Webex für Cisco BroadWorks – Konfigurationshandbuch

Version 45.4

Dokumentenversion 1

Inhaltsverzeichnis

1 Zusammenfassung der Änderungen 1
1.1 Änderungen für Release 45.4, April 2025 1
1.2 Änderungen für Release 45.3, März 2025 1
1.3 Änderungen für Version 45.2, Februar 2025 1
1.4 Änderungen für Version 45.1, Januar 2025 1
1.5 Änderungen für Version 44.12, Dezember 2024 1
1.6 Änderungen für Version 44.11, November 2024 1
1.7 Änderungen für Version 44.10, Oktober 2024 1
1.8 Änderungen für Version 44.9, September 2024 2
1.9 Änderungen für Release 44.8, August 2024 2
1.10 Änderungen für Version 44.7, Juli 2024 2
1.11 Änderungen für Version 44.6, Juni 2024 2
1.12 Änderungen für Version 44.5, Mai 2024 2
1.13 Änderungen für Version 44.4, April 2024 2
1.14 Änderungen für Version 44.3, März 2024 2
1.15 Änderungen für Release 44.2, Februar 2024 3
1.16 Änderungen für Release 44.1, Januar 2024 3
2 Änderungen an Konfigurationsdateien 4
2.1 Änderungen an den Konfigurationsdateien für Version 45.4 4
2.2 Änderungen bei den Konfigurationsdateien für Version 45.3 4
2.3 Änderungen bei den Konfigurationsdateien für Version 45.2 4
2.4 Änderungen an den Konfigurationsdateien für Version 45.1 4
2.5 Änderungen an den Konfigurationsdateien für Version 44.12 4
2.6 Änderungen an den Konfigurationsdateien für Version 44.11 4
2.7 Änderungen bei den Konfigurationsdateien für Version 44.10 5
2.8 Änderungen bei den Konfigurationsdateien für Version 44.9 5
2.9 Änderungen an den Konfigurationsdateien für Version 44.8 5
2.10 Änderungen an den Konfigurationsdateien für Version 44.7 5
2.11 Änderungen bei den Konfigurationsdateien für Version 44.6 5
2.12 Änderungen bei den Konfigurationsdateien für Version 44.5 6
2.13 Änderungen bei den Konfigurationsdateien für Version 44.4 6
2.14 Änderungen bei den Konfigurationsdateien für Version 44.3 6
2.15 Änderungen an den Konfigurationsdateien für Version 44.2 7
2.16 Änderungen bei den Konfigurationsdateien für Version 44.1 9
3 Einführung 10
4 Installation 11
4.1 Lokalisierter Client-Download 11
4.2 Android-Client 11
4.3 iOS-Client 11

Vertrauliche Informationen von Cisco

4.4 Desktop-Client ... 12
5 Geräteverwaltung ... 13
5.1 Tags für die Geräteverwaltung ... 13
5.2 Verbesserungen bei der teilweisen Übereinstimmung bei der Auswahl des Gerätetyps ... 14
5.3 Client-Konfiguration ... 15
5.4 Bereitstellung von config-wxt.xml ... 15
5.5 Konfigurationsdatei (config-wxt.xml) ... 15
5.6 Systemstandard-Tags ... 16
5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags ... 16
6 Benutzerdefinierte Tags ... 19
6.1 Gemeinsame Merkmale ... 32
6.1.1 SIP-Server-Einstellungen ... 32
6.1.2 SIP über TLS und Secure Real-Time Transport Protocol ... 35
6.1.3 3GPP SIP-Header für SRTP ... 38
6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives ... 38
6.1.5 Konfigurierbarer Timeout für das Öffnen des SIP-Sockets ... 40
6.1.6 Dynamische SIP-Proxy-Erkennung ... 41
6.1.7 Bevorzugte Portverwendung für SIP ... 47
6.1.8 SIP-Failover und -Failback ... 47
6.1.9 SIP SUBCSRIBE und REGISTER Aktualisieren und SUBSCRIBE Wiederholen ... 52
6.1.10 P-assoziierte URIs in REGISTER verwenden ... 53
6.1.11 PEM-Header (SIP P-Early Media) ... 53
6.1.12 Unterstützung für SIP-UPDATES ... 54
6.1.13 Ältere SIP-INFO-FIR ... 54
6.1.14 SIP-Port-Verwaltung für NAT-Transversale ... 55
6.1.15 SIP-Sitzungs-ID ... 56
6.1.16 Ablehnungsverhalten bei eingehendem Anruf ... 56
6.1.17 Portbereich des Echtzeit-Transportprotokolls ... 57
6.1.18 ICE-Unterstützung (nur Webex Calling) ... 57
6.1.19 RTCP MUX ... 58
6.1.20 Übergabe ... 59
6.1.21 N-Way-Konferenzanrufe und Teilnehmer ... 60
6.1.22 Anruf pull ... 61
6.1.23 Anruf parken/abrufen ... 61
6.1.24 Anrufstatistik ... 62
6.1.25 Automatische Wiederherstellung von Anrufen/nahtlose Anrufübergabe ... 62
6.1.26 Anrufaufzeichnung ... 63
6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige ... 64
6.1.28 Voicemail-Transkription für Webex Calling ... 66
6.1.29 Anrufeinstellungen ... 67
6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen ... 69

Vertrauliche Informationen von Cisco

6.1.31 Callcenter/Anrufwarteschlange – An-/Abmeldung ... 73
6.1.32 XSI-Stamm und -Pfade ... 73
6.1.33 XSI-Ereigniskanal ... 74
6.1.34 Codec-Konfiguration ... 75
6.1.35 SIP-URI-Wahl ... 77
6.1.36 Anrufverlauf auf allen Geräten ... 78
6.1.37 Videoanrufe deaktivieren ... 78
6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter ... 79
6.1.39 PAI als Identität ... 80
6.1.40 Bildschirmfreigabe deaktivieren ... 81
6.1.41 Spam-Anrufanzeige ... 81
6.1.42 Rauschunterdrückung und Bandbreitenerweiterung für Festnetz-/Mobilanrufe ... 81
6.1.43 QoS DSCP Kennzeichnung ... 82
6.1.44 Primärprofil ... 83
6.1.45 Sperrliste (nur Webex Calling) ... 84
6.1.46 Implementierung von Medienanpassung und Resilienz (MARI) ... 85
6.1.47 gleichzeitige Anrufe mit demselben Benutzer ... 87
6.1.48 RTCP-XR ... 88
6.1.49 Informationen zur Anrufumleitung ... 88
6.1.50 Anrufer-ID ... 89
6.1.51 Mehrzeilig ... 92
6.1.52 Erweiterte SIP-Autorisierung ... 93
6.1.53 persönlicher Assistent (Abwesenheitspräsenz) ... 94
6.2 Nur-Desktop-Funktionen ... 96
6.2.1 Erzwungene Abmeldung ... 96
6.2.2 Anrufübernahme ... 97
6.2.3 Boss-Admin (Executive-Assistant) Support ... 97
6.2.4 SIP-Anrufe an Meeting eskalieren (nur Webex Calling) ... 98
6.2.5 Anrufsteuerung – Automatische Anrufannahme ... 98
6.2.6 Automatische Antwort mit Tonbenachrichtigung ... 99
6.2.7 Steuerung des Tischtelefons – Steuerung während eines Anrufs – Konferenz ... 99
6.2.8 Benachrichtigungen zur Anrufübernahme ... 100
6.2.9 Ereignispaket für die Fernsteuerung ... 102
6.2.10 Anrufwarteschlangen-Agenten-CLID-Auswahl ... 103
6.2.11 Gateway zur Überlebensfähigkeit (nur Webex Calling) ... 103
6.2.12 Ereignispaket für die Remote-Stummschaltung (nur Webex Calling) ... 104
6.2.13 Anruf verschieben ... 105
6.3 Mobile Only-Funktionen ... 107
6.3.1 Notruf ... 107
6.3.2 Push-Benachrichtigungen für Anrufe ... 108
6.3.3 Einzelne Benachrichtigungen ... 111
6.3.4 Klicken zum Wählen (Rückruf) ... 111

Vertrauliche Informationen von Cisco

6.3.5 MNO-Unterstützung 112
6.3.6 ID des eingehenden Anrufers 117
7 Funktionen von Early Field Trial (BETA) 119
8 Zuordnung benutzerdefinierter Tags zwischen Webex für Cisco BroadWorks und UC-One 120
9 Anhang A: TLS Chiffren 128
10 Anhang B: DM-Tag-Bereitstellungsskript 129
10.1 Desktops 130
10.2 Mobil 133
10.3 Tablette 136
10.4 System-Tags 139
11 Akronyme und Abkürzungen 140

Vertrauliche Informationen von Cisco

1 Zusammenfassung der Änderungen

In diesem Abschnitt werden die Änderungen an diesem Dokument für jede Version und Dokumentversion beschrieben.

1.1 Änderungen für Release 45.4, April 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Verschobener Abschnitt *6.1.34.1 KI-Codec* – aus der BETA.
- Abschnitt *6.1.51 Mehrzeilig* hinzugefügt – kombinierte die reinen Desktop- und mobilen BETA-Abschnitte.
- Verschobener Abschnitt *6.1.52 Erweiterte SIP-Autorisierung* – aus der BETA.
- Der Abschnitt *6.1.53 persönlicher Assistent (Abwesenheitspräsenz)* wurde wie üblich für Desktop und Mobilgeräte verschoben

1.2 Änderungen für Release 45.3, März 2025

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.3 Änderungen für Version 45.2, Februar 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *Erweiterte SIP-Autorisierung**Error! Reference source not found.*** in BETA hinzugefügt.

1.4 Änderungen für Version 45.1, Januar 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *persönlicher Assistent (Abwesenheitspräsenz)* aus der BETA verschoben.
- Abschnitt *6.3.2.3 Liefermodus (nur Webex Calling)* aus der BETA verschoben.

1.5 Änderungen für Version 44.12, Dezember 2024

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.6 Änderungen für Version 44.11, November 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *Mobil (nur Webex Calling)* in BETA hinzugefügt.

1.7 Änderungen für Version 44.10, Oktober 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *persönlicher Assistent (Abwesenheitspräsenz)* in BETA***Error! Reference source not found.*** hinzugefügt.
- Abschnitt *Liefermodus (nur Webex Calling)* in BETA hinzugefügt.

Vertrauliche Informationen von Cisco

1.8 Änderungen für Version 44.9, September 2024

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.9 Änderungen für Release 44.8, August 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.34 Codec-Konfiguration* – Klarstellung zu den DTMFs und den unterstützten Übermittlungsmechanismen hinzugefügt.

1.10 Änderungen für Version 44.7, Juli 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *KI-Codec* in BETA hinzugefügt.
- Aktualisierter Abschnitt *6.1.44 Primäres Profil* – Details zum Verhalten der Webex App wurden von vornherein zu Version 43.2 entfernt.

1.11 Änderungen für Version 44.6, Juni 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.3.6. ID des eingehenden* Anrufers – Weitere Details zur nativen Erfahrung und zur Funktionsweise der Funktion wurden hinzugefügt.

1.12 Änderungen für Version 44.5, Mai 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

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

1.13 Änderungen für Version 44.4, April 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.50.1 ID des ausgehenden* Anrufers.
- Aktualisierter Abschnitt *Änderungen bei den Konfigurationsdateien für Version 44.3* – Details zu den Keepalive-Updates in 44.3 hinzugefügt.

1.14 Änderungen für Version 44.3, März 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.3.6. ID des eingehenden* Anrufers
    - Der Abschnitt *6.1.50.1 ID des ausgehenden* Anrufers wurde wie für Desktop und Mobile üblich verschoben und mit mehr Details aktualisiert.
- Aktualisierter Abschnitt *6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives* – Details zu den konfigurierbaren Keepalives mit benutzerdefinierten Tags hinzugefügt.

Vertrauliche Informationen von Cisco

1.15 Änderungen für Release 44.2, Februar 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt hinzugefügt *6.3.6 ID des eingehenden* Anrufers
- Aktualisierter Abschnitt *6.2.8 Benachrichtigungen zur Anrufübernahme*
    - Unterabschnitt *6.2.8.1 Besetztlampenfeld* hinzugefügt – BLF Einzelheiten darin verschoben.
    - Unterabschnitt *6.2.8.2 Anrufübernahmegruppe (nur Webex Calling)* hinzugefügt.
- Abschnitt *6.1.49 Informationen zur Anrufumleitung* hinzugefügt.
- Aktualisierter Abschnitt *6.1.8.3 Erzwingen IP Version* – Details für den neuen *nat64-Modus* hinzugefügt.
- Aktualisierter Abschnitt *6.1.42 Rauschunterdrückung und Bandbreitenerweiterung für Festnetz-/Mobilanrufe* – Details zur neuen Unterstützung der Bandbreitenerweiterung und zu den Aktualisierungen zur Rauschunterdrückung hinzugefügt. Der Abschnitt *"Sprachverbesserungen für Festnetzanrufe* " wurde aus der Betaversion entfernt.

1.16 Änderungen für Release 44.1, Januar 2024

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

Vertrauliche Informationen von Cisco

2 Änderungen an Konfigurationsdateien

2.1 Änderungen an den Konfigurationsdateien für Version 45.4

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

2.2 Änderungen bei den Konfigurationsdateien für Version 45.3

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

2.3 Änderungen bei den Konfigurationsdateien für Version 45.2

- [BETA-Funktion]
  Das Tag <enhanced-authorization> wurde im Abschnitt <protocols><sip> hinzugefügt.

```
<Konfiguration>
<Protokolle>
  <Schluck>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Folgender %TAG% wurde hinzugefügt:

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.4 Änderungen an den Konfigurationsdateien für Version 45.1

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

2.5 Änderungen an den Konfigurationsdateien für Version 44.12

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

2.6 Änderungen an den Konfigurationsdateien für Version 44.11

- [BETA-Funktion] [Nur Mobilgeräte] [Nur Webex Calling]
  Das Attribut mit mehreren Leitungen wurde im Tag <protocols><sip><lines> hinzugefügt.
  Die Abschnitte <persönlich> und <Leitung> für die sekundären Leitungen wurden unter <Protokolle><sip><Leitungen> hinzugefügt.

```
<Konfiguration>
<Protokolle><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
   <Persönlich>
      <Leitungsport>%BWDISPLAYNAMELEITUNGSPORT%</Leitungsport>
   </persönlich>
   <line lineType="%BW-MEMBERTYPE-1%">
      …
   </Leitung>
   <line lineType="%BW-MEMBERTYPE-2%">
      …
   </Leitung>
   …
   <line lineType="%BW-MEMBERTYPE-10%">
      …
   </Leitung>
```


Vertrauliche Informationen von Cisco

```
</Zeilen>
```

2.7 Änderungen bei den Konfigurationsdateien für Version 44.10

- [BETA-Funktion]
  Das Tag <personal-assistant> wurde im Abschnitt <Services> hinzugefügt.

```
<Konfiguration>
<Dienstleistungen>
   <personal-assistant enabled="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

- [BETA-Funktion] [Nur Mobilgeräte] [Nur Webex Calling]
  Unter dem Tag <services><push-notifications-for-calls> wurde das Attribut "delivery mode" hinzugefügt.

```
<Konfiguration>
<Dienstleistungen>
   <push-notifications-for-calls enabled="true" Connect-sip-on-
accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%" ring-Timeout-
seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%" delivery-
mode="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

Die folgenden %TAG%s wurden hinzugefügt:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.8 Änderungen bei den Konfigurationsdateien für Version 44.9

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

2.9 Änderungen an den Konfigurationsdateien für Version 44.8

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

2.10 Änderungen an den Konfigurationsdateien für Version 44.7

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

```
<Konfiguration>
<Services><Anrufe>
  <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="telefon-ereignis" payload="101" in-band="false"/>
```

2.11 Änderungen bei den Konfigurationsdateien für Version 44.6

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

Vertrauliche Informationen von Cisco

2.12 Änderungen bei den Konfigurationsdateien für Version 44.5

- [Nur Webex Calling]
  Das Attribut enable-IPv6-Support wurde dem Tag <protocols><rtp><ice> hinzugefügt.

```
<Konfiguration>
<Protokolle><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%"/>
```

- Im Abschnitt <services><calls><caller-id> wurde der Tag <Remote-name> mit <machine> als untergeordnetem Tag hinzugefügt.

```
<Konfiguration>
<Services><Anrufe>
   <Anrufer-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%

2.13 Änderungen bei den Konfigurationsdateien für Version 44.4

- [Nur Desktop] [Nur Webex Calling]
  Die Tags <additional-numbers>, <hunt-group> und <clid-delivery-blocking> wurden im Abschnitt <Anrufer-ID><ausgehende-Anrufe> hinzugefügt.

```
<Konfiguration>
<Services><Anrufe>
  <Anrufer-ID>
    <ausgehende-anrufe aktiviert="%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%"/>
      <Sammelanschlussgruppe
aktiviert="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </ausgehende Anrufe>
```

2.14 Änderungen bei den Konfigurationsdateien für Version 44.3

- [Nur Desktop] [Nur Webex Calling]
  Unter dem neuen Abschnitt <Anrufer-ID> wurde <ausgehende Anrufe> mit <Callcenter> als untergeordnetem Tag hinzugefügt.

```
<Konfiguration>
<Services><Anrufe>
  <Anrufer-ID>
    <ausgehende-anrufe aktiviert="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <call-Center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_Center_WXT%"/>
    </ausgehende Anrufe>
```


Vertrauliche Informationen von Cisco

- Es wurden benutzerdefinierte Tags (%UDP_KEEPALIVE_ENABLED_WXT%, %TCP_KEEPALIVE_ENABLED_WXT% und %TLS_KEEPALIVE_ENABLED_WXT%) hinzugefügt, um den hartcodierten Keep-Alive-aktivierten Wert für jeden Transport unter <protocols><sip><Transports> zu ersetzen.

```
<Konfiguration>
<Protokolle><sip>
<Transporte>
  <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:

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

2.15 Änderungen an den Konfigurationsdateien für Version 44.2

- [Nur Mobilgeräte]
  Der Abschnitt <Anrufer-ID> wurde unter <services><calls> hinzugefügt. Die Unter-Tags <eingehender Anruf> und <verpasster Anruf> wurden hinzugefügt, wobei für beide neue Unter-Tags <Nummer> angehängt wurden.

```
<Konfiguration>
<Services><Anrufe>
  <Anrufer-ID>
    <Eingehende Anrufe>
      <append-number
enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
    </eingehende Anrufe>
    <Verpasste Anrufe>
      <append-number
enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
    </verpasste Anrufe>
```

- [Nur Mobilgeräte] [Nur Webex Calling]
  <ausgehende Anrufe> wurde unter dem neuen Abschnitt <Anrufer-ID> hinzugefügt.

```
<Konfiguration>
<Services><Anrufe>
  <Anrufer-ID>
    <ausgehende-anrufe aktiviert="%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%"/>
```


Vertrauliche Informationen von Cisco

```
      <Sammelanschlussgruppe
aktiviert="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </ausgehende Anrufe>
```

- Das Tag <call-forwarding-Info> wurde im Abschnitt <services><calls> hinzugefügt.

```
<Konfiguration>
<Services><Anrufe>
  <call-forwarding-Info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

- [Nur Desktop] [Nur Webex Calling]
  Der Abschnitt <group-call-pickup-notifications> wurde unter <services><calls> mit <display-caller> und <max-Timeout> als Unter-Tags hinzugefügt. Außerdem wurde im Abschnitt <Protokolle><sip><Leitungen>> unter jedem <line-Tag >Tag <group-call-pickup hinzugefügt.

```
<Konfiguration>
<Services><Anrufe>
  <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%"/>
  <-/Gruppenanruf-Pickup-Benachrichtigungen>
  …
<Protokolle><sip>
  <Zeilen>
    <Zeile>
      <Gruppenanrufübernahme>%BWGROUP-ANRUFÜBERNAHME-BOOL-
1%</Gruppenanrufübernahme>
      ...
    </Leitung>
    <Zeile>
      <gruppenanrufübernahme>%BWGROUP-ANRUFÜBERNAHME-BOOL-
2%</gruppenanrufübernahme>
      ...
    </Leitung>
    …
```

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%

Vertrauliche Informationen von Cisco

- %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%
- %BWGROUP-CALL-PICKUP-BOOL-n%

Folgender %TAG% ist veraltet:

- %ENABLE_NOISE_REMOVAL_WXT%

2.16 Änderungen bei den Konfigurationsdateien für Version 44.1

Die Konfigurationsdateien für diese Version wurden nicht aktualisiert.

Vertrauliche Informationen von Cisco

3 Einführung

Zweck dieses Dokuments ist es, eine Beschreibung der Konfiguration des Webex für den Cisco BroadWorks-Client bereitzustellen.

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

Die Clients werden mit einer Konfiguration konfiguriert, die für den Benutzer nicht sichtbar ist. Der *config-wxt.xml* stellt serverspezifische Informationen bereit, wie z. B. Serveradressen und Ports sowie Laufzeitoptionen für den Client selbst (z. B. Optionen, die im Einstellungsbildschirm angezeigt werden).

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

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

Vertrauliche Informationen von Cisco

4 Installation

Die Webex für Cisco BroadWorks-Clients können über eine der folgenden Optionen 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 Applikation (Android Application Package [APK]) installiert, der die einstellungs- und konfigurationsrelevanten Daten in seinem privaten Bereich speichert.

Es gibt eine Versionskontrolle, die auf den Google Play-Verfahren basiert. Es wird eine Google Play-Standardbenachrichtigung bereitgestellt, d. h., Android meldet automatisch, dass eine neue Version der Software verfügbar ist.

Wenn die neue Version heruntergeladen wird, wird die alte Software überschrieben. Die Benutzerdaten werden jedoch standardmäßig aufbewahrt.

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" hält und die Daten der Konfigurationsdatei verschlüsselt speichert.

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

Wenn die neue Version heruntergeladen wird, wird die alte Software überschrieben. Die Benutzerdaten werden jedoch standardmäßig aufbewahrt.

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

Vertrauliche Informationen von Cisco

4.4 Desktop-Client

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

Vertrauliche Informationen von Cisco

5 Geräteverwaltung

5.1 Tags für die Geräteverwaltung

Webex für Cisco BroadWorks verwendet die *Tag-Sets* für die Geräteverwaltung in der folgenden Abbildung dargestellt. Der *Systemstandard* und benutzerdefinierte Tag-Sets sind erforderlich, um bestimmte Geräte-/Clienteinstellungen bereitzustellen. Dieser Tag-Satz bietet Flexibilität bei der Verwaltung der Netzwerk-/Service-Konnektivitätseinstellungen des Clients sowie von Steuerelementen für die Funktionsaktivierung.

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

- Mobil: Connect_Tags
- Tablette: ConnectTablet_Tags
- Desktop: BroadTouch_Tags

Erstellen Sie jedes einzelne Tag und legen Sie seinen Wert fest. Abschnittsverweise enthalten detaillierte Beschreibungen für die einzelnen Tags. Die benutzerdefinierten Tags werden basierend auf der Funktionalität in Gruppen unterteilt und weiter unten in diesem Dokument erläutert.

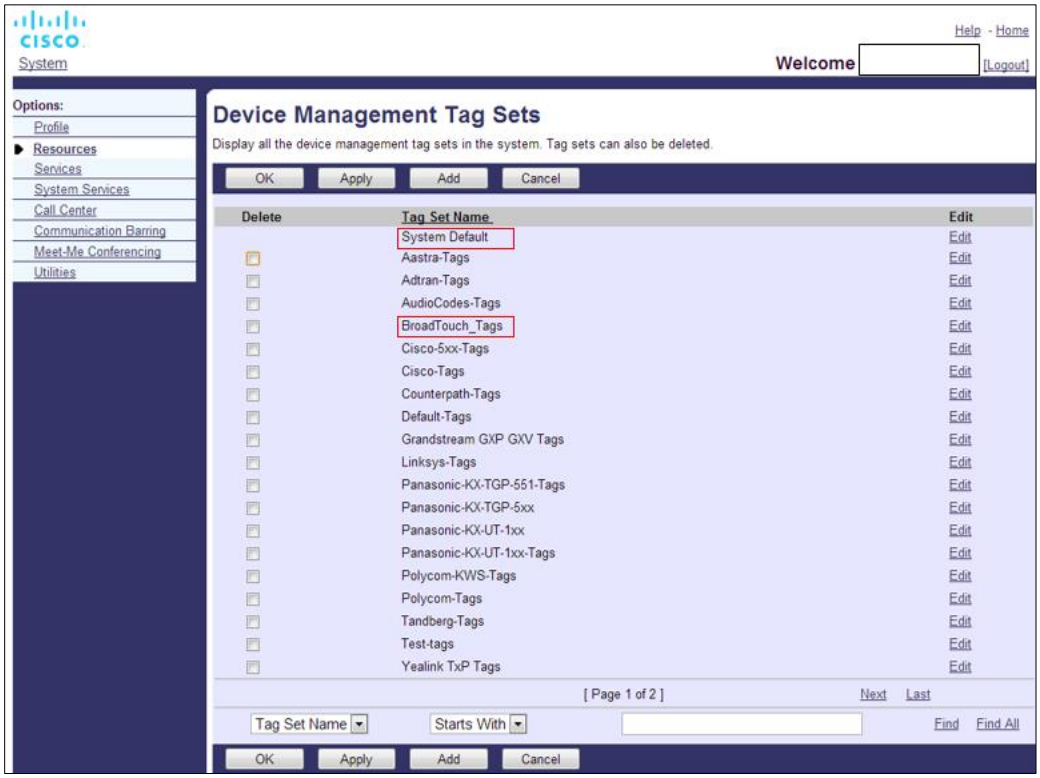


Abbildung 1 der Tag-Sets für die Verwaltung von Desktopgeräten

Vertrauliche Informationen von Cisco

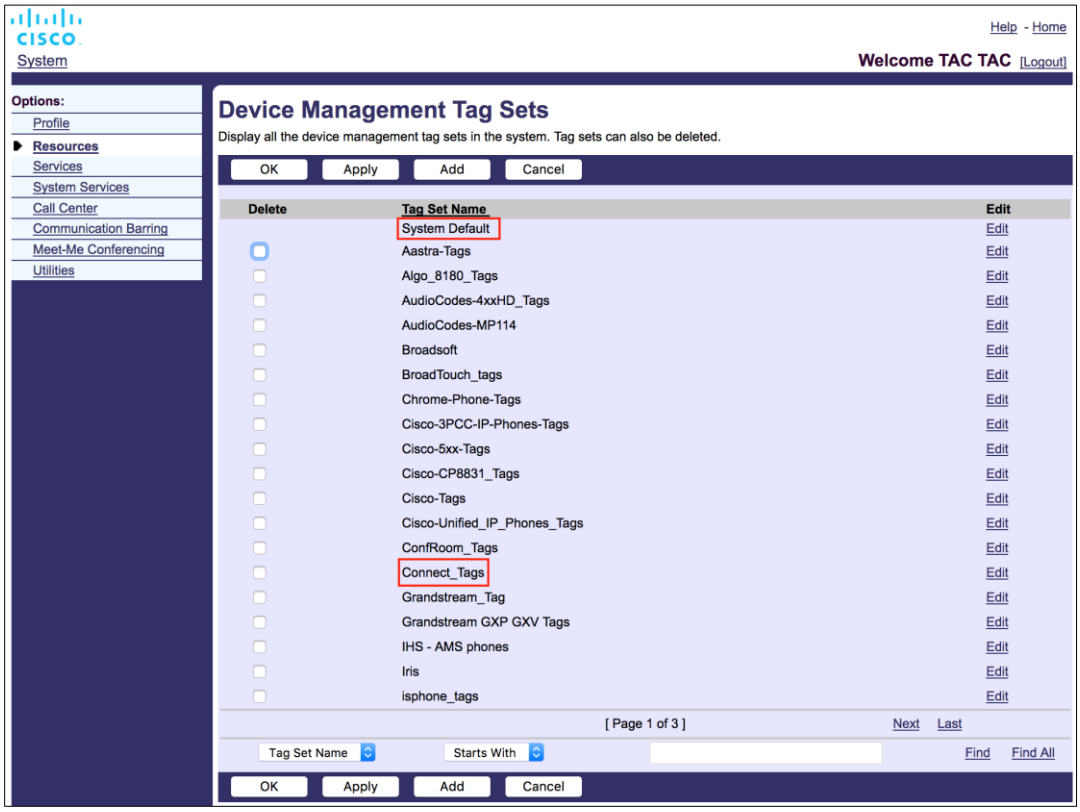


Abbildung 2 Tagsätze für die Verwaltung mobiler Geräte

5.2 Verbesserungen bei der teilweisen Übereinstimmung bei der Auswahl des Gerätetyps

Um eine erhöhte Flexibilität bei der Auswahl von Funktionspaketen für Benutzergruppen oder einzelne Benutzer zu ermöglichen, wird der Geräteprofiltyp auf der Grundlage einer (ersten) Teilübereinstimmung ausgewählt. Dies ermöglicht es Kunden, verschiedene Gerätetypen zu verwenden.

Das allgemeine Verfahren zur Geräteverwaltung gibt an, dass der Cisco BroadWorks-Anwendungsserver einen Geräteprofiltyp bereitstellt. Es heißt "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 die zugeordnete Geräteliste über Xsi ab und sucht nach dem entsprechenden Gerätetypprofil. Der Client wählt das erste Profil aus, das mit dem entsprechenden Gerätetypnamen beginnt. Anschließend werden die diesem Geräteprofil zugeordneten Konfigurationsdaten (Konfigurationsdatei) verwendet, um verschiedene Funktionen zu aktivieren und zu deaktivieren.

Auf diese Weise kann dieselbe ausführbare Clientdatei mit verschiedenen Geräteprofiltypen verwendet werden, sodass der Dienstanbieter Funktionspakete für einzelne Benutzer oder Benutzergruppen ändern kann, indem er einfach den Geräteprofiltyp in DM für einen Benutzer oder eine Benutzergruppe ändert.

Vertrauliche Informationen von Cisco

Der Dienstanbieter kann z. B. über eine beliebige Anzahl von Geräteprofiltypen verfügen, die auf Benutzerrollen basieren, z. B. "Business Communicator – PC Basic", "Business Communicator – PC Executive" oder "Business Communicator – PC-Assistent", und die verfügbaren Funktionen für einzelne Benutzer ändern, indem der Geräteprofiltyp für diese Benutzer geändert wird.

Beachten Sie, dass nicht erwartet wird, dass die Liste der empfangenen Geräteprofile mehrere übereinstimmende Geräteprofiltypen XML sondern nur einen enthält.

5.3 Client-Konfiguration

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

5.4 Bereitstellung von config-wxt.xml

Fügen Sie die entsprechende *config-wxt.xml-Datei* 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.

HINWEIS 1: Für jedes Geräteprofil muss eine Konfigurationsdatei vorhanden sein.

HINWEIS 2: Es wird dringend 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 **_WXT** Suffix werden verwendet, um die neue Webex für die Cisco BroadWorks-Konfigurationsbereitstellung von älteren Clients zu unterscheiden. Es gibt jedoch immer noch einige (System-)Tags, die von UC-One und Webex gemeinsam genutzt werden.

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

- %BWNETWORK-KONFERENZ-SIPURI-n%
- %BWVOICE-PORTAL-NUMMER-N%
- %BWLINEPORT-n%
- %BWAUTHUSER-n%
- %BWAUTHPASSWORT-n%
- %BWE164-n%
- %BWHOST-n%
- %BWNAME-n%
- %BW-Durchwahl-n%
- %BWAUSSEHEN-LABEL-n%

Vertrauliche Informationen von Cisco

- %BWDISPLAYNAMELINEPORT%
- %BWLINEPORT-PRIMARY%
- %BWE911-PRIMÄRE-HELDURL%
- %BWE911-KUNDENID%
- %BWE911-GEHEIMSCHLÜSSEL%
- %BWE911-NOTRUFNUMMERNLISTE%
- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (nur Webex Calling)

5.6 Systemstandard-Tags

Als Systemadministrator können Sie über die Option "Tag-Sets *für* System → Ressourcen → Geräteverwaltung" auf die Systemstandard-Tags zugreifen. Die folgenden Systemstandard-Tags müssen bereitgestellt werden, wenn das VoIP Anrufpaket installiert wird.

Etikett	Beschreibung
%SBC_ADDRESS_WXT%	Dieser sollte als FQDN (Fully Qualified Domain Name) oder als IP Adresse des im Netzwerk bereitgestellten SBC (Session Border Controller) konfiguriert werden. Beispiel: sbc.yourdomain.com
%SBC_PORT_WXT%	Wenn es sich bei dem SBC_ADDRESS_WXT um eine IP Adresse handelt, sollte dieser Parameter auf den SBC-Port festgelegt werden. Wenn der SBC_ADDRESS_WXT ein FQDN ist, kann er nicht festgelegt werden. Beispiel: 5075

5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags

Zusätzlich zu den standardmäßigen Systemtags und den benutzerdefinierten Tags, die definiert werden müssen, gibt es vorhandene Cisco BroadWorks Systemtags, die in der Regel verwendet werden und Teil der empfohlenen Device Type Archive File (DTAF) sind. Diese Tags werden in diesem Abschnitt aufgelistet. Je nach installiertem Lösungspaket werden nicht alle Systemtags verwendet.

Etikett	Beschreibung
%BWNETWORK-KONFERENZ-SIPURI-n%	Dies ist der Server URI der verwendet wird, um N-Way-Konferenzen zu aktivieren.
%BWVOICE-PORTAL-NUMMER-N%	Diese Nummer wird für Voicemail verwendet. Der Client wählt diese Nummer, wenn er Voicemail abruft.
%BWLINEPORT-n%	SIP-Benutzername, der bei der SIP-Signalisierung verwendet wird, z. B. bei der Registrierung.

Vertrauliche Informationen von Cisco

Etikett	Beschreibung
%BWHOST-n%	Dies ist der Domänenteil des bereitgestellten Leitungsports für das Gerät, der dem Benutzer zugewiesen ist. Sie wird aus dem Profil des Benutzers abgerufen. Wird in der Regel als SIP-Domäne verwendet.
%BWAUTHUSER-n%	Dies ist der Benutzername für die Authentifizierung. Wenn dem Abonnenten die Authentifizierung zugewiesen wurde, ist dies die bereitgestellte Benutzer-ID auf der Seite "Authentifizierung", unabhängig vom ausgewählten Authentifizierungsmodus des Gerätetyps. Der SIP-Benutzername, der normalerweise bei 401- und 407-Signalen verwendet wird. Kann sich vom SIP-Standardbenutzernamen unterscheiden.
%BWAUTHPASSWORT-n%	Dies ist das Authentifizierungskennwort des Benutzers. Wenn dem Abonnenten die Authentifizierung zugewiesen wurde, ist dies das auf der Seite "Authentifizierung" bereitgestellte Kennwort, unabhängig vom ausgewählten Authentifizierungsmoduswert des Gerätetyps. Das für die SIP-Signalisierung verwendete SIP-Kennwort.
%BWE164-n%	Dieser Tag stellt die Telefonnummer des Benutzers im internationalen Format bereit.
%BWNAME-n%	Dies ist der Vor- und Nachname des Abonnenten im Profil des Benutzers. Der Vor- und Nachname werden miteinander verkettet. Bei mehrzeiliger Konfiguration, wenn keine Leitungsbeschreibung konfiguriert und wenn nicht leer, wird diese als Anzeigename für die Leitung im Leitungswahlschalter verwendet.
%BW-Durchwahl-n%	Die Durchwahl des Abonnenten wird von der Durchwahl abgerufen, die im Profil des Benutzers angegeben ist. Wenn kein Anschluss bereitgestellt wurde, wird das Tag durch die Telefonnummer (DN) des Teilnehmers ersetzt.
%BWAUSSEHEN-LABEL-n%	Dies ist die konfigurierte Leitungsbeschreibung. 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 (Shared Call Appearance). Dies ist der Leitungsport, der auf dem dem Benutzer zugewiesenen Gerät bereitgestellt wird. Dieser wird aus dem Profil des Benutzers abgerufen. Wird verwendet, um die primäre Leitung des Benutzers zu identifizieren.

Vertrauliche Informationen von Cisco

Etikett	Beschreibung
%BWLINEPORT-PRIMARY%	Der Port der primären Leitung 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-PRIMÄRE-HELDURL%	Gibt die URL zur RedSky Emergency Location Platform an, die das HELD-Protokoll unterstützt.
%BWE911-KUNDENID%	Die Kunden-ID (HeldOrgId, CompanyID), die für die RedSky-HTTPS-Anforderung verwendet wird.
%BWE911-GEHEIMSCHLÜSSEL%	Das Geheimnis, um die RedSky-HTTPS-Anforderung zu authentifizieren.
%BWE911-NOTRUFNUMMERNLISTE%	Die Liste der Notrufnummern, die von RedSky unterstützt werden. Um dieses Tag verwenden zu können, muss das benutzerdefinierte Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% Reserved dem Tagsatz des Gerätetyps hinzugefügt werden. Das "reserved"-Tag muss die Notrufnummern, die auf BroadWorks unter AS_CLI/System/CallP/CallTypes > definiert sind, in einem durch Kommas getrennten Format enthalten, z. B. 911, 0911, 933. **HINWEIS:** Der Webex Client unterstützt keine Platzhalter in Notrufnummern. Daher sollten nur exakte Notrufnummern zum benutzerdefinierten Tag "reserviert" hinzugefügt werden. Das folgende Beispiel zeigt, wie die Funktionalität des reservierten Tags verwendet werden soll: 1) Der native Tag %BWE911-EMERGENCY-NUMBER-LIST% wird der Vorlagendatei des Geräts hinzugefügt 2) Der reservierte benutzerdefinierte Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% wird dem Tag-Satz hinzugefügt, der vom Gerät mit dem Wert 911, 0911, 933 verwendet wird 3) Wenn die Datei neu erstellt wird, wird das native Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% in 911, 0911, 933 aufgelöst
%BW-MEMBERTYPE-n%	Dies ist der Typ für jede Leitung. Dabei kann es sich um "virtuelles Profil", "Benutzer" oder "Ort" handeln.
%BWUSEREXTID-n%	Dies ist die externe ID für die angegebene Leitung (nur Webex Calling)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Zeigt Informationen an, ob für die entsprechende Leitung eine Anrufübernahmegruppe konfiguriert ist. (Nur Webex Anrufe)

Vertrauliche Informationen von Cisco

6 Benutzerdefinierte Tags

In diesem Abschnitt werden die benutzerdefinierten Tags beschrieben, die in Webex für Cisco BroadWorks verwendet werden. Es listet alle benutzerdefinierten Tags auf, die sowohl für Desktop- als auch für Mobil-/Tablet-Plattformen verwendet werden.

Beachten Sie jedoch, dass einige der in diesem Abschnitt beschriebenen Einstellungen nur für die jeweilige Version des Clients unterstützt werden. Um festzustellen, ob eine Einstellung nicht auf eine ältere Clientversion zutrifft, lesen Sie das entsprechende versionsspezifische Konfigurationshandbuch.

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_REJECT_WITH_486_WXT%	J	J	true	*6.1.16 Ablehnungsverhalten bei eingehendem Anruf*
%REJECT_WITH_XSI_MODE_WXT%	N	J	decline_false	*6.3.2 Push-Benachrichtigungen für Anrufe*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	J	Besetzt	*6.3.2 Push-Benachrichtigungen für Anrufe*
%ENABLE_TRANSFER_CALLS_WXT%	J	J	false	*6.1.20 Übergabe*
%ENABLE_CONFERENCE_CALLS_WXT%	J	J	false	*6.1.21 N-Way-Konferenzanrufe und Teilnehmer*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	J	J	false	*6.1.21 N-Way-Konferenzanrufe und Teilnehmer*
%MAX_CONF_PARTIES_WXT%	J	J	10	*6.1.21 N-Way-Konferenzanrufe und Teilnehmer*
%ENABLE_CALL_STATISTICS_WXT%	J	J	false	*6.1.24 Anrufstatistik*
%ENABLE_CALL_PULL_WXT%	J	J	false	*6.1.22 Anruf pull*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	J	false	*6.3.2 Push-Benachrichtigungen für Anrufe*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	J	J	false	*6.1.28 Voicemail-Transkription für Webex Calling*
%ENABLE_MWI_WXT%	J	J	false	*6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%MWI_MODE_WXT%	J	J	leer	*6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige*
%ENABLE_VOICE_MAIL_WXT%	J	J	false	*6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige*
%ENABLE_VISUAL_VOICE_MAIL_WXT%	J	J	false	*6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige*
%ENABLE_FORCED_LOGOUT_WXT%	J	N	false	*6.2.1 Erzwungene* Abmeldung
%FORCED_LOGOUT_APPID_WXT%	J	N	leer	*6.2.1 Erzwungene* Abmeldung
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	J	J	false	*6.1.29.1 Rufumleitung immer aktiviert*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	J	J	true	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_EMERGENCY_DIALING_WXT%	N	J	false	*6.3.1 Notruf*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	J	911, 112	*6.3.1 Notruf*
%ENABLE_USE_RPORT_WXT%	J	J	false	*6.1.14 SIP-Port-Verwaltung für NAT-Transversale*
%RPORT_USE_LOCAL_PORT_WXT%	J	J	false	*6.1.14 SIP-Port-Verwaltung für NAT-Transversale*
%USE_TLS_WXT%	J	J	false	*6.1.2 SIP über TLS und Secure Real-Time Transport Protocol*
%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	false	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%USE_TCP_FROM_DNS_WXT%	J	J	true	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%USE_UDP_FROM_DNS_WXT%	J	J	true	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%USE_TLS_FROM_DNS_WXT%	J	J	true	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%DOMAIN_OVERRIDE_WXT%	J	J	leer	*6.1.6 Dynamische SIP-Proxy-Erkennung*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	J	J	true	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	J	J	true	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Y (nur Windows)	N	false	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	J	J	5000	*6.1.5 Konfigurierbarer Timeout für das Öffnen des* SIP-Sockets
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	J	J	10000	*6.1.5 Konfigurierbarer Timeout für das Öffnen des* SIP-Sockets
%SOURCE_PORT_WXT%	J	J	5060	*6.1.7 Bevorzugte Portverwendung für SIP*
%SIP_FAILBACK_ENABLED_WXT%	J	N	true	*6.1.8.2 SIP-Failback*
%SIP_FAILBACK_TIMEOUT_WXT%	J	N	900	*6.1.8.2 SIP-Failback*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	J	N	false	*6.1.8.2 SIP-Failback*
%SIP_TRANSPORTS_ENFORCE_IP_Version_WXT%	J	J	dns	*6.1.8.3. Erzwingen IP Version*
%USE_ALTERNATIVE_IDENTITIES_WXT%	J	J	false	*6.1.10 P-assoziierte URIs in REGISTER* verwenden
%TCP_SIZE_THRESHOLD_WXT%	J	J	18000	*6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives*
%SIP_REFRESH_ON_TTL_WXT%	J	N	false	*6.1.8.4 DNS TTL-Verwaltung*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	J	J	false	*6.1.12 Unterstützung für SIP-UPDATES*
%ENABLE_PEM_SUPPORT_WXT%	J	J	false	*6.1.11 PEM-Header (SIP P-Early Media)*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_SIP_SESSION_ID_WXT%	J	J	false	*6.1.15 SIP-Sitzungs-ID*
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	J	J	false	*6.1.13 Ältere SIP-INFO-FIR*
%SRTP_ENABLED_WXT%	J	J	false	*6.1.2 SIP über TLS und Secure Real-Time Transport Protocol*
%SRTP_MODE_WXT%	J	J	false	*6.1.2 SIP über TLS und Secure Real-Time Transport Protocol*
%ENABLE_REKEYING_WXT%	J	J	true	*6.1.2 SIP über TLS und Secure Real-Time Transport Protocol*
%RTP_AUDIO_PORT_RANGE_START_WXT%	J	J	8000	*6.1.17 Portbereich des Echtzeit-Transportprotokolls*
%RTP_AUDIO_PORT_RANGE_END_WXT%	J	J	8099	*6.1.17 Portbereich des Echtzeit-Transportprotokolls*
%RTP_VIDEO_PORT_RANGE_START_WXT%	J	J	8100	*6.1.17 Portbereich des Echtzeit-Transportprotokolls*
%RTP_VIDEO_PORT_RANGE_END_WXT%	J	J	8199	*6.1.17 Portbereich des Echtzeit-Transportprotokolls*
%ENABLE_RTCP_MUX_WXT%	J	J	true	*6.1.19 RTCP MUX*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	J	J	true	*6.1.33 XSI-Ereigniskanal*
%CHANNEL_HEARTBEAT_WXT%	J	J	10000	*6.1.33 XSI-Ereigniskanal*
%XSI_ROOT_WXT%	J	J	leer (verwendet die Original-URL)	*6.1.32 XSI-Stamm und -Pfade*
%XSI_ACTIONS_PATH_WXT%	J	J	/com.broadsoft.xsi-actions/	*6.1.32 XSI-Stamm und -Pfade*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%XSI_EVENTS_PATH_WXT%	J	J	/com.broadsoft.xsi-events/	*6.1.32 XSI-Stamm und -Pfade*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	J	J	false	*6.1.25 Automatische Wiederherstellung von Anrufen/nahtlose Anrufübergabe*
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	J	Nur CS	*6.3.1 Notruf*
%ENABLE_CALL_PICKUP_BLIND_WXT%	J	N	false	*6.2.2 Anrufübernahme*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	J	N	false	*6.2.2 Anrufübernahme*
%WEB_CALL_SETTINGS_URL_WXT%	J	J	leer	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%USER_PORTAL_SETTINGS_URL_WXT%	J	J	leer	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%ENABLE_CALL_Center_WXT%	J	J	false	*6.1.31 Callcenter/Anrufwarteschlange – An-/Abmeldung*
%WEB_CALL_SETTINGS_TARGET_WXT%	J	J	äußerlich	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	J	J	true	*6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*
%USE_MEDIASEC_WXT%	J	J	false	*6.1.3 3GPP SIP-Header für SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	J	false	*6.3.4 Klicken zum Wählen (Rückruf)*
%DIALING_CALL_BACK_TIMER_WXT%	N	J	10	*6.3.4 Klicken zum Wählen (Rückruf)*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	J	N	false	*6.2.3 Boss-Admin (Executive-Assistant) Support*
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	J	35	*6.3.2 Push-Benachrichtigungen für Anrufe*
%ENABLE_CALL_RECORDING_WXT%	J	J	false	*6.1.26 Anrufaufzeichnung*
%ENABLE_SINGLE_ALERTING_WXT%	N	J	false	*6.3.3 Einzelne Benachrichtigungen*
%ENABLE_CALL_PARK_WXT%	J	J	false	*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	false	*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	false	*6.1.18 ICE-Unterstützung (nur Webex Calling)*
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	J	N	false	*6.1.8.4 DNS TTL-Verwaltung*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	J	N	false	*6.2.4 SIP-Anrufe an Meeting*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	J	N	false	*6.2.5 Anrufsteuerung – Automatische Anrufannahme*
%ENABLE_DIALING_VOIP_WXT%	N	J	true	*6.3.5 MNO-Unterstützung* *Anruf* mit systemeigenem Dialer

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_DIALING_NATIVE_WXT%	N	J	false	*6.3.5 MNO-Unterstützung* *Anruf* mit systemeigenem Dialer
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	J	J	true	*6.1.35 SIP-URI-Wahl*
%ENABLE_SIP_VIDEOCALLS_WXT%	J	J	true	*6.1.37 Videoanrufe deaktivieren*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	J	J	true	*6.1.37 Videoanrufe deaktivieren*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	J	J	Desktop – true Handy, Tablet – false	*6.1.37 Videoanrufe deaktivieren*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	J	J	false	*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	once_per_login	*6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter*
%ENABLE_AUTO_ANSWER_WXT%	J	N	false	*6.2.6 Automatische Antwort mit Tonbenachrichtigung*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	J	J	false	*6.1.41 Spam-Anrufanzeige*
%ENABLE_NOISE_REMOVAL_WXT%	J	J	false	*6.1.42 Rauschunterdrückung und Bandbreitenerweiterung für Festnetz-/Mobilanrufe*
%ENABLE_AUDIO_MARI_FEC_WXT%	J	J	false	*6.1.46.2 Vorwärtsfehlerkorrektur (FEC) und erneute Übertragung von Paketen (RTX)*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_AUDIO_MARI_RTX_WXT%	J	J	false	*6.1.46.2 Vorwärtsfehlerkorrektur (FEC) und erneute Übertragung von Paketen (RTX)*
%ENABLE_VIDEO_MARI_FEC_WXT%	J	J	false	*6.1.46.2 Vorwärtsfehlerkorrektur (FEC) und erneute Übertragung von Paketen (RTX)*
%ENABLE_VIDEO_MARI_RTX_WXT%	J	J	false	*6.1.46.2 Vorwärtsfehlerkorrektur (FEC) und erneute Übertragung von Paketen (RTX)*
%ENABLE_CALL_BLOCK_WXT%	J	J	false	*6.1.45 Sperrliste (nur Webex Calling)*
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	J	true	*6.3.5.6 MNO-Mobilität – Widget für laufende* Anrufe
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	J	true	*6.3.5.6 MNO-Mobilität – Widget für laufende* Anrufe
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	J	true	*6.3.5.6 MNO-Mobilität – Widget für laufende* Anrufe
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	J	J	false	*6.1.47 gleichzeitige Anrufe mit demselben Benutzer*
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	J	N	false	*6.2.12 Ereignispaket für die Remote-Stummschaltung (nur Webex Calling)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	J	J	true	*6.1.29.2 Anrufweiterleitung an Voicemail*
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	J	J	true	*6.1.8.1 SIP-Failover*
%ENABLE_CALL_MOVE_HERE_WXT%	J	N	false	*6.2.13 Anruf verschieben*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	J	J	false	*6.1.42 Rauschunterdrückung und Bandbreitenerweiterung für Festnetz-/Mobilanrufe*
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	J	leer	*6.3.5.1 Anruf mit systemeigenem Dialer*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	J	J	false	*6.1.20 Übergabe*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	J	J	true	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	J	false	*6.3.6 ID des eingehenden* Anrufers
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	J	false	*6.3.6 ID des eingehenden* Anrufers
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	J	false	*6.1.50 Anrufer-ID* *ID* des ausgehenden Anrufers
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	J	false	*6.1.50 Anrufer-ID* *ID* des ausgehenden Anrufers
%ENABLE_CLID_OUTGOING_CALLS_CALL_Center_WXT%	N	J	false	*6.1.50 Anrufer-ID* *ID* des ausgehenden Anrufers
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	J	false	*6.1.50 Anrufer-ID* *ID* des ausgehenden Anrufers
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	J	false	*6.1.50 Anrufer-ID* *ID* des ausgehenden Anrufers
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	J	J	false	*6.1.49 Informationen zur Anrufumleitung*
%ENABLE_BUSY_LAMP_FIELD_WXT%	J	N	false	*6.2.8.1 Besetztlampenfeld*
%ENABLE_BLF_DISPLAY_CALLER_WXT%	J	N	true	*6.2.8.1 Besetztlampenfeld*
%BLF_NOTIFICATION_DELAY_TIME_WXT%	J	N	0	*6.2.8.1 Besetztlampenfeld*

Vertrauliche Informationen von Cisco

Etikett	Wird auf dem Desktop verwendet	Wird auf Mobilgeräten/Tablets verwendet	Standardwert	Abschnitt
%ENABLE_GCP_NOTIFICATIONS_WXT%	J	N	false	*6.2.8.2 Anrufübernahmegruppe (nur Webex Calling)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	J	N	false	*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	true	*6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives*
%TCP_KEEPALIVE_ENABLED_WXT%	J	J	false	*6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives*
%TLS_KEEPALIVE_ENABLED_WXT%	J	J	false	*6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives*
%ENABLE_MULTI_LINE_WXT%	J	J	false	*6.1.51 Mehrzeilig*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	J	false	*6.2.4 SIP-Anrufe an Konferenz eskalieren (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	J	false	*6.3.5.3 Ausgehende Anrufleitungsidentität (CLID) – Dual Persona*
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	J	false	*6.3.5.3 Ausgehende Anrufleitungsidentität (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	J	J	entschlossen	*6.1.50.2 Remoteanrufer-ID-Name*
%PERSONAL_ASSISTANT_ENABLED_WXT%	J	J	false	*6.1.53 persönlicher Assistent (Abwesenheitspräsenz)**Error! Reference source not found.***
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	J	NPS	***Error! Reference source not found.*** *Liefermodus (nur Webex Calling)*
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	J	J	false	*6.1.52 **Error! Reference source not found.**.*

Vertrauliche Informationen von Cisco

Weitere Informationen zum Zuordnen der benutzerdefinierten Tags, die in Webex für Cisco BroadWorks verwendet werden, zu den von UC-One verwendeten Tags finden Sie in diesem Abschnitt *8 Zuordnung benutzerdefinierter Tags zwischen Webex für Cisco BroadWorks und UC-One*.

Vertrauliche Informationen von Cisco

6.1 Gemeinsame Merkmale

6.1.1 SIP-Server-Einstellungen

Der Client ist üblicherweise für die *Verwendung eines SIP-Netzwerks konfiguriert, indem die config-wxt.xml* Datei geändert wird. In der Regel müssen die folgenden Parameter geändert werden:

- SIP-Domäne. Dieser wird als Domänenteil des eigenen SIP-URI (eigener SIP-URI wird manchmal auch als Leitungsport bezeichnet) im Allgemeinen in SIP-Headern und bei Remote-Anrufen (XSI) verwendet. Der Benutzeranteil der eigenen SIP-URI stammt aus der SIP-Credentials-Konfiguration (Parameter <Benutzername> unter <credentials>).
- SIP-Server-URI oder IP Adresse des SIP-Proxy-Servers, falls DNS Auflösung fehlschlagen sollte. Beachten Sie, dass zur Verwendung von TLS keine IP Adressen im Proxyparameter verwendet werden können, da TLS Zertifikatsüberprüfung 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 eine IP Adresse im Parameter Proxyadresse verwendet wird. Im Allgemeinen wird es aus diesen Gründen nicht empfohlen, eine IP Adresse in diesem Feld zu verwenden.

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

- Registrierung im SIP-Netzwerk.
- Audio- oder Videoanrufe tätigen.
- Durchführung einer DNS-basierten Proxy-Erkennung, die die Verwendung mehrerer Proxys ermöglicht.

Nachdem die SIP-Registrierung aktiviert wurde, muss SIP SUBSCRIBE für MWI über separate Konfigurationsparameter aktiviert werden. Weitere Informationen zu Voicemail finden Sie in diesem Abschnitt *6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige*.

Beachten Sie, dass für MWI immer eine SIP-Grundkonfiguration erforderlich ist, auch wenn SIP-Anrufe deaktiviert sind. MWI verlässt sich auf SIP NOTIFYs.

Die Einrichtung der SIP-Server erfolgt nach folgendem Grundschema:

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

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

```
<Konfiguration>
<Protokolle>
<Schluck>
    <Timer>
        <T1>500</T1>
        <T2>4000</T2>
```


Vertrauliche Informationen von Cisco

```
        <T4>5000</T4>
    </Timer>
```

- T1 – die Zeitspanne in Millisekunden für eine Netzwerk-Roundtrip-Verzögerung.
- T2 – die maximale Zeitspanne in Millisekunden vor der erneuten Übertragung von Nicht-Einladungsanfragen und Einladungsantworten.
- T4 – die maximale Zeitspanne in Millisekunden, die eine Nachricht im Netzwerk verbleiben soll.

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

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

```
<Konfiguration>
<Protokolle><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
       <Zeile>
              <label>%BWAPPEARANCE-LABEL-1%</label>
              <name>%BWNAME-1%</name>
              <Telefonnummer>%BWE164-1%</Telefonnummer>
              <Durchwahl>%BWDURCHWAHL-1%</Durchwahl>
              <external-id>%BWUSEREXTID-1%</external-id>
              <Voicemail-Nummer>%BWVOICE-PORTAL-NUMMER-1%</Voicemail-Nummer>
              <conference-Service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
1%</conference-Service-uri>
              <Domäne>%BWHOST-1%</Domäne>
              <Anmeldeinformationen>
                     <Benutzername>%BWLINEPORT-1%</Benutzername>
                     <Passwort>%BWAUTHPASSWORT-1%</Passwort>
                     <auth>
                            <auth401>
                                   <Standardeinstellung>
                                          <Benutzername>%BWAUTHUSER-
1%</Benutzername>
                                          <Passwort>%BWAUTHPASSWORT-1%</Passwort>
                                   </Standard>
                                   <realm id="%BWHOST-1%">
                                          <Benutzername>%BWAUTHUSER-
1%</Benutzername>
                                          <Passwort>%BWAUTHPASSWORT-1%</Passwort>
                                   </Reich>
                            </auth401>
                            <auth407>
                                   <Standardeinstellung>
                                          <Benutzername>%BWAUTHUSER-
1%</Benutzername>
                                          <Passwort>%BWAUTHPASSWORT-1%</Passwort>
                                   </Standard>
                                   <realm id="%BWHOST-1%">
                                          <Benutzername>%BWAUTHUSER-
1%</Benutzername>
                                          <Passwort>%BWAUTHPASSWORT-1%</Passwort>
                                   </Reich>
                            </auth407>
```


Vertrauliche Informationen von Cisco

```
                    </auth>
                </Anmeldeinformationen>
        </Leitung>
        …
</Zeilen>
<proxy address="%SBC_ADDRESS_WXT%" Port="%SBC_PORT_WXT%" />
<bevorzugter-Port>%SOURCE_PORT_WXT%</bevorzugter-Port>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%BWLINEPORT-n%	leer	Zeichenfolge	In der Regel ein SIP-Benutzername. Weitere Informationen finden Sie im Abschnitt *5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags*. Beispiel: johndoe
%BWAUTHPASSWORT-n%	leer	Zeichenfolge	In der Regel ein SIP-Kennwort. Weitere Informationen finden Sie im Abschnitt *5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags*. Beispiel: geheimes Passwort
%BWE164-n%	leer	Telefonnummer	Standard-Telefonnummer für den Benutzer im internationalen Format. Weitere Informationen finden Sie im Abschnitt *5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags*. Beispiel: 12345678
%SBC_ADDRESS_WXT%	leer	Zeichenfolge	Weitere Informationen finden Sie im Abschnitt *5.6 Systemstandard-Tags*. Beispiel: sbcexample.Domain.com
%SBC_PORT_WXT%	5060	Zahl	Weitere Informationen finden Sie im Abschnitt *5.6 Systemstandard-Tags*. Beispiel: 5060
%BWHOST-n%	leer	Zeichenfolge	Wird in der Regel als SIP-Domäne verwendet. Weitere Informationen finden Sie im Abschnitt *5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags*. Beispiel: exampledomain.com
%SOURCE_PORT_WXT%	5060	Zahl	Wird in der Regel für den *Parameter preferred-Port* verwendet. Weitere Informationen finden Sie im Abschnitt *6.1.7 Bevorzugte Portverwendung für SIP*. Beispiel: 5061

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%BWUSEREXTID-n%	leer	Zeichenfolge	(Nur Webex Calling) Enthält die externe ID der Leitung Weitere Informationen finden Sie unter *6.1.51 Mehrzeilig*. Beispiel: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

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

6.1.2 SIP über TLS und Secure Real-Time Transport Protocol

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

Wenn die dynamische Proxyermittlung nicht verwendet wird, wird sie von der Aktivierung von TLS für SIP verwendet.

Ausführliche Informationen zu den Empfehlungen für SIP-Ports und -Transportprotokolle bei Verwendung von SIP-ALGs im Netzwerk finden Sie im *Webex für Cisco BroadWorks-Lösungshandbuch*.

Beachten Sie, dass das verwendete Zertifikat gültig sein muss. Des Weiteren muss die Zertifikatskette intakt sein, damit auch das Zwischenzertifikat verknüpft ist. Es wird empfohlen, ein weit verbreitetes Zertifikat zu verwenden, das bereits standardmäßig auf den Geräten vorhanden ist. Es ist auch möglich, Zertifikate lokal auf dem Desktopcomputer manuell oder mithilfe der Massenbereitstellung hinzuzufügen, obwohl dies in der Regel nicht der Fall ist.

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

Zusätzlich zu RTP kann RTCP Datenverkehr mit den gleichen Mechanismen gesichert werden, wie RTP mit der obigen Konfiguration verwendet werden.

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

Die SRTP wird verwendet, um die Sicherheit des Medienstreams in dreierlei Hinsicht zu gewährleisten:

- Vertraulichkeit (Daten werden verschlüsselt)

Vertrauliche Informationen von Cisco

- Authentifizierung (Versicherung der Identität der anderen Partei oder Parteien)
- Integrität (Maßnahmen gegen z. B. Replay-Angriffe)

Die aktuelle Version des Medienframeworks unterstützt AES 128 Counter Mode zum Schutz und Hash Message Authentication Code (HMAC)-SHA-1 zur Authentifizierung. Die Größe des Hauptschlüssels beträgt 16 Byte und das Master-Salt 14 Byte.

Das Medienframework unterstützt sowohl vollständige (80 Bit) als auch kurze (32 Bit) Authentifizierungs-Tags. Der Client tauscht die Schlüssel innerhalb des SDP im Rahmen der SIP-Signalisierung aus, beide Seiten des Anrufs senden den verwendeten Schlüssel an die andere Seite.

SRTP kann mit der im folgenden Beispiel gezeigten Konfiguration aktiviert werden. Die aktuelle Implementierung verwendet nur das SDP-Profil für sicheres RTP und unterstützt mehrzeilige Einträge für SDP for Audio Visual Profile (AVP) und Secure Audio Visual Profile (SAVP). Die SRTP Implementierung wurde in der gewohnten Deployment-Konfiguration mit verschiedenen SBCs erfolgreich getestet. Interoperabilitätstests (IOT) mit Endpunkten, die nur die Verschlüsselung mithilfe des AVP-Profils unterstützen, werden nicht unterstützt.

Mehrzeilige SDP-Verfahren im Zusammenhang mit SRTP sind 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 RTP/SAVP im SDP zugeordnet ist, nicht entfernt wird, da in bestimmten Fällen SRTP Anrufe blockiert werden können.

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

Der SBC kann auch die Reihenfolge der SDP-M-Leitungen beim Einrichten des Anrufs ändern, indem die AVP- (unverschlüsselte) oder SAPP-M-Leitung (verschlüsselt) an erster Stelle steht. Daher bevorzugen Clients, die die erste funktionierende M-Line auswählen, entweder verschlüsselten oder unverschlüsselten Datenverkehr. Es gibt folgende Konfigurationsoptionen für SRTP:

- Obligatorisch – Beim Verbindungsaufbau umfasst das anfängliche SDP beim Anbieten nur die SAPP-M-Leitung, und der Client akzeptiert beim Beantworten nur die SAPP-M-Leitung im SDP, daher sind nur SRTP Anrufe möglich.
- Bevorzugt – Beim Anrufaufbau umfasst das anfängliche SDP sowohl die AVP- als auch die SAPP-M-Leitung, aber SAVP steht beim Angebot an erster Stelle und gibt die bevorzugte Reihenfolge an. Beim Beantworten wählt der Client SAVP aus, falls verfügbar, auch wenn es sich nicht um die erste M-Leitung handelt (gemäß SIP-Spezifikationen wird die Reihenfolge der M-Leitungen beim Beantworten nicht geändert).

Vertrauliche Informationen von Cisco

- Optional – Beim Anrufaufbau umfasst der anfängliche SDP sowohl die SAPP- als auch die AVP-M-Leitung, wenn es angeboten wird, aber AVP gibt zuerst die Reihenfolge der Präferenz an. Beim Beantworten wählt der Kunde die erste m-Linie, AVP oder SAVP.
- SRTP nicht aktiviert – Beim Anbieten ist im anfänglichen SDP keine SAPP-M-Leitung vorhanden. Beim Annehmen wird SAVP nicht akzeptiert, 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 und RTP ist in beide Richtungen des Anrufs symmetrisch, d. h., Sende- und Empfangsprofile sind identisch.

```
<Konfiguration>
<Protokolle><sip>
<Sicher>%USE_TLS_WXT%</Sicher>
```

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

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

In einigen Bereitstellungen wird die erneute Eingabe von SRTP nicht unterstützt. Daher gibt es einen Konfigurationsparameter zum Aktivieren/Deaktivieren SRTP erneuten Eingeben. 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.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%USE_TLS_WXT%	false	true, false	Bei "false" wird SIP TLS deaktiviert. Bei Einstellung "true" ist SIP TLS aktiviert. Bitte beachten Sie, dass dieser Parameter ignoriert wird, wenn *6.1.6 Dynamische SIP-Proxy-Erkennung* er verwendet wird.
%SRTP_ENABLED_WXT%	false	true, false	Wenn auf "false" gesetzt, wird SRTP deaktiviert. Wenn auf "true" gesetzt, ist SRTP aktiviert.
%SRTP_MODE_WXT%	wahlfrei	obligatorisch, bevorzugt, optional, Transport	Legt fest, wie bevorzugt SRTP beim Anrufaufbau ist. Der Standardwert ist "optional".
%ENABLE_REKEYING_WXT%	true	true, false	Aktiviert die erneute Eingabe von SIP (SDP) für SRTP.

Vertrauliche Informationen von Cisco

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

6.1.3 3GPP SIP-Header für SRTP

Neuere 3GPP-Spezifikationen erfordern zusätzliche SIP-Header, um das Secure Real-Time Transport Protocol (SRTP) zu verwenden. Weitere Informationen finden Sie unter *3GPP TS 24.229* sowie in den folgenden:

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

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

Es ist nur die Aktivierung der Verwendung der Header konfigurierbar. Für einzelne Header besteht keine weitere Konfigurierbarkeit. Alle Header sind entweder aktiviert oder deaktiviert.

```
<Konfiguration>
<Protokolle><sip>
<use-mediasec enabled="%USE_MEDIASEC_WXT%"/>
```

Das folgende Tag steuert diese Funktion.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%USE_MEDIASEC_WXT%	false	True, false	Aktiviert 3GPP SIP-Header für SRTP Aushandlung.

6.1.4 Erzwingen TCP, TLS oder UDP Verwendung und Keepalives

Die Webex für den Cisco BroadWorks-Client kann so konfiguriert werden, dass entweder TCP, TLS oder UDP sowohl für die SIP-Signalisierung als auch für RTP Medien verwendet werden. Beachten Sie, dass der Client standardmäßig auf TCP eingestellt ist. Beachten Sie außerdem, dass SIP-TCP Verbindungen ohne TCP Keepalive nach einem bestimmten Zeitraum der Inaktivität geschlossen werden.

Im folgenden Beispiel wird dieser Konfigurationsknoten dargestellt.

```
<Konfiguration>
<Protokolle><sip>
<Transporte>
   <tcp-size-threshold>%TCP_SIZE_THRESHOLD_WXT%</tcp-size-threshold>
```


Vertrauliche Informationen von Cisco

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

Etikett	Standard, falls weggelassen	Unterstützte Werte (Byte)	Beschreibung
%TCP_SIZE_THRESHOLD_WXT%	0	0	Erzwingt TCP, die verwendet werden sollen. Die Entscheidung, ob TCP oder UDP für den Client verwendet werden, obliegt dem Service-Provider. Es wird jedoch empfohlen, TCP mit dem Standardwert "0" zu verwenden.
	0	1 - 99,000	Erzwingt, dass UDP verwendet werden, wenn die Nachrichtengröße unter dem hier angegebenen Wert liegt. Der Standardwert ist TCP, wenn die Nachrichtengröße größer als der eingestellte Wert ist. Um UDP zu verwenden, ist 1500 die Standardempfehlung.
	0	100000	Einzusetzende Kräfte UDP.

Derselbe Konfigurationsknoten verfügt auch über Parameter für UDP, TCP und TLS Keepalive, wie im folgenden Beispiel dargestellt.

```
<Konfiguration>
<Protokolle><sip>
<Transporte>
        …
        <udp>
                <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
                        <Zeitüberschreitung>20</Zeitüberschreitung>
                        <Nutzlast>crlf</Nutzlast>
                </Keepalive>
        </UDP>
        <tcp>
                <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
                        <Zeitüberschreitung>0</Zeitüberschreitung>
                        <Nutzlast></Nutzlast>
                </Keepalive>
        </TCP>
        <tls>
                <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
                        <Zeitüberschreitung>0</Zeitüberschreitung>
                        <Nutzlast></Nutzlast>
                </Keepalive>
        </TLS>
</Transporte>
```

Folgende Parameter sind möglich:

- Aktivieren TCP oder TLS Keepalive, mögliche Werte – true/false, der Standardwert ist "false", wenn der Knoten fehlt. Beachten Sie, dass bei Aktivierung dieser Funktion TCP Keepalive-Sätze gesendet werden, selbst wenn UDP Transport für SIP verwendet wird.

Vertrauliche Informationen von Cisco

- Aktivieren UDP Keepalive, mögliche Werte – true/false, der Standardwert ist "true", wenn der Knoten fehlt. Beachten Sie, dass bei Aktivierung dieser Funktion UDP Keepalives gesendet werden, selbst wenn TCP Transport für SIP verwendet wird. Selbst wenn TCP für SIP verwendet wird, akzeptiert der Client gemäß RFC 3261 auch Datenverkehr über UDP .
- 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):
  - Crlf
  - Null (nicht zu verwenden)
  - Benutzerdefinierte Zeichenfolge (**darf nicht verwendet** werden)

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

Die Serveradresse IP und der Port für Keepalives werden mit den normalen Verfahren für die SIP-Proxyerkennung ermittelt. Beachten Sie, dass SIP-Ports und die Auswahl des Transportprotokolls, die über die dynamische SIP-Proxy-Erkennung abgerufen werden, alle statischen Ports oder Transportkonfigurationen außer Kraft setzen. Weitere Informationen zur dynamischen Proxyerkennung finden Sie in diesem Abschnitt *6.1.6 Dynamische SIP-Proxy-Erkennung.*

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%UDP_KEEPALIVE_ENABLED_WXT%	true	true, false	Steuert, ob die Keep-Alive-Pakete für den UDP-Transport gesendet werden sollen.
%TCP_KEEPALIVE_ENABLED_WXT%	false	true, false	Steuert, ob die Keep-Alive-Pakete für den TCP Transport gesendet werden sollen.
%TLS_KEEPALIVE_ENABLED_WXT%	false	true, false	Steuert, ob die Keep-Alive-Pakete für den TLS-Transport gesendet werden sollen.

6.1.5 Konfigurierbarer Timeout für das Öffnen des SIP-Sockets

Bisher war die Zeitüberschreitung für das Öffnen eines SIP-Sockets auf 5 Sekunden für TCP und 10 Sekunden für TLS festgelegt. Diese Zeitüberschreitungen sind nun konfigurierbar.

```
<Konfiguration>
    <Protokolle>
        <Schluck>
            <Transporte>
                <udp>
                    …
                </UDP>
```


Vertrauliche Informationen von Cisco

```
                <tcp>
                    …

<Verbindungszeitüberschreitung>%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%</Verbindung
szeitüberschreitung>
                </TCP>
                <tls>

<Verbindungszeitüberschreitung>%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%</Verbindung
szeitüberschreitung>
                </TCP>
            </Transporte>
```

Die folgenden Tags steuern die Zeitüberschreitung der Socketverbindung (in Millisekunden).

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<integer> – die Zeitüberschreitung in Millisekunden	Die Zeitüberschreitung für die Socketverbindung, wenn TCP Transport verwendet wird.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	<integer> – die Zeitüberschreitung in Millisekunden	Die Zeitüberschreitung für die Socketverbindung, wenn TLS Transport verwendet wird.

6.1.6 Dynamische SIP-Proxy-Erkennung

Im folgenden Beispiel wird die Funktion für die dynamische SIP-Proxyermittlung aktiviert.

```
<Konfiguration>
<Protokolle><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%">
    <Datensatzname>%SBC_ADDRESS_WXT%</Datensatzname>
    <Domain-override>%DOMAIN_OVERRIDE_WXT%</Domain-override>
<-/Proxy-Erkennung>
```

Mit den in diesem Abschnitt beschriebenen Verfahren kann gesteuert werden, welche Transportprotokolleinträge aus DNS SRV verwendet werden, wenn viele verfügbar sind.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%USE_PROXY_DISCOVERY_WXT%	false	True, false	Aktiviert die dynamische SIP-Proxyerkennung für Audio- und Videoanrufe. Der empfohlene Wert ist "true".

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SBC_ADDRESS_WXT%	leer	Zeichenfolge	Dieses Cisco BroadWorks-Tag wird in der Regel für den Parameter record-name verwendet. Es sollte sich um eine gültige URL handeln – nicht um eine IP Adresse. Weitere Informationen finden Sie im Abschnitt *5.6 Systemstandard-Tags*. Beispiel: sbc.Domain.com
%DOMAIN_OVERRIDE_WXT%	leer	Zeichenfolge	Dieses benutzerdefinierte Tag wird für die Domänenüberschreibung verwendet. Weitere Informationen finden Sie im folgenden Abschnitt. Beispiel: other.Domain.com
%USE_TCP_FROM_DNS_WXT%	true	True, false	Wenn dieser Parameterwert "false" ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (TCP) verworfen. Bei "true" werden die Ergebnisse DNS SRV für dieses Transportprotokoll (TCP) verwendet. Abhängig von den SRV-Prioritäten kann noch ein anderer Transport gewählt werden.
%USE_UDP_FROM_DNS_WXT%	true	True, false	Wenn dieser Parameterwert "false" ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (UDP) verworfen. Wenn "true", werden die Ergebnisse DNS SRV für dieses Transportprotokoll (UDP) verwendet. Abhängig von den SRV-Prioritäten kann noch ein anderer Transport gewählt werden.
%USE_TLS_FROM_DNS_WXT%	true	True, false	Wenn dieser Parameterwert "false" ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (TLS) verworfen. 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%	True, false	true	Aktiviert/deaktiviert den DNS Sicherungsdienst. Wenn diese Option aktiviert ist, wird eine A/AAAA-Auflösung für die SIP-Proxyadresse durchgeführt. Sie wird nur berücksichtigt, wenn die SRV/NAPTR-Serviceerkennung aktiviert ist.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	True, false	true	Wenn der Wert auf "true" gesetzt ist und die NAPTR-Service-Erkennung fehlschlägt oder keine Ergebnisse zurückgibt, wird die SRV-Service-Erkennung für den konfigurierten Host durchgeführt. Wenn auf "false" gesetzt, wird keine SRV-Erkennung durchgeführt.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	True, false	false	Ermöglicht die Umgehung des Betriebssystem-DNS-Caches.

Vertrauliche Informationen von Cisco

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

DNS SRV, NAPTR- (Naming Authority Pointer) und A-Datensatz-Abfragen werden unterstützt. Bei der Anmeldung ist der Ablauf in 3 Schritten wie folgt:

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

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

   Wenn kein NAPTR gefunden wird, versucht der Client eine SRV-Abfrage mit dem Datensatznamen von <*Domain*> Parameter, es sei denn <*Domain-override*>*parameter vorhanden, in welchem Fall* <Domain-override> verwendet wird, 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 zu keinem Ergebnis führen, schlägt die Proxyerkennung fehl, und dem Endbenutzer wird eine Fehlermeldung angezeigt, die angibt, dass keine Anrufe verfügbar sind. In diesem Fall erfolgt keine SIP-Registrierung. Aber selbst wenn alle SRV-Abfragen fehlschlagen oder die dort empfangenen Server nicht funktionieren, prüft der Client als Fallback immer noch, ob der konfigurierte statische Proxy funktioniert, nur mit A-Abfragen an die in <Proxy-Adresse> angegebene URI, um zu sehen, ob er eine IP-Adresse ergibt, die eine funktionierende SIP-Registrierung bereitstellt. Port und Transport werden in diesem letzten Fall von *tcp-threshold* und <*secure*> Parameters bestimmt.

3. Lösen Sie gefundene URIs mithilfe der A-Datensatz-Abfrage auf. Die empfangenen endgültigen IP Adressen werden in der Reihenfolge ihres Empfangs versucht, um eine funktionierende Verbindung zum SIP-Proxy herzustellen. Diese Reihenfolge kann vom Service-Provider in der DNS festgelegt werden. Der erste SIP-Proxy URI mit einer erfolgreichen A-Eintrag-Suche wird ausgewählt und verwendet, bis er nicht mehr funktioniert oder der Client sich abmeldet. Im A-Abfrageschritt wird jeweils nur eine IP Adresse verwendet, auch wenn viele empfangen werden. Alle SRV-Einträge werden jedoch bis zur Abmeldung oder bis zur Unterbrechung des Netzwerks aufgelöst.

Wichtige Hinweise

HINWEIS 1: Wenn DNS Proxy-Erkennung zu einer Auswahl des Transportprotokolls im SRV-Schritt führt, indem ein funktionierender SIP-Proxy-URI für ein Transportprotokoll empfangen wird, wird der *Parameter tcp-threshold* überschrieben, der normalerweise zur Auswahl von UDP oder TCP in der Konfigurationsdatei verwendet wird. Gleiches gilt auch für die Konfiguration von SIP/TLS. TCP oder UDP wird je nach Priorität in DNS verwendet.

HINWEIS 2: Elemente, die über SRV empfangen werden, haben Priorität vor dem statischen Proxy in der Konfigurationsdatei. Die NAPTR-Anordnung wird nicht betrachtet; Es zählt nur die SRV-Priorität. Wenn

Vertrauliche Informationen von Cisco

SRV zu mehreren Elementen mit gleichem Transportprotokoll, gleicher Priorität und gleichem Gewicht führt, wird jedes empfangene Element nach dem Zufallsprinzip ausgewählt. NAPTR-Gewichtungen werden in dieser Version nicht unterstützt, aber SRV-Gewichtungen werden unterstützt. Die SRV-Priorität wird zuerst betrachtet, und für Elemente mit gleicher Priorität wird die Gewichtung betrachtet, um die Wahrscheinlichkeit zu bestimmen, mit der ein bestimmter Server als nächstes ausprobiert wird.

HINWEIS 3: Mit dem optionalen *Parameter Domain-override* kann ein anderer A-Eintragsname als der im SIP-Domänenkonfigurationsparameter mit SRV aufgelöst werden, wenn NAPTR-Ergebnisse weggelassen werden. In den folgenden Beispielen finden Sie Informationen zur Verwendung des *Parameters Domain-override* .

HINWEIS 4: Der Client verwendet Betriebssystemprimitive für DNS Vorgänge, und in der Regel werden DNS Antworten zwischengespeichert, um die TTL der DNS Antwort zu berücksichtigen.

HINWEIS 5: Der DNS-Typ (Dienst) für NAPTR-Datensätze muss den Verfahren von RFC 3263 *entsprechen* , andernfalls kann DNS Auflösung fehlschlagen. Beispielsweise ist es erforderlich, SIPS+D2T für SIP über TLS zu verwenden.

HINWEIS 6: 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 einem Präfix enthält, das nicht mit dem Servicetyp übereinstimmt, wird dieser Datensatz ignoriert.

Beispiel 1: Verwenden der DNS Proxyermittlung ohne Domänenüberschreibungskonfigurationsparameter

Im Folgenden finden Sie ein Beispiel für eine Konfiguration mit SIP-Proxyerkennung, bei der nur SIP über TCP verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse zurückgibt.

```
<Konfiguration>
<Protokolle><sip>
<proxy address="Domain.com" Port="5060"/>
<proxy-discovery enabled="true" >
    <Datensatzname>record-Domain.com</Datensatzname>
     <Domain-override>override-Domain.com</Domain-override>
<-/Proxy-Erkennung>
<Domäne>sip-Domain.com</Domäne>
```

Daraus ergeben sich die folgenden Schritte auf 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.
```


Vertrauliche Informationen von Cisco

```
3. A-Record-Abfrage für  Test.sipgeo.record-Domain.com, Antwort:
Test.sipgeo.record-Domain.com. 16 IN EINEM 1.2.3.4
```

Dadurch erfolgt die SIP-Anmeldung über TCP über Port 5061 (im SRV-Schritt empfangen) und in Richtung der IP Adresse 1.2.3.4.

Beispiel 2: **Verwenden des Parameters Domain-override in der Konfigurationsdatei**

Im Folgenden finden Sie ein zweites Beispiel für eine Konfiguration mit SIP-Proxyerkennung, bei der sich die SIP-Domäne von der Proxydomäne unterscheidet und nur SIP über UDP verwendet wird und die NAPTR-Abfrage keine Ergebnisse zurückgibt.

```
<Konfiguration>
<Protokolle><SIP
<proxy address="Domain.com" Port="5060"/>
<proxy-discovery enabled="true">
    <Datensatzname>record-Domain.com</Datensatzname>
     <Domain-override>override-Domain.com</Domain-override>
<-/Proxy-Erkennung>
<Domäne>sip-Domain.com</Domäne>
```

Daraus ergeben sich die folgenden Schritte auf Protokollebene.

```
1. NAPTR-Abfrage für record-Domain.com, keine Antwort.
2. SRV-Abfrage für _sip._tcp.override-Domain.com (aus Konfigurationsdatei), Antwort
_sip._tcp.override-Domain.com. 28635 IN SRV
10 10 5061 Test.override-Domain.com.
3. A-Record-Abfrage für  Test.override-Domain.com, Antwort:
Test.sipgeooverride-Domain.com. 16 IN EINEM 4.3.2.1
```

Dadurch erfolgt die SIP-Registrierung über UDP über Port 5061 (im SRV-Schritt empfangen) und in Richtung der IP Adresse 4.3.2.1.

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

Im Folgenden finden Sie ein weiteres Beispiel für eine Konfiguration mit SIP-Proxyerkennung, bei der nur SIP über TCP verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse zurückgibt, aber mehrere NAPTR- und SRV-Einträge mit unterschiedlichen Prioritäten empfangen werden. In diesem Fall zählt in diesem Freigabeereignis nur die SRV-Priorität, obwohl auch mehrere NAPTR-Datensätze mit unterschiedlichen Prioritäten empfangen werden.

```
<Konfiguration>
<Protokolle><sip>
<proxy address="Domain.com" Port="5060"/>
<proxy-discovery enabled="true">
    <Datensatzname>record-Domain.com</Datensatzname>
     <Domain-override>override-Domain.com</Domain-override>
<-/Proxy-Erkennung>
<Domäne>sip-Domain.com</Domäne>
```

Daraus ergeben sich die folgenden Schritte auf Protokollebene.

```
1. NAPTR-Abfrage für record-Domain.com, Antwort:
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.
```


Vertrauliche Informationen von Cisco

```
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.

SRV-Abfrage für _sip._udp.Test.sip.record-Domain.com (in der NAPTR-Abfrage
empfangen), Antwort
_sip._udp.Test.sip.record-Domain.com. 28635 IN SRV
20 10 5062 Test.sipgeo.record-Domain.com.

3. A-Datensatz-Abfrage für  Test.sipgeo.record-Domain.com, Antwort:
Test.sipgeo.record-Domain.com. 16 IN EINEM 1.2.3.4
```

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

Beispiel 4: Verwenden der DNS Proxy-Erkennung mit NAPTR, wenn der Dienst nicht mit dem Diensttyp übereinstimmt

Im Folgenden finden Sie ein Beispiel für eine Konfiguration, bei der die SIP-Proxyerkennung verwendet wird, wenn SIP über TCP und TLS verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse zurückgibt.

```
<Konfiguration>
<Protokolle><sip>
<proxy address="Domain.com" Port="5060"/>
<proxy-discovery enabled="true" tcp="true" udp="false" tls="true">
    <Datensatzname>record-Domain.com</Datensatzname>
     <Domain-override>override-Domain.com</Domain-override>
<-/Proxy-Erkennung>
<Domäne>sip-Domain.com</Domäne>
```

Daraus ergeben sich die folgenden Schritte auf Protokollebene.

```
1. NAPTR-Abfrage für record-Domain.com, Antwort:
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. Für den ersten Datensatz haben wir den Servicetyp "SIPS+D2T" und das Präfix
ist "sip._tls.". Da dieses Präfix nicht mit dem Servicetyp übereinstimmt (siehe
Hinweis 6 oben), wird es ignoriert.

3. 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 EINEM 1.2.3.4
```

Dies hat zur Folge, dass die SIP-Registrierung über TCP über Port 5061 (im SRV-Schritt empfangen) und in Richtung der IP Adresse 1.2.3.4 erfolgt.

Vertrauliche Informationen von Cisco

6.1.7 Bevorzugte Portverwendung für SIP

Es gab einige Fälle, in denen ein anderes Softwarepaket auf demselben Computer wie der Client ausgeführt wurde und den Standard-SIP-Port belegte. Um den Client so zu konfigurieren, dass ein anderer Port für SIP verwendet wird, 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 verwendet wird, versucht der Client inkrementell Portwerte, die über dem konfigurierten Wert liegen. Wenn z. B. der Wert des *bevorzugten Ports* "6000" ist und dieser Port belegt ist, versucht der Client 6001, 6002, 6003 usw., bis er einen nicht verwendeten Port findet. Sobald ein unbenutzter Port gefunden wird, verwendet er diesen für die eigene SIP-Kommunikation.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SOURCE_PORT_WXT%	5060	Zahl	Gibt den bevorzugten lokalen SIP-Port für die Kommunikation an. Beispiel: 5060

6.1.8 SIP-Failover und -Failback

SIP-Failover und -Failback folgen den Cisco BroadWorks-Verfahren. Dazu müssen mehrere Proxys (in der Regel der SBC) konfiguriert sein.

Auf der Client-Seite sollte der Proxy in mehrere IP Adressen aufgelöst werden. Dies kann erreicht werden durch:

- Die SIP-Proxyermittlung ist aktiviert und der DNS Server hat NAPTR- und/oder SRV-Einträge für den SBC-FQDN (siehe Abschnitt *6.1.6 Dynamische SIP-Proxy-Erkennung*) ODER
- Die SIP-Proxy-Adresse wird als FQDN bereitgestellt und in mehrere IP Adressen aufgelöst (siehe Abschnitt *6.1.1 SIP-Server-Einstellungen*).

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

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

6.1.8.1 SIP-Failover

Das SIP-Failover kann wie folgt durch einen Socket-Fehler, einen Anforderungs-Timeout-Fehler oder eine endgültige Fehlerantwort vom Server ausgelöst werden:

- Socket-Fehler – Wenn der Socket zwischen dem Client und dem Server unterbrochen oder geschlossen wird, wie im Fall eines Verlusts der Netzwerkverbindung, reagiert der Client sofort und löst ein Failover aus.
- Zeitüberschreitung (z. B. wenn der SBC hängt) – basierend auf SIP T1:
  - SIP INVITE – Wenn bei der INVITE-Anforderung eine Zeitüberschreitung auftritt, registriert sich der Client beim nächsten verfügbaren SBC (IP) und wiederholt die INVITE.

Vertrauliche Informationen von Cisco

- Noch eine SIP-Anforderung: Der Client versucht, sich beim nächsten verfügbaren SBC (IP) zu registrieren.

- Endgültige Fehlerantwort vom Server empfangen:
  - Die folgenden SIP-Fehlerantworten des Servers an ein SIP REGISTER lösen einen Failover aus:
    - 5xx
    - 6xx
  - Die folgenden SIP *4xx-Antworten* auf SIP REGISTER verursachen kein Failover:
    - 401 Nicht autorisiert
    - 403 Unzulässig
    - 404 Nicht gefunden
    - 407 Proxy-Authentifizierung erforderlich
    - 423 Intervall zu kurz
  - Darüber hinaus lösen 4xx-Fehlerantworten *auf SIP INVITE kein Failover aus,* 5xx und *6xx* jedoch schon.

Wenn ein Failover ausgelöst wird, nimmt der Client die nächste verfügbare IP Adresse aus der Liste. Der SIP T1-Timer definiert, wie lange ein Proxy in der Liste ausprobiert wird, bevor zum nächsten gewechselt wird. In der Regel wird ein Wert von 32 Sekunden verwendet (64*T1). Wenn alle IP Adressen ausfallen, zeigt der Client einen Benutzeroberflächenfehler für SIP-Verbindungen an. Wenn beim Failover gerade ein VoIP Anruf ausgeführt wird, wird der Anruf beendet.

Die SIP-Failoverlogik stützt sich auf mehrere Konfigurationsparameter:

- SIP-Failover-Timer – Die SIP-Timer T1, T2 und T4 sind in der Konfigurationsdatei verfügbar. Es wird jedoch nicht empfohlen, sie zu ändern.

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

  - T1 – die Zeitspanne in Millisekunden für eine Netzwerk-Roundtrip-Verzögerung.
  - T2 – die maximale Zeitspanne in Millisekunden vor der erneuten Übertragung von Nicht-Einladungsanfragen und Einladungsantworten.
  - T4 – die maximale Zeitspanne in Millisekunden, die eine Nachricht im Netzwerk verbleiben soll.

- SIP-Proxy-Adresse und SIP-Proxy-Erkennung
  - Siehe Abschnitt *6.1.1 SIP-Server-Einstellungen*.
  - Siehe Abschnitt *6.1.6 Dynamische SIP-Proxy-Erkennung*.

Vertrauliche Informationen von Cisco

- Failover-Konfiguration registrieren (siehe unten)

Im Falle eines Failovers sendet die Webex-Anwendung SIP REGISTER mit zwei Kontaktheadern – einen für die alte Sitzung und einen für die neuen Geräteinformationen. Der Kontaktheader für die alte Sitzung ist enthalten, um den SBC zu benachrichtigen, die Daten zu bereinigen. Dieser Header enthält expires=0 und q=0.5.

Der Kontaktheader mit den neuen Geräteinformationen enthält ebenfalls einen q-Wert, der aus dem *Tag <q-value>* gelesen wird. Der *Wert <q-value>* tag wird verwendet, um die Präferenz oder Priorität einer bestimmten Kontaktadresse anzugeben. Sie reicht von 0 bis 1,0, wobei 1,0 die höchste und 0 die niedrigste Präferenz ist. Dieses Tag verfügt nicht über ein benutzerdefiniertes Tag, um den Wert zu steuern – es ist auf 1.0 hartcodiert. Der Wert kann manuell angepasst werden, wenn der im Deployment verwendete SBC über eine umgekehrte Logik verfügt und q=0.0 mit maximaler Priorität behandelt.

Ab Version 42.11 wird ein neuer *Abschnitt <register-Failover>* in die Konfigurationsvorlage eingefügt. Es wurde ein neuer konfigurierbarer Parameter *<registration-cleanup>* hinzugefügt, um zu steuern, ob die Anwendung einen Kontaktheader sendet, um die alten Geräteinformationen zu bereinigen. Einige SBCs bereinigen die alte Sitzung sofort beim Trennen der Socketverbindung, sodass das Vorhandensein des Kontaktheaders für die alte Sitzung nicht erforderlich ist. Standardmäßig ist die Logik für die Registrierungsbereinigung aktiviert.

Aus Gründen der Konsistenz wird das *Tag <q-value>* auch unter den Abschnitt same *<register-Failover>* verschoben.

Beispiel:

```
<Konfiguration>
<Protokolle><sip>
   <q-Wert>1,0</q-Wert> <!-- VERALTET -->
   <Register-Failover>

<Registrierungsbereinigung>%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%</Regist
rierungsbereinigung>
      <q-Wert>1,0</q-Wert>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	true	true, false	Steuert die Bereinigung alter Geräteinformationen im Falle eines SIP-Failovers.

Vertrauliche Informationen von Cisco

6.1.8.2 SIP-Failback

Wenn der Client mit einem Proxy verbunden ist, der nicht der erste nach Priorität ist, versucht er, die Verbindung mit dem IP mit der höchsten Priorität wiederherzustellen. Die Zeit für das Failback richtet sich nach der DNS TTL-Verwaltungskonfiguration (siehe Abschnitt *6.1.8.4 DNS TTL-Verwaltung*). Wenn bei Erreichen des Failback-Timers gerade ein Anruf ausgeführt wird, wartet der Client, bis alle Aufrufe abgeschlossen sind, und löst dann den Failback-Vorgang aus. Beachten Sie, dass dies nur für Desktop-Clients gilt, da die SIP-Verbindung nur während eines Mobilanrufs aktiv ist.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SIP_FAILBACK_ENABLED_WXT%	true	true, false	Aktiviert/deaktiviert SIP-Failback.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Über 60	Die SIP-Failback-Zeitbegrenzung in Sekunden.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	true, false	Fügt einen zufälligen Zeitraum [0-10] % des SIP-Failbacks hinzu.

6.1.8.3 Erzwingen IP Version

Webex Client kann so konfiguriert werden, dass die Liste der aufgelösten Hosts über die DNS sortiert und dann im Falle eines SIP-Failovers durchlaufen wird. In allen Modi werden die Priorität und das Gewicht berücksichtigt.

Folgende Konfigurationen werden unterstützt:

- DNS – Verwendet alle Adressen, die von den DNS Abfragen zurückgegeben werden
- IPv4 – filtert die IPv6-Adressen heraus
- IPv6 – filtert die IPv4 Adressen heraus
- prefer-IPv4 – sortiert die IPv4 Adressen vor IPv6 (Release 42.9)
- prefer-IPv6 – ordnet die IPv6-Adressen vor dem IPv4 (Release 42.9)
- nat64 – ignoriert die IPv6-Adressen, ordnet die IPv4 (Release 44.2)

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

Bei der "DNS"-Konfiguration werden die IPv4 Adressen für den jeweiligen Host gegenüber den IPv6-Adressen priorisiert. Wenn zwei Hosts sowohl mit IPv4- als auch mit IPv6-Adressen vorhanden sind, lautet die Reihenfolge IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

Im Modus "prefer-IPv4" werden die IPv4 Adressen vor den IPv6-Adressen geordnet (die Reihenfolge innerhalb der Gruppen IPv4 und IPv6 bleibt erhalten)

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

Vertrauliche Informationen von Cisco

Im "prefer-IPv6"-Modus ist die Reihenfolge umgekehrt – die IPv6-Adressen werden vor den IPv4-Adressen platziert

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

Im Modus "nat64" werden die IPv6-Adressen ignoriert, die IPv4 Reihenfolge wird eingehalten. Die IPv6-Präfixe wurden ermittelt. 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).

```
<Konfiguration>
<Protokolle><SIP><Transporte>
<enforce-ip-Version>%SIP_TRANSPORTS_ENFORCE_IP_Version_WXT%</enforce-ip-Version>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SIP_TRANSPORTS_ENFORCE_IP_Version_WXT%	dns	IPv4 IPv6 dns Bevorzugtes IPv4 Bevorzugtes IPv6 NAT64	Steuert die Reihenfolge der IPv4-/IPv6-Adressen, die vom Webex-Client zum Herstellen der Verbindung mit der SIP-Sitzung verwendet werden.

6.1.8.4 DNS TTL-Verwaltung

Es wurde ein separater Konfigurationsparameter hinzugefügt, mit dem verwaltet wird, wie DNS Auflösung wiederholt wird, wenn die TTL des DNS Datensatzes des aktuell verwendeten Servers abläuft. Wenn der Parameter in der folgenden Tabelle aktiviert ist, zwingt er den Client, DNS Vorgänge zu wiederholen, sobald die TTL des DNS SRV- oder A-Eintrags des aktuell verwendeten Servers abgelaufen ist.

Nachdem die DNS-Auflösung wiederholt wurde, zwingt dieser Parameter den Client auch, sich erneut mit dem empfangenen Server mit der höchsten Priorität zu verbinden, wenn er sich vom aktuell verwendeten Server unterscheidet, selbst wenn die aktuelle Verbindung vollständig funktioniert. Die erneute Verbindung erfolgt jedoch erst, nachdem die laufenden Anrufe beendet wurden.

Wenn die TTLs für Server A und SRV-Einträge unterschiedlich sind, wird der kleinere Wert gewählt.

Wenn dieser Parameter deaktiviert ist, werden DNS Vorgänge nicht nach Ablauf der Gültigkeitsdauer wiederholt, sondern alle 15 Minuten.

Dieser Parameter funktioniert nur für SIP.

Vertrauliche Informationen von Cisco

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

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

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SIP_REFRESH_ON_TTL_WXT%	false	falsch, wahr	Wenn dieser Wert auf "false" festgelegt ist, ist DNS TTL-Verwaltung für SIP deaktiviert. Wenn dieser Wert auf "true" festgelegt ist, ist die DNS TTL-Verwaltung für SIP aktiviert.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	false	falsch, wahr	Wenn diese Option aktiviert ist, wird der DNS TTL eine zufällige Periode zwischen 0 und 10 % hinzugefügt.

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

6.1.9 SIP SUBCSRIBE und REGISTER Aktualisieren und SUBSCRIBE Wiederholen

Communicator unterstützt das Konfigurieren der Aktualisierungsintervalle für SIP SUBSCRIBE und REGISTER. Für SIP SUBSCRIBE gibt es einen separaten Parameter für das Aktualisierungsintervall (in Sekunden) und wie lange der Client wartet, bevor er SIP SUBSCRIBE bei Fehlern wiederholt (in Sekunden). Der empfohlene Höchstwert für das *Abonnement-Wiederholungsintervall* ist 2000000 Sekunden, während jeder negative, 0- oder leere Wert dazu führt, dass 1800 Sekunden verwendet werden. Jeder negative Wert in for subscribe refresh lässt den *Expires-Header* aus und erstellt somit einen einmaligen SUBSCRIBE-Header.

Der vom Client vorgeschlagene SIP REGISTER-Aktualisierungs-Timer 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 auch der Ablaufwert für SIP-Sitzungen (für SIP INVITE und SUBSCRIBE) konfiguriert werden (in Sekunden).

```
<Konfiguration>
<Protokolle><sip>
<Abonnement-Aktualisierungsintervall>10800</Abonnement-Aktualisierungsintervall>
<Abonnement-Wiederholungsintervall>60</Abonnement-Wiederholungsintervall>
```


Vertrauliche Informationen von Cisco

```
<Aktualisierungsintervall für Registrierung>300</Aktualisierungsintervall für
Registrierung>
<Sitzung>
       <Ablaufwert>3600</Ablaufwert>
</Sitzung>
```

6.1.10 P-assoziierte URIs in REGISTER verwenden

Der folgende Parameter wird beim Registrieren und Verarbeiten der zugehörigen *200 OK-Antwort* verwendet.

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

```
<Konfiguration>
<Protokolle><sip>
<alternative-identitäten>%USE_ALTERNATIVE_IDENTITIES_WXT%</alternative-identitäten
verwenden>
```

Wenn der Parameter auf "true" gesetzt ist, übernimmt 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.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	true, false	Aktiviert die Verwendung alternativer Identitäten in SIP REGISTER. Wenn dieser Wert auf "true" festgelegt ist, übernimmt der Client seine eigene Identität aus dem letzten *P-Associated-URI-Header* für ausgehende SIP-Anforderungen. Wenn auf "false" gesetzt, wird die eigene Identität für ausgehende SIP-Anfragen von der eigenen SIP-URI übernommen.

6.1.11 PEM-Header (SIP P-Early Media)

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

Der Konfigurationsparameter aktiviert die Unterstützung von PEM-Ankündigungen in der SIP-Signalisierung. Die tatsächliche Logik für die frühe Medienverarbeitung ist sowohl für PEM- als auch für Nicht-PEM-Fälle identisch und arbeitet mit unterstützten PEM-Headerwerten.

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


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_PEM_SUPPORT_WXT%	false	True, false	Legen Sie diesen Wert auf "true" fest, um die Unterstützung von Clientankündigungs-PEM im SIP-Signalbau zu aktivieren. Legen Sie "false" fest, um die PEM-Unterstützung für Clientankündigung in der SIP-Signalisierung zu deaktivieren.

6.1.12 Unterstützung für SIP-UPDATES

SIP UPDATE wird z. B. in einigen IMS-Bereitstellungen anstelle der alternativen erneuten INVITE-Anforderung benötigt. Es ermöglicht einem Client, Parameter einer Sitzung zu aktualisieren, z. B. den Satz von Medienströmen und deren Codecs, hat jedoch keine Auswirkungen auf den Status eines SIP-Dialogs.

Typische Anwendungsfälle beziehen sich auf frühe Medien, wenn z. B. Rückrufton und Vorwarnung gleichzeitig verwendet werden.

SIP UPDATE wird derzeit nur unterstützt, wenn es in Anwendungsfällen vor dem Dialog (frühe Medien) empfangen wird und nicht während eines aktiven Dialogs, z. B. für das Halten und Fortsetzen von Anrufen, bei denen re-INVITE noch verwendet wird.

In dieser Version ist es nicht möglich, Video zu Audio mit SIP UPDATE (Medienwechsel) hinzuzufügen. Darüber hinaus unterstützt der Client keinen vollständigen langen IMS-Anrufablauf mit Ressourcenreservierung.

```
<Konfiguration>
<protocols><sip>
<support-Update enabled="%ENABLE_SIP_UPDATE_SUPPORT_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	true, false	Wenn dieser Wert auf "false" gesetzt ist, wird die SIP UPDATE-Unterstützung deaktiviert. Wenn diese Option auf "true" gesetzt ist, ist die SIP UPDATE-Unterstützung aktiviert.

6.1.13 Ältere SIP-INFO-FIR

Dieser Client unterstützt die Legacy-Methode zum Anfordern von Video-Keyframes über die SIP INFO-Mediensteuerungsanforderung. Dies ist notwendig, da einige der Geräte Probleme haben, auf RTCP-FB FIR zu reagieren, und gelegentlich RTCP nicht zum Remote-Endpunkt durchkommt, was zu No-Video oder One-Way-Video führen kann. Weitere Informationen finden Sie unter *RFC 5168*.

Vertrauliche Informationen von Cisco

```
<Konfiguration>
<protocols><sip>
<force-sip-Info-fir enabled="%ENABLE_FORCE_SIP_INFO_FIR_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false	True, false	Wenn dieser Wert auf "false" festgelegt ist, ist die SIP INFO FIR-Unterstützung deaktiviert. Wenn dieser Wert auf "true" gesetzt ist, ist die SIP INFO FIR-Unterstützung aktiviert.

6.1.14 SIP-Port-Verwaltung für NAT-Transversale

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

Weitere Informationen zu den Empfehlungen für SIP-Ports und Transportprotokolle, wenn SIP Application Layer Gateways (ALGs) im Netzwerk verwendet werden, finden Sie im *Webex für Cisco BroadWorks Solution Guide*.

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

Der *Parameter Preferred-Port* ist insofern verwandt, als er den im SIP-Kontaktheader verwendeten Port definiert. Weitere Informationen zur SIP-Port-Zuweisung finden Sie in diesem Abschnitt *6.1.7 Bevorzugte Portverwendung für SIP*.

Es gibt einen separaten Konfigurationsparameter *use-local-Port* , der erzwingt, dass der lokale Port des Client-Sockets im *Contact-Header* festgelegt wird. Dies wird für einige SBCs verwendet, die erkennen, dass der Client über einen echten IP (aus dem *Contact-Header*) verfügt, und der SBC versucht, einen separaten Socket für den Client für seine Anforderungen einzurichten. In den meisten Fällen befindet sich eine Firewall zwischen dem SBC und dem Client und verweigert die eingehenden Verbindungen zum Client.

> **HINWEIS:** In IPv6-Umgebungen sind alle Adressen echt, und der SBC versucht, eine Verbindung zur lauschenden Clientadresse (aus dem *Contact-Header*) herzustellen.

```
<Konfiguration>
<Protokolle><sip>
<use-rport enabled="%ENABLE_USE_RPORT_WXT%" use-local-
Port="%RPORT_USE_LOCAL_PORT_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_USE_RPORT_WXT%	false	true, false	Aktiviert rport für Audio- und Videoanrufe.
%RPORT_USE_LOCAL_PORT_WXT%	false	true, false	Steuert, ob der lokale Port des Client-Sockets im SIP-Kontaktheader hinzugefügt wird.

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 gesamte Lebensdauer der Verbindung/Sitzung für dieses Gerät, für alle Dialoge außerhalb des Anrufs, REGISTRIEREN, ABONNIEREN, BENACHRICHTIGEN usw. verwendet. Dieselbe Sitzungs-ID wird verwendet, bis die Bindung verloren geht. Wenn die Registrierungsbindung verloren geht (DNS Suche, Zurücksetzen der Verbindung, Zurücksetzen des Telefons usw.), wird eine neue lokale Sitzungs-ID generiert.

Der Wert der Sitzungs-ID kann verwendet werden, um alle Dialoge zu finden, die diesem Gerät zugeordnet sind.

```
<Konfiguration>
<Protokolle><sip>
<sip-sessionid enabled="%ENABLE_SIP_SESSION_ID_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SIP_SESSION_ID_WXT%	false	True, false	Steuert die Verwendung der SIP-Sitzungs-ID.

6.1.16 Ablehnungsverhalten bei eingehendem Anruf

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

Wenn der Client so konfiguriert ist, dass ein Anruf mit *der Option 603 Ablehnen* abgelehnt wird, funktionieren die Services "Weiterleiten, wenn besetzt" und "Weiterleiten, wenn keine Antwort" möglicherweise nicht wie erwartet.

```
<Konfiguration>
<Services><Anrufe>
<reject-with-486 enabled="%ENABLE_REJECT_WITH_486_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_REJECT_WITH_486_WXT%	true	true, false	Steuert den SIP-Fehlercode und den Grund, der zum Ablehnen eingehender SIP-Anrufe verwendet wird. Wenn aktiviert, *wird 486 momentan nicht verfügbar* verwendet. Andernfalls *wird 603 Decline* verwendet.

6.1.17 Portbereich des Echtzeit-Transportprotokolls

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

```
<Konfiguration>
<Protokolle><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>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	Zahl	Beginn des Audioport-Bereichs.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	Zahl	Ende des Audioport-Bereichs.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	Zahl	Beginn des Videoport-Bereichs.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	Zahl	Ende des Videoport-Bereichs.

HINWEIS: Portbereiche sollten so festgelegt werden, dass sie sich nicht überlappen.

6.1.18 ICE-Unterstützung (nur Webex Calling)

Der Client unterstützt die ICE-Aushandlung (Interactive Connectivity Establishment), die eine Optimierung des Medienpfads zwischen Endpunkten (auf Peer-zu-Peer-Weise) ermöglicht. Dies geschieht, um die Datenlatenz zu reduzieren, Paketverluste zu verringern und die Betriebskosten für die Bereitstellung der Anwendung zu senken.

Vertrauliche Informationen von Cisco

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

Wenn die ICE-Unterstützung aktiviert ist, wird immer eine erneute Eingabe für SRTP durchgeführt (siehe Abschnitt *6.1.2 SIP über TLS und Secure Real-Time Transport Protocol*).

Ab Version 44.5 bietet Webex App Unterstützung für ICE über IPv6 mit NAT64.

```
<Konfiguration>
<Protokolle><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%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_RTP_ICE_WXT%	false	true, false	Aktivieren/deaktivieren Sie die ICE-Unterstützung.
%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%	false	true, false	Aktiviert ICE über IPv6.

6.1.19 RTCP MUX

RTCP MUX ist konfigurierbar. Durch diese Funktion verwendet der Client für RTP und RTCP denselben Port. In der SIP/SDP-Signalisierungsebene wird dem SDP die Leitung a=rtcp-mux hinzugefügt. Darüber hinaus sind verschiedene Modi möglich:

- Abwärtskompatibilitätsmodus (d. h., Zeile a=rtcp-mux wird in SDP nicht angezeigt)
- Multiplexing-Modus (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 denselben Port.

```
<Konfiguration>
<Protokolle><RTP>
<mux enabled="%ENABLE_RTCP_MUX_WXT%"/>
```

Beachten Sie, dass RTCP MUX nicht für SRTP Anrufe verwendet werden kann.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_RTCP_MUX_WXT%	true	true, false	Um RTPC MUX zu aktivieren, setzen Sie auf "true". Um RTCP MUX zu deaktivieren, setzen Sie auf "false".

6.1.20 Übergabe

Die Webex für den Cisco BroadWorks-Client unterstützt die überwachte (konsultative), semi-konsultative und direkte (blinde) Anrufübergabe.

Bei der halbabfragebasierten Anrufübergabe kann der Anrufer die Übergabe abschließen, bevor der Anruf vom Remote-Anrufer angenommen wird. Die Taste für die halbabfragevolle Vervollständigung wird für den Anrufer erst aktiviert, wenn auf der Seite des Angerufenen das Klingeln gestartet wurde und die entsprechende SIP-Benachrichtigung (*180 Klingeln*) auf der Anruferseite empfangen wurde. Die Blindübergabe wird in der Benutzeroberfläche als "Jetzt übertragen" bezeichnet.

> **HINWEIS:** Der SIP *180-Klingelton* wird in einigen Umgebungen, für einige Nummern oder in einigen serverübergreifenden Kommunikationsszenarien möglicherweise nicht ausgelöst.

In Version 43.9 der Webex App wird die Übergabe an einen anderen eigenständigen, laufenden Anruf desselben Typs eingeführt. Anrufe, die in der App Webex beendet wurden, können an andere Anrufe übergeben werden, die am lokalen Endpunkt beendet wurden. Außerdem können Anrufe, die auf einem Remotegerät beendet wurden, an Anrufe übergeben werden, die auf einem Remoteendpunkt beendet wurden. Für diese Funktion können keine konfigurierbaren Optionen verwendet werden.

Ab Version 43.12 fügt die App Webex eine Konfigurationsoption hinzu, mit der gesteuert werden kann, ob der aktuelle Anruf automatisch gehalten werden soll, wenn der Menüpunkt "Übergeben" ausgewählt wird. Dieses Verhalten wird durch das neue *Auto-Hold-Attribut* gesteuert. Standardmäßig ist die Funktion zum automatischen Halten deaktiviert.

```
<Konfiguration>
<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%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_TRANSFER_CALLS_WXT%	false	true, false	Wenn dieser Wert auf "true" gesetzt ist, ist die Anrufübergabe aktiviert. Wenn dieser Wert auf "false" gesetzt ist, ist die Anrufweiterleitung deaktiviert.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false	true, false	Aktiviert Übergabeoptionen für Remoteanrufe (XSI), die an einem anderen Standort beendet werden.
%TRANSFER_CALL_TYPE_WXT%	voll	Zuerst sprechen, blind, voll	Gibt die Übertragungstypen an, die für den Benutzer in der BroadWorks-Konfiguration verfügbar sind.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	true, false	Legt fest, ob der aktive Anruf automatisch in die Warteschleife gestellt wird, wenn der Benutzer im Menü des Anrufbildschirms die Übergabeoption auswählt.

6.1.21 N-Way-Konferenzanrufe und Teilnehmer

Das folgende benutzerdefinierte Tag kann verwendet werden, um die Verfügbarkeit von Ad-hoc-Konferenzen (N-Wege) über SIP im Webex für den Cisco BroadWorks-Client zu steuern. Darüber hinaus kann der N-way-Besitzer die vollständige Liste der Teilnehmer über SIP SUBSCRIBE/NOTIFY und das Konferenzereignispaket einsehen. Der Client des Besitzers erfährt den URI, an den SIP SUBSCRIBE gesendet werden soll, über den vorangehenden SIP-Kontaktheader der 200 OK-Nachricht *, die* als Antwort auf die EINLADUNG an die Konferenz-URI gesendet wird, während für Teilnehmer die gleichen Informationen in einer vorhergehenden Anruf-Info NOTIFY enthalten sind.

Die maximale Anzahl von Konferenzteilnehmern wird mit der Cisco BroadWorks-Systemeinstellung (*maxConferenceParties)* festgelegt. Für einen bestimmten Anruf zeigt sie die Anzahl der aktiven Teilnehmer an, die ein Benutzer gleichzeitig haben oder über die Steuerungsoption "Teilnehmer hinzufügen" während eines Anrufs oder über die Cisco BroadWorks N-Way-Anruffunktion hinzufügen kann.

Diese Informationen werden vom Anwendungsserver (AS) mit dem folgenden CLI-Befehl (Command Line Interface) abgerufen.

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

Beispielausgabe:
maxKonferenzteilnehmer = 6
KonferenzURI =
```

Nachdem der Wert für maxConferenceParties (der einen Bereich von 4 bis 15 hat) abgerufen wurde, sollte das %MAX_CONF_PARTIES_WXT%-Tag entsprechend festgelegt werden.

```
<Konfiguration>
<Services><Anrufe>
```


Vertrauliche Informationen von Cisco

```
<conference enabled="%ENABLE_CONFERENCE_CALLS_WXT%">
    <service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-1%</service-uri>
    <subscribe-conference-Info enabled="%ENABLE_NWAY_PARTICIPANT_LIST_WXT%"/>
        <max-nway-participants>%MAX_CONF_PARTIES_WXT%</max-nway-participants>
</Konferenz>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CONFERENCE_CALLS_WXT%	false	true, false	Legt fest, ob die Konferenzoption für den Benutzer aktiviert wird.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	false	true, false	Setzen Sie diese Einstellung auf "true", um die Teilnehmerliste des N-Way-Eigentümers zu aktivieren. Setzen Sie auf "false", um die Teilnehmerliste des N-Way-Besitzers zu deaktivieren.
%MAX_CONF_PARTIES_WXT%	10	Anzahl zwischen 4 und 15 (Leer)	Gibt die maximale N-Wege-Teilnehmerzahl an, die vom Client erzwungen wird, z. B. 10. Die Serverseite hat ihre eigenen Grenzen. Ein leerer Wert deaktiviert die clientseitige Erzwingung des N-Wege-Teilnehmerlimits.

6.1.22 Anruf pull

Die Call Pull-Funktion kann mit einem einzigen Konfigurationsparameter aktiviert werden, wie im folgenden Beispiel gezeigt.

```
<Konfiguration>
<Services><Anrufe>
<call-pull enabled="%ENABLE_CALL_PULL_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_PULL_WXT%	false	True, false	Aktiviert das Abrufen von Anrufen.

6.1.23 Anruf parken/abrufen

Mit der Funktion "Gruppenanruf parken" können laufende VoIP Anrufe an einen Server für das Parken von Anrufen weitergeleitet werden, sodass der Anrufer eine andere Aktion ausführen und vom selben Benutzer oder einem anderen Benutzer abgerufen werden kann. Ein aktiver Anruf wird auf dem ersten verfügbaren Anschluss innerhalb der Anrufparkgruppe geparkt.

Das Abrufen des Anrufs kann dadurch erfolgen, dass der Benutzer den Anruf unmittelbar nach dem Parken des Anrufs für eine konfigurierbare Anzahl von Sekunden im Dialogfeld parkt. Der geparkte Anruf kann auch vom Benutzer oder einem anderen Benutzer abgerufen werden, indem er die Option zum Abrufen des Anrufs auswählt und die Nummer oder den Anschluss eingibt.

Vertrauliche Informationen von Cisco

```
<Konfiguration>
<Services><Anrufe>
<call-Park enabled="%ENABLE_CALL_PARK_WXT%"
timer="%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_PARK_WXT%	false	True, false	Aktiviert das Parken/Abrufen von Anrufen.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Anzahl zwischen 5 und 30	Gibt die Anzahl der Sekunden an, die der erfolgreich geführte Anruf geparkt für den Benutzer sichtbar ist, bevor er automatisch geschlossen wird.

6.1.24 Anrufstatistik

Berichte über die Anrufendstatistik in Session Initiation Protocol (SIP) BYE-Nachricht ermöglicht das Senden von Anrufstatistiken an ein Remote-Ende, wenn ein Anruf beendet wird. Die Anrufstatistik wird als neuer Header in der SIP BYE-Nachricht oder in der entsprechenden *200 OK-Antwort* auf die BYE-Nachricht gesendet. Die Statistiken umfassen die gesendeten oder empfangenen RTP-Pakete (Real-Time Transport Protocol), die Gesamtzahl der gesendeten oder empfangenen Bytes, die Gesamtzahl der verlorenen Pakete, den Verzögerungs-Jitter, die Round-Trip-Verzögerung und die Anrufdauer.

```
<Konfiguration>
<Services><Anrufe>
<call-statistics enabled="%ENABLE_CALL_STATISTICS_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_STATISTICS_WXT%	false	true, false	Legen Sie den Wert auf "true" fest, um die Erfassung von Anrufmetriken zu ermöglichen. Legen Sie "false" fest, um die Erfassung von Anrufmetriken zu deaktivieren.

6.1.25 Automatische Wiederherstellung von Anrufen/nahtlose Anrufübergabe

Der Client unterstützt die automatische Wiederherstellung von Anrufen beim Wechseln von Netzwerken, während der Benutzer einen laufenden VoIP Anruf führt. Die automatische Anrufwiederherstellung funktioniert in beide Richtungen – Cellular Data-to-WiFi und WiFi-to-Cellular Data sowie beim Umschalten zwischen WiFi-Netzwerken. Es wird versucht, den Anruf innerhalb eines Zeitrahmens von einer Minute wiederherzustellen, dann wird er beendet. Wenn mehr als ein VoIP Anruf aktiv ist, wird nur der aktive Anruf wiederhergestellt.

Beim Übergang von Mobilfunkdaten zu WLAN behält der Client die laufenden VoIP Anrufe über Mobilfunkdaten bei, bis sie beendet werden oder das Mobilfunkdatennetzwerk unterbrochen wird.

Vertrauliche Informationen von Cisco

```
<Konfiguration>
<Services><Anrufe>
<auto-recovery enabled="%ENABLE_CALLS_AUTO_RECOVERY_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false	true, false	Legt fest, ob der automatische Wiederherstellungsmechanismus für den Benutzer aktiviert wird.

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 *6.1.33 XSI-Ereigniskanal*) und vom Anwendungsserver (AS) ab, der für das Senden *des X-BroadWorks-Correlation-Info* SIP-Headers konfiguriert ist (siehe *Webex für Cisco BroadWorks Solution Guide*).

Wenn die Funktion deaktiviert ist, stehen dem Benutzer keine Aufzeichnungsschaltflächen und -Optionen zur Verfügung. Beachten Sie, dass die Anrufaufzeichnung nicht pro Anruf, sondern pro Benutzer ausgeführt wird. Das heißt, wenn einer der Teilnehmer eines Anrufs die Anrufaufzeichnung unterstützt, kann der Anruf aufgezeichnet werden.

Wenn die Anrufaufzeichnungsfunktion aktiviert ist, wird durch eine visuelle Anzeige immer angezeigt, ob der Anruf aufgezeichnet wird. Die folgenden Anrufaufzeichnungsmodi werden von Cisco BroadWorks unterstützt:

Immer

- Die Anrufaufzeichnung wird automatisch beim Verbindungsaufbau gestartet.
- Der Benutzer kann **die Anrufaufzeichnung NICHT** stoppen/anhalten.

Immer mit Unterstützung für Pause/Fortsetzen

- Die Anrufaufzeichnung wird automatisch gestartet, sobald der Anruf hergestellt wird, der Benutzer kann den Anruf jedoch anhalten und fortsetzen.
- Mögliche Benutzerinteraktionen:
  - Aufzeichnung wird ausgeführt – **Aktion Aufzeichnung anhalten** .
  - Aufzeichnung pausiert – **Aktion Aufzeichnung fortsetzen** .

On-Demand

- Nachdem der Anruf hergestellt wurde, beginnt die Anrufaufzeichnung auf dem Server.
- Wenn der Benutzer während des Anrufs auf die Option "Aufzeichnung starten" klickt, wird die Anrufaufzeichnung gespeichert und der Anruf wird nicht gestartet. Andernfalls wird die Anrufaufzeichnung auf dem Server gelöscht, wenn der Benutzer keine Startaufzeichnung initiiert.

Vertrauliche Informationen von Cisco

- Mögliche Benutzerinteraktionen:
  - Es wurde noch keine Aufzeichnung gestartet – **Aktion Aufzeichnung starten** .
  - Aufzeichnung wird ausgeführt – **Aktion Aufzeichnung anhalten** .
  - Aufzeichnung pausiert – **Aktion Aufzeichnung fortsetzen** .

Auf Anforderung durch einen vom Benutzer initiierten Start

- Der Benutzer kann die Anrufaufzeichnung jederzeit und mehrmals während eines Anrufs starten, stoppen, anhalten und fortsetzen.
- Für jeden Start der Anrufaufzeichnung werden separate Anrufaufzeichnungen erstellt.
- Mögliche Benutzerinteraktionen:
  - Es wurde noch keine Aufzeichnung gestartet – **Aktion Aufzeichnung starten** .
  - Aufzeichnung wird ausgeführt – **Aktion Aufzeichnung anhalten** und **anhalten** .
  - Aufzeichnung pausiert – **Aktion Aufzeichnung anhalten** und **fortsetzen** .

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

```
<Konfiguration>
<Services><Anrufe>
<record enabled="%ENABLE_CALL_RECORDING_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_RECORDING_WXT%	false	true, false	Aktiviert die Steuerelemente für die Anrufaufzeichnung.

6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige

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

Die visuelle Voicemail (Visual Voicemail, VVM) wird nur für Audio unterstützt. Unterstützte Formate sind wav, ulaw und mov mit H264-Video (nur als Audio wiedergegeben). Es ermöglicht Benutzern, eingehende Voicemails in einer Listenansicht anzuzeigen und einzelne Elemente abzuspielen. Diese Funktion basiert auf Xsi, Benachrichtigungen über neue Voicemails werden jedoch über SIP bereitgestellt. Daher muss SIP aktiviert sein, damit die Benachrichtigungen funktionieren. Darüber hinaus ist SIP SUBSCRIBE für die Nachrichtenanzeige (MWI) erforderlich, damit die Benachrichtigungen empfangen werden, und MWI muss aktiviert sein, damit Visual Voicemail funktioniert. Weitere Informationen zur SIP-Konfiguration finden Sie in diesem Abschnitt *6.1.1 SIP-Server-Einstellungen*.

Vertrauliche Informationen von Cisco

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

Visual Voicemail muss in der Konfiguration separat aktiviert werden.

Die folgenden Einstellungen sind im CommPilot-Portal erforderlich, um Visual Voicemail zu haben:

- Sprachnachrichten aktiviert
- Option "Wenn die Nachricht eingeht, verwenden Sie Unified Messaging" ist aktiviert
- Die Option "Signalton für wartende Telefonnachrichten verwenden" ist aktiviert

Wenn dem Benutzer auf der Cisco BroadWorks-Seite kein Visual Voicemail-Service zugewiesen ist, wird die Konfiguration des Service automatisch deaktiviert.

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

Um Voicemail-Nachrichteninformationen auf der Benutzeroberfläche anzuzeigen, muss der Client SIP-MWI-Benachrichtigungen vom Server empfangen (d. h. das Voicemail-Ereignispaket). In der folgenden Tabelle finden Sie Informationen zu den Abonnementoptionen. Beachten Sie außerdem, dass MWI erforderlich ist, damit Benachrichtigungen über die visuelle Voicemail funktionieren.

Beachten Sie, dass der Client bei einem Fehler beim SIP-Abonnement für das Voicemail-Ereignispaket wiederholt, wenn er entsprechend konfiguriert ist. Weitere Informationen zur SIP SUBSCRIBE-Wiederholungskonfiguration finden Sie in diesem Abschnitt *6.1.9 SIP SUBCSRIBE und REGISTER Aktualisieren und SUBSCRIBE Wiederholen.*

```
<Konfiguration>
<Services><Anrufe>
<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>
</Voicemail>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_VOICE_MAIL_WXT%	false	true, false	Legen Sie "true" fest, um die Voicemail-Unterstützung zu aktivieren. Legen Sie "false" fest, um die Voicemail-Unterstützung zu deaktivieren.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	true,false	Wenn diese Option auf "false" gesetzt ist, ist VVM deaktiviert. Wenn diese Option auf "true" gesetzt ist, ist VVM aktiviert. Beachten Sie, dass aus Gründen der Abwärtskompatibilität weiterhin voice-mail enabled=false vor dem eigentlichen VVM-Attribut verwendet wird.
%BWVOICE-PORTAL-NUMMER-1%	leer	Zahl	Der Client ruft diese Nummer an, die normalerweise mithilfe eines vorhandenen Cisco BroadWorks System-Tags beim Wählen von Voicemail angegeben wird.
%ENABLE_MWI_WXT%	false	true, false	Legen Sie den Wert auf "true" fest, um MWI zu aktivieren. Legen Sie "false" fest, um MWI zu deaktivieren.
%MWI_MODE_WXT%	leer	implizit, explizit	Legen Sie diese Einstellung auf "explizit" fest, um SIP SUBSCRIBE für MWI Ereignispaket zu senden, wenn MWI aktiviert ist. Bei Verwendung von "implizit" wird kein SIP SUBSCRIBE für MWI Ereignispaket gesendet, wenn MWI aktiviert ist. Wenn Sie das Feld leer lassen, wird MWI deaktiviert.

6.1.28 Voicemail-Transkription für Webex Calling

Mit diesem Feature werden Voicemail-Nachrichten in Text konvertiert und in der visuellen Voicemail-Nachrichtenansicht in der Webex Calling Desktop- und mobilen App angezeigt.

Die Funktion sollte nur in folgenden Fällen für einen Benutzer aktiviert werden:

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	false	true, false	[Nur Webex Calling] Legt fest, ob das Voicemail-Transkript nur verfügbar ist, wenn die visuelle Voicemail aktiviert ist.

Vertrauliche Informationen von Cisco

6.1.29 Anrufeinstellungen

6.1.29.1 Rufumleitung immer aktiviert

Mit dem folgenden benutzerdefinierten Tag kann die Verfügbarkeit des Cisco BroadWorks Call Forwarding Always Service in der Webex für den Cisco BroadWorks Client gesteuert werden.

```
<Konfiguration>
<Dienstleistungen><Zusatzleistungen>
<call-forwarding-always enabled="%ENABLE_CALL_FORWARDING_ALWAYS_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	true, false	Steuert die Verfügbarkeit des Always Call Forwarding Service. Die Funktion ist standardmäßig deaktiviert.

HINWEIS: Anrufweiterleitung Immer und Anrufweiterleitung an Voicemail (*6.1.29.2 Anrufweiterleitung an Voicemail*) können zusammen verwendet werden, um die Einstellung "Anrufweiterleitung" in den Webex Apps anzuzeigen oder auszublenden. Wenn beide Tags deaktiviert sind, wird die Einstellung "Anrufweiterleitung" in den Webex Apps ausgeblendet.

6.1.29.2 Anrufweiterleitung an Voicemail

Ab Version 43.9 bietet Webex App eine Option, um die Verfügbarkeit der Weiterleitung an Voicemail zu steuern. Standardmäßig ist das Feature aktiviert und kann mit der folgenden Konfigurationsoption deaktiviert werden.

```
<Konfiguration>
<Dienstleistungen>
   <Voicemail>
      <Weiterleitung aktiviert="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	true	true, false	Steuert die Verfügbarkeit der Weiterleitung an Voicemail. Die Funktion ist standardmäßig aktiviert.

HINWEIS 1: Diese Funktion hängt davon ab, ob dem Benutzer einer der Dienste "Voice Messaging User" oder "Third-Party Voicemail Support" zugewiesen wird.

HINWEIS 2: Anrufweiterleitung an Voicemail und Anrufweiterleitung Immer (*6.1.29.1 Rufumleitung immer aktiviert*) können zusammen verwendet werden, um die Einstellung "Anrufweiterleitung" in den

Vertrauliche Informationen von Cisco

Webex-Apps anzuzeigen oder auszublenden. Wenn beide Tags deaktiviert sind, wird die Einstellung "Anrufweiterleitung" in den Webex Apps ausgeblendet.

6.1.29.3 BroadWorks Anywhere (Single Number Reach)

Die folgenden benutzerdefinierten Tags steuern die Verfügbarkeit von BroadWorks Anywhere und die Verfügbarkeit seiner Einstellungen in der Webex für den Cisco BroadWorks Client. Beachten Sie, dass der Name dieser Funktion auf dem Client "Meine Nummern *verwalten" lautet*.

```
<Konfiguration>
<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-überall>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_BROADWORKS_ANYWHERE_WXT%	false	true, false	Aktiviert BroadWorks Anywhere (BWA) auf Konfigurationsebene.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	true	true, false	Legt fest, ob die Beschreibung des BWA-Standorts für den Benutzer verfügbar sein soll.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	true, false	Wird auf "true" gesetzt, um Alert All Locations für den BWA-Service für den Benutzer verfügbar zu machen. Wird auf "false" gesetzt, damit Alert All Locations für den BWA-Service für den Benutzer nicht verfügbar ist.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	false	true, false	Steuert, ob die Anwendung den Status Alle Standorte alarmieren soll, wenn ein zweiter oder jeder nachfolgende neue BWA-Standort hinzugefügt wird.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	true, false	Steuert, ob die Call Control des BWA-Standorts für den Benutzer verfügbar sein soll.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	false	true, false	Steuert den Standardzustand der Call Control für die BWA-Location.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	true, false	Steuert, ob der Umleitungsinhibitor des BWA-Standorts für den Benutzer verfügbar sein soll.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	true, false	Steuert den Standardzustand des Umleitungsinhibitors der BWA-Position.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false	true, false	Legt fest, ob die Antwortbestätigung der BWA-Lokation für den Benutzer zur Verfügung stehen soll.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	false	true, false	Steuert den Standardzustand der Antwortbestätigung der BWA-Lokation.

6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen

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

Darüber hinaus bietet der Client die Möglichkeit, stattdessen die Webansicht für Anrufeinstellungen (Call Settings Web View, 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 ist ratsam, die Einstellungen auszublenden, die bereits in der Anwendung sichtbar sind, wie z. B. Call Center (siehe Abschnitt *6.1.31 Callcenter/Anrufwarteschlange – An-/Abmeldung*) und BroadWorks Anywhere (siehe Abschnitt *6.1.29.3 BroadWorks Anywhere*). Es ist auch ratsam, den remote Office-Dienst auszublenden, da er vom BroadWorks Anywhere-Dienst abgelöst wurde.

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

```
<Konfiguration>
<Dienstleistungen>
<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-Einstellungen>
   <service name="Anrufweiterleitung immer"
visible="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <service name="Anrufweiterleitung besetzt"
visible="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <service name="Anrufweiterleitung nicht erreichbar"
visible="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
   <service name="Anrufweiterleitung ohne Antwort"
visible="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <service name="Bitte nicht stören"
visible="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
```


Vertrauliche Informationen von Cisco

```
   <service name="Anonyme Anrufzurückweisung"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="gleichzeitiger Rufton persönlich"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <service name="Sequenzieller Rufton"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <service name="Automatischer Rückruf"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <service name="Anklopfen" visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Blockieren der Zustellung der Anrufleitungs-ID"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <service name="persönlicher Assistent"
visible="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
   <service name="Callcenter - 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-Büro" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Sprachnachrichten-Benutzer"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 <-/Service-Einstellungen>
<userportal-Settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
Settings>
<-/Web-Call-Einstellungen>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%WEB_CALL_SETTINGS_TARGET_WXT%	äußerlich	Extern, CSW	Steuert den Modus des Verwaltungsportals. Legen Sie diese Option auf "extern" fest, um die konfigurierte Einstellungsportal-URL in einem externen Browser zu öffnen. Legen Sie "csw" fest, um das CSW-Portal in einem eingebetteten Browser zu öffnen, indem Sie den Abschnitt mit den zusätzlichen Parametern <services><web-call-Settings> aus der POST-Anfrage verwenden.
%WEB_CALL_SETTINGS_URL_WXT%	leer	URL-Zeichenfolge	URL für das Einstellungsportal. Beispiel: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option "Anrufweiterleitung immer" für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option "Rufton ein/aus" (Ruhe) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option Anonyme Anrufzurückweisung (ACR) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option Anrufweiterleitung bei besetzt (Call Forwarding Besetzt, CFB) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option Anrufweiterleitung nicht erreichbar (CFNR) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option CFNA (Call Forwarding No Answer, Anrufweiterleitung, keine Antwort) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option SIMRING (Simultaneous Ring Personal) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	true	true, false	Steuert, ob die Option Sequenzieller Rufton (SEQRING) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option Remote-Büro (RO) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option Automatischer Rückruf (ACB) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option Anklopfen für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	true	true, false	Legt fest, ob die CLIDB-Option (Calling Line ID Delivery Blocking) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option "persönlicher Assistent" (PA) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	true	true, false	Steuert, ob die Option BroadWorks Anywhere (BWA) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option "Callcenter" für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	true	true, false	Steuert, ob die Option BroadWorks Mobility (BWM) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. Derzeit lautet der empfohlene Wert "falsch", da es Interoperabilitätsprobleme zwischen Webex für Cisco BroadWorks und BroadWorks Mobility gibt.
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	true	true, false	Legt fest, ob die Option "Sprachverwaltung" (VM) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false	true, false	Legt fest, ob das neue Branding WebView Anrufeinstellungen 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%	true	true, false	Legt fest, ob die Optionen für E-Mail-/Voicemail-Nachrichten in den webbasierten Einstellungen angezeigt werden.
%USER_PORTAL_SETTINGS_URL_WXT%	leer	URL-Zeichenfolge	Gibt die URL zum Portal für Benutzereinstellungen an. Um die Funktion zu aktivieren und die Schaltfläche Auf das Benutzerportal zugreifen in der Benutzeroberfläche anzuzeigen, darf dieses benutzerdefinierte Tag nicht leer sein. Beispiel: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	äußerlich	Extern, intern	Gibt an, ob die URL in einem eingebetteten oder externen Browser geöffnet werden soll.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false	True, false	Nur anwendbar, wenn der eingebettete Browser konfiguriert ist (USER_PORTAL_SETTINGS_TARGET_WXT=intern). Wenn diese Option aktiviert ist, wird eine HTTP POST-Anforderung verwendet, und ein kurzlebiges BroadWorks-Token wird als Teil des BODY hinzugefügt. Wenn diese Option deaktiviert ist, wird die URL mit HTTP GET geöffnet.

Vertrauliche Informationen von Cisco

HINWEIS 1: In den Anrufeinstellungen WebView URL sollte immer ein abschließendes "/" konfiguriert sein. Beispiel: https://<XSP-FQDN>/<CSW-Context-Path>/

HINWEIS 2: Die unterstützte Mindestversion der Anwendung "Anrufeinstellungen WebView ist 1.7.5.

Weitere Informationen zur Installation auf Cisco BroadWorks Version 21.0 finden Sie unter Die zusätzlichen Schritte finden Sie im *Webex Cisco BroadWorks Solution Guide*.

6.1.31 Callcenter/Anrufwarteschlange – An-/Abmeldung

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

Ab Desktop Version 42.8 und Mobile Version 42.12 basiert der Call Center (Anrufwarteschlange)-Agent nicht mehr auf der Webansicht für Anrufeinstellungen (siehe Abschnitt *6.1.30 Einstellungen Portal - und webbasierte Anrufeinstellungen*). Die Agentenkonfiguration des Callcenters (Anrufwarteschlange) kann über die Fußzeile des Desktops und die Einstellungen der Mobile Webex-App aufgerufen werden.

```
<Konfiguration>
<Dienstleistungen>
<call-Center-agent enabled="%ENABLE_CALL_Center_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_Center_WXT%	false	true, false	Aktiviert die Call Center-Unterstützung.

6.1.32 XSI-Stamm und -Pfade

Der Webex für den Cisco BroadWorks-Client verwendet die folgenden Tags, um den XSI-Stammpfad, die Pfade für Aktionen und Ereignisse zu steuern, falls diese so konfiguriert werden müssen, dass sie sich von den für die Anmeldung verwendeten Pfaden unterscheiden.

Der Hauptgrund für die Änderung des XSI-Stamms ist die Implementierung des Lastenausgleichs auf Konfigurationsebene, obwohl empfohlen wird, stattdessen den Lastenausgleich auf der HTTP-Ebene zu verwenden.

Die Pfade für Ereignisse und Aktionen werden in der Regel aufgrund von Brandinganforderungen geändert, um den Domänenverweis auf com.broadsoft aus den URL-Pfaden der XSI-HTTP-Anforderungen zu entfernen, die vom Client ausgeführt werden.

```
<Konfiguration>
<Protokolle><xsi>
       <Pfade>
```


Vertrauliche Informationen von Cisco

```
            <root>%XSI_ROOT_WXT%</root>
            <Aktionen>%XSI_ACTIONS_PATH_WXT%</Aktionen>
            <Ereignisse>%XSI_EVENTS_PATH_WXT%</Ereignisse>
        </Pfade>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%XSI_ROOT_WXT%	Verwendet weiterhin den ursprünglichen, der für den Konfigurationsabruf verwendet wird.	URL-Zeichenfolge	Der XSI-Stamm für alle XSI-Operationen. Beispiel: https://Domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	Zeichenfolge	Gibt den XSI-Aktionspfad an. Er sollte mit "/" beginnen und enden und nur den Aktionskontext enthalten. Beispiel: /com.Domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	Zeichenfolge	Gibt den XSI-Ereignispfad an. Sie sollte mit "/" beginnen und enden und nur den Ereigniskontext enthalten. Beispiel: /com.Domain.xsi-events/

6.1.33 XSI-Ereigniskanal

Der XSI-Ereigniskanal wird z. B. für folgende Dienste verwendet:

- XSI-Steuerelemente während eines Anrufs
- Statusbenachrichtigungen zu Anrufeinstellungen
- Anrufaufzeichnung

XSI-Ereignis-Takt wird verwendet, um den XSI-Ereigniskanal offen zu halten, und das Taktintervall kann mit dem folgenden Parameter angegeben werden.

```
<Konfiguration>
<Protokolle><xsi>
<event-Channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
    <heartbeatInterval> %CHANNEL_HEARTBEAT_WXT%</heartbeatInterval>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_XSI_EVENT_CHANNEL_WXT%	true	true, false	Steuert, ob der XSI-Ereigniskanal aktiviert ist. Sie sollte auf "true" festgelegt werden, um z. B. Ereignisse zu empfangen, die sich auf den Anrufsteuerungsservice beziehen. Der empfohlene Wert ist "true".

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%CHANNEL_HEARTBEAT_WXT%	10000	Zahl	Dies ist der Pulsschlag des XSI-Ereigniskanals (in Millisekunden). Der Standardwert ist "10000".

6.1.34 Codec-Konfiguration

Webex für Cisco BroadWorks bietet eine Vielzahl von Audio- und Videocodecs. Die entsprechenden Codec-Listen befinden sich unter *config/services/calls/* in den *Bereichen audio/codecs* und *video/codecs* . Die Priorität jedes Codecs kann über das *XML-Attribut priority* geändert werden, das ein Wert zwischen 0,0 (niedrig) und 1,0 (hoch) ist.

Die Webex-App unterstützt offiziell die folgenden Codecs:

- Audio
  - Opus
  - G.722
  - G.729
  - PCMU (G.711U)
  - PCMA (G.711A)
  - iLBC
  - KI-Codec
- Video
  - H.264

Vertrauliche Informationen von Cisco

```
<Konfiguration>
<Services><Anrufe>
  <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="telefon-ereignis" payload="101" in-band="false"/>
    …
  <Video>
    <Codecs>
      <codec name="H264" payload="109" resolution="CIF" framerate="25"
bitrate="768000" priority="1.0">
        <Paketmodus>0</Paketmodus>
```

Der Client unterstützt H.264 als Videocodec. Das Attribut für die Videoauflösung kann verwendet werden, um einen der folgenden verfügbaren Werte festzulegen: SUBQCIF, QCIF, CIF, 4CIF, VGA und HD.

Wenn die Bitrate nicht in der Konfiguration angegeben ist, werden die Standardwerte für die Bitrate verwendet. Die Standardwerte für die Bitrate pro Auflösung und Bildrate sind in der folgenden Tabelle aufgeführt.

Auflösung	Videogröße *	FPS (Bilder 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 beworbene 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 und auf beiden Clients gleich.

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

Vertrauliche Informationen von Cisco

Der Packetierungsmodus kann als SingleNAL (0) oder Non-Interleaved (1) konfiguriert werden. Die Vorlage verwendet standardmäßig SingleNAL (<Paketmodus>0</Paketmodus>).

Die Konfiguration von Telefonereignissen, einzeln oder mehrere, wird ebenfalls unterstützt. Während der Codec-Aushandlung sendet der Client alle konfigurierten Codecs, einschließlich des Telefonereignisses. Nachdem der Audiocodec ausgewählt wurde, wird im Angebot nach einem Telefonereignis gesucht. Wenn das Angebot das Telefonereignis mit der Abtastrate des ausgehandelten Audiocodecs enthält, wird dieses Telefonereignis ausgewählt. Andernfalls wird das erste Telefonereignis in der Liste verwendet.

Wenn mindestens ein Telefonereignis ausgehandelt wurde, werden die DTMFs (Dual-Tone Multi-Frequency) als RTP Pakete mit dem entsprechenden Nutzlasttyp gesendet. Und wenn überhaupt keine Telefonereignisse ausgehandelt werden, werden die DTMFs als RTP Pakete mit dem Nutzlasttyp des ausgehandelten Audiocodecs gesendet. Out-of-Band-Mechanismen zum Übermitteln von DTMFs werden von der App Webex nicht unterstützt.

Beispiele für konfigurierte Codecs:

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

Wenn ein Audiocodec mit einer Abtastrate von 48 KBit/s ausgehandelt wird, wird das Telefonereignis mit der Nutzlast 101 verwendet.

6.1.34.1 KI-Codec

Ab Version 44.8 führt die Webex-App die Unterstützung eines neuen Audio-Codecs ein – AI Codec (xCodec). Dieser Audiocodec 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 Verbindung mit dem Opus-Codec. Das bedeutet, dass sowohl der Opus- als auch der KI-Codec während der SDP-Verhandlungen von beiden Seiten beworben und ausgehandelt werden sollten.

6.1.35 SIP-URI-Wahl

Derzeit ist die SIP-URI-Wahl über BroadWorks nicht verfügbar und standardmäßig werden alle SIP-URI-Anrufe über Locus geleitet, auch bekannt als "Free Calling". In manchen Umgebungen ist dies nicht erwünscht und solche Anrufe sollten blockiert werden.

HINWEIS: Dies gilt nur, wenn Locus Calling deaktiviert ist. Nur in diesem Fall funktioniert die SIP URI Wählsperre.

Diese Option wird in der folgenden Konfiguration bereitgestellt.

```
<Konfiguration>
    <Dienstleistungen>
        <Anrufe>
            <sip-uri-dialing enable-locus-
calling="%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	true	true, false	Steuert, ob der SIP-URI über Locus geroutet werden soll (true) oder blockiert (false).

6.1.36 Anrufverlauf auf allen Geräten

Der Client bietet die Möglichkeit, das Anrufprotokoll anstatt lokal auf dem Server zu speichern und abzurufen. Auf diese Weise wird der Anrufverlauf über alle Geräte hinweg vereinheitlicht.

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	true, false	Legt fest, ob die Anwendung den einheitlichen Anrufverlauf oder den clientseitigen (lokalen) Anrufverlauf verwenden soll.

6.1.37 Videoanrufe deaktivieren

In Version 41.9 wurde die Möglichkeit hinzugefügt, Videoanrufe zu deaktivieren. Es gibt separate Konfigurationsoptionen, um diese Funktion für BroadWorks-gestützte und Locus (kostenlose) VoIP Anrufe zu steuern.

Wenn die Funktion aktiviert und der Feature-Tag auf "false" gesetzt ist:

- Die Einstellung "Eingehende Anrufe mit eingeschaltetem Video annehmen" wird dem Benutzer nicht angezeigt
- Wenn alle eingehenden Videoanrufe angenommen werden, handelt es sich um Audioanrufe
- Der Benutzer kann einen Anruf nicht an Video eskalieren und Videoeskalationen werden automatisch abgelehnt.

Wenn Videoanrufe aktiviert sind, wird eine neue Konfigurationseigenschaft hinzugefügt, um den Standardwert der Einstellung "Eingehende Anrufe mit eingeschaltetem Video annehmen" zu steuern. Standardmäßig ist dieses Feature für den Desktop aktiviert und für Mobilgeräte und Tablets deaktiviert.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SIP_VIDEOCALLS_WXT%	true	true, false	Steuert die Verfügbarkeit von SIP-Videoanrufen über BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	true	true, false	Steuert die Verfügbarkeit von Locus (kostenlosen) Videoanrufen.
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Desktop – true Handy/Tablet – false	True, false	Steuert den Standardwert der Einstellung "Eingehende Anrufe annehmen, wenn mein Video aktiviert ist".

6.1.38 Notrufe (911) – Standortberichte mit E911-Anbieter

Der Desktop- und Tablet-Webex-Client unterstützt E911-Standortberichte mit RedSky, Intrado oder Bandwidth als E911-Notrufanbieter für die Webex für die BroadWorks-Bereitstellung. Der E911-Anbieter bietet Unterstützung pro Gerät (für Webex Desktop- und Tablet-Apps und HELD-fähige MPP-Geräte) und ein Netzwerk, das Notrufe an Notrufabfragestellen (PSAPs) in den USA, ihren Territorien (Guam, Puerto Rico und Jungferninseln) und nur in Kanada weiterleitet. Der Service wird für jeden Standort separat aktiviert.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	false	True, false	Aktiviert die Notfallortungsplattform des E911-Anbieters.
%BWE911-PRIMÄRE-HELDURL%	leer	Zeichenfolge	Gibt die URL zur Notfallortplattform des E911-Anbieters an, die das HELD-Protokoll unterstützt.
%BWE911-KUNDENID%	leer	Zeichenfolge	Die Kunden-ID (HeldOrgId, CompanyID), die für die HTTPS-Anforderung des E911-Anbieters verwendet wird.
%BWE911-GEHEIMSCHLÜSSEL%	leer	Zeichenfolge	Das Geheimnis zum Authentifizieren der HTTPS-Anforderung des E911-Anbieters.
%BWE911-NOTRUFNUMMERNLISTE%	leer	CSV Zeichenfolge	Die Liste der vom E911-Provider unterstützten Notrufnummern.
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (Benutzer wird nicht mehr aufgefordert)	Nummer [0 – 43200]	Die Zeitüberschreitung in Minuten, die verwendet wird, um den Benutzer daran zu erinnern, den Notfallort zu aktualisieren, wenn der aktuelle Ort nicht eingegeben wird oder ungültig ist. Der vorgeschlagene Wert, wenn die Option aktiviert wird: 1440 (ein Tag).

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (Benutzer kann den Dialog jederzeit abbrechen)	Anzahl [-1 – 100]	Die Zeiten, zu denen der Benutzer das Dialogfeld "Standort" schließen darf, bevor der Standort obligatorisch wird (d. h., er kann das Standortfenster nicht schließen). Mögliche Werte: ▪ N = -1 (Benutzer kann den Dialog jederzeit abbrechen) ▪ N = 0 (Benutzer darf den Dialog nicht abbrechen – obligatorischer Ort immer) ▪ N > 0 (der Benutzer kann den Dialog N Mal abbrechen, bevor er obligatorisch wird)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	aggressiv, once_per_login	once_per_login	Definiert das Verhalten der E911-Standortaufforderung. Der Wert "aggressiv" zeigt dem Benutzer den Dialog bei jedem Netzwerkwechsel an einem unbekannten Ort an, während der Wert "once_per_login" den Dialog nur einmal anzeigt, um weitere Popups und Ablenkungen für den Benutzer zu vermeiden.

HINWEIS 1: BWE911-*** Tags sind "Dynamic Built-in System Tags". Weitere Informationen finden Sie im Abschnitt *5.7 Integrierte Cisco BroadWorks Dynamic-System-Tags*.

HINWEIS 2: Wenn VOIP-Anrufe deaktiviert sind, ist der einzige sinnvolle Wert für die Notrufnummer (%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 sowie die Priorität, die als Anrufleitungsidentität verwendet werden soll. Wenn in der eingehenden SIP-INVITE-Anfrage ein X-BroadWorks-Remote-Party-Info-Header enthalten ist, wird dieser mit Priorität vor den SIP From- und PAI-Headern verwendet. Wenn in der eingehenden SIP INVITE-Markierung kein X-BroadWorks-Remote-Party-Info-Header enthalten ist, bestimmt dieser neue Parameter, ob der SIP From-Header Vorrang vor dem PAI-Header hat oder umgekehrt.

Wenn das enabled-Attribut des Tags <use-pai-as-calling-identity> auf "true" gesetzt ist, wird der PAI-Header mit Priorität vor dem From-Header verwendet. Die Identität des Anrufers wird verwendet, um den Kontakt aufzulösen und dem Benutzer zu präsentieren.

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

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	true, false	Steuert, ob die dem Benutzer angezeigte Anrufidentität aus den Headern SIP From bzw. SIP P-Asserted-Identity übernommen wird. Legen Sie "true" fest, um den PAI-Header mit Priorität zu verwenden.

6.1.40 Bildschirmfreigabe deaktivieren

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

- Dem Benutzer wird die Option zum Starten der Bildschirmfreigabe in 1-1-Anrufen nicht angezeigt
- Die eingehenden Anfragen zur Bildschirmfreigabe werden abgelehnt und dem Benutzer wird eine informative Meldung angezeigt

Diese Funktion ist standardmäßig aktiviert.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SCREEN_SHARE_WXT%	true	true, false	Gibt an, ob die Bildschirmfreigabe für den Benutzer aktiviert werden soll.

6.1.41 Spam-Anrufanzeige

Wenn die Funktion (pro Bereitstellungstyp) aktiviert und die Funktion in der Konfigurationsdatei aktiviert ist, verarbeitet die Webex App den neuen Parameter, der den Überprüfungsstatus von Spam-Anrufen angibt, wenn sie als Teil der Push-Benachrichtigung für neue Anrufe oder der Anrufprotokolldatensätze empfangen werden.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	true, false	Steuert die Verfügbarkeit der Spam-Anrufanzeige im Bildschirm für eingehende Anrufe und im Anrufprotokoll nur für Webex Calling.

6.1.42 Rauschunterdrückung und Bandbreitenerweiterung für Festnetz-/Mobilanrufe

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

Vertrauliche Informationen von Cisco

In Version 44.2 der Webex-App werden neue Sprach-KI-Verbesserungen für eingehende Audiomedien für Schmalband-Festnetzanrufe eingeführt.

- Ein neuer Bandbreitenerweiterungsalgorithmus wird hinzugefügt, um die Audioqualität zu verbessern, indem die Bandbreite des Schmalband-PSTN-Spektrums erweitert und das Rauschen entfernt wird. Die erweiterte Bandbreite erhöht die Verständlichkeit und verringert die Ermüdung des Hörens.
- Der bereits vorhandene Rauschunterdrückungsalgorithmus wurde verbessert, wodurch die Einschränkungen für Warteschleifenmusik und andere Audiotöne (z. B. Piepsignale) aufgehoben werden.
- Wenn diese Funktion aktiviert ist, sehen Benutzer die Anzeige "Smart Audio – extern" und können die Sprach-KI-Verbesserungen für die eingehenden Audiomedien steuern.

Diese Sprachverbesserungen sind standardmäßig aktiviert und aktiviert. Der Benutzer kann den Anfangszustand über die Smart-Audio-Einstellungen in den Audioeinstellungen steuern.

```
<Konfiguration>
   <Dienstleistungen>
      <Anrufe>
         <speech-enhancements enabled="%ENABLE_SPEECH_ENHANCEMENTS_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	false	true, false	Aktiviert die Spracherweiterungen für externe (eingehende) Medien.

HINWEIS: Die Rauschunterdrückung ist jetzt Teil der zusätzlichen Sprachverbesserungen, und das Tag <Rauschentfernung> wurde durch das neue Tag <Sprachverbesserungen> als veraltet markiert. Das benutzerdefinierte Tag "Rauschentfernung" %ENABLE_NOISE_REMOVAL_WXT% ist ebenfalls veraltet.

6.1.43 QoS DSCP Kennzeichnung

Die QoS-DSCP Markierung wird unterstützt, wenn die Webex-App Medien RTP Paketen (Audio und Video) aufruft. DSCP bestimmt die Klassifizierung des Datenverkehrs für Netzwerkdaten. Dies kann verwendet werden, um zu bestimmen, welcher Netzwerkverkehr eine höhere Bandbreite erfordert, eine höhere Priorität hat und mit größerer Wahrscheinlichkeit Pakete verwirft.

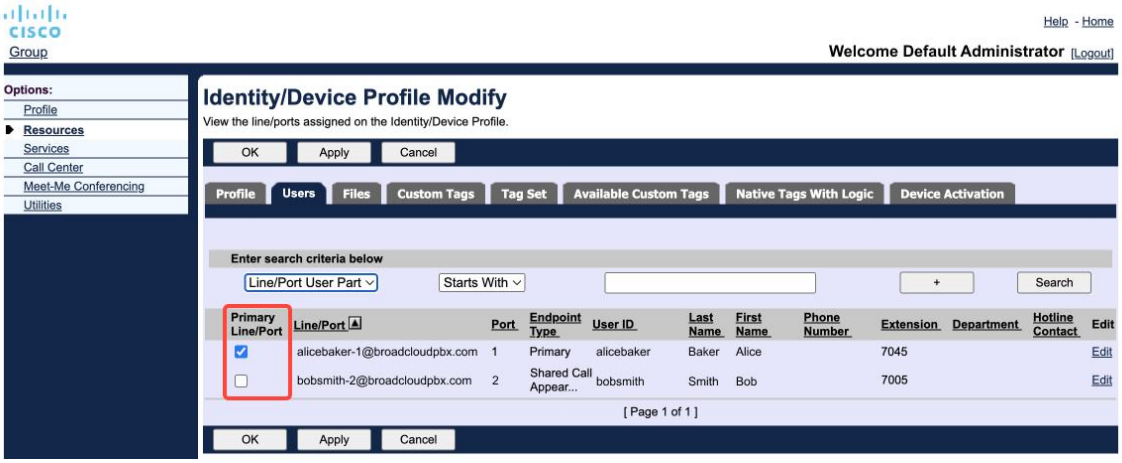
HINWEIS: Neuere Versionen des Betriebssystems Microsoft Windows erlauben es Anwendungen nicht, DSCP oder UP für ausgehende Pakete direkt einzurichten, sondern erfordern stattdessen die Bereitstellung von Gruppenrichtlinienobjekten (Group Policy Objects, GPO), um DSCP Markierungsrichtlinien basierend auf UDP Portbereichen zu definieren.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_AUDIO_QOS_WXT%	true	True, false	Aktiviert QoS für Audioanrufe.
%AUDIO_QOS_VALUE_WXT%	46	0-63	Gibt den QoS-Wert für den ausgewählten QoS-Typ für die Audioanrufe an. Hinweis: Der Standardwert wird verwendet, wenn kein Wert angegeben wird oder der Wert nicht erfolgreich analysiert werden konnte.
%ENABLE_VIDEO_QOS_WXT%	true	True, false	Aktiviert QoS für Videoanrufe
%VIDEO_QOS_VALUE_WXT%	34	0-63	Gibt den QoS-Wert für den ausgewählten QoS-Typ für die Videoanrufe an. Hinweis: Der Standardwert wird verwendet, wenn kein Wert angegeben wird oder der Wert nicht erfolgreich analysiert werden konnte.

6.1.44 Primärprofil

Wenn bei der Integration der gemeinsam genutzten Leitungen (*6.1.51.1 Desktop – Darstellung gemeinsam* genutzter Leitungen**Error! Reference source not found.**) die Leitung des Benutzers mit einem anderen Benutzer geteilt wird, können mehrere Profile desselben Typs für den Benutzer konfiguriert sein. Um das richtige Profil für die Anmeldung bei den Telefondiensten auszuwählen, wurde Cisco BroadWorks erweitert, um anzuzeigen, ob ein Benutzer Eigentümer eines Geräts ist, d. h. ihm ist die Hauptleitung/der Port für ein Gerät zugewiesen. Weitere Informationen zum Cisco BroadWorks-Update finden Sie unter [Besitzer-Flag in der Geräteliste zur Unterstützung Webex gemeinsam genutzten Client-Leitungen](#).



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

Vertrauliche Informationen von Cisco

Ab Release 43.2 wird eine neue Konfigurationsoption (*device-owner-restriction*) hinzugefügt, um zu steuern, ob die primäre Profileinschränkung angewendet werden soll. Diese Einstellung kann verwendet werden, um der Webex-Anwendung zu erlauben, ein nicht primäres Leitungs-/Portprofil für die Anmeldung bei den Telefonservices zu verwenden. Diese Konfigurationsoption wird auf alle Konfigurationen angewendet, unabhängig von der Anzahl der für den Benutzer konfigurierten Profile (**wenn die Beschränkung des Gerätebesitzes aktiviert ist und kein Gerät mit primärer Leitung/Port für die entsprechende Plattform vorhanden ist, werden die Telefonservices nicht verbunden**).

Die gleiche Einschränkung gilt für Geräte, die Benutzer innerhalb der Desktop Webex App koppeln können. Der Benutzer kann nur Geräte sehen und mit ihnen koppeln, die er besitzt. Dies verhindert die Kopplung mit Geräten eines anderen Benutzers, dem eine gemeinsame oder virtuelle Leitung zugewiesen ist. Der Wert desselben Konfigurationsparameters gilt auch für diese Einschränkung.

```
<Konfiguration>
<Services><Anrufe>
<device-owner-restriction enabled="%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	true	true, false	Steuert die Beschränkung des Gerätebesitzers, d. h., ob die Telefonservices das primäre Profil für das jeweilige Gerät verwenden sollen.

HINWEIS: Es wird empfohlen, die Besitzerbeschränkung zu aktivieren. Wenn Bluetooth deaktiviert ist, verwenden die Telefonservices das erste gefundene Profil für die Anmeldung. Wenn mehrere Profile für den Benutzer desselben Typs konfiguriert sind, können einige Probleme auftreten.

6.1.45 Sperrliste (nur Webex Calling)

Ab Version 43.5 führt die Webex App eine benutzerdefinierte Sperrliste von Telefonnummern ein. Wenn die Funktion aktiviert ist, kann der Benutzer festlegen, dass eingehende Anrufe von bestimmten Nummern serverseitig blockiert und nicht an die Geräte des Benutzers zugestellt werden. Der Benutzer kann diese blockierten Anrufe im Anrufprotokoll sehen.

Der Benutzer kann die Sperrliste an zwei Stellen konfigurieren: Anrufeinstellungen und Anrufprotokoll. In den Einstellungen kann der Benutzer die Liste der blockierten Nummern anzeigen und bearbeiten. Im Anrufprotokoll kann der Benutzer die Anrufprotokolleinträge für die Anrufe einsehen, die von der benutzerdefinierten Sperrliste blockiert wurden. Diese Datensätze haben die Anzeige "Blockiert", wenn sich die Nummer in der benutzerdefinierten Sperrliste befindet, und der Benutzer hat die Möglichkeit, die Nummer direkt für den angegebenen Datensatz zu entsperren. Die Blockierungsoption ist ebenfalls verfügbar.

Regeln für die zur benutzerdefinierten Sperrliste hinzugefügten Nummern:

- Zahlenformat

Vertrauliche Informationen von Cisco

- Blockieren in den Anrufeinstellungen Wenden Sie E.164 Formatbeschränkung lokal in der App Webex an
- Das Blockieren des Anrufprotokolls ist für alle Webex Calling Einträge zulässig
- Cisco BroadWorks kann Anforderungen für neue Nummern, die der Sperrliste hinzugefügt wurden, basierend auf dem Nummernformat zulassen oder ablehnen

- Interne Nummern – Eingehende Anrufe von internen Nummern werden dem Benutzer zugestellt, auch wenn sie in der benutzerdefinierten Sperrliste enthalten sind

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

Die benutzerdefinierte Sperrliste wird nach dem STIR/SHAKEN, der vom Administrator definierten Sperrliste und den Richtlinien für die Zurückweisung anonymer Anrufe angewendet.

```
<Konfiguration>
<Services><Anrufe>
<call-Block enabled="%ENABLE_CALL_BLOCK_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_BLOCK_WXT%	true	true, false	Aktiviert die benutzerdefinierte Sperrliste Setzen Sie diese Einstellung auf "true", um die Sperrliste in den Anrufeinstellungen und im Anrufprotokoll anzuzeigen

HINWEIS: Diese Funktion hängt davon ab, ob dem Benutzer der Cisco BroadWorks Call Block-Service zugewiesen ist.

6.1.46 Implementierung von Medienanpassung und Resilienz (MARI)

6.1.46.1 Tarifanpassung

Die Anwendung Webex hat bereits Techniken zur adaptiven Medienqualität integriert, um sicherzustellen, dass die Audiowiedergabe nicht von Videopaketverlusten betroffen ist, und um sicherzustellen, dass die Videoratenanpassung genutzt werden kann, um die Bandbreite zu verwalten, die in Zeiten von Überlastung verwendet wird.

Ratenanpassungen oder dynamische Bitratenanpassungen passen die Anrufrate an die variable verfügbare Bandbreite an, wobei die Video-Bitrate je nach Paketverlustbedingung herunter- oder hochgefahren wird. Ein Endpunkt reduziert die Bitrate, wenn er Nachrichten vom Empfänger empfängt, die darauf hinweisen, dass ein Paketverlust vorliegt. Und sobald der Paketverlust abgenommen hat, wird die Bitrate beschleunigt.

Vertrauliche Informationen von Cisco

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

6.1.46.2 Vorwärtsfehlerkorrektur (FEC) und erneute Übertragung von Paketen (RTX)

Ab Version 43.4 erweitert die Webex App den Medienanpassungsmechanismus um die Unterstützung von Forward Error Correction (FEC) und Packets Retransmission (RTX) für Audio- und Videomedien.

FEC bietet Redundanz für die übertragenen Informationen mithilfe eines vorgegebenen Algorithmus. Die Redundanz ermöglicht es dem Empfänger, eine begrenzte Anzahl von Fehlern zu erkennen und zu korrigieren, ohne dass der Sender nach zusätzlichen Daten gefragt werden muss. FEC gibt dem Empfänger die Möglichkeit, Fehler zu korrigieren, ohne dass ein umgekehrter Kanal (wie RTCP) erforderlich ist, um eine erneute Übertragung von Daten anzufordern, aber dieser Vorteil geht auf Kosten einer festen höheren Vorwärtskanalbandbreite (mehr gesendete Pakete).

Die Endpunkte verwenden FEC nicht bei Bandbreiten unter 768 KBit/s. Außerdem muss ein Paketverlust von mindestens 1,5 % vorliegen, bevor FEC eingeführt wird. Endpunkte überwachen in der Regel die Effektivität von FEC. Wenn FEC nicht effizient ist, wird sie nicht verwendet.

FEC verbraucht mehr Bandbreite als die Neuübertragung, hat aber eine geringere Verzögerung. RTX wird verwendet, wenn eine geringe Verzögerung zulässig ist und Bandbreitenbeschränkungen bestehen. Bei großer Verzögerung und ausreichender Bandbreite ist FEC vorzuziehen.

Die Webex-App wählt RTX oder FEC dynamisch aus, abhängig von der ausgehandelten Bandbreite und der Verzögerungstoleranz für einen bestimmten Medienstream. FEC führt aufgrund redundanter Videodaten zu einer höheren Bandbreitenauslastung, führt jedoch nicht zu einer zusätzlichen Verzögerung bei der Wiederherstellung verlorener Pakete. RTX hingegen trägt nicht zu einer höheren Bandbreitenauslastung bei, da die RTP Pakete nur dann erneut übertragen werden, wenn der Empfänger einen Paketverlust in RTCP Rückkanal anzeigt. RTX führt eine Paketwiederherstellungsverzögerung ein, da es dauert, bis das RTCP Paket den Empfänger vom Absender und das erneut übertragene Paket den Empfänger vom Absender erreicht.

FEC muss aktiviert sein, damit RTX aktiviert ist.

```
<config><services><aufrufe>
<Audio>
       <Verbesserungen der Audioqualität>
              <Mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <X-ULPFecuc>8000</X-ULPFECUC>
                            <Nutzlast>111</Nutzlast>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <>8</m>
                            <multi_ssrc>1</multi_ssrc>
                            <non_seq>1</non_seq>
                            <Feedback>0</Feedback>
                            <Bestellen>FEC_SRTP</Bestellen>
                     </fec>
                     <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
```


Vertrauliche Informationen von Cisco

```
                            <Nutzlast>112</Nutzlast>
                            <Zeit>180</Zeit>
                            <Datenfluss>1</Datenfluss>
                            <Bestellen>RTX_SRTP</Bestellen>
                    </rtx>
            </mari>
...
<Video>
        <Verbesserungen der Videoqualität>
                <Mari>
                    <fec enabled="%ENABLE_VIDEO_MARI_FEC_WXT%">
                            <X-ULPFecuc>8000</X-ULPFECUC>
                            <Nutzlast>111</Nutzlast>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <>8</m>
                            <multi_ssrc>1</multi_ssrc>
                            <non_seq>1</non_seq>
                            <Feedback>0</Feedback>
                            <Bestellen>FEC_SRTP</Bestellen>
                    </fec>
                    <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
                            <Nutzlast>112</Nutzlast>
                            <Zeit>180</Zeit>
                            <Datenfluss>1</Datenfluss>
                            <Bestellen>RTX_SRTP</Bestellen>
                    </rtx>
            </mari>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_AUDIO_MARI_FEC_WXT%	false	true, false	FEC für Audioanrufe aktivieren
%ENABLE_AUDIO_MARI_RTX_WXT%	false	true, false	Aktiviert RTX für Audioanrufe (erfordert aktivierte Audio-FEC)
%ENABLE_VIDEO_MARI_FEC_WXT%	false	true, false	FEC für Videoanrufe aktivieren
%ENABLE_VIDEO_MARI_RTX_WXT%	false	true, false	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 einzelnen Gerät hinzugefügt.

Diese Funktion ist für einige Bereitstellungen nützlich, in denen die dargestellte Identität des Anrufs nicht mit der verbundenen Identität übereinstimmt. Dies führt dazu, dass keine beaufsichtigte Rückübertragung an den ursprünglichen Teilnehmer initiiert werden kann. Wenn diese Funktion aktiviert ist, kann der Benutzer mehrere gleichzeitige Anrufe mit demselben Remote-Teilnehmer verarbeiten.

```
<Konfiguration>
   <Dienstleistungen>
      <Anrufe>
```


Vertrauliche Informationen von Cisco

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false	true, false	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 bietet Webex App eine Aushandlung für den Austausch von RTCP-XR-Paketen während eines Anrufs. Die Aushandlung findet während der Einrichtung der SIP INVITE-Sitzung statt. Wenn beide Endpunkte RTCP-XR-Pakete unterstützen, beginnt die Webex-Medien-Engine mit dem Austausch dieser Pakete und unterstützt die adaptive Anrufqualität. Diese Funktion ist standardmäßig aktiviert.

Darüber hinaus werden diese zusätzlichen Metriken nur Webex Calling über SIP BYE gesendet und auf diese Weise in Control Hub verfügbar gemacht.

```
<Konfiguration>
<Protokolle><sip>
   <RTCP-XR>
      <negotiation enabled="%ENABLE_RTCP_XR_NEGOTIATION_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	true	true, false	Ermöglicht die RTCP-XR-Aushandlung und den Paketaustausch für eine bessere Anrufqualität. Standardmäßig aktiviert.

6.1.49 Informationen zur Anrufumleitung

Mit 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.

```
<Konfiguration>
<Services><Anrufe>
<call-forwarding-Info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	true	true, false	Steuert die Sichtbarkeit der Informationen zur Anrufweiterleitung und -umleitung. Legen Sie "true" fest, um die Informationen auf den Anrufbildschirmen und im Anrufprotokoll anzuzeigen.

6.1.50 Anrufer-ID

6.1.50.1 ID des ausgehenden Anrufers

Mit Webex Apps Mobile (Version 44.2) und Desktop (Version 44.3) kann der Benutzer die bevorzugte externe Anrufer-ID für ausgehende Anrufe auswählen. Die Liste der verfügbaren Optionen umfasst:

- Direkte Leitung (Standard)
- Standortnummer
- Benutzerdefinierte Nummer von derselben Organisation
- Anrufwarteschlangen, zu denen der Benutzer gehört, über die Agenten ihre Anrufer-ID-Nummer verwenden können
- Sammelanschlüsse, denen der Benutzer angehört, die es Agenten ermöglichen, ihre Anrufer-ID-Nummer zu verwenden
- Anrufer-ID ausblenden

Hinweise:

- Die Liste der Optionen hängt von der Zeile 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 Standardanrufer-ID des Benutzers verwendet
- Für Notrufe wird immer die Rückrufnummer des Benutzers verwendet
- Veraltet <ausgehende-Anrufe>-Tag im Abschnitt <services><call-Center-agent>

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

```
<Konfiguration>
<Services><Anrufe>
   <Anrufer-ID>
      <ausgehende-anrufe aktiviert="%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%"/>
```


Vertrauliche Informationen von Cisco

```
        <Sammelanschlussgruppe aktiviert="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
        <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </ausgehende Anrufe>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	true, false	Ermöglicht die Auswahl der Leitungs-ID für ausgehende Anrufe.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	false	true, false	Steuert die Verfügbarkeit der zusätzlichen Nummern, die für den Benutzer konfiguriert werden.
%ENABLE_CLID_OUTGOING_CALLS_CALL_Center_WXT%	false	true, false	Steuert die Verfügbarkeit der für den Benutzer konfigurierten Callcenter-Nummern (DNIS).
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	true, false	Steuert die Verfügbarkeit der für den Benutzer konfigurierten Sammelanschlussgruppennummern.
"%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	true, false	Aktiviert die Blockierung der Anrufer-ID-Zustellung als Auswahl für ausgehende Anrufe.

HINWEIS: Die Desktop-App-Version 44.3 unterstützt nur die Callcenter-CLID, und 44.4 fügt Unterstützung für die restlichen Optionen hinzu.

6.1.50.2 Remoteanrufer-ID-Name

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

- Gemeinsame Identität (CI)
- Kontaktservice (benutzerdefinierte Kontakte)
- Outlook-Kontakte (Desktop)
- Lokales Adressbuch (Mobil)

Bei erfolgreicher Kontaktauflösung für eine der Suchquellen wird der Anzeigename des Remoteteilnehmers aktualisiert. Wenn der Kontakt in CI gefunden wird, ist die Anrufsitzung mit den Webex Cloud-Diensten desselben Benutzers verknüpft, was die Möglichkeit bietet, den Avatar und die Anwesenheit des Remote-Teilnehmers anzuzeigen, einen Chat zu führen, den Bildschirm freizugeben, zu einem Webex-Cloud-Meeting zu eskalieren usw.

Vertrauliche Informationen von Cisco

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

```
<Konfiguration>
<Services><Anrufe>
   <Anrufer-ID>
      <Remote-name>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	entschlossen	Gelöst, 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, den Sie in der SIP INVITE-Sitzung erhalten haben.

Vertrauliche Informationen von Cisco

6.1.51 Mehrzeilig

Der Webex Benutzer kann eine Hauptleitung und bis zu 9 Nebenleitungen haben. Sekundäre Leitungen können gemeinsam genutzt oder virtuell (nur Webex Anrufe) sein.

Webex App ruft die Leitungskonfiguration über die DMS-Konfigurationsdatei ab, die bei der Anmeldung und alle 12 Stunden heruntergeladen wird. Falls eine Aktualisierung der Leitungskonfiguration erkannt wird, wird der Benutzer aufgefordert, die Anwendung neu zu starten, um die Änderungen zu übernehmen. Bei erneuter Anmeldung des Benutzers werden Aktualisierungen der Leitungskonfiguration sofort erkannt und angewendet.

Im Folgenden wird der Abschnitt der DMS-Konfigurationsvorlage dargestellt, der sich auf die Unterstützung mehrerer Leitungen für Desktop und Mobile bezieht.

```
<Konfiguration>
<Protokolle>
   <Schluck>
       <lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
          <Persönlich>
             <Leitungsport>%BWDISPLAYNAMELEITUNGSPORT%</Leitungsport>
          </persönlich>
          <line lineType="%BW-MEMBERTYPE-1%">
             <external-id>%BWUSEREXTID-1%</external-id>
             ...
          </Leitung>
          <line lineType="%BW-MEMBERTYPE-2%">
             <externe-id>%BWUSEREXTID-2%</externe-id>
             ...
          </Leitung>
          ...
          <line lineType="%BW-MEMBERTYPE-10%">
             <externe-id>%BWUSEREXTID-10%</externe-id>
             ...
          </Leitung>
```

Um die Funktion für mehrere Leitungen zu steuern, verwenden Sie das dedizierte benutzerdefinierte Tag.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_MULTI_LINE_WXT%	false	True, false	Aktiviert die Unterstützung von mehreren Leitungen (sofern konfiguriert). Wenn diese Option deaktiviert ist (auf "false" gesetzt), wird nur die erste konfigurierte Zeile von der Anwendung verwendet.

HINWEIS 1: Die Funktion Boss-Admin (Executive-Assistant) ist in Kombination mit der Konfiguration mit mehreren Leitungen nicht verfügbar.

HINWEIS 2: Weitere BroadWorks-Anforderungen finden Sie unter "Darstellung gemeinsam genutzter Leitungen" im Webex-für-Cisco-BroadWorks-Lösungsleitfaden.

Vertrauliche Informationen von Cisco

6.1.51.1 Desktop – Darstellung gemeinsam genutzter Leitungen

Ab Version 42.12 bietet Webex Anwendung Unterstützung für gemeinsam genutzte Leitungen. Der Administrator sollte die Darstellung gemeinsamer Anrufe für jede gemeinsam genutzte Leitung festlegen.

In Version 43.12 wurde die Webex-App verbessert, um das Verschieben (lokale Weiterholen) eines gehaltenen Anrufs auf einer gemeinsam genutzten oder virtuellen Leitung zu ermöglichen, der von einem anderen Benutzer oder demselben Benutzer auf einem anderen Gerät erledigt wird. Weitere Informationen finden Sie unter *6.2.13 Anruf verschieben*.

6.1.51.2 Desktop – virtuelle Leitungen (nur Webex Calling)

Nur für Webex Calling Bereitstellung unterstützt Webex App die Konfiguration mehrerer Leitungen mithilfe virtueller Leitungen. Funktional entspricht die Konfiguration mit virtuellen Leitungen der Multi-Leitung, die gemeinsam genutzte Leitungen verwendet – mit der Möglichkeit, die für den Benutzer konfigurierten virtuellen Leitungen zu sehen und sie für eingehende und ausgehende Anrufe zu verwenden.

In Version 43.4 wird die Unterstützung für virtuelle Leitungen um die Funktionen "Gruppenanruf parken" und "Anruf parken abrufen" erweitert.

In Version 43.12 wurde die Webex-App verbessert, um das Verschieben (lokale Weiterholen) eines gehaltenen Anrufs auf einer gemeinsam genutzten oder virtuellen Leitung zu ermöglichen, der von einem anderen Benutzer oder demselben Benutzer auf einem anderen Gerät erledigt wird. Weitere Informationen finden Sie unter *6.2.13 Anruf verschieben*.

6.1.51.3 Mobil (nur Webex Calling)

Nur für Webex Calling Bereitstellung bietet Version 45.4 Unterstützung für mehrere Leitungen (gemeinsam genutzte und virtuelle) in der mobilen Version der Webex App. Die Leitungszuweisung gilt sowohl für Desktop- als auch für mobile Webex-App.

Aufgrund der Besonderheiten der mobilen Plattform kann der Benutzer auf jeder der Leitungen bis zu zwei gleichzeitige Anrufe führen.

> **HINWEIS 1**: Wenn Anrufe mit nativem Dialer aktiviert ist (siehe *6.3.5.1 Anruf mit systemeigenem Dialer*), ist die Funktion für mehrere Leitungen deaktiviert.
>
> **HINWEIS 2**: Die mehrzeilige Tablet-Version wird nicht unterstützt.

6.1.52 Erweiterte SIP-Autorisierung

Version 45.4 der Webex-App bietet eine konfigurierbare Option zur Optimierung der SIP-Kommunikation, indem die Autorisierung auf alle SIP-Sitzungen aufgeteilt wird. Die App speichert die Autorisierung und verwendet sie wieder, bis sie noch gültig ist.

Dieses Feature beschleunigt die SIP-Kommunikation zwischen dem Server und der Webex-App, reduziert den Datenverkehr, verkürzt die Anrufverbindungszeit und verbessert die Gesamtleistung der Webex-App.

Vertrauliche Informationen von Cisco

```
<Konfiguration>
<Protokolle>
  <Schluck>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	true, false	Wenn dieser Wert auf "true" gesetzt ist, ist die SIP-Berechtigungserweiterung aktiviert.

HINWEIS 1: Für einige SBCs ist möglicherweise bei jeder Sitzung eine neue SIP-Autorisierung erforderlich, daher sollte diese Funktion entsprechend den Bereitstellungsspezifika verwendet werden.

HINWEIS 2: Auch wenn diese Funktion aktiviert ist, wenn die Webex-App 401 Unauthorized empfängt, wird bei der nächsten SIP-Anfrage eine neue Autorisierung verwendet.

6.1.53 persönlicher Assistent (Abwesenheitspräsenz)

Mit Version 44.11 wird die App "Mobile Webex" und Version 45.3 der App "Desktop Webex" um eine Integration mit dem Cisco BroadWorks Personal Assistant (PA)-Dienst erweitert. Dies funktioniert in Kombination mit der Abwesenheitspräsenz des Benutzers und erfordert eine Synchronisierung des PA-Status mit der Webex Cloud-Präsenz.

Der PA-Dienst bietet dem Benutzer die Möglichkeit, die Anrufer über den Grund zu informieren, warum der angerufene Teilnehmer nicht verfügbar ist. Optional können Sie auch Informationen darüber bereitstellen, wann der angerufene Teilnehmer zurückkehrt und ob ein Attendant zur Bearbeitung des Anrufs zur Verfügung steht.

Wenn die PA aktiviert ist, steht dem Benutzer die Präsenzoption "Abwesend" zur Verfügung. Es kann verwendet werden, um die PA auf der Cisco BroadWorks-Seite zu konfigurieren. Wenn die Funktion aktiviert ist, sehen Benutzer die Abwesenheit des Benutzers in Kombination mit dem PA-Status und der konfigurierten Dauer.

Der Benutzer kann nur die manuelle PA-Konfiguration konfigurieren. Wenn es Zeitpläne gibt, die sich auf den PA-Dienst auswirken, wird die Anwesenheit über die Statussynchronisierung des persönlichen Assistenten aktualisiert. Die App "Webex" macht jedoch weder die Zeitplankonfiguration noch die Zeitpläne, die sich auf die PA auswirken, verfügbar.

```
<Konfiguration>
<Dienstleistungen>
  <personal-assistant enabled="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	true, false	Legt fest, ob die Abwesenheitsfunktion für den Benutzer verfügbar ist.

HINWEIS 1: Für diese Funktion muss die Statussynchronisierung des persönlichen Assistenten im Partner Hub aktiviert werden.

HINWEIS 2: Die standardmäßige Anrufweiterleitung von Personal Assistant wird nicht wirksam, wenn die Dienste "Ruhe", "Anrufweiterleitung immer" oder "selektive Anrufweiterleitung" aktiv sind.

HINWEIS 3: Die manuellen Präsenzstatus "Bitte nicht stören" und "Besetzt" haben im Vergleich zu "Abwesend" eine höhere Priorität. Wenn das Benutzerhandbuch einen dieser Präsenzstatus aktiviert, führt die Aktivierung des persönlichen Assistenten nicht dazu, dass sich Ihr Präsenzstatus in Abwesend ändert.

Vertrauliche Informationen von Cisco

6.2 Nur-Desktop-Funktionen

6.2.1 Erzwungene Abmeldung

Diese Funktion ermöglicht es Cisco BroadWorks, Online-Clientinstanzen mit demselben Gerätetyp nachzuverfolgen und jeweils nur eine von ihnen online zu lassen. Wenn Cisco BroadWorks den Client auffordert, sich abzumelden, wird die SIP-Verbindung beendet und der Client gibt an, dass der Anruf nicht verbunden ist.

Dieses Feature wird in einigen Bereitstellungen benötigt, in denen ähnliche Clients ansonsten gleichzeitig online sein können, was zu Nebenwirkungen führen kann. Ein Beispiel ist ein Benutzer mit einem Desktop-Rechner am Arbeitsplatz und zu Hause, wo die eingehenden Anrufe nur von einem der Clients empfangen würden, je nachdem, welche SIP-Registrierung aktiv ist.

Die erzwungene Abmeldung basiert auf SIP. Der Client sendet ein SIP SUBSCRIBE an das *Call-Info-Ereignispaket* mit einem speziellen *appid-Wert* im *From-Header* , unabhängig vom Wert des *Parameters bsoft-call-Info* . Wenn Cisco BroadWorks erkennt, dass mehrere Clientinstanzen mit derselben *Anwendungsanwendung* online sind, sendet es eine spezielle SIP NOTIFY an die ältere Clientinstanz, wodurch diese sich abmeldet. Desktopclients hätten z. B. einen identischen *appid-Wert* , obwohl es keine Einschränkung für die Verwendung dieses Bezeichners auf der Clientseite gibt. Der *appid-Wert* wird vom Serviceanbieter konfiguriert.

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

Weitere Informationen zu den für dieses Feature erforderlichen Cisco BroadWorks-Patches und -Versionen finden Sie im Abschnitt zu den Anforderungen an die Cisco BroadWorks-Software im *Lösungshandbuch* Webex für Cisco BroadWorks.

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

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_FORCED_LOGOUT_WXT%	false	true, false	Aktiviert die erzwungene Abmeldung.
%FORCED_LOGOUT_APPID_WXT%	leer	Zeichenfolge	Appid, die serverseitig für die Korrelation verwendet wird. Dies kann eine beliebige Zeichenfolge sein. Beispiel: "123abc"

Vertrauliche Informationen von Cisco

6.2.2 Anrufübernahme

Die Anrufübernahme ist ein Mehrbenutzerdienst, mit dem ausgewählte Benutzer jede läutende Leitung innerhalb ihrer Anrufübernahmegruppe annehmen können. Eine Anrufübernahmegruppe wird vom Administrator definiert und ist eine Untergruppe der Benutzer in der Gruppe, die die Anrufe der anderen Benutzer annehmen können.

Die folgenden Pickup-Fälle werden unterstützt:

- Blinde Anrufübernahme
- Gezielte Anrufübernahme (die es einem Benutzer ermöglicht, einen an ein anderes Telefon in seiner Gruppe gerichteten Anruf anzunehmen, indem er den entsprechenden Funktionszugriffscode und anschließend die Durchwahl des läutenden Telefons wählt).

```
<Konfiguration>
<Services><Anrufe>
<call-pickup blind="%ENABLE_CALL_PICKUP_BLIND_WXT%"
directed="%ENABLE_CALL_PICKUP_DIRECTED_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	true, false	Legen Sie "true" fest, um die blinde Anrufübernahme zu aktivieren.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	true, false	Legen Sie "true" fest, um die gezielte Anrufübernahme zu aktivieren.

6.2.3 Boss-Admin (Executive-Assistant) Support

Mit der Funktion "Chef-Administrator", die in Cisco BroadWorks als "Assistent der Geschäftsführung" bezeichnet wird, kann ein Assistent im Auftrag einer Führungskraft Anrufe als "Führungskraft" prüfen, annehmen und tätigen. Ein Assistent kann aus vielen Führungskräften bestehen, und es ist möglich:

- Wählen Sie beim Tätigen eines Anrufs die gewünschte Rolle aus.
- Sie nehmen einen eingehenden Anruf im Auftrag einer Führungskraft entgegen und leiten Sie den Anruf dann an die Führungskraft weiter. Darüber hinaus stehen alle gängigen Anrufverwaltungsoptionen zur Verfügung.
- Vergewissern Sie sich, dass ein eingehender Anruf eigentlich für die Führungskraft bestimmt ist.

"Executive" und "Executive-Assistant" sind zwei miteinander verbundene Cisco BroadWorks Services, die zusammen die folgenden Funktionen bieten:

- Ein Benutzer mit dem Executive-Service kann einen Pool von Assistenten definieren, die seine Anrufe verwalten. Die Assistenten müssen unter den Benutzern in derselben Gruppe oder demselben Unternehmen ausgewählt werden, denen der Executive-Assistant-Dienst zugewiesen ist.
- Ein Benutzer mit dem Executive-Assistant-Dienst kann Anrufe im Namen seiner Führungskräfte entgegennehmen und einleiten.

Vertrauliche Informationen von Cisco

- Sowohl die Führungskraft als auch ihre Assistenten können festlegen, welche Anrufe an die Assistenten weitergeleitet werden sollen, wie Assistenten über eingehende Anrufe informiert werden sollen und welche der an die Assistenten weitergeleiteten Anrufe der Führungskraft zur Überprüfung vorgelegt werden sollen.

```
<Konfiguration>
<Dienstleistungen>
<Executive-assistant enabled="%ENABLE_EXECUTIVE_ASSISTANT_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	true, false	Setze auf "true", um die Boss-Admin-Funktion zu aktivieren.

HINWEIS: Die Funktion Boss-Admin (Executive-Assistant) Support ist nicht in Kombination mit Shared-Lines verfügbar.

6.2.4 SIP-Anrufe an Meeting eskalieren (nur Webex Calling)

Der Client stellt die Funktionalität bereit, einen laufenden SIP-Anruf über Webex Calling an ein Meeting zu eskalieren. Wenn diese Funktion anstelle einer Standard-Ad-hoc-Konferenz verwendet wird, kann der Benutzer während der Konferenz sowohl die Videokomponente als auch die Bildschirmfreigabe nutzen.

```
<Konfiguration>
<Services><Anrufe>
       <eskalieren-zum-WebEx-Meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	true, false	Legen Sie diesen Wert auf "true" fest, um die Menüoption "An Webex Konferenz eskalieren" zu aktivieren.

6.2.5 Anrufsteuerung – Automatische Anrufannahme

Die automatische Anrufannahme ermöglicht dem Benutzer, die Tischtelefonsteuerung (Desk Phone Control, DPC) für ausgehende Anrufe auf dem Client zu verwenden, um MPP-Telefone mit Zero-Touch-Anrufannahme zu verwalten.

Das ausgewählte MPP-Telefon überträgt die Audio-/Videoübertragung für den ausgehenden DPC-Anruf.

Vertrauliche Informationen von Cisco

Die automatische Beantwortung funktioniert auf primären und nicht primär bereitgestellten Geräten. Wenn der Benutzer über mehr als ein registriertes Telefon verfügt, das gekoppelt werden kann, wird der Anruf automatisch nur von dem ausgewählten/gekoppelten Gerät angenommen.

```
<Konfiguration>
<Services><Anrufe>
<deskphone-control auto-answer="%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	true	true, false	Wenn diese Einstellung auf "true" festgelegt ist, wird die automatische Anrufannahme aktiviert.

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

6.2.6 Automatische Antwort mit Tonbenachrichtigung

Diese Funktion aktiviert die automatische Unterstützung der Annahme eingehender Anrufe für lokale Geräte, wenn dies in der eingehenden Anrufanforderung angegeben ist.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_AUTO_ANSWER_WXT%	false	true, false	Wenn diese Einstellung auf "true" gesetzt ist, wird die automatische Annahme eingehender Anrufe aktiviert, wenn dies vom Backend angefordert wird.

6.2.7 Steuerung des Tischtelefons – Steuerung während eines Anrufs – Konferenz

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	true, false	Bei Einstellung "true" werden Konferenz- und Zusammenführungsoptionen für Remoteanrufe (XSI) aktiviert, die an einem anderen Standort beendet werden.

Vertrauliche Informationen von Cisco

6.2.8 Benachrichtigungen zur Anrufübernahme

Anrufübernahmebenachrichtigungen ermöglichen dem Benutzer zu erkennen, wenn ein Anruf bei einem Benutzer eingeht, den er überwachen soll. Anrufübernahmebenachrichtigungen können für Watchlists empfangen werden, die über die Anrufübernahmegruppe und die Besetztlampenfeld-Dienste konfiguriert wurden.

Benachrichtigungen zur Anrufübernahme sind nützlich, wenn sich die überwachten Benutzer nicht in unmittelbarer Nähe zueinander 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 der Überwachungsliste für Besetztlampenfeld (BLF) einen eingehenden Anruf im Status "Warnung" hat. Die Benachrichtigung enthält Informationen über den Anrufer und den Benutzer, der den eingehenden Anruf erhalten hat. Sie können den Anruf annehmen, stummschalten oder ignorieren. Durch die Beantwortung eines eingehenden Anrufs durch den Benutzer wird die direkte Anrufübernahme initialisiert.

Ab Version 43.4 ist die Liste der von der BLF-Funktion überwachten Benutzer im Fenster für Anrufe (Multi Call Window, MCW) für Anrufe verfügbar (nur für Windows verfügbar). Die Integration der BLF-Liste in das MCW umfasst:

- Überwachen Sie eingehende Anrufe mit der Option, den Anruf anzunehmen oder die Warnung zu ignorieren.
- Hier finden Sie die vollständige Liste der BLF Benutzer.
- Überwachen Sie die Anwesenheit der Benutzer – Rich Presence ist nur für Benutzer mit Webex Cloud-Berechtigung verfügbar. Die Standardpräsenz (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.

```
<Konfiguration>
  <Dienstleistungen>
    <Anrufe>
      <busy-lamp-field enabled="%ENABLE_BUSY_LAMP_FIELD_WXT%">
        <display-caller enabled="%ENABLE_BLF_DISPLAY_CALLER_WXT%"/>
        <notification-delay time="%BLF_NOTIFICATION_DELAY_TIME_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	true, false	Aktiviert die Überwachung des Besetztlampenfelds und die Benachrichtigung über das Klingeln für andere Benutzer, die Anrufe annehmen können.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_BLF_DISPLAY_CALLER_WXT%	true	true, false	Ermöglicht die Anzeige des Anzeigenamens bzw. der Nummer des Anrufers in der Benachrichtigung über den Anruf.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Steuert, wie viele Sekunden die Benachrichtigung verzögert werden soll, 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 Webex Anwendung ab der Webex Calling Bereitstellung Unterstützung für GCP-Benachrichtigungen (Group Call Pickup). Damit können Benutzer über eingehende Anrufe für alle Benutzer benachrichtigt werden, die über die Anrufübernahmegruppe überwacht werden.

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

Wenn sich innerhalb derselben Anrufübernahmegruppe mehrere Anrufe befinden, werden diese basierend auf der Zeit, zu der sie eingehen, sequenziell verarbeitet. Die Benachrichtigung über den ältesten Anruf wird zuerst an die Gruppe zugestellt, und sobald sie verarbeitet wurde, wird die nächste Benachrichtigung in der Leitung an die Gruppe zugestellt.

Benachrichtigungen können je nach Konfiguration im Control Hub-Verwaltungsportal nur Audio, nur visuell oder akustisch und visuell sein. Wenn eine visuelle GCP-Benachrichtigung angezeigt wird, kann der Benutzer den Anruf mit der Anrufübernahmefunktion annehmen. Wenn nur die Audiobenachrichtigung konfiguriert ist, wird dem Benutzer keine visuelle Benachrichtigung für den eingehenden Anruf angezeigt, er hört einen bestimmten Klingelton und kann den Anruf über das in der Webex-App verfügbare Menü für die Anrufübernahme oder durch manuelles Wählen des FAC-Codes (*98) und des Anschlusses annehmen.

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

Die Funktion funktioniert sowohl für die Hauptleitungen als auch für gemeinsam genutzte oder virtuelle Leitungen, die dem Benutzer zugewiesen sind.

Vertrauliche Informationen von Cisco

```
<Konfiguration>
<Services><Anrufe>
    <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%"/>
    <-/Gruppenanruf-Pickup-Benachrichtigungen>
...
<Protokolle><sip>
    <Zeilen>
        <Zeile>
            <Gruppenanrufübernahme>%BWGROUP-ANRUFÜBERNAHME-BOOL-
1%</Gruppenanrufübernahme>
            ...
        </Leitung>
        <Zeile>
            <gruppenanrufübernahme>%BWGROUP-ANRUFÜBERNAHME-BOOL-
2%</gruppenanrufübernahme>
            ...
        </Leitung>
        ...
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	true, false	Aktiviert die Benachrichtigungen für Gruppenanrufübernahme
%ENABLE_GCP_DISPLAY_CALLER_WXT%	true	true, false	Ermöglicht die Anzeige des Anzeigenamens bzw. der Nummer des Anrufers in der Klingelbenachrichtigung
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5-120	Definiert die maximale Zeit, für die eine GCP-Benachrichtigung für den Benutzer verfügbar ist
%BWGROUP-CALL-PICKUP-BOOL-n%	false	true, false	Gibt an, ob für die entsprechende Leitung eine Anrufübernahmegruppe konfiguriert ist

HINWEIS 1: Dies ist eine Webex Calling einzige Funktion.

HINWEIS 2: Diese Funktion hängt von der Anrufübernahmegruppe ab, die für den Benutzer konfiguriert wird.

6.2.9 Ereignispaket für die Fernsteuerung

Bei Click-to-Dial-Clients wie dem Thin Client "BroadWorks Receptionist" und dem Go-Integrator, bei denen die Webex-App das anrufende Gerät ist, berücksichtigt die Webex-App jetzt das Ereignispaket für die Fernsteuerung, wenn sie einen Anruf erhält oder "Halten/Fortsetzen" verarbeitet.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false	True, false	Gibt an, dass die Fernbedienung für den Benutzer aktiviert sein soll.

6.2.10 Anrufwarteschlangen-Agenten-CLID-Auswahl

Wenn Agenten ihre Kunden anrufen, möchten sie, dass den Kunden die entsprechende Rufleitungs-ID (CLID) angezeigt wird und nicht ihre persönliche/firmeneigene CLID. Wenn z. B. die Agentin Mary Smith in die Anrufwarteschlange des technischen Supports eingereiht wird, möchte Mary beim Anrufen von Kunden, dass ihre CLID den Kunden als technischer Support und nicht als Mary Smith angezeigt wird.

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_Center_AGENT_OUTGOING_CALLS_WXT%	false	True, false	Ermöglicht ausgehende Anrufe (CLID-Auswahl) für die Callcenter-Warteschlange.

6.2.11 Gateway zur Überlebensfähigkeit (nur Webex Calling)

Ab Version 43.2 unterstützt Webex Anwendung den Survivability-Anrufmodus. Wenn die Funktion aktiviert ist und keine Webex Cloud-Konnektivität besteht, kann die Webex-Anwendung im Survivability-Modus ausgeführt werden. In diesem Modus stehen dem Benutzer eingeschränkte Anruffunktionen zur Verfügung.

Das lokale Survivability Gateway wird vom Kunden bereitgestellt.

```
<Konfiguration>
<Protokolle>
<Schluck>
<survivability-Gateway enabled="%ENABLE_SURVIVABILITY_GATEWAY_WXT%" fallback-
time="%SURVIVABILITY_FALLBACK_TIME_WXT%">%BWSURVIVABILITYGATEWAY%</survivability-
Gateway>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	true, false	Aktiviert die Unterstützung für den Survivability-Modus.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Gibt die Fallback-Zeit an (Survivability-Gateway zu SSE)

HINWEIS: Diese Funktion bietet Vertrauen bei der Migration von On-Premises- zu Cloud-Anruflösungen.

6.2.12 Ereignispaket für die Remote-Stummschaltung (nur Webex Calling)

Ab Version 43.9 bietet die App Webex Unterstützung für die Remote-Stummschaltung des Audio-Medienstreams. Auf diese Weise kann die Stummschaltung eines laufenden Anrufs von einem anderen Ort aus ausgelöst werden, z. B. vom Thin Client BroadWorks Receptionist, wo die Webex App das anrufende Gerät ist.

Die Funktion hängt vom neuen SIP *x-cisco-mute-Status* Info-Paket ab. Wenn der *Recv-Info:x-cisco-mute-Status-Header* während des Einrichtens der SIP INVITE-Sitzung empfangen wird, sendet die App von Webex bei jeder Aktualisierung (lokal oder remote) des Stummschaltungsstatus der Audioanrufsitzung SIP INFO mit dem *Info-Paket:x-cisco-mute-Status zurück. muted=true* (oder *muted=false*), wobei der Parameter "Muted" den aktualisierten Status des Audiomedienstreams darstellt.

Die Stummschaltung bzw. Stummschaltung kann lokal oder von einem Remotestandort aus ausgelöst werden. Das Remoteupdate löst eine SIP NOTIFY mit *dem Ereignis: stumm* (oder *Stummschaltung* auf) aus, die vom Anwendungsserver an die Webex App gesendet wird. Die Webex-App berücksichtigt die Remoteanforderung und sendet nach der Aktualisierung des Status des Audiomedienstreams eine SIP NOTIFY mit dem *Info-Package zurück: x-cisco-mute-Status. muted=true* (oder *muted=false*).

```
<Konfiguration>
<Dienstleistungen>
   <Anrufe>
       <Remote-mute-control enabled="%ENABLE_REMOTE_MUTE_CONTROL_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false	True, false	Wenn dieser Wert auf "true" festgelegt ist, ist die Remote-Anrufsteuerung für die Stummschaltung für den Benutzer aktiviert.

Vertrauliche Informationen von Cisco

6.2.13 Anruf verschieben

Webex App ermöglicht die Anrufüberwachung und Anrufsteuerung VoIP Anrufe, die an einem anderen Standort beendet wurden. Diese Option ist derzeit nur für die Hauptleitung des Benutzers verfügbar.

Ab Version 43.12 wurde die Webex-App erweitert, um Anrufe anzuzeigen, die an einem anderen Standort auch für die gemeinsam genutzten und virtuellen Leitungen beendet wurden. Diese Anrufe sind im Bereich für laufende Anrufe zu Informationszwecken und ohne die Möglichkeit, sie zu steuern, sichtbar. Nur wenn ein solcher Anruf gehalten wird, kann der Benutzer ihn auf das lokale Gerät umlegen, indem er ihn auswählt und auf dem Anrufbildschirm fortsetzt. Dieser Mechanismus ist nützlich, wenn der Anruf von demselben Benutzer an einem anderen Standort oder von einem anderen Benutzer auf derselben Leitung bearbeitet wurde.

Beachten Sie, dass die Webex App einen gehaltenen Anruf nicht auf ein gekoppeltes Gerät umlegen kann. Wenn der Benutzer mit einem Gerät gekoppelt ist, muss er zunächst die Verbindung trennen, bevor er den gehaltenen Anruf lokal fortsetzen kann.

Die Anrufüberwachung für gemeinsam genutzte und virtuelle Leitungen hängt vom SIP-Anrufinfo-Ereignispaket ab.

Die Überwachung der Anrufe für die Hauptleitung des Benutzers hängt von den XSI-Ereignissen (Advanced Call Event Package ab) ab, und das Verschieben eines Anrufs auf das lokale Gerät ist für diese Anrufe nicht möglich. Für diese Art von Anrufen kann der Benutzer die Funktion "Call Pull" (*6.1.22 Anruf pull*) verwenden. "Call Pull" funktioniert nur für die letzten aktiven Anrufe des Benutzers, während der Mechanismus für gemeinsam genutzte und virtuelle Leitungen für alle Anrufe des Benutzers funktioniert, die in die Warteschleife gestellt werden.

- Anwendungsfall 1:
    a. Alice hat Bobs Leitung für die Desktop- und Tischtelefonprofile zugewiesen.
    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 auf dem Tischtelefon – der Anruf kann von Alice in der Desktop-App fortgesetzt werden.
- Anwendungsfall 2:
    a. Alice hat Bobs Leitung für die Desktop- und Tischtelefonprofile zugewiesen.
    b. Bob hat ein Telefonat mit Charlie – Alice kann den laufenden Anruf in der Desktop-App sehen.
    c. Bob platziert den Anruf mit Charlie in der Warteschleife – Alice kann den Anruf mit Charlie in der Desktop-App fortsetzen.
- Anwendungsfall 3:
    a. Alice hat Bobs Leitung für die Desktop- und Tischtelefonprofile zugewiesen.
    b. Alice wird über die Desktop-App mit seinem Telefon gekoppelt.
    c. Bob hat ein Telefonat mit Charlie – Alice kann den laufenden Anruf in der Desktop-App sehen.
    d. Bob platziert den Anruf mit Charlie in der Warteschleife – Alice kann den Anruf mit Charlie nicht über die Desktop-App fortsetzen.

Vertrauliche Informationen von Cisco

e. Alice trennt die Verbindung zwischen der Desktop-App und dem Tischtelefon – Alice kann den Anruf mit Charlie über die Desktop-App fortsetzen.

```
<Konfiguration>
<Services><Anrufe>
    <Anruf verschieben>
         <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALL_MOVE_HERE_WXT%	false	True, false	Aktiviert das Umleiten von Anrufen auf dem lokalen Gerät. Wird für das Halten/Fortsetzen an verschiedenen Standorten/Benutzern im Anwendungsfall mit mehreren Leitungen verwendet.

Vertrauliche Informationen von Cisco

6.3 Mobile Only-Funktionen

6.3.1 Notruf

Webex für Cisco BroadWorks unterstützt systemeigene Notrufe.

Wenn die Funktion aktiviert ist und ein ausgehender VoIP Anruf eingeleitet wird, analysiert die Anwendung die gewählte Rufnummer und vergleicht sie mit der Liste der konfigurierten Notrufnummern. Wenn die Nummer als Notrufnummer erkannt wird, führt die Anwendung das konfigurierte Wählverhalten aus. Sie kann mithilfe des Wählzeichen-Tags konfiguriert werden.

Folgende Modi werden unterstützt:

- cs-only – Der Client tätigt Notrufe nur über das Mobilfunknetz, wenn das Netzwerk verfügbar ist.
- cs-first – Bei der Einleitung eines Notrufs überprüft der Client den Netzwerktyp, mit dem das aktuelle Gerät verbunden ist. Wenn das Mobilfunknetz verfügbar ist, tätigt der Client den Anruf über das Mobilnetz. Wenn das Mobilfunknetz nicht verfügbar ist, aber ein mobiles Daten-/WLAN-Netzwerk verfügbar ist, tätigt der Client den Anruf über das Daten-/WLAN-Netzwerk als VoIP Anruf. Wenn der Notruf über das Mobilfunknetz getätigt wird, schlägt der Client dem Benutzer vor, den Notruf erneut zu tätigen, da VoIP.
- Nur VoIP – Der Client tätigt Notrufe nur VoIP, wenn das Mobilfunkdaten-/WLAN-Netzwerk verfügbar ist.
- cs-voip – Der Client analysiert, ob das Gerät ihn als systemeigenen CS-Anruf (Circuit-Switched) 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 Notrufnummer (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) "Nur cs".

Bei der Anmeldung wird eine Meldung zum Haftungsausschluss für Notrufe angezeigt. Sie wird nicht über die Konfigurationsoptionen gesteuert.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_EMERGENCY_DIALING_WXT%	false	true, false	Legen Sie "true" fest, um die Erkennung von Notrufen zu aktivieren. Der Standardwert ist leer.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	Nur CS	cs-only,cs-first,voip-only,cs-voip	Steuert den Wählreihenfolgemodus für Notrufe.

Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	CSV Liste	CSV Liste der Notrufnummern Beispiel: 911.112

6.3.2 Push-Benachrichtigungen für Anrufe

Wenn ein Anruf eingeht, erhält der mobile Client zuerst eine Push-Benachrichtigung (PN). Es gibt einen Konfigurationsparameter, mit dem gesteuert werden kann, wann die SIP REGISTER-Sitzung eingerichtet wird:

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 wird jedoch eine gewisse Verzögerung hinzugefügt, bevor der Anruf hergestellt wird.

Gemäß den Anforderungen von iOS 13 sollten die VoIP PNs nur für eingehende Anrufe verwendet werden. Für die übrigen anrufbezogenen Ereignisse sollten normale PNs verwendet werden.

Um diese Anforderung zu erfüllen, wird eine neue PN-Registrierung API eingeführt, die das entsprechende Patch auf dem Anwendungsserver erfordert. Wenn das Backend nicht für die Unterstützung der iOS 13 PNs konfiguriert ist, kann der Konfigurationsparameter verwendet werden, um die Verwendung der Legacy-Pushbenachrichtigungen zu erzwingen, bei denen alle anrufbezogenen Ereignisse über VoIP PNs übermittelt werden.

Es wird eine Push-Benachrichtigung vom Anwendungsserver (Application Server, AS) gesendet, wenn ein läutender Anruf vom Angerufenen an einem anderen Standort angenommen, vom Anrufer geschlossen oder beispielsweise an das Voicemail-System umgeleitet wird. Mit iOS 13 ist diese Art von Push-Benachrichtigung jetzt eine reguläre und hat einige Einschränkungen. Es kann durch den Apple Push Notification Service (APNS) verzögert oder sogar gar nicht zugestellt werden. Um fehlende oder verzögerte Anrufaktualisierungs-PNs zu behandeln, wird ein konfigurierbares Klingelzeitlimit hinzugefügt, um die maximale Klingelzeit zu steuern. Wenn die maximale Rufzeichenzeit erreicht ist, wird das Klingeln für den Angerufenen angehalten, und der Anruf wird als verpasst behandelt. Auf der Anruferseite kann der Anruf im Klingelstatus verbleiben, bis die auf dem Anwendungsserver (AS) konfigurierte Richtlinie für das Klingeln ohne Antwort ausgeführt wird.

Um das Anwendungsverhalten konsistent zu halten, gilt der konfigurierbare Klingelzeitgeber sowohl für Android als auch für iOS.

Vertrauliche Informationen von Cisco

Eine separate Konfigurationsoption wird hinzugefügt, um das Verhalten der Anrufablehnung festzulegen, wenn ein eingehender Anruf als Push-Benachrichtigung empfangen wird. Der Client kann so konfiguriert werden, dass er den Anruf ignoriert oder dem Server über Xsi antwortet, wobei die Ablehnung auf "true" oder "false" festgelegt ist. In diesem Fall werden die zugewiesenen Cisco BroadWorks-Anrufbehandlungsservices angewendet. Wenn "decline_false" konfiguriert ist, wird der Rufton fortgesetzt, bis der Gesprächspartner den Anruf abbricht oder der Timer für unbeantwortete Anrufe abläuft und die zugehörigen Anrufbehandlungsservices starten. Wenn "decline_true" konfiguriert ist, gibt der Grund für die Ablehnung die Anrufverarbeitung an. Wenn der Grund für die Ablehnung auf "ausgelastet" festgelegt ist, erzwingt der Server sofort den ausgelasteten Behandlungsservice. Wenn "temp_unavailable" konfiguriert ist, wird der vorübergehend nicht verfügbare Behandlungsservice angewendet.

```
<Konfiguration>
<Dienstleistungen>
    <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%"/>
    <Anrufe>
        <reject-with-xsi mode="%REJECT_WITH_XSI_MODE_WXT%"
        declineReason="%REJECT_WITH_XSI_DECLINE_REASON_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	true, false	Steuert, wann die SIP REGISTRSITER-Sitzung aufgebaut wird – beim Empfang einer Push-Benachrichtigung für eingehenden Anruf oder bei deren Annahme.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Steuert die maximale Klingelzeit für eingehende Anrufe, die über PN eingehen. Wenn innerhalb des angegebenen Zeitraums keine CallUpd-PN eingeht, wird der Anruf als verpasst behandelt.
%REJECT_WITH_XSI_MODE_WXT%	decline_false	Ignorieren, decline_true, decline_false	Legt das Verhalten der Anrufzurückweisung fest.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	Besetzt	beschäftigt, temp_unavailable	Gibt den Grund für die Zurückweisung des Anrufs an, wenn der Ablehnungsmodus auf "decline_true" eingestellt ist.

6.3.2.1 MWI

Wenn die Funktion "MWI" aktiviert ist, abonniert der Mobile Webex-Client die MWI Push-Benachrichtigung, um Updates 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. Beispielsweise hört der Benutzer Voicemail-Nachrichten ab oder markiert sie innerhalb des Mobile Webex-Clients als gelesen (die Anzahl der ungelesenen Nachrichten nimmt ab). Es gibt keine konfigurierbare Option, um dies zu steuern.

Vertrauliche Informationen von Cisco

Weitere Informationen zu MWI finden Sie im Abschnitt *6.1.27 Voicemail, visuelle Voicemail, Nachrichtenanzeige*.

6.3.2.2 Ring Splash

BroadWorks-Dienste (z. B. "Ruhe") können Ruftonerinnerungen senden, wenn eingehende Anrufe umgeleitet werden. Der Webex Mobile-Client kann so konfiguriert werden, dass er die Ring Splash-Push-Benachrichtigungen aktiviert und sie dem Benutzer anzeigt, wenn sie von BroadWorks ausgelöst werden.

```
Konfiguration>
<Dienstleistungen>
<ring-splash enabled="%ENABLE_RING_SPLASH_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_RING_SPLASH_WXT%	false	true, false	Aktiviert Ring Splash in der BroadWorks-Konfiguration.

6.3.2.3 Liefermodus (nur Webex Calling)

Die Webex-App verwendet den Benachrichtigungs-Push-Server (Notification Push Server, NPS), um die Pushbenachrichtigungen für Anrufe an APNS/FCM zu übermitteln. Version 45.2 der Webex-App unterstützt jetzt drei verschiedene Übermittlungsmodi, um zu konfigurieren, wie die anrufbezogenen Push-Benachrichtigungen an APNS/FCM übermittelt werden sollen:

- NPS – aktueller Mechanismus, der den NPS verwendet
- Cloud: Erweiterter Mechanismus mit Cisco Webex Cloud-Microservice
- Extern – ein Mechanismus, der Systeme eines Drittanbieters verwendet. Hierfür ist die Integration des Drittanbietersystems mit der Cisco WebHooks-Engine erforderlich

```
<Konfiguration>
<Services><Anrufe>
<push-notifications-for-calls enabled="true"
      Connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
      ring-Timeout-seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"
      delivery-mode="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	NPS	NPS, Cloud, Extern	Legt den Zustellungsmodus der Push-Benachrichtigungen für Anrufe fest.

Vertrauliche Informationen von Cisco

6.3.3 Einzelne Benachrichtigungen

Die Mobile Single Alert-Funktion ist für FMC-Bereitstellungen (Fixed-Mobile Convergence) / Mobile Network Operator (MNO) gedacht, die den BroadWorks Mobility-Service nutzen. Ohne sie erhält der Benutzer, wenn er beim Webex-Client angemeldet ist und einen eingehenden Anruf erhält, gleichzeitig zwei Anrufe – einen nativen Anruf und einen Push-Benachrichtigungsanruf (VoIP). Wenn die Funktion aktiviert ist, deaktiviert die Anwendung die Mobilitätswarnungen am BroadWorks Mobility-Standort des Benutzers, wenn er sich anmeldet, und aktiviert die Warnungen, wenn er sich abmeldet. Eine wichtige Voraussetzung für die Verwendung dieser Funktion ist, dass dem Benutzer der BroadWorks Mobility-Dienst zugewiesen und genau ein Standort konfiguriert ist.

```
<Konfiguration>
<Services><Anrufe>
<single-alerting enabled="%ENABLE_SINGLE_ALERTING_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_SINGLE_ALERTING_WXT%	false	True, false	Legen Sie den Wert auf "true" fest, um die Einzelbenachrichtigung zu aktivieren .

6.3.4 Klicken zum Wählen (Rückruf)

Die ausgehende Click-to-Dial-Funktion stellt sicher, dass der Endbenutzer einen Anruf auf seinem persönlichen Leitungsvermittelten Mobiltelefon durchführen und seine geschäftliche DN als Anrufleitungs-ID übermitteln kann.

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

Wenn die Funktion aktiviert ist, können Benutzer den SNR Standort im Menü "Gerätekopplung" auswählen. Bei Kopplung mit SNR Standort werden alle ausgehenden Anrufe mit Click-to-Dial (Rückruf) eingeleitet. Um doppelte Benachrichtigungen zu vermeiden, sind die Push-Benachrichtigungen für eingehende Anrufe deaktiviert.

Wenn ein Benutzer einen Anruf mit nur einem Mausklick tätigt, wird der Bildschirm für ausgehende Anrufe mit Informationen über den erwarteten eingehenden Anruf am ausgewählten SNR Ort angezeigt. Dieser Bildschirm wird basierend auf einem konfigurierbaren Timer automatisch geschlossen.

Beim Trennen der Verbindung zu einem SNR Standort registriert sich die Anwendung erneut für Push-Benachrichtigungen für eingehende Anrufe.

```
<Konfiguration>
<Dienstleistungen>
  <Wählvorgang>
    <call-back enabled="%ENABLE_DIALING_CALL_BACK_WXT%"
timer="%DIALING_CALL_BACK_TIMER_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_DIALING_CALL_BACK_WXT%	false	True, false	Legen Sie "true" fest, um Click-to-Dial (Rückruf-) Anrufe zu ermöglichen .
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Steuert die Anzahl der Sekunden, bevor der Rückrufbildschirm automatisch geschlossen wird.

6.3.5 MNO-Unterstützung

6.3.5.1 Anruf mit systemeigenem Dialer

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

Die Fähigkeit des Benutzers, Anrufe über das native Dialer zu initiieren, wird durch das **native** Konfigurationstag gesteuert. Wenn aktiviert, startet die Anwendung das systemeigene Wählprogramm und tätigt den Anruf. Darüber hinaus wird die Verfügbarkeit VoIP Anrufe durch das **VoIP-Tag** gesteuert – basierend auf den Bereitstellungsanforderungen, VoIP Anrufe aktiviert oder deaktiviert werden können.

Wenn VoIP und native Anrufe aktiviert sind, kann der Benutzer auswählen, welche Option er verwenden möchte.

Mit dem Tag <Wählmodus> wird gesteuert, ob Benutzer auswählen können, wie eingehende und ausgehende Anrufe gestartet/angenommen werden. Erfordert, dass sowohl die systemeigene als auch die VoIP Anrufe aktiviert sind.

Ab Version 43.12 wurde die systemeigene Wählkonfiguration erweitert. Damit ist auch die Möglichkeit eines benutzerdefinierten Präfixes verfügbar, das der Nummer des ausgehenden Anrufs vorangestellt wird. Dies gilt nur für Mobilfunkanrufe, die über die Webex-App eingeleitet werden, wenn die gewählte Nummer mit einem FAC-Code beginnt.

Diese Funktion ist hilfreich für Kunden mit MNO-Bereitstellungen, bei denen Anrufe nicht an den integrierten Cisco BroadWorks Application Server weitergeleitet werden, sondern die FAC Codes vom Telecom-Backend verarbeitet werden können. Im Abschnitt <dialing><native> wird das neue <fac-prefix>-Tag hinzugefügt, mit dem die Telekommunikationsunternehmen dieses Problem beheben können.

```
<Konfiguration>
<Dienstleistungen>
  <Wählvorgang>
    <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%"/>
    </nativ>
    <dialing-mode enabled="%ENABLE_DIALING_MODE_WXT%" default="%DIALING_MODE_DEFAULT_WXT%"/>
```


Vertrauliche Informationen von Cisco

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_DIALING_VOIP_WXT%	true	true, false	Setzen Sie diesen Wert auf "true", um VoIP Anrufoption zu aktivieren.
%ENABLE_DIALING_NATIVE_WXT%	false	true, false	Legen Sie "true" fest, um die native Anrufoption zu aktivieren.
%ENABLE_DIALING_MODE_WXT%	false	True, false	Aktiviert die Auswahl des Anrufmodus durch den Benutzer über die Anrufeinstellungen in den Einstellungen.
%DIALING_MODE_DEFAULT_WXT%	VoIP	VoIP, NATIV	Gibt den ausgewählten Standardanrufmodus an.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false	true, false	Legt fest, ob die Verfügbarkeit der systemeigenen Anrufe davon abhängt, ob die BroadWorks Mobility-Servicezuweisung und der Mobilitätsstandort für den Benutzer konfiguriert sind.
%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 Mobilfunkanruf initiiert wird. Standardmäßig ist kein FAC Präfix definiert und der Tag ist leer.

HINWEIS 1: Mindestens ein VoIP- **und** nativer Anruf sollte aktiviert sein.

HINWEIS 2: Wenn nur das **native** Aufrufen aktiviert ist, wird in MNO-Bereitstellungen empfohlen, die Einzelbenachrichtigung zu deaktivieren, um zu verhindern, dass der Client die BWM-Benachrichtigung deaktiviert.

HINWEIS 3: Wenn sowohl native **als** auch **VoIP-Anrufe** aktiviert sind, wird in MNO-Bereitstellungen empfohlen, die Einzelalarmierung zu aktivieren, um doppelte Benachrichtigungen zu vermeiden.

6.3.5.2 Steuerelemente während eines Anrufs

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

- BroadWorks Mobility (BWM)-Dienst dem Benutzer zugewiesen ist,
- Es ist nur eine einzige BMW Mobile Identity konfiguriert,
- Der systemeigene Anrufmodus wird vom Benutzer ausgewählt (weitere Informationen finden Sie im Abschnitt). *6.3.5.1 Anruf mit systemeigenem Dialer*
- Es gibt einen Anruf, der auf BroadWorks verankert ist und über den BMW-Dienst läuft.
- Auf dem Mobilgerät wird ein Mobilanruf ausgeführt.

Vertrauliche Informationen von Cisco

Version 43.10 verbessert die Handhabung der Übergabe mit Rücksprache, indem eine Zuordnung zwischen den beiden in der App Webex dargestellten Mobilanrufen erstellt wird und dem Benutzer die Möglichkeit bietet, die Übergabe abzuschließen. Wenn der Benutzer zwei unabhängige Mobilfunkanrufe auf demselben Gerät hat, wird das Übergabemenü erweitert, um die Übergabe eines Anrufs an den anderen zu ermöglichen, auch wenn keine Verknüpfung zwischen ihnen erstellt wird.

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_XSI_CALL_CONTROL_WXT%	false	true, false	Aktiviert die XSI-Anrufsteuerung für die MNO-Umgebung.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Steuert den XSI-MNO-Bereitstellungstyp, der von der Anwendung verwendet wird. Folgende Werte sind möglich: ▪ MNO_Access – Zeigt alle Remote-Anrufe (XSI) mit den im folgenden Knoten definierten Gerätetypen an. ▪ MNO_Network – Zeigt alle Remote-Anrufe (XSI) an.
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	Zeichenfolge	Die Namen der Gerätetypen, die in MNO_Access Bereitstellungstyp verwendet werden sollten.
%ENABLE_XSI_HOLD_CALLS_WXT%	true	True, false	Legt fest, ob die Aktion "Anruf halten" für den Benutzer für mobile XSI-Anrufe verfügbar sein soll.

6.3.5.3 Ausgehende Anrufleitungsidentität (CLID) – Dual Persona

Ab Mobile Version 42.12 ermöglicht die Webex-App den Benutzern, ihre CLID (Calling Line Identity) auszuwählen, die dem Remote-Teilnehmer beim Einleiten eines ausgehenden Anrufs angezeigt wird.

Wenn der Benutzer mit Cisco BroadWorks Mobility konfiguriert ist, die für MNO-Bereitstellungen (Mobile Network Operator) typisch ist, und die systemeigene Anruffunktion aktiviert ist, kann der Benutzer auswählen, welche Identität den angerufenen Personen angezeigt wird. Der Benutzer kann seine geschäftliche oder persönliche Identität wählen. Es besteht auch die Möglichkeit, die eigene Identität zu verbergen und den Anruf als anonym darzustellen.

Vertrauliche Informationen von Cisco

Für VoIP Anrufe hat der Benutzer auch die Möglichkeit, seine CLID zu steuern. Die verfügbare Option besteht in diesem Fall nur darin, zu steuern, ob seine Identität verborgen werden soll oder nicht.

Persona-Management und CLID-Blockierung werden über separate Konfigurationsoptionen gesteuert.

```
<Konfiguration>
<Dienstleistungen>
<Wählvorgang>
   <calling-line-id-delivery-blocking
enabled="%ENABLE_CLID_DELIVERY_BLOCKING_WXT%"/>
   <mobility-persona-Management
enabled="%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	false	True, false	Aktiviert die Blockierung der Zustellung der ID der Rufleitung. Dies gilt für alle ausgehenden Anruftypen für den Benutzer.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	false	True, false	Aktiviert die persönliche Verwaltung für systemeigene Anrufe, wenn der Bereitstellungstyp als MNO_Access oder MNO_Network konfiguriert ist. (BroadWorks Mobility wird für die systemeigenen Anrufe verwendet, und alle systemeigenen Anrufe sind auf BroadWorks verankert.)

6.3.5.4 Benachrichtigung für systemeigene Anrufe

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	true	true, false	Aktiviert das Abonnement für die MOBILE_CALL_INFO Pushbenachrichtigung.

Vertrauliche Informationen von Cisco

6.3.5.5 Systemeigenen Anruf in konvergente Konferenz verschieben

Für Benutzer, die mit MNO bereitgestellt werden, ermöglicht diese Funktion, dass ein systemeigener Sprachanruf zu einer Konferenz für beide Teilnehmer eines 1:1-Anrufs eskaliert wird (auch wenn der andere Teilnehmer kein Webex-Benutzer ist). Wenn es sich bei dem Remote-Benutzer um einen Webex-Benutzer handelt, haben die Parteien in einer Besprechung folgende Möglichkeiten:

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

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	true, false	Aktiviert das Einschalten (Einladen und Meet, Video-Meet-Aktionen).

6.3.5.6 MNO-Mobilität – Widget für laufende Anrufe

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

- Halten/Fortsetzen
- Blinde/konsultative Übertragung – Platziert den Benutzer im Übertragungsdialog in der Webex-App.
- Übertragung abschließen – Bietet die Option zum Durchführen einer Übergabe mit Rücksprache (Version 43.10)
- Videokonferenz – verschiebt die Teilnehmer in ein Webex-Meeting.
- Anruf beenden

```
<Konfiguration>
<Services><Anrufe>
       <Halten 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%"/>
```


Vertrauliche Informationen von Cisco

```
        <escalate-to-webex-Meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%" Widget-
enabled="%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_WIDGET_HOLD_CALLS_WXT%	true	True, false	Steuert die Verfügbarkeit der Halten-Aktion im Anruf-Widget.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	true	True, false	Steuert die Verfügbarkeit der Aktionen "Übergeben" und "Übergabe abschließen" im Anruf-Widget.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	true	True, false	Steuert die Verfügbarkeit der Videokonferenzaktion im Anruf-Widget.

6.3.6 ID des eingehenden Anrufers

Version 44.2 bietet nun die Möglichkeit, die Kontaktinformationen, die dem Benutzer angezeigt werden, basierend auf dem Namen und der Nummer zu steuern. Es wurden zwei Konfigurationsoptionen hinzugefügt, um die Informationen zu steuern, die dem Benutzer im Bildschirm für eingehende Anrufe, in der Benachrichtigung über eingehende Anrufe angezeigt werden, und die Benachrichtigungen über entgangene Anrufe.

6.3.6.1 Bildschirm für eingehenden Anruf

Es gibt Plattformunterschiede zwischen Android und iOS, wenn es darum geht, Daten auf dem Bildschirm für eingehende Anrufe anzuzeigen. Die native Benutzeroberfläche zeigt Informationen für eingehende Anrufe wie folgt an:

Android – Der Bildschirm für eingehende Anrufe enthält zwei separate Felder, in denen sowohl der Name als auch die Nummer angezeigt werden.

iOS – es gibt nur ein Feld, um entweder den Namen oder die Nummer anzuzeigen – wenn beide verfügbar sind, hat der Name Vorrang

Die neue Konfigurationsoption für die eingehenden Anrufe kann verwendet werden, um sicherzustellen, dass die iOS Webex-App die Nummer im Anrufbildschirm neben dem Namen anzeigt (Format: *Name (Nummer)*). Das Verhalten von Android Webex-Apps ist davon nicht betroffen.

6.3.6.2 Benachrichtigung für eingehenden Anruf

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

Vertrauliche Informationen von Cisco

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, hängt die Webex App die Nummer neben den Namen an (Format: *Name (Nummer)*). Dieses Verhalten der Webex-App gilt sowohl für Android als auch für iOS.

6.3.6.3 Benachrichtigung über verpassten Anruf

Es wurde ein zusätzlicher Konfigurationsparameter für die Benachrichtigungen über verpasste Anrufe hinzugefügt. Darüber hinaus können die Informationen des Remote-Teilnehmers (ähnlich wie bei Benachrichtigungen über eingehende Anrufe) gesteuert werden. Die Nummer kann an den Anzeigenamen des Remote-Benutzers angehängt und in der Benachrichtigung über einen entgangenen Anruf angezeigt werden. Dieses Verhalten der Webex-App gilt sowohl für Android als auch für iOS.

```
<Konfiguration>
<Services><Anrufe>
   <Anrufer-ID>
      <Eingehende Anrufe>
         <append-number enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
      </eingehende Anrufe>
      <Verpasste Anrufe>
         <append-number enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
      </verpasste Anrufe>
```

Etikett	Standard, falls weggelassen	Unterstützte Werte	Beschreibung
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false	true, false	Legt fest, ob die Nummer im Bildschirm für eingehende Anrufe (nur iOS) und in Benachrichtigungen an den Namen angehängt wird.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	false	true, false	Legt fest, ob die Nummer an den Namen in der Benachrichtigung über den entgangenen Anruf angehängt wird.

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

Vertrauliche Informationen von Cisco

7 Funktionen von Early Field Trial (BETA)

Es gibt keine Funktionen in der BETA mit der neuesten Version.

Vertrauliche Informationen von Cisco

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

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

Webex für Cisco BroadWorks-Tag	Desktop-Legacy-Tag	Mobiles Legacy-Tag
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	-	%REJECT_WITH_XSI_MODE_MOBIL%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	-	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	-	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	-
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	-
%ENABLE_CALL_STATISTICS_WXT%	-	-
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	-	%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%MWI_MODE_WXT%	%DESKTOP_MWI_MODE%	%MWI_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	-	-
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	-
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	-
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	-
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	-	-
%ENABLE_BROADWORKS_ANYWHERE_WXT%	-	-

Vertrauliche Informationen von Cisco

Webex für Cisco BroadWorks-Tag	Desktop-Legacy-Tag	Mobiles Legacy-Tag
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	-	-
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	-	-
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	-	-
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	-	-
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	-	-
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	-	-
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	-	-
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	-	-
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	-	-
%ENABLE_EMERGENCY_DIALING_WXT%	-	-
%EMERGENCY_DIALING_NUMBERS_WXT%	-	-
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	-	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	-
%SBC_ADDRESS_WXT%	%SBC_ADDRESS%	%SBC_ADDRESS%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBIL%
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	-
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	-

Vertrauliche Informationen von Cisco

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

Vertrauliche Informationen von Cisco

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

Vertrauliche Informationen von Cisco

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

Vertrauliche Informationen von Cisco

Webex für Cisco BroadWorks-Tag	Desktop-Legacy-Tag	Mobiles Legacy-Tag
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	-	-
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	-	-
%USER_PORTAL_SETTINGS_URL_WXT%	-	-
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	-	-
%ENABLE_AUDIO_MARI_FEC_WXT%	-	-
%ENABLE_AUDIO_MARI_RTX_WXT%	-	-
%ENABLE_VIDEO_MARI_FEC_WXT%	-	-
%ENABLE_VIDEO_MARI_RTX_WXT%	-	-
%ENABLE_CALL_BLOCK_WXT%	-	-
%ENABLE_WIDGET_HOLD_CALLS_WXT%	-	-
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	-	-
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	-	-
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	-	-
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	-	-
%ENABLE_CALL_MOVE_HERE_WXT%	-	-
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	-	-
%DIALING_NATIVE_FAC_PREFIX_WXT%	-	-
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	-	-
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	-	-
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	-	-

Vertrauliche Informationen von Cisco

Webex für Cisco BroadWorks-Tag	Desktop-Legacy-Tag	Mobiles Legacy-Tag
%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_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	-
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	-
%BLF_NOTIFICATION_DELAY_TIME_WXT%	-	-
%ENABLE_GCP_NOTIFICATIONS_WXT%	-	-
%ENABLE_GCP_DISPLAY_CALLER_WXT%	-	-
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	-	-
%UDP_KEEPALIVE_ENABLED_WXT%	-	-
%TCP_KEEPALIVE_ENABLED_WXT%	-	-
%TLS_KEEPALIVE_ENABLED_WXT%	-	-
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	-	-
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	-	-

Vertrauliche Informationen von Cisco

HINWEIS: N/A zeigt an, dass kein entsprechender benutzerdefinierter Tag vorhanden ist, der die Funktion in UC-One steuert. Mit "N/A" für ältere Desktop- und Mobile-Tags wird angezeigt, dass der Webex für das Cisco BroadWorks-Tag neu ist und entweder eine neue Funktion oder eine vorhandene Funktion steuert, die nicht durch ein benutzerdefiniertes Tag in UC-One gesteuert wurde.

Vertrauliche Informationen von Cisco

9 Anhang A: TLS Chiffren

Der Webex für den BroadWorks-Client verwendet CiscoSSL, das auf OpenSSL basiert und über zusätzliche Sicherheitshärtung verfügt.

Vertrauliche Informationen von Cisco

10 Anhang B: DM-Tag-Bereitstellungsskript

Die Anzahl der benutzerdefinierten DM-Tags hat sich mit jedem Release erhöht, da viele Kunden Tags für die neuen Konfigurationsparameter bevorzugen. Um Mechanismen für eine einfachere Bereitstellung dieser benutzerdefinierten DM-Tags bereitzustellen, enthält dieser Abschnitt ein Skript, das auf der Seite des Anwendungsservers (Application Server, AS) ausgeführt werden kann, um den benutzerdefinierten DM-Tags Werte zuzuweisen. Dieses Skript ist speziell für neue Bereitstellungen vorgesehen, in 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 auffüllen). Beachten Sie, dass das folgende Beispiel für Mobilgeräte gilt. Verwenden Sie für den Desktop das BroadTouch_tags-Tag-Set anstelle von Connect_Tags. Verwenden Sie für Tablets das ConnectTablet_Tags-Tag-Set anstelle von Connect_Tags.

```
%% ********************************** Connect_Tags – Datei lesen **********************************
%%
%% Anleitung:
%% ------------------
%% – Diese Lesedatei kann verwendet werden, um Webex für BroadWorks zu erstellen,
hinzuzufügen und festzulegen
Benutzerdefinierte %%-Client-Tags
%% – Verwenden Sie %%, um alle Schritte zu kommentieren, die basierend auf den
Bereitstellungsspezifischen nicht erforderlich sind.
%% Serviceanforderungen:
%% Schritt 1 -- nur für neue Bereitstellungen eine anfängliche Tag-Set-Beschriftung erstellen
%% Schritt 2 -- Hinzufügen eines neuen benutzerdefinierten Tags (für jedes neue Tag ist ein Eintrag
erforderlich)
%% Schritt 3 -- Wert für ein vorhandenes benutzerdefiniertes Tag festlegen (Eingabe für jeden
zutreffenden Tag erforderlich)
%% Schritt 4 -- Tag-Einstellungen anzeigen und visuell überprüfen
%%
%% – Bearbeiten und Ändern der Datei nach Bedarf unter Berücksichtigung der Befehlssyntax.
Datei speichern (z.B. WxT_Tags.txt)
%% – SFTP Datei im Verzeichnis /tmp nach AS lesen
%% – Melden Sie sich bei AS, bwcli an (Anmeldung als Admin)
%% – Führen Sie den folgenden Befehl von bwcli aus: AS_CLI> r /tmp/ WxT_Tags.txt
%% – Ergebnisse überprüfen
%%
%% ----------------------------------------------------------------------------------------------------------
%% Schritt 1: Connect-Tag-Set-Label erstellen – Connect_Tags
%% ----------------------------------------------------------------------------------------------------------
Beenden Sie alle; System; DeviceTagSet (Geräte-TagSet)
Connect_Tags hinzufügen
%% ----------------------------------------------------------------------------------------------------------
%% Schritt 2: Hinzufügen von benutzerdefinierten WxT für BWKS-Tags
%% BEISPIEL – für alle mobilen Tags siehe die folgende Liste-----------------------------------------------
--
Beenden Sie alle; System; DeviceTagSet; Schilder
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% true
%% ----------------------------------------------------------------------------------------------------------
```


Vertrauliche Informationen von Cisco

```
%% Schritt 3: Festlegen benutzerdefinierte Tags verbinden (falls Tag bereits vorhanden)
%% BEISPIEL – für alle mobilen Tags siehe die Liste unten
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------
%% Schritt 4: Überprüfen Sie, ob benutzerdefinierte Tags korrekt definiert und festgelegt wurden
%% ----------
Beenden Sie alle; System; DeviceTagSet; Schilder
get tagSetName Connect_Tags
Alle beenden
```

Im Folgenden werden alle benutzerdefinierten Tags aufgeführt, die von Webex für Cisco BroadWorks verwendet werden, mit Beispielwerten (Standard oder empfohlen). Beachten Sie, dass für einige der Tags Werte erforderlich sind, die für die entsprechende Bereitstellung spezifisch sind (z. B. Serveradressen). Aus diesem Grund werden diese Tags am Ende des Skripts hinzugefügt, aber leer gelassen, und es sollten zusätzliche set-Befehle hinzugefügt werden, um sie zu spezifizieren.

10.1 Desktops

```
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
tagSetName hinzufügen 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
tagSetName hinzufügen 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
```


Vertrauliche Informationen von Cisco

```
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
tagSetName hinzufügen BroadTouch_tags %SOURCE_PORT_WXT% 5060
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName BroadTouch_tags %SIP_FAILBACK_ENABLED_WXT% true
tagSetName hinzufügen BroadTouch_tags %SIP_FAILBACK_TIMEOUT_WXT% 900
add tagSetName BroadTouch_tags %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% false
tagSetName hinzufügen BroadTouch_tags %SIP_TRANSPORTS_ENFORCE_IP_Version_WXT% DNS
tagSetName hinzufügen 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
tagSetName hinzufügen BroadTouch_tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
tagSetName hinzufügen 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
tagSetName hinzufügen BroadTouch_tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
tagSetName hinzufügen 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
tagSetName hinzufügen BroadTouch_tags %WEB_CALL_SETTINGS_TARGET_WXT% extern
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
tagSetName hinzufügen BroadTouch_tags %USER_PORTAL_SETTINGS_URL_WXT%
tagSetName hinzufügen BroadTouch_tags %USER_PORTAL_SETTINGS_TARGET_WXT% extern
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_BLIND_WXT% false
tagSetName hinzufügen BroadTouch_tags %ENABLE_CALL_PICKUP_DIRECTED_WXT% false
```


Vertrauliche Informationen von Cisco

```
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
tagSetName hinzufügen 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
tagSetName hinzufügen BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
tagSetName hinzufügen 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
tagSetName hinzufügen BroadTouch_tags %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% 120
add tagSetName BroadTouch_tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_IPv6_WXT% false
add tagSetName BroadTouch_tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% aufgelöst
```


Vertrauliche Informationen von Cisco

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

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
tagSetName hinzufügen Connect_Tags %ENABLE_NOISE_REMOVAL_WXT% false
tagSetName hinzufügen 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
tagSetName hinzufügen 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
tagSetName hinzufügen Connect_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
tagSetName hinzufügen Connect_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
tagSetName hinzufügen Connect_Tags %SOURCE_PORT_WXT% 5060
add tagSetName Connect_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
tagSetName hinzufügen Connect_Tags %SIP_TRANSPORTS_ENFORCE_IP_Version_WXT% dns
tagSetName hinzufügen Connect_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName Connect_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName Connect_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName Connect_Tags %SRTP_ENABLED_WXT% false
add tagSetName Connect_Tags %SRTP_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_REKEYING_WXT% true
tagSetName hinzufügen Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
tagSetName hinzufügen Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
tagSetName hinzufügen 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
```


Vertrauliche Informationen von Cisco

```
add tagSetName Connect_Tags %CHANNEL_HEARTBEAT_WXT% 10000
tagSetName hinzufügen Connect_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
tagSetName hinzufügen 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
tagSetName hinzufügen Connect_Tags %WEB_CALL_SETTINGS_TARGET_WXT% extern
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
tagSetName hinzufügen Connect_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% extern
add tagSetName Connect_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
tagSetName hinzufügen Connect_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% nur cs-only
tagSetName hinzufügen Connect_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName Connect_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
tagSetName hinzufügen Connect_Tags %REJECT_WITH_XSI_MODE_WXT%decline_false
tagSetName hinzufügen Connect_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT % belegt
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
tagSetName hinzufügen Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% false
tagSetName hinzufügen Connect_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
tagSetName hinzufügen Connect_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
tagSetName hinzufügen 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
```


Vertrauliche Informationen von Cisco

```
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
tagSetName hinzufügen 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
tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT% once_per_login
hinzufügen
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
tagSetName hinzufügen Connect_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName Connect_Tags %ENABLE_VIDEO_QOS_WXT% true
tagSetName hinzufügen 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
tagSetName hinzufügen 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
tagSetName hinzufügen Connect_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName Connect_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName Connect_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName Connect_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_Center_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName Connect_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName Connect_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName Connect_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_RTP_ICE_IPv6_WXT% false
tagSetName hinzufügen Connect_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% aufgelöst
add tagSetName Connect_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName Connect_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```


Vertrauliche Informationen von Cisco

10.3 Tablette

```
add tagSetName ConnectTablet_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_CALLS_WXT% false
tagSetName hinzufügen 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
tagSetName hinzufügen 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
tagSetName hinzufügen ConnectTablet_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
tagSetName hinzufügen 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
tagSetName hinzufügen ConnectTablet_Tags %SOURCE_PORT_WXT% 5060
add tagSetName ConnectTablet_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
tagSetName hinzufügen ConnectTablet_Tags %SIP_TRANSPORTS_ENFORCE_IP_Version_WXT% dns
tagSetName hinzufügen ConnectTablet_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName ConnectTablet_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_REKEYING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
tagSetName hinzufügen ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
tagSetName hinzufügen 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
```


Vertrauliche Informationen von Cisco

```
add tagSetName ConnectTablet_Tags %CHANNEL_HEARTBEAT_WXT% 10000
tagSetName hinzufügen ConnectTablet_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
tagSetName hinzufügen 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
tagSetName hinzufügen ConnectTablet_Tags %WEB_CALL_SETTINGS_TARGET_WXT% extern
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
tagSetName hinzufügen ConnectTablet_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% extern
add tagSetName Tablet verbinden_Tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
tagSetName hinzufügen ConnectTablet_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
tagSetName hinzufügen ConnectTablet_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_MODE_WXT%decline_false hinzufügen
tagSetName hinzufügen ConnectTablet_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% belegt
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
tagSetName hinzufügen ConnectTablet_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName ConnectTablet_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
tagSetName hinzufügen ConnectTablet_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%MNO_Access hinzufügen
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
```


Vertrauliche Informationen von Cisco

```
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
tagSetName hinzufügen ConnectTablet_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
tagSetName hinzufügen 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
tagSetName hinzufügen ConnectTablet_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_QOS_WXT% true
tagSetName hinzufügen 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
tagSetName hinzufügen ConnectTablet_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_Center_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName ConnectTablet_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_IPv6_WXT% false
add tagSetName ConnectTablet_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% aufgelöst
add tagSetName ConnectTablet_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```


Vertrauliche Informationen von Cisco

10.4 System-Tags

Im Folgenden sind die Systemtags aufgeführt, die von Webex für BroadWorks verwendet werden.

```
%BWNETWORK-KONFERENZ-SIPURI-n%
%BWVOICE-PORTAL-NUMMER-N%
%BWLINEPORT-n%
%BWHOST-n%
%BWAUTHUSER-n%
%BWAUTHPASSWORT-n%
%BWE164-n%
%BWNAME-n%
%BW-Durchwahl-n%
%BWAUSSEHEN-LABEL-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMARY%
%BWE911-PRIMÄRE-HELDURL%
%BWE911-KUNDENID%
%BWE911-GEHEIMSCHLÜSSEL%
%BWE911-NOTRUFNUMMERNLISTE%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%
```


Vertrauliche Informationen von Cisco

11 Akronyme und Abkürzungen

In diesem Abschnitt werden die in diesem Dokument enthaltenen Akronyme und Abkürzungen aufgeführt. Die Akronyme und Abkürzungen sind in alphabetischer Reihenfolge mit ihrer Bedeutung aufgelistet.

ACB	Automatischer Rückruf
ACD	Automatic Call Distribution
ACR	Ablehnen anonymer Anrufe
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
API	Application Programming Interface
APK	Anwendungspaket
APNS	Apple Push-Benachrichtigungsdienst
ARS	Automatische Bitratenauswahl
WIE	Anwendungsserver (Cisco BroadWorks)
AVP	Audiovisuelles Profil
BW	BroadWorks
BWA	BroadWorks überall
BWKS	BroadWorks
BWM	BroadWorks-Mobilität
BYOD	Bringen Sie Ihr eigenes Gerät mit
CC	Callcenter
CFB	Rufumleitung wenn besetzt
CFNA	Rufumleitung wenn keine Antwort
CFNR	Anrufweiterleitung nicht erreichbar
CIF	Allgemeines Zwischenformat
CLI	Kommandozeilen-Schnittstelle
CLID	Anrufleitungsidentität
CLIDB	Blockieren der Zustellung durch Anrufleitungs-ID
CRLF	Wagenrücklauf Zeilenvorschub
CS	Schaltungsvermittelt
CSWV	Webansicht für Anrufeinstellungen
CW	Anklopfen
DB	Datenbanken
DEZIMETER	Geräteverwaltung
DND	Bitte nicht stören

Vertrauliche Informationen von Cisco

DNS	Domain Name System (DNS)
DPC	Steuerung des Tischtelefons
DTAF	Archivdatei für Gerätetypen
ECACS	Service zum Ändern der Notfalladresse
FMC	Konvergenz zwischen Festnetz und Mobilfunk
FQDN	Vollständiger Domänenname
HMAC	Hashnachrichten-Authentifizierungscode
ICE	Herstellung interaktiver Konnektivität
iLBC	Internet-Codec mit niedriger Bitrate
IM	Instant Messaging
IM&P	Instant Messaging und Präsenz
IOT	Interoperabilitätstests
IP	Internet Protocol
JID (Begriffsklärung	Jabber-Kennung
M/O	Obligatorisch/Optional
MNO	Mobilfunknetzbetreiber
MTU	Maximale Übertragungseinheit
MUC	Chat für mehrere Benutzer
MWI	Anzeige für wartende Nachrichten
NAL	Netzwerkabstraktionsschicht
NAPTR	Zeiger für Benennungsautorität
NAT	Network Address Translation
OTT	Den Bogen überziehen
PA	Persönlicher Assistent
PAI	P-Behauptete-Identität
PEM	P-Frühe Medien
PLI	Anzeige von Bildverlust
PLMN	Öffentliches Mobilfunknetz
PN	Push-Benachrichtigung
QCIF	Viertelallgemeines Zwischenformat
QoS	Quality of Service
RO	Externes Büro
RTCP	Echtzeit-Steuerungsprotokoll
RTP	Real Time Protocol
SaaS	Software-as-a-Service
SAN	Alternativer Name des Subjekts

Vertrauliche Informationen von Cisco

SASL	Einfache Authentifizierungs- und Sicherheitsschicht
SAVP	Sicheres Audio-Video-Profil
SBC	Session Border Controller
SCA	Gemeinsame Leitungsnutzung
SCF	Sitzungskontinuitätsfunktion
SCTP	Stream Control-Übertragungsprotokoll
SDP	Sitzungsdefinitionsprotokoll
SEQRING	Sequenzieller Rufton
SIMRING	Gleichzeitiges Klingeln
SIP	Session Initiation Protocol
SNR	Signal-Rausch-Verhältnis
SNR	Single Number Reach
SRTCP	Secure Real-Time Control Protocol
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
STUN	Session Traversal-Dienstprogramme für NAT
SUBQCIF	Sub-Viertel-CIF
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Zeit zu leben
TURN	Durchquerung mit Relay NAT
UDP	User Datagram Protocol
UI	Benutzeroberfläche
UMS	Messaging-Server (Cisco BroadWorks)
URI	Uniform Resource Identifier
UVS	Videoserver (Cisco BroadWorks)
VGA	Videografik-Array
VoIP	Voice-Over-IP
VVM	Visuelle Voicemail
WXT	Webex
XMPP	Extensible Messaging and Presence Protocol
XR	Erweiterter Bericht
Xsp	Xtended Services-Plattform
Xsi	Xtended Services-Schnittstelle

Vertrauliche Informationen von Cisco