Konfigurasjonsveiledning for Webex for Cisco BroadWorks

Versjon 45.4

Dokument versjon 1

Innholdsfortegnelse

1 Sammendrag av endringer 1
1.1 Endringer for versjon 45.4, april 2025 1
1.2 Endringer for versjon 45.3, mars 2025 1
1.3 Endringer for versjon 45.2, februar 2025 1
1.4 Endringer for versjon 45.1, januar 2025 1
1.5 Endringer for versjon 44.12, desember 2024 1
1.6 Endringer for versjon 44.11, november 2024 1
1.7 Endringer for versjon 44.10, oktober 2024 1
1.8 Endringer for versjon 44.9, september 2024 1
1.9 Endringer for versjon 44.8, august 2024 2
1.10 Endringer for versjon 44.7, juli 2024 2
1.11 Endringer for versjon 44.6, juni 2024 2
1.12 Endringer for versjon 44.5, mai 2024 2
1.13 Endringer for versjon 44.4, april 2024 2
1.14 Endringer for versjon 44.3, mars 2024 2
1.15 Endringer for versjon 44.2, februar 2024 2
1.16 Endringer for versjon 44.1, januar 2024 3
2 Endringer for konfigurasjonsfiler 4
2.1 Endringer for konfigurasjonsfiler for versjon 45.4 4
2.2 Endringer for konfigurasjonsfiler for versjon 45.3 4
2.3 Endringer for konfigurasjonsfiler for versjon 45.2 4
2.4 Endringer for konfigurasjonsfiler for versjon 45.1 4
2.5 Endringer for konfigurasjonsfiler for versjon 44.12 4
2.6 Endringer for konfigurasjonsfiler for versjon 44.11 4
2.7 Endringer for konfigurasjonsfiler for versjon 44.10 5
2.8 Endringer for konfigurasjonsfiler for versjon 44.9 5
2.9 Endringer for konfigurasjonsfiler for versjon 44.8 5
2.10 Endringer for konfigurasjonsfiler for versjon 44.7 5
2.11 Endringer for konfigurasjonsfiler for versjon 44.6 6
2.12 Endringer for konfigurasjonsfiler for versjon 44.5 6
2.13 Endringer for konfigurasjonsfiler for versjon 44.4 6
2.14 Endringer for konfigurasjonsfiler for versjon 44.3 6
2.15 Endringer for konfigurasjonsfiler for versjon 44.2 7
2.16 Endringer for konfigurasjonsfiler for versjon 44.1 9
3 Introduksjon 10
4 Installasjon 11
4.1 Lokalisert klientnedlasting 11
4.2 Android-klient 11
4.3 iOS-klient 11

Cisco konfidensielt

4.4 Desktop-klient ... 11
5 Enhetsadministrasjon ... 13
5.1 Koder for enhetsbehandling ... 13
5.2 Forbedringer av delvis samsvar for valg av enhetstype ... 14
5.3 Klient konfigurasjon ... 15
5.4 Distribusjon av config-wxt.xml ... 15
5.5 Konfigurasjonsfil (config-wxt.xml) ... 15
5.6 Standardkoder for system ... 16
5.7 Cisco BroadWorks dynamisk innebygd system Tags ... 16
6 Egendefinerte merker ... 19
6.1 Fellestrekk ... 31
6.1.1 SIP-serverinnstillinger ... 31
6.1.2 SIP Over TLS og Secure Real-time Transport Protocol ... 34
6.1.3 3GPP SIP-hoder for SRTP ... 36
6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives ... 37
6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-kontakt ... 38
6.1.6 Dynamisk SIP-proxy-oppdagelse ... 39
6.1.7 Foretrukket portbruk for SIP ... 44
6.1.8 SIP-failover og failback ... 45
6.1.9 SIP SUBCSRIBE og REGISTRER Oppdater og abonner Prøv på nytt ... 49
6.1.10 Bruk P-Associated-URIer i REGISTER ... 50
6.1.11 PEM-topptekst (SIP P-Early Media) ... 50
6.1.12 Støtte for SIP-OPPDATERING ... 51
6.1.13 Eldre SIP-INFO FIR ... 51
6.1.14 SIP rport-behandling for NAT-traversering ... 52
6.1.15 SIP-økt-ID ... 53
6.1.16 Virkemåte for avvisning av innkommende anrop ... 53
6.1.17 Portområde for transportprotokoll i sanntid ... 53
6.1.18 ICE-støtte (kun Webex Calling) ... 54
6.1.19 RTCP MUX ... 55
6.1.20 Overføre samtaler ... 55
6.1.21 N-veis konferansesamtaler og deltakere ... 56
6.1.22 Trekk anrop ... 57
6.1.23 Parker/hent anrop ... 58
6.1.24 Anropsstatistikk ... 58
6.1.25 Automatisk gjenoppretting av anrop / Sømløs overlevering av samtale ... 59
6.1.26 Call Recording (Innspilling av samtale) ... 59
6.1.27 Talepost, Visuell talepost, Indikator for Melding venter ... 60
6.1.28 Transkripsjon av talepost for Webex Calling ... 62
6.1.29 Samtaleinnstillinger ... 62
6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger ... 65

Cisco konfidensielt

6.1.31 Call Center / Call Queue Login / Logg ut ... 68
6.1.32 XSI-rot og stier ... 68
6.1.33 XSI-hendelseskanal ... 69
6.1.34 Konfigurasjon av kodek ... 70
6.1.35 SIP-URI-oppringing ... 72
6.1.36 Anropslogg på tvers av alle enheter ... 73
6.1.37 Deaktiver videoanrop ... 73
6.1.38 Nødanrop (911) - Posisjonsrapportering med E911-leverandør ... 74
6.1.39 PAI som identitet ... 75
6.1.40 Deaktiver skjermdeling ... 76
6.1.41 Spam Call Indication ... 76
6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN-/mobilsamtaler ... 76
6.1.43 QoS-DSCP-merking ... 77
6.1.44 Primær profil ... 78
6.1.45 Blokkeringsliste (bare Webex Calling) ... 79
6.1.46 Implementering av medietilpasning og resiliens (MARI) ... 80
6.1.47 Samtidige samtaler med samme bruker ... 82
6.1.48 RTCP-XR ... 83
6.1.49 Informasjon om viderekobling av anrop ... 83
6.1.50 Oppringer-ID ... 83
6.1.51 Flere linjer ... 86
6.1.52 Forbedret SIP-autorisasjon ... 87
6.1.53 Personlig assistent (tilstedeværelse borte) ... 88
6.2 Funksjoner bare for skrivebord ... 90
6.2.1 Tvungen utlogging ... 90
6.2.2 Samtalehenting ... 90
6.2.3 Støtte for Boss-Admin (Executive-Assistant) ... 91
6.2.4 Eskalere SIP-anrop til møte (kun Webex Calling) ... 92
6.2.5 Bordtelefonkontrollanrop - Automatisk svar ... 92
6.2.6 Automatisk svar med tonevarsling ... 93
6.2.7 Bordtelefonkontroll - Mid Call Controls - Konferanse ... 93
6.2.8 Varsler om henting av anrop ... 93
6.2.9 Hendelsespakke for fjernkontroll ... 95
6.2.10 Valg av CLID for agentanrop ... 96
6.2.11 Overlevelsesgateway (kun Webex Calling) ... 96
6.2.12 Hendelsespakke for ekstern demping (kun Webex Calling) ... 97
6.2.13 Flytt samtale ... 97
6.3 Funksjoner kun for mobil ... 99
6.3.1 Nødanrop ... 99
6.3.2 Push-varsler for samtaler ... 100
6.3.3 Enkel varsling ... 102
6.3.4 Klikk for å ringe (ring tilbake) ... 102

Cisco konfidensielt

6.3.5 MNO-støtte 103
6.3.6 Innkommende anroper-ID 108
7 Funksjoner for tidlig prøveversjon (BETA) 110
8 Egendefinerte koder Tilordning mellom Webex for Cisco BroadWorks og UC-One 111
9 Vedlegg A: TLS chiffer 119
10 Vedlegg B: DM Tag Provisioning Script 120
10.1 Skrivebord 121
10.2 Mobiltelefon 124
10.3 Tavle 126
10.4 System Tags 130
11 Akronymer og forkortelser 131

Cisco konfidensielt

1 Sammendrag av endringer

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

1.1 Endringer for versjon 45.4, april 2025

Denne versjonen av dokumentet inneholder følgende endringer:

- Flyttet seksjon *6.1.34.1 AI-kodek* - ut av BETA.
- Lagt til seksjon *6.1.51 Flere* linjer - kombinerte de stasjonære og mobile BETA-seksjonene.
- Flyttet seksjon *6.1.52 Forbedret SIP-autorisasjon* - ut av BETA.
- Flyttet inndeling *6.1.53 Personlig assistent (tilstedeværelse borte)* som vanlig for stasjonær og mobil

1.2 Endringer for versjon 45.3, mars 2025

Det var ingen endringer i dette dokumentet for denne utgivelsen.

1.3 Endringer for versjon 45.2, februar 2025

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til seksjon *Forbedret SIP-autorisasjon**Error! Reference source not found.*** i BETA.

1.4 Endringer for versjon 45.1, januar 2025

Denne versjonen av dokumentet inneholder følgende endringer:

- Flyttet delen *Personlig assistent (tilstedeværelse borte)* ut av BETA.
- Flyttet delen *6.3.2.3 Leveringsmåte (bare Webex Calling)* ut av BETA.

1.5 Endringer for versjon 44.12, desember 2024

Det var ingen endringer i dette dokumentet for denne utgivelsen.

1.6 Endringer for versjon 44.11, november 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til seksjon *Mobil (bare Webex Calling)* i BETA.

1.7 Endringer for versjon 44.10, oktober 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til seksjon *Personlig assistent (tilstedeværelse borte)* i BETA***Error! Reference source not found.***.
- Lagt til seksjon *Leveringsmåte (bare Webex Calling)* i BETA.

1.8 Endringer for versjon 44.9, september 2024

Det var ingen endringer i dette dokumentet for denne utgivelsen.

Cisco konfidensielt

1.9 Endringer for versjon 44.8, august 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert del *6.1.34 Konfigurasjon av* kodek – lagt til avklaring om DTMF-er og støttede leveringsmekanismer.

1.10 Endringer for versjon 44.7, juli 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til seksjon *AI-kodek* i BETA.
- Oppdatert del *6.1.44 Primærprofil* – fjernet detaljer om Webex appens virkemåte før versjon 43.2.

1.11 Endringer for versjon 44.6, juni 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert seksjon *6.3.6. Innkommende anroper-ID* – Lagt til flere detaljer om den opprinnelige opplevelsen og hvordan funksjonen fungerer.

1.12 Endringer for versjon 44.5, mai 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert seksjon *6.1.18 ICE-støtte (kun Webex Calling)* - lagt til IPv6-støtte via NAT64.
- Oppdatert seksjon *6.1.50 Oppringer-ID* - lagt til underavsnitt *6.1.50.2 Navn på ekstern anroper-ID*.

1.13 Endringer for versjon 44.4, april 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert seksjon *6.1.50.1 ID for utgående* anroper.
- Oppdatert seksjon *Endringer for konfigurasjonsfiler for versjon 44.3* – lagt til detaljer om KeepAlive-oppdateringene i 44.3.

1.14 Endringer for versjon 44.3, mars 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Oppdatert seksjon *6.3.6. Innkommende anroper-ID*
    - Flyttet seksjon *6.1.50.1 ID for utgående* anroper som vanlig for stasjonær og mobil, og oppdaterte den med flere detaljer.
- Oppdatert seksjon *6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives* - lagt til detaljer om de konfigurerbare keepalives ved hjelp av egendefinerte koder.

1.15 Endringer for versjon 44.2, februar 2024

Denne versjonen av dokumentet inneholder følgende endringer:

- Lagt til seksjon *6.3.6 Innkommende anroper-ID*

Cisco konfidensielt

- Oppdatert seksjon *6.2.8 Varsler om henting* av anrop
  - Lagt til underavsnitt *6.2.8.1 Opptattlampefelt* - flyttet BLF detaljer i den.
  - Lagt til underavsnitt *6.2.8.2 Hentegruppe for anrop (bare Webex Calling)*.
- Lagt til seksjon *6.1.49 Informasjon om viderekobling* av anrop.
- Oppdatert seksjon *6.1.8.3 Håndheve 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 støtten for båndbreddeutvidelse og oppdateringene for støyfjerning. Delen *Taleforbedringer for PSTN-anrop* fjernes fra BETA.

1.16 Endringer for versjon 44.1, januar 2024

Det var ingen endringer i dette dokumentet for denne utgivelsen.

Cisco konfidensielt

2 Endringer for konfigurasjonsfiler

2.1 Endringer for konfigurasjonsfiler for versjon 45.4

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.2 Endringer for konfigurasjonsfiler for versjon 45.3

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.3 Endringer for konfigurasjonsfiler for versjon 45.2

- [BETA-funksjon]
  La til taggen <utvidet autorisasjon> under avsnittet <protokoller><sip>.

```
<config>
<protokoller>
  < nippe>
    <utvidet autorisasjon aktivert =
"%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Følgende %TAG% ble lagt til:

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.4 Endringer for konfigurasjonsfiler for versjon 45.1

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.5 Endringer for konfigurasjonsfiler for versjon 44.12

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.6 Endringer for konfigurasjonsfiler for versjon 44.11

- [BETA-funksjon] [Bare mobil] [Webex Calling bare]
  La til attributt med flere linjer i koden <protocols><sip><lines>.
  Lagt til <personlige> og <linjer> seksjoner for sekundærlinjene under seksjon <protokoller><sip><linjer>.

```
<config>
<protokoller><sip>
<linjer multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
   <personlig>
      <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
   </personlig>
   <line lineType="%BW-MEMBERTYPE-1 %">
      …
   </linje>
   <line lineType="%BW-MEMBERTYPE-2 %">
      …
   </linje>
   …
   <line lineType="%BW-MEMBERTYPE-10 %">
      …
   </linje>
```


Cisco konfidensielt

```
</linjer>
```

2.7 Endringer for konfigurasjonsfiler for versjon 44.10

- [BETA-funksjon]
  La til taggen <personlig assistent> under delen <tjenester>.

```
<config>
<tjenester>
   <personlig assistent aktivert="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

- [BETA-funksjon] [Bare mobil] [Webex Calling bare]
  La til attributtet for leveringsmåte under taggen <tjenester><push-notifications-for-calls>.

```
<config>
<tjenester>
   <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%">
```

Følgende %TAG%s ble lagt til:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.8 Endringer for konfigurasjonsfiler for versjon 44.9

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.9 Endringer for konfigurasjonsfiler for versjon 44.8

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.10 Endringer for konfigurasjonsfiler for versjon 44.7

- [BETA-funksjon]
  La til AI-kodek (xCodec) under delen <tjenester><anrop><lyd><kodeker>.

```
<config>
<tjenester><samtaler>
  <lyd>
    <kodeker>
      <codec name = "opus" priority = "1" nyttelast = ""/>
      <codec name = "xCodec" mode = "HP" priority = ".99" nyttelast = ""/>
      <codec name = "xCodec" mode = "ULP" priority = ".98" nyttelast = ""/>
      <codec name = "G722" priority = ".9" nyttelast = ""/ >
      <codec name = "PCMU" priority = ".8" nyttelast = ""/>
      <codec name = "PCMA" priority = ".7" nyttelast = ""/>
      <codec name = "G729" priority = ".5" nyttelast = "" vad = ""/>
      <codec name = "iLBC" priority = ".4" nyttelast = "" framelength =
"30"/>
      <codec name = "telefon-event" nyttelast = "101" in-band = "false"/>
```


Cisco konfidensielt

2.11 Endringer for konfigurasjonsfiler for versjon 44.6

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

2.12 Endringer for konfigurasjonsfiler for versjon 44.5

- [Webex Calling bare]
  La til enable-ipv6-support-attributtet til <protocols><rtp><ice>-taggen.

```
<config>
<protokoller><RTP>
  <is aktivert="%ENABLE_RTP_ICE_WXT%"
       aktiver-ipv6-support = "%ENABLE_RTP_ICE_IPV6_WXT%"
       modus="%RTP_ICE_MODE_WXT%"
       service-uri="%RTP_ICE_SERVICE_URI_WXT%"
       port="%RTP_ICE_PORT_WXT%"/>
```

- Taggen <remote-name> er lagt til i delen <services><calls><caller-id> med <maskin> som en undertag.

```
<config>
<tjenester><samtaler>
   <anroper-ID>
      <eksternt navn>
         <maskinmodus="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Følgende %TAG%s ble lagt til:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.13 Endringer for konfigurasjonsfiler for versjon 44.4

- [Bare stasjonære datamaskiner] [Webex Calling bare]
  Det er lagt til tagger <tilleggsnumre>, <søkegruppe> og <blokkering av klid-levering> under delen <caller-id><outgoing-calls>.

```
<config>
<tjenester><samtaler>
  <anroper-ID>
    <utgående anrop aktivert = "%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <tilleggsnumre
aktivert="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <call center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <søkegruppe aktivert="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </utgående-samtaler>
```

2.14 Endringer for konfigurasjonsfiler for versjon 44.3

- [Bare stasjonære datamaskiner] [Webex Calling bare]
  La til <utgående anrop> under den nye delen <anroper-ID>, med <call-center> som en undertag.

```
<config>
<tjenester><samtaler>
  <anroper-ID>
```


Cisco konfidensielt

```
    <utgående anrop aktivert = "%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <call center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
    </utgående-samtaler>
```

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

```
<config>
<protokoller><sip>
<transporterer>
  <UDP>
    <keepalive aktivert="%UDP_KEEPALIVE_ENABLED_WXT%">
      …
  </udp>
  <TCP>
    <keepalive aktivert="%TCP_KEEPALIVE_ENABLED_WXT%">
      …
  </TCP>
  <TLS>
    <keepalive aktivert="%TLS_KEEPALIVE_ENABLED_WXT%">
      …
  </TLS>
```

Følgende %TAG%s ble lagt til:

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

2.15 Endringer for konfigurasjonsfiler for versjon 44.2

- [Bare mobil]
  La til delen <anroper-ID> under <tjenester><anrop>. Det er lagt til undertagger <innkommende anrop> og <tapt anrop>, med ny underkode <tilføyingsnummer> for begge.

```
<config>
<tjenester><samtaler>
  <anroper-ID>
    <innkommende anrop>
      <tilføyingsnummer
aktivert="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
    </innkommende anrop>
    <tapte anrop>
      <vedleggsnummer
aktivert="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
    </tapte anrop>
```

- [Bare mobil] [Webex Calling bare]
  La til <utgående anrop> under den nye delen <anroper-id>.

```
<config>
<tjenester><samtaler>
  <anroper-ID>
    <utgående anrop aktivert = "%ENABLE_CLID_OUTGOING_CALLS_WXT%">
```


Cisco konfidensielt

```
      <tilleggsnumre
aktivert="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <call center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <søkegruppe aktivert="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </utgående-samtaler>
```

- La til taggen <call-forwarding-info> i delen <services><calls>.

```
<config>
<tjenester><samtaler>
  <call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

- [Bare stasjonære datamaskiner] [Webex Calling bare]
  La til <gruppe-anrop-hentingsvarsler> under <tjenester><anrop>, med <display-caller> og <max-timeout> som undertagger. Det er også lagt til <gruppe-anrop-henting>-tagg under hver <linje>kode i delen <protokoller><sip><linjer>.

```
<config>
<tjenester><samtaler>
  <group-call-pickup-notifications enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
    <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
    <maks-tidsavbruddsverdi="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
  </gruppeanrop-henting-varsler>
  …
<protokoller><sip>
  <linjer>
    <linje>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1 %</group-call-pickup>
      ...
    </linje>
    <linje>
      <gruppe-samtale-henting>%BWGROUP-CALL-PICKUP-BOOL-2 %</group-call-
pickup>
      ...
    </linje>
    …
```

Følgende %TAG%s 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%

Cisco konfidensielt

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

Følgende %TAG% ble avskrevet:

- %ENABLE_NOISE_REMOVAL_WXT%

2.16 Endringer for konfigurasjonsfiler for versjon 44.1

Det var ingen oppdateringer i konfigurasjonsfilene for denne versjonen.

Cisco konfidensielt

3 Introduksjon

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

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

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

Konfigurasjonsfilene leses av klienten når den starter, etter at de har blitt hentet fra Enhetsadministrasjon. Informasjonen fra konfigurasjonsfilene lagres kryptert, slik at den blir usynlig og ikke tilgjengelig for sluttbrukeren.

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

Cisco konfidensielt

4 Installasjon

Webex for Cisco BroadWorks-klienter kan installeres fra følgende:

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

4.1 Lokalisert klientnedlasting

Følgende lokaliserte versjoner av Webex for Cisco BroadWorks-klienter 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 er installert som et program (Android-applikasjonspakke [APK]), som holder innstillings- og konfigurasjonsrelaterte data innenfor sitt private område.

Det er versjonskontroll basert på Google Play-prosedyrene. Et 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 lastes ned, overskrives den gamle programvaren; Brukerdata beholdes imidlertid som standard.

Vær oppmerksom på at brukeren ikke trenger å velge noen alternativer for installasjon eller avinstallasjon.

4.3 iOS-klient

IOS-klienten er installert som et program, som holder de innstillingsrelaterte dataene inne i sin "sandkasse" og konfigurasjonsfildataene lagres kryptert.

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

Når den nye versjonen lastes ned, overskrives den gamle programvaren; Brukerdata beholdes imidlertid som standard.

Vær oppmerksom på at brukeren ikke trenger å velge noen alternativer for installasjon eller avinstallasjon.

4.4 Desktop-klient

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.

Cisco konfidensielt

Cisco konfidensielt

5 Enhetsadministrasjon

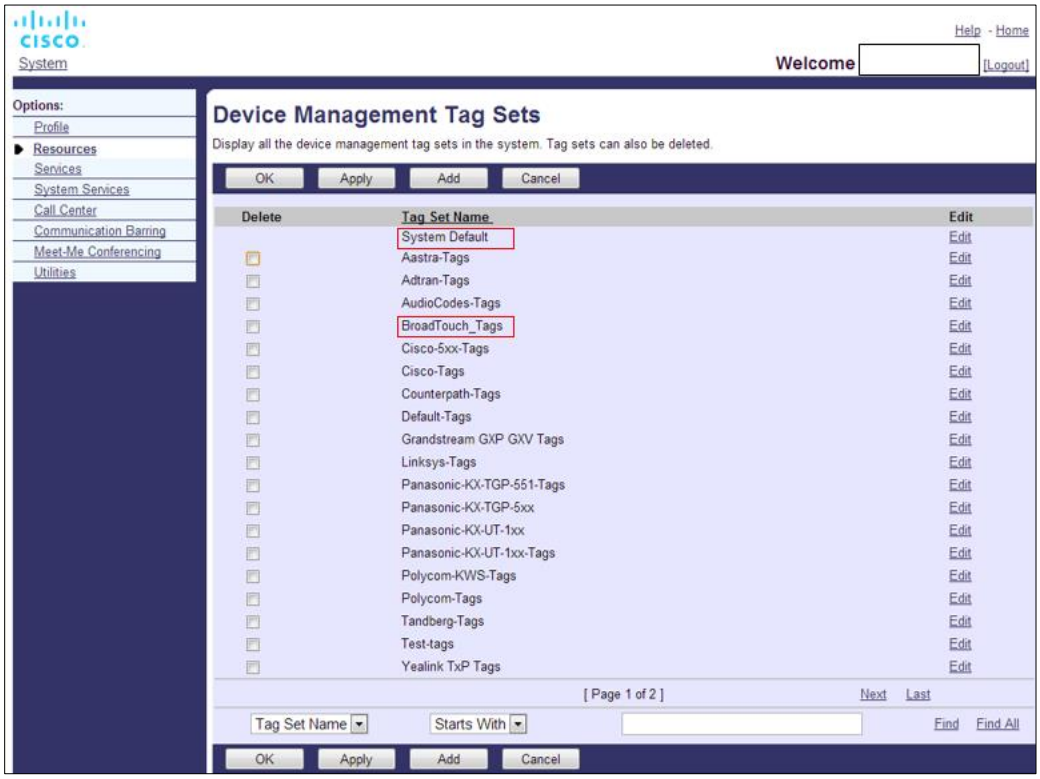
5.1 Koder for enhetsbehandling

Webex for Cisco BroadWorks bruker *Kodesett* for enhetsbehandling vist i figuren nedenfor. *Systemstandard* og egendefinerte kodesett kreves for å klargjøre bestemte enhets-/klientinnstillinger. Dette kodesettet gir fleksibilitet i administrasjon av klientens tilkoblingsinnstillinger for nettverk/tjeneste samt funksjonsaktiveringskontroller.

Dette egendefinerte kodesettet klargjøres av en systemansvarlig via alternativet System →*Resources* → Device Management Tag Set . Administratoren må legge til nye kodesett:

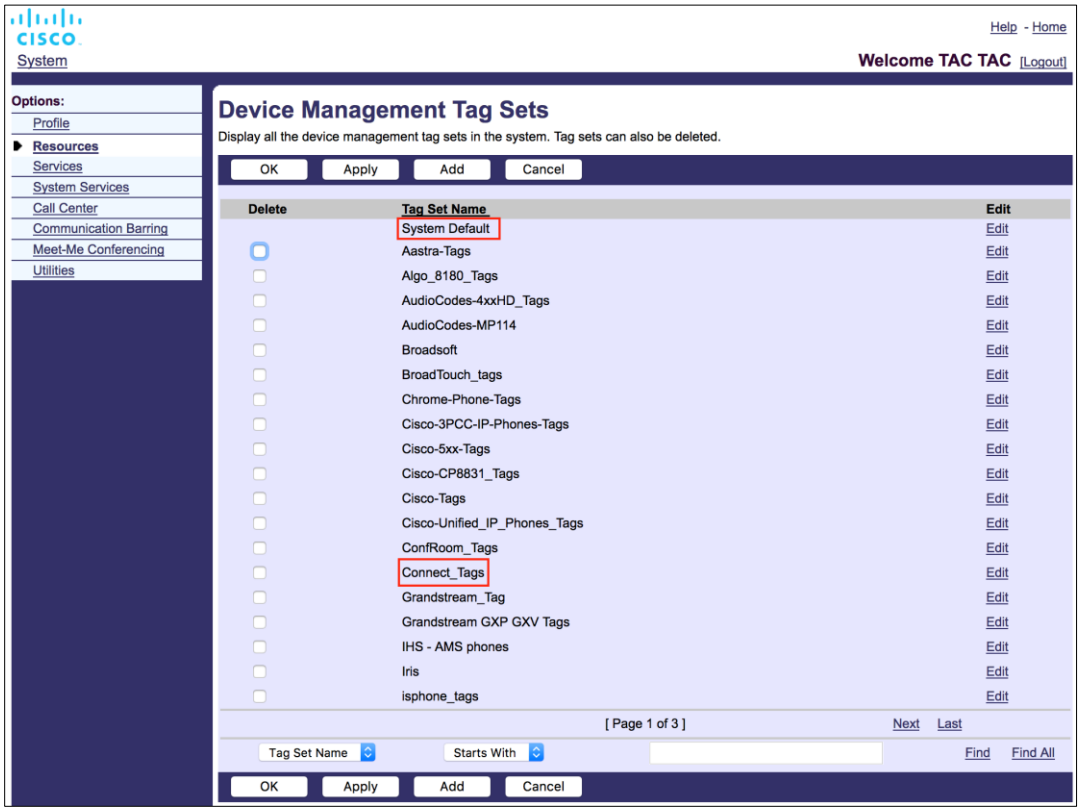
- Mobil: Connect_Tags
- Nettbrett: ConnectTablet_Tags
- Stasjonære PC BroadTouch_Tags

Opprett hver enkelt tag og angi verdien. Delreferanser gir detaljerte beskrivelser for hver kode. De egendefinerte kodene deles inn i grupper basert på funksjonaliteten og diskuteres senere i dette dokumentet.



Figur 1 Desktop Device Management Tag Sets

Cisco konfidensielt



Figur 2 – Brikkesett for administrasjon av mobilenheter

5.2 Forbedringer av delvis samsvar for valg av enhetstype

For å gi økt fleksibilitet ved valg av funksjonalitetspakker for brukergrupper eller enkeltbrukere, velges enhetsprofiltypen basert på et (første) delvis samsvar. Dette gjør at kundene kan bruke forskjellige enhetstyper.

Den generelle prosedyren for enhetsbehandling angir at Cisco BroadWorks-programserveren tilbyr en enhetsprofiltype. Den heter "Business Communicator - PC" for desktop, "Connect - Mobile" for mobil, og "Connect - Tablet" for nettbrett. En enhetsprofil kan opprettes og tilordnes 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 konfigurasjonsdataene for enhetsprofilen (konfigurasjonsfil) som er knyttet til denne enhetsprofilen, til å aktivere og deaktivere forskjellige funksjoner.

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

Tjenesteleverandøren kan for eksempel ha et ubegrenset 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.

Cisco konfidensielt

Vær oppmerksom på at det ikke forventes å ha flere samsvarende enhetsprofiltyper i listen over mottatte enheter XML men bare én.

5.3 Klient konfigurasjon

Webex for Cisco BroadWorks-versjonen av klienten bruker config-wxt.xml filen til konfigurasjon av kallefunksjonaliteten. Det finnes 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 "Connect – Mobile", "Connect – Tablet" og "Business Communicator – PC". Webex for Cisco BroadWorks bruker de samme enhetsprofilene som UC-One for å gjøre det enklere å distribuere.

MERK 1: Det må finnes en konfigurasjonsfil for hver enhetsprofil.

MERK 2: Det anbefales 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 distribusjon av Cisco BroadWorks-konfigurasjon** fra eldre klienter. Imidlertid er det fortsatt noen (system) koder som deles mellom UC-One og Webex.

Noen av de egendefinerte kodene for Cisco BroadWorks-systemet brukes også i konfigurasjonsfilen for *config-wxt.xml* . Hvis du vil ha mer informasjon om hver av følgende koder, kan du se delen *5.7 Cisco BroadWorks dynamisk innebygd* system Tags.

- %BWNETWORK-CONFERENCE-SIPURI-n%
- %BWVOICE-PORTAL-NUMBER-n%
- %BWLINEPORT-n%
- %BWAUTHUSER-n%
- %BWAUTHPASSWORD-n%
- %BWE164-n%
- %BWHOST-n%
- %BWNAME-n%
- %BW-n%
- %BWUTSEENDE-ETIKETT-n%
- %BWDISPLAYNAMELINEPORT%
- %BWLINEPORT-PRIMÆR%
- %BWE911-PRIMÆR-HELDURL%
- %BWE911-CUSTOMERID%

Cisco konfidensielt

- %BWE911-SECRETKEY%
- %BWE911-NØDNUMMER-LISTE%
- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (Webex Calling bare)

5.6 Standardkoder for system

Som systemadministrator kan du få tilgang til systemets standardkoder via *alternativet System → Resources → Device Management Tag Sets* . Følgende systemstandardkoder må klargjøres når VoIP-anropspakken installeres.

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

5.7 Cisco BroadWorks dynamisk innebygd system Tags

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

Merkelapp	Beskrivelse
%BWNETWORK-CONFERENCE-SIPURI-n%	Dette er serveren URI brukes til å aktivere N-veiskonferanser.
%BWVOICE-PORTAL-NUMBER-n%	Dette nummeret brukes til talepost. Klienten ringer dette nummeret når han 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 tilordnet brukeren. Den hentes fra brukerens profil. Brukes vanligvis som SIP-domene.

Cisco konfidensielt

Merkelapp	Beskrivelse
%BWAUTHUSER-n%	Dette er brukernavnet for godkjenning. Hvis abonnenten har blitt tilordnet godkjenning, er dette den klargjorte bruker-ID-en på godkjenningssiden uavhengig av den valgte godkjenningsmodusen for enhetstypen. SIP-brukernavnet, som vanligvis brukes i 401- og 407-signalering. Kan være forskjellig fra standard SIP-brukernavn.
%BWAUTHPASSWORD-n%	Dette er brukerens godkjenningspassord. Hvis abonnenten har blitt tilordnet godkjenning, er dette det klargjorte passordet på siden Godkjenning uavhengig av den valgte verdien for godkjenningsmodus for enhetstypen. SIP-passordet som brukes i SIP-signalering.
%BWE164-n%	Denne taggen oppgir brukerens telefonnummer i internasjonalt format.
%BWNAME-n%	Dette er abonnentens fornavn og etternavn i brukerens profil. Fornavn og etternavn er satt sammen. Hvis ingen linjeetikett er konfigurert og ikke tom, brukes som visningsnavn for linjen i linjevelgeren hvis den ikke er konfigurert med flere linjer.
%BW-n%	Abonnentens internnummer hentes fra utvidelsen som er klargjort i brukerens profil. Hvis et internnummer ikke er klargjort, erstattes brikken med abonnentens telefonnummer (DN).
%BWUTSEENDE-ETIKETT-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 (utseende for delt anrop). Dette er linjeporten som klargjøres på enheten som er tilordnet brukeren. Dette hentes fra brukerens profil. Brukes til å identifisere brukerens primære linje.
%BWLINEPORT-PRIMÆR%	Den primære linjeporten klargjøres på enheten som er tilordnet brukeren. Denne koden inkluderer ikke domenedelen av den klargjorte linjeporten. Den hentes fra brukerens profil.
%BWE911-PRIMÆR-HELDURL%	Angir URL-adressen til RedSky Emergency Location Platform som støtter HOLDD-protokollen.
%BWE911-CUSTOMERID%	Kunde-ID-en (HeldOrgId, CompanyID) som ble brukt for RedSky HTTPS-forespørselen.
%BWE911-SECRETKEY%	Hemmeligheten for å autentisere RedSky HTTPS-forespørselen.

Cisco konfidensielt

Merkelapp	Beskrivelse
%BWE911-NØDNUMMER-LISTE%	Listen over nødnumre som støttes av RedSky. Hvis du vil bruke denne koden, må den reserverte egendefinerte koden %RESERVEDBW911-EMERGENCY-NUMBER-LIST% legges til kodesettet som brukes av enhetstypen. "Reservert"-koden må inneholde nødnumrene som er definert på BroadWorks under AS_CLI/System/CallP/CallTypes > i et kommaseparert format som 911, 0911, 933. **MERK:** Webex-klienten støtter ikke jokertegn i nødnumre. Derfor skal bare eksakte nødnumre legges til den egendefinerte koden "reservert". Følgende eksempel viser hvordan funksjonen for reservert kode er ment å brukes: 1) Den opprinnelige koden %BWE911-EMERGENCY-NUMBER-LIST% legges til malfilen på enheten 2) Den reserverte egendefinerte koden %RESERVEDBW911-EMERGENCY-NUMBER-LIST% legges til i kodesettet som brukes av enheten med verdien 911, 0911, 933 3) Når filen bygges på nytt, løses den opprinnelige koden %RESERVEDBW911-EMERGENCY-NUMBER-LIST% 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 IDen for en gitt linje (bare Webex Calling)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Gir informasjon hvis den tilsvarende linjen har konfigurert anropshentingsgruppe. (Bare Webex ringer)

Cisco konfidensielt

6 Egendefinerte merker

Denne delen beskriver de egendefinerte kodene som brukes i Webex for Cisco BroadWorks. Den viser alle de tilpassede kodene som brukes for både stasjonære og mobile / nettbrettplattformer.

Vær imidlertid oppmerksom på at noen innstillinger som er beskrevet i denne delen, bare støttes for den bestemte versjonen av klienten. Hvis du vil finne ut om en innstilling ikke gjelder for en eldre klientversjon, kan du se den aktuelle versjonsspesifikke konfigurasjonsveiledningen.

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%ENABLE_REJECT_WITH_486_WXT%	J	J	sann	*6.1.16 Virkemåte for avvisning av* innkommende anrop
%REJECT_WITH_XSI_MODE_WXT%	N	J	decline_false	*6.3.2 Push-varsler for samtaler*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	J	opptatt	*6.3.2 Push-varsler for samtaler*
%ENABLE_TRANSFER_CALLS_WXT%	J	J	usann	*6.1.20 Overføre* samtaler
%ENABLE_CONFERENCE_CALLS_WXT%	J	J	usann	*6.1.21 N-veis konferansesamtaler og deltakere*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	J	J	usann	*6.1.21 N-veis konferansesamtaler og deltakere*
%MAX_CONF_PARTIES_WXT%	J	J	10	*6.1.21 N-veis konferansesamtaler og deltakere*
%ENABLE_CALL_STATISTICS_WXT%	J	J	usann	*6.1.24 Anropsstatistikk*
%ENABLE_CALL_PULL_WXT%	J	J	usann	*6.1.22 Trekk anrop*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	J	usann	*6.3.2 Push-varsler for samtaler*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	J	J	usann	*6.1.28 Transkripsjon av talepost for Webex* Calling
%ENABLE_MWI_WXT%	J	J	usann	*6.1.27 Talepost, Visuell talepost, Indikator for Melding* venter
%MWI_MODE_WXT%	J	J	tom	*6.1.27 Talepost, Visuell talepost, Indikator for Melding* venter
%ENABLE_VOICE_MAIL_WXT%	J	J	usann	*6.1.27 Talepost, Visuell talepost, Indikator for Melding* venter

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%ENABLE_VISUAL_VOICE_MAIL_WXT%	J	J	usann	*6.1.27 Talepost, Visuell talepost, Indikator for Melding* venter
%ENABLE_FORCED_LOGOUT_WXT%	J	N	usann	*6.2.1 Tvungen* utlogging
%FORCED_LOGOUT_APPID_WXT%	J	N	tom	*6.2.1 Tvungen* utlogging
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	J	J	usann	*6.1.29.1 Alltid viderekobling*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	J	J	sann	*6.1.29.3 BroadWorks hvor* som helst
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	J	J	usann	*6.1.29.3 BroadWorks hvor* som helst
%ENABLE_EMERGENCY_DIALING_WXT%	N	J	usann	*6.3.1 Nødanrop*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	J	911, 112	*6.3.1 Nødanrop*
%ENABLE_USE_RPORT_WXT%	J	J	usann	*6.1.14 SIP rport-behandling for NAT-traversering*
%RPORT_USE_LOCAL_PORT_WXT%	J	J	usann	*6.1.14 SIP rport-behandling for NAT-traversering*
%USE_TLS_WXT%	J	J	usann	*6.1.2 SIP Over TLS og Secure Real-time Transport Protocol*
%SBC_ADDRESS_WXT%	J	J	tom	*5.6 Standardkoder for system*
%SBC_PORT_WXT%	J	J	5060	*5.6 Standardkoder for system*
%USE_PROXY_DISCOVERY_WXT%	J	J	usann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%USE_TCP_FROM_DNS_WXT%	J	J	sann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%USE_UDP_FROM_DNS_WXT%	J	J	sann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%USE_TLS_FROM_DNS_WXT%	J	J	sann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%DOMAIN_OVERRIDE_WXT%	J	J	tom	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	J	J	sann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	J	J	sann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Y (bare Windows)	N	usann	*6.1.6 Dynamisk SIP-proxy-oppdagelse*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	J	J	5000	*6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-kontakt*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	J	J	10000	*6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-kontakt*
%SOURCE_PORT_WXT%	J	J	5060	*6.1.7 Foretrukket portbruk for SIP*
%SIP_FAILBACK_ENABLED_WXT%	J	N	sann	*6.1.8.2 SIP-failback*
%SIP_FAILBACK_TIMEOUT_WXT%	J	N	900	*6.1.8.2 SIP-failback*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	J	N	usann	*6.1.8.2 SIP-failback*
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	J	J	Dns	*6.1.8.3. Håndheve IP versjon*
%USE_ALTERNATIVE_IDENTITIES_WXT%	J	J	usann	*6.1.10 Bruk P-Associated-URIer i REGISTER*
%TCP_SIZE_THRESHOLD_WXT%	J	J	18000	*6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives*
%SIP_REFRESH_ON_TTL_WXT%	J	N	usann	*6.1.8.4 DNS TTL-ledelse*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	J	J	usann	*6.1.12 Støtte for SIP-OPPDATERING*
%ENABLE_PEM_SUPPORT_WXT%	J	J	usann	*6.1.11 PEM-topptekst (SIP P-Early Media)*
%ENABLE_SIP_SESSION_ID_WXT%	J	J	usann	*6.1.15 SIP-økt-ID*
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	J	J	usann	*6.1.13 Eldre SIP-INFO FIR*
%SRTP_ENABLED_WXT%	J	J	usann	*6.1.2 SIP Over TLS og Secure Real-time Transport Protocol*
%SRTP_MODE_WXT%	J	J	usann	*6.1.2 SIP Over TLS og Secure Real-time Transport Protocol*
%ENABLE_REKEYING_WXT%	J	J	sann	*6.1.2 SIP Over TLS og Secure Real-time Transport Protocol*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%RTP_AUDIO_PORT_RANGE_START_WXT%	J	J	8000	*6.1.17 Portområde for transportprotokoll i sanntid*
%RTP_AUDIO_PORT_RANGE_END_WXT%	J	J	8099	*6.1.17 Portområde for transportprotokoll i sanntid*
%RTP_VIDEO_PORT_RANGE_START_WXT%	J	J	8100	*6.1.17 Portområde for transportprotokoll i sanntid*
%RTP_VIDEO_PORT_RANGE_END_WXT%	J	J	8199	*6.1.17 Portområde for transportprotokoll i sanntid*
%ENABLE_RTCP_MUX_WXT%	J	J	sann	*6.1.19 RTCP MUX*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	J	J	sann	*6.1.33 XSI-hendelseskanal*
%CHANNEL_HEARTBEAT_WXT%	J	J	10000	*6.1.33 XSI-hendelseskanal*
%XSI_ROOT_WXT%	J	J	tom (brukeroppprinnelig URL)	*6.1.32 XSI-rot og stier*
%XSI_ACTIONS_PATH_WXT%	J	J	/com.broadsoft.xsi-actions/	*6.1.32 XSI-rot og stier*
%XSI_EVENTS_PATH_WXT%	J	J	/com.broadsoft.xsi-events/	*6.1.32 XSI-rot og stier*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	J	J	usann	*6.1.25 Automatisk gjenoppretting av anrop / Sømløs overlevering* av samtale
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	J	Bare cs	*6.3.1 Nødanrop*
%ENABLE_CALL_PICKUP_BLIND_WXT%	J	N	usann	*6.2.2 Samtalehenting*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	J	N	usann	*6.2.2 Samtalehenting*
%WEB_CALL_SETTINGS_URL_WXT%	J	J	tom	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%USER_PORTAL_SETTINGS_URL_WXT%	J	J	tom	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%ENABLE_CALL_CENTER_WXT%	J	J	usann	*6.1.31 Call Center / Call Queue Login* / Logg ut
%WEB_CALL_SETTINGS_TARGET_WXT%	J	J	utvendig	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	J	J	sann	*6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*
%USE_MEDIASEC_WXT%	J	J	usann	*6.1.3 3GPP SIP-hoder for SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	J	usann	*6.3.4 Klikk for å ringe (ring* tilbake)
%DIALING_CALL_BACK_TIMER_WXT%	N	J	10	*6.3.4 Klikk for å ringe (ring* tilbake)
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	J	N	usann	*6.2.3 Støtte for Boss-Admin (*Executive-Assistant)
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	J	35	*6.3.2 Push-varsler for samtaler*
%ENABLE_CALL_RECORDING_WXT%	J	J	usann	*6.1.26 Call Recording* (Innspilling av samtale)
%ENABLE_SINGLE_ALERTING_WXT%	N	J	usann	*6.3.3 Enkel varsling*
%ENABLE_CALL_PARK_WXT%	J	J	usann	*6.1.23 Parker/hent anrop*
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	J	J	10	*6.1.23 Parker/hent anrop*
%ENABLE_RTP_ICE_WXT%	J	J	usann	*6.1.18 ICE-støtte (kun Webex Calling)*
%RTP_ICE_MODE_WXT%	J	J	Isstun	*6.1.18 ICE-støtte (kun Webex Calling)*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%RTP_ICE_SERVICE_URI_WXT%	J	J	tom	*6.1.18 ICE-støtte (kun Webex Calling)*
%RTP_ICE_PORT_WXT%	J	J	3478	*6.1.18 ICE-støtte (kun Webex Calling)*
%ENABLE_RTP_ICE_IPV6_WXT%	J	J	usann	*6.1.18 ICE-støtte (kun Webex Calling)*
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	J	N	usann	*6.1.8.4 DNS TTL-ledelse*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	J	N	usann	*6.2.4 Eskalere SIP-anrop til møte*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	J	N	usann	*6.2.5 Bordtelefonkontrollanrop - Automatisk svar*
%ENABLE_DIALING_VOIP_WXT%	N	J	sann	*6.3.5 MNO-støtte* *Ring* med opprinnelig oppringing
%ENABLE_DIALING_NATIVE_WXT%	N	J	usann	*6.3.5 MNO-støtte* *Ring* med opprinnelig oppringing
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	J	J	sann	*6.1.35 SIP-URI-oppringing*
%ENABLE_SIP_VIDEOCALLS_WXT%	J	J	sann	*6.1.37 Deaktiver videoanrop*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	J	J	sann	*6.1.37 Deaktiver videoanrop*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	J	J	Skrivebord – sant Mobil, nettbrett - falsk	*6.1.37 Deaktiver videoanrop*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	J	J	usann	*6.1.38 Nødanrop (911) - Posisjonsrapportering med E911-leverandør*
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	J	J	0	*6.1.38 Nødanrop (911) - Posisjonsrapportering med E911-leverandør*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	J	J	-1	*6.1.38 Nødanrop (911) - Posisjonsrapportering med E911-leverandør*
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	J	J	once_per_login	*6.1.38 Nødanrop (911) - Posisjonsrapportering med E911-leverandør*
%ENABLE_AUTO_ANSWER_WXT%	J	N	usann	*6.2.6 Automatisk svar med tonevarsling*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	J	J	usann	*6.1.41 Spam Call Indication*
%ENABLE_NOISE_REMOVAL_WXT%	J	J	usann	*6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN-/mobilsamtaler*
%ENABLE_AUDIO_MARI_FEC_WXT%	J	J	usann	*6.1.46.2 FEC (Forward Error Correction) og Packets Retransmission (RTX)*
%ENABLE_AUDIO_MARI_RTX_WXT%	J	J	usann	*6.1.46.2 FEC (Forward Error Correction) og Packets Retransmission (RTX)*
%ENABLE_VIDEO_MARI_FEC_WXT%	J	J	usann	*6.1.46.2 FEC (Forward Error Correction) og Packets Retransmission (RTX)*
%ENABLE_VIDEO_MARI_RTX_WXT%	J	J	usann	*6.1.46.2 FEC (Forward Error Correction) og Packets Retransmission (RTX)*
%ENABLE_CALL_BLOCK_WXT%	J	J	usann	*6.1.45 Blokkeringsliste (bare Webex Calling)*
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	J	sann	*6.3.5.6 MNO-mobilitet – widget under samtale*
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	J	sann	*6.3.5.6 MNO-mobilitet – widget under samtale*
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	J	sann	*6.3.5.6 MNO-mobilitet – widget under samtale*
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	J	J	usann	*6.1.47 Samtidige samtaler med samme bruker*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	J	N	usann	*6.2.12 Hendelsespakke for ekstern demping (kun Webex Calling)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	J	J	sann	*6.1.29.2 Viderekobling til talepost*
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	J	J	sann	*6.1.8.1 SIP-overgang*
%ENABLE_CALL_MOVE_HERE_WXT%	J	N	usann	*6.2.13 Flytt samtale*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	J	J	usann	*6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN-/mobilsamtaler*
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	J	tom	*6.3.5.1 Ring med opprinnelig oppringing*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	J	J	usann	*6.1.20 Overføre* samtaler
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	J	J	sann	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	J	usann	*6.3.6 Innkommende anroper-ID*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	J	usann	*6.3.6 Innkommende anroper-ID*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	J	usann	*6.1.50 Oppringer-ID* *ID* for utgående anroper
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	J	usann	*6.1.50 Oppringer-ID* *ID* for utgående anroper
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	J	usann	*6.1.50 Oppringer-ID* *ID* for utgående anroper

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	J	usann	*6.1.50 Oppringer-ID ID* for utgående anroper
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	J	usann	*6.1.50 Oppringer-ID ID* for utgående anroper
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	J	J	usann	*6.1.49 Informasjon om viderekobling* av anrop
%ENABLE_BUSY_LAMP_FIELD_WXT%	J	N	usann	*6.2.8.1 Opptattlampefelt*
%ENABLE_BLF_DISPLAY_CALLER_WXT%	J	N	sann	*6.2.8.1 Opptattlampefelt*
%BLF_NOTIFICATION_DELAY_TIME_WXT%	J	N	0	*6.2.8.1 Opptattlampefelt*
%ENABLE_GCP_NOTIFICATIONS_WXT%	J	N	usann	*6.2.8.2 Hentegruppe for anrop (bare Webex Calling)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	J	N	usann	*6.2.8.2 Hentegruppe for anrop (bare Webex Calling)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	J	N	120	*6.2.8.2 Hentegruppe for anrop (bare Webex Calling)*
%UDP_KEEPALIVE_ENABLED_WXT%	J	J	sann	*6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives*
%TCP_KEEPALIVE_ENABLED_WXT%	J	J	usann	*6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives*
%TLS_KEEPALIVE_ENABLED_WXT%	J	J	usann	*6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives*
%ENABLE_MULTI_LINE_WXT%	J	J	usann	*6.1.51 Flere* linjer
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	J	usann	*6.2.4 Videresende SIP-anrop til møte (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	J	usann	*6.3.5.3 CLID (Outgoing Calling Line Identity) – dobbel identitet*

Cisco konfidensielt

Merkelapp	Brukes i skrivebordet	Brukes i mobil/nettbrett	Standardverdi	Seksjon
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	J	usann	*6.3.5.3 CLID (Outgoing Calling Line Identity)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	J	J	Løst	*6.1.50.2 Navn på ekstern anroper-ID*
%PERSONAL_ASSISTANT_ENABLED_WXT%	J	J	usann	*6.1.53 Personlig assistent (tilstedeværelse borte)**Error! Reference source not found.***
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	J	NPS	***Error! Reference source not found.*** *Leveringsmåte (bare Webex Calling)*
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	J	J	usann	*6.1.52* ***Error! Reference source not found.****.*

Hvis du vil ha mer informasjon om hvordan du tilordner de egendefinerte kodene som brukes i Webex for Cisco BroadWorks, til kodene som brukes av UC-One, kan du se delen *8 Egendefinerte koder Tilordning mellom Webex for Cisco BroadWorks og UC-One*.

Cisco konfidensielt

6.1 Fellestrekk

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-overskrifter og i eksterne (XSI) samtaler. Brukerdelen av egen SIP-URI kommer fra konfigurasjon av SIP-legitimasjon (parameter <brukernavn> under <legitimasjon>).
- SIP-server URI eller IP adressen til SIP proxy-serveren hvis DNS løsning skulle mislykkes. Vær oppmerksom på at for å kunne bruke TLS, kan ikke adressene IP brukes i proxy-parameteren, da TLS sertifikatvalidering mislykkes. Hvis du vil ha mer informasjon om proxy-porten, kan du se DM-koden %SOURCE_PORT_WXT%. Vær oppmerksom på at funksjonen DNS TTL-behandling 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 forskjellige funksjoner for anrop. De foregående innstillingene aktiverer imidlertid grunnleggende funksjonalitet for følgende:

- Registrering på SIP-nettverket.
- Foreta lyd- eller videosamtaler.
- Utfører DNS-basert proxy-oppdagelse, som gjør det mulig å bruke flere proxyer.

Når SIP-registrering er aktivert, må du aktivere SIP SUBSCRIBE for MWI via separate konfigurasjonsparametere. Hvis du vil ha mer informasjon om talepost, kan du se delen *6.1.27 Talepost, Visuell talepost, Indikator for Melding* venter.

Vær oppmerksom på at grunnleggende SIP-konfigurasjon alltid er nødvendig for MWI selv når SIP-anrop er deaktivert. MWI er avhengig av SIP-VARSLER.

Oppsettet av SIP-serverne følger dette grunnleggende skjemaet:

- Proxy-adressen inneholder SIP-serverens URI.
- Bare én proxy kan defineres.
- Den DNS proxy-oppdagelsen gir støtte for mange proxyer, som krever riktig konfigurasjon av DNS.

I tillegg vises SIP-tidtakere i konfigurasjonsfilen (anbefales ikke å endre dem).

```
<config>
<protokoller>
< nippe>
   <tidtakere>
       <T1>500</T1>
       <T2>4000</T2>
       <T4>5000</T4>
   </tidtakere>
```

- T1 – hvor lang tid, i millisekunder, det tar for en nettverksforsinkelse tur-retur.
- T2 – maksimal tid, i millisekunder, før du sender forespørsler og invitasjonssvar på nytt.

Cisco konfidensielt

- T4 - maksimal tid, i millisekunder, for en melding å forbli i nettverket.

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

Følgende eksempel og tabell inneholder informasjon om de vanligste DM-kodene som brukes til SIP-konfigurasjon.

```
<config>
<protokoller><sip>
<linjer multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
       <linje>
              <label>%BWAPPEARANCE-LABEL-1 %</label>
              <navn>%BWNAME-1 %</navn>
              <telefonnummer>%BWE164-1 %</telefonnummer>
              <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>
              <domene>%BWHOST-1 %</domene>
              <legitimasjon>
                     <brukernavn>%BWLINEPORT-1 %</brukernavn>
                     <password>%BWAUTHPASSWORD-1 %</password>
                     <autentisering>
                            <auth401>
                                   <standard>
                                          <brukernavn>%BWAUTHUSER-1 %</brukernavn>
                                          <password>%BWAUTHPASSWORD-1 %</password>
                                   </standard>
                                   <realm id="%BWHOST-1 %">
                                          <brukernavn>%BWAUTHUSER-1 %</brukernavn>
                                          <password>%BWAUTHPASSWORD-1 %</password>
                                   </rike>
                            </auth401>
                            <auth407>
                                   <standard>
                                          <brukernavn>%BWAUTHUSER-1 %</brukernavn>
                                          <password>%BWAUTHPASSWORD-1 %</password>
                                   </standard>
                                   <realm id="%BWHOST-1 %">
                                          <brukernavn>%BWAUTHUSER-1 %</brukernavn>
                                          <password>%BWAUTHPASSWORD-1 %</password>
                                   </rike>
                            </auth407>
                     </autentisering>
              </legitimasjon>
       </linje>
       …
</linjer>
<proxy-adresse="%SBC_ADDRESS_WXT%" port="%SBC_PORT_WXT%" />
<preferred-port>%SOURCE_PORT_WXT%</preferred-port>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%BWLINEPORT-n%	tom	streng	Vanligvis SIP-brukernavn. Hvis du vil ha mer informasjon, kan du se avsnittet *5.7 Cisco BroadWorks dynamisk innebygd system Tags*. Eksempel: johndoe
%BWAUTHPASSWORD-n%	tom	streng	Vanligvis SIP-passord. Hvis du vil ha mer informasjon, kan du se avsnittet *5.7 Cisco BroadWorks dynamisk innebygd system Tags*. Eksempel: hemmeligpassord
%BWE164-n%	tom	telefonnummer	Standard telefonnummer for brukeren i internasjonalt format. Hvis du vil ha mer informasjon, kan du se avsnittet *5.7 Cisco BroadWorks dynamisk innebygd system Tags*. Eksempel: 12345678
%SBC_ADDRESS_WXT%	tom	streng	Hvis du vil ha mer informasjon, kan du se avsnittet *5.6 Standardkoder for system*. Eksempel: sbcexample.domain.com
%SBC_PORT_WXT%	5060	nummer	Hvis du vil ha mer informasjon, kan du se avsnittet *5.6 Standardkoder for system*. Eksempel: 5060
%BWHOST-n%	tom	streng	Brukes vanligvis som SIP-domene. Hvis du vil ha mer informasjon, kan du se avsnittet *5.7 Cisco BroadWorks dynamisk innebygd system Tags*. Eksempel: exampledomain.com
%SOURCE_PORT_WXT%	5060	nummer	Brukes vanligvis for parameteren *foretrukket port* . Hvis du vil ha mer informasjon, kan du se avsnittet *6.1.7 Foretrukket portbruk for SIP*. Eksempel: 5061
%BWUSEREXTID-n%	tom	streng	(Bare Webex Calling) Inneholder den eksterne ID-en til linjen Hvis du vil ha mer informasjon, kan du se *6.1.51 Flere* linjer. Eksempel: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

MERK: Det anbefales på det sterkeste 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.

Cisco konfidensielt

6.1.2 SIP Over TLS og Secure Real-time Transport Protocol

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 eksemplet nedenfor. Vær også oppmerksom på 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. Hvis du vil ha mer informasjon om dynamisk SIP-proxy-oppdagelse, kan du se delen *6.1.6 Dynamisk SIP-proxy-oppdagelse.*

Når dynamisk proxy-gjenkjenning ikke brukes, tas den i bruk når du aktiverer TLS for SIP.

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

Merk at sertifikatet som brukes, må være gyldig. Videre må sertifikatkjeden være intakt slik at det mellomliggende sertifikatet også er koblet sammen. Det anbefales at et mye brukt sertifikat brukes, 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 hjelp av masseklargjøring, selv om dette vanligvis ikke gjøres.

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

I tillegg til RTP kan RTCP trafikk sikres med de samme mekanismene som RTP ved hjelp av den foregående konfigurasjonen.

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

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

- Konfidensialitet (data er kryptert)
- Autentisering (forsikring om identiteten til den andre parten eller partene)
- Integritet (tiltak mot for eksempel repriseangrep)

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

Medierammeverket støtter både full (80-biters) og kort (32-biters) autentiseringskode. 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 hjelp av konfigurasjonen vist i eksemplet nedenfor. Den gjeldende implementeringen bruker bare SDP-profilen for sikker RTP og støtter SDP med flere linjer for oppføringer i profilen Audio Visual Profile (AVP) og Secure Audio Visual Profile (SAVP). Den SRTP implementeringen har blitt testet vellykket i sin vanlige distribusjonskonfigurasjon med forskjellige SBC-er. Interoperabilitetstesting (IOT) med endepunkter som bare støtter kryptering ved hjelp av AVP-profilen, støttes ikke.

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

Cisco konfidensielt

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

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

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

- Obligatorisk – Ved samtaleoppsett inkluderer den første SDP-en bare SAVP m-linjen når den tilbys, og klienten godtar bare SAVP m-linjen i SDP når han svarer, derfor er bare SRTP anrop mulig.
- Foretrukket – Ved samtaleoppsett inkluderer den første SDP-en både AVP- og SAVP m-linjene, men SAVP er først når den tilbyr, noe som indikerer ønsket rekkefølge. Når du svarer, 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 når du svarer).
- Valgfritt - Ved samtaleoppsett inkluderer den første SDP både SAVP og AVP m-linjer når du tilbyr, men AVP indikerer først foretrukket rekkefølge. Når du svarer, velger klienten den første m-linjen, AVP eller SAVP.
- SRTP ikke aktivert – Det er ingen SAVP m-linje i den første SDP-en når den tilbys. Når du svarer, godtas ikke SAVP, derfor er det bare mulig å RTP anrop.
- Transport – Velg automatisk SRTP modus basert på transportprotokollen. Hvis TLS brukes, er obligatorisk SRTP-modus aktivert. Hvis TCP eller UDP brukes, brukes ingen SRTP.

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

```
<config>
<protokoller><sip>
<sikker>%USE_TLS_WXT%</sikker>
```

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

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

I noen distribusjoner støttes ikke omnøkling for SRTP. Derfor finnes det en konfigurasjonsparameter for aktivering/deaktivering SRTP omnøkling. Imidlertid blir nye nøkler alltid tatt i bruk når de mottas i en oppdatert SDP i henhold til rfc3264. Konfigurerbarhet gjelder bare sending av nye nøkler.

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_TLS_WXT%	usann	sant, usant	Når angitt til "false", deaktiveres SIP TLS. Når SIP TLS er satt til "true", aktiveres. Vær oppmerksom på at hvis *6.1.6 Dynamisk SIP-proxy-oppdagelse* den brukes, ignoreres denne parameteren.
%SRTP_ENABLED_WXT%	usann	sant, usant	Når den er satt til "false", deaktiveres SRTP. Når den er satt til "true", aktiveres SRTP.
%SRTP_MODE_WXT%	valgfri	obligatorisk, foretrukket, valgfritt, transport	Definerer hvor foretrukket SRTP er ved samtaleoppsett. Standardverdien er "valgfri".
%ENABLE_REKEYING_WXT%	sann	sant, usant	Aktiverer ny omnøkling av SIP (SDP) for SRTP.

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

6.1.3 3GPP SIP-hoder for SRTP

Nyere 3GPP-spesifikasjoner krever ekstra SIP-overskrifter 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

Hodene som kreves av denne spesifikasjonen, kan bryte SIP-anrop i distribusjoner der dette oppsettet ikke brukes. Derfor anbefales disse meldingshodene bare å brukes i miljøer der serversiden støtter dem.

Bare aktivering av bruk av overskriftene kan konfigureres. Det finnes ingen ytterligere konfigurerbarhet for individuelle topptekster. Alle topptekster er enten aktivert eller deaktivert.

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

Følgende kode styrer denne funksjonen.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_MEDIASEC_WXT%	usann	Sant, usant	Aktiverer 3GPP SIP-hoder for SRTP forhandling.

Cisco konfidensielt

6.1.4 Tving TCP, TLS eller UDP Bruk og Keepalives

Webex for Cisco BroadWorks-klienten kan konfigureres til å bruke enten TCP, TLS eller UDP for både SIP-signalisering og RTP medier. Vær oppmerksom på at klienten bruker TCP som standard. Merk også at uten TCP keepalive, SIP TCP tilkoblinger er stengt etter en periode med inaktivitet.

Følgende eksempel viser denne konfigurasjonsnoden.

```
<config>
<protokoller><sip>
<transporterer>
    <tcp-size-threshold>%TCP_SIZE_THRESHOLD_WXT%</tcp-size-threshold>
```

Følgende -kode kontrollerer om klienten bruker TCP eller UDP.

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

Den samme konfigurasjonsnoden har også parametere for UDP, TCP og TLS keepalive, som vist i eksemplet nedenfor.

```
<config>
<protokoller><sip>
<transporterer>
        …
        <UDP>
                <keepalive aktivert="%UDP_KEEPALIVE_ENABLED_WXT%">
                        <Timeout>20</timeout>
                        <nyttelast>crlf</nyttelast>
                </keepalive>
        </udp>
        <TCP>
                <keepalive aktivert="%TCP_KEEPALIVE_ENABLED_WXT%">
                        <Timeout>0</timeout>
                        <nyttelast></nyttelast>
                </keepalive>
        </TCP>
        <TLS>
                <keepalive aktivert="%TLS_KEEPALIVE_ENABLED_WXT%">
                        <Timeout>0</timeout>
                        <nyttelast></nyttelast>
                </keepalive>
        </TLS>
</transporter>
```


Cisco konfidensielt

De mulige parametrene er:

- Aktivering TCP eller TLS keepalive, mulige verdier - sant / usant, standarden er "false" hvis noden mangler. Vær oppmerksom på at når denne funksjonen er aktivert, sendes TCP keepalives selv om UDP transport brukes til SIP.
- Aktivering UDP keepalive, mulige verdier - sant / usant, standarden er "true" hvis noden mangler. Vær oppmerksom på at når denne funksjonen er aktivert, sendes UDP keepalives selv om TCP transport brukes til SIP. I tillegg, selv om TCP brukes til SIP, godtar klienten også trafikk over UDP i henhold *til RFC 3261*.
- Tidsavbrudd angir den maksimale tiden med inaktivitet i sekunder som KeepAlive-meldingen sendes etter. 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.

Server IP-adressen og porten for keepalives bestemmes ved hjelp av de vanlige prosedyrene for SIP-proxy-oppdagelse. Vær oppmerksom på at SIP-porter og valg av transportprotokoll hentet via SIP dynamisk proxy-oppdagelse overstyrer alle statiske port- eller transportkonfigurasjoner. Hvis du vil ha mer informasjon om dynamisk proxy-oppdagelse, kan du se delen *6.1.6 Dynamisk SIP-proxy-oppdagelse.*

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%UDP_KEEPALIVE_ENABLED_WXT%	sann	sant, usant	Kontrollerer om oppbevaringspakkene skal sendes til UDP transport.
%TCP_KEEPALIVE_ENABLED_WXT%	usann	sant, usant	Kontrollerer om oppbevaringspakkene skal sendes til TCP transport.
%TLS_KEEPALIVE_ENABLED_WXT%	usann	sant, usant	Kontrollerer om Keep-Alive-pakkene skal sendes til TLS-transporten.

6.1.5 Konfigurerbart tidsavbrudd for åpning av SIP-kontakt

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

```
<config>
    <protokoller>
        < nippe>
```


Cisco konfidensielt

```
            <transporterer>
                <UDP>
                    …
                </udp>
                <TCP>
                    …
                    <connect-
timeout>%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </TCP>
                <TLS>
                    <connect-
timeout>%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </TCP>
            </transporter>
```

Følgende koder kontrollerer tidsavbruddet for socket-tilkobling (i millisekunder).

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<heltall> – tidsavbruddet i millisekunder	Tidsavbrudd for socket-tilkobling når TCP transport brukes.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	<heltall> – tidsavbruddet i millisekunder	Tidsavbrudd for socket-tilkobling når TLS transport brukes.

6.1.6 Dynamisk SIP-proxy-oppdagelse

Hvis du vil aktivere SIP-funksjonalitet for dynamisk proxy-oppdaging, kan du se følgende eksempel.

```
<config>
<protokoller><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 transportprotokoller oppføringer fra DNS SRV brukes når mange er tilgjengelige i henhold til prosedyrene i denne delen.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_PROXY_DISCOVERY_WXT%	usann	Sant, usant	Aktiverer dynamisk SIP-proxy-oppdagelse for lyd- og videosamtaler. Den anbefalte verdien er "true".

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SBC_ADDRESS_WXT%	tom	Streng	Denne Cisco BroadWorks-koden brukes vanligvis for postnavnparameteren. Det bør være en gyldig URL - bør ikke være en IP adresse. Hvis du vil ha mer informasjon, kan du se avsnittet *5.6 Standardkoder for system*. Eksempel: sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	tom	Streng	Denne egendefinerte koden brukes for domeneoverstyring. Hvis du vil ha mer informasjon, kan du se delen nedenfor. Eksempel: other.domain.com
%USE_TCP_FROM_DNS_WXT%	sann	Sant, usant	Hvis denne parameterverdien er "false", forkastes de DNS SRV-resultatene for denne transportprotokollen (TCP). Hvis "true", brukes resultatene fra DNS SRV for denne transportprotokollen (TCP). Avhengig av SRVs prioriteringer kan det likevel velges en annen transport.
%USE_UDP_FROM_DNS_WXT%	sann	Sant, usant	Hvis denne parameterverdien er "false", forkastes de DNS SRV-resultatene for denne transportprotokollen (UDP). Hvis "true", brukes resultatene fra DNS SRV for denne transportprotokollen (UDP). Avhengig av SRVs prioriteringer kan det likevel velges en annen transport.
%USE_TLS_FROM_DNS_WXT%	sann	Sant, usant	Hvis denne parameterverdien er "false", forkastes de DNS SRV-resultatene for denne transportprotokollen (TLS). Hvis "sant", brukes resultatene fra DNS for denne transportprotokollen (TLS). Avhengig av SRVs prioriteringer kan det likevel velges en annen transport.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	Sant, usant	sann	Aktiverer/deaktiverer DNS sikkerhetskopieringstjenesten. Hvis aktivert, utføres A/AAAA-løsning for SIP-proxy-adressen. Det tas bare hensyn til når SRV/NAPTR-tjenesteoppdagelse er aktivert.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	Sant, usant	sann	Hvis satt til "true" og NAPTR-tjenesteoppdagelse mislykkes eller ikke returnerer noen resultater, utføres SRV-tjenesteoppdagelse for den konfigurerte verten. Hvis satt til "false", utføres ingen SRV-oppdagelse.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Sant, usant	usann	Tillater omgåelse av OS DNS-hurtigbufferen.

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

Cisco konfidensielt

DNS SRV, Spørringer for navngivningsautoritet (NAPTR) og A-post støttes. Ved pålogging er 3-trinns flyten som følger:

1. Utfør en NAPTR-spørring ved å bruke *feltet* <record-name> ovenfor for å hente server-URIene med transportprotokollene, hvis de finnes. Verdien for parameteren < *postnavn*> må være det fullstendige domenet DNS skal løse, og kan ikke være en IP adresse.

2. Løse elementer som ble funnet i NAPTR-spørringen, ved hjelp av en SRV-spørring for å hente den endelige serverens URI og port. Domenedelen som brukes i SRV-spørringen, hentes fra resultatet av NAPTR-spørringen for å finne den endelige serveren URI (og porten). Porten som mottas fra SRV DNS spørringen, brukes når de DNS SRV-oppføringene er tilgjengelige. Legg merke til at porten, bare fra konfigurasjonsfilen, gjelder for den statiske proxyen i konfigurasjonsfilen, og ikke for URIene som er løst ved hjelp av SRV. Se følgende eksempler for bruk av de forskjellige postnavnene.

   Hvis ingen NAPTR blir funnet, prøver klienten en SRV-spørring med postnavnet hentet fra <*domene*> parameter med mindre det er <*domain-override*> parameter tilstede i hvilket tilfelle< *domain-override*> brukes og prøver automatisk å finne separate oppføringer for TCP, UDP og TLS (*_sip_protocol* [UDP, TCP eller TLS]). Vær oppmerksom på at SCTP (Stream Control Transmission Protocol) ikke støttes. Hvis SRV-spørringer ikke gir noen resultater, mislykkes proxy-oppdaging, og sluttbrukeren får en feilmelding som angir at anrop ikke er tilgjengelige. I dette tilfellet er det ingen SIP-registrering. Men selv om alle SRV-spørringer mislykkes eller hvis serverne som mottas der ikke fungerer, som en reserveløsning, kontrollerer klienten fortsatt om den konfigurerte statiske proxyen fungerer, bare med A-spørringer til URI som er angitt i <proxy-adresse> for å se om den gir en IP-adresse som gir en fungerende SIP-registrering. Havn og transport i dette siste utveistilfellet kommer fra *tcp-terskel* og <*sikre*> parametere.

3. Løs funnet URIer ved hjelp av A-postspørringen. De mottatte endelige IP adressene prøves i den rekkefølgen de mottas, for å få en fungerende tilkobling til SIP-proxyen. Denne ordren kan defineres av tjenesteleverandøren i DNS. Den første SIP-proxy-URI, med et vellykket A-oppslag, velges og brukes til den ikke lenger fungerer, eller klienten logger av. I A-spørringstrinnet brukes bare én IP adresse om gangen, selv om mange mottas. Alle SRV-oppføringer løses imidlertid til 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 tcp-terskelparameteren* som vanligvis brukes til å velge UDP eller TCP i konfigurasjonsfilen. Det samme gjelder også konfigurasjon av SIP/TLS. TCP eller UDP brukes avhengig av prioriteten i DNS.

MERKNAD 2: Elementer mottatt via SRV prioriteres over den statiske proxyen i konfigurasjonsfilen. NAPTR-ordren blir ikke sett på; bare SRV-prioritet teller. Når SRV resulterer i flere varer med lik transportprotokoll, prioritet og vekt, velges alle mottatte tilfeldig. NAPTR-lodd støttes ikke i denne versjonen, men SRV-lodd støttes. SRV-prioritet blir sett på først, og for elementer med samme prioritet blir vekt sett på for å bestemme sannsynligheten for at en bestemt server blir prøvd neste gang.

MERKNAD 3: Den valgfrie *domeneoverstyringsparameteren* tillater at et annet A-postnavn enn det i parameteren SIP-domenekonfigurasjon løses med SRV når NAPTR-resultater utelates. Se følgende eksempler på bruk av parameteren *domeneoverstyring* .

MERKNAD 4: Klienten bruker operativsystemprimitiver for DNS operasjoner, og vanligvis bufres DNS svar for å overholde TTL for det DNS svaret.

Cisco konfidensielt

MERKNAD 5: DNS-typen (tjenesten) for NAPTR-poster må følge *RFC 3263-prosedyrene* , ellers kan DNS løsningen mislykkes. Det er for eksempel nødvendig å bruke SIPS + D2T for SIP over TLS.

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

SIP+D2U -> _sip._udp

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: Bruke 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 returnerer resultater.

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

Dette resulterer i følgende trinn på protokollnivået.

```
1. NAPTR spørring for record-domain.com, svar:
record-domain.com.
28591 I NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.
2. SRV-spørring for _sip._tcp.test.sip.record-domain.com (mottatt i NAPTR-
spørringen), svar
_sip._tcp.test.sip.record-domain.com. 28635 I SRV
10 10 5061 test.sipgeo.record-domain.com.
3. A-postspørring for test.sipgeo.record-domain.com, svar:
test.sipgeo.record-domain.com. 16 I EN 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.

Eksempel 2: **Bruke parameter for domeneoverstyring i konfigurasjonsfil**

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

```
<config>
<protokoller><sip
<proxy-adresse="domain.com" port="5060"/>
<proxy-discovery enabled="true">
```


Cisco konfidensielt

```
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domene>sip-domain.com</domene>
```

Dette resulterer i følgende trinn på protokollnivå.

```
1. NAPTR spørring for record-domain.com, ingen svar.
2. SRV-spørring for _sip._tcp.override-domain.com (fra konfigurasjonsfil), svar
_sip._tcp.override-domain.com. 28635 I SRV
10 10 5061 test.override-domain.com.
3. A-postspørring for test.override-domain.com, svar:
test.sipgeooverride-domain.com. 16 I EN 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-prioriteter**

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 prioriteter mottas. I dette tilfellet er det bare SRV-prioritet som gjelder i denne utgivelseshendelsen, selv om flere NAPTR-poster med varierende prioritet også mottas.

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

Dette resulterer i følgende trinn på protokollnivå.

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

2. SRV-spørring for _sip._tcp.test.sip.record-domain.com (mottatt i NAPTR-
spørringen), svar
_sip._tcp.test.sip.record-domain.com. 28635 I SRV
10 10 5061 test.sipgeo.record-domain.com.

SRV-spørring for _sip._udp.test.sip.record-domain.com (mottatt i NAPTR-spørringen),
svar
_sip._udp.test.sip.record-domain.com. 28635 I SRV
20 10 5062 test.sipgeo.record-domain.com.

3. A-postspørring for test.sipgeo.record-domain.com, svar:
test.sipgeo.record-domain.com. 16 I EN 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.

Cisco konfidensielt

Eksempel 4: Bruke 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>
<protokoller><sip>
<proxy-adresse="domain.com" port="5060"/>
<proxy-discovery enabled="true" tcp="true" udp="false" tls="true">
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domene>sip-domain.com</domene>
```

Dette resulterer i følgende trinn på protokollnivået.

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

2. For den første posten har vi tjenestetype "SIPS + D2T" og prefikset er
"sip._tls.". Siden dette prefikset ikke samsvarer med tjenestetypen (se merknad
6 ovenfor), blir det ignorert.

3. SRV-spørring for _sip._tcp.test.sip.record-domain.com (mottatt i NAPTR-
spørringen), svar
_sip._tcp.test.sip.record-domain.com. 28635 I SRV
10 10 5061 test.sipgeo.record-domain.com.

3. A-postspørring for test.sipgeo.record-domain.com, svar:
test.sipgeo.record-domain.com. 16 I EN 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.

6.1.7 Foretrukket portbruk for SIP

Det har vært noen tilfeller når en annen programvarepakke har kjørt på samme maskin som klienten, opptar standard SIP-porten. Hvis du vil 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 *foretrukket port* , men hvis den tas, prøver klienten trinnvis portverdier over den konfigurerte verdien. Hvis for eksempel verdien for den foretrukne porten er "6000" og den porten blir 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	nummer	Angir foretrukket lokal SIP-port for kommunikasjon. Eksempel: 5060

Cisco konfidensielt

6.1.8 SIP-failover og failback

SIP-failover og failback følger Cisco BroadWorks-prosedyrene. 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
- SIP-proxy-adressen oppgis som et FQDN-navn, og den løses til flere IP adresser (se avsnitt *6.1.1 SIP-serverinnstillinger*).

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

Hvis flere IP adresser løses ved pålogging, sorteres de etter prioritet. Klienten begynner å bruke den første tilgjengelige IP adressen.

6.1.8.1 SIP-overgang

SIP-failover kan utløses av en socket-feil, en tidsavbruddsfeil for forespørsel eller et definitivt feilsvar fra serveren på følgende måte:

- Socket-feil - hvis kontakten mellom klienten og serveren blir ødelagt eller lukkes, som i tilfelle tap av nettverkstilkobling, reagerer klienten umiddelbart og utløser en failover.
- Tidsavbrudd (for eksempel når SBCen 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).
- Endelig feil mottatt fra serveren:
  - Følgende SIP-feilmeldinger fra serveren til et SIP-register utløser en failover:
    - 5xx
    - 6xx
  - Følgende SIP *4xx-svar* på SIP REGISTER <u>forårsaker ikke</u> failover:
    - 401 Unauthorized
    - 403 Forbidden
    - 404 Not Found
    - 407 Proxy Authentication Required
    - 423 Intervall for kort
  - *Videre utløser ikke 4xx* feilsvar på SIP INVITE failover, men *5xx* og *6xx* gjør det.

Cisco konfidensielt

Når en failover utløses, henter klienten neste tilgjengelige IP adresse fra listen. SIP T1-tidtaker definerer hvor lenge en proxy på listen prøves før du går videre til neste, vanligvis brukes 32 sekunders verdi (64*T1). Hvis alle IP adressene mislykkes, viser klienten en brukergrensesnittfeil for SIP-tilkobling. Hvis en VoIP samtale pågår når failoveren inntreffer, avsluttes samtalen.

SIP-failover-logikken er avhengig av flere konfigurasjonsparametere:

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

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

  - T1 – hvor lang tid, i millisekunder, det tar for en nettverksforsinkelse tur-retur.
  - T2 – maksimal tid, i millisekunder, før du sender forespørsler og invitasjonssvar på nytt.
  - T4 - maksimal tid, i millisekunder, for en melding å forbli i nettverket.
- SIP-proxy-adresse og SIP-proxy-oppdagelse
  - Se avsnittet *6.1.1 SIP-serverinnstillinger*.
  - Se avsnittet *6.1.6 Dynamisk SIP-proxy-oppdagelse*.
- Registrere failover-konfigurasjon (se nedenfor)

Ved failover vil det Webex programmet sende SIP REGISTER med to kontaktmeldingshoder – én for den gamle økten og den andre med den nye enhetsinformasjonen. Kontakthodet for den gamle økten er inkludert for å varsle SBCen om å rydde opp i dataene. Denne toppteksten inkluderer utløper = 0 og q = 0,5.

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

Fra og med versjon 42.11 introduseres en ny *<registrer-failover>* seksjon i konfigurasjonsmalen. Det er en ny konfigurerbar parameter *<registration-cleanup>* lagt til for å kontrollere om programmet vil 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, slik at det ikke er nødvendig med kontakthodet for den gamle økten. Registreringsoppryddingslogikken er aktivert som standard.

For konsekvens *flyttes også koden <q-value>* under same *<register-failover>* delen.

Eksempel:

```
<config>
<protokoller><sip>
```


Cisco konfidensielt

```
   <q-verdi>1,0</q-verdi> <!-- DEPRERT -->
   <registrer-failover>
      <registration-
cleanup>%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%</registration-cleanup>
      <q-verdi>1,0</q-verdi>
```

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

6.1.8.2 SIP-failback

Hvis klienten er koblet til en proxy som ikke er først etter prioritet, prøver den å koble til IP med høyest prioritet på nytt. Tidspunktet for failbacken er basert på konfigurasjonen av DNS TTL-administrasjon (se avsnitt *6.1.8.4 DNS TTL-ledelse*). Hvis et anrop pågår når feiltilbakeingstidtakeren nås, venter klienten til alle anrop er fullført, og utløser failback-prosedyren. Merk at dette bare gjelder for stasjonære klienter siden SIP-tilkoblingen bare er aktiv under en samtale på mobil.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_FAILBACK_ENABLED_WXT%	sann	sant, usant	Aktiverer/deaktiverer SIP-failback.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Over 60	Tidsavbrudd for SIP-failback i sekunder.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	usann	sant, usant	Legger til et tilfeldig punktum [0–10]% av SIP-failbacken.

6.1.8.3 Håndheve IP versjon

Webex klient kan konfigureres til å sortere listen over løste verter gjennom DNS og deretter gå gjennom dem i tilfelle SIP-failover. I alle modusene respekteres prioritet og vekt.

Støttede konfigurasjoner er:

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

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

Cisco konfidensielt

Med "dns" -konfigurasjon prioriteres de IPv4 adressene over IPv6-adressene, for gitt vert. Hvis det er to verter med både IPv4- og IPv6-adresser, blir rekkefølgen IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

I "prefer-ipv4" -modus er de IPv4 adressene sortert før IPv6-adressene (rekkefølgen innen IPv4 og IPv6-gruppene forblir)

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

Med "prefer-ipv6" -modus er rekkefølgen motsatt - IPv6-adressene plasseres før IPv4 adressene

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

Med "nat64" -modus - IPv6-adressene ignoreres, respekteres den IPv4 rekkefølgen. IPv6-prefikset/-prefiksene oppdages. For hver IPv4 adresse opprettes en kombinasjon med hvert Pref64-prefiks og/eller suffiks.

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

```
<config>
<protokoller><sip><transporter>
<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 foretrekk-IPv4 foretrekk-IPv6 nat64	Kontrollerer rekkefølgen på IPv4/IPv6-adresser som brukes av Webex-klienten til å koble til SIP-økten.

6.1.8.4 DNS TTL-ledelse

En egen konfigurasjonsparameter er lagt til for å styre måten DNS løse løses på nytt når TTL for den DNS posten for serveren som brukes for øyeblikket, utløper. Når parameteren i følgende tabell er aktivert, tvinges klienten til å gjøre om DNS operasjoner når TTL for DNS SRV eller A-record for serveren som brukes for øyeblikket, utløper.

Etter at den DNS løsningen er gjort på nytt, tvinger denne parameteren også klienten til å koble til den høyest prioriterte serveren mottatt hvis den er forskjellig fra den nåværende serveren, selv i tilfelle når den nåværende tilkoblingen fungerer fullt ut. Ny tilkobling gjøres imidlertid først etter at pågående samtaler er fullført.

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

Når denne parameteren er deaktivert, gjøres ikke operasjonene DNS om når TTL utløper, men heller hvert 15. minutt.

Cisco konfidensielt

Denne parameteren fungerer bare for SIP.

Vær oppmerksom på at funksjonen DNS TTL-behandling ikke kan brukes når en IP adresse brukes i proxy-adresseparameteren.

> **MERK:** Dette er en stasjonær funksjon, siden mobilklientene bare har SIP-tilkobling mens de er i en samtale.

```
<config>
<protokoller><sip>
<refresh-on-ttl enabled="%SIP_REFRESH_ON_TTL_WXT%"
  bruk-random-faktor = "%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_REFRESH_ON_TTL_WXT%	usann	usant, sant	Når angitt til "false", deaktiveres DNS TTL-behandling for SIP. Når angitt til "true" er DNS TTL management aktivert for SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	usann	usant, sant	Hvis aktivert, legger a tilfeldig periode mellom 0-10 % til DNS TTL.

> **MERK:** Det anbefales sterkt å aktivere den DNS tilfeldige TTL-faktoren for å forhindre topper av forespørsler til DNS og potensielt topper av forsøk på ny tilkobling til applikasjonsserveren.

6.1.9 SIP SUBCSRIBE og REGISTRER Oppdater og abonner Prøv på nytt

Communicator støtter konfigurering av oppdateringsintervallene for SIP, SUBSCRIBE og REGISTRER. 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 maksimumsverdien for intervallet *for nytt abonnement* er 2000000 sekunder, mens en negativ, 0 eller tom verdi resulterer i 1800 sekunder som brukes. Enhver negativ verdi i for å abonnere oppdatering utelater *Utløper-overskriften* og oppretter dermed en engangs ABONNER.

SIP REGISTER-oppdateringstidtakeren som foreslås 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 expires-verdien for SIP-økter (for SIP INVITE og SUBSCRIBE) også konfigureres (i sekunder).

```
<config>
<protokoller><sip>
<subscription-refresh-interval>10800</subscription-refresh-interval>
<subscription-retry-interval>60</subscription-retry-interval>
<registration-refresh-interval>300</registration-refresh-interval>
<økt>
```


Cisco konfidensielt

```
        <expires-value>3600</expires-value>
</økt>
```

6.1.10 Bruk P-Associated-URIer i REGISTER

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

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

```
<config>
<protokoller><sip>
<bruk-alternativ-identiteter>%USE_ALTERNATIVE_IDENTITIES_WXT%</bruk-alternativ-
identiteter>
```

Hvis parameteren er satt til "true", henter 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 REGISTERET. I tillegg vises ikke disse URIene som kontakter i kontaktlisten.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USE_ALTERNATIVE_IDENTITIES_WXT%	usann	sant, usant	Aktiverer bruk av alternative identiteter i SIP REGISTER. Hvis satt til "true", henter klienten sin egen identitet fra det siste *P-Associated-URI-hodet* for utgående SIP-forespørsler. Hvis satt til "false", blir sin egen identitet for utgående SIP-forespørsler hentet fra sin egen SIP-URI.

6.1.11 PEM-topptekst (SIP P-Early Media)

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

Konfigurasjonsparameteren aktiverer PEM-støtte for annonsering i SIP-signalering. Den faktiske logikken for tidlig mediehåndtering er den samme for både PEM- og ikke-PEM-tilfeller, og handler på støttede PEM-topptekstverdier.

```
<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%	usann	Sant, usant	Sett til "true" for å aktivere klientannonsering PEM-støtte i SIP-signalering. Sett til "false" for å deaktivere PEM-støtte for klientannonsering i SIP-signalering.

Cisco konfidensielt

6.1.12 Støtte for SIP-OPPDATERING

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

Typiske brukstilfeller er knyttet til tidlige medier når du for eksempel bruker tilbakeringingstone og forhåndsvarsel samtidig.

SIP-OPPDATERING støttes for øyeblikket bare når det mottas i brukstilfeller før dialogboks (early media) og ikke under aktiv dialog, for eksempel for samtale på vent/gjenoppta der re-INVITE fortsatt brukes.

Det er ikke mulig å legge til video i lyden ved hjelp av SIP UPDATE (medieendring) i denne versjonen. I tillegg støtter ikke klienten full IMS lang samtaleflyt med ressursreservering.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	usann	sant, usant	Når satt til "false", er støtte for SIP UPDATE deaktivert. Når SIP UPDATE er satt til "true", aktivert støtte for SIP UPDATE.

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 RTCP ikke kommer gjennom til eksternt endepunkt, noe som kan føre til ingen video eller enveisvideo. Hvis du vil ha mer informasjon, kan du 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%	usann	Sant, usant	Når satt til "false", er SIP INFO FIR-støtte deaktivert. Når satt til "true", er SIP INFO FIR-støtte aktivert.

Cisco konfidensielt

6.1.14 SIP rport-behandling for NAT-traversering

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

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

Vær oppmerksom på at "rport"-strengen alltid finnes i utgående SIP-forespørsler, uavhengig av konfigurasjon. Parameteren påvirker bare bruken av IP adresse og port mottatt fra serveren i SIP-hodene "mottatt" og "rport". Når funksjonen er aktivert, brukes verdiene fra "received" og "rport"-hoder i SIP-kontakthodet i SIP-forespørsler (selv når "mottatt"-hodet mangler i REGISTRER-svar).

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

Det finnes en egen konfigurasjonsparameter *bruk-lokal-port* som tvinger den lokale porten til klientkontakten til å angis i kontakthodet. Dette brukes for noen SBC-er som oppdager at klienten har en reell IP (fra *kontakthodet*), og SBCen prøver å opprette en separat kontakt til klienten for sine forespørsler. I de fleste tilfeller sitter en brannmur mellom SBC og klienten, og den nekter de innkommende tilkoblingene til klienten.

> **MERK:** I IPv6-miljøer er alle adressene ekte, og SBCen prøver å opprette en forbindelse til lytteklientadressen (fra *kontakthodet*).

```
<config>
<protokoller><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%	usann	sant, usant	Aktiverer rport for lyd- og videosamtaler.
%RPORT_USE_LOCAL_PORT_WXT%	usann	sant, usant	Kontrollerer om den lokale porten til klientens socket skal legges til i SIP-kontakthodet .

Cisco konfidensielt

6.1.15 SIP-økt-ID

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

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

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIP_SESSION_ID_WXT%	usann	Sant, usant	Kontrollerer bruken av SIP-økt-ID-en.

6.1.16 Virkemåte for avvisning av innkommende anrop

Klienten tilbyr fleksibilitet til å avvise et anrop med *486* eller *603*.

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

```
<config>
<tjenester><samtaler>
<reject-with-486 enabled="%ENABLE_REJECT_WITH_486_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_REJECT_WITH_486_WXT%	sann	sant, usant	Kontrollerer SIP-feilkoden og årsaken som brukes til å avvise innkommende SIP-anrop. Hvis aktivert,486 *Midlertidig ikke tilgjengelig* brukes. Ellers *brukes 603 Avvis* .

6.1.17 Portområde for transportprotokoll i sanntid

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

```
<config>
<protokoller><RTP>
<foretrukket-lyd-port-start>%RTP_AUDIO_PORT_RANGE_START_WXT%</foretrukket-lyd-port-
start>
```


Cisco konfidensielt

```
<foretrukket-lyd-port-slutt>%RTP_AUDIO_PORT_RANGE_END_WXT%</foretrukket-lyd-port-slutt>
<foretrukket-video-port-start>%RTP_VIDEO_PORT_RANGE_START_WXT%</preferred-video-port-start>
<foretrukket-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	nummer	Starten på lydportområdet.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	nummer	Slutten av lydportområdet.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	nummer	Starten på videoportområdet.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	nummer	Slutten av videoportområdet.

MERK: Portområder bør angis slik at de aldri overlapper.

6.1.18 ICE-støtte (kun Webex Calling)

Klienten støtter ICE-forhandlinger (Interactive Connectivity Establishment) som muliggjør optimalisering av mediebaner mellom endepunkter (på en node-til-node-måte). Dette gjøres for å redusere dataventetiden, redusere pakketap og redusere driftskostnadene ved distribusjon av programmet.

Merk at den nåværende implementeringen støtter STUN-server, mens TURN ikke støttes.

Når ICE-støtte er aktivert, vil omnøkling for SRTP alltid utføres (se avsnitt *6.1.2 SIP Over TLS og Secure Real-time Transport Protocol*).

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

```
<config>
<protokoller><RTP>
   <is aktivert="%ENABLE_RTP_ICE_WXT%"
        aktiver-ipv6-support = "%ENABLE_RTP_ICE_IPV6_WXT%"
        modus="%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%	usann	sant, usant	Aktiver/deaktiver ICE-støtte.
%RTP_ICE_MODE_WXT%	Isstun	Isstun	ICE-støttemodus. For øyeblikket er den eneste støttede verdien "icestun".

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%RTP_ICE_SERVICE_URI_WXT%	(tom)	gyldig STUN-server URI eller (tom)	STUN-server URI.
%RTP_ICE_PORT_WXT%	3478	Antall (0-65535)	STUN-serverport.
%ENABLE_RTP_ICE_IPV6_WXT%	usann	sant, usant	Aktiverer ICE over IPv6.

6.1.19 RTCP MUX

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

- Bakoverkompatibilitetsmodus (det vil si at linje a = rtcp-mux ikke vises i SDP)
- Multipleksingsmodus (a=rtcp-mux-linjen vises to ganger i SDP: én gang i m=audio-delen, og en andre gang i m=video-delen)

Video og lyd bruker ikke samme port.

```
<config>
<protokoller><RTP>
<mux enabled="%ENABLE_RTCP_MUX_WXT%"/>
```

Vær oppmerksom på at RTCP MUX ikke kan brukes med SRTP anrop.

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

6.1.20 Overføre samtaler

Den Webex for Cisco BroadWorks-klienten støtter overvåket (rådgivende), semi-konsultativ, og direkte (blind) samtaleoverføring.

Semi-konsultativ samtaleoverføring lar oppringeren fullføre overføringen før samtalen hentes av den eksterne anroperen. Den semi-konsultative fullføringsknappen aktiveres for oppringeren først etter at ringingen er startet på anropssiden og det tilsvarende SIP-varselet (*180 ringer*) er mottatt på anropersiden. Blind overføring kalles "Overfør nå" i brukergrensesnittet.

MERK: SIP *180-ringefunksjonen* utløses kanskje ikke i enkelte miljøer, for enkelte numre eller i enkelte scenarier for kommunikasjon på tvers av servere.

Cisco konfidensielt

Versjon 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 i det lokale endepunktet. Og samtaler som avsluttes på en ekstern enhet, kan overføres til samtaler som er avsluttet på et eksternt endepunkt. Denne funksjonen har ikke konfigurerbare alternativer.

Fra og med versjon 43.12 legger Webex-appen til konfigurasjonsalternativer for å kontrollere om den gjeldende samtalen skal settes automatisk på vent når menyelementet Overfør er valgt. Denne virkemåten styres av det nye *attributtet auto-hold* . Automatisk tilbakeholdelse er deaktivert som standard.

```
<config>
<tjenester><anrop>
   <overføringssamtale aktivert="%ENABLE_TRANSFER_CALLS_WXT%"
                  xsi-enabled="%ENABLE_XSI_TRANSFER_CALLS_WXT%"
                  type="%TRANSFER_CALL_TYPE_WXT%"
                  auto-hold="%ENABLE_TRANSFER_AUTO_HOLD_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_TRANSFER_CALLS_WXT%	usann	sant, usant	Når "true" er satt til true, er samtaleoverføring aktivert. Når angitt til "false", deaktiveres samtaleoverføring.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	usann	sant, usant	Aktiverer overføringsalternativer for eksterne samtaler (XSI) 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%	usann	sant, usant	Kontrollerer om den aktive samtalen automatisk settes på vent når brukeren velger alternativet Overfør fra menyen på skjermen i samtalen.

6.1.21 N-veis konferansesamtaler og deltakere

Følgende egendefinerte kode kan brukes til å kontrollere tilgjengeligheten til ad hoc-konferansesamtalen (N-vei) via SIP i Webex for Cisco BroadWorks-klienten. I tillegg kan N-vei-eieren se hele deltakerlisten via SIP SUBSCRIBE/NOTIFY og konferansearrangementspakke. Eierens klient lærer URI å sende SIP SUBSCRIBE til via foregående SIP *Contact* header av *200 OK* melding sendt som svar på INVITE til konferansen URI mens for deltakerne den samme informasjonen er i en foregående call-info NOTIFY.

Systeminnstillingen for Cisco BroadWorks (*maxConferenceParties)* brukes til å angi maksimalt antall konferansedeltakere. For et gitt anrop angir det antall aktive samtidige parter en bruker kan ha eller legge til via alternativet Legg til deltakere midt i samtalen eller gjennom Cisco BroadWorks N-way Calling-funksjonen.

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

Cisco konfidensielt

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

Eksempel på utdata:
maxConferenceParties = 6
konferanseURI =
```

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

```
<config>
<tjenester><samtaler>
<konferanse aktivert="%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>
</konferanse>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CONFERENCE_CALLS_WXT%	usann	sant, usant	Kontrollerer om alternativet Konferanse skal være aktivert for brukeren.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	usann	sant, usant	Sett til "true" for å aktivere N-veis eierdeltakerliste. Sett til "false" for å deaktivere deltakerlisten for N-veiseier.
%MAX_CONF_PARTIES_WXT%	10	Tall mellom 4 og 15 (tom)	Angir det maksimale N-veis deltakernummeret, håndhevet av klienten, for eksempel 10. Serversiden har sine egne grenser. Tom verdi deaktiverer håndheving på klientsiden av N-veis deltakergrense.

6.1.22 Trekk anrop

Call Pull-funksjonen kan aktiveres ved hjelp av én enkelt konfigurasjonsparameter, som vist i eksemplet nedenfor.

```
<config>
<tjenester><samtaler>
<call-pull enabled="%ENABLE_CALL_PULL_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_PULL_WXT%	usann	Sant, usant	Aktiverer henting av anrop.

Cisco konfidensielt

6.1.23 Parker/hent anrop

Funksjonen for gruppeparkering gjør det mulig å overføre pågående VoIP samtaler til en samtaleparkeringsserver, noe som gjør det mulig for anroperen å gjøre noe annet og hentes av samme bruker eller en annen bruker. En pågående samtale parkeres mot det første tilgjengelige internnummeret i samtaleparkeringsgruppen.

Henting av samtale kan utføres av brukeren som parkerer samtalen i dialogruten i et konfigurerbart antall sekunder umiddelbart etter parkering av samtalen. Den parkerte samtalen kan også hentes av brukeren eller en annen bruker ved å velge alternativet for henting av anrop og angi nummeret eller internnummeret.

```
<config>
<tjenester><samtaler>
<call-park enabled="%ENABLE_CALL_PARK_WXT%"
timer="%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_PARK_WXT%	usann	Sant, usant	Aktiverer parkering/henting av anrop.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Antall mellom 5 og 30	Angir antall sekunder den vellykkede dialogen Samtaleparkert er synlig for brukeren før den lukkes automatisk.

6.1.24 Anropsstatistikk

Ved hjelp av SIP-melding (Reporting End-of-Call Statistics in Session Initiation Protocol) BYE-melding kan du sende samtalestatistikk til en ekstern ende når et anrop avsluttes. Anropsstatistikken sendes som en ny meldingshode i SIP BYE-meldingen eller i det tilsvarende *200 OK-svaret* på BYE-meldingen. Statistikken omfatter RTP-pakker (Real-time Transport Protocol) som er sendt eller mottatt, totalt antall sendte eller mottatte pakker, totalt antall pakker som går tapt, forsinkelsesvariasjon, rundturforsinkelse og samtalevarighet.

```
<config>
<tjenester><samtaler>
<anropsstatistikk aktivert="%ENABLE_CALL_STATISTICS_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_STATISTICS_WXT%	usann	sant, usant	Sett til «true» for å aktivere registrering av anropsmåledata. Sett til «usann» for å deaktivere registrering av anropsmåledata.

Cisco konfidensielt

6.1.25 Automatisk gjenoppretting av anrop / Sømløs overlevering av samtale

Klienten har støtte for automatisk gjenoppretting av anrop ved bytte av nettverk mens brukeren har en pågående VoIP samtale. Samtale automatisk gjenoppretting fungerer i begge retninger - Cellular Data-til-WiFi og WiFi-til-mobildata, samt mens du bytter mellom WiFi-nettverk. Samtalen forsøkes gjenopprettet innen ett minutt, og stopper deretter. Hvis det er mer enn én pågående VoIP samtaler, gjenopprettes bare den aktive.

I overgangen fra mobildata til WiFi vil klienten beholde de pågående VoIP samtalene på mobildata til de avsluttes eller mobildatanettverket går tapt.

```
<config>
<tjenester><samtaler>
<automatisk gjenoppretting aktivert="%ENABLE_CALLS_AUTO_RECOVERY_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	usann	sant, usant	Kontrollerer om mekanismen for automatisk gjenoppretting skal være aktivert for brukeren.

6.1.26 Call Recording (Innspilling av samtale)

Funksjonen Samtaleopptak støttes av klienten og avhenger av tilgjengeligheten til funksjonen på serversiden, samt konfigurasjonsalternativet. Funksjonen avhenger av aktivert XSI-hendelseskanal (se avsnitt *6.1.33 XSI-hendelseskanal*) og applikasjonsserver (AS) konfigurert til å sende *SIP-hodet X-BroadWorks-Correlation-Info* (se Webex *for Cisco BroadWorks Solution Guide*).

Hvis funksjonen er deaktivert, er det ingen opptaksknapper og alternativer for brukeren. Merk at samtaleopptak opererer per bruker, ikke per samtale - det betyr at hvis en av deltakerne i en samtale støtter samtaleopptak, kan samtalen spilles inn.

Hvis samtaleopptaksfunksjonen er aktivert, er det alltid en visuell indikasjon når samtalen blir spilt inn. Cisco BroadWorks støtter følgende samtaleopptaksmoduser:

Alltid

- Samtaleopptak startes automatisk ved samtaleetablering.
- **Brukeren kan IKKE** stoppe/pause samtaleopptaket.

Alltid med pause/gjenoppta-støtte

- Samtaleopptak startes automatisk ved samtaleetablering, men brukeren kan pause og gjenoppta samtalen.
- Mulige brukersamhandlinger:
  - Innspilling pågår – **Sett innspillingen på pause** .
  - Innspillingen er satt på pause – **Fortsett** innspillingen.

På forespørsel

Cisco konfidensielt

- Når samtalen er opprettet, starter samtaleopptaket på serveren.
- Hvis brukeren trykker på alternativet Start opptak under samtalen, lagres samtaleopptaket, og det vil beholde samtalen fra oppstart. Ellers, hvis ingen startopptak startes fra brukeren, slettes samtaleopptaket på serveren.
- Mulige brukersamhandlinger:
  - Ingen innspilling har startet ennå – **Start** opptakshandling.
  - Innspilling pågår – **Sett innspillingen på pause** .
  - Innspillingen er satt på pause – **Fortsett** innspillingen.

Ved behov med brukerstartet start

- Brukeren kan starte, stoppe, pause og gjenoppta samtaleopptak når som helst, flere ganger i løpet av en samtale.
- Det vil være separate samtaleopptak for hver oppstart av samtaleopptak.
- Mulige brukersamhandlinger:
  - Ingen innspilling har startet ennå – **Start** opptakshandling.
  - Innspilling pågår – **Stopp** og **sett opptaket på pause** .
  - Innspillingen er satt på pause – **Stopp** og **fortsett** innspillingen.

Samtaleopptaksmodusen som er tilordnet brukeren, kan velges fra kontrollhuben.

```
<config>
<tjenester><samtaler>
<record enabled="%ENABLE_CALL_RECORDING_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_RECORDING_WXT%	usann	sant, usant	Aktiverer kontroller for samtaleopptak.

6.1.27 Talepost, Visuell talepost, Indikator for Melding venter

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

Visuell talepost (VVM) støttes bare for lyd. Støttede formater er wav, ulaw og mov som inneholder H264-video (bare spilt av som lyd). Den lar brukerne se innkommende talepost i en listevisning, og individuelle elementer kan spilles av. Denne funksjonen er basert på Xsi, men varsler om ny talepost leveres via SIP. Derfor må SIP være aktivert for at varslene skal fungere. I tillegg er konfigurasjon av SIP SUBSCRIBE for Message Waiting Indicator (MWI) nødvendig for at varslene skal ankomme, og MWI må være aktivert for at visuell talepost skal fungere. Hvis du vil ha mer informasjon om SIP-konfigurasjon, kan du se delen *6.1.1 SIP-serverinnstillinger*.

Cisco konfidensielt

Hvis du vil ha informasjon om krav til utgivelse og oppdatering av Cisco BroadWorks for Visual Voicemail, kan du se Webex
for løsningsveiledningen for Cisco BroadWorks.

Visuell talepost må være aktivert separat i konfigurasjonen.

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

- Talemeldinger aktivert
- Alternativet "Når meldingen kommer, bruk unified messaging" aktivert
- Alternativet "Bruk indikator for telefonmelding venter" er aktivert

Hvis Visual Voicemail-tjenesten ikke er tilordnet på Cisco BroadWorks-siden for brukeren, deaktiveres konfigurasjonen for tjenesten automatisk.

Vær oppmerksom på at deaktivering av SIP-registrering også deaktiverer MWI for nye talepostmeldinger. Se tabellen nedenfor hvis du vil ha mer informasjon om hvordan du aktiverer MWI.

Hvis du vil vise talepostmeldingsinformasjon i brukergrensesnittet, må klienten motta SIP MWI-varsler fra serveren (det vil si hendelsespakken for talepost). Se tabellen nedenfor for abonnementsalternativer. Vær også oppmerksom på at MWI er nødvendig for at visuelle talepostvarsler skal fungere.

Vær oppmerksom på at hvis SIP-abonnement på hendelsespakken for talepost mislykkes, fortsetter klienten å prøve på nytt når den er konfigurert til å gjøre det. Hvis du vil ha mer informasjon om konfigurasjon av SIP SUBSCRIBE nye forsøk, kan du se delen *6.1.9 SIP SUBCSRIBE og REGISTRER Oppdater og abonner Prøv* på nytt.

```
<config>
<tjenester><samtaler>
<mwi enabled="%ENABLE_MWI_WXT%" type="%MWI_MODE_WXT%"/>
<talepost aktivert="%ENABLE_VOICE_MAIL_WXT%" visuell-talepost =
"%ENABLE_VISUAL_VOICE_MAIL_WXT%">
   <center-number>%BWVOICE-PORTAL-NUMBER-1 %</center-number>
</telefonsvarer>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_VOICE_MAIL_WXT%	usann	sant, usant	Sett til "true" for å aktivere støtte for talepost. Sett til "false" for å deaktivere støtte for talepost.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	usann	sant,usant,usant	Når angitt til «false», deaktiveres VVM. Når «true» er satt til «true», er VVM aktivert. Vær oppmerksom på at talepost aktivert=usann før det faktiske VVM-attributtet fortsatt brukes til bakoverkompatibilitet.

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%BWVOICE-PORTAL-ANTALL-1%	tom	nummer	Klienten ringer dette nummeret som vanligvis angis ved hjelp av en eksisterende Cisco BroadWorks-systemkode, når han ringer talepost.
%ENABLE_MWI_WXT%	usann	sant, usant	Sett til "true" for å aktivere MWI. Sett til "false" for å deaktivere MWI.
%MWI_MODE_WXT%	tom	implisitt, eksplisitt	Sett til "eksplisitt" for å sende SIP SUBSCRIBE for MWI hendelsespakke når MWI er aktivert. Bruk av "implisitt" sender ikke SIP SUBSCRIBE for MWI hendelsespakke når MWI er aktivert. Hvis den står tom, deaktiveres MWI.

6.1.28 Transkripsjon av talepost for Webex Calling

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

Funksjonen bør 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 config (det aktiverte attributtet i <services><voice-mail><transkripsjon>koden må settes til "true").

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	usann	sant, usant	[Webex Calling Only] Kontrollerer tilgjengeligheten av transkripsjon av talepost bare hvis Visual Voicemail er aktivert.

6.1.29 Samtaleinnstillinger

6.1.29.1 Alltid viderekobling

Følgende egendefinerte kode kan brukes til å kontrollere tilgjengeligheten til tjenesten Cisco BroadWorks Call Forwarding Always i Webex for Cisco BroadWorks-klienten.

```
<config>
<tjenester><tilleggstjenester>
<viderekobling-alltid aktivert="%ENABLE_CALL_FORWARDING_ALWAYS_WXT%"/>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	usann	sant, usant	Kontrollerer tilgjengeligheten til tjenesten Always Call Forwarding Always (Viderekobling av samtale). Funksjonen er som standard deaktivert.

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

6.1.29.2 Viderekobling til talepost

Fra og med versjon 43.9 gir appen Webex et alternativ for å kontrollere tilgjengeligheten til videresending til talepost. Funksjonen er aktivert som standard, og følgende konfigurasjonsalternativ kan brukes til å deaktivere den.

```
<config>
<tjenester>
   <talepost>
      <videresending aktivert="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	sann	sant, usant	Kontrollerer tilgjengeligheten til viderekobling til talepost. Funksjonen aktiveres som standard.

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

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

6.1.29.3 BroadWorks hvor som helst (Single Number Reach)

Følgende egendefinerte koder kontrollerer tilgjengeligheten til BroadWorks Anywhere og tilgjengeligheten av innstillingene i Webex for Cisco BroadWorks-klienten. Merk at navnet på denne funksjonen i klienten er *Manage My Numbers*.

```
<config>
<tjenester><tilleggstjenester>
<broadworks-anywhere enabled="%ENABLE_BROADWORKS_ANYWHERE_WXT%">
      <description enabled="%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%"/>
```


Cisco konfidensielt

```
        <alert-all-locations
enabled="%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%"
default="%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%"/>
        <anropskontroll aktivert = "%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%"/>
        <svarbekreftelse aktivert =
"%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%	usann	sant, usant	Aktiverer BroadWorks Anywhere (BWA) på konfigurasjonsnivå.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	sann	sant, usant	Kontrollerer om beskrivelsen av BWA-plasseringen skal være tilgjengelig for brukeren.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	usann	sant, usant	Sett til "true" for å gjøre Varsle alle lokasjoner for BWA-tjenesten tilgjengelig for brukeren. Sett til "false" for å gjøre Varsle alle steder for BWA-tjenesten ikke tilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	usann	sant, usant	Kontrollerer om programmet skal aktivere tilstanden Varsle alle plasseringer ved å legge til andre eller hver påfølgende nye BWA-plassering.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	usann	sant, usant	Kontrollerer om samtalestyringen for BWA-plasseringen skal være tilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	usann	sant, usant	Kontrollerer standardtilstanden for samtalekontrollen for BWA-plasseringen.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	usann	sant, usant	Kontrollerer om viderekoblingshemmeren for BWA-plasseringen skal være tilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	usann	sant, usant	Kontrollerer standardtilstanden for avledningshemmeren på BWA-plasseringen.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	usann	sant, usant	Kontrollerer om svarbekreftelsen for BWA-plasseringen skal være tilgjengelig for brukeren.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	usann	sant, usant	Kontrollerer standardtilstanden for svarbekreftelsen for BWA-plasseringen.

Cisco konfidensielt

6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger

Webex for Cisco BroadWorks-klienten gir tilgang til en innstillingsportal (selvhjelp), der brukeren kan konfigurere noen av program- og tjenesteinnstillingene.

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

> **MERK:** Det anbefales å skjule innstillingene som allerede er synlige i applikasjonen som Call Center (se avsnitt *6.1.31 Call Center / Call Queue Login /* Logg ut) og BroadWorks Anywhere (se avsnitt *6.1.29.3 BroadWorks hvor* som helst). Remote Office-tjenesten anbefales også å skjules fordi den har blitt etterfulgt av BroadWorks Anywhere-tjenesten.

Følgende egendefinerte kode kan brukes til å konfigurere URL-adressen for innstillingsportalen (Self Care eller CSWV). Hvis koden er tom, er ikke koblingen til innstillingsportalen synlig for brukeren i programmet.

```
<config>
<tjenester>
<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-innstillinger>
   <tjenestenavn="Alltid viderekobling av anrop"
synlig="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <tjenestenavn="Viderekobling opptatt" synlig
="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <tjenestenavn="Viderekobling kan ikke nås" synlig
="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
   <tjenestenavn="Viderekobling uten svar" synlig
="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <tjenestenavn="Ikke forstyrr" synlig="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
   <tjenestenavn="Anonym anropsavvisning" synlig =
"%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <tjenestenavn = "Samtidig ringing personlig" synlig =
"%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <tjenestenavn="Sekvensiell ring" synlig =
"%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <tjenestenavn="Automatisk tilbakeringing"
synlig="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <tjenestenavn = "Samtale venter" synlig = "%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <tjenestenavn="Leveringsblokkering for anropslinje-ID" synlig
="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <tjenestenavn="Personlig assistent"
synlig="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
   <tjenestenavn="Call Center - Standard"
visible="%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%"/>
   <service name = "BroadWorks Anywhere" synlig =
"%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%"/>
   <tjenestenavn = "BroadWorks Mobility" synlig =
"%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <tjenestenavn = "Remote Office" synlig = "%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <tjenestenavn="Talemeldingsbruker" synlig
="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
```


Cisco konfidensielt

```
</web-call-settings>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%WEB_CALL_SETTINGS_TARGET_WXT%	utvendig	ekstern, CSW	Styrer administrasjonsportalmodusen. Sett til "ekstern" for å åpne konfigurert URL-adresse for portalinnstilling i en ekstern nettleser. Sett til "csw" for å åpne CSW-portalen i en innebygd nettleser ved hjelp av delen for ekstra parametere <services><web-call-settings> til fra POST-forespørselen.
%WEB_CALL_SETTINGS_URL_WXT%	tom	URL-streng	URL-adresse til innstillingsportalen. Eksempel: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Alltid viderekobling av anrop skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Ikke forstyrr (DND) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Anonym anropsavvisning (ACR) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Viderekobling ved opptatt (CFB) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Call Forwarding Not Reachable (CFNR) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Viderekobling uten svar (CFNA) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet SIMRING skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Sequential Ring (SEQRING) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Remote Office (RO) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet for automatisk tilbakeringing (ACB) skal være synlig for brukeren i de nettbaserte innstillingene.

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Samtale venter skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet CLIDB (Calling Line ID Delivery Blocking) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet for personlig assistent skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet BroadWorks Anywhere (BWA) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Telefonsenter skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet BroadWorks Mobility (BWM) skal være synlig for brukeren i de nettbaserte innstillingene. Den anbefalte verdien er for øyeblikket "false" på grunn av interoperabilitetsproblemer mellom Webex for Cisco BroadWorks og BroadWorks Mobility.
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	sann	sant, usant	Kontrollerer om alternativet Talebehandling (VM) skal være synlig for brukeren i de nettbaserte innstillingene.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	usann	sant, usant	Kontrollerer om de nye samtaleinnstillingene WebView varemerkingen 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%	sann	sant, usant	Kontrollerer om alternativene for e-post-/talepostmeldinger er synlige i de nettbaserte innstillingene.
%USER_PORTAL_SETTINGS_URL_WXT%	tom	URL-streng	Angir URL-adressen til portalen for brukerinnstillinger. Hvis du vil aktivere funksjonen og vise knappen Få tilgang til brukerportal i brukergrensesnittet, må denne egendefinerte koden ikke være tom. For eksempel: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	utvendig	Ekstern, intern	Angir om URL-adressen skal åpnes i en innebygd eller ekstern webleser.

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	usann	Sant, usant	Gjelder bare når innebygd nettleser er konfigurert (USER_PORTAL_SETTINGS_TARGET_WXT=intern). Når den er aktivert, brukes HTTP POST-forespørsel, og BroadWorks-kortvarig token legges til som en del av BODY. Når URL-adressen er deaktivert, åpnes den med HTTP GET.

MERK 1: Anropsinnstillingene WebView URL-adressen skal alltid ha en etterfølgende "/" konfigurert. For eksempel: https://<XSP-FQDN>/<CSW-Context-Path>/

MERK 2: Minimum versjon av programmet for samtaleinnstillinger WebView som støttes, er 1.7.5.

For installasjon på Cisco BroadWorks versjon 21.0, se ytterligere trinn beskrevet i *Webex For Cisco BroadWorks Solution Guide*.

6.1.31 Call Center / Call Queue Login / Logg ut

Webex-appen gir tilgang til agentinnstillingene for telefonsenteret (samtalekø). Hvis en bruker er klargjort for telefonsenteret, kan brukeren logge på et telefonsenter og vise tilgjengelige anropskøer, i tillegg til å bli med/fjerne koblingskøer og angi status for automatisk telefondistribusjon (ACD).

Fra og med skrivebordsversjon 42.8 og mobilversjon 42.12 er ikke lenger agenten for telefonsenter (samtalekø) basert på webvisningen Samtaleinnstillinger (se avsnitt *6.1.30 Innstillingsportal og nettbaserte samtaleinnstillinger*). Agentkonfigurasjonen Call Center (samtalekø) er tilgjengelig via bunnteksten på skrivebordet og innstillingene i appen Mobile Webex.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_CENTER_WXT%	usann	sant, usant	Aktiverer telefonsenterstøtte.

6.1.32 XSI-rot og stier

Webex for Cisco BroadWorks-klienten bruker følgende koder til å kontrollere XSI-banen for rot, handlinger og hendelser hvis de må konfigureres til å avvike fra banene som brukes for pålogging.

Cisco konfidensielt

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

Banene for hendelser og handlinger endres vanligvis på grunn av krav til varemerking for å fjerne *com.broadsoft-domenereferansen* fra URL-banene til XSI HTTP-forespørsler som utføres av klienten.

```
<config>
<protokoller><xsi>
       <stier>
              <rot>%XSI_ROOT_WXT%</root>
              <handlinger>%XSI_ACTIONS_PATH_WXT%</handlinger>
              <hendelser>%XSI_EVENTS_PATH_WXT%</hendelser>
       </stier>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%XSI_ROOT_WXT%	Fortsetter å bruke den opprinnelige som ble brukt til konfigurasjon shenting.	URL-streng	XSI-roten for alle XSI-operasjoner. Eksempel: https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	streng	Angir XSI-handlingsbanen. Den skal starte og slutte med "/" og bare inneholde handlingskonteksten. Eksempel: /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	streng	Angir XSI-hendelsesbanen. Den skal starte og slutte med "/" og bare inneholde hendelseskonteksten. Eksempel: /com.domain.xsi-events/

6.1.33 XSI-hendelseskanal

XSI-hendelseskanalen brukes til forskjellige tjenester, for eksempel:

- XSI-kontroller midt i samtalen
- Statusvarsler for samtaleinnstillinger
- Call Recording (Innspilling av samtale)

XSI-hendelsers hjerterytme brukes til å holde XSI-hendelseskanalen åpen, og hjerteslagintervallet kan angis ved hjelp av følgende parameter.

```
<config>
<protokoller><xsi>
<event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
    <hjerteslagIntervall> %CHANNEL_HEARTBEAT_WXT%</hjerteslagIntervall>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_XSI_EVENT_CHANNEL_WXT%	sann	sant, usant	Kontrollerer om XSI-hendelseskanalen er aktivert. Den bør settes til "true" for å motta, for eksempel tjenesterelaterte hendelser for kontroll under samtalen. Den anbefalte verdien er "true".
%CHANNEL_HEARTBEAT_WXT%	10000	nummer	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 finnes under *config/services/calls/* in *the audio/codecs* og *video/codecs* sections. 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:

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

Cisco konfidensielt

```
<config>
<tjenester><samtaler>
  <lyd>
    <kodeker>
      <codec name = "opus" priority = "1" nyttelast = ""/>
      <codec name = "xCodec" mode = "HP" priority = ".99" nyttelast = ""/>
      <codec name = "xCodec" mode = "ULP" priority = ".98" nyttelast = ""/>
      <codec name = "G722" priority = ".9" nyttelast = ""/ >
      <codec name = "PCMU" priority = ".8" nyttelast = ""/>
      <codec name = "PCMA" priority = ".7" nyttelast = ""/>
      <codec name = "G729" priority = ".5" nyttelast = "" vad = ""/>
      <codec name = "iLBC" priority = ".4" nyttelast = "" framelength = "30"/>
      <codec name = "telefon-event" nyttelast = "101" in-band = "false"/>
    …
  <video>
    <kodeker>
      <codec name = "H264" nyttelast = "109" resolution = "CIF" framerate = "25"
bitrate = "768000" prioritet = "1.0">
        <pakkemodus>0</pakkemodus>
```

Klienten støtter H.264 som videokodek. Videooppløsningsattributtet kan brukes til å angi én 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 tabellen nedenfor.

Løsning	Video Størrelse *	FPS (bilder 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 Cisco BroadWorks-klienter avhenger av egenskapene til begge klientene – den vil være den laveste av de to og vil være den samme for begge klientene.

Videooppløsningen for en videosamtale forhandles under øktoppsettet og er basert på egenskapene til de to endepunktene. Videosamtaleoppløsningen er den samme på begge endepunktene. Det vil si at hvis Webex for Cisco BroadWorks-endepunkter 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.

Pakkemodusen kan konfigureres til å være SingleNAL (0) eller Ikke-sammenflettet (1). Malen bruker SingleNAL som standard (<pakkemodus>0</pakkemodus>).

Cisco konfidensielt

Konfigurasjon av telefonhendelser, enkeltstående eller flere, støttes også. Under kodekforhandling sender klienten alle konfigurerte kodeker, inkludert telefonhendelse. Når lydkodeken er valgt, søker den etter telefonhendelse i tilbudet. Hvis tilbudet har telefonhendelsen med samplingsfrekvensen for den forhandlede lydkodeken, velges denne telefonhendelsen. Ellers brukes den første telefonhendelsen i listen.

Hvis det er forhandlet minst én telefonhendelse, sendes tofargede flerfrekvenser (DTMFer) som RTP pakker ved hjelp av den tilsvarende nyttelasttypen. Og hvis det ikke forhandles om noen telefonhendelser 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" nyttelast = "100" in-band = "false" />
<codec name = "telephone-event" nyttelast = "101" clockrate = "48000" in-band =
"false" />
```

Hvis det forhandles om en lydkodek med en samplingsfrekvens på 48 kbps, brukes telefonhendelsen med nyttelast 101.

6.1.34.1 AI-kodek

Fra og med versjon 44.8 introduserer Webex-appen støtte for en ny lydkodek - AI Codec (xCodec). Denne lydkodeken brukes under ugunstige nettverksforhold for å oppnå bedre samtalekvalitet. Webex Media Engine i Webex appen kontrollerer enhetsegenskapene, sporer mediekvaliteten, og AI-kodeken kan brukes hvis den støttes og aktiveres gjennom konfigurasjonsfilen.

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

6.1.35 SIP-URI-oppringing

For øyeblikket er SIP-URI-oppringing gjennom BroadWorks ikke tilgjengelig, og som standard rutes alle SIP-URI-anrop gjennom Locus, også kjent som "Free Calling". 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>
    <tjenester>
        <samtaler>
            <sip-uri-dialing enable-locus-
calling="%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%"/>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	sann	sant, usant	Kontrollerer om SIP-URIen skal rutes gjennom Locus (sann) eller blokkeres (usann).

6.1.36 Anropslogg på tvers av alle enheter

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

> **MERK:** Enhetlig anropslogg bør aktiveres 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%	usann	sant, usant	Kontrollerer om programmet skal bruke Unified Call History eller klientsiden (lokal) loggen.

6.1.37 Deaktiver videoanrop

Versjon 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-samtaler.

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

- Brukeren vil ikke se innstillingen "Godta innkommende anrop med videoen min på"
- Alle innkommende videosamtaler hvis akseptert, vil være lyd seg
- Brukeren vil ikke kunne eskalere en samtale til video- og videoeskaleringer blir automatisk avvist

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SIP_VIDEOCALLS_WXT%	sann	sant, usant	Kontrollerer tilgjengeligheten av SIP-videosamtaler via BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	sann	sant, usant	Kontrollerer tilgjengeligheten av Locus-videosamtaler (gratis).

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Skrivebord – sant Mobil / Tablet - falsk	Sant, usant	Kontrollerer standardverdien for innstillingen «Godta innkommende anrop med videoen min på».

6.1.38 Nødanrop (911) - Posisjonsrapportering med E911-leverandør

Desktop and Tablet Webex-klienten støtter E911-posisjonsrapportering ved hjelp av RedSky, Intrado eller båndbredde som en E911-nødanropsleverandør for Webex for BroadWorks-distribusjon. E911-leverandøren gir posisjonsstøtte per enhet (for Webex skrivebords- og nettbrettapper og HELD-kompatible MPP-enheter) og et nettverk som ruter nødanrop til PSAP-er (Public Safety Answering Points) rundt om i USA, dets territorier (Guam, Puerto Rico og Jomfruøyene) og bare Canada. Tjenesten aktiveres per lokasjon.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	usann	Sant, usant	Aktiverer E911-leverandøren Emergency Location Platform.
%BWE911-PRIMÆR-HELDURL%	tom	streng	Angir URL-adressen til E911-leverandørens nødplasseringsplattform som støtter HOLDD-protokollen.
%BWE911-CUSTOMERID%	tom	streng	Kunde-ID (HeldOrgId, CompanyID) som brukes for HTTPS-forespørselen fra E911-leverandøren.
%BWE911-SECRETKEY%	tom	streng	Hemmeligheten for å godkjenne E911-leverandøren HTTPS-forespørsel.
%BWE911-NØDNUMMER-LISTE%	tom	CSV streng	Listen over nødnumre som støttes av E911-leverandøren.
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (brukeren blir ikke spurt igjen)	antall [0 - 43200]	Tidsavbruddet i minutter som brukes til å minne brukeren på å oppdatere nødplasseringen hvis den gjeldende ikke angis eller er ugyldig. Den foreslåtte verdien hvis besluttet å aktivere: 1440 (én dag).

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (brukeren kan alltid avbryte dialogboksen)	antall [-1 - 100]	Tidspunktene brukerne kan lukke dialogboksen for plassering før plassering blir obligatorisk (det vil si at de ikke kan lukke plasseringsvinduet). Mulige verdier: ▪ N = -1 (brukeren kan alltid avbryte dialogboksen) ▪ 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)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	aggressive, once_per_login	once_per_login	Definerer virkemåten for E911-posisjonsforespørsler. Den "aggressive" verdien vil vise dialogen til brukeren ved hver nettverksendring til et ukjent sted, mens "once_per_login" -verdien bare viser dialogboksen én gang, og forhindrer ytterligere popup og distraksjoner for brukeren.

MERK 1: BWE911-***-koder er "Dynamisk innebygde systemkoder". Hvis du vil ha mer informasjon, kan du se avsnittet *5.7 Cisco BroadWorks dynamisk innebygd system Tags*.

MERKNAD 2: Hvis VOIP-anrop er deaktivert, er den eneste meningsfulle verdien for nødoppringingssekvens (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) bare cs.

6.1.39 PAI som identitet

For **innkommende anrop styrer denne nye parameteren prioriteten til SIP From- og P-Asserted-Identity-overskrifter (PAI), og hva som skal brukes som en anropslinjeidentitet**. Hvis det er en X-BroadWorks-Remote-Party-Info-overskrift i den innkommende SIP INVITE, brukes den med prioritet over SIP From- og PAI-overskriftene. Hvis det ikke er noen X-BroadWorks-Remote-Party-Info-overskrift i den innkommende SIP INVITE, bestemmer denne nye parameteren om SIP From-hodet er prioritert over PAI-overskriften eller omvendt.

Hvis det aktiverte attributtet for <use-pai-as-calling-identity> -koden er satt til "true", brukes PAI-overskriften med prioritet over Fra-overskriften. Denne anropende partidentiteten brukes til å løse kontakten og presentere den for brukeren.

Denne logikken brukes ikke for **utgående anrop**. I 18X, 200 OK-svarene mottas den tilkoblede linjeidentiteten, slik at Webex-programmet alltid bruker SIP PAI-overskriften med prioritet.

Cisco konfidensielt

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

6.1.40 Deaktiver skjermdeling

Versjon 42.5 legger til muligheten til å kontrollere tilgjengeligheten av skjermdeling. Når skjermdeling er deaktivert:

- Brukeren vil ikke se alternativet for å starte skjermdeling i 1-1-samtaler
- De innkommende skjermdelingsforespørslene blir avvist, og brukeren vil se en informativ melding

Denne funksjonen er aktivert som standard.

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

6.1.41 Spam Call Indication

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_SPAM_INDICATION_WXT%	usann	sant, usant	Kontrollerer tilgjengeligheten av spam-anropsindikasjonen på skjermbildet for innkommende anrop og anropsloggen bare for Webex Calling.

6.1.42 Støyfjerning og båndbreddeutvidelse for PSTN-/mobilsamtaler

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

Versjon 44.2 av appen Webex introduserer nye forbedringer for tale-AI for smalbåndsanrop via lydmedier.

Cisco konfidensielt

- 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 forståeligheten 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 indikatoren "Smart lyd – ekstern" og kan kontrollere Speech AI-forbedringene for de innkommende lydmediene.

Som standard er disse taleforbedringene aktivert og slått på. Brukeren kan kontrollere den opprinnelige tilstanden gjennom innstillingene for smartlyd i lydinnstillingene.

```
<config>
   <tjenester>
      <samtaler>
         <taleforbedringer aktivert="%ENABLE_SPEECH_ENHANCEMENTS_WXT%"/>
```

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

MERK: Støyfjerning er nå en del av de ekstra taleforbedringene, og <støyfjerning>-koden er avskrevet av den nye <taleforbedringer>-koden. Den egendefinerte koden for støyfjerning %ENABLE_NOISE_REMOVAL_WXT% er også avskrevet.

6.1.43 QoS-DSCP-merking

QoS DSCP-merking støttes med Webex app som kaller medier 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 slippe pakker.

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

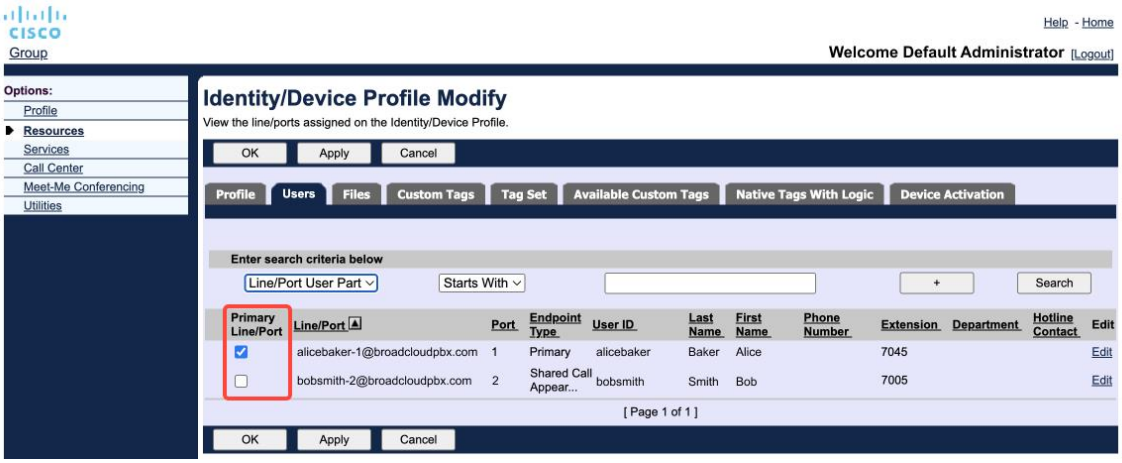
Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_AUDIO_QOS_WXT%	sann	Sant, usant	Aktiverer QoS for lydsamtaler.

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%AUDIO_QOS_VALUE_WXT%	46	0-63	Angir QoS-verdien for den valgte QoS-typen for lydanropene. Merk: Standardverdien brukes hvis ingen verdi er angitt, eller hvis verdien ikke kunne analyseres.
%ENABLE_VIDEO_QOS_WXT%	sann	Sant, usant	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 angitt, eller hvis verdien ikke kunne analyseres.

6.1.44 Primær profil

Med integreringen av de delte linjene (*6.1.51.1 Skrivebord – utseende på* delt linje**Error! Reference source not found.**), hvis brukerens linje deles med en annen bruker, kan det være flere profiler av samme type konfigurert for brukeren. Hvis du vil velge riktig profil for å logge på telefontjenestene, har Cisco BroadWorks blitt forbedret for å indikere om en bruker eier en enhet, dvs. at den er tilordnet hovedlinjen/-porten for en enhet - hvis du vil ha mer informasjon om Cisco BroadWorks-oppdateringen, kan du se Owner Flag In Device List To Support Webex Client Shared Lines.



Primærlinje-/portkonfigurasjon for identitets-/enhetsprofil i administrasjonsportalen

Cisco konfidensielt

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

Den samme begrensningen gjelder for enhetene brukeren kan pare i Desktop Webex-appen. Brukeren kan bare se og pare med enheter han eier. Dette forhindrer sammenkobling med enheter fra en annen bruker som er tilordnet delt eller virtuell linje. Verdien for den samme konfigurasjonsparameteren gjelder også for denne begrensningen.

```
<config>
<tjenester><samtaler>
<device-owner-restriction enabled="%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%"/>
```

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

MERK: Det anbefales eierbegrensning for å være aktivert. Hvis 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.

6.1.45 Blokkeringsliste (bare Webex Calling)

Fra og med 43.5 introduserer Webex-appen 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 – Anropsinnstillinger og Anropslogg. I innstillingene kan brukeren se listen over blokkerte numre og redigere den. I anropsloggen kan brukeren se anropsloggoppføringene for anropene som blokkeres av den brukerdefinerte blokkeringslisten. Disse oppføringene har sperret indikasjon hvis nummeret er i den brukerdefinerte blokkeringslisten, og brukeren vil ha muligheten til å oppheve blokkeringen av nummeret direkte for en gitt post. Blokker alternativet er også tilgjengelig.

Regler for numrene som er lagt til i den brukerdefinerte blokkeringslisten:

- Tallformat
  - Blokkering fra anropsinnstillingene gjelder E.164 formatbegrensning lokalt i Webex appen
  - Blokkering fra anropsloggen er tillatt for alle Webex Calling oppføringer

Cisco konfidensielt

- Cisco BroadWorks kan tillate eller avvise forespørsler om nye numre som legges til i blokkeringslisten, basert på tallformatet

- Interne numre – innkommende anrop fra interne numre leveres 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 admin-definerte blokkeringslisten, som ikke kan konfigureres av brukeren og bare kan kontrolleres av administratorer via kontrollhuben. Det er INGEN anropsloggoppføringer for innkommende anrop som blokkeres av den administratordefinerte blokkeringslisten.

Den brukerdefinerte blokkeringslisten brukes etter STIR/SHAKEN, den administratordefinerte blokkeringslisten og policyene for anonym avvisning av anrop.

```
<config>
<tjenester><samtaler>
<anropsblokk aktivert="%ENABLE_CALL_BLOCK_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_BLOCK_WXT%	sann	sant, usant	Aktiverer den brukerdefinerte blokkeringslisten Sett til "true" for å se blokkeringslisten i Anropspreferanser og Anropslogg

MERK: Denne funksjonen avhenger av at tjenesten Cisco BroadWorks Call Block er tilordnet brukeren.

6.1.46 Implementering av medietilpasning og resiliens (MARI)

6.1.46.1 Tilpasning av priser

Den 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 dynamisk bithastighetsjustering tilpasser anropshastigheten til den tilgjengelige variable 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 er redusert, vil det oppstå opp-hastighet av bithastigheten.

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

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

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

Cisco konfidensielt

FEC gir redundans til den overførte informasjonen ved hjelp av en forhåndsbestemt algoritme. Redundansen gjør det mulig for mottakeren å 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 omvendt kanal (for eksempel RTCP) for å be om ny overføring av data, men denne fordelen er på bekostning av en fast høyere båndbredde fremover (flere pakker sendt).

Endepunktene bruker ikke FEC på båndbredder lavere enn 768 kbps. Det må også være minst 1.5 % pakketap før FEC innføres. Endepunkter overvåker vanligvis effektiviteten til FEC, og hvis FEC ikke er effektiv, brukes den ikke.

FEC bruker mer båndbredde enn ny overføring, 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 RTX eller FEC dynamisk, avhengig av forhandlet båndbredde og forsinkelsestoleranse for en gitt mediestrøm. FEC resulterer i høyere båndbreddebruk på grunn av overflødige videodata, men det introduserer ikke ytterligere forsinkelse for å gjenopprette tapte pakker. Mens RTX ikke bidrar til høyere båndbreddeutnyttelse, fordi de RTP pakkene bare sendes på nytt når mottakeren indikerer pakketap i tilbakemeldingskanalen RTCP. RTX introduserer pakkegjenopprettingsforsinkelse på grunn av tiden det tar for den RTCP pakken å nå mottakeren fra avsenderen og for den sendte pakken på nytt for å nå mottakeren fra avsenderen.

FEC må være aktivert for å ha RTX aktivert.

```
<config><services><calls>
<lyd>
       <forbedringer av lydkvalitet>
              <Mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <nyttelast>111</nyttelast>
                            <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>
                            <bestill>FEC_SRTP</bestill>
                     </fec>
                     <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
                            <nyttelast>112</nyttelast>
                            <tid>180</tid>
                            <data-flow>1</data-flow>
                            <bestill>RTX_SRTP</bestill>
                     </RTX>
              </mari>
...
<video>
       <forbedringer av videokvalitet>
              <Mari>
                     <fec enabled="%ENABLE_VIDEO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <nyttelast>111</nyttelast>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <m>8</m>
                            <multi_ssrc>1</multi_ssrc>
```


Cisco konfidensielt

```
                        <non_seq>1</non_seq>
                        <feedback>0</feedback>
                        <bestill>FEC_SRTP</bestill>
                    </fec>
                    <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                        <mari-rtx>90000</mari-rtx>
                        <nyttelast>112</nyttelast>
                        <tid>180</tid>
                        <data-flow>1</data-flow>
                        <bestill>RTX_SRTP</bestill>
                    </RTX>
                </mari>
```

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

6.1.47 Samtidige samtaler med samme bruker

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

Denne funksjonen er nyttig for enkelte distribusjoner der den presenterte identiteten til anropet ikke er den samme som den tilkoblede identiteten. Dette fører til manglende evne til å initiere en overvåket overføring tilbake til det opprinnelige partiet. Ved å aktivere denne funksjonen vil brukeren kunne håndtere flere samtidige samtaler med samme eksterne part.

```
<config>
   <tjenester>
      <samtaler>
         <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%	usann	sant, usant	Angir om Webex appen bare kan ha ett eller flere WxC-anrop med samme bruker.

Cisco konfidensielt

6.1.48 RTCP-XR

Fra og med versjon 43.8 legger Webex App til forhandling for utveksling av RTCP-XR-pakker under en samtale. Forhandlinger finner sted under etableringen av SIP INVITE-økten. 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, bare for Webex Calling, blir disse ekstra beregningene sendt gjennom SIP BYE og på denne måten eksponert i Control Hub.

```
<config>
<protokoller><sip>
   <RTCP-XR>
      <forhandling aktivert="%ENABLE_RTCP_XR_NEGOTIATION_WXT%"/>
```

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

6.1.49 Informasjon om viderekobling av anrop

Versjon 44.2 av Webex appen introduserer konfigurerbart alternativ for å kontrollere synligheten til viderekobling og viderekoblingsinformasjon i samtalerelaterte skjermbilder og anropslogg.

```
<config>
<tjenester><samtaler>
<call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	sann	sant, usant	Kontrollerer synligheten til informasjonen om viderekobling og viderekobling av anrop. Sett til "true" for å se informasjonen i de samtalerelaterte skjermbildene og anropsloggen.

6.1.50 Oppringer-ID

6.1.50.1 ID for utgående anroper

Webex mobilappene Mobile (versjon 44.2) og Desktop (versjon 44.3) introduserer en ny mulighet der brukeren kan velge foretrukket ekstern anroper-ID for utgående anrop. Listen over tilgjengelige alternativer inkluderer:

- Direkte linje (standard)

Cisco konfidensielt

- Plasseringsnummer
- Egendefinert nummer fra samme organisasjon
- Samtalekøer som brukeren er en del av, som gjør det mulig for agenter å bruke anroper-ID-nummeret sitt
- Arbeidsgrupper som brukeren er en del av, som gjør det mulig for agenter å bruke anroper-ID-nummeret sitt
- Skjul anroper-ID

Notater:

- Listen over alternativer avhenger av linjen:
  - Primærlinje - komplett sett med alternativer
  - Delte linjer – ikke tilgjengelig
  - Virtuelle linjer – bare alternativer for samtalekø
- Hvis den allerede valgte identiteten ikke lenger er tilgjengelig, brukes brukerens standard anroper-ID
- Nødanrop bruker alltid brukerens nødnummer
- Avskriver <utgående anrop> under delen <tjenester><call-center-agent>

Listen over tilgjengelige alternativer kan konfigureres via administrasjonsportalen. Det finnes også separate egendefinerte DMS-koder for å kontrollere tilgjengeligheten til disse forbedringene i Webex appen.

```
<config>
<tjenester><samtaler>
   <anroper-ID>
      <utgående anrop aktivert = "%ENABLE_CLID_OUTGOING_CALLS_WXT%">
         <tilleggsnumre aktivert="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
         <call center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
         <søkegruppe aktivert="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
         <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
      </utgående-samtaler>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_OUTGOING_CALLS_WXT%	usann	sant, usant	Aktiverer nummervalg for anropslinje-ID for utgående anrop.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	usann	sant, usant	Kontrollerer tilgjengeligheten til tilleggsnumrene som er konfigurert for brukeren.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	usann	sant, usant	Kontrollerer tilgjengeligheten til telefonsenternumrene (DNIS) som er konfigurert for brukeren.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	usann	sant, usant	Kontrollerer tilgjengeligheten til søkegruppenumrene som er konfigurert for brukeren.

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
"%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	usann	sant, usant	Aktiverer leveringsblokkering av anroper-ID som valg for utgående anrop.

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

6.1.50.2 Navn på ekstern anroper-ID

Når et anrop mottas/startes, sender Cisco BroadWorks visningsnavnet til den eksterne parten i SIP INVITE. Den brukes som standard av Webex appen. Samtidig starter Webex-appen kontaktløsing mot flere kilder, med følgende prioritet:

- Felles identitet (CI)
- Kontakttjeneste (egendefinerte kontakter)
- Outlook-kontakter (skrivebord)
- Lokal adressebok (mobil)

Hvis en vellykket kontaktløsning oppstår mot noen av søkekildene, oppdateres visningsnavnet til den eksterne parten. Dessuten, hvis kontakten er funnet i CI, er samtaleøkten knyttet til de Webex skytjenestene til samme bruker, og gir muligheten til å se avataren og tilstedeværelsen til den eksterne parten, ha en chat, skjermdeling, mulighet til å eskalere til et Webex skymøte, etc.

Versjon 44.5 av Webex appen legger til konfigurerbart alternativ for å ignorere kontaktoppløsningen og alltid beholde Cisco BroadWorks-visningsnavnet for samtaler med arbeidsområder eller RoomOS-enheter som brukes til 1:1 Cisco BroadWorks-samtale.

```
<config>
<tjenester><samtaler>
   <anroper-ID>
      <eksternt navn>
         <maskinmodus="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	Løst	Løst, SIP	Kontrollerer visningsnavnet for den eksterne parten for arbeidsområder og RoomOS-enheter. Bruk "sip" for å ignorere kontaktoppløsningen og bruke visningsnavnet som ble mottatt i SIP INVITE-økten.

Cisco konfidensielt

6.1.51 Flere linjer

Den Webex brukeren kan ha en primærlinje og opptil 9 sekundære linjer. Sekundære linjer kan være delte eller virtuelle (bare Webex anrop).

Webex app får linjekonfigurasjonen gjennom DMS-konfigurasjonsfilen som lastes ned ved pålogging og hver 12. Hvis oppdateringen av linjekonfigurasjonen oppdages, blir brukeren bedt om å starte programmet på nytt for å bruke endringene. Ny pålogging av brukeren vil oppdage og bruke eventuelle linjekonfigurasjonsoppdateringer umiddelbart.

Nedenfor vises delen av DMS-konfigurasjonsmalen som er relatert til støtte for flere linjer for både stasjonær og mobil.

```
<config>
<protokoller>
   < nippe>
       <linjer multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
          <personlig>
             <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
          </personlig>
          <line lineType="%BW-MEMBERTYPE-1 %">
             <external-id>%BWUSEREXTID-1 %</external-id>
             ...
          </linje>
          <line lineType="%BW-MEMBERTYPE-2 %">
             <external-id>%BWUSEREXTID-2 %</external-id>
             ...
          </linje>
          ...
          <line lineType="%BW-MEMBERTYPE-10 %">
             <external-id>%BWUSEREXTID-10 %</external-id>
             ...
          </linje>
```

For å kontrollere funksjonen med flere linjer, bruk den dedikerte egendefinerte taggen.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_MULTI_LINE_WXT%	usann	Sant, usant	Aktiverer støtte for flere linjer (hvis konfigurert). Hvis deaktivert (satt til "false"), vil bare den første linjen som er konfigurert, bli brukt av programmet.

MERK 1: Funksjonen Boss-Admin (Executive-Assistant)-støtte er ikke tilgjengelig i kombinasjon med konfigurasjon med flere linjer.

MERKNAD 2: Se "Shared line appearance" i Webex-for-Cisco-BroadWorks-Solution-Guide for ytterligere BroadWorks-krav.

6.1.51.1 Skrivebord – utseende på delt linje

Fra og med versjon 42.12 legger programmet Webex til støtte for delte linjer. Administratoren bør konfigurere de delte samtalene for hver delte linje.

Cisco konfidensielt

Versjon 43.12, er Webex-appen forbedret slik at den tillater flytting (gjenoppta lokalt) en samtale på vent på en delt eller virtuell linje, håndtert av en annen bruker eller av samme bruker på en annen enhet. Hvis du vil ha mer informasjon, kan du se *6.2.13 Flytt samtale*.

6.1.51.2 Skrivebord – virtuelle linjer (kun Webex Calling)

Bare for Webex Calling distribusjon støtter appen Webex konfigurasjon av flere linjer ved hjelp av virtuelle linjer. Funksjonelt samsvarer konfigurasjonen med virtuelle linjer med flere linjer ved hjelp av delte linjer - å ha muligheten til å se de virtuelle linjene som er konfigurert for brukeren og bruke dem til innkommende og utgående samtaler.

Versjon 43.4 utvider støtten for virtuelle linjer og legger til gruppesamtaleparkering og henting av samtaleparkering.

Versjon 43.12, er Webex-appen forbedret slik at den tillater flytting (gjenoppta lokalt) en samtale på vent på en delt eller virtuell linje, håndtert av en annen bruker eller av samme bruker på en annen enhet. Hvis du vil ha mer informasjon, kan du se *6.2.13 Flytt samtale*.

6.1.51.3 Mobil (bare Webex Calling)

Versjon 45.4 legger til støtte for flere linjer (delt og virtuelt) bare for Webex Calling distribusjon i mobilversjonen av appen Webex. Linjetilordningen gjelder både for appen for stasjonær og mobil Webex.

På grunn av spesifikasjonene til den mobile plattformen kan brukeren ha opptil to samtidige samtaler samtidig på hvilken som helst av linjene.

> **MERK 1**: Hvis Anrop med opprinnelig oppringer er aktivert (se *6.3.5.1 Ring med opprinnelig oppringing*), er flerlinje deaktivert.
>
> **MERK 2**: Multi-line for Tablet-versjonen støttes ikke.

6.1.52 Forbedret SIP-autorisasjon

Versjon 45.4 av Webex appen gir et konfigurerbart alternativ for å optimalisere SIP-kommunikasjonen ved å dele autorisasjonen mellom alle SIP-øktene. Appen lagrer autorisasjonen og bruker den på nytt til den fortsatt er gyldig.

Denne funksjonen fremskynder SIP-kommunikasjonen mellom serveren og Webex appen, reduserer trafikken, senker tiden for tilkobling av samtaler og forbedrer den generelle ytelsen til Webex appen.

```
<config>
<protokoller>
  < nippe>
    <utvidet autorisasjon aktivert = "%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	usann	sant, usant	Når SIP-godkjenningsforbedringen er satt til "true", er den aktivert.

MERKNAD 1: Noen SBC-er kan kreve ny SIP-autorisasjon på hver økt, så denne funksjonen bør brukes i henhold til distribusjonsspesifikasjonene.

MERKNAD 2: Selv om denne funksjonen er aktivert, hvis Webex appen mottar 401 uautorisert, vil ny autorisasjon bli brukt i neste SIP-forespørsel.

6.1.53 Personlig assistent (tilstedeværelse borte)

Med versjon 44.11 legger Mobile Webex-appen og versjon 45.3, Desktop Webex-appen, til integrering med Cisco BroadWorks Personal Assistant (PA)-tjenesten. Det fungerer i kombinasjon med brukerens Borte-tilstedeværelse og krever synkronisering av PA-statusen med Webex Cloud-tilstedeværelse.

PA-tjenesten gir brukeren et alternativ for å informere innringerne om årsaken til at den oppringte parten ikke er tilgjengelig, eventuelt gi informasjon om når den oppringte parten kommer tilbake og om det er en ledsager til å håndtere samtalen.

Hvis PA er aktivert, vil alternativet Borte være tilgjengelig for brukeren. Den kan brukes til å konfigurere PA på Cisco BroadWorks-siden. Når funksjonen er aktivert, vil brukerne se brukerens Borte-tilstedeværelse i kombinasjon med PA-statusen og varigheten som er konfigurert.

Brukeren kan konfigurere bare den manuelle PA-konfigurasjonen. Hvis det er tidsplaner som påvirker PA-tjenesten, vil tilgjengeligheten bli oppdatert gjennom Personal Assistant Status Sync. Webex-appen eksponerer imidlertid ikke tidsplankonfigurasjonen og tidsplanene som påvirker PA.

```
<config>
<tjenester>
  <personlig assistent aktivert="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%PERSONAL_ASSISTANT_ENABLED_WXT%	usann	sant, usant	Kontrollerer om funksjonen Borte er tilgjengelig for brukeren.

MERKNAD 1: Denne funksjonen krever at statussynkroniseringen for personlig assistent er aktivert fra partnerhuben.

MERKNAD 2: Standard personlig assistent-anropsruting trer ikke i kraft mens selektive tjenester DND, Viderekobling alltid eller Viderekobling av anrop er aktive.

Cisco konfidensielt

MERK 3: Tilstedeværelsestilstandene Manuell Ikke forstyrr og Opptatt har høyere prioritet sammenlignet med Borte. Når brukerhåndboken aktiverer en av disse tilstedeværelsesstatusene, vil ikke aktivering av personlig assistent føre til at tilstedeværelsesstatusen din endres til Borte.

Cisco konfidensielt

6.2 Funksjoner bare for skrivebord

6.2.1 Tvungen utlogging

Med denne funksjonen kan Cisco BroadWorks spore klientforekomster på Internett med samme enhetstype og bare tillate at én av dem er tilkoblet om gangen. Når Cisco BroadWorks varsler klienten om å logge av, avsluttes SIP-tilkoblingen, og klienten indikerer at anrop ikke er tilkoblet.

Denne funksjonen er nødvendig i noen 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, der de innkommende anropene bare vil bli mottatt av en av klientene, avhengig av hvilken SIP-registrering som er aktiv.

Tvungen avlogging er basert på SIP, klienten sender en SIP Abonner på *hendelsespakken call-info* med en spesiell *appid-verdi* i Fra-overskriften , uavhengig av parameterverdien for *bsoft-call-info* . Når Cisco BroadWorks oppdager flere klientforekomster på nettet med samme *appid*, sendes en spesiell SIP NOTIFY til den eldre klientforekomsten, slik at den logger seg av. Desktop-klienter vil for eksempel ha en identisk *appid-verdi* , selv om det ikke er noen begrensninger på bruken av denne identifikatoren på klientsiden. Appid-verdien konfigureres av tjenesteleverandøren.

Vær oppmerksom på at for å bruke tvungen avlogging, må SIP *Call-Info-abonnementet* være aktivert.

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

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

```
<config>
<tjenester>
<tvungen utlogging aktivert="%ENABLE_FORCED_LOGOUT_WXT%" control-protocol="SIP"
appid="%FORCED_LOGOUT_APPID_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_FORCED_ LOGOUT_WXT%	usann	sant, usant	Aktiverer tvungen avlogging.
%FORCED_LOGOUT_ APPID_WXT%	tom	streng	Appid brukes på serversiden for korrelasjon. Dette kan være en hvilken som helst streng. Eksempel: "123abc"

6.2.2 Samtalehenting

Henting av anrop er en flerbrukertjeneste som gjør det mulig for utvalgte brukere å svare på alle ringelinjer i anropshentingsgruppen. En anropshentingsgruppe defineres av administratoren og er et delsett av brukerne i gruppen som kan svare på hverandres anrop.

Følgende hentesaker støttes:

- Henting av blinde anrop

Cisco konfidensielt

- Rettet henting av anrop (som gjør det mulig for en bruker å svare på et anrop rettet til en annen telefon i sin gruppe ved å ringe den respektive funksjonstilgangskoden etterfulgt av internnummeret til den ringende telefonen).

```
<config>
<tjenester><samtaler>
<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%	usann	sant, usant	Sett til "true" for å aktivere Blind Call Pickup.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	usann	sant, usant	Sett til "true" for å aktivere Directed Call Pickup.

6.2.3 Støtte for Boss-Admin (Executive-Assistant)

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

- Velg ønsket rolle når du ringer.
- Svar på et innkommende anrop på vegne av en leder, og send deretter anropet til lederen. I tillegg til dette er alle vanlige samtalehåndteringsalternativer tilgjengelige.
- Se at et innkommende anrop faktisk er for lederen.

Executive og Executive-Assistant er to sammenhengende Cisco BroadWorks-tjenester som sammen leverer følgende funksjonalitet:

- En bruker med Executive-tjenesten kan definere et utvalg av assistenter som administrerer samtalene sine. Assistentene må velges blant brukerne i samme gruppe eller bedrift som har tilordnet tjenesten Executive-Assistant.
- En bruker med tjenesten Lederassistent kan svare på og starte anrop på vegne av sine ledere.
- Både lederen og deres assistenter kan spesifisere hvilke anrop som skal viderekobles til assistentene, hvordan assistenter skal varsles om innkommende anrop, og hvilke av anropene som viderekobles til assistentene, skal presenteres for lederen for screening.

```
<config>
<tjenester>
<Executive-Assistant enabled="%ENABLE_EXECUTIVE_ASSISTANT_WXT%"/>
```

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

Cisco konfidensielt

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

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

Klienten har funksjonalitet til å eskalere en pågående SIP-samtale til et møte via Webex Calling. Ved å bruke denne funksjonaliteten i stedet for en vanlig ad hoc-konferanse, vil brukeren kunne bruke video og skjermdeling under møtet.

```
<config>
<tjenester><samtaler>
       <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%	usann	sant, usant	Sett til "true" for å aktivere menyalternativet Eskaler til Webex Møte.

6.2.5 Bordtelefonkontrollanrop - Automatisk svar

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

Den valgte MPP-telefonen vil bære lyd / video for den utgående DPC-samtalen.

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>
<tjenester><samtaler>
<deskphone-control auto-answer = "%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	sann	sant, usant	Når satt til "true", aktiverer skrivebordet telefonen kontroll autosvar.

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

Cisco konfidensielt

6.2.6 Automatisk svar med tonevarsling

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_AUTO_ANSWER_WXT%	usann	sant, usant	Når satt til "true", aktiveres automatisk innkommende anropssvar hvis dette blir bedt om fra backend.

6.2.7 Bordtelefonkontroll - Mid Call Controls - Konferanse

Denne funksjonen aktiverer konferanse- og sammenslåingsalternativer for eksterne samtaler (XSI) som avsluttes på et annet sted.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	usann	sant, usant	Når "true" er satt til "true", aktiveres konferanse- og sammenslåingsalternativer for eksterne samtaler (XSI), avsluttet på et annet sted.

6.2.8 Varsler om henting av anrop

Varsler om henting av anrop gir brukeren muligheten til å vite når det er et innkommende anrop til en bruker han er konfigurert til å overvåke. Varsler om henting av anrop kan mottas for overvåkningslister som konfigureres via tjenesten Samtalehenting og Opptattlampefelt.

Varsler om henting av anrop er nyttige når de overvåkede brukerne ikke er fysisk nær hverandre og ikke kan høre ringingen på kollegaens telefon.

6.2.8.1 Opptattlampefelt

Skrivebordsprogrammet Webex viser et varsel hvis et medlem i overvåkningslisten for opptattlampefelt (BLF) har et innkommende anrop i varslingstilstand. Varselet har informasjon om oppringeren og brukeren som mottok det innkommende anropet, med muligheter for å svare på anropet, dempe eller ignorere varselet. Når brukeren svarer på det innkommende anropet, starter rettet samtalehenting.

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

- Overvåk de innkommende anropene med mulighet for å hente anropet eller ignorere varselet.
- Se hele listen over de BLF brukerne.
- Overvåk tilstedeværelsen av brukerne - rik tilstedeværelse er bare tilgjengelig for brukere med Webex Cloud-rettighet. Grunnleggende tilstedeværelse (telefoni) er bare tilgjengelig for brukere som bare bruker BroadWorks.
- Start en samtale med en BLF bruker.
- Start en chat med en BLF bruker – bare tilgjengelig for brukere med Webex Cloud-rettighet.

Cisco konfidensielt

- Legg til en BLF bruker som en kontakt.

```
<config>
  <tjenester>
    <samtaler>
      <opptatt-lampe-feltet aktivert = "%ENABLE_BUSY_LAMP_FIELD_WXT%">
        <display-caller enabled="%ENABLE_BLF_DISPLAY_CALLER_WXT%"/>
        <varslingsforsinkelse = "%BLF_NOTIFICATION_DELAY_TIME_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_BUSY_LAMP_FIELD_WXT%	usann	sant, usant	Aktiverer overvåking av opptattlampefelt og ringevarsling for andre brukere med mulighet til å svare på anropene.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	sann	sant, usant	Aktiverer visning av anroperens visningsnavn/nummer i ringevarselet.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Kontrollerer hvor mange sekunder ringevarselet skal utsettes før det vises for brukeren.

MERK: Denne funksjonen avhenger av tjenesten for rettet samtalehenting.

6.2.8.2 Hentegruppe for anrop (bare Webex Calling)

Fra og med versjon 44.2 legger programmet Webex til støtte for GCP-varsler (Group Call Pickup) for Webex Calling distribusjonen. Den gjør det mulig for brukere å bli varslet om innkommende anrop for alle brukerne som overvåkes gjennom samtalehentingsgruppen.

I tilfelle et innkommende anrop for en bruker som er en del av en samtalehentingsgruppe, gis det en sjanse til at anroperen svarer på anropet. Det er en GCP-varslingsforsinkelse som kan konfigureres via Control Hub. Hvis anroperen ikke behandler anropet innen den konfigurerte tiden, sendes et GCP-varsel til gruppen.

Hvis det forekommer flere anrop i samme anropshentingsgruppe, behandles de sekvensielt basert på tidspunktet de mottas. Varselet om det eldste anropet leveres først til gruppen, og når det er behandlet, leveres neste varsel i køen til gruppen.

Varsler kan være bare lyd, bare visuelt eller lyd og visuelt, avhengig av konfigurasjonen i administrasjonsportalen for kontrollhuben. Hvis det vises et visuelt GCP-varsel, kan brukeren svare på anropet ved hjelp av funksjonen for samtalehenting. Hvis varsel med bare lyd er konfigurert, vil ikke brukeren se et visuelt varsel for det innkommende anropet, vil høre en bestemt ringetone, og han kan hente anropet fra menyen for samtalehenting som er tilgjengelig i Webex appen, eller ved å ringe FAC-koden (*98) og internnummeret manuelt.

Brukeren kan dempe GCP-varselet gjennom programinnstillingene. Denne innstillingen gjelder for alle varsler om henting av anrop (BLF og GCP), og som standard er varslinger dempet.

Funksjonen fungerer for hovedlinjene og for delte eller virtuelle linjer som er tilordnet brukeren.

Cisco konfidensielt

```
<config>
<tjenester><samtaler>
    <group-call-pickup-notifications enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
        <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
        <maks-tidsavbruddsverdi="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
    </gruppeanrop-henting-varsler>
...
<protokoller><sip>
    <linjer>
        <linje>
            <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1 %</group-call-pickup>
            ...
        </linje>
        <linje>
            <gruppe-samtale-henting>%BWGROUP-CALL-PICKUP-BOOL-2 %</group-call-
pickup>
            ...
        </linje>
        ...
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_GCP_NOTIFICATIONS_WXT%	usann	sant, usant	Aktiverer varsler om henting av gruppeanrop
%ENABLE_GCP_DISPLAY_CALLER_WXT%	sann	sant, usant	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%	usann	sant, usant	Angir om tilsvarende linje har Anropshentegruppe konfigurert

MERK 1: Dette er en Webex Calling eneste funksjon.

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

6.2.9 Hendelsespakke for fjernkontroll

For Klikk og ring-klienter som tynnklienten BroadWorks Receptionist og Go-integratoren, der Webex-appen er anropsenheten, respekterer Webex-appen nå hendelsespakken for fjernkontrollen når den mottar et anrop eller håndterer vent/gjenoppta.

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

Cisco konfidensielt

6.2.10 Valg av CLID for agentanrop

Når agenter foretar anrop til kundene sine, vil de at kundene skal se riktig anropslinje-ID (CLID) i stedet for deres personlige/bedrifts-CLID. Hvis for eksempel agent Mary Smith er koblet til køen for kundestøtte, vil Mary at kundene skal se CLID-en hennes som teknisk støtte når hun ringer kunder, ikke Mary Smith.

Administratorer i Control Hub eller CommPilot kan angi ett eller flere DNIS-numre som skal brukes for utgående CLID, for en anropskø. Agenter har deretter muligheten til å velge ett av DNIS-numrene som skal brukes som CLID når de foretar utgående anrop. Webex appen gjør det mulig for agenter å velge hvilken DNIS som skal brukes som CLID.

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%	usann	Sant, usant	Aktiverer utgående anrop (CLID-valg) på vegne av telefonsenterkøen.

6.2.11 Overlevelsesgateway (kun Webex Calling)

Fra og med versjon 43.2 legger programmet Webex til støtte for Survivability-anropsmodus. Hvis funksjonen er aktivert og det ikke er noen Webex skytilkobling, kan Webex-programmet kjøre i overlevelsesmodus. I denne modusen er begrenset ringefunksjonalitet tilgjengelig for brukeren.

Lokal Survivability Gateway distribueres av kunden.

```
<config>
<protokoller>
< nippe>
<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%	usann	sant, usant	Aktiverer støtte for overlevelsesmodus.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Angir fallback-tid (gateway for overlevelsesevne til SSE)

MERK: Denne funksjonen gir trygghet ved overføring fra lokale til skyanropsløsninger.

Cisco konfidensielt

6.2.12 Hendelsespakke for ekstern demping (kun Webex Calling)

Fra og med versjon 43.9 legger Webex-appen til støtte for ekstern demping av anropskontroll av lydmediestrømmen. Dette gjør det mulig å dempe/oppheve demping av en pågående samtale utløses fra et annet sted, for eksempel tynnklienten BroadWorks Receptionist, der den Webex appen er anropsenheten.

Funksjonen avhenger av den nye informasjonspakken SIP *x-cisco-mute-status* . *Hvis Recv-Info:x-cisco-mute-status-overskriften* mottas under oppretting av SIP INVITE-økten, sender Webex-appen tilbake SIP INFO med *statusen Info-Package:x-cisco-mute-status hver gang det er en oppdatering (lokal eller ekstern) av lydsamtalen. dempet = sann* (eller *dempet = usann*), der den dempede parameteren representerer den oppdaterte tilstanden til lydmediestrømmen.

Demping eller oppheving av demping kan utløses lokalt eller fra et eksternt sted. Ekstern oppdatering utløser at SIP NOTIFY med *hendelse: demper* (eller *opphever demping*) sendes til Webex appen fra programserveren. Den Webex appen respekterer den eksterne forespørselen, og etter oppdateringen av lydmediestrømtilstanden, sender den tilbake en SIP NOTIFY med *Info-Package:x-cisco-mute-status; dempet = sant* (eller *dempet = usant*).

```
<config>
<tjenester>
   <samtaler>
       <fjerndempingskontroll aktivert="%ENABLE_REMOTE_MUTE_CONTROL_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	usann	Sant, usant	Når den eksterne dempeanropskontrollen er satt til "true", aktiveres den eksterne dempeanropskontrollen for brukeren.

6.2.13 Flytt samtale

Webex appen tilbyr samtaleovervåking og samtalekontroll av VoIP samtaler som avsluttes på et annet sted. Dette er for øyeblikket bare tilgjengelig for brukerens primære linje.

Fra og med versjon 43.12 forbedres Webex-appen slik at anrop som er avsluttet på et annet sted, også vises for de delte og virtuelle linjene. Slike samtaler er synlige i området for pågående samtaler for informasjonsformål og uten mulighet til å kontrollere dem. Bare hvis en slik samtale er satt på vent, vil brukeren kunne flytte den til den lokale enheten ved å velge den og gjenoppta den fra anropsskjermen. Denne mekanismen er nyttig hvis anropet ble behandlet av samme bruker på et annet sted eller av en annen bruker på samme linje.

Vær oppmerksom på at det ikke er mulig for Webex appen å flytte en samtale på vent til en sammenkoblet enhet. Hvis brukeren er paret med en enhet, må han først koble fra, og deretter kan han gjenoppta samtalen som er satt på vent lokalt.

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

Cisco konfidensielt

Overvåking av anropene for brukerens primære linje avhenger av XSI-hendelsene (Advanced Call event package), og flytting av et anrop til den lokale enheten er ikke tilgjengelig for disse samtalene. For denne typen anrop kan brukeren bruke funksjonen Trekk anrop (*6.1.22 Trekk anrop*). Samtalehenting fungerer bare for de siste aktive anropene til brukeren, mens mekanismen for delte og virtuelle linjer fungerer for alle anropene til brukeren som er satt på vent.

- Eksempel 1:
  a. Alice har Bobs linje tilordnet for skrivebords- og bordtelefonprofilene.
  b. Alice har en samtale med Charlie via bordtelefonen – Alice kan se den pågående samtalen i skrivebordsappen.
  c. Alice setter samtalen på vent fra bordtelefonen – samtalen kan gjenopptas av Alice fra skrivebordsappen.
- Eksempel 2:
  a. Alice har Bobs linje tilordnet for skrivebords- og bordtelefonprofilene.
  b. Bob har en samtale med Charlie – Alice kan se den pågående samtalen i skrivebordsappen.
  c. Bob setter samtalen med Charlie på vent – Alice kan gjenoppta samtalen med Charlie fra skrivebordsappen.
- Eksempel 3:
  a. Alice har Bobs linje tilordnet 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 skrivebordsappen.
  d. Bob setter samtalen med Charlie på vent – Alice kan ikke gjenoppta samtalen med Charlie fra skrivebordsappen.
  e. Alice kobler skrivebordsappen fra bordtelefonen – Alice kan gjenoppta samtalen med Charlie fra skrivebordsappen.

```
<config>
<tjenester><samtaler>
    <flytt anrop>
         <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALL_MOVE_HERE_WXT%	usann	Sant, usant	Aktiverer flytting av anrop på lokal enhet. Brukes for vent/gjenoppta på tvers av steder/brukere i brukstilfellet med flere linjer.

Cisco konfidensielt

6.3 Funksjoner kun for mobil

6.3.1 Nødanrop

Webex for Cisco BroadWorks støtter opprinnelig nødanrop.

Når funksjonen er aktivert, ved å starte en utgående VoIP samtale, analyserer programmet det oppringte nummeret og sammenligner det med listen over konfigurerte nødnumre. Hvis nummeret identifiseres som et nødnummer, utfører programmet den konfigurerte oppringingsvirkemåten. Den kan konfigureres ved hjelp av koden for *oppringingssekvens* .

Støttede moduser er:

- cs-only – Klienten plasserer nødanrop bare via mobilnettverket hvis nettverket er tilgjengelig.
- cs-first - Når du starter et nødanrop, sjekker klienten nettverkstypen som den gjeldende enheten er koblet til. Hvis mobilnettverket er tilgjengelig, ringer klienten via mobilnettverket. Hvis mobilnettverket ikke er tilgjengelig, men et mobildata-/WiFi-nettverk er tilgjengelig, plasserer klienten samtalen over mobildata-/WiFi-nettverket som en VoIP-samtale. Hvis nødanropet foretas via mobilnettverket, foreslår klienten også at brukeren prøver nødanropet på nytt som VoIP.
- voip-only - Klienten plasserer nødanrop bare som VoIP hvis mobildata / WiFi-nettverk er tilgjengelig.
- cs-voip - Klienten analyserer om enheten kan starte den som innfødt kretssvitsjet (CS) anrop (uten å ta hensyn til om CS-nettverket er tilgjengelig eller ikke). Hvis enheten kan starte en opprinnelig samtale, ringes nødnummeret som et nødanrop til en CS. Ellers ringes anropet som VoIP.

> **MERK:** Hvis VOIP-anrop er deaktivert, er den eneste meningsfulle verdien for nødoppringingssekvens (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) bare cs.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_EMERGENCY_DIALING_WXT%	usann	sant, usant	Sett til "true" for å aktivere registrering av nødanrop. Standard verdi er tom.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	Bare cs	cs-bare, cs-first, voip-only, cs-voip	Kontrollerer oppringingssekvensmodus for nødanrop.
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	CSV liste	CSV liste over nødnumre. Eksempel: 911 112

Cisco konfidensielt

6.3.2 Push-varsler for samtaler

Når et innkommende anrop mottas, mottar mobilklienten først et push-varsel (PN). Det finnes en config-parameter som kan brukes til å kontrollere når SIP REGISTER-økten skal etableres:

1. Når push-varslingen mottas, ELLER
2. Når anropet godtas av brukeren.

Den andre tilnærmingen anbefales. Sammenlignet med første tilfelle, legger det imidlertid til en viss forsinkelse før samtalen er etablert.

I henhold til iOS 13-kravene skal VoIP PN-er bare brukes til innkommende anrop. Resten av samtalerelaterte hendelser bør bruke vanlige PN-er.

For å oppfylle dette kravet introduseres nye PN-registrerings API, og det krever tilsvarende oppdatering som skal brukes på applikasjonsserveren. Hvis serverdelen ikke er konfigurert til å støtte iOS 13 PN-er, kan konfigurasjonsparameteren brukes til å håndheve bruk av eldre push-varsler, der alle anropsrelaterte hendelser leveres gjennom VoIP PN-er.

Det er et push-varsel som sendes av applikasjonsserveren (AS) når et ringende anrop godtas av anropsmottakeren på et annet sted, lukkes av oppringeren eller for eksempel omdirigeres til talepost. Med iOS 13 er denne typen push-varsling nå 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 PN-er for samtaleoppdatering legges det til et konfigurerbart tidsavbrudd for ringing for å kontrollere maksimal ringetid. Hvis maksimal ringetid er nådd, stoppes ringetonen for anroperen, og anropet behandles som tapt. På anropersiden kan anropet forbli i ringetilstand til policyen for ikke-svar som er konfigurert på programserveren (AS), er utført.

For å holde programvirkemåten konsistent, gjelder den konfigurerbare ringetidtakeren for både Android og iOS.

Et separat konfigurasjonsalternativ er lagt til for å angi virkemåten for anropsavvisning når et innkommende anrop mottas som et push-varsel. Klienten kan konfigureres til å ignorere anropet eller svare serveren via Xsi med avslag satt til "true" eller "false", og i så fall vil de tildelte Cisco BroadWorks-anropsbehandlingstjenestene bli brukt. Hvis "decline_false" er konfigurert, fortsetter anropet å ringe til avsenderen avbryter eller tidtakeren for nei-svar utløper, og de tilknyttede anropsbehandlingstjenestene starter. Hvis "decline_true" er konfigurert, vil årsaken til avslag spesifisere anropsbehandlingen. Hvis avslagsårsaken er satt til "opptatt", tvinger serveren umiddelbart den travle behandlingstjenesten. Hvis "temp_unavailable" er konfigurert, brukes den midlertidige ikke tilgjengelige behandlingstjenesten.

```
<config>
<tjenester>
    <push-notifications-for-calls enabled="true"
    connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
    ring-timeout-sekunder = "%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"/>
    <samtaler>
        <avvis-med-xsi-modus="%REJECT_WITH_XSI_MODE_WXT%"
        declineReason="%REJECT_WITH_XSI_DECLINE_REASON_WXT%"/>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	usann	sant, usant	Kontrollerer når SIP REGSITER-økten etableres – når du mottar en push-varsling for innkommende anrop eller når du godtar den.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Kontrollerer maksimal ringetid for innkommende anrop for anrop mottatt via PN. Hvis ingen CallUpd PN mottas innen den angitte perioden, vil anropet bli behandlet som tapt.
%REJECT_WITH_XSI_MODE_WXT%	decline_usant	ignorere, decline_true, decline_false	Angir virkemåten for anropsavvisning.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	opptatt	opptatt, temp_unavailable	Angir årsaken til avvisning av anrop hvis avvisningsmodus er satt til "decline_true".

6.3.2.1 MWI

Når MWI-funksjonen er aktivert, abonnerer Mobile Webex-klienten på MWI Push Notification for å motta oppdateringer med brukerens talepost og varsle ham.

For å redusere antall varsler og unngå unødvendige distraksjoner undertrykkes MWI push-varsler i noen tilfeller. For eksempel når brukeren lytter til talepostmeldingene eller merker dem som lest fra mobil Webex-klienten (ulest antall synker). Det er ikke noe konfigurerbart alternativ for å kontrollere dette.

Hvis du vil ha mer informasjon om MWI, kan du se delen *6.1.27 Talepost, Visuell talepost, Indikator for Melding* venter.

6.3.2.2 Ringsprut

BroadWorks-tjenester (som DND) kan sende ringepåminnelser når innkommende blir omdirigert. Webex Mobile-klienten kan konfigureres til å aktivere Ring Splash Push Notifications og presentere dem for brukeren når de utløses av BroadWorks.

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

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_RING_SPLASH_WXT%	usann	sant, usant	Aktiverer ringesprut i BroadWorks-konfigurasjonen.

6.3.2.3 Leveringsmåte (bare Webex Calling)

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

- nps - strømmekanisme, ved hjelp av NPS

Cisco konfidensielt

- sky – forbedret mekanisme ved hjelp av Cisco Webex skymikrotjeneste
- ekstern - en mekanisme som bruker tredjepartssystem. Det krever integrering av tredjepartssystemet med Cisco WebHooks-motoren

```
<config>
<tjenester><samtaler>
<push-notifications-for-calls enabled="true"
      connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
      ring-timeout-sekunder = "%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"
      leveringsmodus="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	NPS	NPS, sky, ekstern	Angir leveringsmåte for push-varslene for anrop.

6.3.3 Enkel varsling

Mobile Single Alert-funksjonen er beregnet for distribusjon av fast mobil konvergens (FMC) / MNO (Mobile Network Operator) som bruker BroadWorks Mobility-tjenesten. Uten den, når den er logget på Webex-klienten og mottar et innkommende anrop, vil brukeren motta samtidig to anrop - en innfødt og en Push Notification (VoIP) samtale. Når funksjonen er aktivert, vil programmet deaktivere mobilitetsvarsling på brukerens BroadWorks Mobility-plassering når du logger på, og aktivere varslingen ved avlogging. En viktig forutsetning for å bruke denne funksjonen er at brukeren har BroadWorks Mobility-tjenesten tilordnet og nøyaktig én plassering konfigurert.

```
<config>
<tjenester><samtaler>
<enkeltvarsling aktivert="%ENABLE_SINGLE_ALERTING_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_SINGLE_ALERTING_WXT%	usann	Sant, usant	Sett til "true" for å aktivere Single Alerting.

6.3.4 Klikk for å ringe (ring tilbake)

Klikk og ring sørger for at sluttbrukeren kan ringe på sin personlige kretssvitsjede mobiltelefon og levere sin forretnings-DN som anropslinje-ID.

Mobile Webex-klienten støtter Klikk for å ringe (tilbakeringing) anrop ved hjelp av tjenesten BroadWorks Anywhere. BroadWorks Anywhere-plasseringene i det Webex programmet kalles Single Number Reach (SNR) plasseringer.

Cisco konfidensielt

Når funksjonen er aktivert, kan brukerne velge den SNR plasseringen fra enhetens paringsmeny. Når de kobles sammen med SNR plassering, startes alle utgående anrop ved hjelp av Klikk for å ringe (ring tilbake)-anrop. For å hindre dobbeltvarsling deaktiveres push-varsler for innkommende anrop.

Når en bruker starter et Klikk for å ringe-anrop, vil de se skjermbildet for utgående anrop med informasjon om hvordan de kan forvente innkommende anrop på den valgte SNR plasseringen. Dette skjermbildet lukkes automatisk basert på konfigurerbar tidtaker.

Når du kobler fra et SNR sted, registrerer programmet seg på nytt for push-varsler for innkommende anrop.

```
<config>
<tjenester>
  <ringe>
    <tilbakeringing aktivert = "%ENABLE_DIALING_CALL_BACK_WXT%" timer =
"%DIALING_CALL_BACK_TIMER_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DIALING_ CALL_BACK_WXT%	usann	Sant, usant	Sett til "true" for å aktivere Klikk for å ringe (Ring tilbake).
%DIALING_CALL_ BACK_TIMER_WXT%	10	[3-20]	Kontrollerer antall sekunder før tilbakeringingsskjermen lukkes automatisk.

6.3.5 MNO-støtte

6.3.5.1 Ring med opprinnelig oppringing

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

Brukerens mulighet til å starte anrop via den opprinnelige oppringeren styres av den opprinnelige **konfigurasjonskoden** . Hvis aktivert, vil applikasjonen starte den opprinnelige oppringeren og foreta anropet. I tillegg kontrolleres tilgjengeligheten til VoIP anrop av **voip-koden** – basert på distribusjonskravene VoIP anrop kan aktiveres eller deaktiveres.

Hvis VoIP og Opprinnelig anrop er aktivert, kan brukeren velge hvilket alternativ som skal brukes.

Koden <oppringingsmodus> styrer om brukerne kan velge hvordan innkommende og utgående anrop skal startes/mottas. Krever at både det opprinnelige anropet og det VoIP anropet er aktivert.

Fra og med versjon 43.12 utvides opprinnelig oppringingskonfigurasjon, slik at et egendefinert prefiks kan forhåndsbrukes til det utgående anropsnummeret. Dette gjelder mobilanrop som startes fra Webex appen, bare hvis nummeret som ringes, 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 Cisco BroadWorks-applikasjonsserveren, kan håndtere FAC-kodene av Telecom-serverdelen. Ny <fac-prefiks> tag er lagt til under delen <dialing><native> og telekom kan bruke den til å løse dette problemet.

Cisco konfidensielt

```
<config>
<tjenester>
  <ringe>
    <voip enabled="%ENABLE_DIALING_VOIP_WXT%"/>
    <native enabled="%ENABLE_DIALING_NATIVE_WXT%" enable-bwks-mobility-
dependency="%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%">
      <fac-prefiksverdi="%DIALING_NATIVE_FAC_PREFIX_WXT%"/>
    </innfødt>
    <oppringingsmodus aktivert = "%ENABLE_DIALING_MODE_WXT%" default = "%DIALING_MODE_DEFAULT_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_DIALING_VOIP_WXT%	sann	sant, usant	Sett til "true" for å aktivere VoIP anropsalternativ.
%ENABLE_DIALING_NATIVE_WXT%	usann	sant, usant	Sett til "true" for å aktivere alternativet Native call.
%ENABLE_DIALING_MODE_WXT%	usann	Sant, usant	Aktiverer valg av ringemodus for brukeren via samtaleinnstillingene i Innstillinger.
%DIALING_MODE_DEFAULT_WXT%	VoIP	VoIP, opprinnelig	Angir valgt standard ringemodus.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	usann	sant, usant	Kontrollerer om tilgjengeligheten til det opprinnelige anropet skal avhenge av at BroadWorks Mobility-tjenestetilordningen og mobilitetsplasseringen konfigureres for brukeren.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*tom*	streng	Angir et prefiks som skal legges foran hvis et utgående anrop til et nummer som starter med en FAC-kode, startes som et mobilanrop. Som standard defineres ikke FAC prefiks, og koden er tom.

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

MERKNAD 2: Hvis bare det **opprinnelige** anropet er aktivert, anbefales det i MNO-distribusjoner å deaktivere enkeltvarsling for å forhindre at klienten deaktiverer BWM-varslingen.

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

6.3.5.2 Kontroller midt i samtalen

Med denne funksjonen kan den mobile Webex-klienten styre via XSIs opprinnelige samtaler på mobilenheten som er forankret på Cisco BroadWorks. XSI-samtalekontrollene er bare tilgjengelige hvis:

- BroadWorks Mobility (BWM)-tjenesten er tilordnet brukeren,
- Det er bare én BMW Mobile Identity konfigurert,
- Innfødt ringemodus velges av brukeren (for mer informasjon i avsnittet *6.3.5.1 Ring med opprinnelig oppringing),*

Cisco konfidensielt

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

Versjon 43.10 legger til bedre håndtering av den rådgivende overføringen, skaper tilknytning mellom de to mobilanropene som presenteres i Webex appen, og gir brukeren et alternativ for å fullføre overføringen. Også, hvis brukeren har to uavhengige mobilsamtaler på samme enhet, er overføringsmenyen forbedret for å tillate overføring 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%	usann	sant, usant	Aktiverer XSI-anropskontroll for MNO-miljø.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Kontrollerer XSI MNO-distribusjonstypen som brukes av programmet. Mulige verdier er: ▪ MNO_Access – viser alle eksterne anrop (XSI) med enhetstypene definert i noden nedenfor. ▪ MNO_Network – viser alle eksterne samtaler (XSI).
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	streng	Enhetstypenavnene som skal brukes i den MNO_Access distribusjonstypen.
%ENABLE_XSI_HOLD_CALLS_WXT%	sann	Sant, usant	Kontrollerer om handlingen Samtale på vent skal være tilgjengelig for brukeren for XSI-mobilsamtaler.

6.3.5.3 CLID (Outgoing Calling Line Identity) – dobbel identitet

Med mobilversjon 42.12 lar Webex-appen brukere velge anropslinjeidentitet (CLID) som presenteres for den eksterne parten når de starter en utgående samtale.

Hvis brukeren er konfigurert med Cisco BroadWorks Mobility, typisk konfigurasjon for distribusjon av mobilnettoperatør (MNO) og opprinnelig anrop er aktivert, kan brukeren velge hvilken identitet som skal presenteres for personene de ringer. Brukeren kan velge sin forretningsmessige eller personlige identitet. Det er også et alternativ å skjule egen identitet og samtalen for å bli presentert som anonym.

For VoIP samtaler har brukeren også muligheten til å kontrollere CLID-en. Det tilgjengelige alternativet i dette tilfellet er bare å kontrollere om han skal skjule sin identitet eller ikke.

Cisco konfidensielt

Personaadministrasjon og CLID-blokkering styres gjennom separate konfigurasjonsalternativer.

```
<config>
<tjenester>
<ringe>
   <calling-line-id-delivery-blocking
enabled="%ENABLE_CLID_DELIVERY_BLOCKING_WXT%"/>
   <mobilitet-persona-management
aktivert="%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%"/>
```

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	usann	Sant, usant	Aktiverer leveringsblokkering for anropslinje-ID. Den gjelder for alle utgående anropstyper for brukeren.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	usann	Sant, usant	Aktiverer personlig administrasjon for opprinnelige anrop når distribusjonstypen er konfigurert som MNO_Access eller MNO_Network. (BroadWorks Mobility brukes til de opprinnelige samtalene, og alle de opprinnelige anropene er forankret på BroadWorks)

6.3.5.4 Varsel om opprinnelige anrop

For brukere som er distribuert med MNO, legger denne funksjonen til et varslingsbanner for integrerte anrop, som kan kontrolleres via Webex appen. Dette varselet er avhengig av push-varslinger, sendt av applikasjonsserveren når anropet er etablert.

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

6.3.5.5 Flytte opprinnelig samtale til konvergert møte

For brukere som er distribuert med MNO, gjør denne funksjonen det mulig å eskalere et opprinnelig 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, kan partene gjøre følgende når de er i et møte:

- Starte Webex i møtechat
- Legg til video (merk at lyden fortsetter i den opprinnelige samtalen)
- Del skjerm / innhold
- Utløser opptak av møter

Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	usann	sant, usant	Aktiverer Power Up (Inviter og møt, Video Meet-handlinger).

6.3.5.6 MNO-mobilitet – widget under samtale

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

- Vent/Gjenoppta
- Blind / konsultativ overføring - plasserer brukeren i overføringsdialogen i Webex appen.
- Complete Transfer – gir mulighet til å fullføre rådgivende overføring (versjon 43.10)
- Videomøte – flytter partene inn i et Webex møte.
- Avslutte samtale

```
<config>
<tjenester><samtaler>
       <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%	sann	Sant, usant	Kontrollerer tilgjengeligheten til Vent-handlingen i kontrollprogrammet Anrop.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	sann	Sant, usant	Kontrollerer tilgjengeligheten til handlingene Overfør og Fullfør overføring i kontrollprogrammet Anrop.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	sann	Sant, usant	Kontrollerer tilgjengeligheten til Videomøte-handlingen i kontrollprogrammet Samtale.

Cisco konfidensielt

6.3.6 Innkommende anroper-ID

Versjon 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 vises for brukeren i skjermbildet for innkommende anrop og varsel om innkommende anrop, og varslene om tapte anrop.

6.3.6.1 Skjermbilde for innkommende anrop

Det er plattformforskjeller mellom Android og iOS når det gjelder visning av data på skjermbildet for innkommende anrop. Opprinnelig opplevelse som viser informasjon for innkommende anrop, er som følger:

Android - det er to separate felt i skjermbildet for innkommende anrop for å vise både navn og nummer

iOS - det er bare ett felt som viser enten navnet eller nummeret - hvis begge er tilgjengelige, prioriteres navnet

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

6.3.6.2 Varsel om innkommende anrop

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

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

6.3.6.3 Varsel om tapt anrop

Det er lagt til en ekstra konfigurasjonsparameter for varslene om tapte anrop. Den kan brukes til å kontrollere informasjonen om den eksterne parten, på samme måte som varslene om innkommende anrop, slik at nummeret kan legges til visningsnavnet til den eksterne brukeren og presenteres i varselet om tapt anrop. Dette er virkemåten til Webex appen gjelder både Android og iOS.

```
<config>
<tjenester><samtaler>
   <anroper-ID>
      <innkommende anrop>
         <tilføyingsnummer
aktivert="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
      </innkommende anrop>
      <tapte anrop>
         <vedleggsnummer aktivert="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
      </tapte anrop>
```


Cisco konfidensielt

Merkelapp	Standard hvis utelatt	Støttede verdier	Beskrivelse
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	usann	sant, usant	Kontrollerer om nummeret skal legges til navnet på skjermen for innkommende anrop (bare iOS) og varsler.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	usann	sant, usant	Kontrollerer om nummeret skal legges til navnet i varselet om tapt anrop.

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

Cisco konfidensielt

7 Funksjoner for tidlig prøveversjon (BETA)

Det er ingen funksjoner i BETA med nyeste utgivelse.

Cisco konfidensielt

8 Egendefinerte koder Tilordning mellom Webex for Cisco BroadWorks og UC-One

Tabellen nedenfor viser Webex for egendefinerte Cisco BroadWorks-koder, som samsvarer med de eldre egendefinerte kodene for UC-One.

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	Ikke tilgjengelig	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	Ikke tilgjengelig	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	Ikke tilgjengelig	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	Ikke tilgjengelig
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	Ikke tilgjengelig
%ENABLE_CALL_STATISTICS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	Ikke tilgjengelig	%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%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	Ikke tilgjengelig
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	Ikke tilgjengelig
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	Ikke tilgjengelig
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_BROADWORKS_ANYWHERE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig

Cisco konfidensielt

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_EMERGENCY_DIALING_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%EMERGENCY_DIALING_NUMBERS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	Ikke tilgjengelig	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	Ikke tilgjengelig
%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%	Ikke tilgjengelig
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	Ikke tilgjengelig

Cisco konfidensielt

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%USE_TLS_FROM_DNS_WXT%	%USE_TLS_FROM_DNS%	Ikke tilgjengelig
%DOMAIN_OVERRIDE_WXT%	%DOMAIN_OVERRIDE%	%DOMAIN_OVERRIDE%
%SOURCE_PORT_WXT%	%SOURCE_PORT%	%SOURCE_PORT%
%USE_ALTERNATIVE_IDENTITIES_WXT%	%USE_ALTERNATIVE_IDENTITIES%	Ikke tilgjengelig
%TCP_SIZE_THRESHOLD_WXT%	%TCP_SIZE_THRESHOLD%	Ikke tilgjengelig
%SIP_REFRESH_ON_TTL_WXT%	%SIP_REFRESH_ON_TTL%	Ikke tilgjengelig
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	%ENABLE_SIP_UPDATE_SUPPORT_MOBILE%
%ENABLE_PEM_SUPPORT_WXT%	%ENABLE_PEM_SUPPORT_DESKTOP%	Ikke tilgjengelig
%ENABLE_SIP_SESSION_ID_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%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%	Ikke tilgjengelig
%CHANNEL_HEARTBEAT_WXT%	%CHANNEL_HEARTBEAT%	%CHANNEL_HEARTBEAT_MOBILE%
%XSI_ROOT_WXT%	%XSI_ROOT%	%XSI_ROOT%
%XSI_ACTIONS_PATH_WXT%	Ikke tilgjengelig	%XSI_ACTIONS_PATH_MOBILE%
%XSI_EVENTS_PATH_WXT%	Ikke tilgjengelig	%XSI_EVENTS_PATH_MOBILE%

Cisco konfidensielt

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	Ikke tilgjengelig	%ENABLE_CALLS_AUTO_RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	Ikke tilgjengelig	%EMERGENCY_CALL_DIAL_SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLIND_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%WEB_CALL_SETTINGS_URL_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_URL%
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP%
%ENABLE_CALL_CENTER_WXT%	%ENABLE_CALL_CENTER_DESKTOP%"	Ikke tilgjengelig
%WEB_CALL_SETTINGS_TARGET_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_CFA_VISIBLE%
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_DND_VISIBLE%
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_ACR_VISIBLE%
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_CFB_VISIBLE%
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_CFNR_VISIBLE%
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_CFNA_VISIBLE%
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_SIMRING_VISIBLE%
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_SEQRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_RO_VISIBLE%
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_ACB_VISIBLE%
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_CW_VISIBLE%
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_CLIDB_VISIBLE%
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_PA_VISIBLE%

Cisco konfidensielt

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_BWA_VISIBLE%
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE%
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_BWM_VISIBLE%
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	Ikke tilgjengelig	%WEB_CALL_SETTINGS_VM_VISIBLE%
%ENABLE_DIALING_CALL_BACK_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%DIALING_CALL_BACK_TIMER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	Ikke tilgjengelig
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	Ikke tilgjengelig	%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_MOBILE%
%ENABLE_CALL_RECORDING_WXT%	%ENABLE_CALL_RECORDING_DESKTOP%	%CALL_RECORDING_MOBILE%
%ENABLE_SINGLE_ALERTING_WXT%	Ikke tilgjengelig	%ENABLE_SINGLE_ALERTING%
%ENABLE_CALL_PARK_WXT%	%ENABLE_CALL_PARK_SKRIVEBORD%	Ikke tilgjengelig
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_RTP_ICE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%RTP_ICE_MODE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%RTP_ICE_SERVICE_URI_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%RTP_ICE_PORT_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_DIALING_VOIP_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_DIALING_NATIVE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	Ikke tilgjengelig	Ikke tilgjengelig

Cisco konfidensielt

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%USER_PORTAL_SETTINGS_URL_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_AUDIO_MARI_FEC_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_AUDIO_MARI_RTX_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_VIDEO_MARI_FEC_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_VIDEO_MARI_RTX_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CALL_BLOCK_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_WIDGET_HOLD_CALLS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CALL_MOVE_HERE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%DIALING_NATIVE_FAC_PREFIX_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig

Cisco konfidensielt

Webex for Cisco BroadWorks-kode	Eldre skrivebordskode	Eldre mobil-tag
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CLID_OUTGOING_CALLS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	Ikke tilgjengelig
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	Ikke tilgjengelig
%BLF_NOTIFICATION_DELAY_TIME_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_GCP_NOTIFICATIONS_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_GCP_DISPLAY_CALLER_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%UDP_KEEPALIVE_ENABLED_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%TCP_KEEPALIVE_ENABLED_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%TLS_KEEPALIVE_ENABLED_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	Ikke tilgjengelig	Ikke tilgjengelig
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	Ikke tilgjengelig	Ikke tilgjengelig

Cisco konfidensielt

MERK: I/T angir at det ikke var noen tilsvarende egendefinert kode som kontrollerte funksjonen i UC-One. Hvis du har I/T for eldre koder for både stasjonære og mobile datamaskiner, betyr det at Webex for BroadWorks-koden er ny og kontrollerer enten ny funksjonalitet eller en eksisterende funksjon som ikke ble kontrollert via en egendefinert kode i UC-One.

Cisco konfidensielt

9 Vedlegg A: TLS chiffer

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

Cisco konfidensielt

10 Vedlegg B: DM Tag Provisioning Script

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

Vær oppmerksom på at dette skriptet bare er gyldig for nye distribusjoner der egendefinerte DM-koder opprettes. Hvis du vil endre eksisterende egendefinerte DM-koder, må kommandoen i følgende skript endres fra "add" til "set".

Skriptmal med bare noen få egendefinerte koder angitt (i en reell distribusjon må du fylle ut en større liste over egendefinerte koder). Vær oppmerksom på at følgende eksempel er for mobil. For PC bruker du BroadTouch_tags kodesett i stedet for Connect_Tags. For nettbrett bruker du ConnectTablet_Tags-kodesettet i stedet for Connect_Tags.

```
%% ******************************** Connect_Tags - les fil ********************************
%%
%% Instruksjoner:
%% -------------------
%% – Denne lesefilen kan brukes til å opprette, legge til og angi Webex for BroadWorks
%% tilpassede klientmerker
%% – Bruk %% til å kommentere eventuelle trinn som ikke er nødvendige, basert på
distribusjonsspesifikk distribusjon
%% servicekrav:
%% Trinn 1 -- bare for nye distribusjoner, opprett første tagsettetikett
%% Trinn 2 -- legg til en ny egendefinert kode (en oppføring kreves for hver nye kode)
%% Trinn 3 -- angi verdi for en eksisterende egendefinert tag (oppføring kreves for hver gjeldende
tag)
%% Trinn 4 -- vise og visuelt verifisere kodeinnstillinger
%%
%% - Rediger, endre filen etter behov med respekt for kommandosyntaks. Lagre fil (f.eks.
WxT_Tags.txt)
%% – SFTP lest filen til AS under katalogen /tmp
%% - Logg inn AS, bwcli (logg inn som admin)
%% - Utfør følgende kommando fra bwcli: AS_CLI> r /tmp/ WxT_Tags.txt
%% – Bekreft resultatene
%%
%% ----------------------------------------------------------------------------------------------------------
%% Trinn 1: Opprett etikett for kodesett for Koble til – Connect_Tags
%% ----------------------------------------------------------------------------------------------------------
Avslutt alt; System; DeviceTagSet
legge til Connect_Tags
%% ----------------------------------------------------------------------------------------------------------
%% Trinn 2: Legg til WxT for tilpassede BWKS-koder
%% EKSEMPEL - for alle mobile tagger se listen nedenfor-----------------------------------------------------
Avslutt alt; System; DeviceTagSet; Tags
legge til tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% sant
%% ----------------------------------------------------------------------------------------------------------
%% Trinn 3: Angi egendefinerte koder for tilkobling (hvis koden allerede finnes)
%% EKSEMPEL - for alle mobile tagger se listen nedenfor
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverrideable true
tagvalue false
%% ----------------------------------------------------------------------------------------------------------
%% Trinn 4: Kontroller at egendefinerte koder er riktig definert og angitt
```


Cisco konfidensielt

```
%% ----------------------------------------------------------------------------------------------------------------------
Avslutt alt; System; DeviceTagSet; Tags
få tagSetName Connect_Tags
Avslutt alt
```

Nedenfor vises alle egendefinerte koder som brukes av Webex for Cisco BroadWorks, med eksempelverdier (standard eller anbefalte). Vær oppmerksom på at noen av kodene krever verdier som er spesifikke for den tilsvarende distribusjonen (for eksempel serveradresser). Det er derfor disse kodene legges til på slutten av skriptet, men blir tomme, og flere settkommandoer skal legges til for å spesifisere dem.

10.1 Skrivebord

```
legg til tagSetName BroadTouch_tags %ENABLE_REJECT_WITH_486_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_XSI_TRANSFER_CALLS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_XSI_CONFERENCE_CALLS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_WXT% sant
legge til tagSetName BroadTouch_tags %BLF_NOTIFICATION_DELAY_TIME_WXT% 0
legg til tagSetName BroadTouch_tags %ENABLE_REMOTE_CONTROL_EVENTS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALLS_SPAM_INDICATION_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_NOISE_REMOVAL_WXT% usann
legge til tagSetName BroadTouch_tags %TRANSFER_CALL_TYPE_WXT% full
legg til tagSetName BroadTouch_tags %ENABLE_CONFERENCE_CALLS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% usann
legge til tagSetName BroadTouch_tags %MAX_CONF_PARTIES_WXT% 10
legg til tagSetName BroadTouch_tags %ENABLE_CALL_STATISTICS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_PULL_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_MWI_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_VISUAL_VOICE_MAIL_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_WXT% sann
legg til tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%
usann
legg til tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%
usann
legg til tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% usann
legg til tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% usann
legge til tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%
usann
legg til tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%
usann
legg til tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
usann
legg til tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
usann
legg til tagSetName BroadTouch_tags %ENABLE_USE_RPORT_WXT% usann
legg til tagSetName BroadTouch_tags %RPORT_USE_LOCAL_PORT_WXT% usann
legg til tagSetName BroadTouch_tags %USE_TLS_WXT% usann
legge til tagSetName BroadTouch_tags %SBC_PORT_WXT% 5075
legg til tagSetName BroadTouch_tags %USE_PROXY_DISCOVERY_WXT% usann
legge til tagSetName BroadTouch_tags %USE_TCP_FROM_DNS_WXT% true
legge til tagSetName BroadTouch_tags %USE_UDP_FROM_DNS_WXT% sant
legg til tagSetName BroadTouch_tags %USE_TLS_FROM_DNS_WXT% sann
legge til tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
legge til tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
```


Cisco konfidensielt

legg til tagSetName BroadTouch_tags %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% usann
legge til tagSetName BroadTouch_tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
legge til tagSetName BroadTouch_tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
legge til tagSetName BroadTouch_tags %SOURCE_PORT_WXT% 5060
legg til tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% usann
legg til tagSetName BroadTouch_tags %SIP_FAILBACK_ENABLED_WXT% sant
legge til tagSetName BroadTouch_tags %SIP_FAILBACK_TIMEOUT_WXT% 900
legg til tagSetName BroadTouch_tags %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% usann
Legg til tagSetName BroadTouch_tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
legge til tagSetName BroadTouch_tags %TCP_SIZE_THRESHOLD_WXT% 18000
legg til tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_WXT% usann
legg til tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_PEM_SUPPORT_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_SIP_SESSION_ID_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% usann
legg til tagSetName BroadTouch_tags %SRTP_ENABLED_WXT% usann
legg til tagSetName BroadTouch_tags %SRTP_MODE_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_REKEYING_WXT% sant
legge til tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
legge til tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
legge til tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
legge til tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
legge til tagSetName BroadTouch_tags %ENABLE_RTCP_MUX_WXT% sant
legge til tagSetName BroadTouch_tags %ENABLE_XSI_EVENT_CHANNEL_WXT% sant
legg til tagSetName BroadTouch_tags %CHANNEL_HEARTBEAT_WXT% 10000
legg til tagSetName BroadTouch_tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
legg til tagSetName BroadTouch_tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
legge til tagSetName BroadTouch_tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% sant
legg til tagSetName BroadTouch_tags %USE_MEDIASEC_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_SCREEN_SHARE_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_WXT% usann
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_TARGET_WXT% eksterne
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% sant
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% sann
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% sant
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% sant
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% sant
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% sant
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% sant
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% sann
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% sant
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% sant
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% sant
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% usann
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% usann
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% usann
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% usann
legge til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% sant
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% usann
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% sant
legg til tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_URL_WXT%
legge til tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_TARGET_WXT% ekstern
legg til tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_BLIND_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_DIRECTED_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_SIP_VIDEOCALLS_WXT% true
legg til tagSetName BroadTouch_tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
legge til tagSetName BroadTouch_tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% sant

Cisco konfidensielt

```
legge til tagSetName BroadTouch_tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% usann
legge til tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
legg til tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
legge til tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
legg til tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_PARK_WXT% usann
legge til tagSetName BroadTouch_tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
legge til tagSetName BroadTouch_tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% sant
legge til tagSetName BroadTouch_tags %ENABLE_RTP_ICE_WXT% usann
legg til tagSetName BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
legge til tagSetName BroadTouch_tags %RTP_ICE_PORT_WXT% 3478
legge til tagSetName BroadTouch_tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% usann
legg til tagSetName BroadTouch_tags %RTP_ICE_SERVICE_URI_WXT% sant
legge til tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID_WXT% sant
legg til tagSetName BroadTouch_tags %XSI_ROOT_WXT% sant
legg til tagSetName BroadTouch_tags %SBC_ADDRESS_WXT% sant
legge til tagSetName BroadTouch_tags %SBC_PORT_WXT% true
legg til tagSetName BroadTouch_tags %MWI_MODE_WXT% sann
legg til tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% usann
legg til tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_URL_WXT% sant
legge til tagSetName BroadTouch_tags %DOMAIN_OVERRIDE_WXT% true
legg til tagSetName BroadTouch_tags %ENABLE_AUTO_ANSWER_WXT% usann
legg til tagSetName BroadTouch_tags %USE_PAI_AS_CALLING_IDENTITY_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_MULTI_LINE_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_AUDIO_QOS_WXT% sant
legg til tagSetName BroadTouch_tags %AUDIO_QOS_VALUE_WXT% 46
legge til tagSetName BroadTouch_tags %ENABLE_VIDEO_QOS_WXT% sant
legg til tagSetName BroadTouch_tags %VIDEO_QOS_VALUE_WXT% 34
legg til tagSetName BroadTouch_tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% sann
legge til tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_FEC_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_RTX_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_FEC_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_RTX_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_CALL_BLOCK_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_REMOTE_MUTE_CONTROL_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% sant
legge til tagSetName BroadTouch_tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_CALL_MOVE_HERE_WXT% sant
legge til tagSetName BroadTouch_tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% sant
legg til tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_GCP_NOTIFICATIONS_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_GCP_DISPLAY_CALLER_WXT% usann
legge til tagSetName BroadTouch_tags %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% 120
legge til tagSetName BroadTouch_tags %UDP_KEEPALIVE_ENABLED_WXT% true
legg til tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% usann
legg til tagSetName BroadTouch_tags %TLS_KEEPALIVE_ENABLED_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_RTP_ICE_IPV6_WXT% usann
legg til tagSetName BroadTouch_tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% løst
legge til tagSetName BroadTouch_tags %PERSONAL_ASSISTANT_ENABLED_WXT% usann
legg til tagSetName BroadTouch_tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% usann
```


Cisco konfidensielt

10.2 Mobiltelefon

```
legge til tagSetName Connect_Tags %ENABLE_REJECT_WITH_486_WXT% sant
legg til tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_NOISE_REMOVAL_WXT% usann
legg til tagSetName Connect_Tags %TRANSFER_CALL_TYPE_WXT% full
legg til tagSetName Connect_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_CONFERENCE_CALLS_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% usann
legge til tagSetName Connect_Tags %MAX_CONF_PARTIES_WXT% 10
legg til tagSetName Connect_Tags %ENABLE_CALL_STATISTICS_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_CALL_PULL_WXT% usann
legge til tagSetName Connect_Tags %ENABLE_MWI_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_VOICE_MAIL_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% sant
legg til tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% usann
legge til tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%
usann
legg til tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% usann
legg til tagSetName Connect_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% usann
legg til tagSetName Connect_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
usann
legg til tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
usann
legg til tagSetName Connect_Tags %ENABLE_USE_RPORT_WXT% usann
legg til tagSetName Connect_Tags %RPORT_USE_LOCAL_PORT_WXT% usann
legge til tagSetName Connect_Tags %USE_TLS_WXT% usann
legge til tagSetName Connect_Tags %SBC_PORT_WXT% 5075
legg til tagSetName Connect_Tags %USE_PROXY_DISCOVERY_WXT% usann
legg til tagSetName Connect_Tags %USE_TCP_FROM_DNS_WXT% sant
legg til tagSetName Connect_Tags %USE_UDP_FROM_DNS_WXT% sant
legge til tagSetName Connect_Tags %USE_TLS_FROM_DNS_WXT% sant
legg til tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% sann
legg til tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
legg til tagSetName Connect_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
legg til tagSetName Connect_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
legge til tagSetName Connect_Tags %SOURCE_PORT_WXT% 5060
legg til tagSetName Connect_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% usann
Legg til tagSetName Connect_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% DNS
legge til tagSetName Connect_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
legg til tagSetName Connect_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% usann
legge til tagSetName Connect_Tags %ENABLE_PEM_SUPPORT_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_SIP_SESSION_ID_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% usann
legg til tagSetName Connect_Tags %SRTP_ENABLED_WXT% usann
legg til tagSetName Connect_Tags %SRTP_MODE_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_REKEYING_WXT% sant
legge til tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
legge til tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
legge til tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
legge til tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
legg til tagSetName Connect_Tags %ENABLE_RTCP_MUX_WXT% sann
legg til tagSetName Connect_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% sant
legg til tagSetName Connect_Tags %CHANNEL_HEARTBEAT_WXT% 10000
legg til tagSetName Connect_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
```


Cisco konfidensielt

legg til tagSetName Connect_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
legg til tagSetName Connect_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% sann
legg til tagSetName Connect_Tags %USE_MEDIASEC_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_SCREEN_SHARE_WXT% sant
legg til tagSetName Connect_Tags %ENABLE_CALL_CENTER_WXT% usann
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_TARGET_WXT% ekstern
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% sann
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% sant
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% sant
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% sant
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% sant
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% sant
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% sant
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% sant
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% sant
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% sant
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% usann
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% usann
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% usann
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% usann
legge til tagSetName Connect_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% sant
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% usann
legg til tagSetName Connect_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
legg til tagSetName Connect_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
legge til tagSetName Connect_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% ekstern
legg til tagSetName Connect_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_EMERGENCY_DIALING_WXT% usann
legge til tagSetName Connect_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% bare cs-it
legg til tagSetName Connect_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
legg til tagSetName Connect_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% usann
legge til tagSetName Connect_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
legg til tagSetName Connect_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% opptatt
legg til tagSetName Connect_Tags %ENABLE_DIALING_CALL_BACK_WXT% usann
legg til tagSetName Connect_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
legg til tagSetName Connect_Tags %ENABLE_CALL_RECORDING_WXT% usann
legg til tagSetName Connect_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
legg til tagSetName Connect_Tags %ENABLE_SINGLE_ALERTING_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_CALL_PARK_WXT% usann
legg til tagSetName Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
legg til tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% usann
legg til tagSetName Connect_Tags %RTP_ICE_MODE_WXT% icestun
legg til tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% sant
legge til tagSetName Connect_Tags %RTP_ICE_PORT_WXT% 3478
legge til tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
legg til tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% usann
legge til tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
legg til tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% sant
legg til tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% usann
legge til tagSetName Connect_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
legg til tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% sant
legg til tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% sant
legg til tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% sant
legge til tagSetName Connect_Tags %ENABLE_XSI_HOLD_CALLS_WXT% sant
legg til tagSetName Connect_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% usann
legg til tagSetName Connect_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% usann
legg til tagSetName Connect_Tags %RTP_ICE_SERVICE_URI_WXT% sant
legge til tagSetName Connect_Tags %XSI_ROOT_WXT% sant

Cisco konfidensielt

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

10.3 Tavle

```
legg til tagSetName ConnectTablet_Tags %ENABLE_REJECT_WITH_486_WXT% sant
```


Cisco konfidensielt

legg til tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_CALLS_WXT% usann
legg til tagSetName ConnectTablet_Tags %TRANSFER_CALL_TYPE_WXT% full
legg til tagSetName ConnectTablet_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_NOISE_REMOVAL_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CONFERENCE_CALLS_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% usann
legg til tagSetName ConnectTablet_Tags %MAX_CONF_PARTIES_WXT% 10
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_STATISTICS_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_PULL_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_MWI_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% sant
legg til tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% usann
legg til tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% usann
legg til tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% usann
legg til tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% usann
legg til tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_USE_RPORT_WXT% usann
legg til tagSetName ConnectTablet_Tags %RPORT_USE_LOCAL_PORT_WXT% usann
legg til tagSetName ConnectTablet_Tags %USE_TLS_WXT% usann
legge til tagSetName ConnectTablet_Tags %SBC_PORT_WXT% 5075
legg til tagSetName ConnectTablet_Tags %USE_PROXY_DISCOVERY_WXT% usann
legg til tagSetName ConnectTablet_Tags %USE_TCP_FROM_DNS_WXT% sant
legg til tagSetName ConnectTablet_Tags %USE_UDP_FROM_DNS_WXT% sann
legg til tagSetName ConnectTablet_Tags %USE_TLS_FROM_DNS_WXT% sann
legg til tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
legg til tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
legg til tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% sann
legg til tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
legge til tagSetName ConnectTablet_Tags %SOURCE_PORT_WXT% 5060
legg til tagSetName ConnectTablet_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% usann
Legg til tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% DNS
legge til tagSetName ConnectTablet_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
legg til tagSetName ConnectTablet_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_PEM_SUPPORT_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_SIP_SESSION_ID_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% usann
legg til tagSetName ConnectTablet_Tags %SRTP_ENABLED_WXT% usann
legg til tagSetName ConnectTablet_Tags %SRTP_MODE_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_REKEYING_WXT% true
legge til tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
legge til tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
legge til tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
legge til tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
legge til tagSetName ConnectTablet_Tags %ENABLE_RTCP_MUX_WXT% sant
legge til tagSetName ConnectTablet_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% sant
legge til tagSetName ConnectTablet_Tags %CHANNEL_HEARTBEAT_WXT% 10000

Cisco konfidensielt

legg til tagSetName ConnectTablet_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
legg til tagSetName ConnectTablet_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
legg til tagSetName ConnectTablet_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% sant
legg til tagSetName ConnectTablet_Tags %USE_MEDIASEC_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_SCREEN_SHARE_WXT% true
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_CENTER_WXT% usann
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_TARGET_WXT% eksterne
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% sann
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% sant
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% sant
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% sant
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% sant
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% sant
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% sann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% sant
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% sant
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% sant
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% sann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% usann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% usann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% usann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% usann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% sant
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% usann
legg til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
legg til tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
legge til tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% ekstern
legg til tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
legg til tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_DIALING_WXT% usann
legge til tagSetName ConnectTablet_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% bare cs-it
legg til tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
legg til tagSetName ConnectTablet_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% usann
legge til tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
legge til tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% opptatt
legg til tagSetName ConnectTablet_Tags %ENABLE_DIALING_CALL_BACK_WXT% usann
legge til tagSetName ConnectTablet_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_RECORDING_WXT% usann
legge til tagSetName ConnectTablet_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
legg til tagSetName ConnectTablet_Tags %ENABLE_SINGLE_ALERTING_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_PARK_WXT% usann
legge til tagSetName ConnectTablet_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
legg til tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_WXT% usann
legg til tagSetName ConnectTablet_Tags %RTP_ICE_MODE_WXT% icestun
legge til tagSetName ConnectTablet_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% sant
legg til tagSetName ConnectTablet_Tags %RTP_ICE_PORT_WXT% 3478
legg til tagSetName ConnectTablet_Tags %ENABLE_DIALING_VOIP_WXT% sann
legg til tagSetName ConnectTablet_Tags %ENABLE_DIALING_NATIVE_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_DIALING_MODE_WXT% sant
legge til tagSetName ConnectTablet_Tags %DIALING_MODE_DEFAULT_WXT% sant
legg til tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% usann
legge til tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
legge til tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% sant
legg til tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% sant
legge til tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% sant
legge til tagSetName ConnectTablet_Tags %ENABLE_XSI_HOLD_CALLS_WXT% sant
legge til tagSetName ConnectTablet_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% usann

Cisco konfidensielt

```
legg til tagSetName ConnectTablet_Tags %RTP_ICE_SERVICE_URI_WXT% sann
legg til tagSetName ConnectTablet_Tags %XSI_ROOT_WXT% sant
legge til tagSetName ConnectTablet_Tags %SBC_ADDRESS_WXT% sant
legg til tagSetName ConnectTablet_Tags %SBC_PORT_WXT% sant
legg til tagSetName ConnectTablet_Tags %MWI_MODE_WXT% sann
legg til tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
legge til tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_URL_WXT% sant
legge til tagSetName ConnectTablet_Tags %DOMAIN_OVERRIDE_WXT% sant
legg til tagSetName ConnectTablet_Tags %ENABLE_SIP_VIDEOCALLS_WXT% sant
legg til tagSetName ConnectTablet_Tags %ENABLE_LOCUS_VIDEOCALLS_WXT% sann
legg til tagSetName ConnectTablet_Tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% usann
legg til tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% usann
legge til tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
legg til tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
legg til tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
legg til tagSetName ConnectTablet_Tags %USE_PAI_AS_CALLING_IDENTITY_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_RING_SPLASH_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_PN_MOBILE_CALL_INFO_WXT% true
legge til tagSetName ConnectTablet_Tags %ENABLE_AUDIO_QOS_WXT% sant
legg til tagSetName ConnectTablet_Tags %AUDIO_QOS_VALUE_WXT% 46
legg til tagSetName ConnectTablet_Tags %ENABLE_VIDEO_QOS_WXT% sant
legge til tagSetName ConnectTablet_Tags %VIDEO_QOS_VALUE_WXT% 34
legg til tagSetName ConnectTablet_Tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
legg til tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_FEC_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_RTX_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_FEC_WXT% false
legg til tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_RTX_WXT% false
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_BLOCK_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_WIDGET_HOLD_CALLS_WXT% sant
legg til tagSetName ConnectTablet_Tags %ENABLE_WIDGET_TRANSFER_CALLS_WXT% sann
legg til tagSetName ConnectTablet_Tags %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%
sant
legg til tagSetName ConnectTablet_Tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% sant
legge til tagSetName ConnectTablet_Tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
legge til tagSetName ConnectTablet_Tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% sant
legg til tagSetName ConnectTablet_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
legge til tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% sant
legge til tagSetName ConnectTablet_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% sann
legg til tagSetName ConnectTablet_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%
usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
legg til tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% usann
legge til tagSetName ConnectTablet_Tags %UDP_KEEPALIVE_ENABLED_WXT% sant
legg til tagSetName ConnectTablet_Tags %TCP_KEEPALIVE_ENABLED_WXT% usann
legg til tagSetName ConnectTablet_Tags %TLS_KEEPALIVE_ENABLED_WXT% usann
legg til tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_IPV6_WXT% usann
legg til tagSetName ConnectTablet_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% løst
legg til tagSetName ConnectTablet_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% usann
legg til tagSetName ConnectTablet_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% usann
legge til tagSetName ConnectTablet_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% usann
```


Cisco konfidensielt

10.4 System Tags

Følgende liste 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%
%BW-n%
%BWUTSEENDE-ETIKETT-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMÆR%
%BWE911-PRIMÆR-HELDURL%
%BWE911-CUSTOMERID%
%BWE911-SECRETKEY%
%BWE911-NØDNUMMER-LISTE%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%
```


Cisco konfidensielt

11 Akronymer og forkortelser

Denne delen viser akronymer og forkortelser som finnes i dette dokumentet. Forkortelsene og forkortelsene er oppført i alfabetisk rekkefølge sammen med deres betydning.

ACB	Automatisk tilbakeringing
ACD	Automatisk anropsdistribusjon
ACR	Anonym avvisning av anrop
AES	AES, Avansert krypteringsstandard
ALG	Gateway for programlag
API	Approgrammeringsgrensesnitt
APK	Søknad Package
APNS	Apples push-varslingstjeneste
ARS	Automatisk valg av bithastighet
SOM	Programserver (Cisco BroadWorks)
AVP	Audiovisuell profil
BW	BroadWorks
BWA	BroadWorks hvor som helst
BWKS	BroadWorks
BWM	BroadWorks-mobilitet
BYOD	Ta med din egen enhet
CC	Kundesenter
CFB	Viderekobling av anrop opptatt
CFNA	Viderekobling uten svar
CFNR	Viderekobling kan ikke nås
CIF	Felles mellomliggende format
CLI	Grensesnitt for kommandolinje
KLID	Anropslinjeidentitet
CLIDB	Blokkering av levering av anropslinje-ID
CRLF	Returlinjefeed for transport
CS	Krets-slått
CSWV	Webvisning for samtaleinnstillinger
CW	Samtale venter
DB	Database
DM	Enhetsadministrasjon
IkkeFor	Ikke forstyrr
DNS	Domenenavnsystem

Cisco konfidensielt

DPC	Kontroll for bordtelefon
DTAF	Arkivfil for enhetstype
ECACS	Tjeneste for endring av adresse for nødanrop
FMC	Fast-mobil konvergens
FQDN	Fullstendig kvalifisert domenenavn
HMAC	Hash-melding autentiseringskode
ICE	Etablering av interaktive tilkoblingsmuligheter
iLBC	Internett med lav bithastighetskodek
IM	Chat
IM&P	Direktemeldinger og tilstedeværelse
IOT	Interoperabilitetstesting
IP	Internett-protokoll
JID	Jabber-identifikator
M/O	Obligatorisk/valgfritt
MNO	Mobilnettoperatør
MTU	Maksimal overføringsenhet
MUC	Chat for flere brukere
MWI	Meldingslampe
NAL	Nettverksabstraksjonslag
NAPTR	Peker for navngiving av autoritet
NAT	Oversettelse av nettverksadresse
OTT	Over toppen
PA	Personlig assistent
PAI	P-påstått-identitet
PEM	P-Early Media
PLI	Indikasjon på tap av bilde
PLMN	Offentlig landmobilnett
PN	Push-varsling
QCIF	Kvartal felles mellomliggende format
QoS	Quality of Service
RO	Eksternt kontor
RTCP	Kontrollprotokoll i sanntid
RTP	Sanntidsprotokoll (Real Time Protocol)
SaaS	Programvare som en tjeneste
SAN	Alternativt emnenavn
SASL	Enkelt autentiserings- og sikkerhetslag

Cisco konfidensielt

SAVP	Sikker lydvideoprofil
SBC	Øktgrensekontroller
SCA	Utseende for delt samtale
SCF	Funksjon for øktkontinuitet
SCTP	Overføringsprotokoll for strømkontroll
SDP	Protokoll for øktdefinisjon
SEQRING	Sekvensiell ring
SIMRING	Samtidig ringing
SIP	Session Initiation Protocol
SNR	Signal/støy-forhold
SNR	Single Number Reach
SRTCP	Sikker kontrollprotokoll i sanntid
SRTP	Sikker transportprotokoll i sanntid
SSL	Lag for sikre stikkontakter
STUN	Økttraverseringsverktøy for NAT
SUBQCIF	Sub kvartal CIF
TCP	Transmission Control Protocol
TLS	Transport Layer Security; kryptografisk protokoll
TTL	Tid til å leve
TURN	Traversering ved hjelp av NAT for relé
UDP	User Datagram Protocol
Brukergrensesnitt	Brukergrensesnitt
UMS	Meldingsserver (Cisco BroadWorks)
URI	Uniform Resource Identifier
UVS	Videoserver (Cisco BroadWorks)
VGA	Videografikk Array
VoIP	Voice Over IP
VVM	Visuell talepost
WXT	Webex
XMPP	Extensible Messaging and Presence Protocol
XR	Utvidet rapport
Xsp	Xtended Services Platform
Xsi	Grensesnitt for Xtended Tjenester

Cisco konfidensielt