar sind, fügt die Webex-App die Nummer neben dem Namen hinzu (Format: *Name (Nummer)*). Dieses Verhalten der Webex-App gilt sowohl für Android als auch für iOS.

#### 6.3.6.3 Benachrichtigung bei entgangenen Anrufen

Für die Benachrichtigungen über verpasste Anrufe wird ein zusätzlicher Konfigurationsparameter hinzugefügt. Sie kann verwendet werden, um die Informationen des Remote-Teilnehmers zu steuern, ähnlich wie bei Benachrichtigungen über eingehende Anrufe, sodass die Nummer an den Anzeigenamen des Remote-Benutzers angehängt und in der Benachrichtigung über verpasste Anrufe angezeigt werden kann. Dieses Verhalten der Webex-App gilt sowohl für Android als auch für iOS.



Cisco – vertraulich

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

| Tag | Standard, wenn nicht vorhanden | Unterstützte Werte | Beschreibung |
|---|---|---|---|
| %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% | Falsch | wahr, falsch | Steuert, ob die Nummer im Bildschirm für eingehende Anrufe (nur iOS) und Benachrichtigungen an den Namen angehängt werden soll. |
| %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% | Falsch | wahr, falsch | Steuert, ob die Nummer in der Benachrichtigung über verpasste Anrufe an den Namen angehängt werden soll. |

**HINWEIS:** Wenn die Nummer als Anzeigename geliefert wird oder der Anzeigename mit der Nummer endet, vermeidet die Webex-App Doppelarbeit und zeigt die Nummer nur einmal an.



Cisco – vertraulich

# 7 Funktionen für Early Field Trial (BETA)

## 7.1 KI-Codec

Ab Version 44.7 unterstützt die Webex-App einen neuen Audio-Codec – KI-Codec (xCodec). Dieser Audio-Codec wird unter widrigen Netzwerkbedingungen verwendet, um eine bessere Anrufqualität zu erzielen. Die Webex Media Engine in der Webex-App überprüft die Gerätefunktionen, verfolgt die Medienqualität und der KI-Codec kann verwendet werden, wenn er über die Konfigurationsdatei unterstützt und aktiviert wird.

Der KI-Codec funktioniert nur in Kombination mit dem Opus-Codec. Das bedeutet, dass sowohl der Opus- als auch der AI-Codec während der SDP-Verhandlung von beiden Seiten beworben und ausgehandelt werden sollten.

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



Cisco – vertraulich

# 8 Benutzerdefinierte Tags-Zuordnung zwischen Webex für Cisco BroadWorks und UC-One

In der folgenden Tabelle sind die benutzerdefinierten Tags für Webex für Cisco BroadWorks aufgeführt, die mit ihren älteren benutzerdefinierten Tags für UC-One übereinstimmen.

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %ENABLE_REJECT_WITH_486_WXT% | %ENABLE_REJECT_WITH_486_DESKTOP% | %ENABLE_REJECT_WITH_486_MOBILE% |
| %REJECT_WITH_XSI_MODE_WXT% | k. A. | %REJECT_WITH_XSI_MODE_ <UNK> MOBILE% |
| %REJECT_WITH_XSI_DECLINE_REASON_WXT% | k. A. | %REJECT_WITH_XSI_DECLINE_REASON_MOBILE% |
| %ENABLE_TRANSFER_CALLS_WXT% | %ENABLE_TRANSFER_CALLS% | %ENABLE_TRANSFER_CALLS_MOBILE% |
| %ENABLE_CONFERENCE_CALLS_WXT% | k. A. | %ENABLE_CONFERENCE_CALLS_MOBILE% |
| %ENABLE_NWAY_PARTICIPANT_LIST_WXT% | %ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP% | k. A. |
| %MAX_CONF_PARTIES_WXT% | %MAX_CONF_PARTIES% | k. A. |
| %ENABLE_CALL_STATISTICS_WXT% | k. A. | k. A. |
| %ENABLE_CALL_PULL_WXT% | %ENABLE_CALL_PULL_DESKTOP% | %ENABLE_CALL_PULL_MOBIL% |
| %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% | k. A. | %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_MOBILE% |
| %ENABLE_MWI_WXT% | %DESKTOP_MWI_ENABLE% | %ENABLE_MWI_MOBILE% |
| %ENABLE_MWI_WXT% | %DESKTOP_MWI_ENABLE% | %ENABLE_MWI_MOBILE% |
| %MWI_MODE_WXT% | %DESKTOP_MWI_MODUS% | %MWI_MODE_MOBILE% |
| %ENABLE_VOICE_MAIL_WXT% | k. A. | k. A. |
| %ENABLE_VISUAL_VOICE_MAIL_WXT% | %ENABLE_VISUAL_VOICE_MAIL% | k. A. |
| %ENABLE_FORCED_LOGOUT_WXT% | %ENABLE_FORCED_LOGOUT% | k. A. |
| %FORCED_LOGOUT_APPID_WXT% | %FORCEUT_LOGOUT_APPID% | k. A. |
| %ENABLE_CALL_FORWARDING_ALWAYS_WXT% | k. A. | k. A. |
| %ENABLE_BROADWORKS_ANYWHERE_WXT% | k. A. | k. A. |



Cisco – vertraulich

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% | k. A. | k. A. |
| %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% | k. A. | k. A. |
| %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% | k. A. | k. A. |
| %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% | k. A. | k. A. |
| %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% | k. A. | k. A. |
| %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% | k. A. | k. A. |
| %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% | k. A. | k. A. |
| %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% | k. A. | k. A. |
| %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% | k. A. | k. A. |
| %ENABLE_EMERGENCY_DIALING_WXT% | k. A. | k. A. |
| %EMERGENCY_DIALING_NUMBERS_WXT% | k. A. | k. A. |
| %ENABLE_USE_RPORT_WXT% | %USE_RPORT_IP% | %ENABLE_USE_RPORT_MOBILE% |
| %RPORT_USE_LOCAL_PORT_WXT% | k. A. | %RPORT_USE_LOCAL_PORT_MOBILE% |
| %USE_TLS_WXT% | %USE_TLS% | k. A. |
| %SBC_ADDRESS_WXT% | %SBC_ADDRESS% | %SBC_ADDRESS% |
| %SBC_PORT_WXT% | %SBC_PORT% | %SBC_PORT% |
| %USE_PROXY_DISCOVERY_WXT% | %USE_PROXY_DISCOVERY% | %USE_PROXY_DISCOVERY_ <UNK> MOBILE% |
| %USE_TCP_FROM_DNS_WXT% | %USE_TCP_FROM_DNS% | k. A. |
| %USE_UDP_FROM_DNS_WXT% | %USE_UDP_FROM_DNS% | k. A. |



Cisco – vertraulich

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %USE_TLS_FROM_DNS_WXT% | %USE_TLS_FROM_DNS% | k. A. |
| %DOMAIN_OVERRIDE_WXT% | %DOMAIN_OVERRIDE% | %DOMAIN_OVERRIDE% |
| %SOURCE_PORT_WXT% | %SOURCE_PORT% | %SOURCE_PORT% |
| %USE_ALTERNATIVE_IDENTITIES_WXT% | %USE_ALTERNATIVE_IDENTITIVE% | k. A. |
| %TCP_SIZE_THRESHOLD_WXT% | %TCP_SIZE_THRESHOW% | k. A. |
| %SIP_REFRESH_ON_TTL_WXT% | %SIP_REFRESH_ON_TTL% | k. A. |
| %ENABLE_SIP_UPDATE_SUPPORT_WXT% | %ENABLE_SIP_UPDATE_SUPPORT_DESKTOP% | %ENABLE_SIP_UPDATE_SUPPORT_MOBILE% |
| %ENABLE_PEM_SUPPORT_WXT% | %ENABLE_PEM_SUPPORT_ <UNK> DESKTOP% | k. A. |
| %ENABLE_SIP_SESSION_ID_WXT% | k. A. | k. A. |
| %ENABLE_FORCE_SIP_INFO_FIR_WXT% | k. A. | k. A. |
| %SRTP_ENABLED_WXT% | %USE_SRTP% | %SRTP_ENABLE_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% | k. A. |
| %CHANNEL_HEARTBEAT_WXT% | %CHANNEL_HEARTBEAT% | %CHANNEL_HEARTBEAT_ <UNK> MOBILE% |
| %XSI_ROOT_WXT% | %XSI_ROOT% | %XSI_ROOT% |
| %XSI_ACTIONS_PATH_WXT% | k. A. | %XSI_ACTIONS_PATH_MOBILE% |
| %XSI_EVENTS_PATH_WXT% | k. A. | %XSI_EVENTS_PATH_MOBILE% |



Cisco – vertraulich

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %ENABLE_CALLS_AUTO_ RECOVERY_WXT% | k. A. | %ENABLE_CALLS_AUTO_ <UNK> RECOVERY_MOBILE% |
| %EMERGENCY_CALL_DIAL_ SEQUENCE_WXT% | k. A. | %EMERGENCY_CALL_DIAL_ <UNK> SEQUENCE_MOBILE% |
| %ENABLE_CALL_PICKUP_BLI ND_WXT% | k. A. | k. A. |
| %ENABLE_CALL_PICKUP_ DIRECTED_WXT% | k. A. | k. A. |
| %WEB_CALL_SETTINGS_URL _WXT% | k. A. | %WEB_CALL_SETTINGS_URL % |
| %USE_MEDIASEC_WXT% | %USE_MEDIASEC_MOBILE% | %USE_MEDIASEC_DESKTOP % |
| %ENABLE_CALL_CENTER_ WXT% | %ENABLE_CALL_CENTER_ <UNK> DESKTOP%“ | k. A. |
| %WEB_CALL_SETTINGS_TAR GET_WXT% | k. A. | k. A. |
| %WEB_CALL_SETTINGS_CFA _ VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_CFA _VISIBLE% |
| %WEB_CALL_SETTINGS_DN D_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_DN D_VISIBLE% |
| %WEB_CALL_SETTINGS_AC R_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_AC R_VISIBLE% |
| %WEB_CALL_SETTINGS_CFB _VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_CFB _VISIBLE% |
| %WEB_CALL_SETTINGS_CFN R_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_CFN R_VISIBLE% |
| %WEB_CALL_SETTINGS_CFN A_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_CFN A_VISIBLE% |
| %WEB_CALL_SETTINGS_SIM RING_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_SIM RING_VISIBLE% |
| %WEB_CALL_SETTINGS_ SEQRING_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_SE QRING_VISIBLE% |
| %WEB_CALL_SETTINGS_RO_ VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_RO_ VISIBLE% |
| %WEB_CALL_SETTINGS_ACB _VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_ACB _VISIBLE% |
| %WEB_CALL_SETTINGS_CW _VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_CW _VISIBLE% |
| %WEB_CALL_SETTINGS_CLI DB_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_CLI DB_VISIBLE% |



Cisco – vertraulich

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_PA_VISIBLE% |
| %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_BWA_VISIBLE% |
| %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% | k. A. | %WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE% |
| %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_BWM_VISIBLE% |
| %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% | k. A. | %WEB_CALL_SETTINGS_VM_VISIBLE% |
| %ENABLE_DIALING_CALL_BACK_WXT% | k. A. | k. A. |
| %DIALING_CALL_BACK_TIMER_WXT% | k. A. | k. A. |
| %ENABLE_EXECUTIVE_ASSISTANT_WXT% | %ENABLE_EXECUTIVE_ASSISTANT_DESKTOP% | k. A. |
| %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% | k. A. | %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_MOBILE% |
| %ENABLE_CALL_RECORDING_WXT% | %ENABLE_CALL_RECORDING_DESKTOP% | %CALL_RECORDING_MOBILE% |
| %ENABLE_SINGLE_ALERTING_WXT% | k. A. | %ENABLE_SINGLE_ALERTING% |
| %ENABLE_CALL_PARK_WXT% | %ENABLE_CALL_PARK_DESKTOP% | k. A. |
| %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% | k. A. | k. A. |
| %ENABLE_RTP_ICE_WXT% | k. A. | k. A. |
| %RTP_ICE_MODE_WXT% | k. A. | k. A. |
| %RTP_ICE_SERVICE_URI_WXT% | k. A. | k. A. |
| %RTP_ICE_PORT_WXT% | k. A. | k. A. |
| %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT% | k. A. | k. A. |
| %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | k. A. | k. A. |
| %ENABLE_DIALING_VOIP_WXT% | k. A. | k. A. |
| %ENABLE_DIALING_NATIVE_WXT% | k. A. | k. A. |
| %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% | k. A. | k. A. |



Cisco – vertraulich

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% | k. A. | k. A. |
| %ENABLE_UNIFIED_CALL_HISTORY_WXT% | k. A. | k. A. |
| %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% | k. A. | k. A. |
| %USER_PORTAL_SETTINGS_URL_WXT% | k. A. | k. A. |
| %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% | k. A. | k. A. |
| %ENABLE_AUDIO_MARI_FEC_WXT% | k. A. | k. A. |
| %ENABLE_AUDIO_MARI_RTX_WXT% | k. A. | k. A. |
| %ENABLE_VIDEO_MARI_FEC_WXT% | k. A. | k. A. |
| %ENABLE_VIDEO_MARI_RTX_WXT% | k. A. | k. A. |
| %ENABLE_CALL_BLOCK_WXT% | k. A. | k. A. |
| %ENABLE_WIDGET_HOLD_CALLS_WXT% | k. A. | k. A. |
| %ENABLE_WIDGET_TRANSFER_CALLS_WXT% | k. A. | k. A. |
| %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% | k. A. | k. A. |
| %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% | k. A. | k. A. |
| %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% | k. A. | k. A. |
| %ENABLE_CALL_MOVE_HERE_WXT% | k. A. | k. A. |
| %ENABLE_SPEECH_ENHANCEMENTS_WXT% | k. A. | k. A. |
| %DIALING_NATIVE_FAC_PREFIX_WXT% | k. A. | k. A. |
| %ENABLE_TRANSFER_AUTO_HOLD_WXT% | k. A. | k. A. |
| %ENABLE_RTCP_XR_NEGOTIATION_WXT% | k. A. | k. A. |



Cisco – vertraulich

| Webex für Cisco BroadWorks-Tag | Desktop-Legacy-Tag | Legacy-Tag für Mobilgeräte |
|---|---|---|
| %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% | k. A. | k. A. |
| %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% | k. A. | k. A. |
| %ENABLE_CLID_OUTGOING_CALLS_WXT% | k. A. | k. A. |
| %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% | k. A. | k. A. |
| %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% | k. A. | k. A. |
| %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% | k. A. | k. A. |
| %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% | k. A. | k. A. |
| %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% | k. A. | k. A. |
| %ENABLE_BUSY_LAMP_FIELD_WXT% | %ENABLE_BUSY_LAMP_FIELD_DESKTOP% | k. A. |
| %ENABLE_BLF_DISPLAY_CALLER_WXT% | %ENABLE_BLF_DISPLAY_CALLER_DESKTOP% | k. A. |
| %BLF_NOTIFICATION_DELAY_TIME_WXT% | k. A. | k. A. |
| %ENABLE_GCP_NOTIFICATIONS_WXT% | k. A. | k. A. |
| %ENABLE_GCP_DISPLAY_CALLER_WXT% | k. A. | k. A. |
| %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% | k. A. | k. A. |
| %UDP_KEEPALIVE_ENABLED_WXT% | k. A. | k. A. |
| %TCP_KEEPALIVE_ENABLED_WXT% | k. A. | k. A. |
| %TLS_KEEPALIVE_ENABLED_WXT% | k. A. | k. A. |

**HINWEIS:** N/A zeigt an, dass es kein entsprechendes benutzerdefiniertes Tag gab, das die Funktion in UC-One steuerte. N/A für Desktop- und Mobile Legacy-Tags zeigt an, dass das Webex für Cisco BroadWorks-Tag neu ist und entweder neue Funktionen oder eine vorhandene Funktion steuert, die nicht durch ein benutzerdefiniertes Tag in UC-One gesteuert wurde.



Cisco – vertraulich

# 9 Anhang A: TLS-Schlüssel

Der Webex für BroadWorks-Client verwendet CiscoSSL, das auf OpenSSL basiert und zusätzliche Sicherheitsvorkehrungen bietet.



Cisco – vertraulich

# 10 Anhang B: Skript für die Bereitstellung des DM-Tags

Die Anzahl der benutzerdefinierten DM-Tags ist mit jeder Version gestiegen, da viele Kunden Tags für die neuen Konfigurationsparameter bevorzugen. Um Mechanismen zur leichteren Bereitstellung dieser benutzerdefinierten DM-Tags anzubieten, enthält dieser Abschnitt ein Skript, das auf der Seite des Anwendungsservers (AS) ausgeführt werden kann, um den benutzerdefinierten DM-Tags Werte zuzuweisen. Dieses Skript ist insbesondere für neue Bereitstellungen vorgesehen, bei denen die meisten benutzerdefinierten DM-Tags verwendet werden sollen.

Beachten Sie, dass dieses Skript nur für neue Bereitstellungen gültig ist, in denen benutzerdefinierte DM-Tags erstellt werden. Um vorhandene benutzerdefinierte DM-Tags zu ändern, muss der Befehl im folgenden Skript von „add“ in „set“ geändert werden.

Skriptvorlage mit nur wenigen benutzerdefinierten Tags (in einer echten Bereitstellung müssten Sie eine größere Liste benutzerdefinierter Tags ausfüllen). Beachten Sie, dass das folgende Beispiel für Mobilgeräte gilt. Verwenden Sie für Desktop den Tag BroadTouch_tags anstelle von Connect_Tags. Verwenden Sie für Tablet den Tag „ConnectTablet_Tags“ anstelle von „Connect_Tags“.

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



Cisco – vertraulich

```
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------------------------------------------------------------------------------------------------------------
-----
%% Step 4: Verify custom tags have been correctly defined and set
%% ----------------------------------------------------------------------------------------------------------------
-----
quit all;System;DeviceTagSet;Tags
get tagSetName Connect_Tags
quit all
```

Im Folgenden werden alle benutzerdefinierten Tags aufgeführt, die von Webex für Cisco BroadWorks verwendet werden, mit Beispielwerten (Standard- oder empfohlenen Werten). Beachten Sie, dass einige der Tags spezifische Werte für die entsprechende Bereitstellung erfordern (z. B. Serveradressen). Aus diesem Grund werden diese Tags am Ende des Skripts hinzugefügt, aber leer gelassen, und zusätzliche Set-Befehle sollten hinzugefügt werden, um sie anzugeben.

## 10.1 Desktop

```
add tagSetName BroadTouch_tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_WXT% true
add tagSetName BroadTouch_tags %BLF_NOTIFICATION_DELAY_TIME_WXT% 0
add tagSetName BroadTouch_tags %ENABLE_REMOTE_CONTROL_EVENTS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName BroadTouch_tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName BroadTouch_tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName BroadTouch_tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PULL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MWI_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%
false
add tagSetName BroadTouch_tags
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%
false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%
false
add tagSetName BroadTouch_tags
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% false
add tagSetName BroadTouch_tags
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_USE_RPORT_WXT% false
add tagSetName BroadTouch_tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName BroadTouch_tags %USE_TLS_WXT% false
```



Cisco – vertraulich

```
add tagSetName BroadTouch_tags %SBC_PORT_WXT% 5075
add tagSetName BroadTouch_tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName BroadTouch_tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName BroadTouch_tags %SOURCE_PORT_WXT% 5060
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
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%
```



Cisco – vertraulich

```
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_BLIND_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_DIRECTED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% true
add tagSetName BroadTouch_tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
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
```



Cisco – vertraulich

```
add tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName BroadTouch_tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
```

## 10.2 Mobil

```
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
```



Cisco – vertraulich

```
add tagSetName Connect_Tags %SRTP_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_REKEYING_WXT% true
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName Connect_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName Connect_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName Connect_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName Connect_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName Connect_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName Connect_Tags %USE_MEDIASEC_WXT% false
add tagSetName Connect_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName Connect_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName Connect_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName Connect_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName Connect_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName Connect_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName Connect_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName Connect_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName Connect_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName Connect_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName Connect_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName Connect_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
```



Cisco – vertraulich

```
add tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName Connect_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName Connect_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName Connect_Tags %XSI_ROOT_WXT% true
add tagSetName Connect_Tags %SBC_ADDRESS_WXT% true
add tagSetName Connect_Tags %SBC_PORT_WXT% true
add tagSetName Connect_Tags %MWI_MODE_WXT% true
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName Connect_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
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
```



Cisco – vertraulich

```
add tagSetName Connect_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName Connect_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
```

## 10.3 Tablet

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



Cisco – vertraulich

```
add tagSetName ConnectTablet_Tags %ENABLE_REKEYING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName ConnectTablet_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName ConnectTablet_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName ConnectTablet_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName ConnectTablet_Tags %USE_MEDIASEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName ConnectTablet_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName ConnectTablet_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName ConnectTablet_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName ConnectTablet_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%
false
```



Cisco – vertraulich

```
add tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName ConnectTablet_Tags %XSI_ROOT_WXT% true
add tagSetName ConnectTablet_Tags %SBC_ADDRESS_WXT% true
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% true
add tagSetName ConnectTablet_Tags %MWI_MODE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
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
```



Cisco – vertraulich

```
add tagSetName ConnectTablet_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName ConnectTablet_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
```

## 10.4 Systemkennzeichnungen

In der folgenden Liste sind die von Webex für BroadWorks verwendeten System-Tags aufgeführt.

```
%BWNETWORK-CONFERENCE-SIPURI-n%
%BWVOICE-PORTAL-NUMBER-n%
%BWLINEPORT-n%
%BWHOST-n%
%BWAUTHUSER-n%
%BWAUTHPASSWORD-n%
%BWE164-n%
%BWNAME-n%
%BWEXTENSION-n%
%BWAPPEARANCE-LABEL-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMARY%
%BWE911-PRIMARY-HELDURL%
%BWE911-CUSTOMERID%
%BWE911-SECRETKEY%
%BWE911-EMERGENCY-NUMBER-LIST%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%
```



Cisco – vertraulich

# 11 Abkürzungen und Abkürzungen

In diesem Abschnitt werden die in diesem Dokument enthaltenen Akronyme und Abkürzungen aufgeführt. Die Akronyme und Abkürzungen werden in alphabetischer Reihenfolge zusammen mit ihren Bedeutungen aufgeführt.

| | |
|---|---|
| ACB | Automatischer Rückruf |
| ACD | Automatische Anrufverteilung |
| ACR | Ablehnen anonymer Anrufe |
| AES | Advanced Encryption Standard |
| ALG | Application Layer Gateway |
| API | Anwendungsprogrammierschnittstelle |
| APK | Anwendungspaket |
| APNS | Apple Push-Benachrichtigungsdienst |
| ARS | Automatische Bitratenauswahl |
| ALS | Anwendungsserver (Cisco BroadWorks) |
| AVP | Audio-visuelles Profil |
| BW | BroadWorks |
| BWA | BroadWorks Anywhere |
| BWKS | BroadWorks |
| BWM | BroadWorks-Mobilität |
| BYOD | Bring Your Own Device |
| CC | Callcenter |
| CFB | Rufumleitung bei Besetzt |
| CFNA | Rufumleitung bei Nichtantworten |
| CFNR | Rufumleitung nicht erreichbar |
| CIF | Allgemeines Zwischenformat |
| CLI | Befehlszeilenschnittstelle |
| CLID | Anrufleitungs-ID |
| CLIDB | Anrufleitungs-ID-Bereitstellungsblockierung |
| CRLF | Carriage Return Line Feed |
| CS | Schaltkreis gewechselt |
| Webansicht „CSWV | Anrufeinstellungen“ |
| CW | Anklopfen |
| Datenbank „DB | “ |
| DM | Geräteverwaltung |
| Ruhefunktion | Bitte nicht stören |



Cisco – vertraulich

| | |
|---|---|
| DNS | Domänennamensystem |
| Steuerung des DPC-Tischtelefons | |
| DTAF | Gerätetyp-Archivdatei |
| ECACS | Dienst zum Ändern der Notrufadresse |
| Konvergenz zwischen FMC und Festnetz-Mobil | |
| FQDN | Vollqualifizierter Domänenname |
| HMAC | Authentifizierungscode für Hash-Nachrichten |
| ICE | Interactive Connectivity Establishment |
| iLBC | Internet Niedriger Bitrate-Codec |
| Sofortnachrichten IM | |
| IM&P | Sofortnachrichten und Präsenz |
| IOT | Interoperabilitätsprüfung |
| IP | Internetprotokoll |
| JID | Jabber-ID |
| M/O | Obligatorisch/Optional |
| MNO | Mobilfunknetzbetreiber |
| MTU | Maximale Übertragungseinheit |
| MUC | Chat mit mehreren Benutzern |
| MWI | Anzeige für wartende Nachrichten |
| NAL | Netzwerk-Abstraktionsebene |
| NAPTR | Benennungsautoritätszeiger |
| NAT | Netzwerkadressenübersetzung |
| OTT | Über die Spitze |
| PA | Persönliche Assistentin |
| PAI | P-Asserted-Identity |
| PEM | P-Early-Medien |
| PLI | Anzeige des Bildverlusts |
| PLMN | Öffentliches Land Mobiles Netzwerk |
| PN | Push-Benachrichtigung |
| QCIF | Quartier Allgemeines Zwischenformat |
| QoS | Servicequalität |
| RO | Remote Office |
| RTCP | Echtzeit-Steuerungsprotokoll |
| RTP | Echtzeitprotokoll |
| SaaS | Software as a Service |
| SAN | Betreff für alternativen Namen |



Cisco – vertraulich

| | |
|---|---|
| SASL | Einfacher Authentifizierungs- und Sicherheitslayer |
| SAVP | Sicheres Audiovideoprofil |
| SBC | Session Border Controller |
| SCA | Gemeinsame Leitungsnutzung |
| SCF | Funktion „Sitzungskontinuität“ |
| SCTP | Stream Control Transmission Protocol |
| SDP | Sitzungsdefinitionsprotokoll |
| Sequentielles Klingelzeichen | absetzen |
| SIMRING | Gleichzeitiges Klingeln |
| SIP | Sitzungsinitiierungsprotokoll |
| SNR | Signal-zu-Lärm-Verhältnis |
| SNR | Single Number Reach |
| SRTCP | Sicheres Echtzeit-Steuerungsprotokoll |
| SRTP | Sicheres Echtzeit-Transportprotokoll |
| SSL | Secure Sockets Layer |
| STUN | Session Traversal Utilities für NAT |
| SUBQCIF | Unterviertel CIF |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TTL | Gültigkeitsdauer |
| TURN | Traversal mit Relay-NAT |
| UDP | Benutzerdatagramm-Protokoll |
| Benutzeroberfläche | Benutzeroberfläche |
| UMS | Messaging-Server (Cisco BroadWorks) |
| URI | Uniform Resource Identifier |
| UVS | Videoserver (Cisco BroadWorks) |
| VGA | Video-Grafik-Array |
| VoIP | Voice over IP |
| VVM | Visuelle Voicemail |
| WXT | Webex |
| XMPP | Extensible Messaging and Presence Protocol |
| XR | Erweiterter Bericht |
| Xsp | Xtended Services Platform |
| Xsi | Xtended Services Interface |



Cisco – vertraulich