Webex for Cisco BroadWorks Konfigurasjonsveiledning

Frigjør 45.2

Dokumentversjon 1

Innholdsfortegnelse

1 Sammendrag av endringer 1
1.1 Endringer for utgivelse 45.2, februar 2025 1
1.2 Endringer for utgivelse 45.1, januar 2025 1
1.3 Endringer for utgivelse 44.12, desember 2024 1
1.4 Endringer for utgivelse 44.11, november 2024 1
1.5 Endringer for utgivelse 44.10, oktober 2024 1
1.6 Endringer for utgivelse 44.9, september 2024 1
1.7 Endringer for utgivelse 44.8, august 2024 1
1.8 Endringer for utgivelse 44.7, juli 2024 1
1.9 Endringer for utgivelse 44.6, juni 2024 1
1.10 Endringer for utgivelse 44.5, mai 2024 2
1.11 Endringer for utgivelse 44.4, april 2024 2
1.12 Endringer for utgivelse 44.3, mars 2024 2
1.13 Endringer for utgivelse 44.2, februar 2024 2
1.14 Endringer for utgivelse 44.1, januar 2024 2
2 Endringer for konfigurasjonsfiler 3
2.1 Endringer i konfigurasjonsfiler for utgivelse 45.2 3
2.2 Endringer i konfigurasjonsfiler for utgivelse 45.1 3
2.3 Endringer i konfigurasjonsfiler for utgivelse 44.12 3
2.4 Endringer i konfigurasjonsfiler for utgivelse 44.11 3
2.5 Endringer i konfigurasjonsfiler for utgivelse 44.10 3
2.6 Endringer i konfigurasjonsfiler for utgivelse 44.9 4
2.7 Endringer i konfigurasjonsfiler for utgivelse 44.8 4
2.8 Endringer i konfigurasjonsfiler for utgivelse 44.7 4
2.9 Endringer i konfigurasjonsfiler for utgivelse 44.6 4
2.10 Endringer i konfigurasjonsfiler for utgivelse 44.5 4
2.11 Endringer i konfigurasjonsfiler for utgivelse 44.4 5
2.12 Endringer i konfigurasjonsfiler for utgivelse 44.3 5
2.13 Endringer i konfigurasjonsfiler for utgivelse 44.2 6
2.14 Endringer i konfigurasjonsfiler for utgivelse 44.1 7
3 Introduksjon 8
4 Installasjon 9
4.1 Lokalisert klientnedlasting 9
4.2 Android-klient 9
4.3 iOS-klient 9
4.4 Skrivebordsklient 9
5 Enhetsstyring 10
5.1 Etiketter for enhetsadministrasjon 10
5.2 Delvis samsvarsforbedringer for valg av enhetstype 11

Konfidensiell Cisco

5.3 Klientkonfigurasjon ... 12
5.4 Distribusjon av config-wxt.xml ... 12
5.5 Konfigurasjonsfil (config-wxt.xml) ... 12
5.6 Standardkoder for system ... 13
5.7 Cisco BroadWorks Dynamic Built-in System Tags ... 13
6 Egendefinerte koder ... 16
6.1 Vanlige funksjoner ... 28
6.1.1 SIP-serverinnstillinger ... 28
6.1.2 SIP over TLS og sikker transportprotokoll i sanntid ... 31
6.1.3 3GPP SIP-topptekster for SRTP ... 33
6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives ... 33
6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-sokkelen ... 35
6.1.6 Dynamisk SIP-proxy-oppdagelse ... 36
6.1.7 Foretrukket portbruk for SIP ... 41
6.1.8 SIP Failover og Failback ... 41
6.1.9 SIP ABONNER og REGISTRER Oppdater og ABONNER Prøv på nytt ... 46
6.1.10 Bruk P-tilknyttede URI-er i REGISTER ... 47
6.1.11 SIP P-Early Media (PEM)-topptekst ... 47
6.1.12 Støtte for SIP-OPPDATERING ... 48
6.1.13 Eldre SIP INFO FIR ... 48
6.1.14 SIP rport-administrasjon for NAT-traversering ... 48
6.1.15 SIP-økt-ID ... 49
6.1.16 Avvisning av innkommende anrop ... 50
6.1.17 Portområde for transportprotokoll i sanntid ... 50
6.1.18 ICE-støtte (Webex Calling kun) ... 51
6.1.19 RTCP MUX ... 52
6.1.20 Overfør ... 52
6.1.21 N-Way-konferansesamtaler og deltakere ... 53
6.1.22 Anropstrekk ... 54
6.1.23 Samtaleparkering/hent ... 54
6.1.24 Samtalestatistikker ... 55
6.1.25 Automatisk gjenoppretting av anrop / sømløs overføring av anrop ... 55
6.1.26 Anropsopptak ... 56
6.1.27 Talepost, visuell talepost, indikator for melding venter ... 57
6.1.28 Utskrift av talepost for Webex Calling ... 58
6.1.29 Samtaleinnstillinger ... 59
6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger ... 61
6.1.31 Pålogging/utlogging av telefonsenter / samtalekø ... 64
6.1.32 XSI-rot og -stier ... 65
6.1.33 XSI-hendelseskanal ... 65
6.1.34 Konfigurasjon av kodek ... 66
6.1.35 SIP-URI-oppringing ... 68

Konfidensiell Cisco

6.1.36 Samtalehistorikk på alle enheter ... 68
6.1.37 Deaktiver videosamtaler ... 69
6.1.38 Nødsamtaler (911) – Stedsrapportering med E911-leverandør ... 70
6.1.39 PAI som identitet ... 71
6.1.40 Deaktiver skjermdeling ... 71
6.1.41 Angivelse av søppelanrop ... 72
6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN/mobilsamtaler ... 72
6.1.43 QoS DSCP-merking ... 73
6.1.44 Primærprofil ... 73
6.1.45 Blokkeringsliste (Webex Calling kun) ... 75
6.1.46 Medietilpasning og resiliensimplementering (MARI) ... 76
6.1.47 Samtidige samtaler med samme bruker ... 77
6.1.48 RTCP-XR ... 78
6.1.49 Informasjon om viderekobling av anrop ... 78
6.1.50 Innringer-ID ... 79
6.2 Funksjoner kun for skrivebordet ... 82
6.2.1 Tvungen utlogging ... 82
6.2.2 Mottak av anrop ... 82
6.2.3 Støtte for sjef-administrator (lederassistent) ... 83
6.2.4 Eskalere SIP-anrop til møte (Webex Calling kun) ... 84
6.2.5 Kontrollanrop for bordtelefon – automatisk svar ... 84
6.2.6 Automatisk svar med tonevarsling ... 85
6.2.7 Styring av bordtelefon – Midtsamtalekontroller – Konferanse ... 85
6.2.8 Varsler om mottak av anrop ... 85
6.2.9 Hendelsespakke for fjernstyring ... 87
6.2.10 Utvalg av CLID for ringkøagent ... 88
6.2.11 Gateway for overlevelse (Webex Calling kun) ... 88
6.2.12 Flere linjer – delt linje-utseende ... 89
6.2.13 Flere linjer – virtuelle linjer (Webex Calling kun) ... 89
6.2.14 Hendelsespakke for fjerndemping (Webex Calling kun) ... 90
6.2.15 Flytt samtale ... 91
6.3 Funksjoner kun for mobil ... 93
6.3.1 Nødsamtaler ... 93
6.3.2 Push-varsler for anrop ... 94
6.3.3 Enkeltvarsling ... 96
6.3.4 Klikk for å ringe (Ring tilbake) ... 96
6.3.5 MNO-støtte ... 97
6.3.6 Innkommende innringer-ID ... 102
6.4 Personlig assistent (borte tilstedeværelse) ... 103
7 Funksjoner for tidlig feltprøve (BETA). ... 105
7.1 AI kodek ... 105
7.2 Flerlinje for mobil (Webex Calling kun) ... 105

Konfidensiell Cisco

8 Egendefinerte tagger tilordning mellom Webex for Cisco BroadWorks og UC-One... 107

9 Vedlegg A: TLS-chifre ... 115

10 Vedlegg B: DM Tag Provisioning Script ... 116

10.1 Stasjonær PC ... 117

10.2 Mobil ... 119

10.3 Nettbrett ... 122

10.4 Systemkoder ... 125

11 Akronymer og forkortelser ... 127

Konfidensiell Cisco

1 Sammendrag av endringer

Denne delen beskriver endringene i dette dokumentet for hver utgivelse og dokumentversjon.

1.1 Endringer for utgivelse 45.2, februar 2025

Det var ingen endringer i dette dokumentet for denne utgivelsen.

1.2 Endringer for utgivelse 45.1, januar 2025

Denne versjonen av dokumentet inneholder følgende endringer:

- Flyttet delen *6.4 Personlig assistent (borte* tilstedeværelse) ut av BETA.
- Flyttet avsnitt *6.3.2.3 Leveringsmodus (Webex Calling kun)* ut av BETA.

1.3 Endringer for utgivelse 44.12, desember 2024

Det var ingen endringer i dette dokumentet for denne utgivelsen.

1.4 Endringer for utgivelse 44.11, november 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til delen *Flerlinje for mobil (Webex Calling kun)* i BETA.

1.5 Endringer for utgivelse 44.10, oktober 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- La til delen *Personlig assistent (borte tilstedeværelse)*.
- Lagt til delen *Leveringsmodus (Webex Calling kun)* i BETA.

1.6 Endringer for utgivelse 44.9, september 2024

Det var ingen endringer i dette dokumentet for denne utgivelsen.

1.7 Endringer for utgivelse 44.8, august 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert del *6.1.34 Konfigurasjon* av kodek – lagt til en forklaring om DTMF-ene og støttede leveringsmekanismer.

1.8 Endringer for utgivelse 44.7, juli 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til delen *AI kodek* i BETA.
- Oppdatert del *6.1.44 Primærprofil* – fjernet detaljer om Webex appens oppførsel før utgivelsen 43.2.

1.9 Endringer for utgivelse 44.6, juni 2024

Denne versjonen av dokumentet inneholder følgende endringer:

Konfidensiell Cisco

- Oppdatert del *6.3.6. Innkommende innringer-ID* – lagt til flere detaljer om den opprinnelige opplevelsen og hvordan funksjonen fungerer.

1.10 Endringer for utgivelse 44.5, mai 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert avsnitt *6.1.18 ICE-støtte (Webex Calling kun)* – lagt til IPv6-støtte via NAT64.
- Oppdatert del *6.1.50 Innringer-ID* – lagt til underseksjon *6.1.50.2 Navn på ekstern innringer-ID*.

1.11 Endringer for utgivelse 44.4, april 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert avsnitt *6.1.50.1 Utgående innringer-ID*.
- Oppdatert seksjon *Endringer i konfigurasjonsfiler for utgivelse 44.3* – la til detaljer om keepalive-oppdateringene i 44.3.

1.12 Endringer for utgivelse 44.3, mars 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert del *6.3.6. Innkommende innringer-ID*
    - Flyttet avsnitt *6.1.50.1 Utgående innringer-ID* som vanlig for stasjonær PC og mobil, og oppdaterte den med flere detaljer.
- Oppdatert del *6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives* – lagt til detaljer om de konfigurerbare keepalives ved hjelp av egendefinerte tagger.

1.13 Endringer for utgivelse 44.2, februar 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til del *6.3.6 Innkommende innringer-ID*
- Oppdatert seksjon *6.2.8 Varsler om mottak* av anrop
    - Lagt til underseksjon *6.2.8.1 Opptattlampefelt* – flyttet BLF-spesifikasjoner i den.
    - Lagt til underavsnitt *6.2.8.2 Gruppe for mottak av anrop* (Webex Calling kun).
- Lagt til seksjon *6.1.49 Informasjon om viderekobling* av anrop.
- Oppdatert del *6.1.8.3 Håndhev IP-versjon* – lagt til detaljer for den nye *nat64* -modusen.
- Oppdatert seksjon *6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN/mobilsamtaler* – lagt til detaljer for den nye båndbreddeutvidelsen og oppdateringene for støyfjerning. Del *Taleforbedringer for PSTN-anrop* er fjernet fra BETA.

1.14 Endringer for utgivelse 44.1, januar 2024

Det var ingen endringer i dette dokumentet for denne utgivelsen.

Konfidensiell Cisco

2 Endringer for konfigurasjonsfiler

2.1 Endringer i konfigurasjonsfiler for utgivelse 45.2

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.2 Endringer i konfigurasjonsfiler for utgivelse 45.1

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.3 Endringer i konfigurasjonsfiler for utgivelse 44.12

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.4 Endringer i konfigurasjonsfiler for utgivelse 44.11

- [BETA-funksjon] [Kun mobil] [Webex Calling kun]
  Lagt til attributt med flere linjer i koden <protocols><sip><lines>.
  Lagt til <personal> og <line> seksjoner for de sekundære linjene under seksjon <protocols><sip><lines>.

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

2.5 Endringer i konfigurasjonsfiler for utgivelse 44.10

- [BETA-funksjon]
  La til <personal-assistant> tag under seksjon <services>.

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

- [BETA-funksjon] [Kun mobil] [Webex Calling kun]
  Lagt til attributt for leveringsmodus under koden <services><push-notifications-for-calls>.

```
<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%">
```


Konfidensiell Cisco

Følgende %TAG%er ble lagt til:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.6 Endringer i konfigurasjonsfiler for utgivelse 44.9

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.7 Endringer i konfigurasjonsfiler for utgivelse 44.8

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.8 Endringer i konfigurasjonsfiler for utgivelse 44.7

- [BETA-funksjon]
  La til AI-kodek (xCodec) under delen <services><calls><audio><codecs>.

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

2.9 Endringer i konfigurasjonsfiler for utgivelse 44.6

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.10 Endringer i konfigurasjonsfiler for utgivelse 44.5

- [Webex Calling kun]
  Lagt til attributtet enable-ipv6-support i <protocols><rtp><ice> taggen.

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

- Tag <remote-name> har blitt lagt til i delen <services><calls><caller-id> med <machine> som en undertag.

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


Konfidensiell Cisco

Følgende %TAG%er ble lagt til:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.11 Endringer i konfigurasjonsfiler for utgivelse 44.4

- [Kun skrivebord] [Webex Calling kun]
  Lagt til koder <additional-numbers>, <hunt-group> og <clid-delivery-blocking> under delen <caller-id><outgoing-calls>.

```
<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>
```

2.12 Endringer i konfigurasjonsfiler for utgivelse 44.3

- [Kun skrivebord] [Webex Calling kun]
  Lagt til <outgoing-calls> under den nye <caller-id> delen, med <call-center> som en underkode.

```
<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>
```

- Lagt til egendefinerte tagger (%UDP_KEEPALIVE_ENABLED_WXT%, %TCP_KEEPALIVE_ENABLED_WXT% og %TLS_KEEPALIVE_ENABLED_WXT%) for å erstatte den hardkodede Keep-alive-aktiverte verdien for hver transport under <protocols><sip><transports>.

```
<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>
```


Konfidensiell Cisco

Følgende %TAG%er ble lagt til:

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

2.13 Endringer i konfigurasjonsfiler for utgivelse 44.2

- [Kun mobil]
  Lagt til seksjon <caller-id> under <services><calls>. Lagt til underkoder <incoming-call> og <missed-call>, med ny underkode <append-number> for begge.

```
<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>
```

- [Kun mobil] [Webex Calling kun]
  Lagt til <outgoing-calls> under den nye <caller-id> delen.

```
<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>
```

- Lagt til kode <call-forwarding-info> i delen <services><calls>.

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

- [Kun skrivebord] [Webex Calling kun]
  Lagt til <group-call-pickup-notifications> del under <services><calls>, med <display-caller> og <max-timeout> som underkoder. La også til <group-call-pickup> tag under hver <line> tag i <protocols><sip><lines> delen.

```
<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>
  …
```


Konfidensiell Cisco

```
<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>
    …
```

Følgende %TAG%er ble lagt til:

- %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%

Følgende %TAG% ble avviklet:

- %ENABLE_NOISE_REMOVAL_WXT%

2.14 Endringer i konfigurasjonsfiler for utgivelse 44.1

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

Konfidensiell Cisco

3 Introduksjon

Formålet med dette dokumentet er å gi en beskrivelse av konfigurasjonen av Webex for CiscoBroadWorks -klienten.

Konfigurasjonsfilen *config-wxt.xml* leveres i to versjoner – én for mobil (Android og iOS) og én for skrivebord (Windows og MacOS).

Klientene konfigureres ved hjelp av en konfigurasjon som ikke er synlig for sluttbrukeren. *config-wxt.xml* gir serverspesifikk informasjon, for eksempel serveradresser og porter og kjøretidsalternativer for selve klienten (for eksempel alternativer som er synlige i *Innstillinger* -skjermbildet).

Konfigurasjonsfilene leses av klienten når den starter, etter å ha blitt hentet fra Device Management. Informasjonen fra konfigurasjonsfilene lagres kryptert, og gjør den dermed usynlig og utilgjengelig for sluttbrukeren.

merk: XML-egenskapene skal ikke inneholde mellomrom (for eksempel <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"/> i stedet for <transfer-call enabled = "%ENABLE_TRANSFER_CALLS_WXT%"/>).

Konfidensiell Cisco

4 Installasjon

Webex For Cisco-klienter BroadWorks kan installeres fra følgende:

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

4.1 Lokalisert klientnedlasting

Følgende lokaliserte versjoner av Webex for Cisco-klienter BroadWorks kan lastes ned på følgende måte:

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-klient

Android-klienten installeres som et program (Android-programpakke [APK]), som lagrer innstillinger- og konfigurasjonsrelaterte data i sitt private område.

Det finnes versjonskontroll basert på Google Play-prosedyrene. En standard Google Play-varsel er gitt (det vil si at Android automatisk indikerer at det er en ny versjon av programvare tilgjengelig).

Når den nye versjonen er lastet ned, overskrives den gamle programvaren; brukerdata beholdes imidlertid som standard.

Merk at brukeren ikke er pålagt å velge alternativer for installasjon eller avinstallering.

4.3 iOS-klient

iOS-klienten installeres som et program, som holder innstillingsrelaterte data inne i «sandboksen», og konfigurasjonsfildataene lagres kryptert.

Det finnes versjonskontroll basert på prosedyrene i Apple App Store. App Store-ikonet er uthevet for å indikere at det er en ny versjon av programvare tilgjengelig.

Når den nye versjonen er lastet ned, overskrives den gamle programvaren; brukerdata beholdes imidlertid som standard.

Merk at brukeren ikke er pålagt å velge alternativer for installasjon eller avinstallering.

4.4 Skrivebordsklient

Informasjon om installasjon og versjonskontroll av skrivebordsklienten (Windows og MacOS) finner du på følgende: https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade.

Konfidensiell Cisco

5 Enhetsstyring

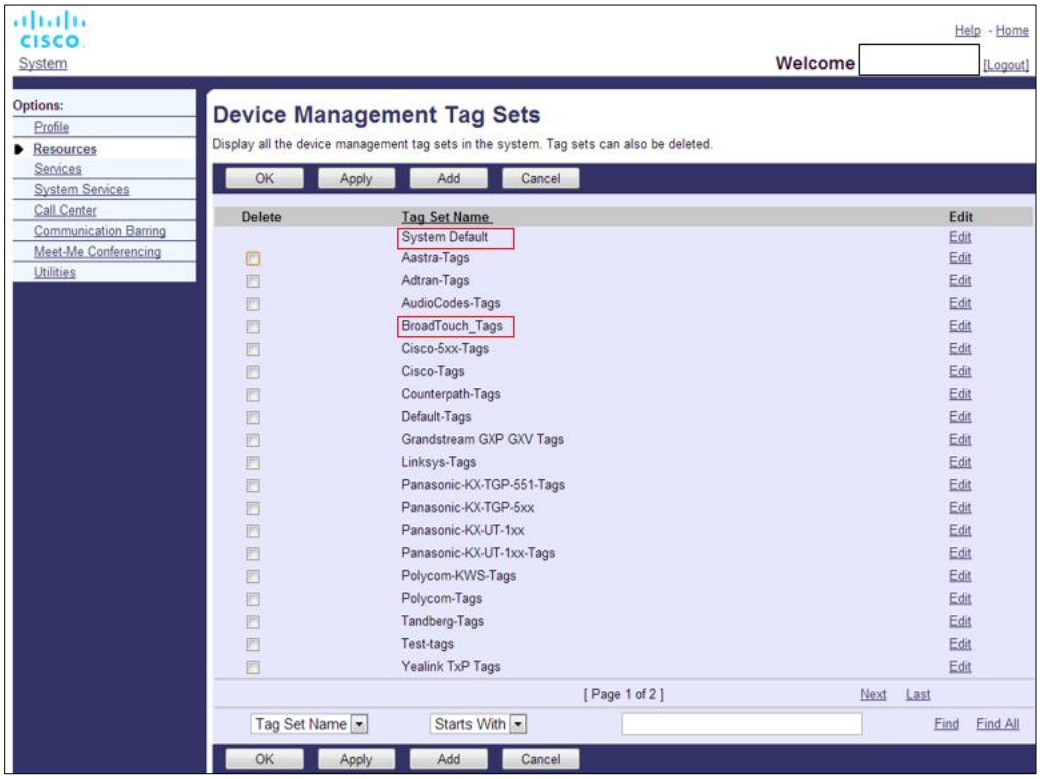
5.1 Etiketter for enhetsadministrasjon

Webex for Cisco BroadWorks bruker *Device Management Tag Set* vist i figuren nedenfor. *Systemstandard* og egendefinerte tag-sett er nødvendige for å klargjøre spesifikke enhets-/klientinnstillinger. Dette kodesettet gir fleksibilitet i å administrere klientens nettverks-/tjenestetilkoblingsinnstillinger samt funksjonsaktiveringskontroller.

Dette egendefinerte tagsettet leveres av en systemadministrator via alternativet *System → Ressurser → Enhetsadministrasjon-tagsett* . Administratoren må legge til nye tagsett:

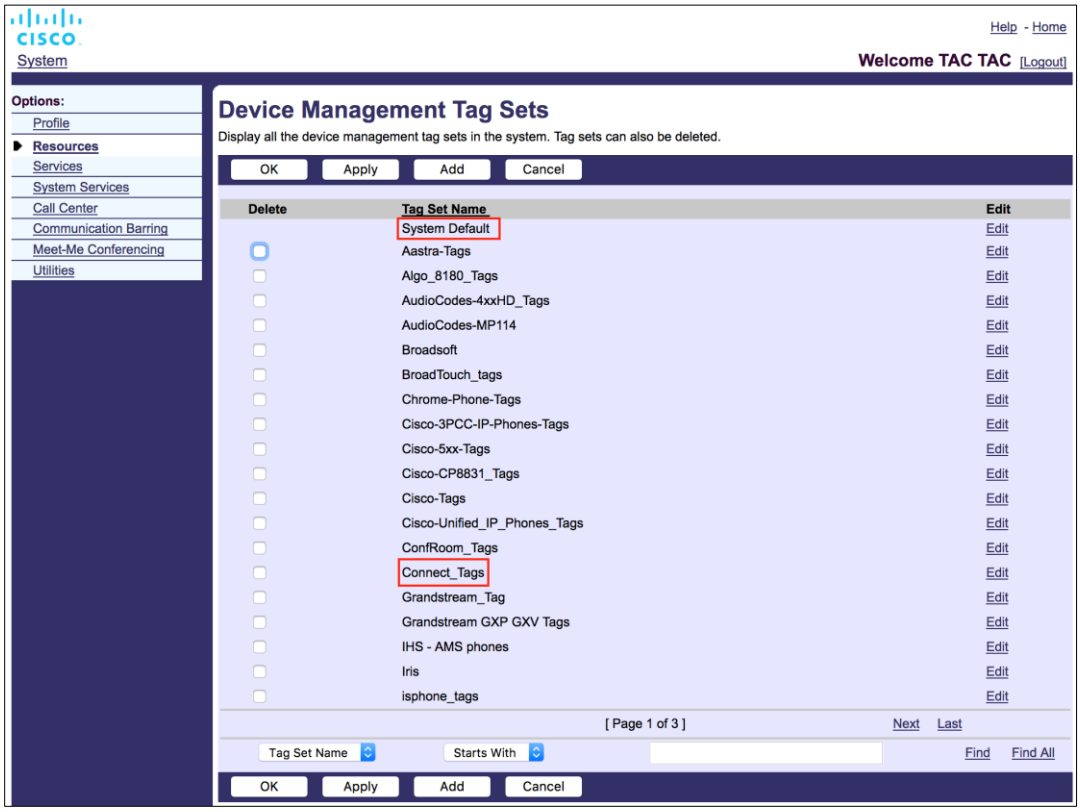
- Mobil: Connect_Tags
- Tablett: ConnectTablet_Tags
- Skrivebord: BroadTouch_Tags

Opprett hver enkelt tag og angi verdien. Seksjonsreferanser gir detaljerte beskrivelser for hver tag. De tilpassede taggene er delt i grupper basert på funksjonaliteten og diskuteres senere i dette dokumentet.



Figur 1 Skrivesett for administrasjon av stasjonære enheter

Konfidensiell Cisco



Figur 2 Etikettsett for administrasjon av mobilenheter

5.2 Delvis samsvarsforbedringer for valg av enhetstype

For å tillate økt fleksibilitet ved valg av funksjonalitetspakker for brukergrupper eller individuelle brukere, velges enhetsprofiltypen basert på et (første) delvis samsvar. Dette lar kundene bruke forskjellige enhetstyper.

Den generelle prosedyren for enhetsadministrasjon angir at Cisco BroadWorks Application Server gir en enhetsprofiltype. Den heter "Business Communicator - PC" for desktop, "Connect - Mobile" for mobil, og "Connect - Tablet" for nettbrett. En enhetsprofil kan opprettes og tildeles til brukeren. Applikasjonsserveren bygger deretter en konfigurasjonsfil og lagrer den på profilserveren.

Ved pålogging spør klienten den tilordnede enhetslisten via Xsi og søker etter den tilsvarende enhetstypeprofilen. Klienten velger den første profilen som starter med det tilsvarende enhetstypenavnet. Deretter brukes enhetsprofilens konfigurasjonsdata (konfigurasjonsfilen) knyttet til denne enhetsprofilen til å aktivere og deaktivere ulike funksjoner.

Dette gjør at den samme kjørbare klienten kan brukes med ulike enhetsprofiltyper, slik at tjenesteleverandøren kan endre funksjonspakker for individuelle brukere eller grupper av brukere ved å bare endre enhetsprofiltypen i DM for en bruker eller gruppe brukere.

Tjenesteleverandøren kan for eksempel ha et hvilket som helst antall enhetsprofiltyper basert på brukerroller, for eksempel "Business Communicator - PC Basic", "Business Communicator - PC Executive" eller "Business Communicator - PC Assistant" og endre funksjonaliteten som er tilgjengelig for individuelle brukere ved å endre enhetsprofiltypen for dem.

Konfidensiell Cisco

Merk at det ikke forventes å ha flere samsvarende enhetsprofiltyper i den mottatte enhetslisten XML, men bare én.

5.3 Klientkonfigurasjon

Webex for CiscoBroadWorks -versjonen av klienten bruker *config-wxt.xml* filen til å konfigurere anropsfunksjonaliteten. Det er en egen konfigurasjonsprosedyre for Webex som ikke dekkes i dette dokumentet.

5.4 Distribusjon av config-wxt.xml

Legg til den tilsvarende *config-wxt.xml* filen i enhetsprofilene «Koble til – Mobil», «Koble til – Nettbrett» og «Business Communicator – PC». Webex for Cisco BroadWorks bruker de samme enhetsprofilene som UC-One, slik at det blir enklere for distribusjon.

MERKNAD 1: En konfigurasjonsfil må eksistere for hver enhetsprofil.

MERKNAD 2: Det anbefales STERKT at malene holdes oppdatert med den nyeste versjonen av Webex appen

5.5 Konfigurasjonsfil (config-wxt.xml)

Nye egendefinerte koder, med **_WXT** -suffiks, brukes til å skille de nye Webex for CiscoBroadWorks -konfigurasjonsdistribusjon fra eldre klienter. Det er imidlertid fortsatt noen (system)-tagger som deles mellom UC-One og Webex.

Noen av Cisco BroadWorks System Custom Tags brukes også i *config-wxt.xml* konfigurasjonsfilen. Hvis du vil ha mer informasjon om hver av følgende koder, kan du se avsnitt *5.7 Cisco BroadWorks Dynamic Built-in* 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%

Konfidensiell Cisco

- %BWE911-SECRETKEY%
- %BWE911-EMERGENCY-NUMBER-LIST%
- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (Webex Calling kun)

5.6 Standardkoder for system

Som systemadministrator kan du få tilgang til systemstandardkodene via alternativet *System → Ressurser → Enhetsadministrasjon-tagsett* . Følgende systemstandardkoder må klargjøres når VoIP Calling-pakken er installert.

Merkelapp	Beskrivelse
%SBC_ADDRESS_WXT%	Dette bør konfigureres som det fullt kvalifiserte domenenavnet (FQDN) eller IP-adressen til sesjonsgrensekontrolleren (SBC) som er distribuert i nettverket. Eksempel: sbc.yourdomain.com
%SBC_PORT_WXT%	Hvis SBC_ADDRESS_WXT er en IP-adresse, bør denne parameteren settes til SBC-porten. Hvis SBC_ADDRESS_WXT det er et FQDN, kan det ikke settes inn. Eksempel: 5075

5.7 Cisco BroadWorks Dynamic Built-in System Tags

I tillegg til standard systemkoder og egendefinerte koder som må defineres, finnes det eksisterende Cisco BroadWorks systemkoder som vanligvis brukes og er en del av den anbefalte DTAF-filen (Device Type Archive File). Disse taggene er oppført i denne delen. Avhengig av den installerte løsningspakken, brukes ikke alle systemkoder.

Merkelapp	Beskrivelse
%BWNETWORK-CONFERENCE-SIPURI-n%	Dette er server-URIen som brukes til å aktivere N-Way-konferanser.
%BWVOICE-PORTAL-NUMBER-n%	Dette nummeret brukes til talepost. Klienten ringer dette nummeret når de henter talepost.
%BWLINEPORT-n%	SIP-brukernavn som brukes i SIP-signalering, for eksempel ved registrering.
%BWHOST-n%	Dette er domenedelen av den klargjorte linjeporten for enheten som er tildelt brukeren. Den hentes fra brukerens profil. Brukes vanligvis som SIP-domene.

Konfidensiell Cisco

Merkelapp	Beskrivelse
%BWAUTHUSER-n%	Dette er autentiseringsbrukernavnet. Hvis abonnenten har blitt tildelt autentisering, er dette den tildelte bruker-IDen på Autentiseringssiden uavhengig av valgt autentiseringsmodus for enhetstypen. SIP-brukernavnet, vanligvis brukt i 401 og 407-signalisering. Kan være forskjellig fra standard SIP-brukernavn.
%BWAUTHPASSWORD-n%	Dette er brukerens godkjenningspassord. Hvis abonnenten har fått tilordnet godkjenning, er dette det klargjorte passordet på Godkjenning-siden, uavhengig av den valgte godkjenningsmodusverdien for enhetstypen. SIP-passordet som brukes i SIP-signalisering.
%BWE164-n%	Denne koden inneholder brukerens telefonnummer i internasjonalt format.
%BWNAME-n%	Dette er abonnentens fornavn og etternavn i brukerens profil. Fornavn og etternavn er koblet sammen. Ved flerlinjekonfigurasjon, hvis ingen linjeetikett er konfigurert og hvis den ikke er tom, brukes som visningsnavn for linjen i linjevelgeren.
%BWEXTENSION-n%	Abonnentens utvidelse hentes fra utvidelsen som er klargjort i brukerens profil. Hvis en utvidelse ikke er klargjort, erstattes taggen med abonnentens telefonnummer (DN).
%BWAPPEARANCE-LABEL-n%	Dette er linjeetiketten som er konfigurert. Brukes som linjenavn, hvis det ikke er tomt.
%BWDISPLAYNAMELINEPORT%	Dette er linjen/porten til den første private linjen, i motsetning til en delt linje (Shared Call Appearance). Dette er linjeporten som er klargjort på enheten som er tilordnet brukeren. Dette hentes fra brukerens profil. Brukes til å identifisere primærlinjen til brukeren.
%BWLINEPORT-PRIMARY%	Den primære linjeporten klargjøres på enheten som er tilordnet brukeren. Denne taggen inkluderer ikke domenedelen av den klargjorte linjeporten. Den hentes fra brukerens profil.
%BWE911-PRIMARY-HELDURL%	Angir URL-en til RedSky Emergency Location Platform som støtter HELD-protokollen.
%BWE911-CUSTOMERID%	Kunde-ID-en (HeldOrgId, CompanyID) som ble brukt for RedSky HTTPS-forespørselen.
%BWE911-SECRETKEY%	Hemmeligheten til å autentisere RedSky HTTPS-forespørselen.

Konfidensiell Cisco

Merkelapp	Beskrivelse
%BWE911-EMERGENCY-NUMBER-LIST%	Listen over nødnumre støttet av RedSky. Hvis du vil bruke denne koden, må den %RESERVEDBW911-EMERGENCY-NUMBER-LIST% reserverte egendefinerte koden legges til i kodesettet som brukes av enhetstypen. "Reservert"-merket må inneholde nødnumrene som er definert på BroadWorks under AS_CLI/System/CallP/CallTypes > i et kommadelt format, for eksempel 911, 0911, 933. **MERK:** Klienten Webex støtter ikke jokertegn i nødnumre. derfor bør bare eksakte nødnumre legges til den "reserverte" tilpassede taggen. Følgende eksempel viser hvordan funksjonen for reservert kode er ment å brukes: 1) Den opprinnelige taggen %BWE911-EMERGENCY-NUMBER-LIST% legges til malfilen på enheten 2) Den reserverte egendefinerte taggen %RESERVEDBW911-EMERGENCY-NUMBER-LIST% legges til kodesettet som brukes av enheten med verdien 911, 0911, 933 3) Når filen gjenoppbygges, blir den %RESERVEDBW911-EMERGENCY-NUMBER-LIST% native taggen løst til 911, 0911, 933
%BW-MEMBERTYPE-n%	Dette er typen for hver linje. Det kan være en av "Virtuell profil", "Bruker" eller "Sted".
%BWUSEREXTID-n%	Dette er den eksterne ID-en for en gitt linje (Webex Calling kun)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Gir informasjon hvis den korresponderende linjen har konfigurert samtalehentingsgruppe. (kun Webex ringer)

Konfidensiell Cisco

6 Egendefinerte koder

Denne delen beskriver egendefinerte taggene som brukes i Webex for Cisco BroadWorks. Den viser alle de egendefinerte taggene som brukes for både skrivebords- og mobil-/nettbrettplattformer.

Vær imidlertid oppmerksom på at enkelte innstillinger beskrevet i denne delen kun støttes for den spesifikke utgivelsen av klienten. For å finne ut om en innstilling ikke gjelder for en eldre klientversjon, se den aktuelle utgivelsesspesifikke konfigurasjonsveiledningen.

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_REJECT_WITH_486_WXT%	Y	Y	sant	*6.1.16 Avvisning av innkommende anrop*
%REJECT_WITH_XSI_MODE_WXT%	N	Y	decline_false	*6.3.2 Push-varsler for anrop*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	Y	opptatt	*6.3.2 Push-varsler for anrop*
%ENABLE_TRANSFER_CALLS_WXT%	Y	Y	feil	*6.1.20 Overfør*
%ENABLE_CONFERENCE_CALLS_WXT%	Y	Y	feil	*6.1.21 N-Way-konferansesamtaler og deltakere*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	Y	Y	feil	*6.1.21 N-Way-konferansesamtaler og deltakere*
%MAX_CONF_PARTIES_WXT%	Y	Y	10	*6.1.21 N-Way-konferansesamtaler og deltakere*
%ENABLE_CALL_STATISTICS_WXT%	Y	Y	feil	*6.1.24 Samtalestatistikker*
%ENABLE_CALL_PULL_WXT%	Y	Y	feil	*6.1.22 Anropstrekk*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	Y	feil	*6.3.2 Push-varsler for anrop*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	Y	Y	feil	*6.1.28 Utskrift av talepost for Webex Calling*
%ENABLE_MWI_WXT%	Y	Y	feil	*6.1.27 Talepost, visuell talepost, indikator for melding venter*
%MWI_MODE_WXT%	Y	Y	tomt	*6.1.27 Talepost, visuell talepost, indikator for melding venter*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_VOICE_MAIL_WXT%	Y	Y	feil	*6.1.27 Talepost, visuell talepost, indikator for melding venter*
%ENABLE_VISUAL_VOICE_MAIL_WXT%	Y	Y	feil	*6.1.27 Talepost, visuell talepost, indikator for melding venter*
%ENABLE_FORCED_LOGOUT_WXT%	Y	N	feil	*6.2.1* *Tvungen* utlogging
%FORCED_LOGOUT_APPID_WXT%	Y	N	tomt	*6.2.1* *Tvungen* utlogging
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	Y	Y	feil	*6.1.29.1 Viderekobling alltid*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	Y	Y	sant	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	Y	Y	feil	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_EMERGENCY_DIALING_WXT%	N	Y	feil	*6.3.1 Nødsamtaler*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	Y	911, 112	*6.3.1 Nødsamtaler*
%ENABLE_USE_RPORT_WXT%	Y	Y	feil	*6.1.14 SIP rport-administrasjon for NAT-traversering*
%RPORT_USE_LOCAL_PORT_WXT%	Y	Y	feil	*6.1.14 SIP rport-administrasjon for NAT-traversering*
%USE_TLS_WXT%	Y	Y	feil	*6.1.2 SIP over TLS og sikker transportprotokoll i sanntid*
%SBC_ADDRESS_WXT%	Y	Y	tomt	*5.6 Standardkoder* for system
%SBC_PORT_WXT%	Y	Y	5060	*5.6 Standardkoder* for system
%USE_PROXY_DISCOVERY_WXT%	Y	Y	feil	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%USE_TCP_FROM_DNS_WXT%	Y	Y	sant	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%USE_UDP_FROM_DNS_WXT%	Y	Y	sant	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%USE_TLS_FROM_DNS_WXT%	Y	Y	sant	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%DOMAIN_OVERRIDE_WXT%	Y	Y	tomt	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	Y	Y	sant	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	Y	Y	sant	*6.1.6 Dynamisk SIP-proxy-oppdagelse*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Y (kun Windows)	N	feil	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	Y	Y	5000	*6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-sokkelen*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	Y	Y	10000	*6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-sokkelen*
%SOURCE_PORT_WXT%	Y	Y	5060	*6.1.7 Foretrukket portbruk for SIP*
%SIP_FAILBACK_ENABLED_WXT%	Y	N	sant	*6.1.8.2 SIP-feilback*
%SIP_FAILBACK_TIMEOUT_WXT%	Y	N	900	*6.1.8.2 SIP-feilback*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	Y	N	feil	*6.1.8.2 SIP-feilback*
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	Y	Y	DNS	*6.1.8.3. Håndhev IP-versjon*
%USE_ALTERNATIVE_IDENTITIES_WXT%	Y	Y	feil	*6.1.10 Bruk P-tilknyttede URI-er i* REGISTER
%TCP_SIZE_THRESHOLD_WXT%	Y	Y	18000	*6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives*
%SIP_REFRESH_ON_TTL_WXT%	Y	N	feil	*6.1.8.4 DNS TTL-administrasjon*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	Y	Y	feil	*6.1.12 Støtte* for SIP-OPPDATERING
%ENABLE_PEM_SUPPORT_WXT%	Y	Y	feil	*6.1.11 SIP P-Early Media (PEM)-topptekst*
%ENABLE_SIP_SESSION_ID_WXT%	Y	Y	feil	*6.1.15 SIP-økt-ID*
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	Y	Y	feil	*6.1.13 Eldre SIP INFO FIR*
%SRTP_ENABLED_WXT%	Y	Y	feil	*6.1.2 SIP over TLS og sikker transportprotokoll i sanntid*
%SRTP_MODE_WXT%	Y	Y	feil	*6.1.2 SIP over TLS og sikker transportprotokoll i sanntid*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_REKEYING_WXT%	Y	Y	sant	*6.1.2 SIP over TLS og sikker transportprotokoll i sanntid*
%RTP_AUDIO_PORT_RANGE_START_WXT%	Y	Y	8000	*6.1.17 Portområde* for transportprotokoll i sanntid
%RTP_AUDIO_PORT_RANGE_END_WXT%	Y	Y	8099	*6.1.17 Portområde* for transportprotokoll i sanntid
%RTP_VIDEO_PORT_RANGE_START_WXT%	Y	Y	8100	*6.1.17 Portområde* for transportprotokoll i sanntid
%RTP_VIDEO_PORT_RANGE_END_WXT%	Y	Y	8199	*6.1.17 Portområde* for transportprotokoll i sanntid
%ENABLE_RTCP_MUX_WXT%	Y	Y	sant	*6.1.19 RTCP MUX*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	Y	Y	sant	*6.1.33 XSI-hendelseskanal*
%CHANNEL_HEARTBEAT_WXT%	Y	Y	10000	*6.1.33 XSI-hendelseskanal*
%XSI_ROOT_WXT%	Y	Y	tom (bruker original URL)	*6.1.32 XSI-rot og -stier*
%XSI_ACTIONS_PATH_WXT%	Y	Y	/com.broadsoft.xsi-actions/	*6.1.32 XSI-rot og -stier*
%XSI_EVENTS_PATH_WXT%	Y	Y	/com.broadsoft.xsi-events/	*6.1.32 XSI-rot og -stier*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	Y	Y	feil	*6.1.25 Automatisk gjenoppretting av anrop / sømløs overføring* av anrop
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	Y	cs-bare	*6.3.1 Nødsamtaler*
%ENABLE_CALL_PICKUP_BLIND_WXT%	Y	N	feil	*6.2.2 Mottak av anrop*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	Y	N	feil	*6.2.2 Mottak av anrop*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%WEB_CALL_SETTINGS_URL_WXT%	Y	Y	tomt	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%USER_PORTAL_SETTINGS_URL_WXT%	Y	Y	tomt	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%ENABLE_CALL_CENTER_WXT%	Y	Y	feil	*6.1.31 Pålogging/utlogging av telefonsenter / samtalekø*
%WEB_CALL_SETTINGS_TARGET_WXT%	Y	Y	eksternt	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	Y	Y	sant	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%USE_MEDIASEC_WXT%	Y	Y	feil	*6.1.3 3GPP SIP-topptekster for SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	Y	feil	*6.3.4 Klikk for å ringe (Ring tilbake)*
%DIALING_CALL_BACK_TIMER_WXT%	N	Y	10	*6.3.4 Klikk for å ringe (Ring tilbake)*
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	Y	N	feil	*6.2.3 Støtte for sjef-administrator (lederassistent)*
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	Y	35	*6.3.2 Push-varsler for anrop*
%ENABLE_CALL_RECORDING_WXT%	Y	Y	feil	*6.1.26 Anropsopptak*
%ENABLE_SINGLE_ALERTING_WXT%	N	Y	feil	*6.3.3 Enkeltvarsling*
%ENABLE_CALL_PARK_WXT%	Y	Y	feil	*6.1.23 Samtaleparkering/hent*
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	Y	Y	10	*6.1.23 Samtaleparkering/hent*
%ENABLE_RTP_ICE_WXT%	Y	Y	feil	*6.1.18 ICE-støtte (Webex Calling kun)*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%RTP_ICE_MODE_WXT%	Y	Y	icestun	*6.1.18 ICE-støtte (Webex Calling kun)*
%RTP_ICE_SERVICE_URI_WXT%	Y	Y	tomt	*6.1.18 ICE-støtte (Webex Calling kun)*
%RTP_ICE_PORT_WXT%	Y	Y	3478	*6.1.18 ICE-støtte (Webex Calling kun)*
%ENABLE_RTP_ICE_IPV6_WXT%	Y	Y	feil	*6.1.18 ICE-støtte (Webex Calling kun)*
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	Y	N	feil	*6.1.8.4 DNS TTL-administrasjon*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	Y	N	feil	*6.2.4 Eskalere SIP-anrop til møte*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	Y	N	feil	*6.2.5 Kontrollanrop for bordtelefon – automatisk svar*
%ENABLE_DIALING_VOIP_WXT%	N	Y	sant	*6.3.5 MNO-støtte* *Ring med Native Dialer*
%ENABLE_DIALING_NATIVE_WXT%	N	Y	feil	*6.3.5 MNO-støtte* *Ring med Native Dialer*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	Y	Y	sant	*6.1.35 SIP-URI-oppringing*
%ENABLE_SIP_VIDEOCALLS_WXT%	Y	Y	sant	*6.1.37 Deaktiver videosamtaler*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	Y	Y	sant	*6.1.37 Deaktiver videosamtaler*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Y	Y	Desktop - sant Mobil, nettbrett - falsk	*6.1.37 Deaktiver videosamtaler*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	Y	Y	feil	*6.1.38 Nødsamtaler (911) – Stedsrapportering med E911-leverandør*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	Y	Y	0	*6.1.38 Nødsamtaler (911) – Stedsrapportering med E911-leverandør*
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	Y	Y	-1	*6.1.38 Nødsamtaler (911) – Stedsrapportering med E911-leverandør*
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	Y	Y	én gang_per_pålogging	*6.1.38 Nødsamtaler (911) – Stedsrapportering med E911-leverandør*
%ENABLE_AUTO_ANSWER_WXT%	Y	N	feil	*6.2.6 Automatisk svar med tonevarsling*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	Y	Y	feil	*6.1.41 Angivelse* av søppelanrop
%ENABLE_NOISE_REMOVAL_WXT%	Y	Y	feil	*6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN/mobilsamtaler*
%ENABLE_AUDIO_MARI_FEC_WXT%	Y	Y	feil	*6.1.46.2 Videresending av fec (FEC) og resending av pakker (RTX)*
%ENABLE_AUDIO_MARI_RTX_WXT%	Y	Y	feil	*6.1.46.2 Videresending av fec (FEC) og resending av pakker (RTX)*
%ENABLE_VIDEO_MARI_FEC_WXT%	Y	Y	feil	*6.1.46.2 Videresending av fec (FEC) og resending av pakker (RTX)*
%ENABLE_VIDEO_MARI_RTX_WXT%	Y	Y	feil	*6.1.46.2 Videresending av fec (FEC) og resending av pakker (RTX)*
%ENABLE_CALL_BLOCK_WXT%	Y	Y	feil	*6.1.45 Blokkeringsliste (Webex Calling kun)*
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	Y	sant	*6.3.5.6 MNO Mobility - modul for* samtale
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	Y	sant	*6.3.5.6 MNO Mobility - modul for* samtale
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	Y	sant	*6.3.5.6 MNO Mobility - modul for* samtale
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	Y	Y	feil	*6.1.47 Samtidige samtaler med samme bruker*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	Y	N	feil	*6.2.14 Hendelsespakke for fjerndemping (Webex Calling kun)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	Y	Y	sant	*6.1.29.2 Viderekobling av anrop* til talepost
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	Y	Y	sant	*6.1.8.1 SIP-failover*
%ENABLE_CALL_MOVE_HERE_WXT%	Y	N	feil	*6.2.15 Flytt samtale*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	Y	Y	feil	*6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN/mobilsamtaler*
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	Y	tomt	*6.3.5.1 Ring med Native Dialer*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	Y	Y	feil	*6.1.20 Overfør*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	Y	Y	sant	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	Y	feil	*6.3.6 Innkommende innringer-ID*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	Y	feil	*6.3.6 Innkommende innringer-ID*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	Y	feil	*6.1.50 Innringer-ID Utgående innringer-ID*
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	Y	feil	*6.1.50 Innringer-ID Utgående innringer-ID*
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	Y	feil	*6.1.50 Innringer-ID Utgående innringer-ID*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	Y	feil	*6.1.50 Innringer-ID Utgående innringer-ID*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	Y	feil	*6.1.50 Innringer-ID Utgående innringer-ID*
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	Y	Y	feil	*6.1.49 Informasjon om viderekobling av anrop*
%ENABLE_BUSY_LAMP_FIELD_WXT%	Y	N	feil	*6.2.8.1 Opptattlampefelt*
%ENABLE_BLF_DISPLAY_CALLER_WXT%	Y	N	sant	*6.2.8.1 Opptattlampefelt*
%BLF_NOTIFICATION_DELAY_TIME_WXT%	Y	N	0	*6.2.8.1 Opptattlampefelt*
%ENABLE_GCP_NOTIFICATIONS_WXT%	Y	N	feil	*6.2.8.2 Gruppe for mottak av anrop (Webex Calling kun)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	Y	N	feil	*6.2.8.2 Gruppe for mottak av anrop (Webex Calling kun)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	Y	N	120	*6.2.8.2 Gruppe for mottak av anrop (Webex Calling kun)*
%UDP_KEEPALIVE_ENABLED_WXT%	Y	Y	sant	*6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives*
%TCP_KEEPALIVE_ENABLED_WXT%	Y	Y	feil	*6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives*
%TLS_KEEPALIVE_ENABLED_WXT%	Y	Y	feil	*6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives*
%ENABLE_MULTI_LINE_WXT%	Y	Y	feil	*6.2.12 Flere linjer – delt linje-utseende Flerlinje for mobil (Webex Calling kun)*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	Y	feil	*6.2.4 Eskalere SIP-anrop til møte (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	Y	feil	*6.3.5.3 Identitet for utgående anropslinje (CLID) – Dual Persona*

Konfidensiell Cisco

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Del
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	Y	feil	*6.3.5.36.3.5.3 Identitet for utgående anropslinje (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	Y	Y	løst	*6.1.50.2 Navn på ekstern innringer-ID*
%PERSONAL_ASSISTANT_ENABLED_WXT%	Y	Y	feil	*6.3.2.3 Personlig assistent (borte* tilstedeværelse)
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	Y	NPS	*6.4 Leveringsmodus (Webex Calling kun)*

Hvis du vil ha mer informasjon om tilordning av de egendefinerte kodene som brukes i Webex for Cisco BroadWorks til de som brukes av UC-One, kan du se avsnitt *8 Egendefinerte tagger tilordning mellom Webex for Cisco BroadWorks og UC-One*.

Konfidensiell Cisco

6.1 Vanlige funksjoner

6.1.1 SIP-serverinnstillinger

Klienten er vanligvis konfigurert til å bruke et SIP-nettverk, noe som gjøres ved å endre *config-wxt.xml* filen. Vanligvis må følgende parametere endres:

- SIP-domene. Dette brukes som domenedelen av egen SIP URI (egen SIP URI kalles også noen ganger linjeport) generelt i SIP-hoder og i eksterne (XSI) anrop. Brukerdelen av egen SIP URI kommer fra SIP-legitimasjonskonfigurasjonen (parameter <username> under <credentials>).
- SIP-serverens URI eller IP-adressen til SIP-proxyserveren hvis DNS-løsningen skulle mislykkes. Merk at for å bruke TLS, kan ikke IP-adresser brukes i proxy-parameteren, da TLS-sertifikatvalidering vil mislykkes. For mer informasjon om proxy-porten, se DM-taggen %SOURCE_PORT_WXT%. Merk at DNS TTL-administrasjonsfunksjonen ikke kan brukes når en IP-adresse brukes i proxy-adresseparameteren. Generelt anbefales det ikke å bruke en IP-adresse i dette feltet av disse grunnene.

Andre parametere kan også endres for å aktivere ulike funksjoner for å ringe. De forrige innstillingene aktiverer imidlertid grunnleggende funksjonalitet for følgende:

- Registrering på SIP-nettverket.
- Foreta lyd- eller videosamtaler.
- Utfører DNS-basert proxy-oppdagelse, som tillater bruk av flere proxyer.

Når SIP-registrering er aktivert, må aktivering av SIP SUBSCRIBE for MWI gjøres via separate konfigurasjonsparametere. For mer informasjon om talepost, se avsnitt *6.1.27 Talepost, visuell talepost, indikator for melding venter*.

Merk at grunnleggende SIP-konfigurasjon alltid er nødvendig for MWI selv når SIP-anrop er deaktivert. MWI er avhengig av SIP NOTIFYs.

Oppsettet av SIP-serverne følger dette grunnleggende skjemaet:

- Proxyadressen inneholder SIP-serverens URI.
- Bare én proxy kan defineres.
- DNS-proxy-oppdagelsen gir støtte for mange proxyer, som krever riktig oppsett av DNS.

I tillegg er SIP-timere eksponert i konfigurasjonsfilen (anbefales ikke å endre dem).

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

- T1 – hvor lang tid, i millisekunder, for en nettverksforsinkelse.
- T2 – maksimal tid, i millisekunder, før overføring av ikke-inviterte forespørsler og invitasjonssvar på nytt.

Konfidensiell Cisco

- T4 – den maksimale tiden, i millisekunder, for en melding å forbli i nettverket.

Hver linje har egne parametere som talepostnummer, konferanse-URI og domenet, samt SIP-autentiseringslegitimasjonen. Separate legitimasjoner kan konfigureres for 401- og 407-signalering om nødvendig.

Følgende eksempel og tabell gir informasjon om de mest typiske DM-taggene som brukes for SIP-konfigurasjon.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%BWLINEPORT-n%	tomt	streng	Vanligvis SIP-brukernavn. Hvis du vil ha mer informasjon, kan du se avsnitt *5.7 Cisco BroadWorks Dynamic Built-in System* Tags. Eksempel: johndoe
%BWAUTHPASSWORD-n%	tomt	streng	Vanligvis SIP-passord. Hvis du vil ha mer informasjon, kan du se avsnitt *5.7 Cisco BroadWorks Dynamic Built-in System* Tags. Eksempel: hemmelig passord
%BWE164-n%	tomt	telefonnummer	Standard telefonnummer for brukeren i internasjonalt format. Hvis du vil ha mer informasjon, kan du se avsnitt *5.7 Cisco BroadWorks Dynamic Built-in System* Tags. Eksempel: 12345678
%SBC_ADDRESS_WXT%	tomt	streng	Hvis du vil ha mer informasjon, kan du se avsnitt *5.6 Standardkoder* for system. Eksempel: sbcexample.domain.com
%SBC_PORT_WXT%	5060	tall	Hvis du vil ha mer informasjon, kan du se avsnitt*5.6 Standardkoder* for system. Eksempel: 5060
%BWHOST-n%	tomt	streng	Brukes vanligvis som SIP-domene. Hvis du vil ha mer informasjon, kan du se avsnitt *5.7 Cisco BroadWorks Dynamic Built-in System* Tags. Eksempel: exampledomain.com
%SOURCE_PORT_WXT%	5060	tall	Brukes vanligvis for parameteren *preferred-port* . For mer informasjon, se avsnitt *6.1.7 Foretrukket portbruk for SIP*. Eksempel: 5061
%BWUSEREXTID-n%	tomt	streng	(Webex Calling bare) Holder linjens eksterne ID Hvis du vil ha mer informasjon, kan du se *6.2.13 Flere linjer – virtuelle linjer (Webex Calling kun)*. Eksempel: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

MERK: Det anbefales sterkt at SIP-porten er forskjellig fra 5060 (for eksempel 5075) på grunn av kjente problemer med bruk av standard SIP-port (5060) med mobile enheter.

Konfidensiell Cisco

6.1.2 SIP over TLS og sikker transportprotokoll i sanntid

Klienten kan konfigureres til å bruke SIP-signalering over TLS og Secure Real-time Transport Protocol (SRTP) for mediekryptering. Disse funksjonene må imidlertid være aktivert i konfigurasjonen som vist i følgende eksempel. Merk også at når dynamisk SIP-proxy-oppdagelse brukes, overstyrer DNS SRV-prioriteter statiske parametere som denne (%USE_TLS_WXT%), og ikke-TLS-transport brukes hvis den har høyere prioritet i DNS SRV. For mer informasjon om dynamisk SIP-proxy-oppdagelse, se avsnitt *6.1.6 Dynamisk SIP-proxy-oppdagelse.*

Når dynamisk proxy-oppdagelse ikke brukes, tar aktivering av TLS for SIP det i bruk.

Hvis du vil ha mer informasjon om anbefalinger for SIP-port og transportprotokoll når SIP ALG brukes i nettverket, kan du se *Webex for Cisco BroadWorks Løsningsveiledning*.

Merk at sertifikatet som brukes må være gyldig. Videre skal sertifikatkjeden være intakt slik at også mellomsertifikatet henger sammen. Det anbefales at det brukes et mye brukt sertifikat, slik at det allerede er til stede, som standard, på enhetene. Det er også mulig å legge til sertifikater lokalt på den stasjonære maskinen enten manuelt eller ved å bruke masseklargjøring, selv om dette vanligvis ikke gjøres.

For å aktivere relatert SRTP for mediekryptering, er det en egen innstilling.

I tillegg til RTP kan RTCP-trafikk sikres med de samme mekanismene som RTP ved å bruke den foregående konfigurasjonen.

For SIP/TLS-chiffer, se *Vedlegg A: TLS-chifre.*

SRTP brukes til å gi sikkerhet for mediestrømmen i tre forskjellige aspekter:

- Konfidensialitet (data er kryptert)
- Autentisering (sikkerhet for identiteten til den eller de andre partene)
- Integritet (måler mot for eksempel replay-angrep)

Den nåværende versjonen av medierammeverket støtter AES 128 Counter Mode for beskyttelse og Hash Message Authentication Code (HMAC)-SHA-1 for autentisering. Hovednøkkelstørrelsen er 16 byte og mastersalt er 14 byte.

Medierammen støtter både den fullstendige (80-biters) og korte (32-biters) autentiseringskoden. Klienten utveksler nøklene inne i SDP som en del av SIP-signalering, begge sider av samtalen sender nøkkelen de bruker til den andre siden.

SRTP kan aktiveres ved å bruke konfigurasjonen vist i følgende eksempel. Den nåværende implementeringen bruker bare den sikre SDP-profilen og støtter flerlinjes SDP for oppføringer for Audio Visual Profile (AVP) og Secure Audio Visual Profile (SAVP). SRTP-implementeringen har blitt testet vellykket i sin vanlige distribusjonskonfigurasjon med forskjellige SBC-er. Interoperabilitetstesting (IOT) med endepunkter som kun støtter kryptering ved hjelp av AVP-profilen støttes ikke.

Multiline SDP-prosedyrer knyttet til SRTP er implementert, slik at flere m-linjer alltid brukes. Det brukes egne m-linjer for AVP og SAVP.

Vær imidlertid oppmerksom på at SBC-konfigurasjonen må vurderes nøye; spesielt å sikre at den innkommende "m="-linjen, assosiert med RTP/SAVP i SDP, ikke fjernes fordi SRTP-anrop i visse tilfeller kan bli blokkert.

Konfidensiell Cisco

Flere forskjellige nettverkskonfigurasjoner er imidlertid mulig, i noen distribusjoner er ikke SBC involvert i medietrafikken, mens i andre distribusjoner er hvert klient-RTP-medieben mot SBC separat kryptert og forhandlet via SBC. I noen distribusjoner tillater ikke SBC flere SDP-linjer.

SBC-en kan også endre rekkefølgen til SDP-m-linjene ved samtaleoppsett, ved å sette AVP (ikke-kryptert) eller SAVP (kryptert) m-linje først. Derfor blir klienter som velger den første fungerende m-linjen laget for å foretrekke enten kryptert eller ukryptert trafikk. De ulike SRTP-konfigurasjonsalternativene er som følger:

- Obligatorisk – Ved anropsoppsett inkluderer den innledende SDP bare SAVP m-linjen ved tilbud og klienten aksepterer bare SAVP m-linjen i SDP når han svarer, derfor er kun SRTP-anrop mulig.
- Foretrukket – Ved oppsett av samtale inkluderer den første SDP-en både AVP- og SAVP-m-linjene, men SAVP er først når du tilbyr, og indikerer preferanserekkefølgen. Ved svar velger klienten SAVP hvis tilgjengelig selv om det ikke er den første m-linjen (i henhold til SIP-spesifikasjonene endres ikke rekkefølgen på m-linjene ved svar).
- Valgfritt – Ved samtaleoppsettet inkluderer den første SDP både SAVP- og AVP-m-linjene ved tilbud, men AVP angir først preferanserekkefølgen. Ved svar velger klienten første m-linje, AVP eller SAVP.
- SRTP ikke aktivert – Det er ingen SAVP m-linje i den innledende SDP når du tilbyr. Ved svar aksepteres ikke SAVP, derfor er kun RTP-anrop mulig.
- Transport – Velg SRTP-modus automatisk basert på transportprotokoll. Hvis TLS brukes, er obligatorisk SRTP-modus aktivert. Hvis TCP eller UDP brukes, brukes ingen SRTP.

SRTP versus RTP er symmetrisk i begge retninger av samtalen, det vil si at sendings- og mottaksprofiler er de samme.

```
<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%"/>
```

SRTCP (Secure Real-Time Control Protocol) brukes også hvis SRTP er aktivert.

I noen distribusjoner støttes ikke ny nøkkel for SRTP. Derfor er det en konfigurasjonsparameter for å aktivere/deaktivere SRTP-omnøkkel. Nye nøkler tas imidlertid alltid i bruk når de mottas i en oppdatert SDP i henhold til rfc3264. Konfigurerbarhet gjelder kun sending av nye nøkler.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_TLS_WXT%	feil	sann, usann	Når satt til "false", er SIP TLS deaktivert. Når satt til «sann», aktiveres SIP TLS. Vær oppmerksom på at hvis *6.1.6 Dynamisk SIP-proxy-oppdagelse* brukes, ignoreres denne parameteren.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SRTP_ENABLED_WXT%	feil	sann, usann	Når satt til «usann», deaktiveres SRTP. Når satt til «sann», aktiveres SRTP.
%SRTP_MODE_WXT%	valgfritt	obligatorisk, foretrukket, valgfritt, transport	Definerer hvor foretrukket SRTP er ved anropsoppsett. Standardverdien er "valgfritt".
%ENABLE_REKEYING_WXT%	sant	sann, usann	Aktiverer SIP (SDP) re-keying for SRTP.

merk: Hvis ICE-støtte er aktivert (se *6.1.18 ICE-støtte (Webex Calling* kun)), vil tilbakestilling alltid utføres (%ENABLE_REKEYING_WXT% verdien fra konfigurasjonen ignoreres).

6.1.3 3GPP SIP-topptekster for SRTP

Nyere 3GPP-spesifikasjoner krever ekstra SIP-hoder for å bruke Secure Real-time Transport Protocol (SRTP). For mer informasjon, se *3GPP TS 24.229* samt følgende:

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

Overskriftene som kreves av denne spesifikasjonen kan bryte SIP-anrop i distribusjoner der denne spesifikasjonen ikke brukes. Derfor anbefales disse overskriftene kun å brukes i miljøer der serversiden støtter dem.

Bare å aktivere bruken av overskriftene kan konfigureres. Det finnes ingen ytterligere konfigurerbarhet for individuelle overskrifter. Alle overskrifter er enten aktivert eller deaktivert.

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

Følgende tag kontrollerer denne muligheten.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_MEDIASEC_WXT%	feil	sann, usann	Aktiverer 3GPP SIP-overskrifter for SRTP-forhandling.

6.1.4 Tving TCP-, TLS- eller UDP-bruk og Keepalives

Webex For CiscoBroadWorks -klienten kan konfigureres til å bruke enten TCP, TLS eller UDP for både SIP-signalisering og RTP-medier. Merk at klienten er standard til TCP. Merk også at uten TCP keepalive, stenges SIP TCP-tilkoblinger etter en periode med inaktivitet.

Følgende eksempel viser denne konfigurasjonsnoden.

```
<config>
```


Konfidensiell Cisco

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

Følgende tag kontrollerer om klienten bruker TCP eller UDP.

Merkelapp	Standard hvis utelatt	Støttede verdier (byte)	Beskrivelse
%TCP_SIZE_THRESHOLD_WXT%	0	0	Tvinger TCP til å brukes. Beslutningen om å bruke TCP eller UDP for klienten er opp til tjenesteleverandøren; anbefalingen er imidlertid å bruke TCP med standardverdien "0".
	0	1 til 99 000	Tvinger UDP til å brukes når meldingsstørrelsen er under verdien angitt her. Dette er standard til TCP når meldingsstørrelsen er større enn den angitte verdien. For å bruke UDP er 1500 standardanbefalingen.
	0	100000	Tvinger UDP til å brukes.

Den samme konfigurasjonsnoden har også parametere for UDP, TCP og TLS keepalive, vist i følgende eksempel.

```
<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>
```

De mulige parameterne er:

- Aktiverer TCP eller TLS keepalive, mulige verdier - true/false, standard er "false" hvis noden mangler. Merk at når denne funksjonen er aktivert, sendes TCP keepalives selv om UDP-transport brukes for SIP.

Konfidensiell Cisco

- Aktivering av UDP holder live, mulige verdier – sann/usann, standarden er «sann» hvis noden mangler. Vær oppmerksom på at når denne funksjonen er aktivert, sendes UDP-oppbevaringer selv om TCP-transport brukes for SIP. I tillegg, selv om TCP brukes for SIP, aksepterer klienten også trafikk over UDP i henhold til *RFC 3261*.
- Tidsavbrudd spesifiserer den maksimale tiden for inaktivitet i sekunder etter at keepalive-meldingen sendes. Ingen verdi betyr at keepalive er deaktivert for protokollen.
- Nyttelast for keepalive-meldingene, mulige verdier (ingen verdi betyr at keepalive er deaktivert for protokollen):
  - Crlf
  - Null (skal ikke brukes)
  - Egendefinert streng (**skal ikke brukes**)

Keepalives kan brukes til NAT-traverseringsformål for å holde NAT-bindinger åpne med lite ekstra trafikk.

Serverens IP-adresse og port for keepalives bestemmes ved å bruke de vanlige prosedyrene for SIP-proxy-oppdagelse. Merk at SIP-porter og valg av transportprotokoll oppnådd via SIP dynamisk proxy-oppdagelse overstyrer enhver statisk port eller transportkonfigurasjon. Hvis du vil ha mer informasjon om dynamisk proxy-oppdagelse, kan du se avsnitt *6.1.6 Dynamisk SIP-proxy-oppdagelse.*

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%UDP_KEEPALIVE_ENABLED_WXT%	sant	sann, usann	Kontrollerer om keep-alive-pakkene skal sendes for UDP-transporten.
%TCP_KEEPALIVE_ENABLED_WXT%	feil	sann, usann	Kontrollerer om oppbevaringspakkene skal sendes for TCP-transport.
%TLS_KEEPALIVE_ENABLED_WXT%	feil	sann, usann	Kontrollerer om de levende pakkene skal sendes til TLS-transporten.

6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-sokkelen

Tidligere var tidsavbruddet for å åpne en SIP-socket hardkodet til 5 sekunder for TCP og 10 sekunder for TLS. Disse tidsavbruddene kan nå konfigureres.

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


Konfidensiell Cisco

```
                </tcp>
                <tls>
                    <connect-
timeout>%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </tcp>
            </transports>
```

Følgende tagger kontrollerer socket-tilkoblingens tidsavbrudd (i millisekunder).

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<integer> - tidsavbruddet i millisekunder	Tidsavbrudd for kontakttilkobling når TCP-transport brukes.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	<integer> - tidsavbruddet i millisekunder	Tidsavbrudd for sokkeltilkobling når TLS-transport brukes.

6.1.6 Dynamisk SIP-proxy-oppdagelse

For å aktivere SIP dynamisk proxy-oppdagingsfunksjonalitet, se følgende eksempel.

```
<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>
```

Det er mulig å kontrollere hvilke transportprotokolloppføringer fra DNS SRV som brukes når mange er tilgjengelige ved å følge prosedyrene gitt i denne delen.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_PROXY_DISCOVERY_WXT%	feil	sann, usann	Aktiverer dynamisk SIP-proxy-oppdagelse for lyd- og videosamtaler. Den anbefalte verdien er "true".
%SBC_ADDRESS_WXT%	tomt	Streng	Denne Cisco-koden BroadWorks brukes vanligvis for parameteren for oppføringsnavn. Det skal være en gyldig URL - bør ikke være en IP-adresse. Hvis du vil ha mer informasjon, kan du se avsnitt*5.6 Standardkoder* for system. Eksempel: sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	tomt	Streng	Denne egendefinerte taggen brukes for domeneoverstyring. Se følgende avsnitt for mer informasjon. Eksempel: other.domain.com

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_TCP_FROM_DNS_WXT%	sant	sann, usann	Hvis denne parameterverdien er "false", blir DNS SRV-resultatene for denne transportprotokollen (TCP) forkastet. Hvis "sant", brukes resultatene fra DNS SRV for denne transportprotokollen (TCP). Avhengig av SRV-prioriteringene, kan en annen transport fortsatt velges.
%USE_UDP_FROM_DNS_WXT%	sant	sann, usann	Hvis parameterverdien er «usann», forkastes DNS SRV-resultatene for denne transportprotokollen (UDP). Hvis «sann», brukes resultatene fra DNS SRV for denne transportprotokollen (UDP). Avhengig av SRV-prioriteringene, kan en annen transport fortsatt velges.
%USE_TLS_FROM_DNS_WXT%	sant	sann, usann	Hvis parameterverdien er «usann», forkastes DNS SRV-resultatene for denne transportprotokollen (TLS). Hvis «sann», brukes resultatene fra DNS for denne transportprotokollen (TLS). Avhengig av SRV-prioriteringene, kan en annen transport fortsatt velges.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	sann, usann	sant	Aktiverer/deaktiverer DNS-sikkerhetskopieringstjenesten. Hvis aktivert, utføres A/AAAA-oppløsning for SIP-proxyadressen. Det tas kun i betraktning når SRV/NAPTR-tjenesteoppdagelse er aktivert.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	sann, usann	sant	Hvis satt til "true" og NAPTR-tjenesteoppdaging mislykkes eller ikke gir noen resultater, utføres SRV-tjenesteoppdagelse for den konfigurerte verten. Hvis satt til "false", utføres ingen SRV-oppdagelse.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	sann, usann	feil	Tillater omgåelse av OS DNS-bufferen.

DNS lar klienten få IP-adressen, porten og transportprotokollen for SIP-proxyen i henhold til RFC 3263.

DNS SRV, Naming Authority Pointer (NAPTR) og A-record-spørringer støttes. Ved pålogging er 3-trinns flyten som følger:

1. Utfør en NAPTR-spørring ved å bruke *<record-name>* feltet ovenfor for å få server-URI-ene med transportprotokollene hvis de finnes. Verdien for *<record-name>* parameteren skal være hele domenet som DNS skal løse, og kan ikke være en IP-adresse.

Konfidensiell Cisco

2. Løs elementer funnet i NAPTR-spørringen ved å bruke en SRV-spørring for å få den endelige server-URI og port. Domenedelen som brukes i SRV-spørringen er hentet fra resultatet av NAPTR-spørringen for å finne den endelige server-URI (og port). Porten mottatt fra DNS SRV-spørring brukes når DNS SRV-oppføringene er tilgjengelige. Merk at porten, kun fra konfigurasjonsfilen, gjelder for den statiske proxyen i konfigurasjonsfilen, og ikke for URIene som er løst med SRV. Se følgende eksempler for bruk av de forskjellige postnavnene.

   Hvis ingen NAPTR blir funnet, prøver klienten en SRV-spørring med postnavnet hentet fra <*domain*> parameteren med mindre det er <*domain-override*> parameter til stede, i så fall <*domain-override*> brukes og prøver automatisk å finne separate oppføringer for TCP , UDP og TLS (*_sip_protocol* [UDP, TCP eller TLS]). Merk at Stream Control Transmission Protocol (SCTP) ikke støttes. Hvis SRV-spørringer ikke gir noen resultater, mislykkes proxy-oppdagelsen, og sluttbrukeren får en feilmelding som indikerer at anrop ikke er tilgjengelige. I dette tilfellet er det ingen SIP-registrering. Men selv om alle SRV-spørringer mislykkes eller om serverne mottatt der ikke fungerer, som en reserve, sjekker klienten fortsatt om den konfigurerte statiske proxy-tjeneren fungerer, bare med A-spørringer til URI-en spesifisert i <proxy address> for å se hvis det gir en IP-adresse som gir en fungerende SIP-registrering. Port og transport i dette siste utvei-tilfellet kommer fra *tcp-threshold* og <*secure*> parametere.

3. Løs funnet URIer ved å bruke A-record-spørringen. De mottatte endelige IP-adressene prøves i den rekkefølgen de mottas for å få en fungerende forbindelse til SIP-proxyen. Denne rekkefølgen kan defineres av tjenesteleverandøren i DNS. Den første SIP-proxy-URIen, med et vellykket A-postoppslag, velges og brukes til den ikke lenger fungerer, eller klienten logger av. I A-spørringstrinnet brukes kun én IP-adresse om gangen selv om mange mottas. Imidlertid løses alle SRV-oppføringer inntil utlogging eller tap av nettverket.

Viktige merknader

MERKNAD 1: Hvis DNS-proxy-oppdagelse resulterer i valg av transportprotokoll i SRV-trinnet ved å motta en fungerende SIP-proxy-URI for en transportprotokoll, overstyrer den parameteren *tcp-threshold* som vanligvis brukes til å velge UDP eller TCP i konfigurasjonsfil. Det samme gjelder også for konfigurasjon av SIP/TLS. TCP eller UDP brukes avhengig av prioritet i DNS.

MERK 2: Elementer mottatt via SRV er prioritert over den statiske proxyen i konfigurasjonsfilen. NAPTR-ordren blir ikke sett på; kun SRV-prioritet teller. Når SRV resulterer i flere elementer med lik transportprotokoll, prioritet og vekt, velges alle mottatt tilfeldig. NAPTR-vekter støttes ikke i denne utgivelsen, men SRV-vekter støttes. SRV-prioritet blir først sett på, og for elementer med lik prioritet blir vekt sett på for å bestemme sannsynligheten for at en bestemt server blir forsøkt neste gang.

MERKNAD 3: Den valgfrie *domeneoverstyringsparameteren* lar A-postnavnet annet enn det i SIP-domenekonfigurasjonsparameteren løses med SRV når NAPTR-resultater utelates. Se følgende eksempler for bruk av parameteren *domeneoverstyring* .

MERKNAD 4: Klienten bruker operativsystemprimitiver for DNS-operasjoner, og vanligvis bufres DNS-svar for å respektere TTL-en til DNS-svaret.

MERK 5: DNS-typen (tjenesten) for NAPTR-poster må følge *RFC 3263* prosedyrer, ellers kan DNS-løsning mislykkes. For eksempel er det påkrevd å bruke SIPS+D2T for SIP over TLS.

MERKNAD 6: Klienten støtter kun visse prefikser for NAPTR-tjenester. Følgende viser de støttede prefiksene:

SIP+D2U ->_sip_utp

Konfidensiell Cisco

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

Hvis NAPTR-svaret inneholder en post med prefiks som ikke samsvarer med tjenestetypen, ignoreres denne posten.

Eksempel 1: Bruker DNS-proxy-oppdagelse uten konfigurasjonsparameter for domeneoverstyring

Følgende er et eksempel på en konfigurasjon som bruker SIP proxy-oppdagelse når bare SIP over TCP brukes og NAPTR-spørring i trinn 1 gir resultater.

```
<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>
```

Dette resulterer i følgende trinn på protokollnivået.

```
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
```

Som et resultat skjer SIP-registreringen over TCP ved bruk av port 5061 (mottatt i SRV-trinnet) og mot IP-adressen 1.2.3.4.

Eksempel 2: **Bruker parameter for domeneoverstyring i konfigurasjonsfilen**

Følgende er et annet eksempel på en konfigurasjon som bruker SIP-proxy-oppdagelse der SIP-domenet er forskjellig fra proxy-domenet, og kun SIP over UDP brukes og NAPTR-spørringen ikke returnerer resultater.

```
<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>
```

Dette resulterer i følgende trinn på protokollnivå.

```
1. NAPTR query for record-domain.com, no answer.
2. SRV query for _sip._tcp.override-domain.com (from configuration file), answer
```


Konfidensiell Cisco

```
_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
```

Som et resultat skjer SIP-registreringen over UDP ved hjelp av port 5061 (mottatt i SRV-trinnet) og mot IP-adressen 4.3.2.1.

Eksempel 3: **Bruke SRV-prioriteringer**

Følgende er et annet eksempel på en konfigurasjon som bruker SIP proxy-oppdagelse når bare SIP over TCP brukes og NAPTR-spørring i trinn 1 returnerer resultater, men flere NAPTR- og SRV-poster med forskjellige prioriteringer mottas. I dette tilfellet er det bare SRV-prioritet som betyr noe i denne utgivelseshendelsen, selv om flere NAPTR-poster med varierende prioriteter også mottas.

```
<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>
```

Dette resulterer i følgende trinn på protokollnivå.

```
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
```

Som et resultat skjer SIP-registreringen over TCP ved hjelp av port 5061 (mottatt i SRV-trinnet) og mot IP-adressen 1.2.3.4 som vil støtte både UDP og TCP.

Eksempel 4: Bruker DNS proxy-oppdagelse med NAPTR når tjenesten ikke samsvarer med tjenestetypen

Følgende er et eksempel på en konfigurasjon som bruker SIP proxy-oppdagelse når SIP over TCP og TLS brukes og NAPTR-spørring i trinn 1 returnerer resultater.

```
<config>
<protocols><sip>
<proxy address="domain.com" port="5060"/>
```


Konfidensiell Cisco

```
<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>
```

Dette resulterer i følgende trinn på protokollnivået.

```
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
```

Som et resultat skjer SIP-registreringen over TCP ved bruk av port 5061 (mottatt i SRV-trinnet) og mot IP-adressen 1.2.3.4.

6.1.7 Foretrukket portbruk for SIP

Det har vært noen tilfeller der en annen programvarepakke har kjørt på samme maskin som klienten, og opptar standard SIP-port. For å konfigurere klienten til å bruke en annen port for SIP, kan parameteren *foretrukket port* brukes. Klienten prøver å bruke den konfigurerte portverdien som er angitt i parameteren *preferred-port* , men hvis den tas, prøver klienten inkrementelt portverdier over den konfigurerte verdien. For eksempel, hvis verdien av *foretrukket-porten* er "6000" og den porten er tatt, prøver klienten 6001, 6002, 6003 og så videre til den finner en ubrukt port. Når en ubrukt port er funnet, bruker den den til sin egen SIP-kommunikasjon.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SOURCE_PORT_WXT%	5060	tall	Spesifiserer foretrukket lokal SIP-port for kommunikasjon. Eksempel: 5060

6.1.8 SIP Failover og Failback

SIP failover og failback følger Ciscos BroadWorks prosedyrer. For dette må mer enn én proxy (vanligvis SBC) konfigureres.

På klientsiden bør proxyen løses til flere IP-adresser. Dette kan oppnås ved enten:

- SIP Proxy Discovery er aktivert og DNS-serveren har NAPTR- og/eller SRV-poster for SBC FQDN (se avsnitt *6.1.6 Dynamisk SIP-proxy-oppdagelse*), ELLER

Konfidensiell Cisco

- SIP-proxyadressen oppgis som en FQDN og den løses til flere IP-adresser (se avsnitt *6.1.1 SIP-serverinnstillinger*).

Operativsystemets DNS-cache brukes for å unngå unødvendig DNS-trafikk. Det er ingen hardkodet grense for maksimalt antall IP-adresser i listen.

Ved pålogging, hvis flere IP-adresser er løst, blir de sortert etter prioritet. Klienten begynner å bruke den første tilgjengelige IP-adressen.

6.1.8.1 SIP-failover

SIP-failover kan utløses av enten en socket-feil, en forespørselstidsavbruddsfeil eller et definitivt feilsvar fra serveren som følger:

- Socketfeil – hvis kontakten mellom klienten og serveren blir ødelagt eller lukket, som ved tap av nettverkstilkobling, reagerer klienten umiddelbart og utløser en failover.
- Tidsavbrudd (for eksempel når SBC henger) – basert på SIP T1:
  - SIP INVITE – hvis INVITE-forespørselen blir tidsavbrutt, registrerer klienten seg til neste tilgjengelige SBC (IP) og prøver INVITE på nytt.
  - En annen SIP-forespørsel – klienten prøver å registrere seg til neste tilgjengelige SBC (IP).
- Definitivt feilsvar mottatt fra server:
  - Følgende SIP-feilsvar fra serveren til et SIP REGISTER utløser en failover:
    - 5xx
    - 6xx
  - Følgende SIP *4xx* -svar på SIP REGISTER forårsaker <u>ikke</u> failover:
    - 401 Uautorisert
    - 403 Forbudt
    - 404 Ikke funnet
    - 407 Proxy-autentisering påkrevd
    - 423 Intervall for kort
  - Dessuten utløser ikke *4xx* -feilsvar på SIP INVITE failover, men *5xx* og *6xx* gjør det.

Når en failover utløses, tar klienten den neste tilgjengelige IP-adressen fra listen. SIP T1-timeren definerer hvor lenge en proxy på listen prøves før den flyttes til neste, vanligvis brukes en 32 sekunders verdi (64*T1). Hvis alle IP-adresser mislykkes, viser klienten en brukergrensesnittfeil for SIP-tilkobling. Hvis et VoIP-anrop pågår når failover oppstår, avsluttes samtalen.

SIP failover-logikken er avhengig av flere konfigurasjonsparametere:

- SIP Failover Timers – SIP-tidtakerne T1, T2 og T4 vises i konfigurasjonsfilen, men det anbefales ikke å endre dem.

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


Konfidensiell Cisco

```
    <T2>4000</T2>
    <T4>5000</T4>
</timers>
```

  - T1 – hvor lang tid, i millisekunder, for en nettverksforsinkelse.
  - T2 – maksimal tid, i millisekunder, før overføring av ikke-inviterte forespørsler og invitasjonssvar på nytt.
  - T4 – den maksimale tiden, i millisekunder, for en melding å forbli i nettverket.
- SIP Proxy Address og SIP Proxy Discovery
  - Se avsnitt *6.1.1 SIP-serverinnstillinger*.
  - Se avsnitt *6.1.6 Dynamisk SIP-proxy-oppdagelse*.
- Registrer failover-konfigurasjon (se nedenfor)

Ved failover sender Webex applikasjonen SIP REGISTER med to kontakthoder – en for den gamle økten og den andre med den nye enhetsinformasjonen. Kontaktoverskriften for den gamle økten er inkludert for å varsle SBC om å rydde opp i dataene. Denne overskriften inkluderer expires=0 og q=0,5.

Kontaktoverskriften med den nye enhetsinformasjonen har også en q-verdi, som leses fra <*q-value*> -taggen. <*q-value*> tag-verdien brukes til å indikere preferansen eller prioriteringen til en bestemt kontaktadresse. Den varierer fra 0 til 1,0, hvor 1,0 er den høyeste preferansen og 0 er den laveste. Denne taggen har ikke en egendefinert kode for å kontrollere verdien – den er hardkodet til 1.0. Verdien kan justeres manuelt hvis SBC-en som brukes i distribusjonen har omvendt logikk og behandler q=0.0 med maksimal prioritet.

Fra og med Utgivelse 42.11introduseres en ny <*register-failover*> del i konfigurasjonsmalen. Det er en ny konfigurerbar parameter <*registration-cleanup*> lagt til for å kontrollere om applikasjonen skal sende kontakthode for å rydde opp i den gamle enhetsinformasjonen eller ikke. Noen SBC-er rydder opp i den gamle økten umiddelbart ved socket-frakobling, så eksistensen av kontaktoverskriften for den gamle økten er ikke nødvendig. Som standard er registreringsoppryddingslogikken aktivert.

For konsistens blir <*q-value*> taggen også flyttet til den samme <*register-failover*> delen.

Eksempel:

```
<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>
```


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	sant	sann, usann	Kontrollerer opprydding av gammel enhetsinformasjon i tilfelle SIP-failover.

6.1.8.2 SIP-feilback

Hvis klienten er koblet til en proxy som ikke har førsteprioritet, prøver den å koble til IP-en med høyest prioritet igjen. Tidspunktet for tilbakekoblingen er basert på DNS TTL-administrasjonskonfigurasjonen (se avsnitt *6.1.8.4 DNS TTL-administrasjon*). Hvis et anrop pågår når tilbakekoblingstidtakeren er nådd, venter klienten til alle anrop er fullført og utløser feiltilbakekoblingsprosedyren. Merk at dette kun er gyldig for stasjonære klienter siden SIP-tilkoblingen er aktiv kun under en samtale på mobil.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_FAILBACK_ENABLED_WXT%	sant	sann, usann	Aktiverer/deaktiverer SIP failback.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Over 60	SIP-failback-tidsavbruddet i sekunder.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	feil	sann, usann	Legger til en tilfeldig periode [0-10] % av SIP-failbacken.

6.1.8.3 Håndhev IP-versjon

Webex klienten kan konfigureres hvordan du bestiller listen over løste verter gjennom DNS og deretter itererer gjennom dem i tilfelle SIP-failover. I alle modusene respekteres prioritet og vekt.

Støttede konfigurasjoner er:

- dns - bruker alle adressene som returneres av DNS-spørringene
- ipv4 – filtrerer ut IPv6-adressene
- ipv6 – filtrerer ut IPv4-adressene
- prefer-ipv4 – bestiller IPv4-adressene før IPv6 (utgivelse 42.9)
- prefer-ipv6 – bestiller IPv6-adressene før IPv4 (utgivelse 42.9)
- nat64 – ignorerer IPv6-adressene, bestiller IPv4-adressene (versjon 44.2)

Standardverdien (dns) anbefales brukt, med mindre miljø/nettverkskonfigurasjon krever en annen modus.

Med «dns»-konfigurasjonen prioriteres IPv4-adressene fremfor IPv6 for gitt vert. Hvis det finnes to verter med både IPv4- og IPv6-adresser, vil bestillingen være IPv4(vert1), IPv6(vert1), IPv4(vert2), IPv6(vert2).

I «prefer-ipv4»-modus blir IPv4-adressene bestilt før IPv6-adressene (rekkefølgen innenfor IPv4- og IPv6-gruppene forblir)

Konfidensiell Cisco

Eksempel: IPv4(vert1), IPv4(vert2), IPv6(vert1), IPv6(vert2).

Med «prefer-ipv6»-modus er rekkefølgen motsatt – IPv6-adressene plasseres før IPv4-adressene

Eksempel: IPv6(vert1), IPv6(vert2), IPv4(vert1), IPv4(vert2).

Med «nat64»-modus ignoreres IPv6-adressene, IPv4-rekkefølgen respekteres. IPv6-prefikset(e) er oppdaget. For hver IPv4-adresse opprettes en kombinasjon med hvert Pref64-prefiks og/eller suffiks.

Eksempel: Pref64(1)::IPv4(vert1), Pref64(2)::IPv4(vert1)::Suff64(2), IPv4(vert1)::Suff64(3), Pref64(1)::IPv4(vert2), Pref64(2)::IPv4(vert2)::Suff64(2), IPv4(vert2)::Suff64(3).

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	DNS	ipv4 ipv6 DNS foretrekker-ipv4 foretrekker-ipv6 nat64	Styrer rekkefølgen på IPv4-/IPv6-adresser som brukes av Webex klienten for å koble til SIP-økten.

6.1.8.4 DNS TTL-administrasjon

En egen konfigurasjonsparameter er lagt til for å administrere måten DNS-løsning gjøres på igjen når TTL-en til DNS-posten til serveren som brukes for øyeblikket, utløper. Parameteren i følgende tabell, når den er aktivert, tvinger klienten til å gjøre om DNS-operasjoner når TTL-en til DNS-SRV-en eller A-posten til serveren som brukes for øyeblikket, utløper.

Etter at DNS-løsningen er gjort på nytt, tvinger denne parameteren også klienten til å koble til den mottatte topprioritetsserveren på nytt hvis den er forskjellig fra serveren som brukes for øyeblikket, selv i tilfelle den gjeldende tilkoblingen fungerer fullt ut. Gjenoppkobling gjøres imidlertid først etter at pågående samtaler er avsluttet.

Hvis TTL-ene for server A og SRV-poster er forskjellige, velges den minste verdien.

Når denne parameteren er deaktivert, gjøres ikke DNS-operasjoner på nytt når TTL utløper, men snarere hvert 15. minutt.

Denne parameteren fungerer kun for SIP.

Merk at DNS TTL-administrasjonsfunksjonen ikke kan brukes når en IP-adresse brukes i proxy-adresseparameteren.

Konfidensiell Cisco

MERK: Dette er en funksjon som kun er for skrivebordet, siden mobilklientene kun har SIP-tilkobling under en samtale.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_REFRESH_ON_TTL_WXT%	feil	usann	Når satt til "false", er DNS TTL-administrasjon deaktivert for SIP. Når satt til «sann», er DNS TTL-administrasjon aktivert for SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	feil	usann	Hvis aktivert, legger du til en tilfeldig periode mellom 0-10 % til DNS TTL.

MERK: Det anbefales på det sterkeste å aktivere DNS TTL tilfeldig faktor for å forhindre topper av forespørsler til DNS og potensielt topper av gjentilkoblingsforsøk til applikasjonsserveren.

6.1.9 SIP ABONNER og REGISTRER Oppdater og ABONNER Prøv på nytt

Communicator støtter konfigurering av oppdateringsintervallene for SIP Abonner og REGISTER. For SIP SUBSCRIBE er det en egen parameter for oppdateringsintervallet (i sekunder) og hvor lenge klienten venter før den prøver SIP SUBSCRIBE på nytt hvis det er feil (i sekunder). Den anbefalte maksimale verdien for *abonnement-gjenforsøk-intervallet* er 2000000 sekunder, mens enhver negativ, 0 eller tom verdi resulterer i at 1800 sekunder brukes. Enhver negativ verdi i for oppdatering av abonnement utelater *Utløper* -overskriften og skaper dermed et engangsabonnement.

SIP REGISTER-oppdateringstimeren foreslått av klienten kan konfigureres på sekunder, men i henhold til SIP-spesifikasjonene kan serveren overstyre verdien. For øyeblikket husker klienten verdien foreslått av serveren for påfølgende oppdateringer i stedet for alltid å bruke den konfigurerte verdien.

Til slutt kan utløpsverdien for SIP-økter (for SIP INVITE og SUBSCRIBE) også konfigureres (i sekunder).

```
<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>
```


Konfidensiell Cisco

6.1.10 Bruk P-tilknyttede URI-er i REGISTER

Følgende parameter brukes når du registrerer og håndterer det relaterte *200 OK* -svaret.

Hvis parameteren er satt til «false», bruker ikke klienten *P-Associated-URI* og bruker i stedet identiteten fra sin egen SIP URI.

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

Hvis parameteren er satt til «true», tar klienten sin egen identitet fra den siste *P-Associated-URI* -overskriften for alle utgående SIP-forespørsler (INVITE, SUBSCRIBE, CANCEL, INFO og REFER) fra *200 OK* -svaret i REGISTER. I tillegg vises ikke disse URI-ene som kontakter i kontaktlisten.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_ALTERNATIVE_IDENTITIES_WXT%	feil	sann, usann	Muliggjør bruk av alternative identiteter i SIP REGISTER. Hvis satt til «true», tar klienten sin egen identitet fra den siste *P-Associated-URI* -overskriften for utgående SIP-forespørsler. Hvis satt til "false", blir dens egen identitet for utgående SIP-forespørsler hentet fra sin egen SIP URI.

6.1.11 SIP P-Early Media (PEM)-topptekst

SIP *P-Early Media* (PEM)-overskriften kan brukes i for eksempel IMS-miljøer innenfor et tillitsdomene for å tillate nettverket å autorisere flere SIP-tidlige mediedialoger, for eksempel i tilfeller der et annet nettverk tillater alle tidlige medier.

Konfigurasjonsparameteren muliggjør reklame-PEM-støtte i SIP-signalering. Den faktiske tidlige mediehåndteringslogikken er den samme for både PEM- og ikke-PEM-saker, og fungerer på støttede PEM-headerverdier.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_PEM_SUPPORT_WXT%	feil	sann, usann	Sett til «true» for å aktivere PEM-støtte for klientannonsering i SIP-signalering. Satt til «usann» for å deaktivere kundeannonsering av PEM-støtte i SIP-signalisering.

Konfidensiell Cisco

6.1.12 Støtte for SIP-OPPDATERING

SIP UPDATE er nødvendig i for eksempel noen IMS-distribusjoner, i stedet for den alternative re-INVITE. Det lar en klient oppdatere parametere for en økt, for eksempel settet med mediestrømmer og kodekene deres, men har ingen innvirkning på tilstanden til en SIP-dialog.

Typiske brukstilfeller er knyttet til tidlige medier når man for eksempel bruker tilbakeringetone og forhåndsvarsling samtidig.

SIP-OPPDATERING støttes foreløpig kun når den mottas i brukstilfeller før dialog (tidlige medier) og ikke under aktiv dialog, for eksempel for venting/fortsett samtale der re-INVITE fortsatt brukes.

Det er ikke mulig å legge til video til lyd ved å bruke SIP UPDATE (medieendring) i denne utgivelsen. I tillegg støtter ikke klienten full IMS lang samtaleflyt med ressursreservasjon.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	feil	sann, usann	Når satt til "false", er SIP UPDATE-støtte deaktivert. Når den er satt til «sann», aktiveres støtte for SIP-OPPDATERING.

6.1.13 Eldre SIP INFO FIR

Denne klienten støtter den eldre måten å be om videonøkkelbilder via SIP INFO-mediekontrollforespørsel. Det er nødvendig fordi noen av enhetene har problemer med å svare på RTCP-FB FIR og noen ganger kommer ikke RTCP gjennom til eksternt endepunkt, noe som kan føre til ingen video eller enveis video. For mer informasjon, se *RFC 5168*.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	feil	sann, usann	Når den er satt til «usann», deaktiveres SIP INFO FIR-støtte. Når den er satt til «sann», aktiveres SIP INFO FIR-støtte.

6.1.14 SIP rport-administrasjon for NAT-traversering

Klienten kan konfigureres til å bruke SIP-rportmekanismen for NAT-gjennomgang. Merk at det vanligvis ikke kan være den eneste løsningen for NAT-gjennomgang og SBC brukes hovedsakelig til dette formålet. For en beskrivelse av rport-spesifikasjonen, se *RFC 3581*.

Konfidensiell Cisco

Hvis du vil ha mer informasjon om anbefalinger for SIP-port og transportprotokoll når SIP Application Layer Gateways (ALG) brukes i nettverket, kan du se *Webex for Cisco BroadWorks Løsningsveiledning*.

Merk at "rport"-strengen alltid er til stede i utgående SIP-forespørsler uavhengig av konfigurasjon. Parameteren påvirker kun bruken av IP-adresse og port mottatt fra serveren i SIP-hodene "mottatt" og "rport". Når funksjonen er aktivert, brukes verdiene fra "mottatt" og "rport"-overskrifter i SIP-kontakthodet til SIP-forespørsler (selv når "mottatt"-overskriften mangler i REGISTER-svaret).

Parameteren *Preferred-port* er relatert ved at den ellers definerer porten som brukes i SIP-kontaktoverskriften. Hvis du vil ha mer informasjon om tildeling av SIP-port, kan du se avsnitt *6.1.7 Foretrukket portbruk for SIP*.

Det er en egen konfigurasjonsparameter *bruk-lokal-port* som tvinger den lokale porten til klientsocket til å angis i *Kontakt* -overskriften. Dette brukes for noen SBC-er som oppdager at klienten har en ekte IP (fra *Contact* -overskriften) og SBC-en prøver å etablere en separat socket til klienten for sine forespørsler. I de fleste tilfeller sitter en brannmur mellom SBC og klienten, og den nekter innkommende tilkoblinger til klienten.

> merk: I IPv6-miljøer er alle adressene virkelige, og SBC prøver å opprette en tilkobling til lytteklientadressen (fra *Contact* -toppteksten).

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_USE_RPORT_WXT%	feil	sann, usann	Aktiverer rport for lyd- og videosamtaler.
%RPORT_USE_LOCAL_PORT_WXT%	feil	sann, usann	Kontrollerer om den lokale porten til klientens socket skal legges til i SIP *Contact* -overskriften.

6.1.15 SIP-økt-ID

Når aktivert, ved første registrering, genereres en lokal økt-ID. Økt-ID-en brukes i løpet av levetiden til tilkoblingen/økten for den enheten, for alle dialogbokser som ikke er anropt, REGISTRER, ABONNER, VARSEL, og så videre. Samme økt-ID brukes til bindingen er tapt. Når registreringsbindingen går tapt (DNS-oppslag, tilbakestilling av tilkobling, tilbakestilling av telefon og så videre), genereres en ny lokal økt-ID.

Verdien av økt-ID-en kan brukes til å finne hele settet med dialogbokser knyttet til den enheten.

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


Konfidensiell Cisco

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIP_SESSION_ID_WXT%	feil	sann, usann	Styrer bruken av SIP-sesjons-IDen.

6.1.16 Avvisning av innkommende anrop

Kunden tilbyr fleksibiliteten til å avvise et anrop med *486* eller *603*.

Vær oppmerksom på at hvis klienten er konfigurert til å avvise et anrop med *603 Decline*, kan det hende at tjenestene Viderekobling opptatt og Viderekobling ikke fungerer som forventet.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_REJECT_WITH_486_WXT%	sant	sann, usann	Kontrollerer SIP-feilkoden og årsaken som brukes til å avvise innkommende SIP-anrop. Hvis aktivert, brukes *486 midlertidig utilgjengelig* . Ellers brukes *603 Decline* .

6.1.17 Portområde for transportprotokoll i sanntid

Klienten kan konfigureres til å bruke et definert portområde for Real-Time Transport Protocol (RTP)-strømmer, som også gjelder for SRTP. Denne konfigurasjonen gjøres ved å angi grenseverdiene for portområde for både lyd- og videostrømmer med taggene vist i følgende eksempel.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	tall	Start av lydportområdet.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	tall	Slutt på lydportområdet.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	tall	Start av videoportområdet.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	tall	Slutt på videoportområdet.

MERK: Portområder bør settes slik at de aldri overlapper hverandre.

6.1.18 ICE-støtte (Webex Calling kun)

Klienten støtter Interactive Connectivity Establishment (ICE)-forhandling som muliggjør mediebaneoptimalisering mellom endepunkter (på en peer-to-peer-måte). Dette gjøres for å redusere dataforsinkelse, redusere pakketap og redusere driftskostnadene ved å distribuere applikasjonen.

Merk at gjeldende implementering støtter STUN-server, mens TURN ikke støttes.

Når ICE-støtte er aktivert, vil re-keying for SRTP alltid utføres (se avsnitt *6.1.2 SIP over TLS og sikker transportprotokoll i sanntid*).

Fra og med Release 44.5, Webex legger appen til støtte for ICE over IPv6 ved hjelp av NAT64.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_RTP_ICE_WXT%	feil	sann, usann	Aktiver / deaktiver ICE-støtte.
%RTP_ICE_MODE_WXT%	icestun	icestun	ICE-støttemodus. For øyeblikket er den eneste støttede verdien "icestun".
%RTP_ICE_SERVICE_URI_WXT%	(tom)	gyldig STUN-server-URI eller (tom)	STUN server URI.
%RTP_ICE_PORT_WXT%	3478	Nummer (0-65535)	STUN-serverport.
%ENABLE_RTP_ICE_IPV6_WXT%	feil	sann, usann	Aktiverer ICE over IPv6.

Konfidensiell Cisco

6.1.19 RTCP MUX

RTCP MUX er konfigurerbar. Denne funksjonen gjør at klienten bruker samme port for RTP og RTCP. I SIP/SDP-signaleringsnivå legges linjen a=rtcp-mux til SDP. I tillegg er forskjellige moduser mulige:

- Bakoverkompatibilitetsmodus (det vil si at linjen a=rtcp-mux ikke vises i SDP)
- Multipleksmodus (a=rtcp-mux-linjen vil vises to ganger i SDP:en: én gang i m=lydseksjonen, og en gang til i m=videoseksjonen)

Video og lyd bruker ikke samme port.

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

Merk at RTCP MUX ikke kan brukes med SRTP-anrop.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_RTCP_MUX_WXT%	sant	sann, usann	For å aktivere RTPC MUX, sett til "true". For å deaktivere RTCP MUX, sett til "false".

6.1.20 Overfør

Webex For CiscoBroadWorks -klienten støtter overvåket (rådgivende), semi-rådgivende og direkte (blind) samtaleoverføring.

Semikonsultativ anropsoverføring lar den som ringer fullføre overføringen før anropet blir tatt opp av den eksterne anroperen. Den semi-konsultative fullføringsknappen er aktivert for den som ringer først etter at ringingen er startet på anropssiden og den tilsvarende SIP-varslingen (*180 Ringing*) er mottatt på den som ringer. Blind overføring kalles "Overfør nå" i brukergrensesnittet.

> merk: SIP *180-ringing* kan ikke utløses i noen miljøer, for noen tall eller i noen kommunikasjonsscenarier på tvers av servere.

Utgivelse 43.9 av Webex appen introduserer overføring til en annen frittstående pågående samtale av samme type. Anrop som avsluttes i Webex appen kan overføres til andre anrop som avsluttes på det lokale endepunktet. Og samtaler som avsluttes på en ekstern enhet kan overføres til samtaler som avsluttes på et eksternt endepunkt. Denne funksjonen har ikke konfigurerbare alternativer.

Fra og med Release 43.12, Webex legger appen til konfigurasjonsalternativet for å kontrollere om den gjeldende samtalen skal settes på vent automatisk når Overfør-menyelementet er valgt. Denne oppførselen kontrolleres av det nye *auto-hold* -attributtet. Som standard er automatisk hold deaktivert.

```
<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%"/>
```


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_TRANSFER_CALLS_WXT%	feil	sann, usann	Når satt til "true", er samtaleoverføring aktivert. Når den er satt til «usann», deaktiveres samtaleoverføring.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	feil	sann, usann	Aktiverer overføringsalternativ(er) for eksterne (XSI)-anrop som avsluttes på et annet sted.
%TRANSFER_CALL_TYPE_WXT%	full	snakk-først, blind, full	Angir overføringstypene som er tilgjengelige for brukeren i BroadWorks konfigurasjonen.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	feil	sann, usann	Kontrollerer om den aktive samtalen skal settes på vent automatisk når brukeren velger alternativet Overfør fra menyen på skjermbildet for samtale.

6.1.21 N-Way-konferansesamtaler og deltakere

Følgende egendefinerte kode kan brukes til å kontrollere tilgjengeligheten til Ad Hoc-konferansesamtalen (N-Way) via SIP i Webex for CiscoBroadWorks -klienten. I tillegg kan N-veiseier se hele deltakerlisten via SIP ABONNEM/MELDE og konferansearrangementspakke. Eierens klient lærer seg URIen som skal sendes SIP SUBSCRIBE til via forrige SIP *Contact* -overskrift i *200 OK* -meldingen som ble sendt som svar på INVITET til konferanse-URI, mens for deltakerne den samme informasjonen er i en foregående anropsinfo NOTIFY.

Ciscos BroadWorks systeminnstilling (*maxConferenceParties)* brukes til å angi maksimalt antall konferanseparter. For et gitt anrop angir det antall aktive samtidige parter en bruker kan ha eller legge til gjennom kontrollalternativet «Legg til deltakere» midt i samtalen eller gjennom Cisco BroadWorks N-veis Calling-funksjonen.

Denne informasjonen hentes fra Application Server (AS) ved hjelp av følgende kommandolinjegrensesnitt (CLI).

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

Example output:
maxConferenceParties = 6
conferenceURI =
```

Når verdien for *maxConferenceParties* er oppnådd, (som har et område på 4 til 15), bør %MAX_CONF_PARTIES_WXT% taggen angis tilsvarende.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CONFERENCE_CALLS_WXT%	feil	sann, usann	Kontrollerer om konferansealternativet skal aktiveres for brukeren.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	feil	sann, usann	Sett til "true" for å aktivere N-veis eier deltakerliste. Satt til «usann» for å deaktivere deltakerlisten over eiere av N-way.
%MAX_CONF_PARTIES_WXT%	10	Tall mellom 4 og 15 (tom)	Angir det maksimale antallet N-veis deltaker, håndhevet av klienten, for eksempel 10. Serversiden har sine egne grenser. Tom verdi deaktiverer håndheving av N-veis deltakergrense på klientsiden.

6.1.22 Anropstrekk

Samtalepull-funksjonen kan aktiveres ved hjelp av en enkelt konfigurasjonsparameter, som vist i eksemplet nedenfor.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_PULL_WXT%	feil	sann, usann	Aktiverer Call Pull.

6.1.23 Samtaleparkering/hent

Gruppeanropsparkeringsfunksjonen lar pågående VoIP-anrop overføres til en samtaleparkeringsserver, som lar innringeren gjøre noe annet og hentes av samme bruker eller en annen bruker. En pågående samtale vil bli parkert mot det første tilgjengelige internnummeret i samtaleparkeringsgruppen.

Anropshenting kan utføres ved at brukeren parkerer anropet i dialogboksen i et konfigurerbart antall sekunder umiddelbart etter at anropet har parkert. Eller den parkerte samtalen kan hentes av brukeren eller en annen bruker ved å velge alternativet for henting av anrop og taste inn nummeret eller internnummeret.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_PARK_WXT%	feil	sann, usann	Aktiverer samtaleparkering/henting.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Tall mellom 5 og 30	Angir antall sekunder den vellykkede samtaleparkerte dialogboksen er synlig for brukeren før den lukkes automatisk.

6.1.24 Samtalestatistikker

Rapportering av sluttstatistikk i SIP (Session Initiation Protocol) BYE-melding gjør det mulig å sende samtalestatistikk til en ekstern slutt når en samtale avsluttes. Anropsstatistikken sendes som en ny overskrift i SIP BYE-meldingen eller i det tilsvarende *200 OK* -svaret på BYE-meldingen. Statistikken inkluderer Real-time Transport Protocol (RTP)-pakker sendt eller mottatt, totale byte sendt eller mottatt, totalt antall pakker som går tapt, forsinkelsesjitter, tur-retur-forsinkelse og samtalevarighet.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_STATISTICS_WXT%	feil	sann, usann	Sett til «true» for å aktivere innhenting av anropsverdier. Satt til «usann» for å deaktivere registrering av anropsmåledata.

6.1.25 Automatisk gjenoppretting av anrop / sømløs overføring av anrop

Klienten har støtte for automatisk gjenoppretting av anrop ved å bytte nettverk mens brukeren har en pågående VoIP-samtale. Automatisk gjenoppretting av anrop fungerer i begge retninger – Mobildata-til-WiFi og WiFi-til-mobildata, så vel som når du bytter mellom WiFi-nettverk. Samtalen forsøkes gjenopprettet innen ett minutts tidsramme og stopper deretter. Hvis det er mer enn én pågående VoIP-anrop, blir bare den aktive gjenopprettet.

I mobildata-til-WiFi-overgang vil klienten beholde de pågående VoIP-samtalene på mobildata til terminert eller mobildatanettverk går tapt.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	feil	sann, usann	Kontrollerer om mekanismen for automatisk gjenoppretting skal aktiveres for brukeren.

Konfidensiell Cisco

6.1.26 Anropsopptak

Anropsopptaksfunksjonen støttes av klienten og avhenger av tilgjengeligheten på serversiden av funksjonen, samt konfigurasjonsalternativer. Funksjonen avhenger av aktivert XSI-hendelseskanal (se avsnitt *6.1.33 XSI-hendelseskanal*) og programserveren (AS) som er konfigurert til å sende *X-BroadWorks-Correlation-Info* SIP-topptekst (se *Webex for BroadWorks Cisco Solution Guide*).

Hvis funksjonen er deaktivert, er det ingen opptaksknapper og alternativer for brukeren. Vær oppmerksom på at samtaleopptak foregår per bruker, ikke per samtale-basis – det betyr at hvis en av deltakerne i en samtale støtter samtaleopptak, kan samtalen tas opp.

Hvis samtaleopptaksfunksjonen er aktivert, er det alltid en visuell indikasjon når samtalen tas opp. Følgende samtaleopptaksmoduser støttes av Cisco BroadWorks:

Alltid

- Samtaleopptak vil startes automatisk ved samtaletablering.
- Brukeren er **IKKE** i stand til å stoppe/pause samtaleopptaket.

Alltid med støtte på pause/gjenoppta

- Samtaleopptak startes automatisk ved samtaleetablering, men brukeren vil kunne stanse og gjenoppta samtalen.
- Mulige brukerinteraksjoner:
  - Opptak pågår – **Sett på pause** Opptakshandling.
  - Opptaket er på pause – **Gjenoppta** opptakshandlingen.

Behovsbasert

- Etter at samtalen er opprettet, starter samtaleopptaket på serveren.
- Hvis brukeren trykker på Start opptak-alternativet under samtalen, vil samtaleopptaket lagres og samtalen beholdes fra oppstart. Ellers, hvis ingen startopptak startes fra brukeren, vil samtaleopptaket bli slettet på serveren.
- Mulige brukerinteraksjoner:
  - Ingen opptak har startet ennå – **Start** opptakshandling.
  - Opptak pågår – **Sett på pause** Opptakshandling.
  - Opptaket er på pause – **Gjenoppta** opptakshandlingen.

På forespørsel med brukerinitiert start

- Brukeren kan starte, stoppe, pause og gjenoppta samtaleopptak når som helst, flere ganger under en samtale.
- Det vil være separate samtaleopptak for hver oppstart av samtaleopptak.
- Mulige brukerinteraksjoner:
  - Ingen opptak har startet ennå – **Start** opptakshandling.

Konfidensiell Cisco

- Opptak pågår – **Stopp** og **Pause** opptak.
- Opptaket er på pause – **Stopp** og **Gjenoppta** opptakshandlingen.

Anropsopptaksmodusen som er tildelt brukeren, kan velges fra kontrollhuben.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_RECORDING_WXT%	feil	sann, usann	Aktiverer samtaleopptakskontroller.

6.1.27 Talepost, visuell talepost, indikator for melding venter

Følgende egendefinerte tagger kan brukes til å kontrollere tilgjengeligheten til Cisco BroadWorks talepost og visuell talepost i Webex for CiscoBroadWorks -klienten. Vær oppmerksom på at en Cisco BroadWorks systemkode (%BWVOICE-PORTAL-NUMBER-1%) brukes med talepost.

Visual Voicemail (VVM) støttes kun for lyd. Støttede formater er wav, ulaw og mov som inneholder H264-video (spilles kun som lyd). Den lar brukere se innkommende talemeldinger i en listevisning og individuelle elementer kan spilles av. Denne funksjonen er basert på Xsi, men varsler om ny talepost leveres over SIP; derfor må SIP være aktivert for at varslene skal fungere. I tillegg er SIP SUBSCRIBE for Message Waiting Indicator (MWI) konfigurasjon nødvendig for at varslene skal komme, og MWI må være aktivert for at Visual Voicemail skal fungere. For mer informasjon om SIP-konfigurasjon, se avsnitt *6.1.1 SIP-serverinnstillinger*.

For Ciscos BroadWorks utgivelses- og oppdateringskrav for visuell talepost, se *Webex for Cisco BroadWorks løsningsveiledning*.

Visuell talepost må aktiveres separat i konfigurasjonen.

Følgende innstillinger er nødvendige på CommPilot-portalen for å ha visuell talepost:

- Talemeldinger aktivert
- "Når melding kommer, bruk enhetlig melding"-alternativet aktivert
- Alternativet "Bruk venteindikator for telefonmelding" er aktivert

Hvis ikke tjenesten for visuell talepost er tilordnet på Ciscos BroadWorks side for brukeren, deaktiveres konfigurasjonen for tjenesten automatisk.

Merk at deaktivering av SIP-registrering også deaktiverer MWI for nye taleposter. Se tabellen som følger for mer informasjon om aktivering av MWI.

For å vise informasjon om talepostmeldinger i brukergrensesnittet, må klienten motta SIP MWI-varsler fra serveren (det vil si taleposthendelsespakken). Se tabellen som følger for abonnementsalternativer. Merk også at MWI er nødvendig for at Visual Voicemail-varsler skal fungere.

Konfidensiell Cisco

Merk at hvis SIP-abonnement på taleposthendelsespakke mislykkes, fortsetter klienten å prøve på nytt når den er konfigurert til å gjøre det. For mer informasjon om konfigurasjon av SIP-ABONNER på nytt, se avsnitt *6.1.9 SIP ABONNER og REGISTRER Oppdater og ABONNER Prøv på* nytt.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_VOICE_MAIL_WXT%	feil	sann, usann	Sett til «true» for å aktivere støtte for talepost. Sett til «false» for å deaktivere støtte for talepost.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	feil	sann, usann	Når satt til «usann», er VVM deaktivert. Når satt til «sann», er VVM aktivert. Merk at talepost enabled=false før det faktiske VVM-attributtet fortsatt brukes for bakoverkompatibilitet.
%BWVOICE-PORTAL-NUMBER-1%	tomt	tall	Klienten ringer dette nummeret som vanligvis er angitt ved hjelp av en eksisterende Cisco BroadWorks systemkode ved oppringing av talepost.
%ENABLE_MWI_WXT%	feil	sann, usann	Sett til "true" for å aktivere MWI. Sett til "false" for å deaktivere MWI.
%MWI_MODE_WXT%	tomt	implisitt, eksplisitt	Sett til "eksplisitt" for å sende SIP SUBSCRIBE for MWI-hendelsespakke når MWI er aktivert. Bruk av "implisitt" sender ikke et SIP-ABONNEMENT på MWI-hendelsespakke når MWI er aktivert. Hvis den står tom, er MWI deaktivert.

6.1.28 Utskrift av talepost for Webex Calling

Med denne funksjonen konverteres talepostmeldinger til tekst og vises i den visuelle talepostmeldingsvisningen i Webex Calling skrivebords- og mobilappene.

Funksjonen skal bare aktiveres for en bruker hvis:

1. Appen kjører i Webex Calling distribusjon.
2. Visual Voicemail-funksjonen er aktivert for brukeren.
3. Funksjonen er aktivert i konfigurasjonen (det aktiverte attributtet i <services><voice-mail><transcription> taggen bør settes til «true»).

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	feil	sann, usann	[Webex Calling Kun] Kontrollerer tilgjengeligheten av talepostutskrift bare hvis visuell talepost er aktivert.

6.1.29 Samtaleinnstillinger

6.1.29.1 Viderekobling alltid

Følgende egendefinerte kode kan brukes til å kontrollere tilgjengeligheten av Cisco BroadWorks Viderekobling Alltid-tjenesten i Webex for CiscoBroadWorks -klienten.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	feil	sann, usann	Styrer tilgjengeligheten av tjenesten Alltid viderekobling. Funksjonen er deaktivert som standard.

MERK: Viderekobling av anrop alltid og viderekobling til talepost (*6.1.29.2 Viderekobling av anrop* til talepost) kan brukes sammen for å vise eller skjule "Viderekobling"-innstillingen i apper.Webex Når begge taggene er deaktivert, er "Viderekobling"-innstillingen i Webex appene skjult.

6.1.29.2 Viderekobling av anrop til talepost

Fra og med utgivelsen 43.9, Webex gir appen et alternativ for å kontrollere tilgjengeligheten av videresending til talepost. Som standard er funksjonen aktivert, og følgende konfigurasjonsalternativ kan brukes til å deaktivere den.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	sant	sann, usann	Kontrollerer tilgjengeligheten av videresending til talepost. Funksjonen er aktivert som standard.

Konfidensiell Cisco

MERKNAD 1: Denne funksjonen avhenger av en av tjenestene "Voice Messaging User" eller "Third-Party Voice Mail Support" som skal tildeles brukeren.

MERKNAD 2: Viderekobling av anrop til talepost og viderekobling av anrop alltid (*6.1.29.1 Viderekobling alltid*) kan brukes sammen til å vise eller skjule innstillingen for viderekobling av anrop i Webex appene. Når begge taggene er deaktivert, er "Viderekobling"-innstillingen i Webex appene skjult.

6.1.29.3 BroadWorks Anywhere (Single Number Reach)

Følgende egendefinerte koder styrer tilgjengeligheten til BroadWorks Hvor som helst og tilgjengeligheten av innstillingene i Webex for CiscoBroadWorks -klienten. Merk at navnet på denne funksjonen i klienten er *Administrer mine numre*.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_BROADWORKS_ANYWHERE_WXT%	feil	sann, usann	Aktiverer BroadWorks Anywhere (BWA) på konfigurasjonsnivå.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	sant	sann, usann	Kontrollerer om beskrivelsen av BWA-lokasjonen skal være tilgjengelig for brukeren.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	feil	sann, usann	Sett til «true» for å gjøre Alert All Locations for BWA-tjenesten tilgjengelig for brukeren. Sett til «usann» for å gjøre Varsle alle steder for BWA-tjenesten utilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	feil	sann, usann	Kontrollerer om applikasjonen skal aktivere tilstanden Alert All Locations, ved å legge til andre eller hver påfølgende ny BWA-posisjon.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	feil	sann, usann	Kontrollerer om samtalekontrollen for BWA-plasseringen skal være tilgjengelig for brukeren.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	feil	sann, usann	Kontrollerer standardtilstanden til anropskontrollen for BWA-lokasjonen.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	feil	sann, usann	Kontrollerer om omdirigeringsinhibitoren for BWA-plasseringen skal være tilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	feil	sann, usann	Kontrollerer standardtilstanden til omdirigeringsinhibitoren for BWA-plasseringen.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	feil	sann, usann	Kontrollerer om svarbekreftelsen av BWA-plasseringen skal være tilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	feil	sann, usann	Kontrollerer standardtilstanden til svarbekreftelsen for BWA-plasseringen.

6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger

Klienten Webex for Cisco BroadWorks gir tilgang til en portal for innstillinger (Self Care) der brukeren kan konfigurere noen av program- og tjenesteinnstillingene.

Videre gir klienten muligheten til å bruke Samtaleinnstillinger Web View (CSWV) i stedet. Det lar brukeren kontrollere flere av de serverbaserte samtaleinnstillingene. Separate tagger kan brukes til å kontrollere om spesifikke tjenester skal være synlige i de nettbaserte anropsinnstillingene.

> merk: Det anbefales å skjule innstillingene som allerede er synlige i programmet, for eksempel Call Center (se avsnitt *6.1.31 Pålogging/utlogging av telefonsenter / samtalekø*) og BroadWorks Anywhere (se avsnitt *6.1.29.3 BroadWorks Anywhere*). Remote Office-tjenesten anbefales også å skjules fordi den har blitt etterfulgt av BroadWorks Hvor som helst-tjenesten.

Følgende egendefinerte tag kan brukes til å konfigurere URL-en for innstillingsportalen (Self Care eller CSWV). Hvis taggen er tom, er ikke lenken til innstillingsportalen synlig for brukeren i applikasjonen.

```
<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%"/>
```


Konfidensiell Cisco

```
   <service name="Anonymous Call Rejection"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="Simultaneous Ring Personal"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <service name="Sequential Ring"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <service name="Automatic Callback"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <service name="Call Waiting" visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Calling Line ID Delivery Blocking"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <service name="Personal Assistant"
visible="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
   <service name="Call Center - Standard"
visible="%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%"/>
   <service name="BroadWorks Anywhere"
visible="%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%"/>
   <service name="BroadWorks Mobility"
visible="%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <service name="Remote Office" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Voice Messaging User"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
</web-call-settings>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%WEB_CALL_SETTINGS_TARGET_WXT%	eksternt	ekstern, csw	Styrer administrasjonsportalmodusen. Sett til "ekstern" for å åpne konfigurert innstillingsportal-URL i en ekstern nettleser. Sett til "csw" for å åpne CSW-portalen i en innebygd nettleser ved å bruke delen for ekstra parametere <services><web-call-settings> for å danne POST-forespørselen.
%WEB_CALL_SETTINGS_URL_WXT%	tomt	URL-streng	URL for innstillingsportalen. Eksempel: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Alltid viderekobling skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Ikke forstyrr (DND) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Anonymt anropsavvisning (ACR) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Viderekobling opptatt (CFB) skal være synlig for brukeren i de nettbaserte innstillingene.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Viderekobling ikke kan nås (CFNR) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Viderekobling uten svar (CFNA) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Personlig samtidig ringing (SIMRING) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Sekvensiell ring (SEQRING) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Remote Office (RO) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Automatisk tilbakeringing (ACB) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Samtale venter (CW) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet Calling Line ID Delivery Blocking (CLIDB) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Personlig assistent (PA) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativet BroadWorks Hvor som helst (BWA) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Call Center skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet BroadWorks Mobility (BWM) skal være synlig for brukeren i de nettbaserte innstillingene. For øyeblikket er den anbefalte verdien «usann» på grunn av interoperabilitetsproblemer mellom Webex for Cisco BroadWorks og BroadWorks Mobility.
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	sant	sann, usann	Styrer om alternativet Voice Management (VM) skal være synlig for brukeren i de nettbaserte innstillingene.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	feil	sann, usann	Styrer om det nye Samtaleinnstillinger WebView-merkevaren skal brukes. Aktiver hvis CSWV-versjonen på serversiden er 1.8.6 eller nyere. Ellers hold det falskt.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	sant	sann, usann	Kontrollerer om alternativer for e-post/talepostmeldinger er synlige i de nettbaserte innstillingene.
%USER_PORTAL_SETTINGS_URL_WXT%	tomt	URL-streng	Angir URL-en til brukerinnstillingsportalen. For å aktivere funksjonen og presentere Access User Portal-knappen i brukergrensesnittet, skal denne egendefinerte taggen ikke være tom. For eksempel: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	eksternt	utvendig, intern	Angir om URL-en skal åpnes i en innebygd eller ekstern nettleser.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	feil	sann, usann	Gjelder bare når den innebygde nettleseren er konfigurert (USER_PORTAL_SETTINGS_TARGET_WXT=internt). Når dette alternativet er aktivert, brukes HTTP POST-forespørsel, og BroadWorks kortvarig token legges til som en del av BRØDTEKSTEN. Når den er deaktivert, åpnes URL-en med HTTP GET.

MERKNAD 1: Anropsinnstillinger WebView URL skal alltid ha en etterfølgende "/" konfigurert. For eksempel: http(s)://<XSP-FQDN>/<CSW-Context-Path>/

MERK 2: Minimumsversjonen for Call Settings WebView-applikasjonen som støttes er 1.7.5.

For installasjon på Cisco BroadWorks versjon 21.0, se tilleggstrinnene som er beskrevet i *Webex For Cisco BroadWorks Solution Guide*.

6.1.31 Pålogging/utlogging av telefonsenter / samtalekø

Webex -appen gir tilgang til agentinnstillingene for Call Center (Call Queue). Hvis en bruker er klargjort for Call Center, lar denne funksjonen brukeren logge på et kundesenter og se de tilgjengelige samtalekøene, samt bli med/oppheve køer og angi status for automatisk samtalefordeling (ACD).

Fra og med skrivebordsutgivelsen 42.8 og mobilutgivelsen42.12 er ikke Call Center-agenten lenger basert på nettvisningen for samtaleinnstillinger (se avsnitt *6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*). Agentkonfigurasjonen for Call Center (Call Queue) er tilgjengelig via bunnteksten på skrivebordet og innstillingene for mobilappen Webex .

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_CENTER_WXT%	feil	sann, usann	Aktiverer kundesenterstøtte.

6.1.32 XSI-rot og -stier

Webex For CiscoBroadWorks -klienten bruker følgende koder til å kontrollere banen for XSI Root, Actions og Events hvis de må konfigureres til å være forskjellige fra de som brukes til pålogging.

Hovedgrunnen til å endre XSI Root er å implementere lastbalansering på konfigurasjonsnivå, selv om det anbefales å bruke lastbalansering på HTTP-laget i stedet.

Event- og handlingsbanene endres vanligvis på grunn av merkevarekrav for å fjerne *com.broadsoft* -domenereferansen fra URL-banene til XSI HTTP-forespørslene utført av klienten.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%XSI_ROOT_WXT%	Fortsetter å bruke den originale som ble brukt til konfigurasjonshenting.	URL-streng	XSI-roten for alle XSI-operasjoner. Eksempel: https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	streng	Spesifiserer XSI Actions-banen. Den skal begynne og slutte med "/" og kun inneholde handlingskonteksten. Eksempel: /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	streng	Angir banen for XSI-hendelser. Den skal starte og slutte med «/» og inneholde bare hendelseskonteksten. Eksempel: /com.domain.xsi-events/

6.1.33 XSI-hendelseskanal

XSI Event-kanalen brukes til ulike tjenester som:

- XSI-kontroller midt i samtalen
- Statusvarsler for samtaleinnstillinger
- Anropsopptak

Konfidensiell Cisco

XSI Events-hjerteslag brukes til å holde XSI Event-kanalen åpen, og hjerteslagintervallet kan spesifiseres ved hjelp av følgende parameter.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_XSI_EVENT_CHANNEL_WXT%	sant	sann, usann	Kontrollerer om XSI Event-kanalen er aktivert. Den bør settes til "true" for å motta for eksempel tjenesterelaterte hendelser for kontrolltjeneste midt i samtalen. Den anbefalte verdien er "true".
%CHANNEL_HEARTBEAT_WXT%	10000	tall	Dette er XSI Event-kanalens hjerteslag (i millisekunder). Standard er "10000".

6.1.34 Konfigurasjon av kodek

Webex for Cisco BroadWorks tilbyr en rekke lyd- og videokodeker. De respektive listene over kodeker finner du under *config/services/calls/* i delene *audio/codecs* og *video/codecs* . Prioriteten til hver kodek kan endres via *XML-attributtprioriteten*, som er en verdi mellom 0,0 (lavest) og 1,0 (høyest).

Webex Appen støtter offisielt følgende kodeker:

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

Konfidensiell Cisco

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

Klienten støtter H.264 som videokodek. Videooppløsningsattributt kan brukes til å angi en av følgende tilgjengelige verdier: SUBQCIF, QCIF, CIF, 4CIF, VGA og HD.

Hvis bithastigheten ikke er angitt i konfigurasjonen, brukes standard bithastighetsverdier. Standard bithastighetsverdier, per oppløsning og bildefrekvens, er oppført i følgende tabell.

Oppløsning	Videostørrelse *	FPS (rammer per sekund)	Standard bithastighetsverdier per oppløsning og 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

***** Maksimal annonsert videooppløsning. Den faktiske videooppløsningen under en samtale mellom to Webex for CiscoBroadWorks -klienter avhenger av kapasiteten til begge klientene – den vil være den laveste av de to og vil være den samme for begge klientene.

Videooppløsning for en videosamtale forhandles under øktoppsett og er basert på egenskapene til de to endepunktene. Videoanropsoppløsningen er den samme på begge endepunktene. Det vil si at hvis Webex for CiscoBroadWorks -endepunktene har forskjellige funksjoner (og derfor støtter forskjellige oppløsninger), forhandles den lavere oppløsningen for samtalen. Videooppløsningen kan endres under en samtale hvis nettverksforholdene forverres. I dette tilfellet kan de to mobile endepunktene bruke forskjellige videooppløsninger.

Pakkedannelsesmodusen kan konfigureres til å være SingleNAL (0) eller Non-interleaved (1). Malen bruker SingleNAL som standard (<packet-mode>0</packet-mode>).

Konfidensiell Cisco

Konfigurasjon av telefonhendelser, enkelt eller flere, støttes også. Under kodekforhandling sender klienten alle de konfigurerte kodekene, inkludert telefonhendelser. Etter at lydkodeken er valgt, søker den etter telefonhendelse i tilbudet. Hvis tilbudet har telefonhendelsen med samplingsfrekvensen til den forhandlede lydkodeken, velges denne telefonhendelsen. Ellers brukes den første telefonhendelsen i listen.

Hvis det er minst én telefonhendelse forhandlet, sendes dual-tone multi-frekvensene (DTMF) som RTP-pakker ved å bruke den tilsvarende nyttelasttypen. Og hvis det ikke er noen telefonhendelser forhandlet i det hele tatt, sendes DTMF-ene som RTP-pakker med nyttelasttypen til den forhandlede lydkodeken. Out-of-band-mekanisme for å levere DTMF-er støttes ikke av Webex appen.

Eksempel på konfigurerte kodeker:

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

Hvis en lydkodek med samplingshastighet på 48 kbps forhandles, brukes telefonhendelsen med nyttelast 101.

6.1.35 SIP-URI-oppringing

For øyeblikket er SIP-URI-oppringing gjennom BroadWorks ikke tilgjengelig, og som standard rutes alle SIP-URI-samtaler gjennom Locus, også kjent som «Gratis anrop». I noen miljøer er dette ikke ønskelig og slike samtaler bør blokkeres.

> **MERK**: Dette gjelder bare hvis Locus-anrop er deaktivert. Bare i dette tilfellet vil SIP URI-oppringingsblokkering fungere.

Følgende konfigurasjon gir dette alternativet.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	sant	sann, usann	Kontrollerer om SIP-URI skal rutes gjennom Locus (true) eller blokkert (false).

6.1.36 Samtalehistorikk på alle enheter

Klienten gir muligheten til å lagre og hente anropshistorikken fra serveren i stedet for å lagre den lokalt. På denne måten er anropsloggen enhetlig på tvers av alle enheter.

Konfidensiell Cisco

MERK: Samlet anropshistorikk bør være aktivert samtidig på klient- og serversiden for å unngå manglende anropshistorikk eller dupliserte poster.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	feil	sann, usann	Kontrollerer om applikasjonen skal bruke Unified Call History eller klientsiden (lokal).

6.1.37 Deaktiver videosamtaler

Release 41.9 la til muligheten til å deaktivere videosamtaler. Det finnes separate konfigurasjonsalternativer for å kontrollere denne funksjonen for BroadWorks-støttede og Locus (gratis) VoIP-anrop.

Når funksjonen er aktivert og funksjonskoden er satt til "false":

- brukeren vil ikke se "Godta innkommende anrop med videoen min på"-innstillingen
- alle innkommende videosamtaler hvis de godtas, vil være lydanrop
- brukeren vil ikke kunne eskalere et anrop til video, og videoeskaleringer vil automatisk bli avvist

Når videosamtaler er aktivert, legges en ny konfigurasjonsegenskap til for å kontrollere standardverdien for «Godta innkommende anrop med videoen min på»-innstillingen. Som standard er denne funksjonen slått PÅ for skrivebord og slått AV for mobil og nettbrett.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIP_VIDEOCALLS_WXT%	sant	sann, usann	Kontrollerer tilgjengeligheten av SIP-videosamtaler gjennom BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	sant	sann, usann	Styrer tilgjengeligheten av Locus (gratis) videosamtaler.
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Desktop - sant Mobil / nettbrett - usann	sann, usann	Kontrollerer standardverdien for «Godta innkommende anrop med videoen min på»-innstillingen.

Konfidensiell Cisco

6.1.38 Nødsamtaler (911) – Stedsrapportering med E911-leverandør

Skrivebords- og nettbrettklienten Webex støtter E911-stedsrapportering ved hjelp av RedSky, Intrado eller båndbredde som leverandør av E911-nødanrop for Webex for BroadWorks distribusjon. E911-leverandøren tilbyr posisjonsstøtte per enhet (for apper for Webex stasjonære og nettbrett og HELD-kompatible MPP-enheter) og et nettverk som ruter nødanrop til Public Safety Answering Points (PSAP) rundt i USA, dets territorier (Guam, Puerto Rico og Jomfruøyene) og bare i Canada. Tjenesten er aktivert per sted.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	feil	sann, usann	Aktiverer E911-leverandørens plattform for nødplassering.
%BWE911-PRIMARY-HELDURL%	tomt	streng	Angir URL-adressen til E911-leverandørens plattform for nødplassering som støtter HELD-protokollen.
%BWE911-CUSTOMERID%	tomt	streng	Kunde-ID-en (HeldOrgId, CompanyID) som ble brukt for E911-leverandørens HTTPS-forespørsel.
%BWE911-SECRETKEY%	tomt	streng	Hemmeligheten til å godkjenne E911-leverandørens HTTPS-forespørsel.
%BWE911-EMERGENCY-NUMBER-LIST%	tomt	CSV-streng	Listen over nødnumre som støttes av E911-leverandøren.
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (brukeren vil ikke bli spurt igjen)	nummer [0 - 43200]	Tidsavbruddet i minutter som vil bli brukt til å minne brukeren på å oppdatere nødstedet hvis det gjeldende ikke er angitt eller er ugyldig. Den foreslåtte verdien hvis du bestemmer deg for å aktivere: 1440 (en dag).
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (brukeren kan avbryte dialogen alltid)	nummer [-1 - 100]	Tidspunktene da brukeren har tillatelse til å lukke stedsdialogen før plasseringen blir obligatorisk (det vil si at brukeren ikke kan lukke stedsvinduet). Mulige verdier: ▪ N = -1 (brukeren kan alltid avbryte dialogen) ▪ N = 0 (brukeren har ikke lov til å avbryte dialogen - obligatorisk plassering alltid) ▪ N > 0 (brukeren har lov til å avbryte dialogen N ganger før den blir obligatorisk)

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	aggressiv, én gang_per_pålogging	én gang_per_pålogging	Definerer virkemåten for bekreftelse av E911-plassering. Den "aggressive" verdien vil vise dialogen til brukeren på hver nettverksendring til en ukjent plassering, mens verdien "once_per_login" vil vise dialogen bare én gang, og forhindrer ytterligere popup og distraksjoner for brukeren.

MERKNAD 1: BWE911-*** koder er "dynamiske innebygde systemkoder". Hvis du vil ha mer informasjon, kan du se avsnitt *5.7 Cisco BroadWorks Dynamic Built-in System* Tags.

MERKNAD 2: Hvis VOIP-anrop er deaktivert, er den eneste betydningsfulle verdien for nødnummersekvens (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) kun cs.

6.1.39 PAI som identitet

For **innkommende anrop** kontrollerer denne nye parameteren prioriteten til SIP From- og P-Asserted-Identity (PAI)-overskrifter, og hva som skal brukes som en anropslinjeidentitet. Hvis det finnes en X-BroadWorks-Remote-Party-Info-topptekst i den innkommende SIP-invitasjonen, brukes den med prioritet over SIP From- og PAI-topptekstene. Hvis det ikke finnes noen X-BroadWorks-Remote-Party-Info-topptekst i den innkommende SIP-invitasjonen, avgjør denne nye parameteren om SIP Fra-toppteksten er prioritert over PAI-toppteksten eller omvendt.

Hvis aktivert attributt for <use-pai-as-calling-identity> -taggen er satt til «true», brukes PAI-overskriften med prioritet over Fra-overskriften. Denne anropsidentiteten brukes til å løse kontakten og presentere den for brukeren.

For **utgående anrop** brukes ikke denne logikken. I 18X, 200 OK-svar mottas den tilkoblede linjeidentiteten, så Webex applikasjonen bruker alltid SIP PAI-headeren med prioritet.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_PAI_AS_CALLING_IDENTITY_WXT%	feil	sann, usann	Kontrollerer om anropsidentiteten, presentert for brukeren, skal hentes fra SIP From- eller SIP P-Asserted-Identity-hodene. Sett til "true" for å bruke PAI-overskriften med prioritet.

6.1.40 Deaktiver skjermdeling

Release 42.5 legger til muligheten til å kontrollere tilgjengeligheten for skjermdeling. Når skjermdeling er deaktivert:

- brukeren vil ikke se alternativet for å starte skjermdeling i 1-1 samtaler

Konfidensiell Cisco

- de innkommende skjermdelingsforespørslene blir avvist og brukeren vil se en informativ melding

Som standard er denne funksjonen aktivert.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SCREEN_SHARE_WXT%	sant	sann, usann	Angir om skjermdeling skal aktiveres for brukeren.

6.1.41 Angivelse av søppelanrop

Når funksjonsvekslingen (per distribusjonstype) er aktivert, og funksjonen er aktivert i konfigurasjonsfilen, behandler Webex appen den nye parameteren som indikerer verifiseringsstatusen for spam-anrop, hvis de mottas som en del av NewCall Push-varsling eller anropshistorikk.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_SPAM_INDICATION_WXT%	feil	sann, usann	Kontrollerer tilgjengeligheten av søppelanropsindikasjonen på skjermen for innkommende anrop og anropslogg for Webex Calling bare.

6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN/mobilsamtaler

Støyfjerning gir en bedre ringeopplevelse for brukere når de snakker med ikke-Webex -brukere på PSTN eller mobile enheter. Med utgivelse 43.12 er støyfjerning slått på som standard.

Utgivelse 44.2 av Webex appen introduserer nye innkommende lydmedieforbedringer Speech AI for smalbånds-PSTN-anrop.

- En ny båndbreddeutvidelsesalgoritme er lagt til for å forbedre lydkvaliteten ved å utvide båndbredden til smalbånds-PSTN-spekteret og fjerne støyen. Den utvidede båndbredden vil øke forståelighet og redusere lyttetretthet.
- Den allerede eksisterende støyfjerningsalgoritmen er forbedret, og fjerner begrensningene for Music on Hold og andre lydtoner (f.eks. pipesignaler).
- Når denne funksjonen er aktivert, ser brukerne "Smart lyd – ekstern"-indikatoren og kan kontrollere tale AI-forbedringer for innkommende lydmedier.

Som standard er disse taleforbedringene aktivert og slått på. Brukeren kan kontrollere starttilstanden gjennom Smart-lydinnstillinger i lydinnstillingene.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	feil	sann, usann	Aktiverer taleforbedringer for eksterne (innkommende) medier.

MERK: Støyfjerning er nå en del av de ekstra taleforbedringene, og <noise-removal> taggen har blitt avviklet av den nye <speech-enhancements> taggen. Den tilpassede støyfjerning-taggen %ENABLE_NOISE_REMOVAL_WXT% er også avviklet.

6.1.43 QoS DSCP-merking

QoS DSCP-merking støttes med Webex appen som ringer media RTP-pakker (lyd og video). DSCP bestemmer trafikkklassifisering for nettverksdata. Dette kan brukes til å bestemme hvilken nettverkstrafikk som krever høyere båndbredde, har høyere prioritet og er mer sannsynlig å droppe pakker.

MERK: Nylige versjoner av Microsoft Windows-operativsystemet tillater ikke applikasjoner å angi DSCP eller UP direkte på utgående pakker, men krever i stedet distribusjon av gruppepolicyobjekter (GPO) for å definere DSCP-merkingspolicyer basert på UDP-portområder.

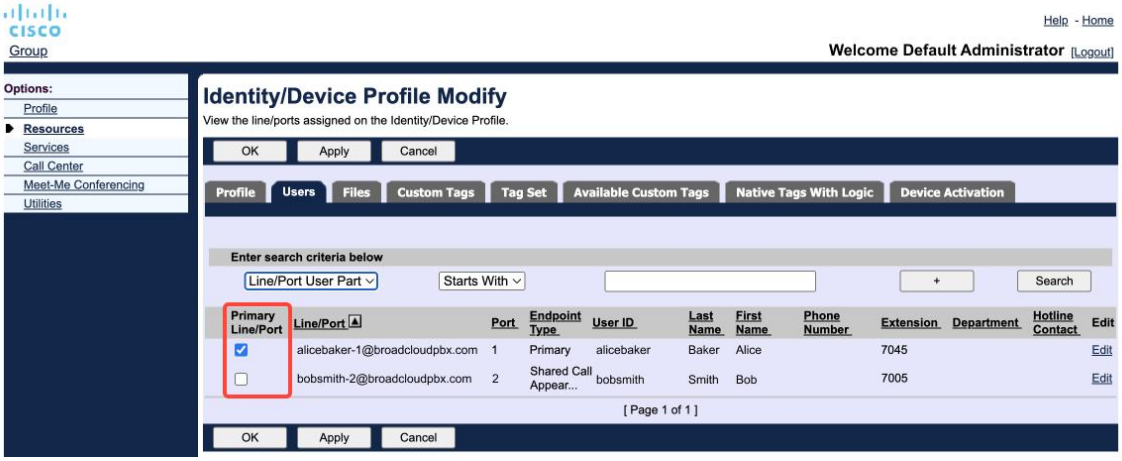
Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_AUDIO_QOS_WXT%	sant	sann, usann	Aktiverer QoS for lydsamtaler.
%AUDIO_QOS_VALUE_WXT%	46	0-63	Angir QoS-verdien for den valgte QoS-typen for lydanropene. Merk: Standardverdien brukes hvis ingen verdi er oppgitt, eller verdien ikke kunne analyseres.
%ENABLE_VIDEO_QOS_WXT%	sant	sann, usann	Aktiverer QoS for videosamtaler
%VIDEO_QOS_VALUE_WXT%	34	0-63	Angir QoS-verdien for den valgte QoS-typen for videosamtalene. Merk: Standardverdien brukes hvis ingen verdi er oppgitt, eller verdien ikke kunne analyseres.

6.1.44 Primærprofil

Med integrasjonen av de delte linjene (*6.2.12 Flere linjer – delt* linje-utseende), kan det være flere profiler av samme bruker hvis brukerens linje deles med en annen bruker type konfigurert for brukeren. For å velge riktig profil for å logge på telefontjenestene har Cisco BroadWorks blitt

Konfidensiell Cisco

forbedret for å indikere om en bruker eier en enhet, dvs. den er tilordnet primærlinje/port for en enhet – hvis du vil ha mer informasjon om Cisco-oppdateringenBroadWorks , kan du se Eierflagg i enhetslisten for å støtte Webex klientdelte linjer.



Primærlinje/portkonfigurasjon for identitets-/enhetsprofil i adminportalen

Fra og med versjon 43.2 legges et nytt konfigurasjonsalternativ (*enhetseierbegrensning*) til for å kontrollere om den primære profilbegrensningen skal brukes. Den kan brukes til å la Webex appen bruke en ikke-primær linje/port-profil for å logge på telefontjenestene. Dette konfigurasjonsalternativet brukes for alle konfigurasjonene, uavhengig av antall profiler som er konfigurert for brukeren (**Hvis enhetsbegrensningen er aktivert og det ikke er noen enhet med primærlinje/port for den tilsvarende plattformen, kobles ikke telefontjenester til**).

Samme begrensning gjelder enhetene brukeren kan pare med i skrivebords-Webex appen. Brukeren kan kun se og pare med enheter han eier. Dette forhindrer sammenkobling med enheter til en annen bruker som har delt eller virtuell linje tildelt. Verdien til den samme konfigurasjonsparameteren gjelder også for denne begrensningen.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	sant	sann, usann	Kontrollerer enhetseierbegrensningen – hvis telefontjenestene skal bruke primærprofilen for den gitte enheten

MERK: Det anbefales at eierens begrensning er aktivert. Hvis de er deaktivert, vil telefontjenestene bruke den første profilen som ble funnet for å logge på, og noen problemer kan oppstå hvis det er konfigurert flere profiler for brukeren av samme type.

Konfidensiell Cisco

6.1.45 Blokkeringsliste (Webex Calling kun)

Fra og med 43.5Webex appen introduserer brukerdefinert blokkeringsliste over telefonnumre. Hvis funksjonen er aktivert, kan brukeren spesifisere innkommende anrop fra bestemte numre som skal blokkeres på serversiden og ikke leveres på noen av brukerens enheter. Brukeren kan se disse blokkerte anropene i anropsloggen.

Brukeren kan konfigurere blokkeringslisten fra to steder - anropspreferanser og anropslogg. I innstillingene kan brukeren se listen over blokkerte numre og redigere den. I anropsloggen kan brukeren se anropshistorikken for anropene som er blokkert av den brukerdefinerte blokkeringslisten. Disse postene har blokkert indikasjon hvis nummeret er i den brukerdefinerte blokkeringslisten og brukeren vil ha muligheten til å oppheve blokkeringen direkte for gitt post. Blokkeringsalternativ er også tilgjengelig.

Regler for tallene lagt til i den brukerdefinerte blokkeringslisten:

- Nummerformat
  - Blokkering fra anropsinnstillingene gjelder E.164-formatbegrensninger lokalt i Webex appen
  - Blokkering fra anropsloggen er tillatt for alle Webex Calling oppføringene
  - Cisco BroadWorks kan tillate eller avvise forespørsler om nye numre som legges til i blokkeringslisten basert på nummerformatet
- Interne numre - innkommende anrop fra interne numre vil bli levert til brukeren, selv om de er en del av den brukerdefinerte blokkeringslisten

Den brukerdefinerte blokkeringslisten konfigureres på Cisco BroadWorks og brukes på alle WxC-enhetene for brukeren. Denne funksjonen fungerer sammen med den administratordefinerte blokkeringslisten, som ikke kan konfigureres av brukeren og bare kan kontrolleres av administratorene via Control Hub. Det er INGEN anropshistorikk for innkommende anrop som er blokkert av den admindefinerte blokkeringslisten.

Den brukerdefinerte blokkeringslisten brukes etter STIR/SHAKEN, admin-definerte blokkeringsliste og de anonyme anropsavvisningspolicyene.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_BLOCK_WXT%	sant	sann, usann	Aktiverer den brukerdefinerte blokkeringslisten Sett til «true» for å se blokkeringslisten i anropspreferanser og anropslogg

MERK: Denne funksjonen avhenger av at Cisco BroadWorks Call Block-tjenesten tilordnes brukeren.

Konfidensiell Cisco

6.1.46 Medietilpasning og resiliensimplementering (MARI)

6.1.46.1 Pristilpasning

Webex Applikasjonen har allerede integrert adaptive mediekvalitetsteknikker for å sikre at lyden ikke påvirkes av tap av videopakker, og for å sikre at video kan utnytte videohastighetstilpasning for å administrere mengden båndbredde som brukes i tider med overbelastning.

Hastighetstilpasning eller dynamiske bithastighetsjusteringer tilpasser anropshastigheten til den variable tilgjengelige båndbredden, og reduserer eller øker hastigheten på videobithastigheten basert på pakketapstilstanden. Et endepunkt vil redusere bithastigheten når det mottar meldinger fra mottakeren som indikerer at det er pakketap; og når pakketapet har avtatt, vil opphastigheten av bithastigheten skje.

Det er ingen konfigurerbare innstillinger for å kontrollere bruken av hastighetstilpasningsmekanismen.

6.1.46.2 Videresending av fec (FEC) og resending av pakker (RTX)

Fra og med utgivelsen 43.4 legger Webex appen til medietilpasningsmekanismen støtte for Forward Error Correction (FEC) og Packets Retransmission (RTX) for både lyd- og videomedier.

FEC gir redundans til den overførte informasjonen ved å bruke en forhåndsbestemt algoritme. Redundansen gjør at mottakeren kan oppdage og korrigere et begrenset antall feil, uten å måtte be avsenderen om ytterligere data. FEC gir mottakeren en mulighet til å korrigere feil uten å trenge en reverskanal (som RTCP) for å be om overføring av data, men denne fordelen er på bekostning av en fast høyere foroverkanalbåndbredde (flere pakker sendt).

Endepunktene bruker ikke FEC på båndbredder lavere enn 768 kbps. Dessuten må det også være minst 1,5 % pakketap før FEC introduseres. Endepunkter overvåker vanligvis effektiviteten til FEC, og hvis FEC ikke er effektiv, brukes den ikke.

FEC bruker mer båndbredde enn reoverføring, men har mindre forsinkelse. RTX brukes når liten forsinkelse er tillatt og det er båndbreddebegrensninger. Ved stor forsinkelse og nok båndbredde er FEC å foretrekke.

Webex Appen velger dynamisk RTX eller FEC avhengig av forhandlet båndbredde og forsinkelsestoleranse for en gitt mediestrøm. FEC resulterer i høyere båndbreddeutnyttelse på grunn av redundante videodata, men det introduserer ikke ytterligere forsinkelser for å gjenopprette tapte pakker. Mens RTX ikke bidrar til høyere båndbreddeutnyttelse, fordi RTP-pakkene bare sendes på nytt når mottakeren indikerer pakketap i RTCP-tilbakemeldingskanalen. RTX introduserer pakkegjenopprettingsforsinkelse på grunn av tiden det tar for RTCP-pakken å nå mottakeren fra avsenderen og for den overførte pakken å nå mottakeren fra avsenderen.

FEC må være aktivert for å ha RTX aktivert.

```
<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>
```


Konfidensiell Cisco

```
                        <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>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_AUDIO_MARI_FEC_WXT%	feil	sann, usann	Aktiverer FEC for lydanrop
%ENABLE_AUDIO_MARI_RTX_WXT%	feil	sann, usann	Aktiverer RTX for lydanrop (krever aktivert lyd-FEC)
%ENABLE_VIDEO_MARI_FEC_WXT%	feil	sann, usann	Aktiverer FEC for videosamtaler
%ENABLE_VIDEO_MARI_RTX_WXT%	feil	sann, usann	Aktiverer RTX for videosamtaler (krever aktivert video-FEC)

6.1.47 Samtidige samtaler med samme bruker

Legger til støtte for samtidige samtaler med samme bruker på én enhet.

Konfidensiell Cisco

Denne funksjonen er nyttig for enkelte distribusjoner, der den presenterte identiteten til samtalen ikke er den samme som den tilkoblede identiteten. Dette fører til manglende evne til å starte en deltatt overføring tilbake til den opprinnelige parten. Ved å aktivere denne funksjonen vil brukeren kunne håndtere flere samtidige samtaler med samme eksterne part.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	feil	sann, usann	Angir om Webex appen kan ha bare én eller flere WxC-anrop med samme bruker.

6.1.48 RTCP-XR

Fra og med utgivelsen 43.8 legger Webex appen til forhandling for RTCP-XR-pakkeutveksling under en samtale. Forhandling skjer under etableringen av SIP INVITE-sesjonen. Hvis begge endepunktene støtter RTCP-XR-pakker, vil Webex Media Engine begynne å utveksle disse pakkene og hjelpe den adaptive samtalekvalitetsmekanismen. Denne funksjonen er aktivert som standard.

I tillegg, for Webex Calling bare, vil disse ekstra målingene sendes gjennom SIP BYE og på denne måten eksponeres i Control Hub.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	sant	sann, usann	Muliggjør RTCP-XR-forhandling og pakkeutveksling for bedre samtalekvalitet. Aktivert som standard.

6.1.49 Informasjon om viderekobling av anrop

Utgivelsen 44.2 av Webex appen introduserer et konfigurerbart alternativ for å kontrollere synligheten av viderekoblings- og omdirigeringsinformasjonen i de anropsrelaterte skjermene og anropsloggen.

```
<config>
```


Konfidensiell Cisco

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	sant	sann, usann	Styrer synligheten av viderekoblings- og omdirigeringsinformasjonen. Sett til «true» for å se informasjonen i de anropsrelaterte skjermene og anropsloggen.

6.1.50 Innringer-ID

6.1.50.1 Utgående innringer-ID

Webex Mobil (utgivelse 44.2) og skrivebord (utgivelse 44.3)-apper introduserer en ny mulighet for brukeren til å velge den foretrukne eksterne anrops-ID for utgående anrop. Listen over tilgjengelige alternativer inkluderer:

- Direkte linje (standard)
- Stedsnummer
- Egendefinert nummer fra samme organisasjon
- Samtalekøer brukeren er en del av, som gjør det mulig for agenter å bruke innringer-ID-nummeret sitt
- Huntgrupper brukeren er en del av, som gjør det mulig for agenter å bruke oppringer-ID-nummeret sitt
- Skjul anroper-ID

Merknader:

- Liste over alternativer avhenger av linjen:
  - Primærlinje – komplett sett med alternativer
  - Delte linjer – ikke tilgjengelig
  - Virtuelle linjer – kun alternativer for samtalekø
- Hvis den allerede valgte identiteten ikke lenger er tilgjengelig, brukes brukerens standard oppringer-ID
- Nødanrop bruker alltid brukerens tilbakeringingsnummer
- Avvikler <outgoing-calls> tag under seksjon <services><call-center-agent>

Listen over tilgjengelige alternativer kan konfigureres gjennom adminportalen. Det finnes også separate egendefinerte DMS-tagger for å kontrollere tilgjengeligheten av disse forbedringene i Webex appen.

```
<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%"/>
```


Konfidensiell Cisco

```
        <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
        <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </outgoing-calls>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_OUTGOING_CALLS_WXT%	feil	sann, usann	Aktiverer valg av telefonlinje-ID-nummer for utgående anrop.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	feil	sann, usann	Styrer tilgjengeligheten av tilleggsnumrene som er konfigurert for brukeren.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	feil	sann, usann	Kontrollerer tilgjengeligheten til telefonsenternumrene (DNIS) som er konfigurert for brukeren.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	feil	sann, usann	Kontrollerer tilgjengeligheten til huntgruppenumrene som er konfigurert for brukeren.
«%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	feil	sann, usann	Aktiverer blokkering av levering av oppringer-ID som valg for utgående anrop.

MERK: Desktop-appversjon 44.3 støtter bare Call Center CLID og 44.4 legger til støtte for resten av alternativene.

6.1.50.2 Navn på ekstern innringer-ID

Ved mottak/initiering av et anrop BroadWorks sender Cisco visningsnavnet til den eksterne parten i SIP-invitasjonen. Den brukes som standard av Webex appen. Samtidig starter Webex appen kontaktløsning mot flere kilder, med følgende prioritet:

- Common Identity (CI)
- Kontakttjeneste (egendefinerte kontakter)
- Outlook-kontakter (skrivebord)
- Lokal adressebok (mobil)

I tilfelle en vellykket kontaktoppløsning mot noen av søkekildene oppdateres visningsnavnet til den eksterne parten. Hvis kontakten finnes i CI, er samtaleøkten koblet til Webex skytjenestene til den samme brukeren, noe som gir muligheten til å se avataren og tilstedeværelsen til den eksterne parten, ha en chat, skjermdeling, mulighet til å eskalere til et Webex skymøte osv.

Utgivelsen 44.5 av appen Webex legger til konfigurerbare alternativer for å ignorere kontaktoppløsningen og alltid beholde Ciscos BroadWorks visningsnavn for samtaler med arbeidsområder eller en RoomOS-enhet som brukes til 1:1 Cisco BroadWorks samtaler.

```
<config>
<services><calls>
   <caller-id>
```


Konfidensiell Cisco

```
    <remote-name>
       <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	løst	løst, slurk	Styrer visningsnavnet for den eksterne parten for arbeidsområder og RoomOS-enheter. Bruk "sip" for å ignorere kontaktoppløsningen og bruk visningsnavnet mottatt i SIP INVITE-økten.

Konfidensiell Cisco

6.2 Funksjoner kun for skrivebordet

6.2.1 Tvungen utlogging

Denne funksjonen gjør det mulig for Cisco BroadWorks å spore nettbaserte klientforekomster med samme enhetstype, og kun én av dem kan være tilkoblet på én gang. Når Cisco BroadWorks varsler klienten om å logge av, avsluttes SIP-tilkoblingen, og klienten angir at anropet ikke er tilkoblet.

Denne funksjonen er nødvendig i enkelte distribusjoner der lignende klienter ellers kan være online samtidig, noe som forårsaker bivirkninger. Et eksempel er en bruker med en stasjonær maskin på jobb og hjemme, hvor de innkommende samtalene kun vil bli mottatt av en av klientene, avhengig av hvilken SIP-registrering som er aktiv.

Tvunget utlogging er basert på SIP, klienten sender en SIP Abonner på hendelsespakken *anropsinfo* med en spesiell *appid-verdi* i *Fra* -overskriften, uansett av *bsoft-call-info* parameterverdien. Når Cisco BroadWorks oppdager flere klientforekomster på nettet med samme *appid*, sender den en spesiell SIP-varsel til den eldre klientforekomsten, noe som får den til å logge av. For eksempel vil skrivebordsklienter ha en identisk *appid-verdi* , selv om det ikke er noen begrensning på bruken av denne identifikatoren på klientsiden. *Appid-verdien* konfigureres av tjenesteleverandøren.

Merk at for å bruke tvungen utlogging, må SIP *Call-Info* -abonnementet være aktivert.

Hvis du vil ha informasjon om Cisco BroadWorks oppdateringer og versjoner som trengs for denne funksjonen, kan du se avsnittet om Cisco BroadWorks programvarekrav i *Webex for Cisco BroadWorks Solution Guide*.

Se følgende eksempel for konfigurasjonsdetaljer (SIP er den eneste støttede kontrollprotokollen i denne utgivelsen).

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_FORCED_ LOGOUT_WXT%	feil	sann, usann	Aktiverer tvungen utlogging.
%FORCED_LOGOUT_ APPID_WXT%	tomt	streng	Appid brukt på serversiden for korrelasjon. Dette kan være hvilken som helst streng. Eksempel: «123abc»

6.2.2 Mottak av anrop

Henting av anrop er en flerbrukertjeneste som lar utvalgte brukere svare på en hvilken som helst ringelinje innenfor deres hentingsgruppe. En samtalehentingsgruppe er definert av administratoren og er en undergruppe av brukerne i gruppen som kan svare på hverandres samtaler.

Følgende hentetilfeller støttes:

Konfidensiell Cisco

- Blind henting
- Henting av anrop (som gjør det mulig for en bruker å svare på et anrop rettet til en annen telefon i gruppen deres ved å slå den respektive funksjonstilgangskoden etterfulgt av forlengelsen til den ringende telefonen).

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_PICKUP_BLIND_WXT%	feil	sann, usann	Sett til "true" for å aktivere blind samtale.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	feil	sann, usann	Satt til «sann» for å aktivere Styrt mottak av anrop.

6.2.3 Støtte for sjef-administrator (lederassistent)

Sjef-Admin, kjent som Executive-Assistant-funksjonen på Cisco BroadWorks, gjør det mulig for en assistent å operere på vegne av en leder for å skjerme, svare på og ringe som «leder». En assistent kan ha mange ledere og det er mulig å:

- Velg ønsket rolle når du ringer.
- Besvar en innkommende samtale på vegne av en leder og send deretter samtalen til lederen. I tillegg til det er alle vanlige samtaleadministrasjonsalternativer tilgjengelige.
- Se at en innkommende samtale faktisk er for lederen.

Leder og lederassistent er to sammenhengende Cisco-tjenesterBroadWorks , som sammen leverer følgende funksjonalitet:

- En bruker med Executive-tjenesten kan definere en gruppe assistenter som administrerer samtalene deres. Assistentene må velges blant brukerne i samme gruppe eller virksomhet som har tildelt Executive-Assistant-tjenesten.
- En bruker med Executive-Assistant-tjenesten kan besvare og starte anrop på vegne av sine ledere.
- Både leder og deres assistenter kan spesifisere hvilke samtaler som skal viderekobles til assistentene, hvordan assistenter skal varsles om innkommende samtaler, og hvilke av samtalene som videresendes til assistentene som skal presenteres for lederen for screening.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	feil	sann, usann	Sett til "true" for å aktivere Boss-Admin-funksjonen.

MERK: Funksjonen Boss-Admin (Executive-Assistant)-støtte er ikke tilgjengelig i kombinasjon med Shared-Lines.

6.2.4 Eskalere SIP-anrop til møte (Webex Calling kun)

Klienten gir funksjonaliteten til å eskalere en pågående SIP-samtale til et møte via Webex Calling. Ved å bruke denne funksjonaliteten i stedet for en standard ad-hoc-konferanse, vil brukeren kunne bruke video så vel som skjermdeling under møtet.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	feil	sann, usann	Sett til «true» for å aktivere menyalternativet Eskaler til Webex Møte.

6.2.5 Kontrollanrop for bordtelefon – automatisk svar

Autosvar gjør det mulig for brukeren å bruke Desk Phone Control (DPC) for utgående anrop på klienten for å administrere MPP-telefoner med null berøringssvar.

Den valgte MPP-telefonen vil bære lyd/video for det utgående DPC-anropet.

Automatisk svar kan fungere på primære og ikke-primære klargjorte enheter. Hvis brukeren har mer enn én registrert bordtelefon som kan pares med, skal kun den valgte/sammenkoblede enheten svare automatisk.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	sant	sann, usann	Når satt til "true", aktiverer bordtelefonkontroll automatisk svar.

Konfidensiell Cisco

MERK: Autosvar vil ikke påvirke innkommende anrop i DPC-modus, slik at bordtelefonen ringer for innkommende anrop.

6.2.6 Automatisk svar med tonevarsling

Denne funksjonen aktiverer automatisk svar på innkommende anrop for lokale enheter, hvis dette er indikert i forespørselen om innkommende anrop.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_AUTO_ANSWER_WXT%	feil	sann, usann	Når satt til "true", aktiverer automatisk svar på innkommende anrop hvis dette blir bedt om fra backend.

6.2.7 Styring av bordtelefon – Midtsamtalekontroller – Konferanse

Denne funksjonen aktiverer alternativer for konferanse og sammenslåing for eksterne (XSI) samtaler som er avsluttet på et annet sted.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	feil	sann, usann	Når satt til «sann», aktiveres Konferanse- og Slå sammen-alternativer for eksterne samtaler (XSI), avsluttet på et annet sted.

6.2.8 Varsler om mottak av anrop

Anropsvarslinger gir brukeren muligheten til å vite når det er et innkommende anrop til en bruker han er konfigurert til å overvåke. Anropsvarslinger kan mottas for overvåkningslister som er konfigurert gjennom Anropshentingsgruppen og Busy Lamp Field-tjenestene.

Anropsvarslinger er nyttige når de overvåkede brukerne ikke er fysisk i nærheten av hverandre og ikke kan høre ringen fra kollegaens telefon.

6.2.8.1 Opptattlampefelt

Skrivebords-Webex programmet viser et varsel hvis et medlem i overvåkningslisten Busy Lamp Field (BLF) har et innkommende anrop i varslingstilstand. Varslingen har informasjon om den som ringer og brukeren som mottok det innkommende anropet, med muligheter for å besvare anropet, stille eller ignorere varselet. Svar på det innkommende anropet av brukeren starter rettet samtalehenting.

Fra og med versjon 43.4 er listen over BLF-overvåkede brukere tilgjengelig i Multi Call Window (MCW) for Calling (kun tilgjengelig for Windows). Integrasjon av BLF-listen i MCW inkluderer:

- Overvåk innkommende anrop med mulighet for å besvare anropet eller ignorere varselet.
- Se hele listen over BLF-brukere.

Konfidensiell Cisco

- Overvåk tilstedeværelsen til brukerne – rik tilstedeværelse er kun tilgjengelig for brukere med Webex Cloud-rettigheter. Grunnleggende (telefoni) tilstedeværelse er bare tilgjengelig for BroadWorks-bare brukere.
- Start en samtale med en BLF-bruker.
- Start en chat med en BLF-bruker – kun tilgjengelig for brukere med Webex Cloud-rettigheter.
- Legg til en BLF-bruker som kontakt.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_BUSY_LAMP_FIELD_WXT%	feil	sann, usann	Aktiverer Busy Lamp Field-overvåking og ringevarsling for andre brukere med mulighet til å svare på anropene.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	sant	sann, usann	Gjør det mulig å vise oppringerens visningsnavn/nummer i ringevarselet.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Styrer hvor mange sekunder ringevarselet skal utsettes før det vises til brukeren.

MERK: Denne funksjonen avhenger av tjenesten Henting av anrop.

6.2.8.2 Gruppe for mottak av anrop (Webex Calling kun)

Fra og med Utgivelse 44.2, Webex legger programmet til støtte for varsler om mottak av gruppeanrop (GCP) for Webex Calling distribusjonen. Den lar brukere bli varslet om innkommende anrop for alle brukerne som overvåkes gjennom samtalehentingsgruppen.

I tilfelle et innkommende anrop for en brukerdel av en samtalehentingsgruppe, får den som ringer en sjanse til å svare på anropet. Det er en GCP-varslingsforsinkelse som kan konfigureres via Control Hub. Hvis den som ringer ikke behandler anropet innen den konfigurerte tiden, sendes et GCP-varsel til gruppen.

I tilfelle av flere anrop innenfor samme gruppe for samtalehenting, behandles de sekvensielt basert på tidspunktet de mottas. Varslingen om den eldste samtalen blir først levert til gruppen, og når den er behandlet, leveres den neste varslingen i kø til gruppen.

Varsler kan være kun lyd, visuell eller lyd og visuell avhengig av konfigurasjonen i Control Hub-administrasjonsportalen. Hvis det er en visuell GCP-varsling, kan brukeren besvare anropet ved å bruke funksjonen Henting av anrop. Hvis kun lydvarsling er konfigurert, vil brukeren ikke se et visuelt varsel for det innkommende anropet, vil høre en spesifikk ringetone og han kan svare på anropet fra menyen Anropshenting som er tilgjengelig i Webex appen, eller ved å ringe FAC kode (*98) og utvidelsen manuelt.

Brukeren kan dempe GCP-varslingen gjennom applikasjonsinnstillingene. Denne innstillingen gjelder for alle varslinger om samtalehenting (BLF og GCP), og varsler er som standard dempet.

Konfidensiell Cisco

Funksjonen fungerer for primærlinjene og for delte eller virtuelle linjer som er tildelt brukeren.

```
<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>
        ...
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_GCP_NOTIFICATIONS_WXT%	feil	sann, usann	Aktiverer varslinger for gruppeanrop
%ENABLE_GCP_DISPLAY_CALLER_WXT%	sant	sann, usann	Aktiverer visning av anroperens visningsnavn/nummer i ringevarselet
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5-120	Definerer den maksimale tiden et GCP-varsel er tilgjengelig for brukeren
%BWGROUP-CALL-PICKUP-BOOL-n%	feil	sann, usann	Indikerer om den korresponderende linjen har konfigurert samtalehentingsgruppe

MERKNAD 1: Dette er Webex Calling bare en funksjon.

MERKNAD 2: Denne funksjonen avhenger av samtalehentingsgruppen som er konfigurert for brukeren.

6.2.9 Hendelsespakke for fjernstyring

For Klikk for å ringe klienter som BroadWorks Resepsjonisttynnklienten og Gå-integratoren der Webex appen er anropsenheten, når du mottar et anrop eller håndterer vent/gjenoppta Webex appen nå hendelsespakken for fjernkontroll.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	feil	sann, usann	Når satt til "true", spesifiserer at fjernkontrollen skal være aktivert for brukeren.

6.2.10 Utvalg av CLID for ringkøagent

Når agenter ringer til kundene sine, vil de at kundene skal se den aktuelle Calling Line ID (CLID) i stedet for deres personlige/bedriftsCLID. Hvis for eksempel agent Mary Smith er koblet til anropskøen for teknisk støtte, vil Mary at kundene skal se CLID-en hennes som teknisk støtte, ikke Mary Smith når hun ringer kunder.

Administratorer i Control Hub eller CommPilot kan spesifisere for en anropskø ett eller flere DNIS-numre som skal brukes for utgående CLID. Agenter har da muligheten til å velge et av DNIS-numrene som skal brukes som deres CLID når de foretar utgående anrop. Webex Appen gir agenter muligheten til å velge hvilken DNIS som skal brukes som CLID.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%	feil	sann, usann	Aktiverer utgående anrop (CLID-valg) på vegne av Call Center-køen.

6.2.11 Gateway for overlevelse (Webex Calling kun)

Fra og med utgivelsen 43.2 legger Webex applikasjonen til støtte for modus for overlevelsesanrop. hvis funksjonen er aktivert og det ikke er noen Webex Cloud-tilkobling, kan Webex applikasjonen kjøres i overlevelsesmodus. I denne modusen er det begrenset ringefunksjonalitet tilgjengelig for brukeren.

Local Survivability Gateway er distribuert av kunden.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	feil	sann, usann	Aktiverer støtte for overlevelsesmodus.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Spesifiserer tilbakefallstiden (overlevelsesporten til SSE)

Konfidensiell Cisco

MERK: Denne funksjonen gir trygghet ved migrering fra lokale til sky-anropsløsninger.

6.2.12 Flere linjer – delt linje-utseende

Fra og med Release 42.12, Webex legger programmet til støtte for flere linjer. En Webex bruker kan ha en primærlinje og opptil 9 delelinjer med andre brukere.

Administrator bør sette opp delte anropsvisninger for hver delt linje.

Webex klienten vil oppdage linjekonfigurasjonsoppdateringer innen 12 timers tidsramme og vil be brukeren om å starte applikasjonen på nytt. Re-innlogging av brukeren vil bruke linjeoppdateringene umiddelbart.

Fra og med Utgivelse 43.12 er Webex appen forbedret for å tillate å flytte (lokalt gjenoppta) en samtale på en delt linje, håndtert av en annen bruker eller av samme bruker på en annen enhet. For mer informasjon, se *6.2.15 Flytt samtale*.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_MULTI_LINE_WXT%	feil	sann, usann	Aktiverer støtte for flere linjer (hvis konfigurert). Hvis deaktivert (sett til "false"), vil bare den første konfigurerte linjen bli brukt av applikasjonen.

MERKNAD 1: Funksjonen Boss-Admin (Executive-Assistant) er ikke tilgjengelig i kombinasjon med delte linjer.

MERKNAD 2: Se «Delt linje utseende» i Webex-for-Cisco-BroadWorks-Solution-Guide for ytterligere BroadWorks krav.

6.2.13 Flere linjer – virtuelle linjer (Webex Calling kun)

Kun for Webex Calling distribusjon støtter Webex appen konfigurasjon med flere linjer ved hjelp av virtuelle linjer. Funksjonelt sett samsvarer konfigurasjonen med virtuelle linjer med multilinje ved bruk av delte linjer – med muligheten til å se de virtuelle linjene som er konfigurert for brukeren og bruke dem for innkommende og utgående anrop. Maksimalt 9 kombinerte virtuelle linjer og delte linjer kan konfigureres.

Release 43.4 utvider støtten for virtuelle linjer og legger til samtaleparkering og samtaleparkeringshenting.

Fra og med Utgivelse 43.12 er Webex appen forbedret for å tillate å flytte (lokalt gjenoppta) en samtale på vent på en virtuell linje, håndtert av en annen bruker eller av samme bruker på en annen enhet. For mer informasjon, se *6.2.15 Flytt samtale*.

Det følgende viser endringene i konfigurasjonsmalen relatert til støtte for virtuelle linjer.

Konfidensiell Cisco

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

6.2.14 Hendelsespakke for fjerndemping (Webex Calling kun)

Fra og med utgivelsen 43.9 legger Webex appen til støtte for fjerndemping av anropskontroll av lydmediestrømmen. Dette gjør det mulig å utløse demping/oppheving av demping av en pågående samtale fra et annet sted som BroadWorks resepsjonisttynnklient, der Webex appen er anropsenheten.

Funksjonen avhenger av den nye SIP *x-cisco-mute-status* informasjonspakken. Hvis *Recv-Info:x-cisco-mute-status* -overskriften mottas under etableringen av samtalen SIP INVITE-økten, så når det er en oppdatering (lokal eller ekstern) til mute-tilstanden for lydanropsøkten , sender Webex appen tilbake SIP-INFO med *Info-Package:x-cisco-mute-status;muted=true* (eller *muted=false*), der muted-parameteren representerer den oppdaterte tilstanden til lydmediestrømmen.

Demp eller opphev demping kan utløses lokalt eller fra et eksternt sted. Ekstern oppdatering utløser en SIP NOTIFY med *Hendelse: mute* (eller *unmute*) for å sendes til Webex appen fra applikasjonstjeneren. Webex Appen respekterer den eksterne forespørselen, og etter oppdateringen av lydmediestrømmen sender den tilbake en SIP NOTIFY med *Info-Package:x-cisco-mute-status;muted=true* (eller *muted=false*).

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	feil	sann, usann	Når den er satt til «sann», aktiveres fjernkontrollen for demping av samtalen for brukeren.

Konfidensiell Cisco

6.2.15 Flytt samtale

Webex app gir samtaleovervåking og samtalekontroll av VoIP-samtaler som avsluttes på et annet sted. Dette er for øyeblikket bare tilgjengelig for brukerens primærlinje.

Fra og med Utgivelse 43.12 er Webex appen forbedret for å vise samtaler som er avsluttet på et annet sted, også for delte og virtuelle linjer. Slike samtaler er synlige i området for pågående samtaler for informasjonsformål og uten mulighet til å kontrollere dem. Bare hvis en slik samtale settes på vent, vil brukeren kunne flytte den til den lokale enheten ved å velge den og gjenoppta den fra samtaleskjermen. Denne mekanismen er nyttig hvis samtalen ble håndtert av samme bruker på et annet sted eller av en annen bruker som bruker samme linje.

Merk at det ikke er mulig med Webex appen å flytte en samtale på venting til en sammenkoblet enhet. Hvis brukeren er sammenkoblet med en enhet, må han først koble fra og deretter kan han gjenoppta den ventende samtalen lokalt.

Samtaleovervåking for delt og virtuell linje avhenger av hendelsespakken for SIP-anropsinfo.

Overvåkingen av samtalene for brukerens primærlinje avhenger av XSI-hendelsene (Advanced Call Event Package) og flytting av en samtale til den lokale enheten er ikke tilgjengelig for disse samtalene. For denne typen samtaler kan brukeren bruke funksjonen Call Pull (*6.1.22 Anropstrekk*). Call pull fungerer kun for de siste aktive samtalene til brukeren, mens mekanismen for delte og virtuelle linjer fungerer for alle samtalene til brukeren som er satt på vent.

1. Brukstilfelle 1:
    a. Alice har Bobs linje tildelt for skrivebords- og bordtelefonprofilene.
    b. Alice har en samtale med Charlie gjennom bordtelefonen – Alice kan se den pågående samtalen i skrivebordsappen.
    c. Alice setter samtalen på vent fra bordtelefonen – samtalen kan gjenopptas av Alice fra skrivebordsappen.
2. Brukstilfelle 2:
    a. Alice har Bobs linje tildelt for skrivebords- og bordtelefonprofilene.
    b. Bob har en samtale med Charlie – Alice kan se den pågående samtalen i skrivebordsprogrammet.
    c. Bob setter samtalen med Charlie på vent – Alice kan gjenoppta samtalen med Charlie fra skrivebordsappen.
3. Brukstilfelle 3:
    a. Alice har Bobs linje tildelt for skrivebords- og bordtelefonprofilene.
    b. Alice er sammenkoblet med bordtelefonen sin fra skrivebordsappen.
    c. Bob har en samtale med Charlie – Alice kan se den pågående samtalen i skrivebordsprogrammet.
    d. Bob setter samtalen med Charlie på vent – Alice kan ikke gjenoppta samtalen med Charlie fra skrivebordsprogrammet.
    e. Alice kobler fra Desktop-appen fra bordtelefonen – Alice kan gjenoppta samtalen med Charlie fra Desktop-appen.

```
<config>
<services><calls>
    <call-move>
```


Konfidensiell Cisco

```
        <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_MOVE_HERE_WXT%	feil	sann, usann	Aktiverer samtaleflytting på lokal enhet. Brukes for å holde/gjenoppta på tvers av lokasjoner/brukere i brukssaken med flere linjer.

Konfidensiell Cisco

6.3 Funksjoner kun for mobil

6.3.1 Nødsamtaler

Webex for Cisco BroadWorks støtter Native Emergency Calling.

Når funksjonen er aktivert, ved å starte et utgående VoIP-anrop, analyserer applikasjonen det oppringte nummeret og sammenligner det med listen over nødnumre som er konfigurert. Hvis nummeret er identifisert som et nødnummer, utfører applikasjonen den konfigurerte ringeatferden. Den kan konfigureres ved hjelp av *oppringingssekvensen* -taggen.

Støttede moduser er:

- *cs-only* – Klienten foretar nødanrop bare via mobilnettverket hvis nettverket er tilgjengelig.
- *cs-first* – Ved å starte et nødanrop, sjekker klienten nettverkstypen som gjeldende enhet er koblet til. Hvis mobilnettverket er tilgjengelig, ringer klienten over mobilnettverket. Hvis mobilnettverket ikke er tilgjengelig, men et mobildata-/WiFi-nettverk er tilgjengelig, plasserer klienten anropet over mobildata-/WiFi-nettverket som et VoIP-anrop. Dessuten, hvis nødanropet er plassert gjennom mobilnettet, foreslår klienten brukeren å prøve nødanropet på nytt som VoIP.
- *Kun voip* – Klienten foretar nødanrop som VoIP bare hvis mobildata-/WiFi-nettverket er tilgjengelig.
- *cs-voip* – Klienten analyserer om enheten kan starte den som et naturlig kretssvitsjet (CS) anrop (uten å ta hensyn til om CS-nettverket er tilgjengelig eller ikke). Hvis enheten kan starte et eget anrop, ringes nødnummeret som et nødanrop. Ellers ringes anropet som VoIP.

> merk: Hvis VOIP-anrop er deaktivert, er den eneste betydningsfulle verdien for nødnummersekvens (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) kun cs.

Det vises en ansvarsfraskrivelse for nødanrop til brukeren ved pålogging. Det styres ikke gjennom konfigurasjonsalternativene.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_EMERGENCY_DIALING_WXT%	feil	sann, usann	Sett til «true» for å aktivere registrering av nødanrop. Standardverdien er tom.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	cs-bare	cs-only, cs-first, voip-only, cs-voip	Styrer oppringingssekvensmodus for nødanrop.
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	CSV-liste	CSV-liste over nødnumre. Eksempel: 911,112

Konfidensiell Cisco

6.3.2 Push-varsler for anrop

Når et innkommende anrop mottas, mottar mobilklienten en push-varsling (PN) først. Det er en konfigurasjonsparameter som kan brukes til å kontrollere når SIP REGISTER-sesjonen skal etableres:

1. Når push-varslingen er mottatt, ELLER
2. Når anropet er akseptert av brukeren.

Den andre tilnærmingen anbefales. Men sammenlignet med det første tilfellet, legger det til en viss forsinkelse før samtalen er etablert.

I henhold til iOS 13-kravene skal VoIP PN-ene bare brukes for innkommende anrop. Resten av de anropsrelaterte hendelsene bør bruke vanlige PN-er.

For å oppfylle dette kravet introduseres ny PN-registrerings-API, og den krever at tilsvarende oppdatering brukes på applikasjonsserveren. Hvis backend ikke er konfigurert til å støtte iOS 13 PN-er, kan konfigurasjonsparameteren brukes til å fremtvinge bruk av de eldre push-varslene, der alle samtalerelaterte hendelser leveres gjennom VoIP PN-er.

Det er en push-varsling sendt av applikasjonsserveren (AS) når en ringende anrop aksepteres av den som ringer på et annet sted, lukkes av den som ringer, eller for eksempel omdirigeres til talepost. Med iOS 13 er denne typen push-varsling nå en vanlig, og den har noen begrensninger. Det kan bli forsinket av Apple Push Notification Service (APNS) eller til og med ikke levert i det hele tatt. For å håndtere manglende eller forsinkede anropsoppdateringer, legges det til en konfigurerbar ringetid for å kontrollere maksimal ringetid. Hvis maksimal ringetid er nådd, stoppes ringingen for den som ringte og anropet behandles som ubesvart. På innringersiden kan anropet forbli i ringetilstand til policyen for ringing-ikke-svar som er konfigurert på applikasjonsserveren (AS) blir utført.

For å holde programmet konsekvent, gjelder den konfigurerbare ringetimeren både for Android og iOS.

Et eget konfigurasjonsalternativ er lagt til for å spesifisere avvisningsadferden når et innkommende anrop mottas som en push-varsling. Klienten kan konfigureres til å ignorere anropet eller svare serveren via Xsi med avslag satt til «sann» eller «usann». I så fall vil de tilordnede Cisco BroadWorks samtalebehandlingstjenestene bli brukt. Hvis "decline_false" er konfigurert, fortsetter samtalen å ringe til avsenderen forlater eller timeren for ikke-svar utløper, og de tilknyttede samtalebehandlingstjenestene starter. Hvis "decline_true" er konfigurert, spesifiserer avvisningsårsaken samtalebehandlingen. Hvis årsaken til avvisningen er satt til "opptatt", tvinger serveren umiddelbart til den opptatte behandlingstjenesten. Hvis "temp_unavailable" er konfigurert, brukes den midlertidig utilgjengelige behandlingstjenesten.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	feil	sann, usann	Kontrollerer når SIP REGSITER-sesjonen er etablert – ved mottak av en push-varsling for innkommende anrop eller ved å akseptere den.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Styrer maksimal ringetid for innkommende anrop for anrop mottatt via PN. Hvis ingen CallUpd PN mottas innen den gitte perioden, vil anropet bli behandlet som ubesvart.
%REJECT_WITH_XSI_MODE_WXT%	decline_false	ignore, decline_true, decline_false	Angir atferden for avvisning av anrop.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	opptatt	opptatt, midlertidig_ikke tilgjengelig	Spesifiserer årsaken til avvisning av anrop, hvis avvisningsmodus er satt til "decline_true".

6.3.2.1 MWI

Med MWI-funksjonen aktivert abonnerer den mobile Webex klienten på MWI Push Notification for å motta oppdateringer med taleposten til brukeren og varsle ham.

For å redusere antall varsler og for å unngå unødvendig distraksjon, undertrykkes MWI Push Notifications i noen tilfeller. For eksempel når brukeren lytter til talepostmeldingene eller merker dem som lest fra mobilWebex klienten (ulest nummer synker). Det er ikke noe konfigurerbart alternativ for å kontrollere dette.

Hvis du vil ha mer informasjon om MWI, kan du se avsnitt *6.1.27 Talepost, visuell talepost, indikator for melding* venter.

6.3.2.2 Ringsprut

BroadWorks tjenester (som DND) kan sende ringelyd når innkommende omdirigeres. Den Webex Mobilklienten kan konfigureres til å aktivere Ring Splash Push Notifications og presentere dem for brukeren når de utløses av BroadWorks.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_RING_SPLASH_WXT%	feil	sann, usann	Aktiverer ringsplash i BroadWorks konfigurasjonen.

6.3.2.3 Leveringsmodus (Webex Calling kun)

Webex Appen bruker Notification Push Server (NPS) for å levere push-varslene for anrop til APNS/FCM. Utgivelsen 45.2 av Webex appen støtter nå tre forskjellige leveringsmoduser for å konfigurere hvordan de anropsrelaterte push-varslene skal leveres til APNS/FCM:

Konfidensiell Cisco

- nps - gjeldende mekanisme, ved hjelp av NPS
- sky – forbedret mekanisme, ved hjelp av Cisco Webex Cloud-mikrotjeneste
- ekstern - en mekanisme som bruker tredjepartssystem. Det krever integrering av tredjepartssystemet med Cisco WebHooks-motoren

```
<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%">
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	nps	nps, sky, ekstern	Angir leveringsmodus for push-varslene for samtaler.

6.3.3 Enkeltvarsling

Funksjonen Mobile Single Alert er ment for distribusjoner av fast-mobil konvergens (FMC) / Mobile Network Operator (MNO) som utnytter BroadWorks Mobility-tjenesten. Uten det, når brukeren er logget på Webex klienten og mottar et innkommende anrop, vil brukeren motta to anrop samtidig – en innfødt og en Push Notification (VoIP)-anrop. Når funksjonen er aktivert, deaktiverer programmet Mobilitetsvarsel på brukerens BroadWorks Mobilitetssted når du logger på og aktiverer varselet når du logger av. En viktig forutsetning for å bruke denne funksjonen er at brukeren har BroadWorks Mobilitetstjenesten tilordnet og nøyaktig ett sted konfigurert.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SINGLE_ALERTING_WXT%	feil	sann, usann	Sett til "true" for å aktivere enkeltvarsling.

6.3.4 Klikk for å ringe (Ring tilbake)

Den utgående Click to Dial sikrer at sluttbrukeren kan ha en samtale på sin personlige kretssvitsjede mobiltelefon og levere bedriftens DN som telefonlinje-ID.

Mobilklienten Webex støtter klikk for å ringe (tilbakeringing) anrop ved hjelp av BroadWorks Hvor som helst-tjenesten. BroadWorks Hvor som helst-plasseringene i Webex programmet kalles Single Number Reach (SNR)-plasseringer.

Konfidensiell Cisco

Når funksjonen er aktivert, kan brukere velge SNR-plassering fra enhetsparingsmenyen. Når paret med SNR-posisjon, startes alle utgående anrop ved hjelp av Klikk for å ringe (Call Back)-anrop. For å forhindre dobbel varsling er Push-varsler for innkommende anrop deaktivert.

Når en bruker starter et klikk for å ringe-anrop, vil de se skjermen for utgående anrop med informasjon om å forvente innkommende anrop på den valgte SNR-posisjonen. Denne skjermen lukkes automatisk basert på konfigurerbar timer.

Ved frakobling fra et SNR-sted, registrerer applikasjonen seg på nytt for Push-varsler for innkommende anrop.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DIALING_CALL_BACK_WXT%	feil	sann, usann	Sett til «true» for å aktivere Klikk for å ringe (Call Back)-anrop.
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Styrer antall sekunder før tilbakeringingsskjermen lukkes automatisk.

6.3.5 MNO-støtte

6.3.5.1 Ring med Native Dialer

Denne funksjonen legger til støtte for MNO-distribusjoner (Mobile Network Operator) som utnytter tjenesten BroadWorks Mobility (BWM). Det antas at brukeren har BroadWorks Mobilitetstjenesten tilordnet dem og har minst ett sted konfigurert.

Brukerens evne til å starte anrop gjennom den opprinnelige oppringeren kontrolleres av den **native** konfigurasjonskoden. Hvis aktivert, vil applikasjonen starte den opprinnelige oppringeren og ringe. Videre kontrolleres tilgjengeligheten av VoIP-anrop av **voip** -taggen – basert på implementeringskravene VoIP-anrop kan aktiveres eller deaktiveres.

Hvis VoIP og Native calling er aktivert, vil brukeren kunne velge hvilket alternativ som skal brukes.

<dialing-mode> -taggen kontrollerer om brukere kan velge hvordan innkommende og utgående anrop skal startes/mottas. Krever at både det opprinnelige og VoIP-anropet er aktivert.

Fra og med Utgivelse 43.12 utvides den opprinnelige oppringingskonfigurasjonen, noe som gir muligheten til et egendefinert prefiks som kan forhåndsstilles til det utgående anropsnummeret. Dette gjelder mobilanrop som startes fra Webex appen, bare hvis nummeret som slås starter med en FAC-kode.

Denne funksjonen er nyttig for kunder som bruker MNO-distribusjoner, der anrop i stedet for å bli omdirigert til den integrerte BroadWorks Cisco-programserveren, kan FAC-kodene håndteres av Telecom-motoren. Ny <fac-prefix> tag er lagt til under seksjon <dialing><native> og telekom kan bruke den til å løse dette problemet.

Konfidensiell Cisco

```
<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%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DIALING_VOIP_WXT%	sant	sann, usann	Sett til "true" for å aktivere VoIP-anropsalternativ.
%ENABLE_DIALING_NATIVE_WXT%	feil	sann, usann	Satt til «sann» for å aktivere alternativet Opprinnelig samtale.
%ENABLE_DIALING_MODE_WXT%	feil	sann, usann	Aktiverer valg av anropsmodus av brukeren gjennom samtaleinnstillingene i innstillingene.
%DIALING_MODE_DEFAULT_WXT%	voip	voip, innfødt	Angir standard anropsmodus som er valgt.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	feil	sann, usann	Kontrollerer om tilgjengeligheten av det opprinnelige anropet skal avhenge av at BroadWorks Mobilitetstjenesten og Mobilitetsplasseringen er konfigurert for brukeren.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*tomt*	streng	Angir et prefiks som skal settes foran hvis utgående anrop til et nummer som starter med en FAC-kode startes som et mobilanrop. Som standard er ingen FAC-prefiks definert og taggen er tom.

MERKNAD 1: Minst ett av **voip** og **native** -anrop bør være aktivert.

MERK 2: Hvis bare det **native** anropet er aktivert, i MNO-implementeringer, anbefales det å deaktivere enkeltvarslingen for å forhindre at klienten deaktiverer BWM-varslingen.

MERK 3: Hvis både **native** og **voip** -anrop er aktivert, i MNO-distribusjoner, anbefales det å aktivere enkeltvarsling for å forhindre dobbeltvarsling.

6.3.5.2 Kontroller midt i samtalen

Denne funksjonen gjør det mulig for Webex mobilklienten å kontrollere via XSI innebygde anrop på mobilenheten som er forankret på Cisco BroadWorks. XSI Call Controls er kun tilgjengelig hvis:

- BroadWorks Mobilitetstjenesten (BWM) er tilordnet brukeren,
- Det er bare en enkelt BMW Mobile Identity konfigurert,
- Native anropsmodus velges av brukeren (for mer informasjon se avsnitt *6.3.5.1 Ring med Native Dialer),*

Konfidensiell Cisco

- Det er en samtale forankret på BroadWorks, som går gjennom BMW-tjenesten,
- Det er pågående mobilanrop på mobilenheten.

Utgivelse 43.10 legger til bedre håndtering av den rådgivende overføringen, oppretter sammenheng mellom de to mobilsamtalene som presenteres i Webex appen og gir brukeren et alternativ for å fullføre overføringen. Dessuten, hvis brukeren har to uavhengige mobilanrop på samme enhet, forbedres overføringsmenyen for å tillate overføring av den ene til den andre selv om det ikke er opprettet noen tilknytning mellom dem.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_XSI_CALL_CONTROL_WXT%	feil	sann, usann	Aktiverer XSI-anropskontroll for MNO-miljø.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Tilgang	MNO_Access, MNO_Nettverk	Kontrollerer XSI MNO-distribusjonstypen som brukes av applikasjonen. Mulige verdier er: ▪ MNO_Access – viser alle eksterne (XSI) anrop med enhetstypene definert i noden nedenfor. ▪ MNO_Network - viser alle eksterne (XSI) anrop.
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	streng	Enhetstypenavnet(e) som skal brukes i MNO_Access-distribusjonstypen.
%ENABLE_XSI_HOLD_CALLS_WXT%	sant	sann, usann	Kontrollerer om handlingen Hold samtale skal være tilgjengelig for brukeren for XSI-mobilanrop.

6.3.5.3 Identitet for utgående anropslinje (CLID) – Dual Persona

Med Mobile Release 42.12 lar Webex appen brukere velge Calling Line Identity (CLID) presentert for den eksterne parten når de starter en utgående samtale.

Hvis brukeren er konfigurert med Cisco BroadWorks Mobility, typisk konfigurasjon for MNO-distribusjoner (Mobile Network Operator) og integrert anrop er aktivert, kan brukeren velge hvilken identitet som skal presenteres for personene de ringer. Brukeren kan velge sin forretnings- eller personlige identitet. Det er også en mulighet for å skjule egen identitet og oppfordringen for å bli presentert som anonym.

For VoIP-samtaler har brukeren også en mulighet til å kontrollere sin CLID. Det tilgjengelige alternativet i dette tilfellet er kun å kontrollere om identiteten hans skal skjules eller ikke.

Konfidensiell Cisco

Personaadministrasjon og CLID-blokkering kontrolleres gjennom separate konfigurasjonsalternativer.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	feil	sann, usann	Aktiverer leveringsblokkering av anrops-ID. Det gjelder alle utgående typer samtaler for brukeren.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	feil	sann, usann	Aktiverer personlig administrasjon for opprinnelige samtaler når distribusjonstypen er konfigurert som MNO_Access eller MNO_Network. (BroadWorks Mobilitet brukes for opprinnelige samtaler, og alle opprinnelige samtaler er forankret på BroadWorks)

6.3.5.4 Varsling for innfødte anrop

For brukere som er distribuert med MNO, legger denne funksjonen til et varslingsbanner for innfødte anrop, som kan kontrolleres gjennom Webex appen. Denne varslingen er avhengig av push-varsling, sendt av applikasjonsserveren når samtalen er opprettet.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	sant	sann, usann	Aktiverer abonnementet for MOBILE_CALL_INFO push-varsling.

6.3.5.5 Flytt Native Call til Converged Meeting

For brukere som er distribuert med MNO, gjør denne funksjonen det mulig å eskalere et innfødt taleanrop til et møte for begge parter i en 1:1-samtale (selv om den andre parten ikke er en Webex bruker). Hvis den eksterne brukeren er en Webex bruker, vil partene en gang i et møte ha muligheten til å:

- Start Webex i Meeting Chat
- Legg til video (merk at lyden fortsetter i den opprinnelige samtalen)
- Del skjerm/innhold
- Trigger Meetings-opptak

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	feil	sann, usann	Aktiverer oppstart (inviter og møt, videomøtehandlinger).

6.3.5.6 MNO Mobility - modul for samtale

Utgivelsen 43.7 av Android-appen Webex (mobil og nettbrett) introduserer offisielt en ny samtalekontroll (boble), som gir ekstra samtalekontroll for opprinnelige samtaler forankret på Cisco BroadWorks, ved hjelp av Mobility-tjenesten. Widgeten vil vises på toppen av det opprinnelige brukergrensesnittet og vil tillate brukeren følgende handlinger:

- Vent/fortsett
- Blind/konsultativ overføring – plasserer brukeren i overføringsdialogen i Webex appen.
- Fullfør overføring – gir muligheten til å fullføre konsultasjonsoverføring (versjon 43.10)
- Videomøte – flytter partene til et Webex møte.
- Avslutt samtale

```
<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%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_WIDGET_HOLD_CALLS_WXT%	sant	sann, usann	Kontrollerer tilgjengeligheten til handlingen Hold i anropsmodulen.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	sant	sann, usann	Kontrollerer tilgjengeligheten av Overføring og Fullfør overføring -handlingene i samtalewidgeten.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	sant	sann, usann	Kontrollerer tilgjengeligheten av handlingen Videomøte i samtalewidgeten.

Konfidensiell Cisco

6.3.6 Innkommende innringer-ID

Release 44.2 legger til muligheten til å kontrollere kontaktinformasjonen som presenteres for brukeren basert på navn og nummer. Det er lagt til to konfigurasjonsalternativer for å kontrollere informasjonen som presenteres for brukeren på skjermen for innkommende anrop og varsling om innkommende anrop, og varslene om tapt anrop.

6.3.6.1 Skjerm for innkommende anrop

Det er plattformforskjeller mellom Android og iOS når det gjelder å vise data på skjermen for innkommende anrop. Den opprinnelige opplevelsen av å vise informasjon for innkommende anrop er som følger:

- Android – det er to separate felt på skjermen for innkommende anrop for å vise både navn og nummer
- iOS – det er bare ett felt å vise enten navnet eller nummeret – hvis begge er tilgjengelige, prioriteres navnet

Det nye konfigurasjonsalternativet for innkommende anrop kan brukes til å sikre at iOS-appen Webex viser nummeret på samtaleskjermen ved siden av navnet (format: *Navn (nummer)*). Atferden til Webex Android-appen påvirkes ikke.

6.3.6.2 Varsel om innkommende samtale

I noen tilfeller blir det innkommende anropet presentert for brukeren som et varsel. På grunn av begrenset plass vises ikke alltid nummeret der.

Det nye konfigurasjonsalternativet for innkommende anrop kontrollerer også informasjonen som vises i varslene om innkommende anrop. Hvis aktivert og både navnet og nummeret er tilgjengelig, vil Webex appen legge til nummeret ved siden av navnet (format: *Navn (nummer)*). Dette er atferden til Webex appen gjelder både for Android og iOS.

6.3.6.3 Varsel om tapt anrop

Det er lagt til en ekstra konfigurasjonsparameter for varslene om tapt anrop. Den kan brukes til å kontrollere informasjonen om den eksterne parten, i likhet med varslene om innkommende anrop, slik at nummeret kan legges til visningsnavnet til den eksterne brukeren og presenteres i varselet om tapt anrop. Dette er atferden til Webex appen gjelder både for Android og 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>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	feil	sann, usann	Kontrollerer om nummeret skal legges til navnet på skjermen for innkommende anrop (kun iOS) og varsler.

Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	feil	sann, usann	Kontrollerer om nummeret skal legges til navnet i det tapte anropsvarselet.

merk: Hvis nummeret leveres som et visningsnavn eller visningsnavnet slutter med nummeret, vil Webex appen unngå duplisering og viser nummeret bare én gang.

6.4 Personlig assistent (borte tilstedeværelse)

Med utgivelse 44.11 legger mobilappen til Webex integrasjon med Cisco BroadWorks Personal Assistant (PA)-tjenesten. Den fungerer i kombinasjon med brukerens Borte-tilstedeværelse og krever synkronisering av PA-statusen med Webex Cloud-tilstedeværelse.

PA-tjenesten gir brukeren en mulighet til å informere de som ringer om årsaken til at den oppringte parten ikke er tilgjengelig, og gir valgfritt informasjon om når den oppringte parten vil returnere og om det er en telefonist til å håndtere samtalen.

Hvis PA er aktivert, vil alternativet Bortetilstedeværelse være tilgjengelig for brukeren. Den kan brukes til å konfigurere PA på Ciscos BroadWorks side. Når funksjonen er aktivert, vil brukere se brukerens Borte-tilstedeværelse i kombinasjon med PA-status og konfigurert varighet.

Brukeren kan kun konfigurere den manuelle PA-konfigurasjonen. Hvis det er noen tidsplaner som påvirker PA-tjenesten, vil tilstedeværelsen oppdateres gjennom Personal Assistant Status Sync. Webex -appen viser imidlertid ikke tidsplankonfigurasjonen og tidsplanene som påvirker PA.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	sann, usann	Kontrollerer om funksjonen Bortetilstedeværelse er tilgjengelig for brukeren.

MERKNAD 1: Denne funksjonen krever at Personal Assistant Status Sync er aktivert fra Partner Hub.

MERKNAD 2: Funksjonen er ennå ikke tilgjengelig for skrivebordsversjonene av Webex appen. Likevel vil Bortetilstedeværelsen vises riktig uten tilleggsopplysningene om personlig assistent.

MERK 3: Standard samtaleruting for personlig assistent trer ikke i kraft mens DND, Viderekobling alltid eller Selektive tjenester for viderekobling av anrop er aktive.

Konfidensiell Cisco

MERKNAD 4: De manuelle Tilstedeværelsestilstandene Ikke forstyrr og Opptatt har høyere prioritet sammenlignet med Borte. Når brukerhåndboken aktiverer en av disse tilstedeværelsesstatusene, vil ikke aktivering av Personal Assistant føre til at tilstedeværelsesstatusen endres til Borte.

Konfidensiell Cisco

7 Funksjoner for tidlig feltprøve (BETA).

7.1 AI kodek

Fra og med Release 44.8, Webex introduserer appen støtte for en ny lydkodek – AI Codec (xCodec). Denne lydkodeken brukes under ugunstige nettverksforhold for å oppnå bedre samtalekvalitet. Webex Mediemotoren i Webex appen sjekker enhetens funksjoner, sporer mediekvaliteten og AI-kodeken kan brukes hvis den støttes og er aktivert gjennom konfigurasjonsfilen.

AI-kodeken fungerer bare i kombinasjon med Opus-kodeken. Dette betyr at både Opus og AI Codec bør annonseres og forhandles av begge sider under SDP-forhandlingene.

```
<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"/>
```

MERK: For å prøve denne funksjonen, vennligst kontakt BETA-teamet for ytterligere funksjonsaktivering. AI-kodeken vil ikke bli annonsert og brukt før det er tillatt av BETA-teamet.

7.2 Flerlinje for mobil (Webex Calling kun)

Utgivelse Webex Calling bare for distribusjon 44.11 legger til støtte for flere linjer (delt og virtuell) i mobilversjonen av Webex appen. Tilordning av flere linjer for brukeren er nå tilgjengelig i skrivebords- og Webex mobilappen – brukeren kan ha en primærlinje og opptil 9 sekundære linjer.
På grunn av spesifikasjonene til den mobile plattformen, kan brukeren ha opptil to samtidige samtaler samtidig på hvilken som helst av linjene.

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


Konfidensiell Cisco

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_MULTI_LINE_WXT%	feil	sann, usann	Aktiverer støtte for flere linjer (hvis konfigurert). Hvis deaktivert (sett til "false"), vil bare den første konfigurerte linjen bli brukt av applikasjonen.

MERKNAD 1: Hvis anropsmodus er aktivert (se *6.3.5.1 Ring med Native Dialer*), er flerlinjer deaktivert.

MERK 2: Multi-line for nettbrett-versjonen støttes ikke.

Konfidensiell Cisco

8 Egendefinerte tagger tilordning mellom Webex for Cisco BroadWorks og UC-One

Tabellen nedenfor viser egendefinerte koder Webex for CiscoBroadWorks , samsvarer med deres eldre egendefinerte koder for UC-One.

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	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_PARTICIPANT_LIST_DESKTOP%	N/A
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	N/A
%ENABLE_CALL_STATISTICS_WXT%	N/A	N/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_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	N/A	N/A
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	N/A
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	N/A
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	N/A
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_WXT%	N/A	N/A

Konfidensiell Cisco

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	Mobile Legacy Tag
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	N/A	N/A
%ENABLE_EMERGENCY_DIALING_WXT%	N/A	N/A
%EMERGENCY_DIALING_NUMBERS_WXT%	N/A	N/A
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	N/A	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	N/A
%SBC_ADDRESS_WXT%	%SBC_ADDRESS%	%SBC_ADDRESS%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILE%
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	N/A
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	N/A

Konfidensiell Cisco

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	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%

Konfidensiell Cisco

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	Mobile Legacy Tag
%ENABLE_CALLS_AUTO_ RECOVERY_WXT%	N/A	%ENABLE_CALLS_AUTO_ RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_ SEQUENCE_WXT%	N/A	%EMERGENCY_CALL_DIAL_ SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLI ND_WXT%	N/A	N/A
%ENABLE_CALL_PICKUP_ DIRECTED_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_URL _WXT%	N/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_TAR GET_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_CFA _ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFA _VISIBLE%
%WEB_CALL_SETTINGS_DN D_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_DN D_VISIBLE%
%WEB_CALL_SETTINGS_AC R_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_AC R_VISIBLE%
%WEB_CALL_SETTINGS_CFB _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFB _VISIBLE%
%WEB_CALL_SETTINGS_CFN R_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFN R_VISIBLE%
%WEB_CALL_SETTINGS_CFN A_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFN A_VISIBLE%
%WEB_CALL_SETTINGS_SIM RING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SIM RING_VISIBLE%
%WEB_CALL_SETTINGS_ SEQRING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SE QRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_RO_ VISIBLE%
%WEB_CALL_SETTINGS_ACB _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_ACB _VISIBLE%
%WEB_CALL_SETTINGS_CW _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CW _VISIBLE%
%WEB_CALL_SETTINGS_CLI DB_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CLI DB_VISIBLE%
%WEB_CALL_SETTINGS_PA_ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_PA_ VISIBLE%

Konfidensiell Cisco

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	Mobile Legacy Tag
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_BWA_VISIBLE%
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	N/A	%WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE%
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_BWM_VISIBLE%
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_VM_VISIBLE%
%ENABLE_DIALING_CALL_BACK_WXT%	N/A	N/A
%DIALING_CALL_BACK_TIMER_WXT%	N/A	N/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%	N/A	N/A
%ENABLE_RTP_ICE_WXT%	N/A	N/A
%RTP_ICE_MODE_WXT%	N/A	N/A
%RTP_ICE_SERVICE_URI_WXT%	N/A	N/A
%RTP_ICE_PORT_WXT%	N/A	N/A
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	N/A	N/A
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/A	N/A
%ENABLE_DIALING_VOIP_WXT%	N/A	N/A
%ENABLE_DIALING_NATIVE_WXT%	N/A	N/A
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	N/A	N/A
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	N/A	N/A

Konfidensiell Cisco

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	Mobile Legacy Tag
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	N/A	N/A
%USER_PORTAL_SETTINGS_URL_WXT%	N/A	N/A
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	N/A	N/A
%ENABLE_AUDIO_MARI_FEC_WXT%	N/A	N/A
%ENABLE_AUDIO_MARI_RTX_WXT%	N/A	N/A
%ENABLE_VIDEO_MARI_FEC_WXT%	N/A	N/A
%ENABLE_VIDEO_MARI_RTX_WXT%	N/A	N/A
%ENABLE_CALL_BLOCK_WXT%	N/A	N/A
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N/A	N/A
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N/A	N/A
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/A	N/A
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	N/A	N/A
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	N/A	N/A
%ENABLE_CALL_MOVE_HERE_WXT%	N/A	N/A
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	N/A	N/A
%DIALING_NATIVE_FAC_PREFIX_WXT%	N/A	N/A
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	N/A	N/A
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	N/A	N/A
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N/A	N/A

Konfidensiell Cisco

Webex for Cisco BroadWorks Merkelapp	Legacy tag for skrivebord	Mobile Legacy Tag
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N/A	N/A
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	N/A	N/A
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	N/A
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	N/A
%BLF_NOTIFICATION_DELAY_TIME_WXT%	N/A	N/A
%ENABLE_GCP_NOTIFICATIONS_WXT%	N/A	N/A
%ENABLE_GCP_DISPLAY_CALLER_WXT%	N/A	N/A
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	N/A	N/A
%UDP_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%TCP_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%TLS_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N/A	N/A

Konfidensiell Cisco

merk: N/A indikerer at det ikke var noen tilsvarende egendefinert tag som kontrollerte funksjonen i UC-One. Å ha N/A for både eldre skrivebords- og mobilkoder indikerer at koden Webex for CiscoBroadWorks er ny og kontrollerer enten ny funksjonalitet eller en eksisterende funksjon, som ikke ble kontrollert gjennom en egendefinert kode i UC-One.

Konfidensiell Cisco

9 Vedlegg A: TLS-chifre

Webex for BroadWorks klienten bruker CiscoSSL, som er basert på OpenSSL med ekstra sikkerhetsforsterkning.

Konfidensiell Cisco

10 Vedlegg B: DM Tag Provisioning Script

Antallet tilpassede DM-tagger har økt med hver utgivelse, ettersom mange kunder foretrekker tagger for de nye konfigurasjonsparametrene. For å tilby mekanismer for enklere klargjøring av de tilpassede DM-taggene, inneholder denne delen et skript som kan kjøres på Application Server (AS)-siden for å tilordne verdier til de tilpassede DM-taggene. Dette skriptet er spesielt ment for nye distribusjoner der de fleste tilpassede DM-taggene er ment å brukes.

Merk at dette skriptet bare er gyldig for nye distribusjoner der tilpassede DM-tagger opprettes. For å endre eksisterende tilpassede DM-tagger, må kommandoen i følgende skript endres fra "legg til" til "sett".

Skriptmal med bare noen få tilpassede tagger satt (i en reell distribusjon må du fylle ut en større liste over egendefinerte tagger). Merk at følgende eksempel er for mobil. For datamaskiner, bruk BroadTouch_tags-tagsettet i stedet for Connect_Tags. For nettbrett, bruk ConnectTablet_Tags-tagsettet i stedet for 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
%% ----------------------------------------------------------------------------------------------------------------
quit all;System;DeviceTagSet;Tags
get tagSetName Connect_Tags
quit all
```


Konfidensiell Cisco

Følgende viser alle egendefinerte tagger som brukes av Webex for Cisco BroadWorks, med eksempelverdier (standard eller anbefalt). Merk at noen av taggene krever verdier som er spesifikke for den tilsvarende distribusjonen (som serveradresser). Det er grunnen til at disse kodene legges til på slutten av skriptet, men står tomme, og flere settkommandoer bør legges til for å spesifisere dem.

10.1 Stasjonær PC

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


Konfidensiell Cisco

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


Konfidensiell Cisco

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

10.2 Mobil

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


Konfidensiell Cisco

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


Konfidensiell Cisco

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


Konfidensiell Cisco

```
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
```

10.3 Nettbrett

```
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
```


Konfidensiell Cisco

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


Konfidensiell Cisco

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


Konfidensiell Cisco

```
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
```

10.4 Systemkoder

Følgende viser systemkodene som brukes av Webex for BroadWorks.

```
%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%
```


Konfidensiell Cisco

%BWE911-EMERGENCY-NUMBER-LIST%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%

Konfidensiell Cisco

11 Akronymer og forkortelser

Denne delen viser akronymene og forkortelsene som finnes i dette dokumentet. Akronymene og forkortelsene er oppført i alfabetisk rekkefølge sammen med deres betydninger.

ACB	Automatisk tilbakeringing
ACD	Automatisk samtaledistribusjon
ACR	Avvisning av anonymt anrop
AES	Avansert krypteringsstandard
ALG	Gateway for programlag
API	Grensesnitt for programmering
APK	Søknadspakke
APNS	Apple Push-varslingstjeneste
ARS	Automatisk bithastighetsvalg
AS	Programserver (Cisco BroadWorks)
AVP	Visuell lydprofil
BW	BroadWorks
BWA	BroadWorks Hvor som helst
BWKS	BroadWorks
BWM	BroadWorks Mobilitet
BYOD	Ta med din egen enhet
CC	Anropssenter
CFB	Viderekobling av anrop opptatt
CFNA	Viderekobling uten svar
CFNR	Kan ikke viderekoble anrop
CIF	Felles mellomformat
CLI	Kommandolinjegrensesnitt
CLID	Oppringingslinjeidentitet
CLIDB	Blokkering av levering av ringelinje-ID
CRLF	Transportreturlinjefeed
CS	Kretskortssviktet
CSWV	Nettvisning for samtaleinnstillinger
CW	Samtale venter
DB	Database
DM	Enhetshåndtering
DND	Ikke forstyrr
DNS	Domenenavn System

Konfidensiell Cisco

DPC	Telefonkontroll for skrivebord
DTAF	Arkivfil for enhetstype
ECACS	Tjeneste for endring av adresse for nødanrop
FMC	Fast-mobil konvergens
FQDN	Fullt kvalifisert domenenavn
HMAC	Autentiseringskode for hash-melding
ICE	Etablering av interaktiv tilkobling
iLBC	Internett-kodek med lav bitrate
IM	Direktemeldinger
IM&P	Direktemeldinger og tilstedeværelse
IOT	Interoperabilitetstesting
IP	Internett-protokoll
JID	Jabber Identifikator
M/O	Obligatorisk/valgfritt
MNO	Operatør av mobilnettverk
MTU	Maksimal overføringsenhet
MUC	Chat med flere brukere
MWI	Melding venter-indikator
NAL	Nettverksabstraksjonslag
NAPTR	Pekeren for navngivning av myndighet
NAT	Oversettelse av nettverksadresse
OTT	Over toppen
PA	Personlig assistent
PAI	P-bekreftet identitet
PEM	P-tidlige medier
PLI	Indikasjon på bildetap
PLMN	Offentlig land mobilnettverk
PN	Push-varsel
QCIF	Kvartalsvise mellomliggende format
QoS	Tjenestekvalitet
RO	Eksternt kontor
RTCP	Kontrollprotokoll i sanntid
RTP	Sanntidsprotokoll
SaaS	Programvare som tjeneste
SAN	Alternativt navn for emne
SASL	Enkelt godkjennings- og sikkerhetslag

Konfidensiell Cisco

SAVP	Sikker lyd-videoprofil
SBC	Grensekontroller for økt
SCA	Utseende for delt samtale
SCF	Øktkontinuitet
SCTP	Overføringsprotokoll for strømkontroll
SDP	Protokoll for øktdefinisjon
SEQRING	Sekvensiell ringing
SIMRING	Samtidig ringing
SIP	Protokoll for øktinitiering
SNR	Signal- til støyforhold
SNR	Single Number Reach
SRTCP	Sikker kontrollprotokoll i sanntid
SRTP	Sikker transportprotokoll i sanntid
SSL	Lag for sikre kontakter
STUN	Verktøy for økttraversering for NAT
SUBQCIF	Underkvartal CIF
TCP	Protokoll for overføringskontroll
TLS	Sikkerhet for transportlag
TTL	På tide å leve
TURN	Traversering ved hjelp av relé NAT
UDP	Brukerdatagram-protokoll
UI	Brukergrensesnitt
UMS	Meldingsserver (Cisco BroadWorks)
URI	Id for ensartet ressurs
UVS	Videoserver (Cisco BroadWorks)
VGA	Grafikkmatrise for video
VoIP	Tale over IP
VVM	Visuell talepost
WXT	Webex
XMPP	Utvidbar meldings- og tilstedeværelsesprotokoll
XR	Utvidet rapport
Xsp	Xtended Services-plattform
Xsi	Grensesnitt for Xtended-tjenester

Konfidensiell Cisco