Webex für Cisco Broadworks – Konfigurationsleitfaden

Freigeben 45.10

Dokumentversion 3

Inhaltsverzeichnis

1 Zusammenfassung der Änderungen 1
1.1 Änderungen in Version 45.10, Oktober 2025 1
1.2 Änderungen in Version 45.9, September 2025 1
1.3 Änderungen in Version 45.8, August 2025 1
1.4 Änderungen in Version 45.7, Juli 2025 2
1.5 Änderungen in Version 45.6, Juni 2025 2
1.6 Änderungen in Version 45.5, Mai 2025 2
1.7 Änderungen in Version 45.4, April 2025 2
1.8 Änderungen in Version 45.3, März 2025 2
1.9 Änderungen in Version 45.2, Februar 2025 2
1.10 Änderungen zu Release 45.1, Januar 2025 2
1.11 Änderungen zu Release 44.12, Dezember 2024 3
1.12 Änderungen in Version 44.11, November 2024 3
1.13 Änderungen in Version 44.10, Oktober 2024 3
1.14 Änderungen in Version 44.9, September 2024 3
1.15 Änderungen in Version 44.8, August 2024 3
1.16 Änderungen in Version 44.7, Juli 2024 3
1.17 Änderungen in Version 44.6, Juni 2024 3
1.18 Änderungen in Version 44.5, Mai 2024 3
1.19 Änderungen in Version 44.4, April 2024 3
1.20 Änderungen in Version 44.3, März 2024 4
1.21 Änderungen in Version 44.2, Februar 2024 4
1.22 Änderungen in Version 44.1, Januar 2024 4
2 Änderungen für Konfigurationsdateien 5
2.1 Änderungen an Konfigurationsdateien für die Version 45.10 5
2.2 Änderungen an Konfigurationsdateien für die Version 45.9 6
2.3 Änderungen an Konfigurationsdateien für die Version 45.8 6
2.4 Änderungen an Konfigurationsdateien für die Version 45.7 6
2.5 Änderungen an Konfigurationsdateien für die Version 45,6 7
2.6 Änderungen an Konfigurationsdateien für die Version 45,5 7
2.7 Änderungen an Konfigurationsdateien für die Version 45,4 8
2.8 Änderungen an Konfigurationsdateien für die Version 45,3 8
2.9 Änderungen an Konfigurationsdateien für die Version 45,2 8
2.10 Änderungen an Konfigurationsdateien für die Version 45,1 8
2.11 Änderungen an Konfigurationsdateien für die Version 44,12 8
2.12 Änderungen an Konfigurationsdateien für die Version 44,11 8
2.13 Änderungen an Konfigurationsdateien für die Version 44,1 9
2.14 Änderungen an Konfigurationsdateien für die Version 44.9 9
2.15 Änderungen an Konfigurationsdateien für die Version 44.8 9

2.16 Änderungen an Konfigurationsdateien für die Version 44.7 9
2.17 Änderungen an Konfigurationsdateien für die Version 44.6 10
2.18 Änderungen an Konfigurationsdateien für die Version 44.5 10
2.19 Änderungen an Konfigurationsdateien für die Version 44,4 10
2.20 Änderungen an Konfigurationsdateien für die Version 44,3 11
2.21 Änderungen an Konfigurationsdateien für die Version 44,2 11
2.22 Änderungen an Konfigurationsdateien für die Version 44,1 13
3 Einführung 14
4 Installation 15
4.1 Lokalisierter Client Download 15
4.2 Android-Client 15
4.3 iOS-Client 15
4.4 Desktop-Client 16
5 Geräteverwaltung 17
5.1 Geräteverwaltungs-Tags 17
5.2 Teilweise Übereinstimmungserweiterungen für die Gerätetypauswahl 18
5.3 Client-Konfiguration 19
5.4 Bereitstellung von config-wxt.xml 19
5.5 Konfigurationsdatei (config-wxt.xml) 19
5.6 System-Standard-Tags 20
5.7 Cisco BroadWorks Dynamic integrierte System-Tags 20
6 Benutzerdefinierte Tags 23
6.1 Gemeinsame Merkmale 36
6.1.1 SIP-Server-Einstellungen 36
6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll 39
6.1.3 SIP-Header 3GPP für SRTP 41
6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen 42
6.1.5 Konfigurierbare Zeitüberschreitung beim Öffnen des SIP-Sockets 44
6.1.6 Dynamische SIP-Proxy-Erkennung 45
6.1.7 Nutzung des bevorzugten Ports für SIP 50
6.1.8 SIP-Failover und Failback 51
6.1.9 SIP SUBCSRIBE und REGISTER Refresh und SUBSCRIBE Retry 56
6.1.10 P-Associated-URIs im REGISTER verwenden 56
6.1.11 SIP P-Early Media (PEM)-Header 57
6.1.12 Unterstützung VON SIP-AKTUALISIERUNGEN 58
6.1.13 Ältere SIP-INFO-FIR 58
6.1.14 SIP Rport-Verwaltung für NAT-Traversal 59
6.1.15 SIP Sitzungs-ID 60
6.1.16 Verhalten beim Ablehnen eingehender Anrufe 60
6.1.17 Portbereich des Transportprotokolls in Echtzeit 60
6.1.18 ICE-Unterstützung (nur Webex Calling) 61

Cisco – vertraulich

6.1.19 RTCP-MUX 62
6.1.20 Übertragen 62
6.1.21 N-Wege-Konferenzanrufe 64
6.1.22 Anrufübergabe 65
6.1.23 Anruf parken/Abrufen 67
6.1.24 Anrufstatistik 68
6.1.25 Automatische Wiederherstellung von Anrufen /Nahtlose Übergabe von Anrufen 68
6.1.26 Anrufaufzeichnung 69
6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten 70
6.1.28 Voicemail-Abschrift für Webex Calling 72
6.1.29 Anrufeinstellungen 72
6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen 75
6.1.31 Callcenter/Anrufwarteschlange-Anmeldung/Abmeldung 79
6.1.32 XSI-Wurzel und Pfade 79
6.1.33 XSI-Ereigniskanal 80
6.1.34 Codec-Konfiguration 81
6.1.35 SIP-URI-Wahl 83
6.1.36 Anrufprotokoll 84
6.1.37 Videoanrufe deaktivieren 84
6.1.38 Notrufe (911) – Standortberichte beim E911-Anbieter 85
6.1.39 PAI als Identität 87
6.1.40 Bildschirmfreigabe deaktivieren 87
6.1.41 Spam-Anruf-Anzeige 88
6.1.42 Entfernen von Geräuschen und Erweiterung der Bandbreite für PSTN-/Mobilanrufe . 88
6.1.43 QoS-DSCP-Markierung 89
6.1.44 Primäres Profil 90
6.1.45 Sperrliste (nur Webex Calling) 91
6.1.46 Umsetzung der Medienanpassung und Resilienz (MARI) 92
6.1.47 Gleichzeitige Anrufe mit demselben Benutzer 94
6.1.48 RTCP-XR 95
6.1.49 Informationen zur Anrufweiterleitung 95
6.1.50 Anrufer-ID 95
6.1.51 Mehrere Leitungen 99
6.1.52 Verbesserte SIP-Autorisierung 101
6.1.53 Persönlicher Assistent (Abwesenheitsstatus) 101
6.2 Nur Desktop-Funktionen 103
6.2.1 Erzwungene Abmeldung 103
6.2.2 Anrufannahme 104
6.2.3 Unterstützung von Chef-Admin (Führungskraft-Assistent) 104
6.2.4 SIP-Anrufe an Meeting eskalieren (nur Webex Calling) 105
6.2.5 Anrufe mit Steuerung des Tischtelefons – Automatische Anrufannahme 105
6.2.6 Automatische Anrufannahme mit Tonbenachrichtigung 106

Cisco – vertraulich

6.2.7 Tischtelefonsteuerung - Mid Call Controls - Konferenz 106
6.2.8 Benachrichtigungen für Anrufannahme 107
6.2.9 Event-Paket für Remotesteuerung 109
6.2.10 Survivability Gateway (nur Webex Calling) 110
6.2.11 Event-Paket für Remote-Stummschaltungssteuerung (nur Webex Calling) 110
6.2.12 Anruf verschieben 111
6.3 Funktionen nur für Mobilgeräte 113
6.3.1 Notrufe 113
6.3.2 Pushbenachrichtigungen für Anrufe 114
6.3.3 Einzelne Warnungen 116
6.3.4 Click to Dial (Rückruf) 117
6.3.5 MNO-Unterstützung 118
6.3.6 ID des eingehenden Anrufers 123
7 Merkmale des frühen Feldversuchs (BETA) 125
7.1 Notrufe (911) – Cisco Emergency Location Information Service (nur Webex Calling) und Konfigurationsbereinigung 125
7.2 Unified-Anrufprotokoll für sekundäre Leitungen (nur Webex Calling) 129
7.3 Durchgängige Verschlüsselung (nur Webex Calling) 129
Benutzerdefinierte Tags-Zuordnung zwischen Webex for Cisco BroadWorks und UC-One 130
8 Anhang A: TLS-Schlüssel 138
9 Anhang B: DM Tag Provisioning Script 139
9.1 Desktop 140
9.2 Mobil 143
9.3 Tablet 146
9.4 System-Tags 149
10 Akronyme und Abkürzungen 150

Cisco – vertraulich

1 Zusammenfassung der Änderungen

In diesem Abschnitt werden die Änderungen an für die einzelnen Releases und Dokumentversionen beschrieben.

1.1 Änderungen in Version 45.10, Oktober 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.21 N-Wege-Konferenzanrufe* – hat den BETA-Abschnitt *N-Way-Konferenzanrufe-Verbesserung (nur Webex Calling)* zusammengeführt.
- Abschnitt *6.1.22 Anrufübergabe* – Der BETA-Abschnitt *Anrufübernahme-Verbesserungen* wurde zusammengeführt.
- [**Wichtig**] Abschnitt wurde in der BETA-VERSION hinzugefügt.
    - Dokumentversion 3 – es wurden zusätzliche Details zur Verfügbarkeit des Cisco Emergency Location Information-Dienstes ausschließlich für den Webex Calling-Bereitstellungstyp aufgenommen.
- Der Abschnitt *Unified-Anrufprotokoll für sekundäre Leitungen (nur Webex Calling)* wurde in der BETA-VERSION hinzugefügt.
- Abschnitt *6.1.36 Anrufprotokoll* aktualisiert – es wurde eine Klarstellung hinzugefügt, dass das Anrufprotokoll über alle Geräte hinweg nur für die Hauptleitung des Benutzers synchronisiert wird.
- Abschnitt *Durchgängige Verschlüsselung (nur Webex* Calling) in der BETA-VERSION hinzugefügt.

1.2 Änderungen in Version 45.9, September 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Der Abschnitt *Verbesserungen bei der Anrufübernahme* wurde aktualisiert – weitere Details wurden hinzugefügt.
- Abschnitt *6.1.22 Anrufübergabe* aktualisiert – weitere Details zur Funktionsabhängigkeit von der serverseitigen Dienstkonfiguration wurden hinzugefügt.
- Aktualisierter Abschnitt *6.1.25 Automatische Wiederherstellung von Anrufen /Nahtlose Übergabe von* Anrufen – es wurden weitere Details zur Abhängigkeit der Funktion von der Anrufübertragungsfunktion und dem während der Wiederherstellung von Anrufen abgespielten Ton hinzugefügt.

1.3 Änderungen in Version 45.8, August 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.34 Codec-Konfiguration* – Details zur maximalen H.264-Videoauflösung pro Plattform und Aktualisierung für die Desktop-Version der Webex-App wurden hinzugefügt.

1.4 Änderungen in Version 45.7, Juli 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Der Abschnitt *N-Way-Konferenzanrufe (nur Webex Calling)* wurde in der BETA-VERSION hinzugefügt.
- Der Abschnitt *Verbesserungen bei der Anrufübernahme* wurde in der BETA-VERSION hinzugefügt.

1.5 Änderungen in Version 45.6, Juni 2025

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.6 Änderungen in Version 45.5, Mai 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt „CLID-Auswahl des Anrufwarteschlangen-Agenten“ entfernt – eingestellt von *6.1.50.1 Ausgehende Anrufer-ID*.
- Veraltete Tags und Attribute wurden entfernt.

1.7 Änderungen in Version 45.4, April 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.34.1 AI-Codec* verschoben – aus BETA.
- Abschnitt *6.1.51 Mehrere* Leitungen – kombiniert die reinen Desktop- und mobilen BETA-Abschnitte.
- Abschnitt verschoben *6.1.52 Verbesserte SIP-Autorisierung* – Außerhalb der BETA-VERSION.
- Abschnitt *6.1.53 Persönlicher Assistent (Abwesenheitsstatus)* wurde verschoben als üblich für Desktop und Mobilgeräte

1.8 Änderungen in Version 45.3, März 2025

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.9 Änderungen in Version 45.2, Februar 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *Verbesserte SIP-Autorisierung* in BETA hinzugefügt.

1.10 Änderungen zu Release 45.1, Januar 2025

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *Persönlicher Assistent (Abwesenheitsstatus)* wurde aus der BETA-VERSION VERSCHOBEN.
- Abschnitt *6.3.2.3 Bereitstellungsmodus (nur Webex Calling)* aus der BETA-VERSION verschoben.

1.11 Änderungen zu Release 44.12, Dezember 2024

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.12 Änderungen in Version 44.11, November 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

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

1.13 Änderungen in Version 44.10, Oktober 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *Persönlicher Assistent (Abwesenheitsstatus)* in BETA *hinzugefügt.*
- Abschnitt *Bereitstellungsmodus (nur Webex Calling)* in der BETA-VERSION hinzugefügt.

1.14 Änderungen in Version 44.9, September 2024

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

1.15 Änderungen in Version 44.8, August 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.1.34 Codec-Konfiguration* - Klärung der DTMFs und der unterstützten Übertragungsmechanismen hinzugefügt.

1.16 Änderungen in Version 44.7, Juli 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt hinzugefügt *AI-Codec* in BETA.
- Abschnitt *6.1.641P44mary Profile* aktualisiert – Details zum Verhalten der Webex-App wurden von Anfang an auf Version 43,2 entfernt.

1.17 Änderungen in Version 44.6, Juni 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.3.6. ID des* eingehenden Anrufers - mehr Details über das native Erlebnis und die Funktionsweise der Funktion hinzugefügt.

1.18 Änderungen in Version 44.5, Mai 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

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

1.19 Änderungen in Version 44.4, April 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Abschnitt *6.1.50.1 Ausgehende Anrufer-ID* aktualisiert.
- Aktualisierter Abschnitt *Änderungen an Konfigurationsdateien für die Version* 44,3 – Details zu den keepalive-Aktualisierungen wurden in 44,3 hinzugefügt.

1.20 Änderungen in Version 44.3, März 2024

Diese Version des Dokuments enthält die folgenden Änderungen:

- Aktualisierter Abschnitt *6.3.6. ID des eingehenden* Anrufers
    - Abschnitt *6.1.50.1 Ausgehende Anrufer-ID* wurde verschoben und mit weiteren Details aktualisiert.
- Aktualisierter Abschnitt *6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen* - Details zu den konfigurierbaren Keepalives unter Verwendung benutzerdefinierter Tags hinzugefügt.

1.21 Änderungen in Version 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 für Anrufannahme*
    - Unterabschnitt *6.2.8.1 Besetztlampenfeld* hinzugefügt - BLF-Spezifikationen dorthin verschoben.
    - Unterabschnitt *6.2.8.2 Anrufannahmegruppe (nur Webex Calling)* hinzugefügt.
- Abschnitt hinzugefügt *6.1.49 Informationen zur Anrufweiterleitung*.
- Aktualisierter Abschnitt *6.1.8.3 IP-Version durchsetzen* - Details für den neuen Modus *nat64* hinzugefügt.
- Aktualisierter Abschnitt *6.1.42 Entfernen von Geräuschen und Erweiterung der* Bandbreite für PSTN-/Mobilanrufe - Details zur neuen Unterstützung der Bandbreitenerweiterung und zur Rauschunterdrückung hinzugefügt. Abschnitt *Sprachverbesserungen für PSTN-Anrufe* wird aus BETA entfernt.

1.22 Änderungen in Version 44.1, Januar 2024

Für diese Version wurden keine Änderungen an diesem Dokument vorgenommen.

2 Änderungen für Konfigurationsdateien

2.1 Änderungen an Konfigurationsdateien für die Version 45.10

- [Nur Webex Calling] Das Tag im Abschnitt steuert jetzt eine offizielle Funktion.

```
<config>
<services><calls>
   <conference>
      <drop-two-party-conference
enabled="%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%"/>
```

- Der Modus und die Standard-active-move-option (nur Desktop)-Attribute im Tag steuern jetzt eine offizielle Funktion.

```
<config>
<services><calls>
   <call-pull enabled="%ENABLE_CALL_PULL_WXT%" mode="%CALL_PULL_MODE_WXT%"
default-active-move-option="%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%"/>
```

- [Wichtig] [BETA-Funktion] [Nur Desktop und Tablet] Der Abschnitt wurde hinzugefügt unter , wodurch der Abschnitt eingestellt wird.

```
<config><services>
<emergency-dialing enabled="%ENABLE_EMERGENCY_DIALING_WXT%">
   <redsky enabled="%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%"> <!-- DEPRECATED
by <emergency-location> -->
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-
timeout>%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%</user-reminder-timeout>
      <user-mandatory-
location>%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%</user-mandatory-
location>
      <user-location-
prompting>%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%</user-location-
prompting>
   </redsky>
   <emergency-location enabled="%ENABLE_EMERGENCY_LOCATION_WXT%"
               provider="%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%">
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-
timeout>%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%</user-reminder-
timeout>
      <user-mandatory-
location>%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%</user-mandatory-
location>
      <user-location-
prompting>%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%</user-location-
prompting>
   </emergency-location>
</emergency-dialing>
```


Cisco – vertraulich

- [Nur Webex Calling] Tag im Abschnitt hinzugefügt.

```
<config>
<services><calls>
   <e2ee enabled="%ENABLE_CALLS_E2EE_WXT%"/>
```

Die folgenden %TAG%s wurden hinzugefügt:

- [BETA] %ENABLE_EMERGENCY_LOCATION_WXT%
- [BETA] %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%
- [BETA] %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%
- [BETA] %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
- [BETA] %ENABLE_CALLS_E2EE_WXT%

Die folgenden %TAG%s wurden veraltet:

- [BETA] %EMERGENCY_DIALING_ENABLE_REDSKY_WXT%
- [BETA] %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%
- [BETA] %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%
- [BETA] %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%

Weitere Informationen finden Sie unter .

2.2 Änderungen an Konfigurationsdateien für die Version 45.9

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.3 Änderungen an Konfigurationsdateien für die Version 45.8

- [Nur Desktop] Die Videoauflösung von H.264 wurde auf WIDE_FULL_HD aktualisiert und die Attribute für Auflösung, Framerate und Bitrate wurden im -Tag für H.264 Codec im Abschnitt hinzugefügt.<video>

```
<config>
<services><calls>
<video><codecs>
       <codec name="H264" resolution="WIDE_FULL_HD" framerate="30"
bitrate="4000000" priority="1.0" payload="109">
```

2.4 Änderungen an Konfigurationsdateien für die Version 45.7

- [BETA-Funktion] [Nur Webex Calling] Tag im Abschnitt hinzugefügt.

```
<config>
<services><calls>
   <conference>
      <drop-two-party-conference
enabled="%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%"/>
```

- [BETA-Funktion]Hinzugefügte Modus- und Standard-Active-Move-Option-Attribute (nur Desktop) im Tag .

```
<config>
<services><calls>
   <call-pull enabled="%ENABLE_CALL_PULL_WXT%" mode="%CALL_PULL_MODE_WXT%"
default-active-move-option="%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%"/>
```

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%
- %CALL_PULL_MODE_WXT%
- %CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%

2.5 Änderungen an Konfigurationsdateien für die Version 45,6

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.6 Änderungen an Konfigurationsdateien für die Version 45,5

Die folgenden Abschnitte/Tags wurden entfernt:

- [D/M]
  - Veraltet mit Version 42,12
  - Ersetzt durch die für jede Leitung unter
- [D]
  - Ersetzt durch für jede Leitung unter
- [D/M]
  - Veraltet mit Version 43,11
  - Ersetzt durch den in
- [D/M] <Service-URI>
  - Veraltet mit Version 42,12
  - Ersetzt durch die. für jede Leitung unter
- [D/M] <Geräuschunterdrückung>
  - Veraltet mit Version 43,12
  - Ersetzt durch
- [D/M] <Rufnummer>
  - Veraltet mit Version 42,12
  - Ersetzt durch die für jede Leitung unter
- [D]

Cisco – vertraulich

- Veraltet mit Version 44,3
- Ersetzt durch

Die folgenden Attribute wurden entfernt:

- [D/M] URL-Attribut unter
- [D/M] Branding-fähiges Attribut unter

Die folgenden %TAG%s wurden entfernt:

- [D] %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%

2.7 Änderungen an Konfigurationsdateien für die Version 45,4

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.8 Änderungen an Konfigurationsdateien für die Version 45,3

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.9 Änderungen an Konfigurationsdateien für die Version 45,2

- [BETA-Funktion] Tag im Abschnitt hinzugefügt.

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

Der folgende %TAG% wurde hinzugefügt:

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.10 Änderungen an Konfigurationsdateien für die Version 45,1

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.11 Änderungen an Konfigurationsdateien für die Version 44,12

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.12 Änderungen an Konfigurationsdateien für die Version 44,11

- [BETA-Funktion] [Nur Mobilgeräte] [Nur Webex Calling]Attribut mit mehreren Leitungen im Tag hinzugefügt.

  Abschnitte und für die sekundären Leitungen im Abschnitt hinzugefügt.

```
<config>
<protocols><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
```


Cisco – vertraulich

```
   <personal>
      <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
   </personal>
   <line lineType="%BW-MEMBERTYPE-1%">
      …
   </line>
   <line lineType="%BW-MEMBERTYPE-2%">
      …
   </line>
   …
   <line lineType="%BW-MEMBERTYPE-10%">
      …
   </line>
</lines>
```

2.13 Änderungen an Konfigurationsdateien für die Version 44,1

- [BETA-Funktion] Tag im Abschnitt hinzugefügt.

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

- [BETA-Funktion] [Nur Mobilgeräte] [Nur Webex Calling]Attribut für den Bereitstellungsmodus unter dem Tag hinzugefügt.

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

Die folgenden %TAG%s wurden hinzugefügt:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.14 Änderungen an Konfigurationsdateien für die Version 44.9

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.15 Änderungen an Konfigurationsdateien für die Version 44.8

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.16 Änderungen an Konfigurationsdateien für die Version 44.7

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

```
<config>
<services><calls>
  <audio>
    <codecs>
      <codec name="opus" priority="1" payload=""/>
```


Cisco – vertraulich

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

2.17 Änderungen an Konfigurationsdateien für die Version 44.6

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

2.18 Änderungen an Konfigurationsdateien für die Version 44.5

- [Nur Webex Calling] Dem Tag -Tag wurde das Attribut „enable-ipv6-support“ hinzugefügt.

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

- Das Tag wurde im Abschnitt mit als Untertag hinzugefügt.

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

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.19 Änderungen an Konfigurationsdateien für die Version 44,4

- [Nur Desktop] [Nur Webex Calling] Tags , und wurden im Abschnitt hinzugefügt.

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

2.20 Änderungen an Konfigurationsdateien für die Version 44,3

- [Nur Desktop] [Nur Webex Calling] Ausgehende Anrufe> im Abschnitt mit als Untertag hinzugefügt.

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

- Benutzerdefinierte Tags (%UDP_KEEPALIVE_ENABLED_WXT%, %TCP_KEEPALIVE_ENABLED_WXT% und %TLS_KEEPALIVE_ENABLED_WXT%) wurden hinzugefügt, um den hardcodierten aktivierten Keep-Alive-Wert für jeden Transport unter zu ersetzen.

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

Die folgenden %TAG%s wurden hinzugefügt:

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

2.21 Änderungen an Konfigurationsdateien für die Version 44,2

- [Nur Mobilgeräte] Der Abschnitt wurde unter hinzugefügt.
  Untertags und hinzugefügt, mit einem neuen Untertag für beide.

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


Cisco – vertraulich

- [Nur Mobilgeräte] [Nur Webex Calling] Ausgehende Anrufe> im Abschnitt hinzugefügt.

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

- Tag im Abschnitt hinzugefügt.

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

- [Nur Desktop] [Nur Webex Calling] Abschnitt unter mit und als Untertags hinzugefügt.
  Im Abschnitt wurde auch unter jedem Tag im Abschnitt hinzugefügt.

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

Die folgenden %TAG%s wurden hinzugefügt:

- %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%

- %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%
- %ENABLE_GCP_NOTIFICATIONS_WXT%
- %ENABLE_GCP_DISPLAY_CALLER_WXT%
- %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%
- %BWGROUP-CALL-PICKUP-BOOL-n%

Der folgende %TAG% wurde veraltet:

- %ENABLE_NOISE_REMOVAL_WXT%

2.22 Änderungen an Konfigurationsdateien für die Version 44,1

Die Konfigurationsdateien wurden in dieser Version nicht aktualisiert.

3 Einführung

Dieses Dokument enthält eine Beschreibung der Konfiguration von Webex für den Cisco BroadWorks-Client.

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

Die Clients werden mithilfe einer Konfiguration konfiguriert, die für den Endbenutzer nicht sichtbar ist. Das *config-wxt.xml* stellt serverspezifische Informationen bereit, z. B. Serveradressen und Ports sowie Laufzeitoptionen für den Client selbst (z. B. Optionen, die im Bildschirm *Einstellungen* angezeigt werden).

Die Konfigurationsdateien werden vom Client nach dem Abrufen aus der Geräteverwaltung gelesen, wenn sie gestartet werden. Die Informationen aus den Konfigurationsdateien werden verschlüsselt gespeichert und somit für den Endnutzer unsichtbar und unzugänglich.

> **HINWEIS**: Die XML-Eigenschaften sollten keine Leerzeichen enthalten (z. B. anstelle von).

4 Installation

Die Webex für Cisco BroadWorks-Clients können über die folgenden Möglichkeiten installiert werden:

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

4.1 Lokalisierter Client Download

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

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

4.2 Android-Client

Der Android-Client wird als Anwendung (Android-Anwendungspaket [APK]) installiert, die die einstellungen- und konfigurationsbezogenen Daten in ihrem privaten Bereich speichert.

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

Wenn die neue Version heruntergeladen wird, wird die alte Software überschrieben; die Benutzerdaten bleiben jedoch standardmäßig erhalten.

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

4.3 iOS-Client

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

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

Wenn die neue Version heruntergeladen wird, wird die alte Software überschrieben; die Benutzerdaten bleiben jedoch standardmäßig erhalten.

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

Cisco – vertraulich

4.4 Desktop-Client

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

Cisco – vertraulich

5 Geräteverwaltung

5.1 Geräteverwaltungs-Tags

Webex for Cisco BroadWorks verwendet die *Tag-Sets für die Geräteverwaltung* , die in der folgenden Abbildung dargestellt sind. Die *Systemvorgabe* und benutzerdefinierte Tag-Sets sind erforderlich, um bestimmte Geräte-/Client-Einstellungen bereitzustellen. Dieses Tag-Set bietet Flexibilität bei der Verwaltung der Netzwerk-/Dienstkonnektivitätseinstellungen des Clients sowie bei der Steuerung der Funktionsaktivierung.

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

- Mobil: Verbinden_Tags
- Tablette: ConnectTablet_Tags
- Desktop: BroadTouch_Tags

Erstellen Sie jedes einzelne Tag und legen Sie seinen Wert fest. Die Verweise auf die Abschnitte enthalten ausführliche Beschreibungen für jedes Kennzeichen. Die benutzerdefinierten Tags sind je nach Funktionalität in Gruppen unterteilt und werden später in diesem Dokument erläutert.

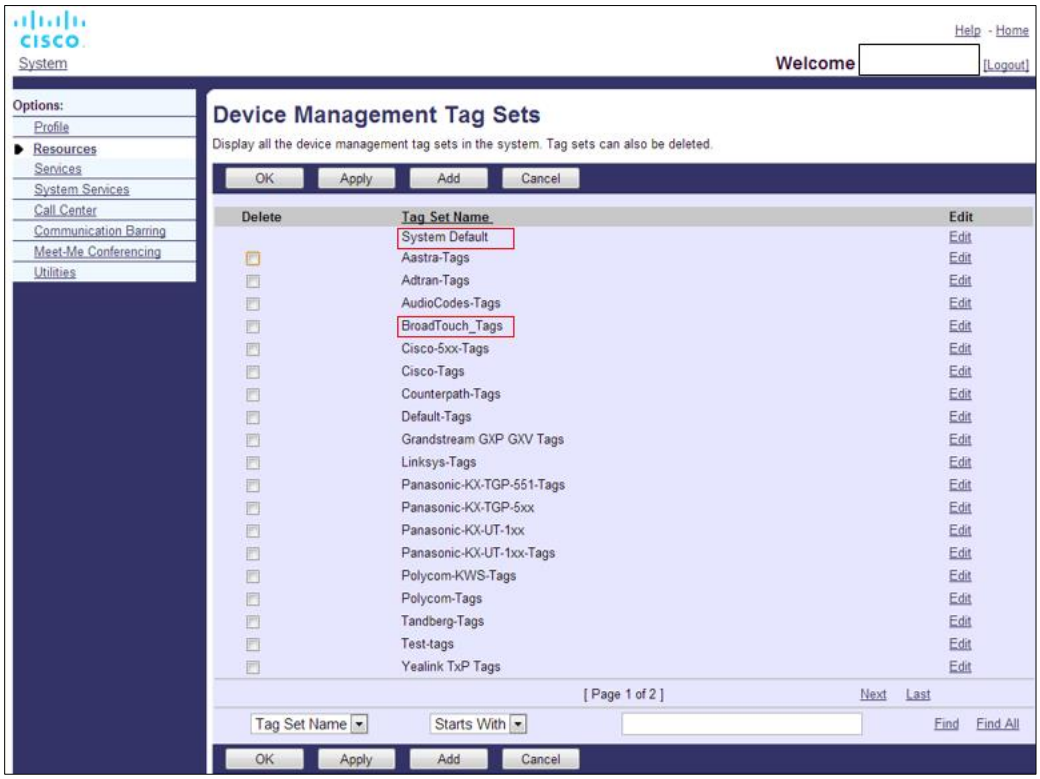


Abbildung 1 Desktop Device Management Tag Sets

Cisco – vertraulich

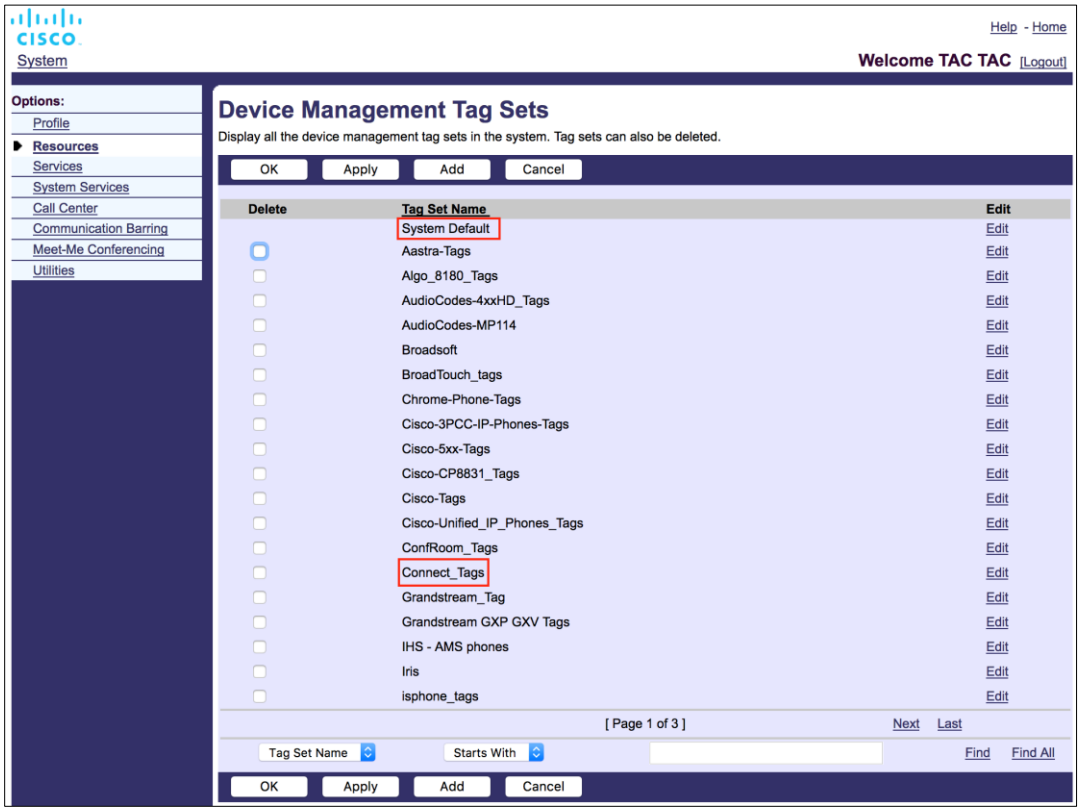


Abbildung 2 Mobile Device Management Tag Sets

5.2 Teilweise Übereinstimmungserweiterungen für die Gerätetypauswahl

Um die Flexibilität bei der Auswahl von Funktionspaketen für Benutzergruppen oder einzelne Benutzer zu erhöhen, wird der Geräteprofiltyp auf der Grundlage einer (ersten) Teilübereinstimmung ausgewählt. Dadurch können die Kunden verschiedene Gerätetypen verwenden.

Das allgemeine Verfahren zur Geräteverwaltung legt fest, dass der Cisco BroadWorks-Anwendungsserver einen Geräteprofiltyp bereitstellt. Es heißt "Business Communicator - PC" für den Desktop, "Connect - Mobile" für das Handy und "Connect - Tablet" für das Tablet. 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 zugewiesene Geräteliste über Xsi ab und sucht nach dem entsprechenden Gerätetypprofil. Der Client wählt das erste Profil, das mit dem entsprechenden Gerätetypnamen beginnt. Anschließend werden die mit diesem Geräteprofil verbundenen Konfigurationsdaten (Konfigurationsdatei) verwendet, um verschiedene Funktionen zu aktivieren und zu deaktivieren.

Dadurch kann dieselbe ausführbare Client-Datei mit verschiedenen Geräteprofiltypen verwendet werden, so dass der Dienstanbieter Funktionspakete für einzelne Benutzer oder Benutzergruppen ändern kann, indem er einfach den Geräteprofiltyp in DM für einen Benutzer oder eine Benutzergruppe ändert.

Cisco – vertraulich

Der Dienstanbieter könnte beispielsweise eine beliebige Anzahl von Geräteprofiltypen auf der Grundlage von Benutzerrollen haben, wie "Business Communicator - PC Basic", "Business Communicator - PC Executive" oder "Business Communicator - PC Assistant", und die für einzelne Benutzer verfügbaren Funktionen ändern, indem er den Geräteprofiltyp für sie ändert.

Beachten Sie, dass nicht erwartet wird, dass mehrere übereinstimmende Geräteprofiltypen in der XML-Liste der empfangenen Geräte enthalten sind, sondern nur einer.

5.3 Client-Konfiguration

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

5.4 Bereitstellung von config-wxt.xml

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

> **ANMERKUNG 1**: Für jedes Geräteprofil muss eine Konfigurationsdatei vorhanden sein.
>
> **HINWEIS 2**: Es wird DRINGEND EMPFOHLEN, dass die Vorlagen über die neueste Version der Webex-App auf dem neuesten Stand gehalten werden.

5.5 Konfigurationsdatei (config-wxt.xml)

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

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

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

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

5.6 System-Standard-Tags

Als Systemadministrator können Sie über die Option *System → Ressourcen → Device Management Tag Sets* auf die Systemstandard-Tags zugreifen. Die folgenden Systemstandard-Tags müssen bei der Installation des VoIP Calling-Pakets bereitgestellt werden.

Markierung	Beschreibung
%SBC_ADDRESS_WXT%	Dies sollte als vollqualifizierter Domänenname (FQDN) oder IP-Adresse des im Netzwerk eingesetzten Session Border Controllers (SBC) konfiguriert werden. Beispiel: sbc.yourdomain.com
%SBC_PORT_WXT%	Wenn die SBC_ADDRESS_WXT eine IP-Adresse ist, sollte dieser Parameter auf den SBC-Port gesetzt werden. Wenn die SBC_ADDRESS_WXT ein FQDN ist, kann sie nicht gesetzt werden. Beispiel: 5075

5.7 Cisco BroadWorks Dynamic integrierte System-Tags

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

Markierung	Beschreibung
%BWNETWORK-CONFERENCE-SIPURI-n%	Dies ist der Server-URI, der für die Aktivierung von N-Way-Konferenzen verwendet wird.
%BWVOICE-PORTAL-NUMBER-n%	Diese Nummer wird für die Voicemail verwendet. Der Client wählt diese Nummer, wenn die Voicemail abgerufen wird.
%BWLINEPORT-n%	Sip-Benutzername, der bei der SIP-Signalisierung verwendet wird, zum Beispiel bei der Registrierung.

Cisco – vertraulich

Markierung	Beschreibung
%BWHOST-n%	Dies ist der Domänenanteil des bereitgestellten Leitungsanschlusses für das dem Benutzer zugewiesene Gerät. Sie wird aus dem Profil des Nutzers abgerufen. In der Regel als SIP-Domäne verwendet.
%BWAUTHUSER-n%	Dies ist der Name des Authentifizierungsbenutzers. Wenn dem Teilnehmer eine Authentifizierung zugewiesen wurde, ist dies die bereitgestellte Benutzer-ID auf der Seite Authentifizierung, unabhängig vom ausgewählten Authentifizierungsmodus des Gerätetyps. Der SIP-Benutzername, der üblicherweise für die 401- und 407-Signalisierung verwendet wird. Kann sich vom standardmäßigen SIP-Benutzernamen unterscheiden.
%BWAUTHPASSWORD-n%	Dies ist das Authentifizierungskennwort des Benutzers. Wenn dem Abonnenten eine Authentifizierung zugewiesen wurde, ist dies das auf der Seite „Authentifizierung“ bereitgestellte Kennwort, unabhängig vom ausgewählten Wert im Authentifizierungsmodus des Gerätetyps. Das in der SIP-Signalisierung verwendete SIP-Kennwort.
%BWE164-n%	Dieser Tag stellt die Telefonnummer des Benutzers im internationalen Format zur Verfügung.
%BWNAME-n%	Dies ist der Vor- und Nachname des Teilnehmers im Profil des Benutzers. Vor- und Nachname werden aneinandergereiht. Im Falle einer Mehrzeilenkonfiguration, wenn keine Zeilenbeschriftung konfiguriert ist und wenn sie nicht leer ist, als Anzeigename für die Zeile im Zeilenselektor verwendet.
%BWEXTENSION-n%	Die Durchwahl des Teilnehmers wird aus der im Profil des Benutzers hinterlegten Durchwahl abgerufen. Wenn eine Nebenstelle nicht eingerichtet wurde, wird die Markierung durch die Telefonnummer (DN) des Teilnehmers ersetzt.
%BWAPPEARANCE-LABEL-n%	Dies ist die konfigurierte Zeilenbeschriftung. Wird als Zeilenname verwendet, wenn er nicht leer ist.
%BWDISPLAYNAMELINEPORT%	Dies ist die Leitung/der Anschluss 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. Dies wird aus dem Profil des Benutzers abgerufen. Dient zur Identifizierung der Hauptleitung des Benutzers.
%BWLINEPORT-PRIMARY%	Der Port der primären Leitung wird auf dem Gerät bereitgestellt, das dem Benutzer zugewiesen ist. Diese Kennzeichnung umfasst nicht den Domänenanteil des bereitgestellten Leitungsanschlusses. Sie wird aus dem Profil des Nutzers abgerufen.

Markierung	Beschreibung
%BWE911-PRIMARY-HELDURL%	Gibt die URL zur RedSky Emergency Location Platform an, die das HELD-Protokoll unterstützt.
%BWE911-CUSTOMERID%	Die Kunden-ID (HeldOrgId, CompanyID), die für die RedSky HTTPS-Anfrage verwendet wird.
%BWE911-SECRETKEY%	Das Geheimnis zur Authentifizierung der RedSky-HTTPS-Anfrage.
%BWE911-EMERGENCY-NUMBER-LIST%	Die Liste der von RedSky unterstützten Notrufnummern. Um dieses Tag zu verwenden, muss das benutzerdefinierte %RESERVEDBW911-EMERGENCY-NUMBER-LIST% reservierte Tag dem vom Gerätetyp verwendeten Tag hinzugefügt werden. Das Tag "reserved" muss die Notrufnummern enthalten, die auf BroadWorks unter AS_CLI/System/CallP/CallTypes > in einem durch Kommata getrennten Format wie 911, 0911, 933 definiert sind. **HINWEIS:** Der Webex-Client unterstützt keine Platzhalter in Notrufnummern. Daher sollten nur exakte Notrufnummern zum benutzerdefinierten „reservierten“ Tag hinzugefügt werden. Das folgende Beispiel veranschaulicht, wie die reservierte Tag-Funktionalität verwendet werden soll: 1) Das native Tag %BWE911-EMERGENCY-NUMBER-LIST% wird zur Vorlagendatei des Geräts hinzugefügt. 2) Das reservierte benutzerdefinierte Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% wird zum vom Gerät verwendeten Tag mit dem Wert 911, 0911, 933 hinzugefügt. 3) Wenn die Datei neu erstellt wird, wird das native Tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% aufgelöst in 911, 0911, 933
%BW-MEMBERTYPE-n%	Dies ist der Typ für jede Zeile. Es kann eines von "Virtuelles Profil", "Benutzer" oder "Ort" sein.
%BWUSEREXTID-n%	Dies ist die externe ID für die angegebene Leitung (nur Webex Calling)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Gibt Informationen an, ob für die entsprechende Leitung eine Anrufübernahmegruppe konfiguriert ist. (Nur Webex Calling)

Cisco – vertraulich

6 Benutzerdefinierte Tags

In diesem Abschnitt werden die benutzerdefinierten Tags beschrieben, die in Webex für Cisco BroadWorks verwendet werden. Sie 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 von der jeweiligen Version des Clients unterstützt werden. Um festzustellen, ob eine Einstellung nicht für eine ältere Client-Version gilt, lesen Sie die entsprechende versionsspezifische Konfigurationsanleitung.

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%ENABLE_REJECT_WITH_486_WXT%	J	J	wahr	*6.1.16 Verhalten beim Ablehnen eingehender Anrufe*
%REJECT_WITH_XSI_MODE_WXT%	N	J	decline_false	*6.3.2 Pushbenachrichtigungen für Anrufe*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	J	beschäftigt	*6.3.2 Pushbenachrichtigungen für Anrufe*
%ENABLE_TRANSFER_CALLS_WXT%	J	J	false	*6.1.20 Übertragen*
%ENABLE_CONFERENCE_CALLS_WXT%	J	J	false	*6.1.21 N-Wege-Konferenzanrufe*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	J	J	false	*6.1.21 N-Wege-Konferenzanrufe*
%MAX_CONF_PARTIES_WXT%	J	J	10	*6.1.21 N-Wege-Konferenzanrufe*
%ENABLE_CALL_STATISTICS_WXT%	J	J	false	*6.1.24 Anrufstatistik*
%ENABLE_CALL_PULL_WXT%	J	J	false	*6.1.22 Anrufübergabe*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	J	false	*6.3.2 Pushbenachrichtigungen für Anrufe*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	J	J	false	*6.1.28 Voicemail-Abschrift für Webex Calling*
%ENABLE_MWI_WXT%	J	J	false	*6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten*
%MWI_MODE_WXT%	J	J	leer	*6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%ENABLE_VOICE_MAIL_WXT%	J	J	false	*6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten*
%ENABLE_VISUAL_VOICE_MAIL_WXT%	J	J	false	*6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten*
%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 Immer Rufumleitung*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	J	J	wahr	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	J	J	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*
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	J	J	false	*6.1.29.3 BroadWorks Anywhere*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%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 Notrufe*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	J	911, 112	*6.3.1 Notrufe*
%ENABLE_USE_RPORT_WXT%	J	J	false	*6.1.14 SIP Rport-Verwaltung für NAT-Traversal*
%RPORT_USE_LOCAL_PORT_WXT%	J	J	false	*6.1.14 SIP Rport-Verwaltung für NAT-Traversal*
%USE_TLS_WXT%	J	J	false	*6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll*
%SBC_ADDRESS_WXT%	J	J	leer	*5.6 System-Standard-Tags*
%SBC_PORT_WXT%	J	J	5060	*5.6 System-Standard-Tags*
%USE_PROXY_DISCOVERY_WXT%	J	J	false	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%USE_TCP_FROM_DNS_WXT%	J	J	wahr	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%USE_UDP_FROM_DNS_WXT%	J	J	wahr	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%USE_TLS_FROM_DNS_WXT%	J	J	wahr	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%DOMAIN_OVERRIDE_WXT%	J	J	leer	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	J	J	wahr	*6.1.6 Dynamische SIP-Proxy-Erkennung*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	J	J	wahr	*6.1.6 Dynamische SIP-Proxy-Erkennung*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%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 Konfigurierbare Zeitüberschreitung beim Öffnen des SIP-Sockets*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	J	J	10000	*6.1.5 Konfigurierbare Zeitüberschreitung beim Öffnen des SIP-Sockets*
%SOURCE_PORT_WXT%	J	J	5060	*6.1.7 Nutzung des bevorzugten Ports* für SIP
%SIP_FAILBACK_ENABLED_WXT%	J	N	wahr	*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. IP-Version durchsetzen*
%USE_ALTERNATIVE_IDENTITIES_WXT%	J	J	false	*6.1.10 P-Associated-URIs im REGISTER verwenden*
%TCP_SIZE_THRESHOLD_WXT%	J	J	18000	*6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen*
%SIP_REFRESH_ON_TTL_WXT%	J	N	false	*6.1.8.4 DNS-TTL-Verwaltung*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	J	J	false	*6.1.12 Unterstützung VON SIP-AKTUALISIERUNGEN*
%ENABLE_PEM_SUPPORT_WXT%	J	J	false	*6.1.11 SIP P-Early Media (PEM)-Header*
%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 sicheres Echtzeit-Transportprotokoll*
%SRTP_MODE_WXT%	J	J	false	*6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%ENABLE_REKEYING_WXT%	J	J	wahr	*6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll*
%RTP_AUDIO_PORT_RANGE_START_WXT%	J	J	8000	*6.1.17 Portbereich des Transportprotokolls in* Echtzeit
%RTP_AUDIO_PORT_RANGE_END_WXT%	J	J	8099	*6.1.17 Portbereich des Transportprotokolls in* Echtzeit
%RTP_VIDEO_PORT_RANGE_START_WXT%	J	J	8100	*6.1.17 Portbereich des Transportprotokolls in* Echtzeit
%RTP_VIDEO_PORT_RANGE_END_WXT%	J	J	8199	*6.1.17 Portbereich des Transportprotokolls in* Echtzeit
%ENABLE_RTCP_MUX_WXT%	J	J	wahr	*6.1.19 RTCP-MUX*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	J	J	wahr	*6.1.33 XSI-Ereigniskanal*
%CHANNEL_HEARTBEAT_WXT%	J	J	10000	*6.1.33 XSI-Ereigniskanal*
%XSI_ROOT_WXT%	J	J	leer (verwendet die ursprüngliche URL)	*6.1.32 XSI-Wurzel und Pfade*
%XSI_ACTIONS_PATH_WXT%	J	J	/com.broadsoft.xsi-actions/	*6.1.32 XSI-Wurzel und Pfade*
%XSI_EVENTS_PATH_WXT%	J	J	/com.broadsoft.xsi-events/	*6.1.32 XSI-Wurzel und Pfade*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	J	J	false	*6.1.25 Automatische Wiederherstellung von Anrufen /Nahtlose Übergabe von Anrufen*
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	J	cs-nur	*6.3.1 Notrufe*
%ENABLE_CALL_PICKUP_BLIND_WXT%	J	N	false	*6.2.2 Anrufannahme*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	J	N	false	*6.2.2 Anrufannahme*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%WEB_CALL_SETTINGS_URL_WXT%	J	J	leer	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%USER_PORTAL_SETTINGS_URL_WXT%	J	J	leer	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%ENABLE_CALL_CENTER_WXT%	J	J	false	*6.1.31 Callcenter/Anrufwarteschlange-Anmeldung/Abmeldung*
%WEB_CALL_SETTINGS_TARGET_WXT%	J	J	Extern	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	J	J	wahr	*6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*
%USE_MEDIASEC_WXT%	J	J	false	*6.1.3 SIP-Header 3GPP für SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	J	false	*6.3.4 Click to Dial (Rückruf)*
%DIALING_CALL_BACK_TIMER_WXT%	N	J	10	*6.3.4 Click to Dial (Rückruf)*
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	J	N	false	*6.2.3 Unterstützung von Chef-Admin (Führungskraft-Assistent)*
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	J	35	*6.3.2 Pushbenachrichtigungen für Anrufe*
%ENABLE_CALL_RECORDING_WXT%	J	J	false	*6.1.26 Anrufaufzeichnung*
%ENABLE_SINGLE_ALERTING_WXT%	N	J	false	*6.3.3 Einzelne* Warnungen
%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)*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%RTP_ICE_MODE_WXT%	J	J	Eissturm	*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 eskalieren*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	J	N	false	*6.2.5 Anrufe mit Steuerung des Tischtelefons* – Automatische Anrufannahme
%ENABLE_DIALING_VOIP_WXT%	N	J	wahr	*6.3.5 MNO-Unterstützung Anrufen mit Native Dialer*
%ENABLE_DIALING_NATIVE_WXT%	N	J	false	*6.3.5 MNO-Unterstützung Anrufen mit Native Dialer*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	J	J	wahr	*6.1.35 SIP-URI-Wahl*
%ENABLE_SIP_VIDEOCALLS_WXT%	J	J	wahr	*6.1.37 Videoanrufe deaktivieren*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	J	J	wahr	*6.1.37 Videoanrufe deaktivieren*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	J	J	Desktop - wahr Handy, Tablet - falsch	*6.1.37 Videoanrufe deaktivieren*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	Y	Mobil – N Tablet – Y	false	*6.1.38 Notrufe (911) – Standortberichte beim E911-Anbieter*

Cisco – vertraulich

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	Y	Mobil – N Tablet – Y	0	*6.1.38 Notrufe (911) – Standortberichte beim E911-Anbieter*
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	Y	Mobil – N Tablet – Y	-1	*6.1.38 Notrufe (911) – Standortberichte beim E911-Anbieter*
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	Y	Mobil – N Tablet – Y	einmal_pro_Anmeldung	*6.1.38 Notrufe (911) – Standortberichte beim E911-Anbieter*
%ENABLE_AUTO_ANSWER_WXT%	J	N	false	*6.2.6 Automatische Anrufannahme mit Tonbenachrichtigung*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	J	J	false	*6.1.41 Spam-Anruf-Anzeige*
%ENABLE_NOISE_REMOVAL_WXT%	J	J	false	*6.1.42 Entfernen von Geräuschen und Erweiterung der* Bandbreite für PSTN-/Mobilanrufe
%ENABLE_AUDIO_MARI_FEC_WXT%	J	J	false	*6.1.46.2 Korrektur von Weiterleitungsfehlern (Forward Error Correction,* FEC) und Packet Retransmission (Packet Retransmission, RTX)
%ENABLE_AUDIO_MARI_RTX_WXT%	J	J	false	*6.1.46.2 Korrektur von Weiterleitungsfehlern (Forward Error Correction,* FEC) und Packet Retransmission (Packet Retransmission, RTX)
%ENABLE_VIDEO_MARI_FEC_WXT%	J	J	false	*6.1.46.2 Korrektur von Weiterleitungsfehlern (Forward Error Correction,* FEC) und Packet Retransmission (Packet Retransmission, RTX)
%ENABLE_VIDEO_MARI_RTX_WXT%	J	J	false	*6.1.46.2 Korrektur von Weiterleitungsfehlern (Forward Error Correction,* FEC) und Packet Retransmission (Packet Retransmission, RTX)
%ENABLE_CALL_BLOCK_WXT%	J	J	false	*6.1.45 Sperrliste (nur Webex Calling)*
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	J	wahr	*6.3.5.6 MNO-Mobilität – Widget im Anruf*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	J	wahr	*6.3.5.6 MNO-Mobilität – Widget im Anruf*
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	J	wahr	*6.3.5.6 MNO-Mobilität – Widget im Anruf*
%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	*6.2.11 Event-Paket für Remote-Stummschaltungssteuerung (nur Webex Calling)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	J	J	wahr	*6.1.29.2 Anrufweiterleitung an Voicemail*
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	J	J	wahr	*6.1.8.1 SIP-Failover*
%ENABLE_CALL_MOVE_HERE_WXT%	J	N	false	*6.2.12 Anruf verschieben*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	J	J	false	*6.1.42 Entfernen von Geräuschen und Erweiterung der* Bandbreite für PSTN-/Mobilanrufe
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	J	leer	*6.3.5.1 Anrufen mit Native Dialer*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	J	J	false	*6.1.20 Übertragen*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	J	J	wahr	*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* *Ausgehende Anrufer-ID*

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	J	false	*6.1.50 Anrufer-ID Ausgehende Anrufer-ID*
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	J	false	*6.1.50 Anrufer-ID Ausgehende Anrufer-ID*
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	J	false	*6.1.50 Anrufer-ID Ausgehende Anrufer-ID*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	J	false	*6.1.50 Anrufer-ID Ausgehende Anrufer-ID*
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	J	J	false	*6.1.49 Informationen zur Anrufweiterleitung*
%ENABLE_BUSY_LAMP_FIELD_WXT%	J	N	false	*6.2.8.1 Besetztlampenfeld*
%ENABLE_BLF_DISPLAY_CALLER_WXT%	J	N	wahr	*6.2.8.1 Besetztlampenfeld*
%BLF_NOTIFICATION_DELAY_TIME_WXT%	J	N	0	*6.2.8.1 Besetztlampenfeld*
%ENABLE_GCP_NOTIFICATIONS_WXT%	J	N	false	*6.2.8.2 Anrufannahmegruppe (nur Webex Calling)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	J	N	false	*6.2.8.2 Anrufannahmegruppe (nur Webex Calling)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	J	N	120	*6.2.8.2 Anrufannahmegruppe (nur Webex Calling)*
%UDP_KEEPALIVE_ENABLED_WXT%	J	J	wahr	*6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen*
%TCP_KEEPALIVE_ENABLED_WXT%	J	J	false	*6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen*
%TLS_KEEPALIVE_ENABLED_WXT%	J	J	false	*6.1.4 TCP-, TLS- oder UDP-Nutzung und Keepalives erzwingen*
%ENABLE_MULTI_LINE_WXT%	J	J	false	*6.1.51 Mehrere* Leitungen

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	J	false	*6.2.4 SIP-Anrufe an Meeting eskalieren (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	J	false	*6.3.5.3 Identität der ausgehenden Anrufleitung (Outgoing Calling Line Identity,* CLID) – Dual Persona
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	J	false	*6.3.5.36.3.5.3 CLID (Identity der ausgehenden Anrufleitung)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	J	J	gelöst	*6.1.50.2 Name der Remote-Anrufer-ID*
%PERSONAL_ASSISTANT_ENABLED_WXT%	J	J	false	*6.1.53 Persönlicher Assistent (Abwesenheitsstatus)*
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	J	NPS	*Bereitstellungsmodus (nur Webex Calling)*
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	J	J	false	*6.1.52 Verbesserte SIP-Autorisierung*
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	J	J	false	*6.1.21 N-Wege-Konferenzanrufe*
%CALL_PULL_MODE_WXT%	J	J	blind	*6.1.22 Anrufübergabe*
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	J	N	Anruf_verschieben	*6.1.22 Anrufübergabe*
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	J	J	false	*6.1.36 Anrufprotokoll*
%ENABLE_EMERGENCY_LOCATION_WXT%	Y	Mobil – N Tablet – Y	false	
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	Y	Mobil – N Tablet – Y	0	

Markierung	Verwendet in Desktop	Verwendet in Mobile/ Tablet	Standardwert	Abschnitt
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	Y	Mobil – N Tablet – Y	-1	
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	Y	Mobil – N Tablet – Y	einmal_pro_Anmeldung	
%ENABLE_CALLS_E2EE_WXT %	J	J	false	*Durchgängige Verschlüsselung (nur Webex Calling)*

Weitere Informationen zur Zuordnung der in Webex for Cisco BroadWorks verwendeten benutzerdefinierten Tags mit den von UC-One verwendeten finden Sie im Abschnitt *0 Benutzerdefinierte Tags-Zuordnung zwischen Webex for Cisco BroadWorks und UC-One*.

Cisco – vertraulich

6.1 Gemeinsame Merkmale

6.1.1 SIP-Server-Einstellungen

Der Client wird 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. Dies wird als Domänenteil der eigenen SIP-URI (die eigene SIP-URI wird manchmal auch als Leitungsport bezeichnet) im Allgemeinen in SIP-Headern und in Remote- (XSI-)Anrufen verwendet. Der Benutzerteil des eigenen SIP-URI stammt über die Konfiguration der SIP-Anmeldeinformationen (Parameter unter).
- SIP-Server-URI oder IP-Adresse des SIP-Proxyservers, falls die DNS-Auflösung fehlschlägt. Beachten Sie, dass für die Verwendung von TLS keine IP-Adressen im Proxy-Parameter verwendet werden können, da die Validierung des TLS-Zertifikats 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 für die Proxy-Adresse verwendet wird. Im Allgemeinen ist es aus diesen Gründen nicht empfehlenswert, in diesem Feld eine IP-Adresse zu verwenden.

Andere Parameter können ebenfalls geändert werden, um verschiedene Funktionen für den Anruf zu aktivieren. Die bisherigen Einstellungen ermöglichen jedoch folgende Grundfunktionen:

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

Sobald die SIP-Registrierung aktiviert ist, muss die Aktivierung von SIP SUBSCRIBE für MWI über separate Konfigurationsparameter erfolgen. Weitere Informationen zu Voicemail finden Sie im Abschnitt *6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten*.

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

Die Einrichtung der SIP-Server folgt diesem Grundschema:

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

Außerdem werden die SIP-Timer in der Konfigurationsdatei angezeigt (es wird nicht empfohlen, sie zu ändern).

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


Cisco – vertraulich

```
    </timers>
```

- T1 - die Zeitspanne in Millisekunden für eine Verzögerung beim Netzrundlauf.
- T2 - die maximale Zeitspanne in Millisekunden, bevor Nicht-Einladungsanfragen und Einladungsantworten erneut gesendet werden.
- T4 - die maximale Zeitspanne in Millisekunden, die eine Nachricht im Netz verbleibt.

Jede Leitung hat eigene Parameter wie die Voicemail-Nummer, die Konferenz-URI und die Domain sowie die SIP-Authentifizierungsdaten. Für die 401- und 407-Signalisierung können bei Bedarf getrennte Anmeldeinformationen konfiguriert werden.

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

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%BWLINEPORT-n%	leer	Schnur	Typischerweise SIP-Benutzername. Weitere Informationen finden Sie im Abschnitt *5.7 Cisco BroadWorks Dynamic integrierte System-Tags*. Beispiel: johndoe
%BWAUTHPASSWORD-n%	leer	Schnur	Typischerweise SIP-Passwort. Weitere Informationen finden Sie im Abschnitt *5.7 Cisco BroadWorks Dynamic integrierte System-Tags*. Beispiel: Geheimpasswort
%BWE164-n%	leer	Telefonnummer	Standardtelefonnummer für den Benutzer im internationalen Format. Weitere Informationen finden Sie im Abschnitt *5.7 Cisco BroadWorks Dynamic integrierte System-Tags*. Beispiel: 12345678
%SBC_ADDRESS_WXT%	leer	Schnur	Weitere Informationen finden Sie im Abschnitt *5.6 System-Standard-Tags*. Beispiel: sbcexample.domain.com
%SBC_PORT_WXT%	5060	Nummer	Weitere Informationen finden Sie im Abschnitt *5.6 System-Standard-Tags*. Beispiel: 5060
%BWHOST-n%	leer	Schnur	In der Regel als SIP-Domäne verwendet. Weitere Informationen finden Sie im Abschnitt *5.7 Cisco BroadWorks Dynamic integrierte System-Tags*. Beispiel: exampledomain.com
%SOURCE_PORT_WXT%	5060	Nummer	Wird in der Regel für den Parameter *preferred-port* verwendet. Weitere Informationen finden Sie in Abschnitt *6.1.7 Nutzung des bevorzugten Ports* für SIP. Beispiel: 5061
%BWUSEREXTID-n%	leer	Schnur	(Nur Webex Calling) Enthält die externe ID der Leitung Weitere Informationen finden Sie unter *6.1.51 Mehrere Leitungen*. Beispiel: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

Cisco – vertraulich

HINWEIS: Es empfiehlt sich dringend, dass der SIP-Port von 5060 abgesehen wird (z. B. 5075), da bekannte Probleme mit der Verwendung des Standard-SIP-Ports (5060) bei mobilen Geräten bekannt sind.

6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll

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

Wenn die dynamische Proxy-Erkennung nicht verwendet wird, wird sie durch die Aktivierung von TLS für SIP aktiviert.

Weitere Informationen zu den Empfehlungen für den SIP-Port und das Transportprotokoll bei der Verwendung von SIP-ALGs im Netzwerk finden Sie im *Webex für Cisco BroadWorks-Lösungsleitfaden*.

Beachten Sie, dass das verwendete Zertifikat gültig sein muss. Außerdem muss die Zertifikatskette intakt sein, damit auch das Zwischenzertifikat verlinkt 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 Desktop-Rechner hinzuzufügen, entweder manuell oder durch Massenbereitstellung, obwohl dies normalerweise nicht gemacht wird.

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

Zusätzlich zu RTP kann der RTCP-Verkehr mit denselben Mechanismen wie RTP gesichert werden, indem die oben beschriebene Konfiguration verwendet wird.

Für SIP/TLS-Chiffren siehe *Anhang A: TLS-Schlüssel.*

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

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

Die aktuelle Version des Medien-Frameworks unterstützt AES 128 Counter Mode zum Schutz und Hash Message Authentication Code (HMAC)-SHA-1 zur Authentifizierung. Der Hauptschlüssel hat eine Größe von 16 Byte und das Hauptsalz von 14 Byte.

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

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

Mehrzeilige SDP-Verfahren im Zusammenhang mit SRTP sind implementiert, so dass immer mehrere m-Leitungen verwendet werden. Es werden getrennte m-Zeilen für AVP und SAVP verwendet.

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

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

Der SBC kann auch die Reihenfolge der SDP-m-Zeilen beim Rufaufbau ändern, indem er die AVP- (nicht verschlüsselt) oder SAVP- (verschlüsselt) m-Zeile an die erste Stelle setzt. Daher werden Clients, die die erste funktionierende m-Leitung wählen, dazu gebracht, entweder verschlüsselten oder unverschlüsselten Verkehr zu bevorzugen. Die verschiedenen SRTP-Konfigurationsoptionen sind wie folgt:

- Obligatorisch - Beim Verbindungsaufbau enthält das anfängliche SDP nur die SAVP-m-Leitung, wenn es angeboten wird, und der Client akzeptiert nur die SAVP-m-Leitung im SDP, wenn er antwortet, so dass nur SRTP-Anrufe möglich sind.
- Bevorzugt - Beim Rufaufbau enthält das anfängliche SDP sowohl die AVP- als auch die SAVP-m-Zeilen, aber SAVP steht beim Angebot an erster Stelle, was die Reihenfolge der Bevorzugung angibt. Bei der Beantwortung wählt der Client SAVP, falls verfügbar, auch wenn es nicht die erste m-Leitung ist (gemäß den SIP-Spezifikationen wird die Reihenfolge der m-Leitungen bei der Beantwortung nicht geändert).
- Optional: Beim Anruf-Setup umfasst das anfängliche SDP beim Angebot sowohl die SAVP- als auch die AVP-M-Leitungen, aber AVP gibt zuerst die Reihenfolge der Präferenz an. Bei der Beantwortung wählt der Kunde die erste m-Leitung, AVP oder SAVP.
- SRTP nicht aktiviert - Es gibt keine SAVP m-Zeile in der anfänglichen SDP beim Angebot. Beim Beantworten wird SAVP nicht akzeptiert, daher sind nur RTP-Anrufe möglich.
- Transport - Automatische Auswahl des SRTP-Modus auf der Grundlage des Transportprotokolls. Wenn TLS verwendet wird, ist der obligatorische SRTP-Modus aktiviert. Wenn TCP oder UDP verwendet wird, wird kein SRTP eingesetzt.

SRTP und RTP sind in beide Richtungen des Anrufs symmetrisch, d. h. Sende- und Empfangsprofil sind gleich.

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

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

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

In einigen Bereitstellungen wird die Wiederholung des Schlüssels für SRTP nicht unterstützt. Daher gibt es einen Konfigurationsparameter zum Aktivieren/Deaktivieren der SRTP-Wiederholungskennzeichnung. 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	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%USE_TLS_WXT%	false	wahr, falsch	Bei der Einstellung "false" ist SIP TLS deaktiviert. Wenn „true“ (wahr) festgelegt ist, wird SIP TLS aktiviert. Bitte beachten Sie, dass dieser Parameter ignoriert wird, wenn *6.1.6 Dynamische SIP-Proxy-Erkennung* verwendet wird.
%SRTP_ENABLED_WXT%	false	wahr, falsch	Wenn der Wert auf „false“ festgelegt ist, wird SRTP deaktiviert. Wenn „true“ festgelegt ist, ist SRTP aktiviert.
%SRTP_MODE_WXT%	optional	obligatorisch, bevorzugt, fakultativ, Transport	Legt fest, wie bevorzugt SRTP beim Verbindungsaufbau ist. Der Standardwert ist "optional".
%ENABLE_REKEYING_WXT%	wahr	wahr, falsch	Aktiviert SIP (SDP) Re-Keying für SRTP.

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

6.1.3 SIP-Header 3GPP 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 im Folgenden:

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

Cisco – vertraulich

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

Nur die Verwendung der Kopfzeilen ist konfigurierbar. Für einzelne Kopfzeilen gibt es keine weiteren Konfigurationsmöglichkeiten. Alle Kopfzeilen sind entweder aktiviert oder deaktiviert.

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

Das folgende Tag steuert diese Fähigkeit.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%USE_MEDIASEC_WXT%	false	wahr, falsch	Aktiviert 3GPP-SIP-Header für die SRTP-Aushandlung.

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

Der Webex für Cisco BroadWorks-Client kann so konfiguriert werden, dass entweder TCP, TLS oder UDP für SIP-Signalisierung und RTP-Medien verwendet werden. Beachten Sie, dass der Client standardmäßig auf TCP eingestellt ist. Beachten Sie auch, dass ohne TCP-Keepalive SIP-TCP-Verbindungen nach einer gewissen Zeit der Inaktivität geschlossen werden.

Im folgenden Beispiel wird dieser Konfigurationsknoten dargestellt.

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte (Byte)	Beschreibung
%TCP_SIZE_THRESHOLD_WXT%	0	0	Erzwingt die Verwendung von TCP. Die Entscheidung über die Verwendung von TCP oder UDP für den Client liegt beim Dienstanbieter; empfohlen wird jedoch die Verwendung von TCP mit dem Standardwert "0".
	0	1 - 99,000	Erzwingt die Verwendung von UDP, wenn die Nachrichtengröße unter dem hier angegebenen Wert liegt. Die Standardeinstellung ist TCP, wenn die Nachrichtengröße größer als der eingestellte Wert ist. Für die Verwendung von UDP ist 1500 die Standardempfehlung.
	0	100000	Erzwingt die Verwendung von UDP.

Cisco – vertraulich

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

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

Die möglichen Parameter sind:

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

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

Die Server-IP-Adresse und der Port für Keepalives werden mit den normalen Verfahren für die SIP-Proxy-Ermittlung ermittelt. Beachten Sie, dass die SIP-Ports und die Auswahl des Transportprotokolls, die über die dynamische SIP-Proxy-Ermittlung ermittelt werden, jede statische Port- oder Transportkonfiguration außer Kraft setzen. Weitere Informationen zur dynamischen Proxy-Erkennung finden Sie im Abschnitt *6.1.6 Dynamische SIP-Proxy-Erkennung.*

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%UDP_KEEPALIVE_ENABLED_WXT%	wahr	wahr, falsch	Steuert, ob die Keep-Alive-Pakete für den UDP-Transport gesendet werden sollen.
%TCP_KEEPALIVE_ENABLED_WXT%	false	wahr, falsch	Steuert, ob die Keep-Alive-Pakete für den TCP-Transport gesendet werden sollen.
%TLS_KEEPALIVE_ENABLED_WXT%	false	wahr, falsch	Steuert, ob die Keep-Alive-Pakete für den TLS-Transport gesendet werden sollen.

6.1.5 Konfigurierbare Zeitüberschreitung beim Öffnen des SIP-Sockets

Zuvor war die Zeitüberschreitung für das Öffnen eines SIP-Sockets auf 5 Sekunden für TCP und 10 Sekunden für TLS fest einprogrammiert. Diese Zeitüberschreitungen sind jetzt konfigurierbar.

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

Die folgenden Tags steuern den Timeout der Socket-Verbindung (in Millisekunden).

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	- die Zeitüberschrei	Die Zeitüberschreitung der Socket-Verbindung, wenn der TCP-Transport verwendet wird.

Cisco – vertraulich

		tung in Millisekunden	
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	- die Zeitüberschreitung in Millisekunden	Die Zeitüberschreitung bei der Steckplatzverbindung, wenn der TLS-Transport verwendet wird.

6.1.6 Dynamische SIP-Proxy-Erkennung

Das folgende Beispiel zeigt, wie Sie die dynamische SIP-Proxy-Erkennung aktivieren.

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

Es ist möglich zu steuern, welche Transportprotokolleinträge aus DNS SRV verwendet werden, wenn viele Einträge vorhanden sind, indem die in diesem Abschnitt beschriebenen Verfahren befolgt werden.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%USE_PROXY_DISCOVERY_WXT%	false	wahr, falsch	Ermöglicht die dynamische SIP-Proxy-Erkennung für Audio- und Videoanrufe. Der empfohlene Wert ist "true".
%SBC_ADDRESS_WXT%	leer	String	Dieses Cisco BroadWorks-Tag wird normalerweise für den Parameter "Datensatzname" verwendet. Es sollte sich um eine gültige URL handeln, nicht um eine IP-Adresse. Weitere Informationen finden Sie im Abschnitt *5.6 System-Standard-Tags*. Beispiel: sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	leer	String	Dieses benutzerdefinierte Tag wird für den Domain-Override verwendet. Weitere Informationen finden Sie im folgenden Abschnitt. Beispiel: other.domain.com
%USE_TCP_FROM_DNS_WXT%	wahr	wahr, falsch	Wenn dieser Parameterwert "false" ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (TCP) verworfen. Wenn "true", dann werden die Ergebnisse von DNS SRV für dieses Transportprotokoll (TCP) verwendet. Je nach den SRV-Prioritäten kann noch ein anderer Transport gewählt werden.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%USE_UDP_FROM_DNS_WXT%	wahr	wahr, falsch	Wenn dieser Parameterwert „false“ ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (UDP) verworfen. Wenn „true“ (wahr) lautet, werden die Ergebnisse von DNS SRV für dieses Transportprotokoll (UDP) verwendet. Je nach den SRV-Prioritäten kann noch ein anderer Transport gewählt werden.
%USE_TLS_FROM_DNS_WXT%	wahr	wahr, falsch	Wenn dieser Parameterwert „false“ ist, werden die DNS SRV-Ergebnisse für dieses Transportprotokoll (TLS) verworfen. Bei „true“ (wahr) werden die Ergebnisse aus dem DNS für dieses Transportprotokoll (TLS) verwendet. Je nach den SRV-Prioritäten kann noch ein anderer Transport gewählt werden.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	wahr, falsch	wahr	Aktiviert/deaktiviert den DNS-Backup-Dienst. Wenn diese Option aktiviert ist, wird die A/AAAA-Auflösung für die SIP-Proxy-Adresse durchgeführt. Sie wird nur berücksichtigt, wenn die SRV/NAPTR-Dienstsuche aktiviert ist.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	wahr, falsch	wahr	Wenn auf "true" gesetzt und die NAPTR-Dienstsuche fehlschlägt oder keine Ergebnisse liefert, wird die SRV-Dienstsuche für den konfigurierten Host durchgeführt. Wenn sie auf "false" gesetzt ist, wird keine SRV-Ermittlung durchgeführt.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	wahr, falsch	false	Ermöglicht die Umgehung des DNS-Caches des Betriebssystems.

Über DNS kann der Client die IP-Adresse, den Port und das Transportprotokoll für den SIP-Proxy gemäß RFC 3263 abrufen.

DNS SRV, Naming Authority Pointer (NAPTR) und A-record-Abfragen werden unterstützt. Bei der Anmeldung sieht der 3-Schritt-Ablauf wie folgt aus:

1. Führen Sie mithilfe des obigen Felds eine NAPTR-Abfrage durch, um die Server-URIs mit den Transportprotokollen abzurufen, falls diese vorhanden sind. Der Wert für den Parameter muss die vollständige Domäne sein, die DNS auflösen soll, und darf keine IP-Adresse sein.
2. Lösen Sie die in der NAPTR-Abfrage gefundenen Elemente mit einer SRV-Abfrage auf, um die endgültige Server-URI und den Port zu erhalten. Der in der SRV-Abfrage verwendete Domänenteil wird dem Ergebnis der NAPTR-Abfrage entnommen, um den endgültigen Server-URI (und Port) zu finden. Der von der DNS-SRV-Abfrage empfangene Port wird verwendet, wenn die DNS-SRV-Einträge verfügbar sind. Beachten Sie, dass der Port nur in der Konfigurationsdatei für den statischen Proxy in der Konfigurationsdatei gilt und nicht für die URIs, die mit SRV aufgelöst werden. In den folgenden Beispielen wird die Verwendung der verschiedenen Datensatznamen erläutert.

Wenn kein NAPTR gefunden wird, versucht der Client eine SRV-Abfrage mit dem Datensatznamen aus dem Parameter , es sei denn, der Parameter ist vorhanden. In diesem Fall wird verwendet und versucht automatisch, separate Einträge für TCP, UDP und TLS zu finden (_sip_protocol [UDP, TCP oder TLS]). Beachten Sie, dass das Stream Control Transmission Protocol (SCTP) nicht unterstützt wird. Wenn SRV-Abfragen keine Ergebnisse liefern, schlägt die Proxy-Ermittlung fehl, und der Endbenutzer erhält eine Fehlermeldung, die besagt, dass keine Anrufe verfügbar sind. In diesem Fall findet keine SIP-Registrierung statt. Selbst wenn jedoch alle SRV-Abfragen fehlschlagen oder die dort empfangenen Server nicht funktionieren, prüft der Client weiterhin, ob der konfigurierte statische Proxy funktioniert, nur mit A-Abfragen an den URI, der in der angegeben ist, um zu sehen, ob er eine IP-Adresse liefert, die eine funktionierende SIP-Registrierung bereitstellt. Port und Transport stammen in diesem letzten Ausweg aus den Parametern tcp-threshold und .

3. Auflösung der gefundenen URIs mit Hilfe der A-Record-Abfrage. Die empfangenen endgültigen IP-Adressen werden in der Reihenfolge ihres Empfangs ausprobiert, um eine funktionierende Verbindung zum SIP-Proxy herzustellen. Diese Reihenfolge kann vom Dienstanbieter im DNS festgelegt werden. Der erste SIP-Proxy-URI mit einem erfolgreichen A-Record-Lookup wird ausgewählt und so lange verwendet, bis er nicht mehr funktioniert oder sich der Client abmeldet. Bei der A-Abfrage wird jeweils nur eine IP-Adresse verwendet, auch wenn viele empfangen werden. Alle SRV-Einträge werden jedoch bis zur Abmeldung oder dem Verlust des Netzwerks aufgelöst.

Wichtige Hinweise

HINWEIS 1: Wenn die DNS-Proxy-Ermittlung im SRV-Schritt zur Auswahl des Transportprotokolls führt, indem ein funktionierender SIP-Proxy-URI für ein Transportprotokoll empfangen wird, setzt sie den Parameter *tcp-threshold* außer Kraft, der normalerweise zur Auswahl von UDP oder TCP in der Konfigurationsdatei verwendet wird. Das Gleiche gilt auch für die Konfiguration von SIP/TLS. Je nach Priorität im DNS wird TCP oder UDP verwendet.

HINWEIS 2: Über SRV empfangene Elemente werden gegenüber dem statischen Proxy in der Konfigurationsdatei priorisiert. Die NAPTR-Reihenfolge wird nicht beachtet; es zählt nur die SRV-Priorität. Wenn SRV mehrere Einträge mit gleichem Transportprotokoll, gleicher Priorität und gleichem Gewicht ergibt, wird ein beliebiger eingegangener Eintrag zufällig ausgewählt. NAPTR-Gewichte werden in dieser Version nicht unterstützt, SRV-Gewichte hingegen schon. Die SRV-Priorität wird zuerst betrachtet, und bei Elementen mit gleicher Priorität wird die Gewichtung betrachtet, um die Wahrscheinlichkeit zu bestimmen, mit der ein bestimmter Server als nächstes versucht wird.

ANMERKUNG 3: Der optionale Parameter *domain-override* ermöglicht es, dass ein anderer A-Record-Name als der im SIP-Domain-Konfigurationsparameter angegebene mit SRV aufgelöst wird, wenn NAPTR-Ergebnisse weggelassen werden. Siehe die folgenden Beispiele für die Verwendung des Parameters *domain-override* .

ANMERKUNG 4: Der Client verwendet Betriebssystemprimitive für DNS-Operationen, und in der Regel werden DNS-Antworten zwischengespeichert, um die TTL der DNS-Antwort einzuhalten.

ANMERKUNG 5: Der DNS-Typ (Dienst) für NAPTR-Einträge muss dem *RFC 3263* Verfahren entsprechen, andernfalls kann die DNS-Auflösung fehlschlagen. Für SIP über TLS ist zum Beispiel die Verwendung von SIPS+D2T erforderlich.

ANMERKUNG 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 Diensttyp übereinstimmt, wird dieser Datensatz ignoriert.

Beispiel 1: Verwendung der DNS-Proxy-Ermittlung ohne den Konfigurationsparameter domain-override

Es folgt ein Beispiel für eine Konfiguration mit SIP-Proxy-Erkennung, wenn nur SIP über TCP verwendet wird und die NAPTR-Abfrage in Schritt 1 Ergebnisse liefert.

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

Daraus ergeben sich die folgenden Schritte auf der Protokollebene.

```
1. NAPTR query for record-domain.com, answer:
record-domain.com.
28591 IN NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.
2. SRV query for _sip._tcp.test.sip.record-domain.com (received in the NAPTR
query), answer
_sip._tcp.test.sip.record-domain.com. 28635 IN SRV
10 10 5061 test.sipgeo.record-domain.com.
3. A-record query for test.sipgeo.record-domain.com, answer:
test.sipgeo.record-domain.com. 16 IN A 1.2.3.4
```

Daher erfolgt die SIP-Registrierung über TCP unter Verwendung des Ports 5061 (der im SRV-Schritt empfangen wurde) und in Richtung der IP-Adresse 1.2.3.4.

Beispiel 2: **Verwendung des Parameters domain-override in der Konfigurationsdatei**

Es folgt ein zweites Beispiel für eine Konfiguration mit SIP-Proxy-Erkennung, bei der die SIP-Domäne nicht mit der Proxy-Domäne übereinstimmt und nur SIP über UDP verwendet wird und die NAPTR-Abfrage keine Ergebnisse liefert.

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

Dies führt zu den folgenden Schritten auf Protokollebene.

Cisco – vertraulich

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

Infolgedessen erfolgt die SIP-Registrierung über UDP mithilfe des Ports 5061 (im SRV-Schritt empfangen) und in Richtung der IP-Adresse 4.3.2.1.

Beispiel 3: **SRV-Prioritäten verwenden**

Im Folgenden sehen Sie ein weiteres Beispiel für eine Konfiguration, bei der die SIP-Proxy-Erkennung verwendet wird, wenn nur SIP über TCP verwendet wird und die NAPTR-Abfrage im Schritt 1 Ergebnisse liefert, aber mehrere NAPTR- und SRV-Datensätze mit unterschiedlichen Prioritäten empfangen werden. In diesem Fall spielt nur die SRV-Priorität eine Rolle, obwohl auch mehrere NAPTR-Einträge mit unterschiedlichen Prioritäten empfangen werden.

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

Dies führt zu den folgenden Schritten auf Protokollebene.

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

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

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

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

Daher erfolgt die SIP-Registrierung über TCP mithilfe des Ports 5061 (der im SRV-Schritt empfangen wurde) und in Richtung der IP-Adresse 1.2.3.4, die sowohl UDP als auch TCP unterstützt.

Beispiel 4: Verwendung der DNS-Proxy-Ermittlung mit NAPTR, wenn der Dienst nicht dem Diensttyp entspricht

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

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

Daraus ergeben sich die folgenden Schritte auf der Protokollebene.

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

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

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

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

Daher erfolgt die SIP-Registrierung über TCP unter Verwendung des Ports 5061 (der im SRV-Schritt empfangen wurde) und in Richtung der IP-Adresse 1.2.3.4.

6.1.7 Nutzung des bevorzugten Ports für SIP

Es gab einige Fälle, in denen ein anderes Softwarepaket auf demselben Rechner wie der Client ausgeführt wurde und den Standard-SIP-Port belegte. Um den Client so zu konfigurieren, dass er einen anderen Port für SIP verwendet, kann der Parameter *preferred-port* verwendet werden. Der Client versucht, den konfigurierten Portwert zu verwenden, der im Parameter *preferred-port* angegeben ist. Ist dieser jedoch besetzt, versucht der Client schrittweise Portwerte oberhalb des konfigurierten Wertes. Wenn z. B. der Wert des *preferred-port* "6000" ist und dieser Port belegt ist, versucht der Client 6001, 6002, 6003 usw., bis er einen freien Port findet. Sobald ein ungenutzter Anschluss gefunden wird, wird dieser für die eigene SIP-Kommunikation verwendet.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%SOURCE_PORT_WXT%	5060	Nummer	Gibt den bevorzugten lokalen SIP-Port für die Kommunikation an. Beispiel: 5060

Cisco – vertraulich

6.1.8 SIP-Failover und Failback

Für SIP-Failover und Failback gelten die Cisco BroadWorks-Verfahren. Hierfür muss mehr als ein Proxy (in der Regel der SBC) konfiguriert werden.

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

- Die SIP-Proxy-Ermittlung ist aktiviert und der DNS-Server verfügt über NAPTR- und/oder SRV-Einträge für den FQDN des SBC (siehe Abschnitt *6.1.6 Dynamische SIP-Proxy-Erkennung*), ODER
- Die SIP-Proxy-Adresse wird als FQDN angegeben und kann in mehrere IP-Adressen aufgelöst werden (siehe Abschnitt *6.1.1 SIP-Server-Einstellungen*).

Der DNS-Cache des Betriebssystems wird verwendet, um unnötigen DNS-Verkehr zu vermeiden. Es gibt keine
fest kodierte Grenze für die maximale Anzahl von IP-Adressen in der Liste.

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

6.1.8.1 SIP-Failover

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

- Socket-Fehler - wenn der Socket zwischen dem Client und dem Server unterbrochen oder geschlossen wird, z. B. bei einem Verlust der Netzwerkverbindung, reagiert der Client sofort und löst einen Failover aus.
- Timeout (z. B. wenn der SBC sich aufhängt) - basierend auf dem SIP T1:
  - SIP INVITE - wenn die INVITE-Anfrage eine Zeitüberschreitung aufweist, meldet sich der Client beim nächsten verfügbaren SBC (IP) an und versucht die INVITE-Anfrage erneut.
  - Eine weitere SIP-Anfrage - der Client versucht, sich beim nächsten verfügbaren SBC (IP) zu registrieren.
- Definitive Fehlerantwort vom Server erhalten:
  - Die folgenden SIP-Fehlerantworten des Servers auf ein SIP REGISTER lösen ein Failover aus:
    - 5xx
    - 6xx
  - Die folgenden SIP *4xx* Antworten auf SIP REGISTER führen nicht zum Failover:
    - 401 nicht berechtigt
    - 403 Verboten
    - 404 nicht gefunden
    - 407 Proxy-Authentifizierung erforderlich
    - 423 Intervall zu kurz

Cisco – vertraulich

- Außerdem lösen *4xx* Fehlerantworten auf SIP INVITE kein Failover aus, aber *5xx* und *6xx* schon.

Wenn ein Failover ausgelöst wird, nimmt der Client die nächste verfügbare IP-Adresse aus der Liste. Der SIP-T1-Timer legt fest, wie lange ein Proxy auf der Liste ausprobiert wird, bevor zum nächsten gewechselt wird. Normalerweise wird ein Wert von 32 Sekunden verwendet (64*T1). Wenn alle IP-Adressen fehlschlagen, zeigt der Client einen Fehler auf der Benutzeroberfläche für die SIP-Konnektivität an. Wenn zum Zeitpunkt des Failover ein VoIP-Gespräch geführt wird, wird dieses beendet.

Die SIP-Failover-Logik hängt von mehreren Konfigurationsparametern ab:

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

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

  - T1 - die Zeitspanne in Millisekunden für eine Verzögerung beim Netzrundlauf.
  - T2 - die maximale Zeitspanne in Millisekunden, bevor Nicht-Einladungsanfragen und Einladungsantworten erneut gesendet werden.
  - T4 - die maximale Zeitspanne in Millisekunden, die eine Nachricht im Netz verbleibt.
- SIP-Proxy-Adresse und SIP-Proxy-Ermittlung
  - Siehe Abschnitt *6.1.1 SIP-Server-Einstellungen*.
  - Siehe Abschnitt *6.1.6 Dynamische SIP-Proxy-Erkennung*.
- Failover-Konfiguration registrieren (siehe unten)

Bei einem Failover sendet die Webex-Anwendung SIP REGISTER mit zwei Kontakt-Kopfzeilen – einen für die alte Sitzung und einen mit den neuen Geräteinformationen. Der Kontakt-Header für die alte Sitzung ist enthalten, um den SBC zu informieren, die Daten zu bereinigen. Diese Kopfzeile enthält expires=0 und q=0,5.

Die Kopfzeile „Kontakt“ mit den neuen Geräteinformationen hat ebenfalls q-Wert, der aus dem Tag gelesen wird. Der Tag-Wert wird verwendet, um die Präferenz oder Priorität einer bestimmten Kontaktadresse anzugeben. Er reicht von 0 bis 1,0, wobei 1,0 die höchste und 0 die niedrigste Präferenz darstellt. Dieses Tag hat kein benutzerdefiniertes Tag zur Steuerung des Wertes - es ist fest auf 1,0 kodiert. Der Wert kann manuell angepasst werden, wenn der im Einsatz verwendete SBC über eine umgekehrte Logik verfügt und q=0,0 mit höchster Priorität behandelt.

Ab Version 42,11wird ein neuer Abschnitt in der Konfigurationsvorlage eingeführt. Es wurde ein neuer konfigurierbarer Parameter hinzugefügt, mit dem gesteuert wird, ob die Anwendung die Kopfzeile „Contact“ sendet, um die alten Geräteinformationen zu bereinigen. Einige SBCs bereinigen die alte Sitzung sofort beim Trennen des Sockets, so dass die Existenz des Kontakt-Headers für die alte Sitzung nicht erforderlich ist. Standardmäßig ist die Logik zur Bereinigung der Registrierung aktiviert.

Aus Gründen der Einheitlichkeit wird das Tag auch unter denselben Abschnitt verschoben.

Beispiel

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	wahr	wahr, falsch	Steuert die Bereinigung alter Geräteinformationen im Falle eines SIP-Failover.

6.1.8.2 SIP-Failback

Wenn der Client mit einem Proxy verbunden ist, der nicht an erster Stelle der Prioritätenliste steht, versucht er, sich erneut mit der IP-Adresse mit der höchsten Priorität zu verbinden. Die Zeit für den Failback richtet sich nach der Konfiguration der DNS-TTL-Verwaltung (siehe Abschnitt *6.1.8.4 DNS-TTL-Verwaltung*). Wenn bei Erreichen des Failback-Timers ein Anruf läuft, wartet der Client, bis alle Anrufe beendet sind, und löst dann das Failback-Verfahren aus. Beachten Sie, dass dies nur für Desktop-Clients gilt, da die SIP-Verbindung nur während eines Anrufs auf dem Mobiltelefon aktiv ist.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%SIP_FAILBACK_ENABLED_WXT%	wahr	wahr, falsch	Aktiviert/deaktiviert SIP-Failback.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Über 60	Die SIP-Failback-Zeitüberschreitung in Sekunden.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	wahr, falsch	Fügt einen zufälligen Zeitraum [0-10]% des SIP-Failbacks hinzu.

Cisco – vertraulich

6.1.8.3 IP-Version durchsetzen

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

Unterstützte Konfigurationen sind:

- 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 – bestellt die IPv4-Adressen vor IPv6 (Version 42,9)
- prefer-ipv6 – Bestellt die IPv6-Adressen vor IPv4 (Version 42,9)
- nat64 – ignoriert die IPv6-Adressen, bestellt die IPv4 (Version 44,2)

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

Bei der „dns“-Konfiguration werden die IPv4-Adressen für einen bestimmten Host gegenüber den IPv6-Adressen priorisiert. Wenn es zwei Hosts mit IPv4- und IPv6-Adressen gibt, ist die Reihenfolge IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

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

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

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

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

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

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

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

Etikett	Standard wert bei Auslassung	Unterstützte Werte	Beschreibung
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	DNS	ipv4 ipv6 DNS prefer-ipv4 prefer-IPv6 nat64	Kontrolliert die Reihenfolge der IPv4/IPv6-Adressen, die vom Webex-Client zum Verbinden der SIP-Sitzung verwendet werden.

6.1.8.4 DNS-TTL-Verwaltung

Ein separater Konfigurationsparameter wurde hinzugefügt, um die Art und Weise zu verwalten, wie die DNS-Auflösung erneut durchgeführt wird, wenn die TTL des DNS-Eintrags des aktuell verwendeten Servers abläuft. Wenn der Parameter in der folgenden Tabelle aktiviert ist, wird der Client gezwungen, DNS-Operationen zu wiederholen, sobald die TTL des DNS SRV- oder A-Eintrags des aktuell verwendeten Servers abläuft.

Nachdem die DNS-Auflösung erneut durchgeführt wurde, zwingt dieser Parameter den Client, sich erneut mit dem Server mit der höchsten Priorität zu verbinden, wenn dieser sich von dem derzeit verwendeten Server unterscheidet, selbst wenn die aktuelle Verbindung vollständig funktioniert. Die Verbindung wird jedoch erst wiederhergestellt, wenn laufende Gespräche beendet sind.

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 TTL, sondern alle 15 Minuten neu gestartet.

Dieser Parameter funktioniert nur für SIP.

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

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%SIP_REFRESH_ON_TTL_WXT%	Falsch	falsch, wahr	Bei der Einstellung "false" ist die DNS-TTL-Verwaltung für SIP deaktiviert. Wenn „true“ (wahr) 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 ein zufälliger Zeitraum zwischen 0 und 10 % zur DNS-TTL hinzugefügt.

HINWEIS: Es wird dringend empfohlen, den DNS-TTL-Zufallsfaktor zu aktivieren, um Spitzen bei den DNS-Anfragen und potenzielle Spitzen bei den Wiederverbindungsversuchen mit dem Anwendungsserver zu vermeiden.

6.1.9 SIP SUBCSRIBE und REGISTER Refresh und SUBSCRIBE Retry

Communicator unterstützt die Konfiguration der Aktualisierungsintervalle für SIP SUBSCRIBE und REGISTER. Für SIP SUBSCRIBE gibt es einen separaten Parameter für das Aktualisierungsintervall (in Sekunden) und die Zeit, die der Client wartet, bevor er SIP SUBSCRIBE bei Fehlern wiederholt (in Sekunden). Der empfohlene Höchstwert für *subscription-retry-interval* ist 2000000 Sekunden, während ein negativer, 0 oder leerer Wert dazu führt, dass 1800 Sekunden verwendet werden. Ein negativer Wert für subscribe refresh lässt den *Expires* Header weg und erzeugt somit ein einmaliges SUBSCRIBE.

Der vom Client vorgeschlagene SIP REGISTER Refresh 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).

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

6.1.10 P-Associated-URIs im REGISTER verwenden

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

Wenn der Parameter auf "false" gesetzt ist, verwendet der Client nicht die *P-Associated-URI* und verwendet stattdessen die Identität aus seiner eigenen SIP-URI.

```
<config>
```


Cisco – vertraulich

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

Wenn der Parameter auf "true" gesetzt ist, dann entnimmt 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. Darüber hinaus werden diese URIs nicht als Kontakte in der Kontaktliste angezeigt.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	wahr, falsch	Ermöglicht die Verwendung von alternativen Identitäten in SIP REGISTER. Wenn auf "true" gesetzt, dann übernimmt der Client seine eigene Identität aus dem letzten *P-Associated-URI* Header für ausgehende SIP-Anfragen. Wenn sie auf "false" gesetzt ist, wird ihre eigene Identität für ausgehende SIP-Anfragen von ihrer eigenen SIP-URI übernommen.

6.1.11 SIP P-Early Media (PEM)-Header

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

Der Konfigurationsparameter aktiviert die PEM-Unterstützung für die SIP-Signalisierung. Die eigentliche Logik für die Behandlung der frühen Medien ist für PEM- und Nicht-PEM-Fälle gleich und wirkt auf unterstützte PEM-Header-Werte.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_PEM_SUPPORT_WXT%	false	wahr, falsch	Setzen Sie diesen Wert auf "true", um die PEM-Unterstützung für Client-Werbung in der SIP-Signalisierung zu aktivieren. Legen Sie den Wert auf „false“ fest, um die Client-Werbe-PEM-Unterstützung in der SIP-Signalisierung zu deaktivieren.

Cisco – vertraulich

6.1.12 Unterstützung VON SIP-AKTUALISIERUNGEN

SIP UPDATE wird z. B. in einigen IMS-Implementierungen anstelle des alternativen re-INVITE benötigt. Sie ermöglicht es einem Client, die Parameter einer Sitzung zu aktualisieren, z. B. die Menge der Medienströme und ihre Codecs, hat aber keine Auswirkungen auf den Status eines SIP-Dialogs.

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

SIP UPDATE wird derzeit nur unterstützt, wenn es in Anwendungsfällen vor dem Dialog (frühe Medien) empfangen wird, nicht aber während eines aktiven Dialogs, z. B. beim Halten/Wiederaufnehmen von Anrufen, bei denen weiterhin re-INVITE verwendet wird.

In dieser Version ist es nicht möglich, mit SIP UPDATE (Medienwechsel) Video zu Audio hinzuzufügen. Außerdem unterstützt der Client nicht den vollständigen IMS-Langstrecken-Callflow mit Ressourcenreservierung.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	wahr, falsch	Bei der Einstellung "false" ist die Unterstützung von SIP UPDATE deaktiviert. Wenn „true“ (wahr) festgelegt ist, ist die Unterstützung für SIP UPDATE aktiviert.

6.1.13 Ältere SIP-INFO-FIR

Dieser Client unterstützt die herkömmliche Art der Anforderung von Videokeyframes über die SIP INFO-Mediensteuerungsanforderung. Dies ist notwendig, da einige der Geräte Probleme haben, auf RTCP-FB FIR zu reagieren, und RTCP gelegentlich nicht zum entfernten Endpunkt durchkommt, was zu keinem Video oder Einweg-Video führen kann. Weitere Informationen finden Sie unter *RFC 5168*.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false	wahr, falsch	Wenn „false“ festgelegt ist, ist die Unterstützung für SIP INFO FIR deaktiviert. Wenn „true“ (wahr) festgelegt ist, ist die SIP INFO FIR-Unterstützung aktiviert.

Cisco – vertraulich

6.1.14 SIP Rport-Verwaltung für NAT-Traversal

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

Weitere Informationen zu den Empfehlungen für den SIP-Port und das Transportprotokoll bei der Verwendung von SIP Application Layer Gateways (ALGs) im Netzwerk finden Sie im *Webex für Cisco BroadWorks-Lösungsleitfaden*.

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

Der Parameter *Preferred-port* ist insofern verwandt, als er ansonsten den im SIP-Kontakt-Header verwendeten Port definiert. Weitere Informationen zur SIP-Portzuweisung finden Sie im Abschnitt *6.1.7 Nutzung des bevorzugten Ports* für SIP.

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

> **HINWEIS**: In IPv6-Umgebungen sind alle Adressen real, und der SBC versucht, eine Verbindung zur Adresse des zuhörenden Clients herzustellen (über die Kopfzeile *Contact*).

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_USE_RPORT_WXT%	false	wahr, falsch	Aktiviert rport für Audio- und Videoanrufe.
%RPORT_USE_LOCAL_PORT_WXT%	false	wahr, falsch	Steuert, ob der lokale Port des Sockets des Clients im SIP *Contact* Header hinzugefügt werden soll.

Cisco – vertraulich

6.1.15 SIP Sitzungs-ID

Wenn diese Option aktiviert ist, wird bei der ersten Registrierung eine lokale Sitzungs-ID generiert. Die Sitzungs-ID wird für die gesamte Lebensdauer der Verbindung/Sitzung für dieses Gerät verwendet, für alle Dialoge außerhalb des Anrufs, REGISTER, SUBSCRIBE, NOTIFY usw. Dieselbe Sitzungs-ID wird verwendet, bis die Bindung verloren geht. Wenn die Registrierungsbindung verloren geht (DNS-Lookup, Zurücksetzen der Verbindung, Zurücksetzen des Telefons usw.), wird eine neue lokale Sitzungs-ID generiert.

Der Wert der Sitzungs-ID kann verwendet werden, um den vollständigen Satz von Dialogen zu finden, die mit diesem Gerät verbunden sind.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SIP_SESSION_ID_WXT%	false	wahr, falsch	Steuert die Verwendung der SIP-Sitzungs-ID.

6.1.16 Verhalten beim Ablehnen eingehender Anrufe

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

Beachten Sie, dass, wenn der Client so konfiguriert ist, dass er einen Anruf mit *603 Decline* ablehnt, die Dienste Call Forward Busy und Call Forward No Answer möglicherweise nicht wie erwartet funktionieren.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_REJECT_WITH_486_WXT%	wahr	wahr, falsch	Steuert den SIP-Fehlercode und den Grund für die Ablehnung eingehender SIP-Anrufe. Wenn aktiviert, wird *486 Vorübergehend nicht verfügbar* verwendet. Andernfalls wird *603 Decline* verwendet.

6.1.17 Portbereich des Transportprotokolls in Echtzeit

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

```
<config>
```


Cisco – vertraulich

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	Nummer	Beginn des Audio-Port-Bereichs.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	Nummer	Ende des Audio-Portbereichs.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	Nummer	Beginn des Videoport-Bereichs.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	Nummer	Ende des Videoport-Bereichs.

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

6.1.18 ICE-Unterstützung (nur Webex Calling)

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

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

Wenn die ICE-Unterstützung aktiviert ist, wird für SRTP immer ein neuer Schlüssel verwendet (siehe Abschnitt *6.1.2 SIP über TLS und sicheres Echtzeit-Transportprotokoll*).

Ab Version 44,5 fügt die Webex-App Unterstützung für ICE über IPv6 mit NAT64. hinzu

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_RTP_ICE_WXT%	false	wahr, falsch	Aktivieren/Deaktivieren der ICE-Unterstützung.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%RTP_ICE_MODE_WXT%	Eissturm	Eissturm	ICE-Unterstützungsmodus. Derzeit wird nur der Wert "icestun" unterstützt.
%RTP_ICE_SERVICE_URI_WXT%	(leer)	gültige STUN-Server-URI oder (leer)	STUN-Server-URI.
%RTP_ICE_PORT_WXT%	3478	Nummer (0-65535)	STUN-Serverport.
%ENABLE_RTP_ICE_IPV6_WXT%	false	wahr, falsch	Aktiviert ICE über IPv6.

6.1.19 RTCP-MUX

Der RTCP-MUX ist konfigurierbar. Diese Funktion sorgt dafür, dass der Client denselben Port für RTP und RTCP verwendet. In der SIP/SDP-Signalisierungsebene wird die Zeile a=rtcp-mux in das SDP eingefügt. Darüber hinaus sind verschiedene Modi möglich:

- Abwärtskompatibilitätsmodus (d. h. die Zeile a=rtcp-mux erscheint nicht im SDP)
- Multiplexing-Modus (die Zeile a=rtcp-mux erscheint zweimal in der SDP: einmal im Abschnitt m=Audio und ein zweites Mal im Abschnitt m=Video)

Video und Audio verwenden nicht denselben Anschluss.

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_RTCP_MUX_WXT%	wahr	wahr, falsch	Um RTPC MUX zu aktivieren, auf "true" setzen. Um RTCP MUX zu deaktivieren, setzen Sie den Wert auf "false".

6.1.20 Übertragen

Der Webex for Cisco BroadWorks-Client unterstützt die Übergabe von betreuten (beratenden), halbberatenden und direkten (blinden) Anrufen.

Bei der semikonsultativen Vermittlung kann der Anrufer die Vermittlung abschließen, bevor der Anruf von der Gegenstelle entgegengenommen wird. Die semikonsultative Beendigungstaste wird für den Anrufer erst aktiviert, nachdem das Klingeln auf der Anruferseite gestartet und die entsprechende SIP-Benachrichtigung (*180 Ringing*) auf der Anruferseite empfangen wurde. Die Blindübertragung wird in der Benutzeroberfläche "Jetzt übertragen" genannt.

Cisco – vertraulich

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

Mit Version 43,9 der Webex-App wird die Übergabe an einen anderen eigenständigen laufenden Anruf desselben Typs eingeführt. Anrufe, die in der Webex-App beendet werden, können an andere Anrufe übergeben werden, die am lokalen Endpunkt beendet werden. Und Anrufe, die auf einem entfernten Gerät beendet wurden, können auf Anrufe übertragen werden, die auf einem entfernten Endpunkt beendet wurden. Diese Funktion hat keine konfigurierbaren Optionen.

Ab Version 43,12 fügt die Webex-App eine Konfigurationsoption hinzu, mit der festgelegt wird, ob der aktuelle Anruf automatisch in die Warteschleife gestellt werden soll, wenn das Menüelement „Übergabe“ ausgewählt wird. Dieses Verhalten wird durch das neue Attribut *auto-hold* gesteuert. Standardmäßig ist das automatische Halten deaktiviert.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_TRANSFER_CALLS_WXT%	false	wahr, falsch	Wenn diese Option auf "true" gesetzt ist, ist die Anrufweiterleitung aktiviert. Wenn die Option auf „false“ festgelegt ist, ist die Anrufübergabe deaktiviert.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false	wahr, falsch	Aktiviert die Übertragungsoption(en) für die an einem anderen Standort beendeten Ferngespräche (XSI).
%TRANSFER_CALL_TYPE_WXT%	voll	talk-first, blind, voll	Gibt an, welche Übertragungsarten für den Benutzer in der BroadWorks-Konfiguration verfügbar sind.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	wahr, falsch	Legt fest, ob der aktive Anruf automatisch in die Warteschleife gelegt wird, wenn der Benutzer die Option Übergeben aus dem Bildschirmmenü während des Anrufs auswählt.

6.1.21 N-Wege-Konferenzanrufe

Das folgende benutzerdefinierte Tag kann verwendet werden, um die Verfügbarkeit des Ad-hoc-Konferenzanrufs (N-Way) über SIP im Webex for Cisco BroadWorks-Client zu steuern. Außerdem kann der N-Weg-Eigentümer die vollständige Liste der Teilnehmer über SIP SUBSCRIBE/NOTIFY und das Konferenz-Event-Paket einsehen. Der Client des Eigentümers erfährt den URI, an den er den SIP SUBSCRIBE senden soll, über den vorangehenden SIP *Contact* Header der *200 OK* Nachricht, die als Antwort auf den INVITE an den Konferenz-URI gesendet wird, während für die Teilnehmer dieselben Informationen in einem vorangehenden call-info NOTIFY enthalten sind.

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

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

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

Example output:
maxConferenceParties = 6
conferenceURI =
```

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

Mit der Version 45,7 unterstützt die Webex-Anwendung ausschließlich die Bereitstellung von Webex Calling den automatischen Übergang von einem N-Way-Ad-hoc-Konferenzanruf zu einer 1:1-Anrufsitzung, vorausgesetzt, der Gastgeber und ein weiterer Teilnehmer bleiben im Anruf. Eine neue konfigurierbare Option (*Drop-Two-Party-Conference*) wurde hinzugefügt, um die Aktivierung dieser Verbesserung zu steuern.

```
<config>
<services><calls>
<conference enabled="%ENABLE_CONFERENCE_CALLS_WXT%" xsi-
enabled="%ENABLE_XSI_CONFERENCE_CALLS_WXT%">
    <subscribe-conference-info enabled="%ENABLE_NWAY_PARTICIPANT_LIST_WXT%"/>
    <max-nway-participants>%MAX_CONF_PARTIES_WXT%</max-nway-participants>
    <drop-two-party-conference enabled="%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%"/>
</conference>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CONFERENCE_CALLS_WXT%	false	wahr, falsch	Steuert, ob die Option "Konferenz" für den Benutzer aktiviert werden soll.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	false	wahr, falsch	Setzen Sie diesen Wert auf "true", um die N-way owner Teilnehmerliste zu aktivieren. Setzen Sie den Wert auf „false“, um die N-Wege-Besitzer-Teilnehmerliste zu deaktivieren.
%MAX_CONF_PARTIES_WXT%	10	Zahl zwischen 4 und 15 (leer)	Gibt die maximale Anzahl der N-Wege-Teilnehmer an, die vom Client erzwungen wird, z. B. 10. Die Serverseite hat ihre eigenen Grenzen. Ein leerer Wert deaktiviert die clientseitige Erzwingung der N-fachen Teilnehmergrenze.
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	false	wahr, falsch	Steuert, ob das Ad-hoc-Konferenzgespräch nur dann in eine 1:1-Anrufsitzung umgewandelt werden soll, wenn zwei Teilnehmer im Konferenzgespräch bleiben.

6.1.22 Anrufübergabe

Die Webex-App unterstützt Call Pull, mit dem Benutzer Remote-Anrufe, die auf ihren Geräten beendet werden, auf das aktuelle Gerät verschieben können. Es gibt eine statische (blinde) Anrufübertragungsoption, die Benutzer auch dann verwenden können, wenn kein laufender Anruf vorhanden ist.

Version 45,1 der Webex-App verbessert die Funktion, indem die aktive Anrufüberwachung hinzugefügt und die Option angeboten wird, den Remote-Anruf aus dem Anruf an das aktuelle Gerät zu übertragen. Diese Option ist nur verfügbar, wenn es für den Benutzer einen einzelnen laufenden Anruf gibt, der auf einem anderen Gerät beendet wird, das dem Benutzer gehört.

In der Desktop-App gibt es eine neue konfigurierbare Option, die in den Anrufeinstellungen der Webex-App angezeigt wird, die eine unterschiedliche Handhabung von Remote-Anrufen ermöglicht:

- Remote-Anrufsteuerung – Dies ist das aktuelle Verhalten der Webex-App, bei der die Remote-Anrufe mit einem Timer in der Anrufliste angezeigt werden. Wenn der Timer ausgewählt ist, kann der Benutzer den Bildschirm zur Anrufsteuerung sehen. Mit der neuen Verbesserung kann der Benutzer die neue Option „Anruf auf Computer verschieben“ im Menü „Mehr“ verwenden, um einen Anrufübergriff zu initiieren.
- Anruf verschieben – Mit dieser Option kann der Benutzer den Bildschirm für die Anrufsteuerung für Remote-Anrufe nicht öffnen. Dem Benutzer wird nur dann die Option „Verschieben“ für den Anruf angezeigt, wenn es einen einzelnen Remote-Anruf gibt, der auf einem Gerät beendet wird, das dem Benutzer gehört. Wenn die Option „Verschieben“ ausgewählt ist, wird dem Benutzer ein Bestätigungsdialogfeld angezeigt, bevor die Webex-App die Anrufübergabe initiiert.

Cisco – vertraulich

- Immer fragen – Bei diesem Konfigurationstyp wird dem Benutzer der Timer für den Remote-Anruf in der Anrufliste angezeigt und wenn er ausgewählt ist, wird er gefragt, wie er fortfahren soll – ob die Remote-Anrufsteuerung angezeigt werden soll, der Anrufübergriff, der initiiert werden soll (falls verfügbar), oder den Vorgang abbrechen soll

Version 45,1 verbessert auch die mobile App. Wenn der aktive Anrufübertragungsmodus aktiviert ist, werden alle Remote-Anrufe für den Benutzer angezeigt, wodurch die aktive Anrufüberwachung aktiviert wird und die Option zum Verschieben von Anrufen in bestimmten Situationen bereitgestellt wird. Wenn nur ein Anruf auf einem Remote-Gerät (im Besitz des Benutzers) beendet wird, ist die Option „Verschieben“ für diesen Anruf verfügbar. Wenn es jedoch mehrere Anrufe für den Benutzer gibt oder der Anruf auf einem gemeinsam genutzten Gerät beendet wird, sind die Anrufe weiterhin sichtbar, jedoch nur zu Informationszwecken – es gibt keine Option, den Anruf remote zu verschieben oder zu steuern.

Zur Steuerung der Funktion gibt es mehrere konfigurierbare Optionen – eine zur Steuerung der Verfügbarkeit und zwei weitere – *Modus* und *Standard-active-move-option* (nur Desktop), um das Funktionsverhalten zu steuern. Der *Modus* kann auf eine der folgenden Optionen eingestellt werden:

- blind
    - der Standardmodus
    - Desktop – eine Anrufübertragungstaste im Tastenfeld
    - Mobil – eine Anrufübertragungsoption auf der Registerkarte „Anrufe“
- aktiv
    - Desktop
        - keine Anrufübertragungstaste im Tastenfeld
        - ermöglicht das Abrufen eines aktiv überwachten Anrufs
        - ermöglicht die Konfigurierbarkeit der Aktion, wenn ein Anruf ausgewählt wird
    - Mobil
        - keine Anrufübertragungsoption in den Optionen der Registerkarte „Anrufe“
        - ermöglicht die aktive Überwachung aller Remote-Anrufe des Benutzers
        - ermöglicht das Abrufen eines aktiv überwachten Anrufs
- voll – kombiniert den blinden und aktiven Modus

```
<config>
<services><calls>
<call-pull enabled="%ENABLE_CALL_PULL_WXT%"
           mode="%CALL_PULL_MODE_WXT%"
           default-active-move-option="%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%"/>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_PULL_WXT%	false	wahr, falsch	Ermöglicht Call Pull.
%CALL_PULL_MODE_WXT%	blind	blind, aktiv, voll	Steuert, welche Anrufübertragungsoptionen für den Benutzer verfügbar sind – es kann sich um eine der aktuellen Optionen für blinde Anrufe, eine Anrufübergabe basierend auf der aktiven Überwachung oder beides handeln.
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	Anruf_verschieben	Anrufsteuerung, Anruf_verschieben, immer_fragen	nur Desktops Wenn die aktive Verschiebung verfügbar ist (aktiver oder vollständiger Modus ist konfiguriert), gibt diese Einstellung die Standardaktion an, die für den Benutzer in der Anrufliste aktiviert ist

HINWEIS: Diese Funktion erfordert, dass für den Benutzer der Dienst für die gemeinsame Darstellung von Anrufen aktiviert wird, indem das Kontrollkästchen „Anrufannahme von einem anderen Standort zulassen“ auf der Konfigurationsseite für die gemeinsame Darstellung von Anrufen im CommPilot-Portal aktiviert wird.

6.1.23 Anruf parken/Abrufen

Mit der Funktion "Gruppenanrufe parken" können laufende VoIP-Anrufe an einen Call-Park-Server weitergeleitet werden, so dass der Anrufer etwas anderes tun kann und von demselben oder einem anderen Benutzer abgerufen werden kann. Ein laufender Anruf wird bei der ersten verfügbaren Nebenstelle innerhalb der Anrufparkgruppe geparkt.

Die Anrufrückholung kann dadurch erfolgen, dass der Benutzer den Anruf unmittelbar nach dem Parken des Anrufs für eine konfigurierbare Anzahl von Sekunden im Dialog parkt. Oder der geparkte Anruf kann vom Benutzer oder einem anderen Benutzer abgerufen werden, indem er die Option zum Abrufen von Anrufen auswählt und die Nummer oder Nebenstelle eingibt.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_PARK_WXT%	false	wahr, falsch	Aktiviert das Parken/Abrufen von Anrufen.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Nummer zwischen 5 und 30	Legt die Anzahl der Sekunden fest, die das Dialogfeld "Erfolgreicher Anruf geparkt" für den Benutzer sichtbar ist, bevor es automatisch geschlossen wird.

Cisco – vertraulich

6.1.24 Anrufstatistik

Reporting End-of-Call Statistics in Session Initiation Protocol (SIP) Die BYE-Nachricht ermöglicht das Senden von Anrufstatistiken an ein entferntes Ende, wenn ein Anruf beendet wird. Die Anrufstatistiken werden als neuer Header in der SIP BYE-Nachricht oder in der entsprechenden *200 OK* Antwort auf die BYE-Nachricht gesendet. Zu den Statistiken gehören gesendete oder empfangene RTP-Pakete (Real-Time Transport Protocol), die Gesamtzahl der gesendeten oder empfangenen Bytes, die Gesamtzahl der verlorenen Pakete, Verzögerungs-Jitter, Round-Trip-Verzögerung und die Anrufdauer.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_STATISTICS_WXT%	false	wahr, falsch	Setzen Sie diesen Wert auf "true", um die Aufzeichnung von Anrufmetriken zu aktivieren. Legen Sie den Wert auf „false“ fest, um die Erfassung von Anrufmetriken zu deaktivieren.

6.1.25 Automatische Wiederherstellung von Anrufen /Nahtlose Übergabe von Anrufen

Der Client unterstützt die automatische Wiederherstellung von Anrufen bei einem Netzwechsel, während der Benutzer ein VoIP-Gespräch führt. Die automatische Wiederherstellung von Anrufen funktioniert in beide Richtungen - Mobilfunkdaten-zu-WiFi und WiFi-zu-Mobilfunkdaten sowie beim Wechsel zwischen WiFi-Netzwerken. Es wird versucht, den Anruf innerhalb eines einminütigen Zeitrahmens wiederherzustellen und dann zu beenden. Wenn mehrere VoIP-Anrufe laufen, wird nur der aktive Anruf wiederhergestellt.

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

Bei einer automatischen Wiederherstellung eines Anrufs aufgrund einer Netzwerkänderung wird für den Benutzer während des Verbindungsversuchs des Anrufs ein Signalton ausgegeben.

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false	wahr, falsch	Steuert, ob der automatische Wiederherstellungsmechanismus für den Benutzer aktiviert werden soll.

HINWEIS: Diese Funktion hängt davon ab, ob die Anrufübertragungsfunktion für den Benutzer aktiviert ist. Weitere Informationen finden Sie im Abschnitt *6.1.22 Anrufübergabe*.

6.1.26 Anrufaufzeichnung

Die Funktion Anrufaufzeichnung 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 zum Senden des *X-BroadWorks-Correlation-Info* -SIP-Headers konfiguriert ist (siehe *Lösungsleitfaden für Webex für Cisco BroadWorks*).

Wenn die Funktion deaktiviert ist, stehen dem Benutzer keine Aufzeichnungsschaltflächen und -optionen zur Verfügung. Beachten Sie, dass die Aufzeichnung von Anrufen pro Benutzer und nicht pro Anruf erfolgt, d. h. wenn einer der Teilnehmer eines Anrufs die Aufzeichnung unterstützt, kann der Anruf aufgezeichnet werden.

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

Immer

- Die Aufzeichnung von Anrufen wird automatisch beim Verbindungsaufbau gestartet.
- Der Benutzer ist **NICHT** in der Lage, die Gesprächsaufzeichnung zu stoppen/pausieren.

Immer mit Unterstützung für Pause/Wiederaufnahme

- Die Anrufaufzeichnung wird automatisch bei der Anrufeinrichtung gestartet, aber der Benutzer kann den Anruf anhalten und fortsetzen.
- Mögliche Benutzerinteraktionen:
  - Die Aufnahme läuft - **Pause** Aufnahmeaktion.
  - Aufzeichnung ist angehalten – **Aufzeichnung fortsetzen** Aktion.

Auf Anfrage

- Nachdem der Anruf aufgebaut wurde, beginnt die Aufzeichnung des Anrufs auf dem Server.
- Wenn der Benutzer die Option Aufzeichnung starten während des Gesprächs drückt, wird die Aufzeichnung des Anrufs gespeichert und der Anruf bleibt von Anfang an erhalten. Andernfalls wird die Aufzeichnung des Anrufs auf dem Server gelöscht, wenn der Benutzer keine Aufzeichnung startet.
- Mögliche Benutzerinteraktionen:

Cisco – vertraulich

- Es wurde noch keine Aufzeichnung gestartet - **Start** Aufzeichnungsaktion.
- Die Aufnahme läuft - **Pause** Aufnahmeaktion.
- Aufzeichnung ist angehalten – **Aufzeichnung fortsetzen** Aktion.

Auf Anfrage mit vom Benutzer initiiertem Start

- Der Benutzer kann die Aufzeichnung von Anrufen jederzeit starten, stoppen, anhalten und fortsetzen, auch mehrmals während eines Anrufs.
- Für jeden Start der Gesprächsaufzeichnung wird es separate Aufzeichnungen geben.
- Mögliche Benutzerinteraktionen:
  - Es wurde noch keine Aufzeichnung gestartet - **Start** Aufzeichnungsaktion.
  - Aufzeichnung ist in Bearbeitung – Aktion **Aufzeichnung stoppen** und **Pause** .
  - Aufzeichnung wird angehalten – die Aktion **Aufzeichnung beenden** und **fortsetzen** .

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_RECORDING_WXT%	false	wahr, falsch	Aktiviert die Steuerung der Anrufaufzeichnung.

6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten

Die folgenden benutzerdefinierten Tags können verwendet werden, um die Verfügbarkeit der Cisco BroadWorks-Voicemail und der visuellen Voicemail im Webex für Cisco BroadWorks-Client zu steuern.

Visual Voicemail (VVM) wird nur für Audio unterstützt. Unterstützte Formate sind wav, ulaw und mov mit H264-Video (nur als Audio abgespielt). Sie ermöglicht es den Nutzern, eingehende Sprachnachrichten in einer Listenansicht anzuzeigen und einzelne Elemente abzuspielen. Diese Funktion basiert auf Xsi, aber die Benachrichtigung über neue Voicemails erfolgt über SIP; daher muss SIP aktiviert sein, damit die Benachrichtigungen funktionieren. Darüber hinaus ist die Konfiguration von SIP SUBSCRIBE für Message Waiting Indicator (MWI) erforderlich, damit die Benachrichtigungen ankommen, und MWI muss aktiviert sein, damit Visual Voicemail funktioniert. Weitere Informationen zur SIP-Konfiguration finden Sie in Abschnitt *6.1.1 SIP-Server-Einstellungen*.

Informationen zu den Cisco BroadWorks-Versionsanforderungen und Patch-Anforderungen für Visual Voicemail finden Sie im
Lösungsleitfaden für Webex für Cisco BroadWorks.

Cisco – vertraulich

Visual Voicemail muss in der Konfiguration separat aktiviert werden.

Die folgenden Einstellungen sind auf dem CommPilot-Portal erforderlich, um Visual Voicemail zu nutzen:

- Sprachnachrichten aktiviert
- Option "Wenn Nachricht eintrifft, Unified Messaging verwenden" aktiviert
- Option "Anzeige für wartende Telefonnachrichten verwenden" aktiviert

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

Beachten Sie, dass die Deaktivierung der SIP-Registrierung auch die MWI für neue Sprachnachrichten deaktiviert. In der folgenden Tabelle finden Sie weitere Informationen zur Aktivierung von MWI.

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

Wenn das SIP-Abonnement für das Voicemail-Ereignispaket fehlschlägt, versucht der Client es erneut, wenn er dafür konfiguriert ist. Weitere Informationen zur Konfiguration der SIP-SUBSCRIBE-Wiederholungsversuche finden Sie in Abschnitt *6.1.9 SIP SUBCSRIBE und REGISTER Refresh und SUBSCRIBE Retry.*

```
<config>
<services><calls>
<mwi enabled="%ENABLE_MWI_WXT%" type="%MWI_MODE_WXT%"/>
<voice-mail enabled="%ENABLE_VOICE_MAIL_WXT%" visual-
voicemail="%ENABLE_VISUAL_VOICE_MAIL_WXT%">
    <transcription enabled="%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%"/>
    <forwarding enabled="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
</voice-mail>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_MWI_WXT%	false	wahr, falsch	Auf "true" setzen, um MWI zu aktivieren. Auf "false" setzen, um MWI zu deaktivieren.
%MWI_MODE_WXT%	leer	implizit, explizit	Setzen Sie diese Option auf "explicit", um SIP SUBSCRIBE für MWI-Ereignispakete zu senden, wenn MWI aktiviert ist. Wenn „implizit“ verwendet wird, wird kein SIP SUBSCRIBE für MWI-Ereignispaket gesendet, wenn MWI aktiviert ist. Bleibt der Eintrag leer, ist MWI deaktiviert.
%ENABLE_VOICE_MAIL_WXT%	false	wahr, falsch	Setzen Sie diese Option auf "true", um die Unterstützung von Voicemail zu aktivieren. Legen Sie den Wert auf „false“ fest, um die Voicemail-Unterstützung zu deaktivieren.

Cisco – vertraulich

Etikett	Standard wert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	wahr, falsch	Wenn die Option auf „false“ festgelegt ist, ist VVM deaktiviert. Wenn „true“ festgelegt ist, ist VVM aktiviert. Beachten Sie, dass voice-mail enabled=false vor dem eigentlichen VVM-Attribut aus Gründen der Abwärtskompatibilität weiterhin verwendet wird.

6.1.28 Voicemail-Abschrift für Webex Calling

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

Die Funktion sollte für einen Benutzer nur aktiviert werden, wenn:

1. Die App wird in einer Webex Calling-Bereitstellung ausgeführt.
2. Die Funktion Visual Voicemail ist für den Benutzer aktiviert.
3. Die Funktion ist in der Konfiguration aktiviert (das aktivierte Attribut im Tag sollte auf „true“ gesetzt werden).

Etikett	Standard wert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	false	wahr, falsch	[Nur Webex Calling] Steuert die Verfügbarkeit der Voicemail-Transkription nur, wenn Visual Voicemail aktiviert ist.

6.1.29 Anrufeinstellungen

6.1.29.1 Immer Rufumleitung

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

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	wahr, falsch	Steuert die Verfügbarkeit des Dienstes "Anrufumleitung immer". Die Funktion ist standardmäßig deaktiviert.

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

6.1.29.2 Anrufweiterleitung an Voicemail

Ab Version 43,9 bietet die Webex-App eine Option, um die Verfügbarkeit der Weiterleitung an Voicemail zu steuern. Standardmäßig ist die Funktion aktiviert, und mit der folgenden Konfigurationsoption kann sie deaktiviert werden.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	wahr	wahr, falsch	Steuert die Verfügbarkeit der Weiterleitung an die Voicemail. Die Funktion ist standardmäßig aktiviert.

ANMERKUNG 1: Diese Funktion hängt von einem der Dienste "Voice Messaging User" oder "Third-Party Voice Mail Support" ab, die dem Benutzer zugewiesen werden.

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

6.1.29.3 BroadWorks Anywhere (Einzelnummernreichweite)

Die folgenden benutzerdefinierten Tags steuern die Verfügbarkeit von BroadWorks Anywhere und die Verfügbarkeit seiner Einstellungen im Webex für Cisco BroadWorks-Client. Beachten Sie, dass der Name dieser Funktion innerhalb des Clients *Manage My Numbers* lautet.

```
<config>
```


Cisco – vertraulich

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_BROADWORKS_ANYWHERE_WXT%	false	wahr, falsch	Aktiviert BroadWorks Anywhere (BWA) auf der Konfigurationsebene.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	wahr	wahr, falsch	Steuert, ob die Beschreibung des BWA-Standorts für den Benutzer verfügbar sein soll.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	wahr, falsch	Setzen Sie diesen Wert auf "true", um dem Benutzer den Alarm "Alle Standorte" für den BWA-Dienst zur Verfügung zu stellen. Legen Sie den Wert auf „false“ fest, damit die Benachrichtigung aller Standorte für den BWA-Dienst für den Benutzer nicht verfügbar ist.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	false	wahr, falsch	Steuert, ob die Anwendung den Status "Alle Standorte alarmieren" beim Hinzufügen des zweiten oder jedes weiteren neuen BWA-Standorts aktivieren soll.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	wahr, falsch	Steuert, ob die Anrufsteuerung des BWA-Standorts für den Benutzer verfügbar sein sollte.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	false	wahr, falsch	Steuert den Standardstatus der Anrufsteuerung für den BWA-Standort.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	wahr, falsch	Steuert, ob der Umleitungshemmer des BWA-Standorts für den Benutzer verfügbar sein soll.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	wahr, falsch	Steuert den Standardstatus des Umleitungshemmers des BWA-Standorts.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false	wahr, falsch	Steuert, ob die Antwortbestätigung des BWA-Standorts für den Benutzer verfügbar sein sollte.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	false	wahr, falsch	Steuert den Standardstatus der Antwortbestätigung des BWA-Standorts.

6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen

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

Außerdem bietet der Client die Möglichkeit, stattdessen die Webansicht für Anrufeinstellungen (CSWV) zu verwenden. Dadurch kann der Benutzer mehr der serverbasierten Anrufeinstellungen steuern. Mit separaten Tags lässt sich steuern, ob bestimmte Dienste in den webbasierten Anrufeinstellungen sichtbar sein sollen.

> **HINWEIS**: Es ist ratsam, die Einstellungen auszublenden, die bereits in der Anwendung wie Call Center (siehe Abschnitt *6.1.31 Callcenter/Anrufwarteschlange-Anmeldung/Abmeldung*) und BroadWorks Anywhere (siehe Abschnitt *6.1.29.3 BroadWorks Anywhere*) sichtbar sind. Es ist auch ratsam, den Remote Office-Dienst auszublenden, da er durch den BroadWorks Anywhere-Dienst ersetzt wurde.

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

```
<config>
<services>
<web-call-settings target="%WEB_CALL_SETTINGS_TARGET_WXT%"
 <url>%WEB_CALL_SETTINGS_URL_WXT%</url>
<branding-enabled="%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%">
  <service-settings>
   <service name="Call Forwarding Always"
visible="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <service name="Call Forwarding Busy"
visible="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <service name="Call Forwarding Not Reachable"
visible="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
   <service name="Call Forwarding No Answer"
visible="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <service name="Do Not Disturb" visible="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
   <service name="Anonymous Call Rejection"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="Simultaneous Ring Personal"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <service name="Sequential Ring"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <service name="Automatic Callback"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <service name="Call Waiting" visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Calling Line ID Delivery Blocking"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <service name="Personal Assistant"
visible="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
```


Cisco – vertraulich

```
   <service name="Call Center – Standard"
visible="%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%"/>
   <service name="BroadWorks Anywhere"
visible="%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%"/>
   <service name="BroadWorks Mobility"
visible="%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <service name="Remote Office" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Voice Messaging User"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
</web-call-settings>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%WEB_CALL_SETTINGS_TARGET_WXT%	Extern	extern, csw	Steuert den Modus des Verwaltungsportals. Setzen Sie diese Option auf "extern", um die konfigurierte URL des Einstellungsportals in einem externen Browser zu öffnen. Legen Sie „csw“ fest, um das CSW-Portal in einem eingebetteten Browser mithilfe des Abschnitts „zusätzliche Parameter“ zu öffnen, um die POST-Anforderung zu erstellen.
%WEB_CALL_SETTINGS_URL_WXT%	leer	URL-Kette	URL für das Einstellungsportal. Beispiel: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option Anrufumleitung immer für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	wahr	wahr, falsch	Legt fest, ob die Ruhefunktion für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Anonyme Anrufe ablehnen“ (ACR) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Rufumleitung besetzt“ (CFB) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Rufumleitung nicht erreichbar“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Rufumleitung Keine Antwort“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option SIMRING (Simultaneous Ring Personal) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option SEQRING (Sequential Ring) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Remote Office (RO)“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option für den automatischen Rückruf (ACB) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Anklopfen“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	wahr	wahr, falsch	Kontrolliert, ob die Option CLIDB (Calling Line ID Delivery Blocking) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Persönlicher Assistent“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „BroadWorks Anywhere“ (BWA) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Callcenter-Option für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option BroadWorks-Mobilität (BWM) für den Benutzer in den webbasierten Einstellungen sichtbar sein soll. Derzeit lautet der empfohlene Wert aufgrund von Interoperabilitätsproblemen zwischen Webex for Cisco BroadWorks und BroadWorks Mobility „falsch“.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Option „Sprachverwaltung (VM)“ für den Benutzer in den webbasierten Einstellungen sichtbar sein soll.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false	wahr, falsch	Steuert, ob das neue Branding der WebView Anrufeinstellungen verwendet werden soll. Aktivieren, wenn die serverseitige CSWV-Version 1.8.6 oder höher ist. Andernfalls lassen Sie es falsch.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	wahr	wahr, falsch	Steuert, ob die Optionen für E-Mail-/Voicemail-Nachrichten in den webbasierten Einstellungen sichtbar sind.
%USER_PORTAL_SETTINGS_URL_WXT%	leer	URL-Kette	Gibt die URL zum Portal für Benutzereinstellungen an. Um die Funktion zu aktivieren und die Schaltfläche Zugriff auf das Benutzerportal in der Benutzeroberfläche anzuzeigen, sollte dieses benutzerdefinierte Tag nicht leer sein. Zum Beispiel: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	Extern	extern, intern	Gibt an, ob die URL in einem eingebetteten oder externen Browser geöffnet werden soll.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false	wahr, falsch	Gilt nur, wenn der eingebettete Browser konfiguriert ist (USER_PORTAL_SETTINGS_TARGET_WXT=internal). Wenn diese Option aktiviert ist, wird eine HTTP-POST-Anforderung verwendet, und das kurzlebige BroadWorks-Token wird als Teil des BODY hinzugefügt. Wenn diese Option deaktiviert ist, wird die URL mit HTTP GET geöffnet.

ANMERKUNG 1: Die URL der WebView Anrufeinstellungen sollte immer ein nachgestelltes "/" enthalten. Zum Beispiel: http(s):////

HINWEIS 2: Die WebView-Anwendung "Anrufeinstellungen" wird mindestens in der Version 1.7.5 unterstützt.

Die Installation auf Cisco BroadWorks-Version 21finden Sie in den zusätzlichen Schritten, die im *Leitfaden zur Webex Für Cisco BroadWorks-Lösung* beschrieben sind.

Cisco – vertraulich

6.1.31 Callcenter/Anrufwarteschlange-Anmeldung/Abmeldung

Die Webex-App bietet Zugriff auf die Einstellungen für den Callcenter-Agenten (Anrufwarteschlange). Wenn ein Benutzer für Call Center vorgesehen ist, kann er sich mit dieser Funktion bei einem Call Center anmelden und die verfügbaren Warteschlangen anzeigen, Warteschlangen beitreten bzw. trennen und den Status der automatischen Anrufverteilung (ACD) festlegen.

Ab Desktop-Version 42,8 und Mobile Version 42,12 basiert der Call Center (Anrufwarteschlange)-Agent nicht mehr auf der Webansicht der Anrufeinstellungen (siehe Abschnitt *6.1.30 Einstellungsportal und webbasierte Anrufeinstellungen*). Die Konfiguration des Call Center-Agenten (Anrufwarteschlange) ist über die Fußzeile des Desktops und der Einstellungen der mobilen Webex-App zugänglich.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_CENTER_WXT%	false	wahr, falsch	Ermöglicht Call Center-Unterstützung.

6.1.32 XSI-Wurzel und Pfade

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

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

Die Ereignis- und Aktionspfade werden in der Regel aufgrund von Branding-Anforderungen geändert, um den Domänenverweis *com.broadsoft* aus den URL-Pfaden der vom Client durchgeführten XSI-HTTP-Anfragen zu entfernen.

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%XSI_ROOT_WXT%	Verwendet weiterhin die ursprünglich für den Konfigurationsabruf verwendete.	URL-Kette	Die XSI-Wurzel für alle XSI-Operationen. Beispiel: https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	Schnur	Gibt den Pfad für XSI-Aktionen an. Sie sollte mit "/" beginnen und enden und nur den Aktionskontext enthalten. Beispiel: /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	Schnur	Gibt den Pfad für XSI-Ereignisse an. Sie sollte mit „/“ beginnen und enden und nur den Kontext der Ereignisse enthalten. Beispiel: /com.domain.xsi-events/

6.1.33 XSI-Ereigniskanal

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

- XSI-Anrufsteuerungen
- Benachrichtigung über den Status der Anrufeinstellungen
- Anrufaufzeichnung

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_XSI_EVENT_CHANNEL_WXT%	wahr	wahr, falsch	Steuert, ob der XSI-Ereigniskanal aktiviert ist. Er sollte auf "true" gesetzt werden, um z. B. Ereignisse zu empfangen, die sich auf den Kontrolldienst während eines Anrufs beziehen. Der empfohlene Wert ist "true".
%CHANNEL_HEARTBEAT_WXT%	10000	Nummer	Dies ist der XSI Event Channel Heartbeat (in Millisekunden). Der Standardwert ist "10000".

Cisco – vertraulich

6.1.34 Codec-Konfiguration

Webex für Cisco BroadWorks bietet eine Vielzahl von Audio- und Video-Codecs. Die entsprechenden Codec-Listen befinden sich unter *config/services/calls/* in den Abschnitten *audio/codecs* und *video/codecs* . Die Priorität der einzelnen Codecs kann über das *XML-Attribut priority* geändert werden, das einen Wert zwischen 0,0 (niedrigste Priorität) und 1,0 (höchste Priorität) hat.

Die Webex-App unterstützt offiziell die folgenden Codecs:

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

Cisco – vertraulich

```
<config>
<services><calls>
  <audio>
    <codecs>
      <codec name="opus" priority="1" payload=""/>
      <codec name="xCodec" mode="HP" priority=".99" payload=""/>
      <codec name="xCodec" mode="ULP" priority=".98" payload=""/>
      <codec name="G722" priority=".9" payload=""/>
      <codec name="PCMU" priority=".8" payload=""/>
      <codec name="PCMA" priority=".7" payload=""/>
      <codec name="G729" priority=".5" payload="" vad=""/>
      <codec name="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="telephone-event" payload="101" in-band="false"/>
    …
  <video>
    <codecs>
      <codec name="H264" payload="109" resolution="HD" framerate="30"
bitrate="2000000" priority="1.0">
        <packet-mode>0</packet-mode>
```

Der Client unterstützt H.264 als Videocodec. Das Attribut für die Videoauflösung, das die von der App angekündigte maximale Videoauflösung angibt, kann auf einen der folgenden verfügbaren Werte festgelegt werden: SUBQCIF, QCIF, CIF, 4CIF, VGA, HD und WIDE_FULL_HD.

Ab der Version 45,8 wird die maximale Videoauflösung, die von der Desktop-App verwendet wird, von der Standard-HD auf WIDE_FULL_HD aktualisiert, und die für die mobilen und Tablet-Apps bleibt 4CIF.

Wenn die Bitrate nicht in der Konfiguration angegeben wird, 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
WIDE_FULL_HD	1920 x 1080	30	4000000

***** Maximale beworbene Videoauflösung. Die tatsächliche Videoauflösung bei einem Anruf zwischen zwei Webex für Cisco BroadWorks-Clients hängt von den Funktionen beider Clients ab. Sie ist die niedrigere der beiden Clients und ist auf beiden Clients gleich.

Die Videoauflösung für einen Videoanruf wird während des Sitzungsaufbaus ausgehandelt und richtet sich nach den Fähigkeiten der beiden Endpunkte. Die Auflösung von Videoanrufen ist an 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. Die Videoauflösung kann sich während eines Anrufs ändern, wenn sich die Netzbedingungen verschlechtern. In diesem Fall verwenden die beiden mobilen Endpunkte möglicherweise unterschiedliche Videoauflösungen.

Der Paketierungsmodus kann als SingleNAL (0) oder Non-interleaved (1) konfiguriert werden. Die Vorlage verwendet standardmäßig SingleNAL ().

Die Konfiguration von einzelnen oder mehreren Telefonereignissen wird ebenfalls unterstützt. Während der Codec-Aushandlung sendet der Client alle konfigurierten Codecs, einschließlich des Telefonereignisses. Nachdem der Audiocodec ausgewählt ist, sucht er im Angebot nach Telefonereignissen. Verfügt das Angebot über das Telefonereignis mit der Abtastrate des ausgehandelten Audiocodecs, so wird dieses Telefonereignis ausgewählt. Andernfalls wird das erste Telefonereignis in der Liste verwendet.

Wenn mindestens ein Telefonereignis ausgehandelt wurde, werden die Dual-Tone-Multifrequenzen (DTMF) als RTP-Pakete mit dem entsprechenden Payload-Typ gesendet. Und wenn überhaupt keine Telefonereignisse ausgehandelt werden, werden die DTMFs als RTP-Pakete mit dem Nutzlasttyp des ausgehandelten Audiocodecs gesendet. Out-of-Band-Mechanismus zur Bereitstellung von DTMFs wird von der Webex-App nicht unterstützt.

Beispiel für konfigurierte Codecs:

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

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

6.1.34.1 AI-Codec

Ab Version 44,8 unterstützt die Webex-App einen neuen Audio-Codec – KI-Codec (xCodec). Dieser Audiocodec wird bei ungünstigen Netzbedingungen verwendet, um eine bessere Gesprächsqualität zu erreichen. 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 AI Codec funktioniert nur in Kombination mit dem Opus Codec. Dies bedeutet, dass sowohl der Opus- als auch der AI-Codec von beiden Seiten während der SDP-Verhandlung angekündigt 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, auch bekannt als "Free Calling", geleitet. In manchen Umgebungen ist dies nicht erwünscht und solche Anrufe sollten blockiert werden.

Cisco – vertraulich

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

Die folgende Konfiguration bietet diese Möglichkeit.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	wahr	wahr, falsch	Steuert, ob die SIP-URI durch Locus geleitet (true) oder blockiert (false) werden soll.

6.1.36 Anrufprotokoll

Die Webex-App unterstützt das Anrufprotokoll, um die Anrufe für den Benutzer nachzuverfolgen. Für die primäre Leitung des Benutzers wird das Anrufprotokoll über alle Geräte des Benutzers synchronisiert. Für die sekundären Leitungen (gemeinsam genutzt und virtuell) bewahrt die App nur lokale Datensätze zum Anrufprotokoll auf.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	wahr, falsch	Steuert nur für die Hauptleitung, ob die Anwendung das einheitliche Anrufprotokoll oder das clientseitige (lokale) Anrufprotokoll verwenden soll.

6.1.37 Videoanrufe deaktivieren

Mit Version 41,9 wurde die Möglichkeit zum Deaktivieren von Videoanrufen hinzugefügt. Es gibt separate Konfigurationsoptionen zur Steuerung dieser Funktion für BroadWorks-gestützte und Locus (kostenlose) VoIP-Anrufe.

Wenn das Merkmal aktiviert ist und das Merkmal-Tag auf "false" gesetzt ist:

- der Benutzer sieht die Einstellung "Eingehende Anrufe bei eingeschaltetem Video annehmen" nicht
- alle eingehenden Videoanrufe werden, wenn sie angenommen werden, zu Audioanrufen
- der Nutzer kann einen Anruf nicht auf Video umstellen 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 diese Funktion für den Desktop eingeschaltet und für Handy und Tablet ausgeschaltet.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SIP_VIDEOCALLS_WXT%	wahr	wahr, falsch	Steuert die Verfügbarkeit von SIP-Videoanrufen über BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	wahr	wahr, falsch	Steuert die Verfügbarkeit von (kostenlosen) Locus-Videoanrufen.
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Desktop - wahr Mobiltelefon/ Tablet – false	wahr, falsch	Steuert den Standardwert für die Einstellung "Eingehende Anrufe bei eingeschaltetem Video annehmen".

6.1.38 Notrufe (911) – Standortberichte beim E911-Anbieter

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	false	wahr, falsch	Aktiviert die E911-Plattform für den Notfall-Standort des Anbieters.
%BWE911-PRIMARY-HELDURL%	leer	Schnur	Gibt die URL zur E911-Anbieter-Notfallstandort-Plattform an, die das HELD-Protokoll unterstützt.
%BWE911-CUSTOMERID%	leer	Schnur	Die Kunden-ID (HeldOrgId, CompanyID), die für die E911-Anbieter-HTTPS-Anforderung verwendet wird.
%BWE911-SECRETKEY%	leer	Schnur	Der Geheimschlüssel zur Authentifizierung der HTTPS-Anforderung des E911-Anbieters.
%BWE911-EMERGENCY-NUMBER-LIST%	leer	CSV-Zeichenfolge	Die Liste der vom E911-Anbieter unterstützten Notfallnummern.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (der Benutzer wird nicht mehr gefragt)	Nummer [0 - 43200]	Die Zeitüberschreitung in Minuten, die verwendet wird, um den Benutzer daran zu erinnern, den Notfallstandort zu aktualisieren, wenn der aktuelle Standort nicht eingegeben oder ungültig ist. Der vorgeschlagene Wert, wenn Sie sich für die Aktivierung entscheiden: 1440 (ein Tag).
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (Benutzer kann den Dialog immer abbrechen)	Nummer [-1 - 100]	Gibt an, wie oft 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 können das Dialogfeld immer abbrechen) ▪ N = 0 (der 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, einmal_pro_Anmeldung	einmal_pro_Anmeldung	Definiert das Eingabeverhalten für den E911-Standort. Der Wert "aggressive" zeigt dem Benutzer den Dialog bei jedem Netzwechsel zu einem unbekannten Standort, während der Wert "once_per_login" den Dialog nur einmal anzeigt und so weitere Popups und Ablenkungen für den Benutzer verhindert.

HINWEIS 1: BWE911-***-Tags sind „dynamische integrierte System-Tags“. Weitere Informationen finden Sie im Abschnitt *5.7 Cisco BroadWorks Dynamic integrierte System-Tags*.

HINWEIS 2: Wenn VOIP-Anrufe deaktiviert sind, ist der einzige aussagekräftige Wert für die Notrufwahlsequenz (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) nur cs-only.

Cisco – vertraulich

6.1.39 PAI als Identität

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

Wenn das aktivierte Attribut des Tags auf „true“ gesetzt ist, wird die PAI-Kopfzeile vorrangig gegenüber der From-Kopfzeile verwendet. Diese Identität des Anrufers wird verwendet, um den Kontakt aufzulösen und ihn 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.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	wahr, falsch	Steuert, ob die Identität des Anrufers, die dem Benutzer präsentiert wird, aus den SIP From- oder SIP P-Asserted-Identity-Headern übernommen werden soll. Auf "true" gesetzt, um den PAI-Header mit Priorität zu verwenden.

6.1.40 Bildschirmfreigabe deaktivieren

Mit der Version 42,5 können Sie die Verfügbarkeit der Bildschirmfreigabe steuern. Wenn die Bildschirmfreigabe deaktiviert ist:

- der Benutzer sieht nicht die Option, die Bildschirmfreigabe bei 1-1-Anrufen zu initiieren
- die eingehenden Anfragen zur gemeinsamen Nutzung des Bildschirms werden abgelehnt und der Benutzer erhält eine entsprechende Meldung

Diese Funktion ist standardmäßig aktiviert.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SCREEN_SHARE_WXT%	wahr	wahr, falsch	Gibt an, ob die Bildschirmfreigabe für den Benutzer aktiviert werden soll.

Cisco – vertraulich

6.1.41 Spam-Anruf-Anzeige

Wenn der Funktionsumschalter (je Bereitstellungstyp) aktiviert und die Funktion in der Konfigurationsdatei aktiviert ist, verarbeitet die Webex-App den neuen Parameter, der den Verifizierungsstatus des Spam-Anrufs angibt, wenn sie als Teil der Push-Benachrichtigung „NewCall“ oder des Anrufprotokolls empfangen werden.

Etikett	Standard wert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	wahr, falsch	Kontrolliert die Verfügbarkeit der Spam-Anrufanzeige im Bildschirm für eingehende Anrufe und im Anrufprotokoll nur für Webex Calling.

6.1.42 Entfernen von Geräuschen und Erweiterung der Bandbreite für PSTN-/Mobilanrufe

Die Geräuschunterdrückung bietet Calling-Benutzern ein besseres Anruferlebnis, wenn sie mit Nicht-Webex-Benutzern über PSTN oder Mobilgeräte sprechen. Mit Version 43.12 ist die Rauschunterdrückung standardmäßig aktiviert.

In Version 44,2 der Webex-App werden neue Verbesserungen der Sprach-KI für eingehende Audiomedien für Schmalband-PSTN-Anrufe eingeführt.

- Ein neuer Algorithmus zur Bandbreitenerweiterung verbessert die Audioqualität, indem er die Bandbreite des schmalbandigen PSTN-Spektrums erweitert und das Rauschen entfernt. Die erweiterte Bandbreite erhöht die Verständlichkeit und verringert die Ermüdung des Hörers.
- Der bereits vorhandene Algorithmus zur Rauschunterdrückung wurde verbessert, indem die Einschränkungen für Wartemusik und andere Töne (z. B. Pieptöne) aufgehoben wurden.
- Wenn diese Funktion aktiviert ist, sieht der Benutzer die Anzeige "Smart Audio - extern" und kann die Sprach-KI-Erweiterungen für die eingehenden Audiomedien steuern.

Standardmäßig sind diese Spracherweiterungen aktiviert und eingeschaltet. Der Benutzer kann den Ausgangszustand über die Smart-Audio-Einstellungen in den Audio-Voreinstellungen steuern.

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	false	wahr, falsch	Aktiviert die Spracherweiterungen für externe (eingehende) Medien.

HINWEIS: Das Entfernen von Geräuschen ist jetzt Teil der zusätzlichen Sprachverbesserungen, und das Tag wurde durch das neue Tag eingestellt. Das benutzerdefinierte Tag %ENABLE_NOISE_REMOVAL_WXT% für die Geräuschentfernung ist ebenfalls veraltet.

6.1.43 QoS-DSCP-Markierung

Die QoS-DSCP-Markierung wird von den Webex-App-Anrufmedien-RTP-Paketen (Audio und Video) unterstützt. DSCP bestimmt die Verkehrsklassifizierung für Netzwerkdaten. Auf diese Weise kann festgestellt werden, welcher Netzwerkverkehr mehr Bandbreite benötigt, eine höhere Priorität hat und mit größerer Wahrscheinlichkeit Pakete fallen lässt.

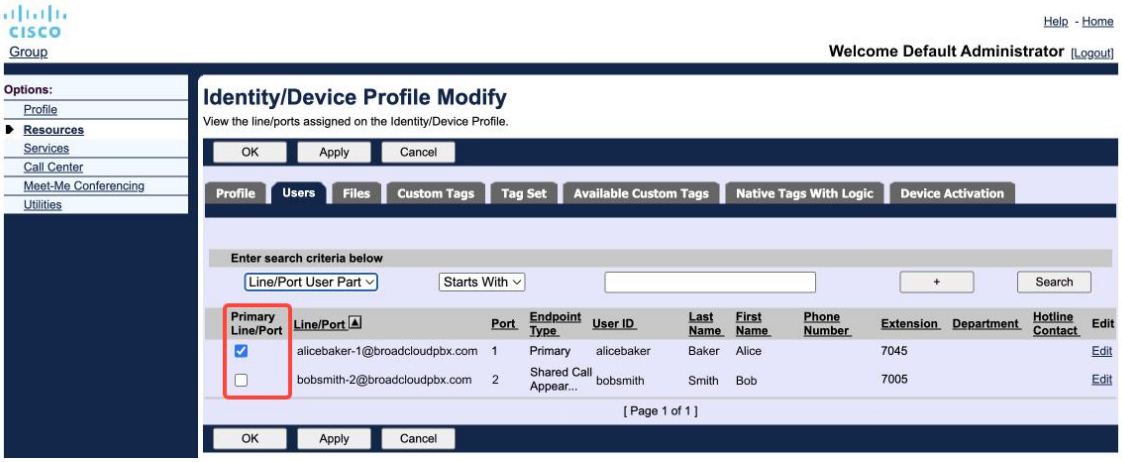
HINWEIS: Aktuelle Versionen des Microsoft Windows-Betriebssystems erlauben es Anwendungen nicht, DSCP oder UP für ausgehende Pakete direkt einzurichten. Stattdessen ist die Bereitstellung von Gruppenrichtlinienobjekten (Group Policy Objects, GPO) erforderlich, um DSCP-Markierungsrichtlinien basierend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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_AUDIO_QOS_WXT%	wahr	wahr, falsch	Aktiviert QoS für Audioanrufe.
%AUDIO_QOS_VALUE_WXT%	46	0-63	Gibt den QoS-Wert für den ausgewählten QoS-Typ für die Audioanrufe an. Hinweis: Der Standardwert wird verwendet, wenn kein Wert angegeben wird oder der Wert nicht erfolgreich geparst werden konnte.
%ENABLE_VIDEO_QOS_WXT%	wahr	wahr, falsch	Aktiviert QoS für Videoanrufe
%VIDEO_QOS_VALUE_WXT%	34	0-63	Gibt den QoS-Wert für den ausgewählten QoS-Typ für die Videoanrufe an. Hinweis: Der Standardwert wird verwendet, wenn kein Wert angegeben wird oder der Wert nicht erfolgreich geparst werden konnte.

Cisco – vertraulich

6.1.44 Primäres Profil

Mit der Integration der gemeinsam genutzten Leitungen (*6.1.51.1 Desktop – Darstellung gemeinsam genutzter Leitungen***Error! Reference source not found.**). Wenn die Leitung des Benutzers mit einem anderen Benutzer geteilt wird, können mehrere Profile des gleichen Typs für den Benutzer konfiguriert sein. Um das richtige Profil für die Anmeldung bei den Telefondiensten auszuwählen, wurde Cisco BroadWorks verbessert, um anzuzeigen, ob ein Benutzer ein Gerät besitzt, d. h. es ist die primäre Leitung/der primäre Port für ein Gerät zugewiesen. Weitere Informationen zur Cisco BroadWorks-Aktualisierung finden Sie unter Besitzermarkierung In Geräteliste zur Unterstützung von gemeinsam genutzten Webex-Client-Leitungen.



Konfiguration der primären Leitung/Port für das Identitäts-/Geräteprofil im Verwaltungsportal

Ab Version 43,2 wird eine neue Konfigurationsoption (*Gerätebesitzer-Einschränkung*) hinzugefügt, um zu steuern, ob die primäre Profileinschränkung angewendet werden soll. Er kann verwendet werden, um der Webex-Anwendung zu ermöglichen, ein nicht-primäres Leitungs-/Portprofil für die Anmeldung der Telefondienste zu verwenden. Diese Konfigurationsoption gilt für alle Konfigurationen, unabhängig von der Anzahl der für den Benutzer konfigurierten Profile (**Wenn die Beschränkung des Geräteeigentums aktiviert ist und es kein Gerät mit primärer Leitung/Port für die entsprechende Plattform gibt, werden die Telefondienste keine Verbindung herstellen**).

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	wahr	wahr, falsch	Steuert die Einschränkung des Gerätebesitzers - ob die Telefondienste das primäre Profil für das angegebene Gerät verwenden sollen

HINWEIS: Es wird empfohlen, die Eigentumsbeschränkung zu aktivieren. Wenn diese Option deaktiviert ist, verwenden die Telefondienste das erste gefundene Profil für die Anmeldung, und es kann zu Problemen kommen, wenn für den Benutzer mehrere Profile desselben Typs konfiguriert sind.

6.1.45 Sperrliste (nur Webex Calling)

Beginnend mit 43,5 der Webex-App wird eine benutzerdefinierte Sperrliste mit Telefonnummern eingeführt. Wenn die Funktion aktiviert ist, kann der Benutzer festlegen, dass eingehende Anrufe von bestimmten Nummern serverseitig blockiert und auf keinem der Geräte des Benutzers zugestellt werden. Der Benutzer kann diese blockierten Anrufe in der Anrufliste sehen.

Der Benutzer kann die Sperrliste an zwei Stellen konfigurieren - Anrufeinstellungen und Anrufliste. In den Einstellungen kann der Benutzer die Liste der blockierten Nummern einsehen und bearbeiten. In der Anrufliste kann der Benutzer die Anrufprotokolle der durch die benutzerdefinierte Sperrliste blockierten Anrufe einsehen. Diese Datensätze haben die Anzeige "Gesperrt", wenn die Nummer in der benutzerdefinierten Sperrliste enthalten ist, und der Benutzer hat die Möglichkeit, die Sperrung der Nummer für den jeweiligen Datensatz direkt aufzuheben. Die Option Block ist ebenfalls verfügbar.

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

Nummernformat

- Blockieren der Anrufeinstellungen, E.164-Formatbeschränkung lokal in der Webex-App anwenden
- Die Sperre aus dem Anrufprotokoll ist für alle Webex Calling-Datensätze zulässig.
- Cisco BroadWorks kann Anforderungen für neue Nummern, die in der Sperrliste hinzugefügt werden, 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 in Cisco BroadWorks konfiguriert und auf alle WxC-Geräte für den Benutzer angewendet. Diese Funktion funktioniert mit der vom Administrator definierten Sperrliste, die vom Benutzer nicht konfiguriert werden kann und nur von Administratoren über den Control Hub gesteuert werden kann. Für eingehende Anrufe, die durch die vom Administrator definierte Sperrliste blockiert werden, gibt es KEINE Aufzeichnungen über die Anrufliste.

Die benutzerdefinierte Sperrliste wird nach der STIR/SHAKEN-, der verwaltungsdefinierten Sperrliste und den Richtlinien zur Abweisung anonymer Anrufe angewendet.

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


Cisco – vertraulich

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_BLOCK_WXT%	wahr	wahr, falsch	Aktiviert die benutzerdefinierte Blockliste Setzen Sie diese Option auf "true", um die Sperrliste in den Anrufeinstellungen und der Anrufliste zu sehen.

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

6.1.46 Umsetzung der Medienanpassung und Resilienz (MARI)

6.1.46.1 Tarifanpassung

Die Webex-Anwendung verfügt bereits über adaptive Medienqualitätstechniken, um sicherzustellen, dass das Audio nicht durch Videopaketverlust beeinträchtigt wird, und um sicherzustellen, dass Video die Anpassung der Videolate nutzen kann, um die in Zeiten der Überlastung genutzte Bandbreite zu verwalten.

Die Ratenanpassung oder dynamische Bitratenanpassung passt die Gesprächsrate an die verfügbare variable Bandbreite an, indem sie die Videobitrate je nach Paketverlust herunter- oder hochfährt. Ein Endpunkt reduziert die Bitrate, wenn er Nachrichten vom Empfänger erhält, die auf einen Paketverlust hinweisen; sobald der Paketverlust zurückgegangen ist, wird die Bitrate erhöht.

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

6.1.46.2 Korrektur von Weiterleitungsfehlern (Forward Error Correction, FEC) und Packet Retransmission (Packet Retransmission, RTX)

Ab Version 43,4 fügt die Webex-App dem Medienanpassungsmechanismus die Unterstützung für FEC (Forward Error Correction) und RTX (Packet Retransmission) für Audio- und Videomedien hinzu.

FEC bietet Redundanz für die übertragenen Informationen, indem ein vorher festgelegter Algorithmus verwendet wird. Die Redundanz ermöglicht es dem Empfänger, eine begrenzte Anzahl von Fehlern zu erkennen und zu korrigieren, ohne dass er den Sender um zusätzliche Daten bitten muss. FEC gibt dem Empfänger die Möglichkeit, Fehler zu korrigieren, ohne einen Rückkanal (z. B. RTCP) zu benötigen, um die erneute Übertragung von Daten anzufordern.

Die Endpunkte verwenden FEC nicht bei Bandbreiten unter 768 kbps. Außerdem muss der Paketverlust mindestens 1,5 % betragen, bevor FEC eingeführt wird. Die Endpunkte überwachen in der Regel die Wirksamkeit des FEC, und wenn der FEC nicht effizient ist, wird er nicht verwendet.

Cisco – vertraulich

FEC verbraucht mehr Bandbreite als eine erneute Übertragung, hat aber eine geringere Verzögerung. RTX wird verwendet, wenn eine geringe Verzögerung zulässig ist und Bandbreitenbeschränkungen bestehen. Im Falle einer großen 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 zu einer höheren Bandbreitennutzung aufgrund redundanter Videodaten, aber es führt nicht zu zusätzlichen Verzögerungen bei der Wiederherstellung verlorener Pakete. RTX hingegen trägt nicht zu einer höheren Bandbreitennutzung bei, da die RTP-Pakete nur dann erneut übertragen werden, wenn der Empfänger einen Paketverlust im RTCP-Rückkanal anzeigt. RTX führt zu einer Verzögerung bei der Wiederherstellung von Paketen, da das RTCP-Paket vom Sender zum Empfänger und das neu übertragene Paket vom Sender zum Empfänger gelangen muss.

FEC muss aktiviert sein, damit RTX aktiviert werden kann.

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

```
                        <order>RTX_SRTP</order>
                    </rtx>
                </mari>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_AUDIO_MARI_FEC_WXT%	false	wahr, falsch	Aktiviert FEC für Audioanrufe
%ENABLE_AUDIO_MARI_RTX_WXT%	false	wahr, falsch	Aktiviert RTX für Audioanrufe (erfordert aktivierten Audio-FEC)
%ENABLE_VIDEO_MARI_FEC_WXT%	false	wahr, falsch	Aktiviert FEC für Videoanrufe
%ENABLE_VIDEO_MARI_RTX_WXT%	false	wahr, falsch	Aktiviert RTX für Videoanrufe (erfordert aktiviertes Video-FEC)

6.1.47 Gleichzeitige Anrufe mit demselben Benutzer

Hinzufügen der Unterstützung für gleichzeitige Anrufe mit demselben Benutzer auf einem einzigen Gerät.

Diese Funktion ist für einige Einsätze nützlich, bei denen die präsentierte Identität des Anrufs nicht mit der verbundenen Identität übereinstimmt. Dies führt dazu, dass keine Übermittlung an den ursprünglichen Teilnehmer eingeleitet werden kann. Wenn Sie diese Funktion aktivieren, können Sie mehrere gleichzeitige Anrufe mit demselben Fernteilnehmer führen.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false	wahr, falsch	Gibt an, ob die Webex-App nur einen oder mehrere WxC-Anrufe mit demselben Benutzer durchführen kann.

Cisco – vertraulich

6.1.48 RTCP-XR

Ab Version 43,8 fügt die Webex-App die Aushandlung für den Austausch von RTCP-XR-Paketen während eines Anrufs hinzu. Die Aushandlung erfolgt während des Aufbaus der SIP INVITE-Sitzung. Wenn beide Endpunkte RTCP-XR-Pakete unterstützen, startet die Webex Media Engine mit dem Austausch dieser Pakete und unterstützt den adaptiven Anrufqualitätsmechanismus. Diese Option ist standardmäßig aktiviert.

Zusätzlich werden diese zusätzlichen Metriken nur für Webex Calling über SIP BYE gesendet und auf diese Weise im Control Hub offengelegt.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	wahr	wahr, falsch	Ermöglicht die RTCP-XR-Aushandlung und den Austausch von Paketen für eine bessere Gesprächsqualität. Standardmäßig aktiviert.

6.1.49 Informationen zur Anrufweiterleitung

Version 44,2 der Webex-App führt eine konfigurierbare Option ein, um die Sichtbarkeit der Informationen zu Anrufweiterleitung und Umleitung in den anrufbezogenen Bildschirmen und dem Anrufprotokoll zu steuern.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	wahr	wahr, falsch	Steuert die Sichtbarkeit der Informationen zur Anrufweiterleitung und -umleitung. Setzen Sie diese Option auf "true", um die Informationen in den anrufbezogenen Bildschirmen und der Anrufliste zu sehen.

6.1.50 Anrufer-ID

6.1.50.1 Ausgehende Anrufer-ID

Webex Mobile (Version 44,2) und Desktop (Version 44,3) Apps bieten dem Benutzer eine neue Möglichkeit, die bevorzugte externe Anrufer-ID für ausgehende Anrufe auszuwählen. Die Liste der verfügbaren Optionen umfasst:

Cisco – vertraulich

- Direktdurchwahl (Standard)
- Standortnummer
- Benutzerdefinierte Nummer der gleichen Organisation
- Anrufwarteschlangen, zu denen der Benutzer gehört, so dass die Agenten ihre Anrufer-ID-Nummer verwenden können
    - Wenn DNIS-Optionen konfiguriert sind, können sie ausgewählt werden
- Sammelanschlüsse, zu denen der Benutzer gehört, ermöglichen es Agenten, ihre Anrufer-ID-Nummer zu verwenden
- Anrufer-ID ausblenden

Anmerkungen:

- Die Liste der Optionen hängt von der jeweiligen Zeile ab:
    - Primäre Linie - vollständige Palette von Optionen
    - Gemeinsame Leitungen - nicht verfügbar
    - Virtuelle Leitungen - nur Anrufwarteschlangenoptionen
- Wenn die bereits ausgewählte Identität nicht mehr verfügbar ist, wird die Standard-Anrufer-ID des Benutzers verwendet.
- Notrufe verwenden immer die Notrufnummer des Benutzers
- Das Tag wird im Abschnitt deaktiviert

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	wahr, falsch	Ermöglicht die Auswahl der Rufnummer des Anrufers für ausgehende Anrufe.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	false	wahr, falsch	Steuert die Verfügbarkeit der für den Benutzer konfigurierten zusätzlichen Nummern.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	false	wahr, falsch	Steuert die Verfügbarkeit der für den Benutzer konfigurierten Callcenter-Nummern (DNIS).
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	wahr, falsch	Kontrolliert die Verfügbarkeit der für den Benutzer konfigurierten Sammelanschlussnummern.
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	wahr, falsch	Aktiviert die Blockierung der Anrufer-ID als Auswahl für ausgehende Anrufe.

HINWEIS: Die Version der Desktop-App 44,3 unterstützt nur Call Center-CLID und 44,4 fügt Unterstützung für die restlichen Optionen hinzu.

6.1.50.2 Name der Remote-Anrufer-ID

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

- Gemeinsame Benutzeridentität
- Kontaktdienst (benutzerdefinierte Kontakte)
- Outlook-Kontakte (Desktop)
- Lokales Adressbuch (Mobil)

Im Falle einer erfolgreichen Kontaktauflösung mit einer der Suchquellen wird der Anzeigename der Gegenstelle aktualisiert. Wenn der Kontakt in CI gefunden wird, ist die Anrufsitzung auch mit den Webex-Cloud-Diensten desselben Benutzers verknüpft und bietet die Möglichkeit, den Avatar und die Anwesenheit des Remote-Teilnehmers zu sehen, einen Chat durchzuführen, den Bildschirm freizugeben, die Option zum Eskalieren zu einem Webex-Cloud-Meeting usw.

Mit der Version 44,5 der Webex-App wird eine konfigurierbare Option hinzugefügt, mit der die Kontaktauflösung ignoriert und der Cisco BroadWorks-Anzeigename für Anrufe mit Arbeitsbereichen oder einem RoomOS-Gerät, die für 1:1 Cisco BroadWorks-Anrufe verwendet werden, immer beibehalten wird.

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	gelöst	aufgelöst, sip	Steuert den Anzeigenamen des Fernteilnehmers für Arbeitsbereiche und RoomOS-Geräte. Verwenden Sie "sip", um die Kontaktauflösung zu ignorieren und den in der SIP-INVITE-Sitzung empfangenen Anzeigenamen zu verwenden.

Cisco – vertraulich

6.1.51 Mehrere Leitungen

Der Webex-Benutzer kann eine primäre Leitung und bis zu 9 sekundäre Leitungen haben. Sekundäre Leitungen können gemeinsam genutzt oder virtuell sein (nur Webex Calling). Für die Webex für BroadWorks-Bereitstellung funktioniert die Desktop-App nur mit gemeinsam genutzten Leitungen und die Funktion wird in der mobilen App nicht unterstützt.

Die Webex-App erhält die Leitungskonfiguration über die DMS-Konfigurationsdatei, die bei der Anmeldung und bei jedem Zeitrahmen von 12h heruntergeladen wird. Wenn eine Aktualisierung der Leitungskonfiguration erkannt wird, wird der Benutzer aufgefordert, die Anwendung neu zu starten, um die Änderungen zu übernehmen. Durch eine erneute Anmeldung des Benutzers werden Aktualisierungen der Leitungskonfiguration erkannt und sofort angewendet.

Im Folgenden wird der Abschnitt der DMS-Konfigurationsvorlage in Bezug auf die Unterstützung mehrerer Leitungen für Desktop und Mobile dargestellt.

```
<config>
<protocols>
   <sip>
       <lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
          <personal>
              <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
          </personal>
          <line lineType="%BW-MEMBERTYPE-1%">
              <external-id>%BWUSEREXTID-1%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-1%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
1%</conference-service-uri>
              <domain>%BWHOST-1%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
             ...
          </line>
          <line lineType="%BW-MEMBERTYPE-2%">
              <external-id>%BWUSEREXTID-2%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-2%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
2%</conference-service-uri>
              <domain>%BWHOST-2%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>

             ...
          </line>
          ...
          <line lineType="%BW-MEMBERTYPE-10%">
              <external-id>%BWUSEREXTID-10%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-10%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
10%</conference-service-uri>
              <domain>%BWHOST-10%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-10%</group-call-pickup>
             ...
          </line>
```

Verwenden Sie das dedizierte benutzerdefinierte Tag, um die Funktion mit mehreren Leitungen zu steuern.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_MULTI_LINE_WXT%	false	wahr, falsch	Aktiviert die Unterstützung mehrerer Leitungen (falls konfiguriert). Ist diese Funktion deaktiviert (auf "false" gesetzt), wird nur die erste konfigurierte Zeile von der Anwendung verwendet.

HINWEIS 1: Die Funktion Unterstützung für den Chef-Admin (Führungskraft-Assistent) ist nicht in Kombination mit einer Konfiguration mit mehreren Leitungen verfügbar.

ANMERKUNG 2: Weitere BroadWorks-Anforderungen finden Sie unter „Darstellung einer gemeinsam genutzten Leitung“ im Webex-for-Cisco-BroadWorks-Lösungsleitfaden.

6.1.51.1 Desktop – Darstellung gemeinsam genutzter Leitungen

Ab Version 42,12 fügt die Webex-Anwendung Unterstützung für gemeinsam genutzte Leitungen hinzu. Der Administrator sollte für jede gemeinsam genutzte Leitung die gemeinsamen Anrufe einrichten.

Version 43,12: Die Webex-App wurde verbessert, sodass ein gehaltener Anruf auf einer gemeinsam genutzten oder virtuellen Leitung verschoben (lokal fortgesetzt) werden kann, der von einem anderen Benutzer oder demselben Benutzer auf einem anderen Gerät bearbeitet wird. Weitere Informationen finden Sie unter *6.2.12 Anruf verschieben*.

6.1.51.2 Desktop – Virtuelle Leitungen (nur Webex Calling)

Nur für die Webex Calling-Bereitstellung unterstützt die Webex-App die Konfiguration mehrerer Leitungen mit virtuellen Leitungen. Funktional entspricht die Konfiguration mit virtuellen Leitungen der Konfiguration mit mehreren Leitungen unter Verwendung gemeinsam genutzter Leitungen. Sie können die für den Benutzer konfigurierten virtuellen Leitungen sehen und für eingehende und ausgehende Anrufe verwenden.

Die Version 43,4 erweitert die Unterstützung für virtuelle Leitungen durch Hinzufügen von Gruppenanruf parken und Anruf parken abrufen.

Version 43,12: Die Webex-App wurde verbessert, sodass ein gehaltener Anruf auf einer gemeinsam genutzten oder virtuellen Leitung verschoben (lokal fortgesetzt) werden kann, der von einem anderen Benutzer oder demselben Benutzer auf einem anderen Gerät bearbeitet wird. Weitere Informationen finden Sie unter *6.2.12 Anruf verschieben*.

6.1.51.3 Mobil (nur Webex Calling)

Nur für die Webex Calling-Bereitstellung bietet Version 45,4 die Unterstützung für mehrere (gemeinsam genutzte und virtuelle) Leitungen in der mobilen Version der Webex-App. Die Leitungszuweisung gilt sowohl für die Desktop- als auch für die mobile Webex-App.

Aufgrund der Besonderheiten der mobilen Plattform können die Benutzer bis zu zwei gleichzeitige Anrufe auf einer der Leitungen führen.

HINWEIS 1: Wenn „Anrufe mit nativem Dialer“ aktiviert ist (siehe *6.3.5.1 Anrufen mit Native Dialer*), sind mehrere Leitungen deaktiviert.

HINWEIS 2: Die Mehrzeiligkeit für die Tablet-Version wird nicht unterstützt.

6.1.52 Verbesserte SIP-Autorisierung

Die Version 45,4 der Webex-App bietet konfigurierbare Optionen zur Optimierung der SIP-Kommunikation, indem die Autorisierung zwischen allen SIP-Sitzungen freigegeben wird. Die App speichert die Autorisierung und verwendet sie erneut, bis sie noch gültig ist.

Diese Funktion beschleunigt die SIP-Kommunikation zwischen dem Server und der Webex-App, reduziert den Datenverkehr, reduziert die Verbindungszeit für Anrufe und verbessert die Gesamtleistung der Webex-App.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	wahr, falsch	Wenn „true“ (wahr) festgelegt ist, ist die Verbesserung der SIP-Autorisierung aktiviert.

ANMERKUNG 1: Einige SBCs erfordern möglicherweise eine neue SIP-Autorisierung für jede Sitzung, daher sollte diese Funktion gemäß den spezifischen Bereitstellungsspezifikationen verwendet werden.

HINWEIS 2: Selbst wenn diese Funktion aktiviert ist und die Webex-App 401 „Nicht autorisiert“ erhält, wird in der nächsten SIP-Anfrage eine neue Autorisierung verwendet.

6.1.53 Persönlicher Assistent (Abwesenheitsstatus)

Mit Version 44,11, der mobilen Webex-App, und Version 45,3, der Desktop-Webex-App, wird die Integration mit dem Cisco BroadWorks Personal Assistant (PA)-Dienst hinzugefügt. Es funktioniert in Kombination mit der Abwesenheitspräsenz des Benutzers und erfordert eine Synchronisierung des PA-Status mit der Webex Cloud-Präsenz.

Der Beschallungsdienst bietet dem Benutzer die Möglichkeit, die Anrufer über den Grund der Nichterreichbarkeit des angerufenen Teilnehmers zu informieren und ihnen optional mitzuteilen, wann der angerufene Teilnehmer zurückkehren wird und ob ein Vermittlungsdienst den Anruf entgegennimmt.

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

Der Benutzer kann nur die manuelle PA-Konfiguration vornehmen. Wenn es Termine gibt, die sich auf den PA-Dienst auswirken, wird die Anwesenheit über den Personal Assistant Status Sync aktualisiert. Die Webex-App veröffentlicht jedoch nicht die Zeitplankonfiguration und die Zeitpläne, die sich auf die PA auswirken.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	wahr, falsch	Steuert, ob die Anwesenheitsfunktion "Abwesend" für den Benutzer verfügbar ist.

ANMERKUNG 1: Diese Funktion setzt voraus, dass der Personal Assistant Status Sync im Partner Hub aktiviert ist.

HINWEIS 2: Die Anrufverteilung für den persönlichen Assistenten wird nicht wirksam, wenn die Dienste „Ruhefunktion“, „Immer anrufen“ oder „Selektive Anrufweiterleitung“ aktiv sind.

ANMERKUNG 3: Die manuellen Anwesenheitszustände "Nicht stören" und "Besetzt" haben im Vergleich zu "Abwesend" eine höhere Priorität. Wenn der Benutzer manuell einen dieser Anwesenheitsstatus aktiviert, führt die Aktivierung des Persönlichen Assistenten nicht dazu, dass Ihr Anwesenheitsstatus auf Abwesend wechselt.

Cisco – vertraulich

6.2 Nur Desktop-Funktionen

6.2.1 Erzwungene Abmeldung

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

Diese Funktion wird in einigen Bereitstellungen benötigt, in denen ähnliche Clients gleichzeitig online sein können, was zu Nebeneffekten führen kann. Ein Beispiel ist ein Benutzer mit einem Desktop-Rechner am Arbeitsplatz und zu Hause, bei dem die eingehenden Anrufe nur von einem der beiden Clients empfangen werden, 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 *bsoft-call-info* Parameterwert. Wenn Cisco BroadWorks mehrere Client-Instanzen online mit derselben *Appid* erkennt, sendet es ein spezielles SIP NOTIFY an die ältere Client-Instanz, wodurch sie sich abmeldet. Desktop-Clients hätten beispielsweise einen identischen *appid-value* , obwohl es keine Beschränkung für die Verwendung dieses Bezeichners auf der Client-Seite gibt. Der *appid-value* wird vom Dienstanbieter konfiguriert.

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

Informationen zu den Cisco BroadWorks-Patches und -Versionen, die für diese Funktion benötigt werden, finden Sie im Abschnitt zu Cisco BroadWorks-Softwareanforderungen im *Webex für Cisco BroadWorks-Lösungsleitfaden*.

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_FORCED_LOGOUT_WXT%	false	wahr, falsch	Ermöglicht die erzwungene Abmeldung.
%FORCED_LOGOUT_APPID_WXT%	leer	Schnur	Appid, die auf der Serverseite für die Korrelation verwendet wird. Dies kann eine beliebige Zeichenkette sein. Beispiel: "123abc"

Cisco – vertraulich

6.2.2 Anrufannahme

Die Anrufübernahme ist ein Mehrbenutzerdienst, der es ausgewählten Benutzern ermöglicht, jede läutende Leitung innerhalb ihrer Anrufübernahmegruppe zu beantworten. Eine Anrufübernahmegruppe wird vom Administrator definiert und ist eine Untergruppe der Benutzer in der Gruppe, die die Anrufe der anderen Benutzer übernehmen können.

Die folgenden Abholvorgänge werden unterstützt:

- Blinde Rufannahme
- Gezielte Anrufübernahme (die es einem Benutzer ermöglicht, einen an ein anderes Telefon in seiner Gruppe gerichteten Anruf anzunehmen, indem er den entsprechenden Funktions-Zugangscode gefolgt von der Nebenstelle des klingelnden Telefons wählt).

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	wahr, falsch	Setzen Sie diese Option auf "true", um Blind Call Pickup zu aktivieren.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	wahr, falsch	Legen Sie den Wert auf „true“ fest, um die gezielte Anrufübernahme zu aktivieren.

6.2.3 Unterstützung von Chef-Admin (Führungskraft-Assistent)

Die Funktion „Boss-Admin“ in Cisco BroadWorks als „Führungskraft/Assistent“ bezeichnet, ermöglicht es einem Assistenten, im Namen einer Führungskraft zu arbeiten, um Anrufe als „Führungskraft“ zu filtern, zu beantworten und zu tätigen. Ein Assistent kann viele Führungskräfte haben, und das ist auch möglich:

- Wählen Sie die gewünschte Rolle, wenn Sie einen Anruf tätigen.
- Nehmen Sie einen eingehenden Anruf im Namen einer Führungskraft entgegen und leiten Sie den Anruf dann an die Führungskraft weiter. Darüber hinaus sind alle üblichen Optionen für das Anrufmanagement verfügbar.
- Vergewissern Sie sich, dass ein eingehender Anruf tatsächlich für die Führungskraft bestimmt ist.

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

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

Cisco – vertraulich

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	wahr, falsch	Auf "true" setzen, um die Boss-Admin-Funktion zu aktivieren.

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

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

Der Client stellt die Funktion zur Verfügung, um einen laufenden SIP-Anruf über Webex Calling an ein Meeting weiterzuleiten. Wenn diese Funktion anstelle einer Standard-Ad-hoc-Konferenz verwendet wird, kann der Nutzer während der Besprechung sowohl Video als auch Bildschirmfreigabe nutzen.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	wahr, falsch	Legen Sie den Wert auf „true“ fest, um die Menüoption „Zu Webex-Meeting eskalieren“ zu aktivieren.

6.2.5 Anrufe mit Steuerung des Tischtelefons – Automatische Anrufannahme

Die automatische Beantwortung ermöglicht es dem Benutzer, Desk Phone Control (DPC) für ausgehende Anrufe auf dem Client zu verwenden, um MPP-Telefone ohne Berührung zu verwalten.

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

Die automatische Antwort kann auf primären und nicht primären Geräten funktionieren. Wenn der Benutzer mehr als ein registriertes Tischtelefon hat, mit dem es gekoppelt werden kann, wird nur das ausgewählte/gekoppelte Gerät automatisch geantwortet.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	wahr	wahr, falsch	Wenn diese Option auf "wahr" gesetzt ist, wird die automatische Beantwortung der Anrufe über das Tischtelefon aktiviert.

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

6.2.6 Automatische Anrufannahme mit Tonbenachrichtigung

Diese Funktion ermöglicht die automatische Annahme von eingehenden Anrufen für lokale Geräte, wenn dies in der Anfrage für eingehende Anrufe angegeben ist.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_AUTO_ANSWER_WXT%	false	wahr, falsch	Wenn auf "true" gesetzt, wird die automatische Annahme eingehender Anrufe aktiviert, wenn dies vom Backend angefordert wird.

6.2.7 Tischtelefonsteuerung - Mid Call Controls - Konferenz

Diese Funktion aktiviert die Optionen „Konferenz“ und „Zusammenführen“ für Remote-Anrufe (XSI), die an einem anderen Standort beendet wurden.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	wahr, falsch	Wenn „true“ festgelegt ist, werden die Optionen „Konferenz“ und „Zusammenführen“ für Remote-Anrufe (XSI) aktiviert, die an einem anderen Standort beendet werden.

6.2.8 Benachrichtigungen für Anrufannahme

Benachrichtigungen bei Anrufübernahme geben dem Benutzer die Möglichkeit zu erfahren, wenn ein Anruf bei einem Benutzer eingeht, den er zur Überwachung konfiguriert hat. Benachrichtigungen zur Anrufübernahme können für Watchlists empfangen werden, die über die Dienste Anrufübernahmegruppe und Besetztlampenfeld konfiguriert wurden.

Anrufübernahme-Benachrichtigungen 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 Webex-Desktop-Anwendung zeigt eine Benachrichtigung an, wenn ein Mitglied in seiner BLF-Watchlist (Besetztlampenfeld) einen eingehenden Anruf im Benachrichtigungsstatus hat. Die Benachrichtigung enthält Informationen über den Anrufer und den Benutzer, der den eingehenden Anruf erhalten hat, sowie die Optionen, den Anruf anzunehmen, die Benachrichtigung stumm zu schalten oder zu ignorieren. Die Annahme des eingehenden Anrufs durch den Benutzer löst die gezielte Anrufübernahme aus.

Ab Version 43,4 ist die Liste der mit Besetztlampenfeld überwachten Benutzer im Fenster „Mehrere Anrufe“ (MCW) für Anrufe verfügbar (nur für Windows verfügbar). Die Integration der BLF-Liste in die MCW umfasst:

Überwachen Sie die eingehenden Anrufe mit der Option, den Anruf anzunehmen oder den Alarm zu ignorieren.

Siehe die vollständige Liste der BLF-Benutzer.

Überwachen Sie die Präsenz der Benutzer – Rich Presence ist nur für Benutzer mit Berechtigung für die Webex Cloud verfügbar. Die Basispräsenz (Telefonie) ist nur für BroadWork-Nutzer verfügbar.

Starten Sie einen Anruf mit einem BLF-Benutzer.

Starten Sie einen Chat mit einem Besetztlampenfeld-Benutzer – nur für Benutzer mit Berechtigung für Webex Cloud verfügbar.

Fügen Sie einen Besetztlampenfeld-Benutzer als Kontakt hinzu.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	wahr, falsch	Ermöglicht die Überwachung des Besetztlampenfelds und die Benachrichtigung über das Klingeln für andere Benutzer mit der Möglichkeit, die Anrufe entgegenzunehmen.

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_BLF_DISPLAY_CALLER_WXT%	wahr	wahr, falsch	Ermöglicht die Anzeige des Anrufernamens/der Anrufernummer in der Klingelbenachrichtigung.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Legt fest, um wie viele Sekunden die Klingelbenachrichtigung verzögert werden soll, bevor sie dem Benutzer angezeigt wird.

HINWEIS: Diese Funktion hängt vom Dienst der gezielten Anrufübernahme ab.

6.2.8.2 Anrufannahmegruppe (nur Webex Calling)

Ab Version 44,2 bietet die Webex-Anwendung Unterstützung für GCP-Benachrichtigungen (Group Call Pickup) für die Webex Calling-Bereitstellung. Sie ermöglicht die Benachrichtigung der Benutzer über eingehende Anrufe für alle Benutzer, die über die Anrufübernahmegruppe überwacht werden.

Bei einem eingehenden Anruf für einen Benutzer, der zu einer Anrufübernahmegruppe gehört, erhält der Angerufene die Möglichkeit, den Anruf entgegenzunehmen. Es gibt eine GCP-Benachrichtigungsverzögerung, die über Control Hub konfiguriert werden kann. Wenn der Angerufene den Anruf nicht innerhalb der konfigurierten Zeit bearbeitet, wird eine GCP-Benachrichtigung an die Gruppe gesendet.

Wenn mehrere Anrufe innerhalb derselben Anrufübernahmegruppe eingehen, werden sie in der Reihenfolge ihres Eingangszeitpunkts bearbeitet. Die Meldung des ältesten Anrufs wird zunächst der Gruppe zugestellt, und sobald sie bearbeitet ist, wird die nächste Meldung in der Reihe an die Gruppe zugestellt.

Die Benachrichtigungen können je nach Konfiguration im Control Hub-Administrationsportal nur akustisch, nur visuell oder akustisch und visuell sein. Wenn eine visuelle GCP-Benachrichtigung angezeigt wird, kann der Benutzer den Anruf mit der Anrufübernahmefunktion annehmen. Wenn die Benachrichtigung „Nur Audio“ konfiguriert ist, sieht der Benutzer keine visuelle Benachrichtigung für den eingehenden Anruf, hört einen bestimmten Klingelton und kann den Anruf über das in der Webex-App verfügbare Menü „Anrufübernahme“ oder indem er den FAC-Code (*98) und die Durchwahl manuell wählt.

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

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

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	wahr, falsch	Aktiviert die Benachrichtigung über die Übernahme von Gruppenanrufen
%ENABLE_GCP_DISPLAY_CALLER_WXT%	wahr	wahr, falsch	Ermöglicht die Anzeige des Anruferanzeigenamens/der Anrufernummer in der Klingelbenachrichtigung
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5-120	Legt fest, wie lange eine GCP-Benachrichtigung für den Benutzer maximal verfügbar ist
%BWGROUP-CALL-PICKUP-BOOL-n%	false	wahr, falsch	Zeigt an, ob für die entsprechende Leitung eine Anrufübernahmegruppe konfiguriert ist

ANMERKUNG 1: Dies ist eine reine Webex Calling-Funktion.

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

6.2.9 Event-Paket für Remotesteuerung

Für Click-to-Dial-Clients wie den BroadWorks-Empfangs-Thin-Client und den Go-Integrator, bei dem die Webex-App das anrufende Gerät ist, ehrt die Webex-App jetzt das Event-Paket mit Remotesteuerung, wenn sie einen Anruf erhalten oder Halten/Fortsetzen bearbeiten.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false	wahr, falsch	Bei der Einstellung "true" wird angegeben, dass die Fernsteuerung für den Benutzer aktiviert werden soll.

6.2.10 Survivability Gateway (nur Webex Calling)

Ab Version 43,2 fügt die Webex-Anwendung Unterstützung für den Survivability-Anrufmodus hinzu. Wenn die Funktion aktiviert ist und keine Webex Cloud-Konnektivität vorhanden ist, kann die Webex-Anwendung im Survivability-Modus ausgeführt werden. In diesem Modus stehen dem Benutzer nur eingeschränkte Anruffunktionen zur Verfügung.

Das Local Survivability Gateway wird vom Kunden eingesetzt.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	wahr, falsch	Aktiviert die Unterstützung des Survivability-Modus.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Gibt die Rückfallzeit an (Survivability-Gateway zur SSE)

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

6.2.11 Event-Paket für Remote-Stummschaltungssteuerung (nur Webex Calling)

Ab Version 43,9 bietet die Webex-App Unterstützung für die Remotesteuerung zum Stummschalten von Anrufen des Audiomedienstreams. Auf diese Weise kann ein laufender Anruf von einem anderen Standort wie dem BroadWorks Receptionist Thin Client, bei dem die Webex-App das anrufende Gerät ist, stumm- bzw. freigeschaltet werden.

Die Funktion hängt von dem neuen SIP *x-cisco-mute-status* info Paket ab. Wenn die Kopfzeile *Recv-Info:x-cisco-mute-status* beim Einrichten der SIP INVITE-Sitzung des Anrufs empfangen wird, sendet die Webex-App SIP INFO mit *Info-Package:x-cisco-mute-status;muted=true* (oder *muted=false*) zurück, wobei der stummgeschaltete Parameter den aktualisierten Status des Audiomedien-Streams darstellt.

Die Stummschaltung oder Aufhebung der Stummschaltung kann lokal oder von einem entfernten Standort aus ausgelöst werden. Die Fernaktualisierung löst ein SIP NOTIFY mit *Event aus: stummschalten* (oder *Stummschaltung aufheben*), um vom Anwendungsserver an die Webex-App gesendet zu werden. Die Webex-App honoriert die Remote-Anforderung und sendet nach der Aktualisierung des Audiomedien-Stream-Status ein SIP NOTIFY mit dem Inhalt *Info-Package:x-cisco-mute-status;muted=true* (oder *muted=false*) zurück.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false	wahr, falsch	Wenn „true“ (wahr) festgelegt ist, ist die Remote-Stummschaltung für den Benutzer aktiviert.

6.2.12 Anruf verschieben

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

Ab Version 43,12 wurde die Webex-App verbessert, sodass auch für die gemeinsam genutzten und virtuellen Leitungen Anrufe an einem anderen Standort angezeigt werden. Solche Anrufe sind im Bereich der laufenden Anrufe zu Informationszwecken und ohne die Möglichkeit, sie zu steuern, sichtbar. Nur wenn ein solcher Anruf in die Warteschleife gelegt wird, kann der Benutzer ihn auf das lokale Gerät verschieben, indem er ihn auswählt und vom Anrufbildschirm aus wieder aufnimmt. Dieser Mechanismus ist nützlich, wenn der Anruf von demselben Benutzer an einem anderen Standort oder von einem anderen Benutzer über dieselbe Leitung getätigt wurde.

Beachten Sie, dass es in der Webex-App nicht möglich ist, einen gehaltenen Anruf auf ein gekoppeltes Gerät zu verschieben. Wenn der Benutzer mit einem Gerät gekoppelt ist, muss er zuerst die Verbindung trennen und kann dann das gehaltene Gespräch lokal wieder aufnehmen.

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

Die Überwachung der Anrufe für die Hauptleitung des Benutzers hängt von den XSI-Ereignissen (Advanced Call Event Package) ab, und das Verschieben eines Anrufs zum lokalen Gerät ist für diese Anrufe nicht möglich. Für diese Art von Anrufen kann der Benutzer die Funktion Call Pull (*6.1.22 Anrufübergabe*) verwenden. Das Ziehen von Anrufen 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 der Warteschleife gehalten werden.

- Anwendung Fall 1:
    a. Alice hat Bobs Leitung für die Telefonprofile Desktop und Desk zugewiesen.

Cisco – vertraulich

b. Alice führt ein Gespräch mit Charlie über das Tischtelefon - Alice kann das laufende Gespräch in der Desktop-App sehen.

c. Alice setzt den Anruf vom Tischtelefon aus in die Warteschleife - der Anruf kann von Alice über die Desktop-App wieder aufgenommen werden.

- Anwendung Fall 2:
  a. Alice hat Bobs Leitung für die Telefonprofile Desktop und Desk zugewiesen.
  b. Bob hat einen Anruf mit Charlie – Alice kann den laufenden Anruf in der Desktop-App sehen.
  c. Bob legt das Gespräch mit Charlie in die Warteschleife - Alice kann das Gespräch mit Charlie über die Desktop-App wieder aufnehmen.
- Anwendung Fall 3:
  a. Alice hat Bobs Leitung für die Telefonprofile Desktop und Desk zugewiesen.
  b. Alice ist über die Desktop-App mit seinem Tischtelefon gekoppelt.
  c. Bob hat einen Anruf mit Charlie – Alice kann den laufenden Anruf in der Desktop-App sehen.
  d. Bob hält den Anruf mit Charlie – Alice kann den Anruf mit Charlie nicht über die Desktop-App fortsetzen.
  e. Alice trennt die Verbindung zwischen der Desktop-App und dem Tischtelefon - Alice kann das Gespräch mit Charlie über die Desktop-App wieder aufnehmen.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALL_MOVE_HERE_WXT%	false	wahr, falsch	Ermöglicht die Rufumleitung auf dem lokalen Gerät. Wird für Halten/Fortsetzen an verschiedenen Standorten/Benutzern im Anwendungsfall mit mehreren Leitungen verwendet.

6.3 Funktionen nur für Mobilgeräte

6.3.1 Notrufe

Webex for Cisco BroadWorks unterstützt native Notrufe.

Wenn die Funktion aktiviert ist, analysiert die Anwendung beim Einleiten eines abgehenden VoIP-Anrufs die gewählte Nummer und vergleicht sie mit der Liste der konfigurierten Notrufnummern. Wenn die Nummer als Notruf identifiziert wird, führt die Anwendung das konfigurierte Wahlverhalten aus. Sie ist mit dem Tag *dial-sequence* konfigurierbar.

Unterstützte Modi sind:

- cs-only – Der Client tätigt Notrufe nur über das Mobilfunknetz, wenn das Netzwerk verfügbar ist.
- cs-first - Beim Auslösen eines Notrufs überprüft der Client den Netztyp, mit dem das aktuelle Gerät verbunden ist. Wenn das Mobilfunknetz verfügbar ist, tätigt der Client den Anruf über das Mobilfunknetz. Wenn das Mobilfunknetz nicht verfügbar ist, aber ein mobiles Daten-/WiFi-Netz verfügbar ist, führt der Client den Anruf über das mobile Daten-/WiFi-Netz als VoIP-Anruf. Wenn der Notruf über das Mobilfunknetz getätigt wird, schlägt der Client dem Benutzer vor, den Notruf als VoIP erneut zu versuchen.
- Nur VoIP – Der Client tätigt Notrufe nur als VoIP, wenn das Mobilfunk-Daten-/WLAN-Netzwerk verfügbar ist.
- cs-voip - Der Client analysiert, ob das Gerät den Anruf als nativen leitungsvermittelten (CS) Anruf initiieren kann (ohne zu berücksichtigen, ob das CS-Netz verfügbar ist oder nicht). Wenn das Gerät einen nativen 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 Notrufwahlsequenz (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) nur cs-only.

Bei der Anmeldung wird dem Benutzer eine Haftungsausschlussmeldung für Notrufe angezeigt. Sie wird nicht über die Konfigurationsoptionen gesteuert.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_EMERGENCY_DIALING_WXT%	false	wahr, falsch	Auf "true" setzen, um die Notruferkennung zu aktivieren. Der Standardwert ist leer.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	cs-nur	Nur cs-first, cs-first, nur VoIP, cs-voip	Steuert den Wählsequenzmodus für Notrufe.
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	CSV-Liste	CSV-Liste der Notrufnummern. Beispiel: 911,112

Cisco – vertraulich

6.3.2 Pushbenachrichtigungen für Anrufe

Bei einem eingehenden Anruf erhält der mobile Client zunächst eine Push-Benachrichtigung (PN). Es gibt einen Konfigurationsparameter, der verwendet werden kann, um zu steuern, wann die SIP REGISTER-Sitzung aufgebaut werden soll:

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

Der zweite Ansatz wird empfohlen. Im Vergleich zum ersten Fall kommt es jedoch zu einer gewissen Verzögerung, bevor der Anruf aufgebaut wird.

Gemäß den iOS-Anforderungen 13 sollten die VoIP-PNs nur für eingehende Anrufe verwendet werden. Für die übrigen aufrufbezogenen Ereignisse sollten reguläre PNs verwendet werden.

Um diese Anforderung zu erfüllen, wird eine neue API für die PN-Registrierung eingeführt, für die ein entsprechender Patch auf dem Anwendungsserver installiert werden muss. Wenn das Backend nicht für die Unterstützung der iOS-PNs konfiguriert ist13 , kann der Konfigurationsparameter verwendet werden, um die Verwendung der älteren Push-Benachrichtigungen zu erzwingen, bei denen alle anrufbezogenen Ereignisse über VoIP-PNs bereitgestellt werden.

Es gibt eine Push-Benachrichtigung, die vom Application Server (AS) gesendet wird, wenn ein läutender Anruf vom Angerufenen an einem anderen Standort angenommen, vom Anrufer beendet oder z. B. an Voicemail weitergeleitet wird. Mit dem iOS 13 ist diese Art von Push-Benachrichtigung jetzt regulär und hat einige Einschränkungen. Sie kann durch den Apple Push Notification Service (APNS) verzögert oder sogar überhaupt nicht zugestellt werden. Um fehlende oder verzögerte Call Update PNs zu behandeln, wurde eine konfigurierbare Klingelzeitüberschreitung hinzugefügt, um die maximale Klingelzeit zu kontrollieren. Wenn die maximale Rufzeit erreicht ist, wird das Klingeln für den Angerufenen beendet und der Anruf als verpasst behandelt. Auf der Seite des Anrufers kann der Anruf im Klingelzustand verbleiben, bis die auf dem Anwendungsserver (AS) konfigurierte Klingel-ohne-Antwort-Richtlinie ausgeführt wird.

Um das Anwendungsverhalten konsistent zu halten, gilt der konfigurierbare Klingelton-Timer für Android und iOS.

Eine separate Konfigurationsoption wurde hinzugefügt, um das Verhalten bei der Ablehnung von Anrufen festzulegen, wenn ein eingehender Anruf als Push-Benachrichtigung empfangen wird. Der Client kann so konfiguriert werden, dass er den Anruf ignoriert oder über Xsi an den Server antwortet und die Ablehnung auf „true“ oder „false“ gesetzt wird. In diesem Fall werden die zugewiesenen Cisco BroadWorks-Anrufbehandlungsdienste angewendet. Wenn "decline_false" konfiguriert ist, klingelt der Anruf so lange, bis der Anrufer aufgibt oder der Zeitgeber für die Nichtbeantwortung abläuft, und die zugehörigen Anrufbehandlungsdienste beginnen. Wenn "decline_true" konfiguriert ist, gibt der Ablehnungsgrund die Bearbeitung des Anrufs an. Wenn der Ablehnungsgrund auf "besetzt" gesetzt ist, erzwingt der Server sofort den Besetztdienst. Wenn "temp_unavailable" konfiguriert ist, wird der Dienst für die vorübergehende Nichtverfügbarkeit angewendet.

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


Cisco – vertraulich

```
    <calls>
        <reject-with-xsi mode="%REJECT_WITH_XSI_MODE_WXT%"
        declineReason="%REJECT_WITH_XSI_DECLINE_REASON_WXT%"/>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	wahr, falsch	Steuert, wann die SIP-REGSITER-Sitzung aufgebaut wird - beim Empfang einer Push-Benachrichtigung für einen 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	ignore, decline_true, decline_false	Legt das Verhalten bei der Ablehnung von Anrufen fest.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	beschäftigt	beschäftigt, temp_unverfügbar	Gibt den Grund für die Ablehnung des Anrufs an, wenn der Ablehnungsmodus auf "decline_true" eingestellt ist.

6.3.2.1 Nachrichtenwartesignal (MWI)

Wenn die MWI-Funktion 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. Zum Beispiel, wenn der Benutzer die Voicemail-Nachrichten hört oder sie innerhalb des mobilen Webex-Clients als gelesen markiert (die Anzahl der ungelesenen Nachrichten nimmt ab). Es gibt keine konfigurierbare Option, um dies zu steuern.

Weitere Informationen zu MWI finden Sie im Abschnitt *6.1.27 Voicemail, visuelle Voicemail, Anzeige für wartende Nachrichten*.

6.3.2.2 Splash anklingeln

BroadWorks-Dienste (z. B. DND) können bei der Umleitung eingehender Anrufe Klingelhinweise senden. Der Webex Mobile-Client kann so konfiguriert werden, dass die Push-Benachrichtigungen für Klingelton aktiviert und dem Benutzer angezeigt werden, wenn diese durch BroadWorks ausgelöst werden.

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_RING_SPLASH_WXT%	false	wahr, falsch	Aktiviert Ring Splash in der BroadWorks-Konfiguration.

6.3.2.3 Bereitstellungsmodus (nur Webex Calling)

Die Webex-App nutzt den Benachrichtigungs-Push-Server (NPS), um Push-Benachrichtigungen für Anrufe an APNS/FCM bereitzustellen. Die Version 45,2 der Webex-App unterstützt jetzt drei verschiedene Bereitstellungsmodi, um zu konfigurieren, wie die anrufbezogenen Push-Benachrichtigungen an APNS/FCM übermittelt werden sollen:

- nps - aktueller Mechanismus, der den NPS verwendet
- Cloud – verbesserter Mechanismus unter Verwendung von Cisco Webex Cloud Microservice
- extern - ein Mechanismus, der das System eines Dritten nutzt. Es erfordert die Integration des Drittanbietersystems mit der Cisco WebHooks-Engine

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	NPS	nps, wolke, extern	Gibt den Zustellungsmodus der Push-Benachrichtigungen für Anrufe an.

6.3.3 Einzelne Warnungen

Die Funktion Mobile Single Alert ist für Fixed-Mobile Convergence (FMC) / Mobile Network Operator (MNO) Bereitstellungen gedacht, die den BroadWorks Mobility Service nutzen. Ohne diese Funktion erhält der Benutzer, wenn er beim Webex-Client angemeldet ist und einen eingehenden Anruf erhält, gleichzeitig zwei Anrufe – einen nativen und einen Push-Benachrichtigungs-Anruf (VoIP). Wenn die Funktion aktiviert ist, deaktiviert die Anwendung die Mobilitätswarnung für den BroadWorks Mobility-Standort des Benutzers bei der Anmeldung und aktiviert die Warnung bei der Abmeldung. Eine wichtige Voraussetzung für die Nutzung dieser Funktion ist, dass dem Benutzer der BroadWorks Mobility-Dienst zugewiesen und genau ein Standort konfiguriert wurde.

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


Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_SINGLE_ALERTING_WXT%	false	wahr, falsch	Setzen Sie diesen Wert auf "true", um die Einzelbenachrichtigung zu aktivieren.

6.3.4 Click to Dial (Rückruf)

Die abgehende Click to Dial-Funktion stellt sicher, dass der Endbenutzer einen Anruf auf seinem persönlichen Circuit Switched Mobiltelefon entgegennehmen und seine Unternehmens-DN als Rufnummer angeben kann.

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

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

Wenn ein Benutzer einen Click-to-Dial-Anruf einleitet, wird der Bildschirm für ausgehende Anrufe mit Informationen über eingehende Anrufe an dem ausgewählten SNR-Standort angezeigt. Dieser Bildschirm wird nach einem konfigurierbaren Timer automatisch geschlossen.

Beim Trennen der Verbindung von einem SNR-Standort registriert sich die Anwendung erneut für Push-Benachrichtigungen bei eingehenden Anrufen.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_DIALING_CALL_BACK_WXT%	false	wahr, falsch	Setzen Sie diese Option auf "true", um Click to Dial (Rückruf) zu aktivieren.
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Steuert die Anzahl der Sekunden, bevor der Rückruf-Bildschirm automatisch geschlossen wird.

6.3.5 MNO-Unterstützung

6.3.5.1 Anrufen mit Native Dialer

Diese Funktion bietet Unterstützung für Bereitstellungen von Mobilfunknetzbetreibern (MNO), die den BroadWorks Mobility (BWM) Service nutzen. Es wird davon ausgegangen, dass dem Benutzer der BroadWorks Mobility-Dienst zugewiesen wurde und mindestens ein Standort konfiguriert wurde.

Die Fähigkeit des Benutzers, Anrufe über das native Wählgerät zu tätigen, wird durch das Konfigurations-Tag **native** gesteuert. Wenn diese Option aktiviert ist, wird die Anwendung das native Wählprogramm starten und den Anruf tätigen. Darüber hinaus wird die Verfügbarkeit von VoIP-Anrufen über das Tag **voip** gesteuert - je nach den Einsatzanforderungen können VoIP-Anrufe aktiviert oder deaktiviert werden.

Wenn VoIP und Native Calling aktiviert sind, kann der Benutzer wählen, welche Option er verwenden möchte.

Mit dem Tag können Benutzer auswählen, wie eingehende und ausgehende Anrufe gestartet bzw. empfangen werden. Erfordert, dass sowohl der native als auch der VoIP-Anruf aktiviert sind.

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

Diese Funktion ist hilfreich für Kunden, die MNO-Bereitstellungen verwenden, bei denen Anrufe anstatt an den integrierten Cisco BroadWorks-Anwendungsserver umgeleitet zu werden, die FAC-Codes möglicherweise vom Telecom-Backend verarbeitet werden. Ein neues -Tag wird im Abschnitt hinzugefügt, das von den Telekommunikationsunternehmen zur Lösung des Problems verwendet werden kann.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_DIALING_VOIP_WXT%	wahr	wahr, falsch	Setzen Sie diesen Wert auf "true", um die VoIP-Anrufoption zu aktivieren.
%ENABLE_DIALING_NATIVE_WXT%	false	wahr, falsch	Legen Sie den Wert auf „true“ fest, um die native Anrufoption zu aktivieren.
%ENABLE_DIALING_MODE_WXT%	false	wahr, falsch	Ermöglicht die Auswahl des Anrufmodus durch den Benutzer über die Anrufeinstellungen in den Präferenzen.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%DIALING_MODE_DEFAULT_WXT%	VoIP	voip, nativ	Gibt den gewählten Standardaufrufmodus an.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false	wahr, falsch	Steuert, ob die Verfügbarkeit des nativen Anrufs von der Zuweisung des BroadWorks Mobility-Dienstes und dem für den Benutzer konfigurierten Mobility-Standort abhängen soll.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*leer*	Schnur	Gibt ein Präfix an, das vorangestellt werden soll, wenn ein ausgehender Anruf zu einer Nummer, die mit einem FAC-Code beginnt, als Mobilfunkanruf eingeleitet wird. Standardmäßig ist kein FAC-Präfix definiert und das Tag ist leer.

ANMERKUNG 1: Mindestens eine der Funktionen **voip** und **native** sollte aktiviert sein.

HINWEIS 2: Wenn nur der **native** Aufruf aktiviert ist, wird bei MNO-Einsätzen 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 bei MNO-Einsätzen empfohlen, die Einzelbenachrichtigung zu aktivieren, um eine doppelte Benachrichtigung zu vermeiden.

6.3.5.2 Anrufsteuerungen

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

- Der BroadWorks Mobility (BWM)-Dienst wird dem Benutzer zugewiesen,
- Es ist nur eine einzige BMW Mobile Identity konfiguriert,
- Der Benutzer wählt den Modus "Native Calling" aus (weitere Informationen finden Sie in Abschnitt *6.3.5.1 Anrufen mit Native Dialer),*
- Bei BroadWorks ist ein Anruf verankert, der über den BMW-Dienst läuft,
- Auf dem mobilen Gerät läuft ein Mobilfunkgespräch.

Version 43,1 ermöglicht eine bessere Handhabung der beratenden Übergabe, indem eine Verknüpfung zwischen den beiden Mobilfunkanrufen hergestellt wird, die in der Webex-App angezeigt werden, und dem Benutzer eine Option zum Abschließen der Übergabe bietet. Wenn der Benutzer zwei unabhängige Mobilfunkanrufe auf demselben Gerät hat, wurde das Übertragungsmenü so erweitert, dass die Übertragung eines Anrufs auf den anderen möglich ist, auch wenn keine Verbindung zwischen den beiden hergestellt wurde.

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_XSI_CALL_CONTROL_WXT%	false	wahr, falsch	Aktiviert die XSI-Anrufsteuerung für die MNO-Umgebung.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Steuert den von der Anwendung verwendeten XSI MNO-Bereitstellungstyp. Mögliche Werte: ▪ MNO_Access - zeigt alle Remote (XSI)-Aufrufe mit den im unteren Knoten definierten Gerätetypen. ▪ MNO_Network - zeigt alle Ferngespräche (XSI) an.
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	Schnur	Der/die Gerätetypenname(n), der/die in der Bereitstellungsart MNO_Access verwendet werden soll(en).
%ENABLE_XSI_HOLD_CALLS_WXT%	wahr	wahr, falsch	Steuert, ob die Aktion "Anruf halten" für den Benutzer bei XSI-Mobilanrufen verfügbar sein soll.

6.3.5.3 Identität der ausgehenden Anrufleitung (Outgoing Calling Line Identity, CLID) – Dual Persona

Mit der mobilen Version 42,12 ermöglicht die Webex-App Benutzern, ihre CLID (Calling Line Identity) auszuwählen, die dem Remoteteilnehmer angezeigt wird, wenn ein ausgehender Anruf initiiert wird.

Wenn der Benutzer mit Cisco BroadWorks-Mobilität konfiguriert ist, was einer typischen Konfiguration für Mobilnetzbetreiber-Bereitstellungen entspricht, und native Anrufe aktiviert sind, kann der Benutzer auswählen, welche Identität den angerufenen Personen angezeigt werden soll. Der Benutzer kann seine geschäftliche oder persönliche Identität wählen. Es besteht auch die Möglichkeit, die eigene Identität zu verbergen und den Anruf als Anonym zu präsentieren.

Bei VoIP-Anrufen hat der Benutzer auch die Möglichkeit, seine CLID zu kontrollieren. In diesem Fall besteht die einzige verfügbare Option darin, zu kontrollieren, ob er seine Identität verbergen will oder nicht.

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

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


Cisco – vertraulich

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	false	wahr, falsch	Aktiviert die Bereitstellungsblockierung der Anrufleitungs-ID. Sie gilt für alle Arten von ausgehenden Anrufen des Benutzers.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	false	wahr, falsch	Aktiviert die persönliche Verwaltung für native Anrufe, wenn der Bereitstellungstyp als MNO_Access oder MNO_Network konfiguriert ist. (BroadWorks Mobility wird für die nativen Anrufe verwendet und alle nativen Anrufe sind in BroadWorks verankert)

6.3.5.4 Benachrichtigung bei nativen Anrufen

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	wahr	wahr, falsch	Aktiviert das Abonnement für die Push-Benachrichtigung MOBILE_CALL_INFO.

6.3.5.5 Native Anrufe in konvergente Besprechungen verschieben

Für Benutzer, die mit MNO bereitgestellt werden, ermöglicht diese Funktion, dass ein nativer Sprachanruf für beide Parteien eines 1:1-Anrufs zu einem Meeting eskaliert wird (auch wenn der andere Teilnehmer kein Webex-Benutzer ist). Wenn der Remote-Benutzer ein Webex-Benutzer ist, haben die Teilnehmer nach der Teilnahme an einem Meeting die folgenden Möglichkeiten:

- Webex im Meeting-Chat initiieren
- Video hinzufügen (beachten Sie, dass der Ton während des ursprünglichen Anrufs weiterläuft)
- Bildschirm/Inhalt freigeben

- Aufzeichnung von Meetings auslösen

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	wahr, falsch	Ermöglicht das Einschalten (Einladen und Treffen, Video-Meeting-Aktionen).

6.3.5.6 MNO-Mobilität – Widget im Anruf

In der Version 43,7 der Android Webex-App (Mobil und Tablet) wird offiziell ein neues Anrufsteuerungs-Widget (Blase) eingeführt, das über den Mobilitätsdienst eine zusätzliche Anrufsteuerung für native Anrufe bietet, die in Cisco BroadWorks verankert sind. Das Widget wird oben auf der nativen Benutzeroberfläche angezeigt und ermöglicht dem Benutzer die folgenden Aktionen:

- Halten / Fortsetzen
- Übergabe ohne Rücksprache – Schaltet den Benutzer in das Übergabedialogfeld in der Webex-App ein.
- Übergabe abschließen – bietet die Möglichkeit, die beratende Übergabe abzuschließen (Version 43,1)
- Video-Meeting – Verschiebt die Teilnehmer in ein Webex-Meeting.
- Anruf beenden

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_WIDGET_HOLD_CALLS_WXT%	wahr	wahr, falsch	Steuert die Verfügbarkeit der Aktion Halten im Anruf-Widget.

Cisco – vertraulich

%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	wahr	wahr, falsch	Steuert die Verfügbarkeit der Aktionen Übergabe und Übergabe abschließen im Anruf-Widget.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	wahr	wahr, falsch	Steuert die Verfügbarkeit der Aktion Video-Meeting im Anruf-Widget.

6.3.6 ID des eingehenden Anrufers

Mit der Version 44,2 können Sie die Kontaktinformationen steuern, die dem Benutzer basierend auf dem Namen und der Nummer angezeigt werden. Es wurden zwei Konfigurationsoptionen hinzugefügt, mit denen die Informationen gesteuert werden können, die dem Benutzer auf dem Bildschirm für eingehende Anrufe und Benachrichtigungen über eingehende Anrufe sowie über verpasste Anrufe angezeigt werden.

6.3.6.1 Bildschirm für eingehende Anrufe

Es gibt Plattformunterschiede zwischen Android und iOS, wenn es um die Anzeige von Daten im Bildschirm für eingehende Anrufe geht. Die Informationen für eingehende Anrufe werden wie folgt angezeigt:

Android – Im Bildschirm für eingehende Anrufe sind zwei separate Felder vorhanden, in denen der Name und die Nummer angezeigt werden.

iOS – es gibt nur ein Feld, in dem entweder der Name oder die Nummer angezeigt werden – wenn beide verfügbar sind, hat der Name Priorität.

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

6.3.6.2 Benachrichtigung bei eingehendem Anruf

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

Die neue Konfigurationsoption für die eingehenden Anrufe steuert auch die Informationen, die in den Benachrichtigungen über 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 dem Namen an (Format: *Name (Nummer)*). Dieses Verhalten der Webex-App gilt sowohl für Android als auch für iOS.

Cisco – vertraulich

6.3.6.3 Benachrichtigung bei entgangenen Anrufen

Es wurde ein zusätzlicher Konfigurationsparameter für die Benachrichtigung über verpasste Anrufe hinzugefügt. Sie kann verwendet werden, um die Informationen über den Fernteilnehmer zu steuern, ähnlich wie bei den Benachrichtigungen über eingehende Anrufe, so dass die Nummer an den Anzeigenamen des Fernteilnehmers angehängt und in der Benachrichtigung über entgangene Anrufe angezeigt werden kann. Dieses Verhalten der Webex-App gilt sowohl für Android als auch für iOS.

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

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false	wahr, falsch	Steuert, ob die Nummer an den Namen im Bildschirm für eingehende Anrufe (nur iOS) und Benachrichtigungen angehängt werden soll.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	false	wahr, falsch	Steuert, ob die Nummer an den Namen in der Benachrichtigung über verpasste Anrufe angehängt werden soll.

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

7 Merkmale des frühen Feldversuchs (BETA)

7.1 Notrufe (911) – Cisco Emergency Location Information Service (nur Webex Calling) und Konfigurationsbereinigung

Die Webex-App unterstützt bereits Notfallstandort für Notrufe mithilfe von Drittanbietern, wie unter 6.1.36 1x38d="1" />*6.1.38* dokumentiert.Notrufe (911) – Standortberichte beim E911-Anbieter Diese Funktion gilt nur für Notrufe bei Notrufen an PSAPs (Public Safety Answering Points) in den USA, ihren Gebieten (Guam, Puerto Rico und Jungferninseln) und Kanada.

Exklusiv für die Webex Calling-Bereitstellung hat Cisco einen eigenen Dienst für Standortinformationen für den Notfall hinzugefügt, um HELD/HELD+-Interaktionen abzuwickeln und zu speichern, von Unternehmen und Benutzern erstellte Drahtkarten zu verwalten, Adressen mit ihren PIDF-LO-Attributen zu speichern und die Standortinformationen für Notrufe zu senden.

Version 45,1 der Webex-App fügt die Integration mit dem Cisco Emergency Location Service hinzu. Die DMS-Konfigurationsvorlage wurde aktualisiert, um Unterstützung für verschiedene Notrufstandortanbieter hinzuzufügen:

- Der aktuelle Abschnitt unter der DMS-Konfigurationsvorlage ist veraltet. Stattdessen wird ein neuer Abschnitt hinzugefügt, der in Zukunft von der Webex-App verwendet wird.
- Im neuen Abschnitt ist jetzt eine neue *Anbieteroption* verfügbar, die die Steuerung des Notrufstandortanbieters ermöglicht, den die Webex-App verwenden sollte. Zu den verfügbaren Optionen gehören *redsky*, *intrado*, *9line* und *webex*. Die ersten drei Optionen sind für die Webex für BroadWorks-Bereitstellung verfügbar und werden hauptsächlich für Verfolgungszwecke verwendet, wobei das HELD+-Protokoll für die Kommunikation mit Drittanbietern verwendet wird. Die *Webex* -Option ist nur für die Webex Calling-Bereitstellung verfügbar und ermöglicht der App die Nutzung des Cisco Emergency Location Information Service mit verbesserter Unterstützung für die Leitungskarte und PIDF-LO für Notrufe.
- Es wurden neue benutzerdefinierte Tags hinzugefügt, die eine manuelle Einrichtung erfordern, die der aktuellen Konfiguration entspricht (wenn die Funktion bereits verwendet wird). Ohne festgelegt zu werden, werden die Standardwerte verwendet, die die Funktion deaktivieren oder das Verhalten ändern können
- Die System-Tags für , , und werden nicht aktualisiert.
- [**Wichtig**] Verhindern Sie, dass die Notfallstandortfunktion aufgrund von Fehlkonfigurationen deaktiviert wird, und stellen Sie sicher, dass das neue benutzerdefinierte Tag, mit dem die Verfügbarkeit der Notfallstandortfunktion (%ENABLE_EMERGENCY_LOCATION_WXT%) gesteuert wird, auf dieselbe Weise festgelegt ist wie das ältere Tag (%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%).

Cisco – vertraulich

- [**Wichtig**] Damit diese kritische Funktion nicht aufgrund von Fehlkonfigurationen verloren geht, wurde der Webex-App eine Abwärtskompatibilitätslogik hinzugefügt. Wenn der neue Konfigurationsabschnitt in der Vorlage fehlt oder das neue benutzerdefinierte Tag (%ENABLE_EMERGENCY_LOCATION_WXT%) nicht konfiguriert ist, wodurch das Attribut aktiviert auf „false“ gesetzt wird, versucht die Webex-App, den alten Konfigurationsabschnitt () zu lesen und seine Werte anzuwenden.
- Wenn die Funktion deaktiviert ist, werden die Notrufe vom ERC (Emergency Relay Center) zur Triage weitergeleitet, um den Standort des Anrufers zu validieren, bevor sie an eine geeignete PSAP weitergeleitet werden, was zu zusätzlichen Gebühren führen kann.

Im folgenden Ausschnitt werden die Änderungen in der DMS-Konfigurationsvorlage angezeigt:

```
<config><services>
<emergency-dialing enabled="%ENABLE_EMERGENCY_DIALING_WXT%">
   <redsky enabled="%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%">  <!-- DEPRECATED by <emergency-
location> -->
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-timeout>%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%</user-reminder-
timeout>
      <user-mandatory-location>%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%</user-
mandatory-location>
      <user-location-prompting>%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%</user-location-
prompting>
   </redsky>
   <emergency-location enabled="%ENABLE_EMERGENCY_LOCATION_WXT%"
                       provider="%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%">
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-timeout>%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%</user-reminder-
timeout>
      <user-mandatory-location>%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%</user-
mandatory-location>
      <user-location-prompting>%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%</user-
location-prompting>
   </emergency-location>
</emergency-dialing>
```

In der folgenden Tabelle wird die Zuordnung zwischen den neuen und den älteren benutzerdefinierten Tags aufgeführt:

Konfigurationsoption	Veraltetes benutzerdefiniertes Tag	Neues benutzerdefiniertes Tag
Das Attribut aktiviert im Tag im Vergleich zum gleichen Attribut	%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	%ENABLE_EMERGENCY_LOCATION_WXT%

markieren	%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%
markieren	%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%
markieren	%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_EMERGENCY_LOCATION_WXT%	false	wahr, falsch	Aktiviert die Nutzung der Notfall-Standortplattform.
%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%	Red Sky	Redsky, Intrado, 9Leitung, Webex	Gibt an, welchen Notfallstandortanbieter verwendet werden soll. „webex“ gilt nur für die Webex Calling-Bereitstellung und sollte für die Nutzung des Cisco Emergency Location Information Service konfiguriert werden.
%BWE911-PRIMARY-HELDURL%	leer	Schnur	Gibt die URL zum E911-Anbieter an, der das HELD-Protokoll unterstützt.
%BWE911-CUSTOMERID%	leer	Schnur	Die Kunden-ID (HeldOrgId, CompanyID), die für die E911-Anbieter-HTTPS-Anforderung verwendet wird.
%BWE911-SECRETKEY%	leer	Schnur	Der Geheimschlüssel zur Authentifizierung der HTTPS-Anforderung des E911-Anbieters. Nicht verwendet (leer) mit „Webex“ als E911-Anbieter
%BWE911-EMERGENCY-NUMBER-LIST%	leer	CSV-Zeichenfolge	Die Liste der vom E911-Anbieter unterstützten Notfallnummern.
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	0 (der Benutzer wird nicht mehr gefragt)	Nummer [0 - 43200]	Die Zeitüberschreitung in Minuten, die verwendet wird, um den Benutzer daran zu erinnern, den Notfallstandort zu aktualisieren, wenn der aktuelle Standort nicht eingegeben oder ungültig ist. Der vorgeschlagene Wert, wenn Sie sich für die Aktivierung entscheiden: 1440 (ein Tag).
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	-1 (Benutzer kann den Dialog immer abbrechen)	Nummer [-1 - 100]	Gibt an, wie oft 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 können das Dialogfeld immer abbrechen) ▪ N = 0 (der Benutzer darf den Dialog nicht abbrechen - obligatorischer Ort immer) N > 0 (der Benutzer kann den Dialog N-mal abbrechen, bevor er obligatorisch wird)

Cisco – vertraulich

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	einmal_pro_Anmeldung	aggressiv, einmal_pro_Anmeldung	▪ Definiert das Eingabeverhalten für den E911-Standort. Der Wert "aggressive" zeigt dem Benutzer den Dialog bei jedem Netzwechsel zu einem unbekannten Standort, während der Wert "once_per_login" den Dialog nur einmal anzeigt und so weitere Popups und Ablenkungen für den Benutzer verhindert.

7.2 Unified-Anrufprotokoll für sekundäre Leitungen (nur Webex Calling)

Die Webex-App unterstützt das synchronisierte Anrufprotokoll über alle Geräte für die primäre Leitung des Benutzers, wie in Abschnitt *6.1.36 Anrufprotokoll* beschrieben.

Exklusiv für die Webex Calling-Bereitstellung erweitert Version 45,1 die Funktion für die sekundären Leitungen (gemeinsam genutzt und virtuell).

7.3 Durchgängige Verschlüsselung (nur Webex Calling)

Ab Version 45,1 fügt die Webex-App nur für die Webex Calling-Bereitstellung End-to-End-Verschlüsselung (E2EE) für die Audio- und Videomedien für die 1-on-1-Anrufe innerhalb derselben Organisation hinzu. E2EE garantiert, dass nur die Teilnehmer der Kommunikation den Inhalt entschlüsseln können.

Anrufe beginnen mit der Standard-SRTP-Verschlüsselung, bei der die Schlüssel während der SDP-Aushandlung ausgetauscht werden. Wenn beide Parteien E2EE unterstützen, werden neue Schlüssel verwendet, die nur die beiden Teilnehmer kennen, um die Medien zu verschlüsseln.

```
<config><services>
<calls>
      <e2ee enabled="%ENABLE_CALLS_E2EE_WXT%"/>
```

Etikett	Standardwert bei Auslassung	Unterstützte Werte	Beschreibung
%ENABLE_CALLS_E2EE_WXT%	false	wahr, falsch	Steuert, ob E2EE für die 1:1-Anrufe aktiviert werden soll.

Cisco – vertraulich

Benutzerdefinierte Tags-Zuordnung zwischen Webex for Cisco BroadWorks und UC-One

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

Webex für Cisco BroadWorks-Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	N/A	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N/A	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	N/A	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_TEILNEHMER_LIST_DESKTOP%	N/A
%MAX_CONF_PARTIES_WXT%	%MAX_KONF_PARTEIEN%	k. A.
%ENABLE_CALL_STATISTICS_WXT%	k. A.	k. A.
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N/A	%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%MWI_MODE_WXT%	%DESKTOP_MWI_MODE%	%MWI_MODUS_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	k. A.	k. A.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	N/A
%ENABLE_FORCED_LOGOUT_WXT%	%ERZWUNGENE_ABMELDUNG AKTIVIEREN%	N/A
%FORCED_LOGOUT_APPID_WXT%	%ERZWUNGENE_LOGOUT_APPID%	k. A.
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	k. A.	k. A.
%ENABLE_BROADWORKS_ANYWHERE_WXT%	k. A.	k. A.

Cisco – vertraulich

Webex für Cisco BroadWorks-Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	k. A.	k. A.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	k. A.	k. A.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	k. A.	k. A.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	k. A.	k. A.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	k. A.	k. A.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	k. A.	k. A.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	k. A.	k. A.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	k. A.	k. A.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	k. A.	k. A.
%ENABLE_EMERGENCY_DIALING_WXT%	k. A.	k. A.
%EMERGENCY_DIALING_NUMBERS_WXT%	k. A.	k. A.
%ENABLE_USE_RPORT_WXT%	%VERWENDUNG_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	N/A	%RPORT_VERWENDEN_LOKALER_PORT_MOBILE%
%USE_TLS_WXT%	%VERWENDEN_TLS%	N/A
%SBC_ADDRESS_WXT%	%SBC_ADRESSE%	%SBC_ADRESSE%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILE%
%USE_TCP_FROM_DNS_WXT%	%VERWENDUNG_TCP_FROM_DNS%	N/A
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	k. A.

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

Cisco – vertraulich

Webex für Cisco BroadWorks-Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	k. A.	%ENABLE_CALLS_AUTO_RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	k. A.	%EMERGENCY_CALL_DIAL_SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLIND_WXT%	k. A.	k. A.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	k. A.	k. A.
%WEB_CALL_SETTINGS_URL_WXT%	k. A.	%WEB_CALL_SETTINGS_URL%
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP%
%ENABLE_CALL_CENTER_WXT%	%ENABLE_CALL_CENTER_DESKTOP%"	N/A
%WEB_CALL_SETTINGS_TARGET_WXT%	k. A.	N/A
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_CFA_VISIBLE%
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_DND_VISIBLE%
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_ACR_VISIBLE%
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_CFB_VISIBLE%
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_CFNR_VISIBLE%
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_CFNA_VISIBLE%
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_SIMRING_VISIBLE%
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_SEQRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_RO_VISIBLE%
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_ACB_VISIBLE%
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_CW_VISIBLE%
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_CLIDB_VISIBLE%
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	k. A.	%WEB_CALL_SETTINGS_PA_VISIBLE%

Cisco – vertraulich

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

Cisco – vertraulich

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

Cisco – vertraulich

Webex für Cisco BroadWorks-Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	k. A.	k. A.
%ENABLE_CLID_OUTGOING_CALLS_WXT%	k. A.	k. A.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	k. A.	k. A.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	k. A.	k. A.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	k. A.	k. A.
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	k. A.	k. A.
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	k. A.	k. A.
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	k. A.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	k. A.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	k. A.	k. A.
%ENABLE_GCP_NOTIFICATIONS_WXT%	k. A.	k. A.
%ENABLE_GCP_DISPLAY_CALLER_WXT%	k. A.	k. A.
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	k. A.	k. A.
%UDP_KEEPALIVE_ENABLED_WXT%	k. A.	k. A.
%TCP_KEEPALIVE_ENABLED_WXT%	k. A.	k. A.
%TLS_KEEPALIVE_ENABLED_WXT%	k. A.	k. A.
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	k. A.	k. A.
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	k. A.	k. A.
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	k. A.	k. A.

Cisco – vertraulich

Webex für Cisco BroadWorks-Tag	Desktop Legacy Tag	Mobile Legacy Tag
%CALL_PULL_MODE_WXT%	k. A.	k. A.
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	k. A.	k. A.
%ENABLE_EMERGENCY_LOCATION_WXT%	k. A.	k. A.
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	k. A.	k. A.
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	k. A.	k. A.
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	k. A.	k. A.
%ENABLE_CALLS_E2EE_WXT%	k. A.	k. A.

HINWEIS: N/A bedeutet, dass es kein entsprechendes benutzerdefiniertes Tag gibt, das die Funktion in UC-One steuert. Die Angabe „N/A“ für Desktop- und Mobile-Legacy-Tags zeigt an, dass das Webex for Cisco BroadWorks-Tag neu ist und steuert entweder neue Funktionen oder eine vorhandene Funktion, die nicht über ein benutzerdefiniertes Tag in UC-One gesteuert wurde.

8 Anhang A: TLS-Schlüssel

Der Webex für BroadWorks-Client verwendet CiscoSSL, das auf OpenSSL mit zusätzlicher Sicherheitshärtung basiert.

Cisco – vertraulich

9 Anhang B: DM Tag Provisioning Script

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

Beachten Sie, dass dieses Skript nur für neue Einsätze gültig ist, bei 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 (bei einer echten Bereitstellung müssten Sie eine größere Liste benutzerdefinierter Tags einfügen). Beachten Sie, dass das folgende Beispiel für Mobiltelefone gilt. Verwenden Sie für den Desktop den Tagsatz BroadTouch_tags anstelle von Connect_Tags. Für Tablets verwenden Sie den Tagsatz ConnectTablet_Tags anstelle von Connect_Tags.

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


Cisco – vertraulich

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

Im Folgenden werden alle von Webex für Cisco BroadWorks verwendeten benutzerdefinierten Tags mit Beispielwerten (Standard oder empfohlene) aufgeführt. Beachten Sie, dass einige der Tags Werte erfordern, die für den entsprechenden Einsatz spezifisch sind (wie Serveradressen). Deshalb werden diese Tags am Ende des Skripts hinzugefügt, aber leer gelassen, und es sollten zusätzliche Set-Befehle hinzugefügt werden, um sie anzugeben.

9.1 Desktop

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


Cisco – vertraulich

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


Cisco – vertraulich

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


Cisco – vertraulich

```
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName BroadTouch_tags %ENABLE_CALLS_E2EE_WXT% false
```

9.2 Mobil

```
add tagSetName Connect_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName Connect_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName Connect_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName Connect_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName Connect_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName Connect_Tags %ENABLE_MWI_WXT% false
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName Connect_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName Connect_Tags %USE_TLS_WXT% false
add tagSetName Connect_Tags %SBC_PORT_WXT% 5075
add tagSetName Connect_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName Connect_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName Connect_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName Connect_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName Connect_Tags %SOURCE_PORT_WXT% 5060
add tagSetName Connect_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName Connect_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName Connect_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName Connect_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName Connect_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName Connect_Tags %SRTP_ENABLED_WXT% false
add tagSetName Connect_Tags %SRTP_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_REKEYING_WXT% true
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
```


Cisco – vertraulich

```
add tagSetName Connect_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName Connect_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName Connect_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName Connect_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName Connect_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName Connect_Tags %USE_MEDIASEC_WXT% false
add tagSetName Connect_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName Connect_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName Connect_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName Connect_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName Connect_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName Connect_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName Connect_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName Connect_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName Connect_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName Connect_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName Connect_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName Connect_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
```


Cisco – vertraulich

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


Cisco – vertraulich

```
add tagSetName Connect_Tags %CALL_PULL_MODE_WXT% blind
add tagSetName Connect_Tags %ENABLE_EMERGENCY_LOCATION_WXT% false
add tagSetName Connect_Tags %EMERGENCY_LOCATION_PROVIDER_NAME_WXT% redsky
add tagSetName Connect_Tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName Connect_Tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName Connect_Tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT% once_per_login
add tagSetName Connect_Tags %ENABLE_CALLS_E2EE_WXT% false
```

9.3 Tablet

```
add tagSetName ConnectTablet_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName ConnectTablet_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName ConnectTablet_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_MWI_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%
false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName ConnectTablet_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName ConnectTablet_Tags %USE_TLS_WXT% false
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% 5075
add tagSetName ConnectTablet_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName ConnectTablet_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName ConnectTablet_Tags %SOURCE_PORT_WXT% 5060
add tagSetName ConnectTablet_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName ConnectTablet_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName ConnectTablet_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
```


Cisco – vertraulich

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


Cisco – vertraulich

```
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName ConnectTablet_Tags %XSI_ROOT_WXT% true
add tagSetName ConnectTablet_Tags %SBC_ADDRESS_WXT% true
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% true
add tagSetName ConnectTablet_Tags %MWI_MODE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName ConnectTablet_Tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName ConnectTablet_Tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RING_SPLASH_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PN_MOBILE_CALL_INFO_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName ConnectTablet_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName ConnectTablet_Tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName ConnectTablet_Tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_TRANSFER_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName ConnectTablet_Tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName ConnectTablet_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
```

```
add tagSetName ConnectTablet_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName ConnectTablet_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT% false
add tagSetName ConnectTablet_Tags %CALL_PULL_MODE_WXT% blind
add tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_LOCATION_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_PROVIDER_NAME_WXT% redsky
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_E2EE_WXT% false
```

9.4 System-Tags

Im Folgenden werden die von Webex für BroadWorks verwendeten System-Tags aufgeführt.

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

10 Akronyme und Abkürzungen

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

ACB	Automatischer Rückruf
ACD	Automatische Anrufverteilung
ACR	Anonyme Anrufablehnung
AES	Erweiterter Verschlüsselungsstandard
ALG	Application Layer-Gateway
API	Schnittstelle für die Anwendungsplanung
APK	Bewerbungspaket
APNS	Apple Push-Benachrichtigungsdienst
ARS	Automatische Bitratenauswahl
AS	Anwendungsserver (Cisco BroadWorks)
Durchschn.	Audio und visuelles Profil
BW	BroadWorks
BWA	BroadWorks Anywhere
BWKS	BroadWorks
Fußball-Weltmeisterschaft	BroadWorks Mobility
BYOD	Eigenes Gerät verwenden
CC	Call-Center
CFB	Besetzte Rufumleitung
CFNA	Rufumleitung ohne Antwort
CFNR	Rufumleitung nicht erreichbar
CIF	Allgemeines Zwischenformat
CLI	Befehlszeilenschnittstelle
CLID	Anrufleitungsidentität
CLIDB	Bereitstellungsblockierung der Anrufleitungs-ID
CRLF	Wagenrücklauf-Leitungszuführung
CS	Stromkreisgeschaltet

Cisco – vertraulich

CSWV	Webansicht der Anrufeinstellungen
CW	Wartender Anruf
DB	Datenbank
DM	Geräteverwaltung
DND	Bitte nicht stören
DNS	Domain-Name-System
DPC	Steuerung für Tischtelefone
DTAF	Gerätetyp-Archivdatei
ECACS	Dienst zur Änderung der Notrufadresse
FMC	Festnetz-Mobile Konvergenz
FQDN	Voll qualifizierter Domain-Name
HMAC	Authentifizierungscode für Hash-Nachrichten
ICE	Interaktive Konnektivitätseinrichtung
iLBC	Internet-Codec Mit niedriger Bitrate
Chat	Instant Messaging
IM &8211; P	Instant Messaging und Präsenz
IOT	Interoperabilitätstests
IP	Internetprotokoll
JID	Jabber-ID
M/O	Obligatorisch/Optional
MNO	Mobilfunknetzbetreiber
MTU	Maximale Getriebeeinheit
MUC	Chat für mehrere Benutzer
Nachrichtenwartesignal (MWI)	WMI-Anzeige zur wartenden Nachricht (MWI, Message Waiting Indicator)
NAL	Netzwerkabstraktionsschicht
NAPTR	Zeiger der Benennungsbehörde
NAT	Übersetzung von Netzwerkadressen
Ott	Über der Oberseite
PA	Persönlicher Assistent
PAI	P-Bestätigte Identität

Cisco – vertraulich

PEM	P-Early Media
PLI	Anzeige des Bildverlusts
PLMN	Öffentliches Land-Mobil-Netzwerk
PN	Push-Benachrichtigung
QCIF	Viertelallgemeines Zwischenformat
QoS	Servicequalität
RO	Remote-Büro
RTCP	Echtzeit-Steuerungsprotokoll
RTP	Echtzeitprotokoll
SaaS	Software-as-a-Service
SAN	Betreff für alternativen Namen
SASL	Einfache Authentifizierung und Sicherheitsschicht
SAVP	Sicheres Audio- und Videoprofil
SBC	Sitzungsgrenz-Controller
SCA	Darstellung freigegebener Anrufe
SCF	Funktion „Sitzungskontinuität“
SCTP	Übertragungsprotokoll für Stream-Steuerung
SDP	Sitzungsdefinitionsprotokoll
SEQRING	
SIMRING	
SIP:	Session Initiation Protocol
SNR	Signal-Rausch-Verhältnis
SNR	Erreichbarkeit unter einer Rufnummer (SNR)
SRTCP	Sicheres Echtzeit-Steuerungsprotokoll
SRTP	Sicheres Echtzeit-Transportprotokoll
SSL	Secure Sockets Layer
STUN	Sitzungstraversal-Dienstprogramme für NAT
SUBQCIF	
TCP	Übertragungskontrollprotokoll
TLS	Sicherheit der Transportschicht

TTL	Gültigkeitsdauer
TURN	Traversal Mit Relay-NAT
UDP	Benutzer-Datagram-Protokoll
UI	Benutzeroberfläche
UMS	Nachrichtenserver (Cisco BroadWorks)
URI	Uniform Resource Identifier
UVS	Videoserver (Cisco BroadWorks)
VGA	Video-Grafik-Array
VoIP	Voice-over-IP
VVM	Visuelle Sprachmailbox
WXT	Webex
XMPP	Extensible Messaging und Presence Protocol
XR	Erweiterter Bericht
XSP	Xtended-Services-Plattform
XSI	Xtended Services-Schnittstelle

Cisco – vertraulich