Guide de configuration de Webex pour Cisco BroadWorks

Version 44.7

Version du document 1

Table des matières

1 Résumé des modifications 1
1.1 Changements pour la version 44.7, juillet 2024 1
1.2 Changements pour la version 44.6, juin 2024 1
1.3 Changements pour la version 44.5, mai 2024 1
1.4 Changements pour la version 44.4, avril 2024 1
1.5 Changements pour la version 44.3, mars 2024 1
1.6 Changements pour la version 44.2, février 2024 1
1.7 Changements pour la version 43.1, janvier 2024 2
1.8 Changements pour la version 43.12, décembre 2023 2
1.9 Changements pour la version 43.11, novembre 2023 2
1.10 Changements pour la version 43.10, octobre 2023 2
1.11 Changements pour la version 43.9, septembre 2023 3
1.12 Changements pour la version 43.8, août 2023 3
1.13 Changements pour la version 43.7, juillet 2023 3
1.14 Changements pour la version 43.6, juin 2023 3
1.15 Changements pour la version 43.5, mai 2023 3
1.16 Changements pour la version 43.4, avril 2023 4
1.17 Changements pour la version 43.3, mars 2023 4
1.18 Changements pour la version 43.2, février 2023 4
1.19 Changements pour la version 43.1, janvier 2023 4
2 Modifications des fichiers de configuration 5
2.1 Modifications apportées aux fichiers de configuration pour la version 44.7 5
2.2 Modifications apportées aux fichiers de configuration pour la version 44.6 5
2.3 Modifications apportées aux fichiers de configuration pour la version 44.5 5
2.4 Modifications apportées aux fichiers de configuration de la version 44.4 6
2.5 Modifications apportées aux fichiers de configuration de la version 44.3 6
2.6 Modifications apportées aux fichiers de configuration de la version 44.2 7
2.7 Modifications apportées aux fichiers de configuration de la version 44.1 8
2.8 Modifications apportées aux fichiers de configuration de la version 43.12 8
2.9 Modifications apportées aux fichiers de configuration de la version 43.11 10
2.10 Modifications apportées aux fichiers de configuration de la version 43.10 10
2.11 Modifications apportées aux fichiers de configuration de la version 43.9 10
2.12 Modifications apportées aux fichiers de configuration de la version 43.8 11
2.13 Modifications apportées aux fichiers de configuration de la version 43.7 11
2.14 Modifications apportées aux fichiers de configuration de la version 43.6 11
2.15 Modifications apportées aux fichiers de configuration de la version 43.5 11
2.16 Modifications apportées aux fichiers de configuration de la version 43.4 12
2.17 Modifications apportées aux fichiers de configuration de la version 43.3 13
2.18 Modifications apportées aux fichiers de configuration de la version 43.2 13

Confidentiel à Cisco

2.19 Modifications apportées aux fichiers de configuration de la version 43.1 14
3 Introduction 15
4 Installation 16
4.1 Téléchargement localisé du client 16
4.2 Client Android 16
4.3 Client iOS 16
4.4 Client de bureau 17
5 Gestion des périphériques 18
5.1 Balises de gestion des périphériques 18
5.2 Améliorations de correspondance partielle pour la sélection du type de périphérique 19
5.3 Configuration du client 20
5.4 Déploiement de config-wxt.xml 20
5.5 Fichier de configuration (config-wxt.xml) 20
5.6 Balises par défaut système 21
5.7 Balises système intégré Cisco BroadWorks Dynamic 21
6 Balises personnalisées 24
6.1 Caractéristiques communes 36
6.1.1 Paramètres du serveur SIP 36
6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel 39
6.1.3 En-têtes SIP 3GPP pour SRTP 41
6.1.4 Forcer l'utilisation de TCP, TLS ou UDP et Keepalives 42
6.1.5 Délai d'expiration configurable pour l'ouverture du socket SIP 44
6.1.6 Découverte dynamique du proxy SIP 45
6.1.7 Utilisation du port préféré pour SIP 50
6.1.8 Basculement et restauration SIP 51
6.1.9 SIP SUBCSRIBE et REGISTER Actualiser et S'ABONNER Réessayer 56
6.1.10 Utiliser les URI P-Associated dans REGISTER 56
6.1.11 En-tête SIP P-Early Media (PEM) 57
6.1.12 Prise en charge de la MISE À JOUR SIP 57
6.1.13 Ancien SIP INFO FIR 58
6.1.14 Gestion du port SIP pour la traversée NAT 58
6.1.15 ID de session SIP 59
6.1.16 Comportement de rejet d'appel entrant 60
6.1.17 Plage de ports de protocole de transport en temps réel 60
6.1.18 Prise en charge ICE (Webex Calling uniquement) 61
6.1.19 MUX RTCP 62
6.1.20 Transférer 62
6.1.21 Conférences téléphoniques à N-Way et participants 64
6.1.22 Call Pull (Transfert d'appel) 65
6.1.23 Parcage/Récupération d'appels 65
6.1.24 Stat. appels 66

Confidentiel à Cisco

6.1.25 Récupération automatique des appels / Transfert d'appel fluide 66
6.1.26 Enregistrement des appels 67
6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente ... 68
6.1.28 Transcription de la messagerie vocale pour Webex Calling 70
6.1.29 Paramètres des appels 70
6.1.30 Portail des paramètres et paramètres d'appel basés sur le Web 73
6.1.31 Connexion/déconnexion du centre d'appels/de la file d'attente d'appels 76
6.1.32 Racine et chemins XSI 77
6.1.33 Canal d'événement XSI 77
6.1.34 Configuration du codec 78
6.1.35 Numérotation SIP-URI 80
6.1.36 Historique des appels sur tous les périphériques 80
6.1.37 Désactiver les appels vidéo 81
6.1.38 Appels d'urgence (911) - Création de rapports de localisation avec le fournisseur E911 82
6.1.39 PAI comme identité 83
6.1.40 Désactiver le partage d'écran 84
6.1.41 Indication d'appel de spam 84
6.1.42 Suppression du bruit et extension de la bande passante pour les appels RTCP/mobiles 85
6.1.43 Marquage DSCP QoS 85
6.1.44 Profil principal 86
6.1.45 Liste de blocage (Webex Calling uniquement) 88
6.1.46 Adaptation des médias et mise en œuvre de la résilience (MARI) 89
6.1.47 Appels simultanés avec le même utilisateur 91
6.1.48 RTCP-XR 91
6.1.49 Informations sur le transfert d'appel 92
6.1.50 ID de l'appelant 92
6.2 Fonctionnalités du bureau uniquement 96
6.2.1 Déconnexion forcée 96
6.2.2 Prise d'appel 96
6.2.3 Prise en charge Boss-Admin (Cadre de direction-Assistant) 97
6.2.4 Transférer les appels SIP vers une réunion (Webex Calling uniquement) 98
6.2.5 Appel de contrôle du téléphone de bureau – Réponse automatique 98
6.2.6 Réponse automatique avec notification de tonalité 99
6.2.7 Contrôle du téléphone de bureau – Commandes en cours d'appel – Conférence 99
6.2.8 Notifications d'interception d'appels 99
6.2.9 Pack d'événements de contrôle à distance 102
6.2.10 Sélection CLID de l'agent de la file d'attente d'appels 102
6.2.11 Passerelle de survivabilité (Webex Calling uniquement) 103
6.2.12 Multiligne - Apparence de ligne partagée 103
6.2.13 Multi-lignes - Lignes virtuelles (Webex Calling uniquement) 104

Confidentiel à Cisco

6.2.14 Pack d’événements de contrôle de coupure du son à distance (Webex Calling uniquement) 105
6.2.15 Déplacer l'appel 106
6.3 Fonctionnalités mobiles uniquement 108
6.3.1 Appels d’urgence 108
6.3.2 Notifications push pour les appels 109
6.3.3 Alerte unique 111
6.3.4 Cliquer pour composer (Rappel) 111
6.3.5 Prise en charge du MNO 112
6.3.6 ID de l'appelant entrant 117
7 Fonctionnalités de l'essai précoce sur le terrain (BÊTA) 119
7.1 Codec IA 119
8 Mappage des balises personnalisées entre Webex pour Cisco BroadWorks et UC-One 120
9 Annexe A : Codes de chiffrement TLS 127
10 Annexe B : Script de mise à disposition de la balise DM 128
10.1 Bureau 129
10.2 Mobile 132
10.3 Tablette 135
10.4 Balises système 138
11 Acronymes et abréviations 139

Confidentiel à Cisco

1 Résumé des modifications

Cette section décrit les modifications apportées à ce document pour chaque version et version du document.

1.1 Changements pour la version 44.7, juillet 2024

Cette version du document intègre les évolutions suivantes :

- Ajout de la section *Codec IA* dans BETA.
- Mise à jour de la section *6.1.44 Primary Profile* – suppression des détails sur le comportement priori de l'application Webex vers la version 43.2.

1.2 Changements pour la version 44.6, juin 2024

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.3.6. ID de l&*apos;appelant entrant – ajout de plus de détails sur l'expérience native et le fonctionnement de la fonctionnalité

1.3 Changements pour la version 44.5, mai 2024

Cette version du document intègre les évolutions suivantes :

- Section mise à jour*6.1.18Prise en charge ICE (Webex* Calling uniquement)– ajout de la prise en charge IPv6 via NAT64.
- Section mise à jour *6.1.50ID de* l'appelant - ajout de la sous-section *6.1.50.2Nom de l'ID de* l'appelant distant.

1.4 Changements pour la version 44.4, avril 2024

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.1.50.1ID de l'appelant sortant (Webex* Calling uniquement).
- Section mise à jour *Modifications apportées aux fichiers de configuration de* la version 44.3 – ajout de détails sur les mises à jour keepalive dans 44.3.

1.5 Changements pour la version 44.3, mars 2024

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.3.6. ID de l&*apos;appelant entrant
    - La section *6.1.50.1ID de l'appelant sortant (Webex* Calling uniquement) a été déplacée comme commune pour Desktop et Mobile, et l'a mise à jour avec plus de détails.
- Mise à jour de la section *6.1.4Forcer l'utilisation de TCP, TLS ou UDP et* Keepalives – ajout de détails sur les keepalives configurables utilisant des balises personnalisées.

1.6 Changements pour la version 44.2, février 2024

Cette version du document intègre les évolutions suivantes :

Confidentiel à Cisco

- Ajout de la section *6.3.6ID de l*'appelant entrant avec des sous-sections :
  - 6.3.6.1 ID de l'appelant entrant
  - 6.3.6.2 ID de l'appelant sortant (Webex Calling uniquement)
- Section mise à jour *6.2.8 Notifications d'interception* d'appels
  - Ajout de la sous-section *6.2.8.1Voyant d'occupation de* ligne (BLF) - déplacement des détails FLO dans celle-ci.
  - Ajout du paragraphe *6.2.8.2Groupe d'interception d'appels (Webex* Calling uniquement).
- Ajout de la section *6.1.49Informations sur le* transfert d'appel.
- Mise à jour de la section *6.1.8.3Appliquer la version* IP – ajout de détails pour le nouveau mode *nat64*.
- Mise à jour de la section *6.1.42Suppression du bruit et extension de la bande passante* pour les appels RTCP/mobiles – ajout de détails pour la prise en charge des nouvelles extensions de bande passante et les mises à jour de la suppression du bruit. La section *Améliorations vocales pour les appels RTCP* est supprimée de la version BÊTA.

1.7 Changements pour la version 43.1, janvier 2024

Aucun changement n'a été apporté à ce document pour cette version.

1.8 Changements pour la version 43.12, décembre 2023

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.1.1Paramètres du serveur* SIP – mise à jour de l'exemple (ajout de domaine et d'identifiant externe par ligne).
- Ajout de la section*6.2.15Déplacer l'appel*.
- Mise à jour de la section *6.3.5.1Appel avec numéroteur natif* – ajout de détails sur la prise en charge du préfixe configurable pour les appels sortants cellulaires.
- Mise à jour de la section *6.1.20Transférer* – ajout de détails sur la nouvelle option de maintien automatique.
- Ajout de la section *6.1.48RTCP-XR*.
- Ajout de la section *Améliorations vocales pour les appels RTCP* dans la version BÊTA.

1.9 Changements pour la version 43.11, novembre 2023

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.1.8.1Basculement SIP* – ajout de détails sur le nettoyage des inscriptions et les mises à jour de la valeur q.

1.10 Changements pour la version 43.10, octobre 2023

Cette version du document intègre les évolutions suivantes :

- La section *6.1.29.2Transfert d'appel vers la messagerie vocale*a été déplacée à partir de la version BÊTA.
- Section mise à jour *6.3.5.2Commandes en* cours d'appel– ajout de détails sur le transfert consultatif et le transfert vers un autre appel en cours.
- Mise à jour de la section *6.3.5.6MNO Mobility - Widget en* cours d'appel – ajout de détails sur le transfert complet.

1.11 Changements pour la version 43.9, septembre 2023

Cette version du document intègre les évolutions suivantes :

- Section déplacée*6.1.47Appels simultanés avec le même* utilisateurhors de BETA.
- Mise à jour de la section*6.1.20Transférer* – ajout de détails sur le transfert vers un appel en cours.
- Section ajoutée *6.2.14*
- *Pack d'événements de contrôle de coupure du* son à distance (Webex Calling uniquement).
- Ajout de la section *Transfert d'appel vers la messagerie vocale* dans la version BÊTA.

1.12 Changements pour la version 43.8, août 2023

Cette version du document intègre les évolutions suivantes :

- Ajout de la section*Appels simultanés avec le même* utilisateurdans BETA.

1.13 Changements pour la version 43.7, juillet 2023

Cette version du document intègre les évolutions suivantes :

- Déplacement de la section *6.3.5.6MNO Mobility - Widget en* cours d'appel hors de BETA.

1.14 Changements pour la version 43.6, juin 2023

Cette version du document intègre les évolutions suivantes :

- Déplacement de la section *6.1.46Adaptation des médias et mise en œuvre* de la résilience (MARI) hors de BETA.
- Ajout de la section *MNO Mobility - Widget en* cours d'appel dans BETA.
- Mise à jour de la section *5.4Déploiement de config-wxt.xml* - ajout d'une recommandation pour maintenir le modèle de configuration à jour avec la dernière version de l'application Webex.

1.15 Changements pour la version 43.5, mai 2023

Cette version du document intègre les évolutions suivantes :

- Ajout de la section *6.1.45Liste de blocage (Webex Calling* uniquement).
- Mise à jour de la section *6.1.44 Primary Profile*.

Confidentiel à Cisco

1.16 Changements pour la version 43.4, avril 2023

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.2.8Notifications d'interception* d'appels. Notifications d'interception d'appels
- Ajout de la section *6.2.13Multi-lignes - Lignes virtuelles (Webex Calling uniquement)*.
- Ajout de la section *Adaptation des médias et mise en œuvre* de la résilience (MARI) dans BETA.

1.17 Changements pour la version 43.3, mars 2023

Cette version du document intègre les évolutions suivantes :

- Ajout de la section *6.1.44 Primary Profile.*
- Section mise à jour *6.2.12*
- *Multiligne - Apparence* de ligne partagée.

1.18 Changements pour la version 43.2, février 2023

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.2.12*
- *Multiligne - Apparence* de ligne partagée.
- Ajout de *6.2.11Passerelle de survivabilité (Webex Calling* uniquement).
- Section mise à jour *6.1.4Forcer l'utilisation de TCP, TLS ou UDP et* Keepalives.

1.19 Changements pour la version 43.1, janvier 2023

Cette version du document intègre les évolutions suivantes :

- Section mise à jour *6.2.12*
- *Multiligne - Apparence* de ligne partagée.

Confidentiel à Cisco

2 Modifications des fichiers de configuration

2.1 Modifications apportées aux fichiers de configuration pour la version 44.7

- [Fonctionnalité BÊTA] Ajout du codec AI (xCodec) dans la section <services><calls><audio><codecs>.

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

2.2 Modifications apportées aux fichiers de configuration pour la version 44.6

Aucune mise à jour n'a été effectuée dans les fichiers de configuration pour cette version.

2.3 Modifications apportées aux fichiers de configuration pour la version 44.5

- [Webex Calling uniquement]
  Ajout de l'attribut enable-ipv6-support à la balise <protocols><rtp><ice>.

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

- La balise <remote-name> a été ajoutée dans la section <services><calls><caller-id> avec <machine> comme sous-balise.

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

Les %TAG%s suivants ont été ajoutés :

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

Confidentiel à Cisco

2.4 Modifications apportées aux fichiers de configuration de la version 44.4

- [Bureau uniquement] [Webex Calling uniquement]
  Ajout des balises <additional-numbers>, <hunt-group> et <clid-delivery-blocking> sous la section <caller-id><appels sortants>.

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

2.5 Modifications apportées aux fichiers de configuration de la version 44.3

- [Bureau uniquement] [Webex Calling uniquement]
  Ajout de <appels sortants> sous la nouvelle section <caller-id>, avec <call-center> comme sous-balise.

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

- Ajout de balises personnalisées (%UDP_KEEPALIVE_ENABLED_WXT%,%TCP_KEEPALIVE_ENABLED_WXT% et %TLS_KEEPALIVE_ENABLED_WXT%) pour remplacer la valeur activée keep-alive codée en dur pour chaque transport sous <protocols><sip><transports>.

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

Les %TAG%s suivants ont été ajoutés :

- %UDP_KEEPALIVE_ENABLED_WXT%

Confidentiel à Cisco

- %TCP_KEEPALIVE_ENABLED_WXT%
- %TLS_KEEPALIVE_ENABLED_WXT%

2.6 Modifications apportées aux fichiers de configuration de la version 44.2

- [Mobile uniquement]
  Ajout de la section <caller-id> sous <services><calls>. Ajout des sous-balises <incoming-call> et <missed-call>, avec une nouvelle sous-balise <append-number> pour les deux.

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

- [Mobile uniquement] [Webex Calling uniquement]
  Ajout de <appels sortants> sous la nouvelle section <caller-id>.

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

- Ajout de la balise <call-forwarding-info> dans la section <services><calls>.

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

- [Bureau uniquement] [Webex Calling uniquement]
  Ajout de la section <group-call-pickup-notifications> sous <services><calls>, avec <display-caller> et <max-timeout> comme sous-balises. Ajout également de balise <group-call-pickup> sous chaque balise <line> dans la section <protocols><sip><lines>.

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


Confidentiel à Cisco

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

Les %TAG%s suivants ont été ajoutés :

- %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%
- %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%
- %ENABLE_GCP_NOTIFICATIONS_WXT%
- %ENABLE_GCP_DISPLAY_CALLER_WXT%
- %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%
- %BWGROUP-CALL-PICKUP-BOOL-n%

Le %TAG% suivant a été déprécié :

- %ENABLE_NOISE_REMOVAL_WXT%

2.7 Modifications apportées aux fichiers de configuration de la version 44.1

Aucune mise à jour n'a été effectuée dans les fichiers de configuration pour cette version.

2.8 Modifications apportées aux fichiers de configuration de la version 43.12

- Ajout de la balise <domain> pour chaque section <line> sous <config><protocols><sip><lines>.

```
<config>
<protocols><sip>
    <lines>
        <line>
            <domain>%BWHOST-1%</domain>
            ...
        </line>
        <line>
            <domain>%BWHOST-2%</domain>
```


Confidentiel à Cisco

```
            ...
        </line>
        ...
```

- [Bureau uniquement]
  Ajout de la section <call-move> avec la balise <move-here> sous la section <config><services><calls>.

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

- Ajout de la balise <speech-enhancements> sous la section <config><services><calls>.

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

- [Mobile uniquement]
  Ajout de la balise <fac-prefix> sous la section <config><services><dialing><native>.

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

- Ajout de l'attribut de mise en attente automatique dans la balise <config><services><calls><transfer-call>.

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

- Ajout de la section <rtcp-xr> sous <config><protocols><sip>.

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

Les %TAG%s suivants ont été ajoutés :

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

Confidentiel à Cisco

2.9 Modifications apportées aux fichiers de configuration de la version 43.11

- Ajout d'une nouvelle section <register-failover> avec <registration-cleanup> comme sous-balise sous la section <config><protocols><sip>. La balise <q-value> a été déplacée sous la balise <register-failover>.

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

Le %TAG% suivant a été ajouté :

- %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%

2.10 Modifications apportées aux fichiers de configuration de la version 43.10

Aucune mise à jour n'a été effectuée dans les fichiers de configuration pour cette version.

2.11 Modifications apportées aux fichiers de configuration de la version 43.9

- Renommer la balise <multiple-calls-per-user> dans la section <config><services><calls> par <simultaneous-calls-with-same-user>.

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

- Ajout d'une nouvelle balise <remote-mute-control> dans la section <config><services><calls>.

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

- Ajout d'une nouvelle balise <forwarding> dans la section <config><services><voice-mail>.

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

Le %TAG% suivant a été mis à jour :

- %ENABLE_MULTIPLE_CALLS_PER_USER_WXT% was renamed to %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%

Les %TAG%s suivants ont été ajoutés :

- %ENABLE_REMOTE_MUTE_CONTROL_WXT%
- %ENABLE_VOICE_MAIL_FORWARDING_WXT%

Confidentiel à Cisco

2.12 Modifications apportées aux fichiers de configuration de la version 43.8

- Ajout d'une nouvelle balise <multiple-calls-per-user> dans la section <config><services><calls>.

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

Le %TAG% suivant a été ajouté :

- %ENABLE_MULTIPLE_CALLS_PER_USER_WXT%

2.13 Modifications apportées aux fichiers de configuration de la version 43.7

Aucune mise à jour n'a été effectuée dans les fichiers de configuration pour cette version.

2.14 Modifications apportées aux fichiers de configuration de la version 43.6

- [Mobile uniquement]
  Ajout de nouveaux attributs activés par widget dans les balises <hold>, <transfer-call> et <escalate-to-webex-meeting> sous la section <config><services><calls>

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

Les %TAG%s suivants ont été ajoutés :

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

2.15 Modifications apportées aux fichiers de configuration de la version 43.5

- [Webex Calling uniquement]
  Ajout de la balise <call-block> sous la section <config><services><calls>

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

Le %TAG% suivant a été ajouté :

- %ENABLE_CALL_BLOCK_WXT%

Confidentiel à Cisco

2.16 Modifications apportées aux fichiers de configuration de la version 43.4

- [Webex Calling uniquement]
  Ajout de l'attribut *lineType* pour chaque balise <line>. Ajout de la balise <external-id> sous chaque balise <line>.

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

- Ajout de la section <audio-quality-enhancements> sous la section <services><calls><audio> et <video-quality-enhancements> sous <services><calls><video>

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


Confidentiel à Cisco

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

- [Bureau uniquement]
  Suppression de la valeur codée en dur pour le nom de l'étiquette de la première ligne sous la section <ligne> correspondante sous <protocoles><sip>.

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

Les %TAG%s suivants ont été ajoutés :

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

Le niveau système suivant %TAG%s a été ajouté :

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

2.17 Modifications apportées aux fichiers de configuration de la version 43.3

Aucune mise à jour n'a été effectuée dans les fichiers de configuration pour cette version.

2.18 Modifications apportées aux fichiers de configuration de la version 43.2

Ajout de la balise <device-owner-restriction> sous la section <services><calls>.

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


Confidentiel à Cisco

Le %TAG% suivant a été ajouté :

- %ENABLE_DEVICE_OWNER_RESTRICTION_WXT%

2.19 Modifications apportées aux fichiers de configuration de la version 43.1

Aucune mise à jour n'a été effectuée dans les fichiers de configuration pour cette version.

Confidentiel à Cisco

3 Introduction

L'objectif de ce document est de fournir une description de la configuration du client Webex pour Cisco BroadWorks.

Le fichier de configuration *config-wxt.xml* est fourni en deux versions : une pour mobile (Android et iOS) et une pour ordinateur de bureau (Windows et MacOS).

Les clients sont configurés à l'aide d'une configuration qui n'est pas visible par l'utilisateur final. Le fichier *config-wxt.xml* fournit des informations spécifiques au serveur, telles que les adresses et les ports du serveur et les options d'exécution pour le client lui-même (par exemple, les options visibles dans l'écran *Paramètres*).

Les fichiers de configuration sont lus par le client au démarrage, après avoir été récupérés à partir de la gestion des périphériques. Les informations provenant des fichiers de configuration sont stockées chiffrées, ce qui les rend invisibles et inaccessibles à l'utilisateur final.

> **REMARQUE :** Les propriétés XML ne doivent pas contenir d'espaces (par exemple, <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"/> au lieu de <transfer-call enabled = "%ENABLE_TRANSFER_CALLS_WXT%"/>).

Confidentiel à Cisco

4 Installation

Les clients Webex pour Cisco BroadWorks peuvent être installés à partir des éléments suivants :

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

4.1 Téléchargement localisé du client

Les versions localisées suivantes des clients Webex pour Cisco BroadWorks peuvent être téléchargées comme suit :

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 Client Android

Le client Android est installé en tant qu'application (pack d'application Android [APK]), qui conserve les données relatives aux paramètres et à la configuration dans sa zone privée.

Il existe un contrôle de version basé sur les procédures de Google Play. Une notification Google Play standard est fournie (c'est-à-dire qu'Android indique automatiquement qu'une nouvelle version du logiciel est disponible).

Lorsque la nouvelle version est téléchargée, l'ancien logiciel est écrasé ; cependant, les données utilisateur sont conservées par défaut.

Notez que l'utilisateur n'est pas tenu de sélectionner des options d'installation ou de désinstallation.

4.3 Client iOS

Le client iOS est installé en tant qu'application, qui conserve les données relatives aux paramètres dans son « sandbox » et les données du fichier de configuration sont stockées chiffrées.

Il existe un contrôle de version basé sur les procédures de l'Apple App Store. L'icône App Store est mise en surbrillance pour indiquer qu'une nouvelle version du logiciel est disponible.

Lorsque la nouvelle version est téléchargée, l'ancien logiciel est écrasé ; cependant, les données utilisateur sont conservées par défaut.

Notez que l'utilisateur n'est pas tenu de sélectionner des options d'installation ou de désinstallation.

Confidentiel à Cisco

4.4 Client de bureau

Des informations sur l'installation et le contrôle de version du client de bureau (Windows et MacOS) sont disponibles sur les sites suivants : https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade.

Confidentiel à Cisco

5 Gestion des périphériques

5.1 Balises de gestion des périphériques

Webex pour Cisco BroadWorks utilise les *ensembles de balises de gestion des périphériques* illustrés dans la figure suivante. Les ensembles de balises *Système par défaut* et personnalisées sont nécessaires pour fournir des paramètres spécifiques du périphérique/client. Cet ensemble d'étiquettes offre une flexibilité dans la gestion des paramètres de connectivité réseau/service du client ainsi que des contrôles d'activation des fonctionnalités.

Cet ensemble de balises personnalisé est mis à disposition par un administrateur système via l'option *Système → Ressources → Ensembles de balises de gestion des périphériques*. L'administrateur doit ajouter de nouveaux ensembles de balises :

- Mobile : Tags_Connexion
- Tablette : Tags_ConnectTablet
- Bureau : Balises_BroadTouch

Créez chaque tag individuel et définissez sa valeur. Les références des sections fournissent des descriptions détaillées pour chaque étiquette. Les balises personnalisées sont séparées en groupes en fonction de la fonctionnalité et sont abordées plus loin dans ce document.

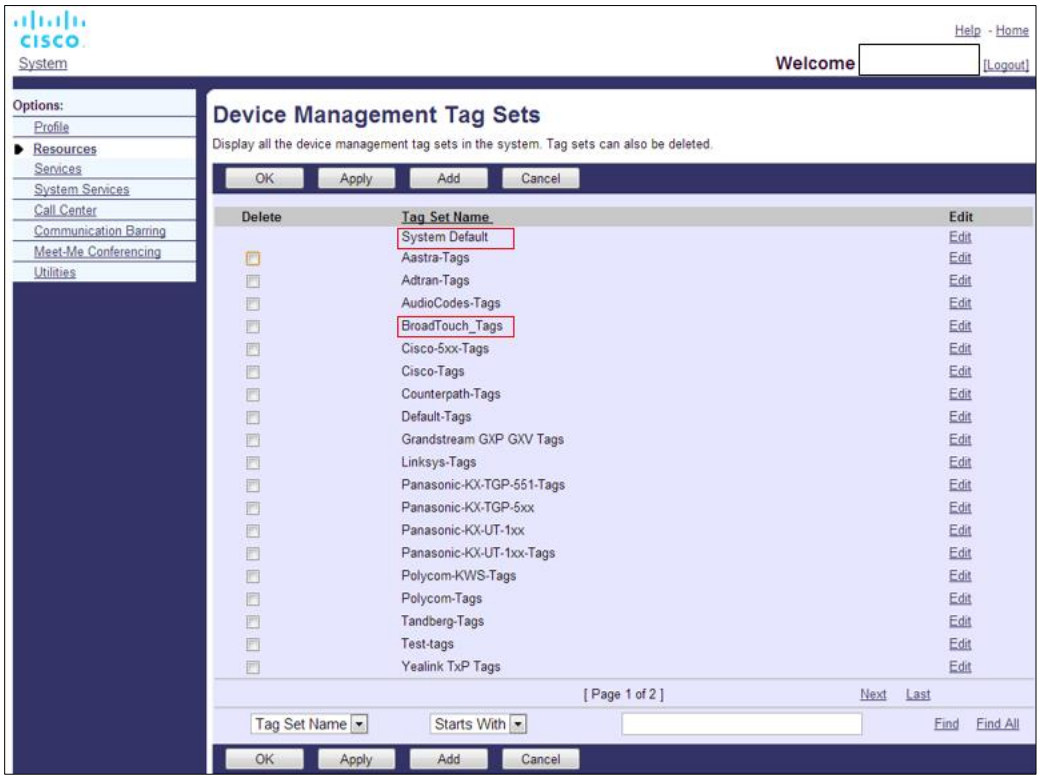


Figure 1 Ensembles d'étiquettes de gestion des périphériques de bureau

Confidentiel à Cisco

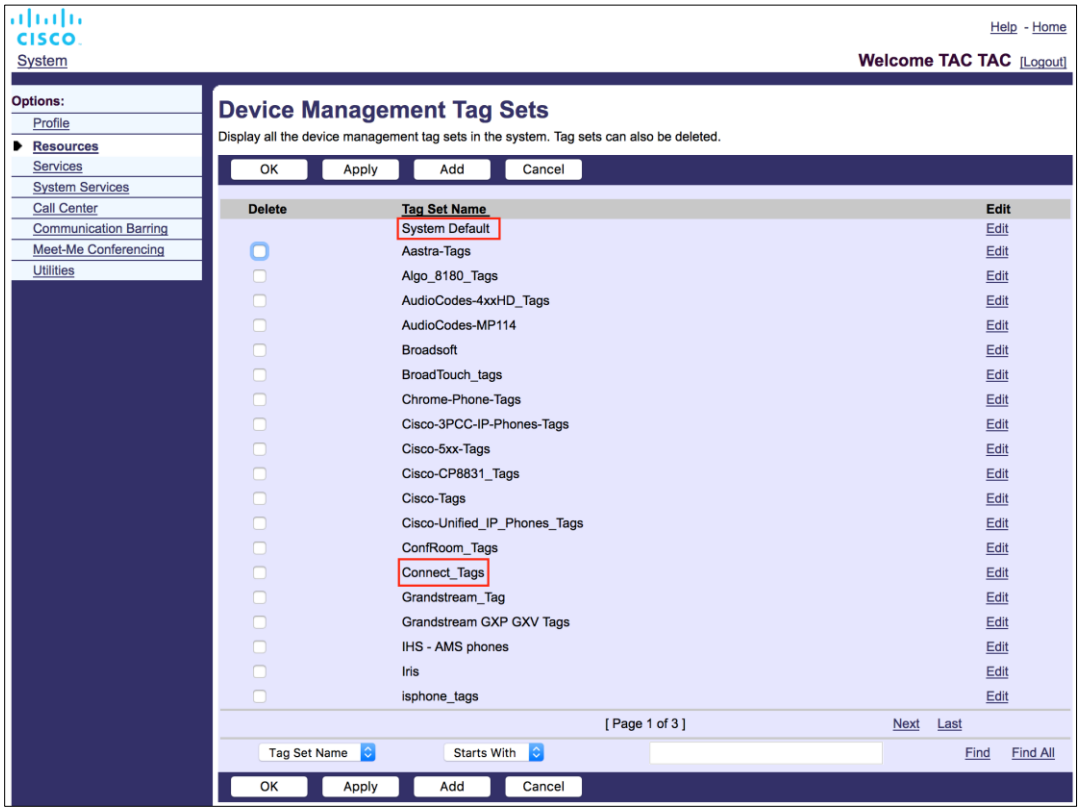


Figure 2 Ensembles d'étiquettes de gestion des périphériques mobiles

5.2 Améliorations de correspondance partielle pour la sélection du type de périphérique

Pour permettre une flexibilité accrue lors de la sélection de packs de fonctionnalités pour des groupes d'utilisateurs ou des utilisateurs individuels, le type de profil de périphérique est sélectionné en fonction d'une (première) correspondance partielle. Cela permet aux clients d'utiliser différents types de périphériques.

La procédure générale de gestion des périphériques spécifie que le serveur d'application Cisco BroadWorks fournit un type de profil de périphérique. Il est nommé « Business Communicator – PC » pour ordinateur de bureau, « Connect - Mobile » pour mobile et « Connect – Tablet » pour tablette. Un profil de périphérique peut être créé et attribué à l'utilisateur. Le serveur d'applications crée ensuite un fichier de configuration et le stocke sur le serveur de profils.

Lors de la connexion, le client interroge la liste des périphériques attribués via Xsi et recherche le profil de type de périphérique correspondant. Le client choisit le premier profil qui commence par le nom du type de périphérique correspondant. Ensuite, les données de configuration du profil du périphérique (fichier de configuration) associées à ce profil de périphérique sont utilisées pour activer et désactiver diverses fonctionnalités.

Cela permet d'utiliser le même exécutable client avec différents types de profils de périphériques, de sorte que le fournisseur de services peut changer les paquets de fonctionnalités pour des utilisateurs individuels ou des groupes d'utilisateurs en modifiant simplement le type de profil de périphérique dans le DM pour un utilisateur ou un groupe d'utilisateurs.

Confidentiel à Cisco

Par exemple, le fournisseur de services peut avoir un certain nombre de types de profils de périphériques en fonction des rôles d'utilisateur, tels que « Business Communicator – PC Basic », « Business Communicator – PC Executive » ou « Business Communicator – PC Assistant » et modifier la fonctionnalité disponible pour les utilisateurs individuels en changeant le type de profil de périphérique pour eux.

Notez qu'il n'est pas prévu qu'il ait plusieurs types de profil de périphérique correspondants dans la liste des périphériques reçus XML, mais un seul.

5.3 Configuration du client

La version Webex pour Cisco BroadWorks du client utilise le fichier *config-wxt.xml* pour configurer sa fonctionnalité d'appel. Il existe une procédure de configuration distincte pour Webex qui n'est pas couverte dans ce document.

5.4 Déploiement de config-wxt.xml

Ajoutez le fichier *config-wxt.xml* correspondant aux profils des périphériques « Connect – Mobile », « Connect – Tablet » et « Business Communicator – PC ». Webex pour Cisco BroadWorks utilise les mêmes profils de périphérique que UC-One afin de faciliter le déploiement.

> **NOTE 1** : Un fichier de configuration doit exister pour chaque profil de périphérique.
>
> **NOTE 2** : Il est VIVEMENT RECOMMANDÉ de tenir les modèles à jour avec la dernière version de l'application Webex

5.5 Fichier de configuration (config-wxt.xml)

De nouvelles balises personnalisées, avec le suffixe _**WXT**, sont utilisées pour différencier le nouveau déploiement de la configuration Webex pour Cisco BroadWorks des clients existants. Cependant, certaines balises (système) sont toujours partagées entre UC-One et Webex.

Certaines des balises personnalisées du système Cisco BroadWorks sont également utilisées dans le fichier de configuration *config-wxt.xml*. Pour plus d'informations sur chacune des balises suivantes, reportez-vous à la section*5.7Balises système intégré Cisco* BroadWorks Dynamic.

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

Confidentiel à Cisco

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

5.6 Balises par défaut système

En tant qu'administrateur système, vous pouvez accéder aux balises par défaut du système via l'option *Système → Ressources → Ensembles de balises de gestion des périphériques*. Les balises système par défaut suivantes doivent être mises à disposition lorsque le pack d'appel VoIP est installé.

Balise	Description
%SBC_ADDRESS_WXT%	Ceci doit être configuré comme le nom de domaine complet (FDQN) ou l'adresse IP du contrôleur de limites de session (SBC) déployé sur le réseau. Exemple : sbc.yourdomain.com
%SBC_PORT_WXT%	Si SBC_ADDRESS_WXTest une adresse IP, ce paramètre doit être défini sur le port SBC. Si SBC_ADDRESS_WXT est un nom de domaine complet (FQDN), alors il peut être laissé non défini. Exemple : 5075

5.7 Balises système intégré Cisco BroadWorks Dynamic

Outre les balises système par défaut et les balises personnalisées qui doivent être définies, il existe des balises système Cisco BroadWorks existantes qui sont généralement utilisées et font partie du fichier d'archivage des types de périphériques (DTAF) recommandé. Ces balises sont répertoriées dans cette section. En fonction du pack de solution installé, toutes les balises système ne sont pas utilisées.

Balise	Description
%BWNETWORK-CONFERENCE-SIPURI-n%	Ceci est l'URI du serveur utilisé pour activer la conférence N-Way.
%BWVOICE-PORTAL-NUMBER-n%	Ce numéro est utilisé pour la messagerie vocale. Le client compose ce numéro lors de la récupération de la messagerie vocale.

Confidentiel à Cisco

Balise	Description
%BWLINEPORT-n%	Nom d'utilisateur SIP utilisé dans la signalisation SIP, par exemple, dans l'enregistrement.
%BWHOST-n%	Il s'agit de la partie de domaine du port de ligne mis à disposition pour le périphérique affecté à l'utilisateur. Il est récupéré à partir du profil de l'utilisateur. Généralement utilisé comme domaine SIP.
%BWAUTHUSER-n%	Il s'agit du nom d'utilisateur d'authentification. Si l'authentification a été attribuée à l'abonné, il s'agit de l'ID utilisateur provisionné sur la page d'authentification quel que soit le mode d'authentification sélectionné du type de périphérique. Le nom d'utilisateur SIP, généralement utilisé dans la signalisation 401 et 407. Peut être différent du nom d'utilisateur SIP par défaut.
%BWAUTHPASSWORD-n%	Il s'agit du mot de passe d'authentification de l'utilisateur. Si l'authentification a été attribuée à l'abonné, il s'agit du mot de passe provisionné sur la page Authentification quelle que soit la valeur du mode d'authentification sélectionné du type de périphérique. Le mot de passe SIP utilisé dans la signalisation SIP.
%BWE164-n%	Cette balise fournit le numéro de téléphone de l'utilisateur au format international.
%BWNAME-n%	Il s'agit du prénom et du nom de l'abonné dans le profil de l'utilisateur. Les noms et prénoms sont concaténés ensemble. En cas de configuration multi-lignes, si aucune étiquette de ligne n'est configurée et si elle n'est pas vide, utilisée comme nom d'affichage de la ligne dans le sélecteur de ligne.
%BWEXTENSION-n%	Le poste de l'abonné est récupéré à partir du poste provisionné dans le profil de l'utilisateur. Si un numéro de poste n'a pas été fourni, la balise est remplacée par le numéro de téléphone (DN) de l'abonné.
%BWAPPEARANCE-LABEL-n%	Il s'agit du libellé de la ligne configuré. Utilisé comme nom de ligne, s'il n'est pas vide.
%BWDISPLAYNAMELINEPORT%	Il s'agit de la ligne/port de la première ligne privée, par opposition à une ligne partagée (apparence d'appel partagé). Il s'agit du port de ligne mis à disposition sur le périphérique affecté à l'utilisateur. Ceci est récupéré à partir du profil de l'utilisateur. Utilisé pour identifier la ligne principale de l'utilisateur.
%BWLINEPORT-PRIMARY%	Le port de la ligne principale est mis à disposition sur le périphérique qui est affecté à l'utilisateur. Cette balise n'inclut pas la partie du domaine du port de ligne mis à disposition. Il est récupéré à partir du profil de l'utilisateur.

Confidentiel à Cisco

Balise	Description
%BWE911-PRIMARY-HELDURL%	Indique l'URL de la plateforme de localisation d'urgence RedSky prenant en charge le protocole HELD.
%BWE911-CUSTOMERID%	L'ID du client (HeldOrgId, CompanyID) utilisé pour la demande HTTPS RedSky.
%BWE911-SECRETKEY%	Le secret pour authentifier la demande HTTPS RedSky.
%BWE911-EMERGENCY-NUMBER-LIST%	La liste des numéros d'urgence pris en charge par RedSky. Pour utiliser cette balise, la balise personnalisée %RESERVEDBW911-EMERGENCY-NUMBER-LIST% réservée doit être ajoutée à l'ensemble de balise utilisé par le type de périphérique. La balise « réservé » doit contenir les numéros d'urgence définis sur BroadWorks sous AS_CLI/System/CallP/CallTypes > dans un format séparé par des virgules tel que 911, 0911, 933. **REMARQUE :** Le client Webex ne prend pas en charge les caractères génériques dans les numéros d'urgence ; par conséquent, seuls les numéros d'urgence exacts doivent être ajoutés à la balise personnalisée « réservée ». L'exemple suivant montre comment la fonctionnalité de balise réservée est destinée à être utilisée : 1) La balise native %BWE911-EMERGENCY-NUMBER-LIST% est ajoutée au fichier modèle du périphérique 2) La balise personnalisée réservée %RESERVEDBW911-EMERGENCY-NUMBER-LIST% est ajoutée à l'ensemble de balise utilisé par le périphérique avec la valeur 911, 0911, 933 3) Lorsque le fichier est reconstruit, la balise native %RESERVEDBW911-EMERGENCY-NUMBER-LIST% est résolue à 911, 0911, 933
%BW-MEMBERTYPE-n%	Il s'agit du type de chaque ligne. Il peut s'agir de « Profil virtuel », « Utilisateur » ou « Emplacement ».
%BWUSEREXTID-n%	Il s'agit de l'ID externe de la ligne donnée (Webex Calling uniquement)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Fournit des informations si un groupe d'interception d'appels est configuré sur la ligne correspondante. (Webex calling uniquement)

Confidentiel à Cisco

6 Balises personnalisées

Cette section décrit les balises personnalisées utilisées dans Webex pour Cisco BroadWorks. Il répertorie toutes les balises personnalisées utilisées pour les plateformes de bureau et mobiles/tablettes.

Notez toutefois que certains paramètres décrits dans cette section ne sont pris en charge que pour la version spécifique du client. Pour déterminer si un paramètre ne s'applique pas à une ancienne version du client, consultez le guide de configuration spécifique à la version appropriée.

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_REJECT_WITH_486_WXT%	O	O	vrai	*6.1.16 Comportement de rejet d'appel* entrant
%REJECT_WITH_XSI_MODE_WXT%	N	O	refuser_faux	*6.3.2 Notifications push pour les* appels
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	O	occupé	*6.3.2 Notifications push pour les* appels
%ENABLE_TRANSFER_CALLS_WXT%	O	O	false (faux)	*6.1.20 Transférer*
%ENABLE_CONFERENCE_CALLS_WXT%	O	O	false (faux)	*6.1.21 Conférences téléphoniques à N-Way et* participants
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	O	O	false (faux)	*6.1.21 Conférences téléphoniques à N-Way et* participants
%MAX_CONF_PARTIES_WXT%	O	O	10	*6.1.21 Conférences téléphoniques à N-Way et* participants
%ENABLE_CALL_STATISTICS_WXT%	O	O	false (faux)	*6.1.24 Stat.* appels
%ENABLE_CALL_PULL_WXT%	O	O	false (faux)	*6.1.22 Call Pull* (Transfert d'appel)
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	O	false (faux)	*6.3.2 Notifications push pour les* appels
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	O	O	false (faux)	*6.1.28 Transcription de la messagerie vocale* pour Webex Calling
%ENABLE_MWI_WXT%	O	O	false (faux)	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente
%MWI_MODE_WXT%	O	O	vide	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_VOICE_MAIL_WXT%	O	O	false (faux)	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente
%ENABLE_VISUAL_VOICE_MAIL_WXT%	O	O	false (faux)	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente
%ENABLE_FORCED_LOGOUT_WXT%	O	N	false (faux)	*6.2.1 Déconnexion* forcée
%FORCED_LOGOUT_APPID_WXT%	O	N	vide	*6.2.1 Déconnexion* forcée
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	O	O	false (faux)	*6.1.29.1 Renvoi d'appel* Toujours
%ENABLE_BROADWORKS_ANYWHERE_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	O	O	vrai	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	O	O	false (faux)	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_EMERGENCY_DIALING_WXT%	N	O	false (faux)	*6.3.1 Appels d'urgence*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	O	911,112	*6.3.1 Appels d'urgence*
%ENABLE_USE_RPORT_WXT%	O	O	false (faux)	*6.1.14 Gestion du port SIP pour la* traversée NAT
%RPORT_USE_LOCAL_PORT_WXT%	O	O	false (faux)	*6.1.14 Gestion du port SIP pour la* traversée NAT
%USE_TLS_WXT%	O	O	false (faux)	*6.1.2 SIP sur TLS et protocole de transport sécurisé* en temps réel
%SBC_ADDRESS_WXT%	O	O	vide	*5.6 Balises par défaut* système
%SBC_PORT_WXT%	O	O	5060	*5.6 Balises par défaut* système
%USE_PROXY_DISCOVERY_WXT%	O	O	false (faux)	*6.1.6 Découverte dynamique du proxy* SIP
%USE_TCP_FROM_DNS_WXT%	O	O	vrai	*6.1.6 Découverte dynamique du proxy* SIP
%USE_UDP_FROM_DNS_WXT%	O	O	vrai	*6.1.6 Découverte dynamique du proxy* SIP
%USE_TLS_FROM_DNS_WXT%	O	O	vrai	*6.1.6 Découverte dynamique du proxy* SIP
%DOMAIN_OVERRIDE_WXT%	O	O	vide	*6.1.6 Découverte dynamique du proxy* SIP
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	O	O	vrai	*6.1.6 Découverte dynamique du proxy* SIP
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	O	O	vrai	*6.1.6 Découverte dynamique du proxy* SIP

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	O (Windows uniquement)	N	false (faux)	*6.1.6 Découverte dynamique du proxy* SIP
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	O	O	5000	*6.1.5 Délai d'expiration configurable pour l'ouverture du* socket SIP
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	O	O	10 000	*6.1.5 Délai d'expiration configurable pour l'ouverture du* socket SIP
%SOURCE_PORT_WXT%	O	O	5060	*6.1.7 Utilisation du port préféré* pour SIP
%SIP_FAILBACK_ENABLED_WXT%	O	N	vrai	*6.1.8.2 Restauration SIP*
%SIP_FAILBACK_TIMEOUT_WXT%	O	N	900	*6.1.8.2 Restauration SIP*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	O	N	false (faux)	*6.1.8.2 Restauration SIP*
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	O	O	dns	*6.1.8.3. Appliquer la version* IP
%USE_ALTERNATIVE_IDENTITIES_WXT%	O	O	false (faux)	*6.1.10 Utiliser les URI P-Associated* dans REGISTER
%TCP_SIZE_THRESHOLD_WXT%	O	O	18000	*6.1.4 Forcer l'utilisation de TCP, TLS ou UDP et* Keepalives
%SIP_REFRESH_ON_TTL_WXT%	O	N	false (faux)	*6.1.8.4 Gestion du TTL* DNS
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	O	O	false (faux)	*6.1.12 Prise en charge* de la MISE À JOUR SIP
%ENABLE_PEM_SUPPORT_WXT%	O	O	false (faux)	*6.1.11 En-tête SIP P-Early Media (PEM)*
%ENABLE_SIP_SESSION_ID_WXT%	O	O	false (faux)	*6.1.15 ID de session* SIP
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	O	O	false (faux)	*6.1.13 Ancien SIP INFO FIR*
%SRTP_ENABLED_WXT%	O	O	false (faux)	*6.1.2 SIP sur TLS et protocole de transport sécurisé* en temps réel

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%SRTP_MODE_WXT%	O	O	false (faux)	*6.1.2 SIP sur TLS et protocole de transport sécurisé* en temps réel
%ENABLE_REKEYING_WXT%	O	O	vrai	*6.1.2 SIP sur TLS et protocole de transport sécurisé* en temps réel
%RTP_AUDIO_PORT_RANGE_START_WXT%	O	O	8000	*6.1.17 Plage de ports de protocole* de transport en temps réel
%RTP_AUDIO_PORT_RANGE_END_WXT%	O	O	8099	*6.1.17 Plage de ports de protocole* de transport en temps réel
%RTP_VIDEO_PORT_RANGE_START_WXT%	O	O	8100	*6.1.17 Plage de ports de protocole* de transport en temps réel
%RTP_VIDEO_PORT_RANGE_END_WXT%	O	O	8199	*6.1.17 Plage de ports de protocole* de transport en temps réel
%ENABLE_RTCP_MUX_WXT%	O	O	vrai	*6.1.19 MUX RTCP*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	O	O	vrai	*6.1.33 Canal d'événement XSI*
%CHANNEL_HEARTBEAT_WXT%	O	O	10 000	*6.1.33 Canal d'événement XSI*
%XSI_ROOT_WXT%	O	O	vide (utilise l'URL d'origine)	*6.1.32 Racine et chemins XSI*
%XSI_ACTIONS_PATH_WXT%	O	O	/com.broadsoft.xsi-actions/	*6.1.32 Racine et chemins XSI*
%XSI_EVENTS_PATH_WXT%	O	O	/com.broadsoft.xsi-events/	*6.1.32 Racine et chemins XSI*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	O	O	false (faux)	*6.1.25 Récupération automatique des appels / Transfert d'appel* fluide
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	O	uniquement cs	*6.3.1 Appels d'urgence*
%ENABLE_CALL_PICKUP_BLIND_WXT%	O	N	false (faux)	*6.2.2 Prise d'appel*

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	O	N	false (faux)	*6.2.2 Prise d'appel*
%WEB_CALL_SETTINGS_URL_WXT%	O	O	vide	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%USER_PORTAL_SETTINGS_URL_WXT%	O	O	vide	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%ENABLE_CALL_CENTER_WXT%	O	O	false (faux)	*6.1.31 Connexion/déconnexion du centre d'appels/de* la file d'attente d'appels
%WEB_CALL_SETTINGS_TARGET_WXT%	O	O	extérieur	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	O	O	vrai	*6.1.30 Portail des paramètres et paramètres d'appel* basés sur le Web
%USE_MEDIASEC_WXT%	O	O	false (faux)	*6.1.3 En-têtes SIP 3GPP pour SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	O	false (faux)	*6.3.4 Cliquer pour composer (Rappel)*
%DIALING_CALL_BACK_TIMER_WXT%	N	O	10	*6.3.4 Cliquer pour composer (Rappel)*
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	O	N	false (faux)	*6.2.3 Prise en charge Boss-Admin* (Cadre de direction-Assistant)
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	O	35	*6.3.2 Notifications push pour les* appels
%ENABLE_CALL_RECORDING_WXT%	O	O	false (faux)	*6.1.26 Enregistrement des* appels
%ENABLE_SINGLE_ALERTING_WXT%	N	O	false (faux)	*6.3.3 Alerte unique*
%ENABLE_CALL_PARK_WXT%	O	O	false (faux)	*6.1.23 Parcage/Récupération d'appels*
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	O	O	10	*6.1.23 Parcage/Récupération d'appels*

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_RTP_ICE_WXT%	O	O	false (faux)	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%RTP_ICE_MODE_WXT%	O	O	ictère	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%RTP_ICE_SERVICE_URI_WXT%	O	O	vide	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%RTP_ICE_PORT_WXT%	O	O	3478	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%ENABLE_RTP_ICE_IPV6_WXT%	O	O	false (faux)	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	O	N	false (faux)	*6.1.8.4 Gestion du TTL* DNS
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	O	N	false (faux)	*6.2.4 Transférer les appels SIP vers* une réunion
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	O	N	false (faux)	*6.2.5 Appel de contrôle du téléphone de bureau* – Réponse automatique
%ENABLE_DIALING_VOIP_WXT%	N	O	vrai	*6.3.5 Prise en* charge du MNO *Appel avec numéroteur natif*
%ENABLE_DIALING_NATIVE_WXT%	N	O	false (faux)	*6.3.5 Prise en* charge du MNO *Appel avec numéroteur natif*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	O	O	vrai	*6.1.35 Numérotation SIP-URI*
%ENABLE_SIP_VIDEOCALLS_WXT%	O	O	vrai	*6.1.37 Désactiver les appels* vidéo
%ENABLE_LOCUS_VIDEOCALLS_WXT%	O	O	vrai	*6.1.37 Désactiver les appels* vidéo
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	O	O	Bureau - vrai Mobile, Tablette - faux	*6.1.37 Désactiver les appels* vidéo
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	O	O	false (faux)	*6.1.38 Appels d'urgence (911) - Création de rapports de* localisation avec le fournisseur E911

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	O	O	0	*6.1.38 Appels d'urgence (911) - Création de rapports de* localisation avec le fournisseur E911
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	O	O	-1	*6.1.38 Appels d'urgence (911) - Création de rapports de* localisation avec le fournisseur E911
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	O	O	once_par_connexion	*6.1.38 Appels d'urgence (911) - Création de rapports de* localisation avec le fournisseur E911
%ENABLE_AUTO_ANSWER_WXT%	O	N	false (faux)	*6.2.6 Réponse automatique avec notification de* tonalité
%ENABLE_CALLS_SPAM_INDICATION_WXT%	O	O	false (faux)	*6.1.41 Indication d'appel de* spam
%ENABLE_NOISE_REMOVAL_WXT%	O	O	false (faux)	*6.1.42 Suppression du bruit et extension de la bande passante* pour les appels RTCP/mobiles
%ENABLE_AUDIO_MARI_FEC_WXT%	O	O	false (faux)	*6.1.46.2 Correction d'erreur directe (FEC) et retransmission de paquets* (RTX)
%ENABLE_AUDIO_MARI_RTX_WXT%	O	O	false (faux)	*6.1.46.2 Correction d'erreur directe (FEC) et retransmission de paquets* (RTX)
%ENABLE_VIDEO_MARI_FEC_WXT%	O	O	false (faux)	*6.1.46.2 Correction d'erreur directe (FEC) et retransmission de paquets* (RTX)
%ENABLE_VIDEO_MARI_RTX_WXT%	O	O	false (faux)	*6.1.46.2 Correction d'erreur directe (FEC) et retransmission de paquets* (RTX)
%ENABLE_CALL_BLOCK_WXT%	O	O	false (faux)	*6.1.45 Liste de blocage (Webex Calling* uniquement)
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	O	vrai	*6.3.5.6 MNO Mobility - Widget en* cours d'appel
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	O	vrai	*6.3.5.6 MNO Mobility - Widget en* cours d'appel
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	O	vrai	*6.3.5.6 MNO Mobility - Widget en* cours d'appel

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	O	O	false (faux)	*6.1.47 Appels simultanés avec le même* utilisateur
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	O	N	false (faux)	*6.2.14 Pack d'événements de contrôle de coupure du* son à distance (Webex Calling uniquement)
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	O	O	vrai	*6.1.29.2 Transfert d'appel vers* la messagerie vocale
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	O	O	vrai	*6.1.8.1 Basculement SIP*
%ENABLE_CALL_MOVE_HERE_WXT%	O	N	false (faux)	*6.2.15 Déplacer l'appel*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	O	O	false (faux)	*6.1.42 Suppression du bruit et extension de la bande passante* pour les appels RTCP/mobiles
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	O	vide	*6.3.5.1 Appel avec numéroteur natif*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	O	O	false (faux)	*6.1.20 Transférer*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	O	O	vrai	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	O	false (faux)	*6.3.6 ID de l*'appelant entrant
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	O	false (faux)	*6.3.6 ID de l*'appelant entrant
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	O	false (faux)	*6.1.50 ID de* l'appelant *ID de l'appelant sortant* (Webex Calling uniquement)
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	O	false (faux)	*6.1.50 ID de* l'appelant *ID de l'appelant sortant* (Webex Calling uniquement)

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	O	false (faux)	*6.1.50 ID de* l'appelant *ID de l'appelant sortant* (Webex Calling uniquement)
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	O	false (faux)	*6.1.50 ID de* l'appelant *ID de l'appelant sortant* (Webex Calling uniquement)
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	O	false (faux)	*6.1.50 ID de* l'appelant *ID de l'appelant sortant* (Webex Calling uniquement)
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	O	O	false (faux)	*6.1.49 Informations sur le* transfert d'appel
%ENABLE_BUSY_LAMP_FIELD_WXT%	O	N	false (faux)	*6.2.8.1 Voyant d'occupation de* ligne (BLF)
%ENABLE_BLF_DISPLAY_CALLER_WXT%	O	N	vrai	*6.2.8.1 Voyant d'occupation de* ligne (BLF)
%BLF_NOTIFICATION_DELAY_TIME_WXT%	O	N	0	*6.2.8.1 Voyant d'occupation de* ligne (BLF)
%ENABLE_GCP_NOTIFICATIONS_WXT%	O	N	false (faux)	*6.2.8.2 Groupe d'interception d'appels (Webex* Calling uniquement)
%ENABLE_GCP_DISPLAY_CALLER_WXT%	O	N	false (faux)	*6.2.8.2 Groupe d'interception d'appels (Webex* Calling uniquement)
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	O	N	120	*6.2.8.2 Groupe d'interception d'appels (Webex* Calling uniquement)
%UDP_KEEPALIVE_ENABLED_WXT%	O	O	vrai	*6.1.4 Forcer l'utilisation de TCP, TLS ou UDP et* Keepalives
%TCP_KEEPALIVE_ENABLED_WXT%	O	O	false (faux)	*6.1.4 Forcer l'utilisation de TCP, TLS ou UDP et* Keepalives
%TLS_KEEPALIVE_ENABLED_WXT%	O	O	false (faux)	*6.1.4 Forcer l'utilisation de TCP, TLS ou UDP et* Keepalives
%ENABLE_MULTI_LINE_WXT%	O	N	false (faux)	*6.2.12 Multiligne - Apparence de* ligne partagée
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	O	false (faux)	*6.2.4 Transférer les appels SIP vers une réunion (Webex Calling)*

Confidentiel à Cisco

Balise	Utilisé dans le bureau	Utilisé sur mobile/tablette	Valeur par défaut	Section
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	O	false (faux)	*6.3.5.3 Identité de la ligne d'appel sortante (CLID)* – Double personnalité
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	O	false (faux)	*6.3.5.3 Identité de la ligne d'appel sortante (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	O	O	résolu(s)	*6.1.50.2 Nom de l'ID de* l'appelant distant

Pour plus d'informations sur le mappage des balises personnalisées utilisées dans Webex pour Cisco BroadWorks avec celles utilisées par UC-One, reportez-vous à la section *8Mappage des balises personnalisées entre Webex pour Cisco BroadWorks et* UC-One.

Confidentiel à Cisco

6.1 Caractéristiques communes

6.1.1 Paramètres du serveur SIP

Le client est généralement configuré pour utiliser un réseau SIP, ce qui se fait en modifiant le fichier *config-wxt.xml*. En règle générale, les paramètres suivants doivent être modifiés :

- Domaine SIP. Ceci est utilisé comme partie du domaine de son propre URI SIP (son propre URI SIP est également parfois appelé port de ligne) en général dans les en-têtes SIP et dans les appels distants (XSI). La partie utilisateur de son propre URI SIP provient de la configuration des identifiants SIP (paramètre <username> sous <credentials>).
- URI du serveur SIP ou adresse IP du serveur proxy SIP si la résolution DNS doit échouer. Notez que pour utiliser TLS, les adresses IP ne peuvent pas être utilisées dans le paramètre proxy car la validation du certificat TLS échouera. Pour plus d'informations sur le port proxy, voir la balise DM %SOURCE_PORT_WXT%. Notez que la fonction de gestion DNS TTL ne peut pas être utilisée lorsqu'une adresse IP est utilisée dans le paramètre d'adresse proxy. En général, il n'est pas recommandé d'utiliser une adresse IP dans ce champ pour ces raisons.

D'autres paramètres peuvent également être modifiés pour activer diverses fonctionnalités d'appel. Cependant, les paramètres précédents activent les fonctionnalités de base pour les éléments suivants :

- Enregistrement sur le réseau SIP.
- Passer des appels audio ou vidéo.
- Exécution de la détection de proxy basée sur DNS, qui permet d'utiliser plusieurs proxys.

Une fois l'enregistrement SIP activé, l'activation de SIP SUBSCRIBE pour MWI doit être effectuée via des paramètres de configuration distincts. Pour plus d'informations sur la messagerie vocale, reportez-vous à la section*6.1.27Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente.

Notez que la configuration SIP de base est toujours nécessaire pour MWI même lorsque les appels SIP sont désactivés. MWI s'appuie sur les SIP NOTIFYs.

La configuration des serveurs SIP suit ce schéma de base :

- L'adresse proxy contient l'URI du serveur SIP.
- Un seul proxy peut être défini.
- La détection de proxy DNS prend en charge de nombreux proxys, qui nécessitent la configuration correcte du DNS.

De plus, les minuteurs SIP sont exposés dans le fichier de configuration (il n'est pas recommandé de les modifier).

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


Confidentiel à Cisco

```
    </timers>
```

- T1 – la durée, en millisecondes, d'un délai aller-retour réseau.
- T2 – la durée maximale, en millisecondes, avant de retransmettre les demandes non invitées et les réponses invitées.
- T4 – la durée maximale, en millisecondes, pour qu'un message reste dans le réseau.

Chaque ligne a ses propres paramètres tels que le numéro de messagerie vocale, l'URI de conférence et le domaine, ainsi que les informations d'authentification SIP. Des informations d'authentification séparées peuvent être configurées pour la signalisation 401 et 407 si nécessaire.

L'exemple et le tableau suivants fournissent des informations sur les balises DM les plus typiques utilisées pour la configuration SIP.

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


Confidentiel à Cisco

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%BWLINEPORT-n%	vide	chaîne de caractères	Généralement le nom d'utilisateur SIP. Pour plus d'informations, reportez-vous à la section *5.7Balises système intégré Cisco BroadWorks Dynamic*. Exemple : jeûne
%BWAUTHPASSWORD-n%	vide	chaîne de caractères	Généralement mot de passe SIP. Pour plus d'informations, reportez-vous à la section *5.7Balises système intégré Cisco BroadWorks Dynamic*. Exemple : mot de passe secrète
%BWE164-n%	vide	numéro de téléphone	Numéro de téléphone par défaut de l'utilisateur au format international. Pour plus d'informations, reportez-vous à la section *5.7Balises système intégré Cisco BroadWorks Dynamic*. Exemple : 12345678
%SBC_ADDRESS_WXT%	vide	chaîne de caractères	Pour plus d'informations, reportez-vous à la section *5.6Balises par défaut* système. Exemple : sbcexample.domain.com
%SBC_PORT_WXT%	5060	numéro	Pour plus d'informations, reportez-vous à la section *5.6Balises par défaut* système. Exemple : 5060
%BWHOST-n%	vide	chaîne de caractères	Généralement utilisé comme domaine SIP. Pour plus d'informations, reportez-vous à la section *5.7Balises système intégré Cisco BroadWorks Dynamic*. Exemple : exampledomain.com
%SOURCE_PORT_WXT%	5060	numéro	Généralement utilisé pour le paramètre *port préféré*. Pour plus d'informations, reportez-vous à la section *6.1.7Utilisation du port préféré* pour SIP. Exemple : 5061
%BWUSEREXTID-n%	vide	chaîne de caractères	(Webex Calling uniquement) Contient l'ID externe de la ligne Pour plus d'informations, consultez *6.2.13Multi-lignes - Lignes virtuelles (Webex Calling uniquement)*. Exemple : 30f69bf7-710b-4cd0-ab4b-35ab393a1709

Confidentiel à Cisco

REMARQUE : Il est fortement conseillé que le port SIP soit différent de 5060 (par exemple, 5075) en raison de problèmes connus liés à l'utilisation du port SIP standard (5060) avec des périphériques mobiles.

6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel

Le client peut être configuré pour utiliser la signalisation SIP sur TLS et SRTP (Secure Real-time Transport Protocol) pour le chiffrement média. Cependant, ces fonctionnalités doivent être activées dans la configuration comme indiqué dans l'exemple suivant. Notez également que lorsque la détection de proxy SIP dynamique est utilisée, les priorités DNS SRV remplacent les paramètres statiques tels que celui-ci (%USE_TLS_WXT%), et le transport non-TLS est utilisé s'il a une priorité plus élevée dans DNS SRV. Pour plus d'informations sur la découverte dynamique de proxy SIP, reportez-vous à la section*6.1.6Découverte dynamique du proxy* SIP*.*

Lorsque la détection dynamique du proxy n'est pas utilisée, l'activation de TLS pour SIP l'utilise.

Pour plus de détails sur les recommandations de port SIP et de protocole de transport lorsque des ALG SIP sont utilisés sur le réseau, consultez le *Guide de la solution Webex pour Cisco BroadWorks*.

Notez que le certificat utilisé doit être valide. De plus, la chaîne de certificats doit être intacte afin que le certificat intermédiaire soit également lié. Il est recommandé d'utiliser un certificat largement utilisé afin qu'il soit déjà présent, par défaut, sur les périphériques. Il est également possible d'ajouter des certificats localement sur la machine de bureau manuellement ou en utilisant la mise à disposition en masse, bien que cela ne soit généralement pas fait.

Pour activer le protocole SRTP associé pour le chiffrement média, il existe un paramètre séparé.

En plus du protocole RTP, le trafic RTCP peut être sécurisé avec les mêmes mécanismes que le protocole RTP en utilisant la configuration précédente.

Pour les codes de chiffrement SIP/TLS, voir *Annexe A : Codes* de chiffrement TLS*.*

Le protocole SRTP est utilisé pour assurer la sécurité du flux média sous trois aspects différents :

- Confidentialité (données chiffrées)
- Authentification (assurance de l'identité du ou des autres parties)
- Intégrité (mesures contre, par exemple, les attaques de rejeu)

La version actuelle de l'infrastructure média prend en charge le mode compteur AES 128 pour la protection et le code d'authentification des messages de hachage (HMAC)-SHA-1 pour l'authentification. La taille de la clé principale est de 16 octets et le sel principal est de 14 octets.

Le cadre média prend en charge à la fois la balise d'authentification complète (80 bits) et courte (32 bits). Le client échange les clés à l'intérieur du SDP dans le cadre de la signalisation SIP, les deux côtés de l'appel envoient la clé qu'ils utilisent à l'autre côté.

Confidentiel à Cisco

SRTP peut être activé en utilisant la configuration illustrée dans l'exemple suivant. La mise en œuvre actuelle utilise uniquement le profil RTP sécurisé SDP et prend en charge le SDP multiligne pour les entrées Profil Audio Visuel (AVP) et Profil Audio Visuel Sécurisé (SAVP). La mise en œuvre de SRTP a été testée avec succès dans sa configuration de déploiement habituelle avec différents SBC. Le test d'interopérabilité (IOT) avec des terminaux qui prennent uniquement en charge le chiffrement à l'aide du profil AVP n'est pas pris en charge.

Les procédures SDP multilignes liées à SRTP sont mises en œuvre, de sorte que plusieurs lignes m sont toujours utilisées. Des m-lines séparées pour AVP et SAVP sont utilisées.

Remarque, cependant, une attention particulière doit être accordée à la configuration SBC ; en particulier, en veillant à ce que la ligne « m= » entrante, associée à RTP/SAVP dans le SDP, ne soit pas supprimée car dans certains cas, les appels SRTP peuvent être bloqués.

Plusieurs configurations réseau différentes sont cependant possibles, dans certains déploiements le SBC n'est pas impliqué dans le trafic média tandis que dans d'autres déploiements, chaque branche média RTP client vers le SBC est chiffrée séparément et négociée via le SBC. Dans certains déploiements, le SBC n'autorise pas plusieurs lignes SDP.

Le SBC peut également modifier l'ordre des m-lignes SDP lors de la configuration de l'appel, en plaçant la m-ligne AVP (non chiffrée) ou SAVP (chiffrée) en premier. Par conséquent, les clients qui sélectionnent la première ligne m de travail sont amenés à préférer le trafic chiffré ou non chiffré. Les différentes options de configuration SRTP sont les suivantes :

- Obligatoire – Lors de la configuration de l'appel, le SDP initial n'inclut que la ligne m SAVP lors de l'offre et le client n'accepte que la ligne m SAVP dans le SDP lors de la réponse. Par conséquent, seuls les appels SRTP sont possibles.
- Préféré – Lors de la configuration de l'appel, le SDP initial inclut à la fois les lignes m AVP et SAVP, mais SAVP est le premier lors de l'offre, indiquant l'ordre de préférence. Lors de la réponse, le client sélectionne SAVP s'il est disponible même s'il ne s'agit pas de la première ligne m (conformément aux spécifications SIP, l'ordre des lignes m n'est pas modifié lors de la réponse).
- Facultatif – Lors de la configuration de l'appel, le SDP initial inclut à la fois les lignes m SAVP et AVP lors de l'offre, mais AVP indique d'abord l'ordre de préférence. Lors de la réponse, le client sélectionne la première ligne m, AVP ou SAVP.
- SRTP non activé – Il n'y a pas de ligne m SAVP dans le SDP initial lors de l'offre. Lors de la réponse, le protocole SAVP n'est pas accepté, donc seuls les appels RTP sont possibles.
- Transport – Sélectionnez automatiquement le mode SRTP en fonction du protocole de transport. Si TLS est utilisé, le mode SRTP obligatoire est activé. Si TCP ou UDP est utilisé, aucun SRTP n'est utilisé.

SRTP versus RTP est symétrique dans les deux sens de l'appel, c'est-à-dire que les profils d'envoi et de réception sont identiques.

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

```
<config>
<protocols><rtp>
```


Confidentiel à Cisco

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

Le protocole de contrôle en temps réel sécurisé (SRTCP) est également utilisé si SRTP est activé.

Dans certains déploiements, la re-saisie pour SRTP n'est pas prise en charge. Par conséquent, il existe un paramètre de configuration pour activer/désactiver la re-clé SRTP. Cependant, les nouvelles clés sont toujours utilisées lorsqu'elles sont reçues dans un SDP mis à jour conformément à rfc3264. La configurabilité ne concerne que l'envoi de nouvelles clés.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USE_TLS_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « faux », SIP TLS est désactivé. Lorsque ce paramètre est défini sur « vrai », SIP TLS est activé. Veuillez noter que si *6.1.6Découverte dynamique du proxy* SIP est utilisé, ce paramètre est ignoré.
%SRTP_ENABLED_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « faux », SRTP est désactivé. Lorsque ce paramètre est défini sur « vrai », SRTP est activé.
%SRTP_MODE_WXT%	facultatif	obligatoire, préféré, optionnel, transport	Définit comment SRTP préféré est lors de la configuration de l'appel. La valeur par défaut est « facultatif ».
%ENABLE_REKEYING_WXT%	vrai	vrai, faux	Active la ré-encodage SIP (SDP) pour SRTP.

REMARQUE : Si la prise en charge ICE est activée (voir *6.1.18Prise en charge ICE (*Webex Calling uniquement)), une nouvelle saisie sera toujours effectuée (la valeur %ENABLE_REKEYING_WXT% de la configuration est ignorée).

6.1.3 En-têtes SIP 3GPP pour SRTP

Les nouvelles spécifications 3GPP nécessitent des en-têtes SIP supplémentaires pour utiliser le protocole SRTP (Secure Real-time Transport Protocol). Pour plus d'informations, voir *3GPP TS 24.229* ainsi que :

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

Les en-têtes requis par cette spécification peuvent interrompre l'appel SIP dans les déploiements où cette spécification n'est pas utilisée. Par conséquent, il est recommandé d'utiliser ces en-têtes uniquement dans les environnements où le côté serveur les prend en charge.

Seule l'activation de l'utilisation des en-têtes est configurable. Aucune autre configuration n'existe pour les en-têtes individuels. Tous les en-têtes sont activés ou désactivés.

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

La balise suivante contrôle cette capacité.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USE_MEDIASEC_WXT%	false (faux)	vrai, faux	Active les en-têtes SIP 3GPP pour la négociation SRTP.

6.1.4 Forcer l'utilisation de TCP, TLS ou UDP et Keepalives

Le client Webex pour Cisco BroadWorks peut être configuré pour utiliser TCP, TLS ou UDP pour la signalisation SIP et les médias RTP. Notez que le client utilise par défaut TCP. Notez également que sans clé TCP, les connexions SIP TCP sont fermées après une période d'inactivité.

L'exemple suivant décrit ce nœud de configuration.

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

La balise suivante contrôle si le client utilise TCP ou UDP.

Balise	Valeur par défaut si Omis	Valeurs prises en charge (octets)	Description
%TCP_SIZE_THRESHOLD_WXT%	0	0	Force le TCP à être utilisé. La décision d'utiliser TCP ou UDP pour le client appartient au prestataire de services ; cependant, la recommandation est d'utiliser TCP avec la valeur par défaut « 0 ».
	0	1 à 99 000	Force le protocole UDP à être utilisé lorsque la taille du message est inférieure à la valeur spécifiée ici. La valeur par défaut est TCP lorsque la taille du message est supérieure à la valeur définie. Pour utiliser UDP, 1500 est la recommandation par défaut.
	0	100 000	Force l'utilisation du protocole UDP.

Le même nœud de configuration a également des paramètres pour la connexion UDP, TCP et TLS, illustrés dans l'exemple suivant.

```
<config>
```


Confidentiel à Cisco

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

Les paramètres possibles sont :

- Activation de la clé TCP ou TLS, valeurs possibles - vrai/faux, la valeur par défaut est « faux » si le nœud est manquant. Notez que lorsque cette fonctionnalité est activée, les keepalives TCP sont envoyées même si le transport UDP est utilisé pour SIP.
- Activation de la clé UDP, valeurs possibles - vrai/faux, la valeur par défaut est « vrai » si le nœud est manquant. Notez que lorsque cette fonctionnalité est activée, les keepalives UDP sont envoyés même si le transport TCP est utilisé pour SIP. En outre, même si TCP est utilisé pour SIP, le client accepte également le trafic via UDP conformément à la norme *RFC 3261*.
- Le délai d'expiration spécifie la durée maximale d'inactivité en secondes après laquelle le message de conservation est envoyé. Aucune valeur signifie que le maintien en vie est désactivé pour le protocole.
- Charge utile pour les messages de conservation, valeurs possibles (aucune valeur signifie que la conservation est désactivée pour le protocole) :
  - Crlf
  - Null (à ne pas utiliser)
  - Chaîne personnalisée (**à ne pas utiliser**)

Les keepalives peuvent être utilisés pour la traversée NAT afin de garder les liaisons NAT ouvertes avec peu de trafic supplémentaire.

L'adresse IP du serveur et le port pour keepalives sont déterminés à l'aide des procédures normales pour la découverte du proxy SIP. Notez que les ports SIP et la sélection du protocole de transport obtenus via la détection de proxy dynamique SIP remplacent tout port statique ou toute configuration de transport. Pour plus d'informations sur la détection dynamique de proxy, voir la section*6.1.6Découverte dynamique du proxy* SIP*.*

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%UDP_KEEPALIVE_ENABLED_WXT%	vrai	vrai, faux	Contrôle si les paquets de conservation doivent être envoyés pour le transport UDP.
%TCP_KEEPALIVE_ENABLED_WXT%	false (faux)	vrai, faux	Contrôle si les paquets de conservation doivent être envoyés pour le transport TCP.
%TLS_KEEPALIVE_ENABLED_WXT%	false (faux)	vrai, faux	Contrôle si les paquets de conservation doivent être envoyés pour le transport TLS.

6.1.5 Délai d'expiration configurable pour l'ouverture du socket SIP

Auparavant, le délai d'expiration pour ouvrir un socket SIP était codé en dur sur 5 secondes pour TCP et 10 secondes pour TLS. Ces délais sont maintenant configurables.

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

Les balises suivantes contrôlent le délai d'expiration de la connexion du socket (en millisecondes).

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<integer> - le délai d'expiration en millisecondes	Le délai d'expiration de la connexion de la prise lorsque le transport TCP est utilisé.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10 000	<integer> - le délai d'expiration	Le délai d'expiration de la connexion de la prise lorsque le transport TLS est utilisé.

Confidentiel à Cisco

		en millisecondes	

6.1.6 Découverte dynamique du proxy SIP

Pour activer la fonctionnalité de découverte de proxy dynamique SIP, reportez-vous à l'exemple suivant.

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

Il est possible de contrôler les entrées de protocoles de transport de DNS SRV qui sont utilisées lorsque beaucoup sont disponibles en suivant les procédures fournies dans cette section.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USE_PROXY_DISCOVERY_WXT%	false (faux)	vrai, faux	Active la détection dynamique du proxy SIP pour les appels audio et vidéo. La valeur recommandée est « vrai ».
%SBC_ADDRESS_WXT%	vide	Chaîne de caractères	Cette balise Cisco BroadWorks est généralement utilisée pour le paramètre du nom de l'enregistrement. Il doit s'agir d'une URL valide et non d'une adresse IP. Pour plus d’informations, reportez-vous à la section *5.6Balises par défaut* système. Exemple : sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	vide	Chaîne de caractères	Cette balise personnalisée est utilisée pour le remplacement du domaine. Pour plus d’informations, reportez-vous à la section suivante. Exemple : autre.domaine.com
%USE_TCP_FROM_DNS_WXT%	vrai	vrai, faux	Si cette valeur de paramètre est « false », alors les résultats DNS SRV pour ce protocole de transport (TCP) sont rejetés. Si « true », alors les résultats de DNS SRV pour ce protocole de transport (TCP) sont utilisés. En fonction des priorités du SRV, un autre transport peut encore être élu.
%USE_UDP_FROM_DNS_WXT%	vrai	vrai, faux	Si cette valeur de paramètre est « false », alors les résultats DNS SRV pour ce protocole de transport (UDP) sont rejetés. Si « true », alors les résultats de DNS SRV pour ce protocole de transport (UDP) sont utilisés. En fonction des priorités du SRV, un autre transport peut encore être élu.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USE_TLS_FROM_DNS_WXT%	vrai	vrai, faux	Si cette valeur de paramètre est « false », alors les résultats DNS SRV pour ce protocole de transport (TLS) sont rejetés. Si « true », alors les résultats de DNS pour ce protocole de transport (TLS) sont utilisés. En fonction des priorités du SRV, un autre transport peut encore être élu.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	vrai, faux	vrai	Active/désactive le service de sauvegarde DNS. Si cette option est activée, la résolution A/AAAA est effectuée pour l'adresse du proxy SIP. Elle est prise en compte uniquement lorsque la détection du service SRV/NAPTR est activée.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	vrai, faux	vrai	Si la valeur est définie sur « true » et que la découverte du service NAPTR échoue ou ne renvoie aucun résultat, alors la découverte du service SRV est effectuée pour l'hôte configuré. Si ce paramètre est défini sur « faux », aucune détection SRV n'est effectuée.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	vrai, faux	false (faux)	Permet le contournement du cache DNS du système d'exploitation.

DNS permet au client d'obtenir l'adresse IP, le port et le protocole de transport pour le proxy SIP conformément à la norme RFC 3263.

Les requêtes DNS SRV, Naming Authority Pointer (NAPTR) et A-record sont prises en charge. Lors de la connexion, le flux en 3 étapes est le suivant :

1. Effectuez une requête NAPTR en utilisant le champ *<record-name>* ci-dessus pour obtenir les URI du serveur avec les protocoles de transport s'ils existent. La valeur du paramètre *<record-name>* doit être le domaine complet que DNS doit résoudre et ne peut pas être une adresse IP.
2. Résolvez les éléments trouvés dans la requête NAPTR en utilisant une requête SRV pour obtenir l'URI et le port finaux du serveur. La partie de domaine utilisée dans la requête SRV est extraite du résultat de la requête NAPTR pour trouver l'URI (et le port) du serveur final. Le port reçu de la requête DNS SRV est utilisé lorsque les entrées DNS SRV sont disponibles. Notez que le port, uniquement à partir du fichier de configuration, s'applique au proxy statique dans le fichier de configuration et non aux URI résolues en utilisant SRV. Reportez-vous aux exemples suivants pour l'utilisation des différents noms d'enregistrement.

Confidentiel à Cisco

Si aucun NAPTR n'est trouvé, le client tente une requête SRV avec le nom d'enregistrement pris dans le paramètre <*domain*> sauf si le paramètre <*domain-override*> est présent, auquel cas <*domain-override*> est utilisé et tente automatiquement de trouver des entrées séparées pour TCP, UDP et TLS (*_sip_protocol* [UDP, TCP ou TLS]). Notez que le protocole SCTP (Stream Control Transmission Protocol) n'est pas pris en charge. Si les requêtes SRV ne produisent aucun résultat, la détection du proxy échoue et l'utilisateur final reçoit une erreur indiquant que les appels ne sont pas disponibles. Dans ce cas, il n'y a pas d'enregistrement SIP. Cependant, même si toutes les requêtes SRV échouent ou si les serveurs reçus ne fonctionnent pas, en tant que secours, le client vérifie toujours si le proxy statique configuré fonctionne, uniquement avec des requêtes A à l'URI spécifié dans <adresse proxy> afin de voir s'il fournit une adresse IP qui fournit un enregistrement SIP fonctionnel. Le port et le transport dans ce cas de dernier recours proviennent des paramètres *tcp-threshold* et <*secure*>.

3. Résolvez les URI trouvées à l'aide de la requête d'enregistrement A. Les adresses IP finales reçues sont testées dans l'ordre dans lequel elles sont reçues pour obtenir une connexion de travail au proxy SIP. Cet ordre peut être défini par le prestataire dans le DNS. Le premier proxy URI SIP, avec une recherche d'enregistrement A réussie, est sélectionné et est utilisé jusqu'à ce qu'il ne fonctionne plus ou que le client se déconnecte. Dans l'étape de requête A, une seule adresse IP est utilisée à la fois, même si plusieurs sont reçues. Cependant, toutes les entrées SRV sont résolues jusqu'à la déconnexion ou la perte du réseau.

Remarques importantes

NOTE 1 : Si la découverte du proxy DNS entraîne la sélection du protocole de transport dans l'étape SRV en recevant une URI proxy SIP opérationnelle pour un protocole de transport, elle remplace le paramètre *tcp-threshold* généralement utilisé pour sélectionner UDP ou TCP dans le fichier de configuration. La même chose s'applique également à la configuration de SIP/TLS. TCP ou UDP est utilisé en fonction de la priorité dans DNS.

NOTE 2 : Les éléments reçus via SRV sont priorisés sur le proxy statique dans le fichier de configuration. L'ordre NAPTR n'est pas examiné ; seule la priorité SRV compte. Lorsque SRV aboutit à plusieurs articles avec un protocole de transport, une priorité et un poids égaux, l'un des articles reçus est sélectionné au hasard. Les poids NAPTR ne sont pas pris en charge dans cette version mais les poids SRV sont pris en charge. La priorité SRV est examinée en premier, et pour les éléments de priorité égale, le poids est examiné afin de déterminer la probabilité dans laquelle un certain serveur est essayé ensuite.

NOTE 3 : Le paramètre facultatif *de remplacement de domaine* permet de résoudre le nom d'enregistrement A autre que celui du paramètre de configuration du domaine SIP avec SRV lorsque les résultats NAPTR sont omis. Reportez-vous aux exemples suivants pour l'utilisation du paramètre *domain-override*.

NOTE 4 : Le client utilise des primitives de système d'exploitation pour les opérations DNS et, généralement, les réponses DNS sont mises en cache pour honorer le TTL de la réponse DNS.

NOTE 5 : Le type DNS (service) pour les enregistrements NAPTR doit suivre les procédures *RFC 3263*, sinon la résolution DNS peut échouer. Par exemple, il est nécessaire d'utiliser SIPS+D2T pour SIP sur TLS.

NOTE 6 : Le client prend en charge uniquement certains préfixes pour les services NAPTR. La liste suivante répertorie les préfixes pris en charge :

SIP+D2U -> _sip._udp

Confidentiel à Cisco

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

Si la réponse NAPTR contient un enregistrement avec préfixe qui ne correspond pas au type de service, cet enregistrement est ignoré.

Exemple 1 : Utilisation de la découverte du proxy DNS sans paramètre de configuration de remplacement de domaine

L'exemple suivant est un exemple de configuration utilisant la découverte du proxy SIP lorsque seul SIP sur TCP est utilisé et que la requête NAPTR à l'étape 1 renvoie les résultats.

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

Ceci se traduit par les étapes suivantes au niveau du protocole.

```
1. Requête NAPTR pour record-domain.com, réponse:
record-domain.com.
28591 DANS NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-
domain.com.
2. Requête SRV pour _sip._tcp.test.sip.record-domain.com (reçue dans la
requête NAPTR), répondre
_sip._tcp.test.sip.record-domain.com. 28635 DANS SRV
10 10 5061 test.sipgeo.record-domain.com.
3. Requête A-record pour test.sipgeo.record-domain.com, réponse :
test.sipgeo.record-domain.com. 16 DANS UN 1.2.3.4
```

Par conséquent, l'enregistrement SIP se déroule sur TCP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 1.2.3.4.

Exemple 2 : Utilisation du paramètre de remplacement de domaine dans le fichier de configuration

Ce qui suit est un deuxième exemple de configuration utilisant la découverte de proxy SIP où le domaine SIP est différent du domaine proxy et où seul SIP sur UDP est utilisé et la requête NAPTR ne renvoie pas les résultats.

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


Confidentiel à Cisco

Il en résulte les étapes suivantes au niveau du protocole.

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

Par conséquent, l'enregistrement SIP se déroule sur UDP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 4.3.2.1.

Exemple 3 : **Utilisation des priorités SRV**

L'exemple suivant est un autre exemple de configuration utilisant la découverte du proxy SIP lorsque seul SIP sur TCP est utilisé et que la requête NAPTR à l'étape 1 renvoie les résultats, mais plusieurs enregistrements NAPTR et SRV avec des priorités différentes sont reçus. Dans ce cas, seule la priorité SRV est importante dans cet événement de version, bien que plusieurs enregistrements NAPTR avec des priorités variables soient également reçus.

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

Il en résulte les étapes suivantes au niveau du protocole.

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

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

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

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

Par conséquent, l'enregistrement SIP se déroule sur TCP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 1.2.3.4 qui prendrait en charge à la fois UDP et TCP.

Exemple 4 : Utilisation de la détection du proxy DNS avec NAPTR lorsque le service ne correspond pas au type de service

L'exemple suivant est un exemple de configuration utilisant la découverte du proxy SIP lorsque SIP sur TCP et TLS est utilisé et que la requête NAPTR à l'étape 1 renvoie les résultats.

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

Ceci se traduit par les étapes suivantes au niveau du protocole.

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

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

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

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

Par conséquent, l'enregistrement SIP se déroule sur TCP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 1.2.3.4.

6.1.7 Utilisation du port préféré pour SIP

Il y a eu des cas où un autre progiciel était en cours d'exécution sur la même machine que le client, occupant le port SIP par défaut. Pour configurer le client pour qu'il utilise un autre port pour SIP, le paramètre *port préféré* peut être utilisé. Le client tente d'utiliser la valeur de port configurée spécifiée dans le paramètre *port préféré*, mais si elle est prise, le client tente progressivement des valeurs de port supérieures à la valeur configurée. Par exemple, si la valeur du *port préféré* est « 6000 » et que ce port est pris, le client tente 6001, 6002, 6003, etc. jusqu'à ce qu'il trouve un port inutilisé. Une fois qu'un port inutilisé est trouvé, il l'utilise pour sa propre communication SIP.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SOURCE_PORT_WXT%	5060	numéro	Spécifie le port SIP local préféré pour la communication. Exemple : 5060

Confidentiel à Cisco

6.1.8 Basculement et restauration SIP

Le basculement et la restauration SIP suivent les procédures Cisco BroadWorks. Pour cela, plusieurs proxy (généralement le SBC) doivent être configurés.

Côté client, le proxy doit être résolu en plusieurs adresses IP. Ceci peut être réalisé soit :

- La détection du proxy SIP est activée et le serveur DNS a des enregistrements NAPTR et/ou SRV pour le FDQN SBC (voir section*6.1.6Découverte dynamique du proxy* SIP), OU
- L'adresse proxy SIP est fournie en tant que nom de domaine complet et elle est résolue en plusieurs adresses IP (voir section*6.1.1Paramètres du serveur* SIP).

Le cache DNS du système d'exploitation est utilisé pour éviter le trafic DNS inutile. Il n'y a pas de limite
codée en dur pour le nombre maximum d'adresses IP dans la liste.

Lors de la connexion, si plusieurs adresses IP sont résolues, elles sont classées par priorité. Le client commence à utiliser la première adresse IP disponible.

6.1.8.1 Basculement SIP

Le basculement SIP peut être déclenché par une erreur de socket, une erreur de délai de demande ou une réponse d'erreur définitive du serveur comme suit :

- Erreur de socket – si la socket entre le client et le serveur est cassée ou est fermée, comme dans le cas d'une perte de connectivité réseau, le client réagit immédiatement et déclenche un basculement.
- Délai d'expiration (par exemple, lorsque le SBC se bloque) – basé sur le SIP T1 :
  - SIP INVITE – si la demande INVITE expire, le client s'enregistre au prochain SBC (IP) disponible et retente l'INVITE.
  - Une autre demande SIP – le client tente de s'inscrire au prochain SBC (IP) disponible.
- Réponse d'erreur définitive reçue du serveur :
  - Les réponses d'erreur SIP suivantes du serveur vers un REGISTRE SIP déclenchent un basculement :
    - 5xx
    - 6xx
  - Les réponses SIP *4xx* suivantes à SIP REGISTER ne provoquent pas le basculement :
    - 401 Non autorisé
    - 403 Interdit
    - 404 Non trouvé
    - 407 Authentification du proxy requise
    - 423 Intervalle trop bref
  - En outre, les réponses d'erreur *4xx* à SIP INVITE ne déclenchent pas le basculement, mais *5xx* et *6xx* le font.

Confidentiel à Cisco

Lorsqu'un basculement est déclenché, le client prend l'adresse IP suivante disponible de la liste. Le minuteur SIP T1 définit la durée pendant laquelle un proxy de la liste est essayé avant de passer au proxy suivant, généralement une valeur de 32 secondes est utilisée (64*T1). Si toutes les adresses IP échouent, le client affiche une erreur d'interface utilisateur pour la connectivité SIP. Si un appel VoIP est en cours lors du basculement, l'appel est interrompu.

La logique de basculement SIP repose sur plusieurs paramètres de configuration :

- Minuteurs de basculement SIP – Les minuteurs SIP T1, T2 et T4 sont exposés dans le fichier de configuration, mais il n'est pas recommandé de les modifier.

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

  - T1 – la durée, en millisecondes, d'un délai aller-retour réseau.
  - T2 – la durée maximale, en millisecondes, avant de retransmettre les demandes non invitées et les réponses invitées.
  - T4 – la durée maximale, en millisecondes, pour qu'un message reste sur le réseau.
- Découverte de l'adresse du proxy SIP et du proxy SIP
  - Voir section *6.1.1Paramètres du serveur* SIP.
  - Voir section *6.1.6Découverte dynamique du proxy* SIP.
- Enregistrer la configuration de basculement (voir ci-dessous)

En cas de basculement, l'application Webex envoie SIP REGISTER avec deux en-têtes de contact - un pour l'ancienne session et le second avec les informations sur le nouveau périphérique. L'en-tête Contact de l'ancienne session est inclus pour informer le SBC de nettoyer les données. Cet en-tête inclut expires=0 et q=0.5.

L'en-tête Contact contenant les informations du nouveau périphérique a également la valeur q, qui est lue à partir de la balise <*q-value*>. La valeur de la balise <*q-value*> est utilisée pour indiquer la préférence ou la priorité d'une adresse de contact particulière. Elle varie de 0 à 1.0, 1.0 étant la préférence la plus élevée et 0 la plus faible. Cette balise n'a pas de balise personnalisée pour contrôler la valeur - elle est codée en dur sur 1.0. La valeur peut être ajustée manuellement, si le SBC utilisé dans le déploiement a une logique inverse et traite q=0.0 avec priorité maximale.

À partir de la version 42.11, une nouvelle section <*register-failover*> est introduite dans le modèle de configuration. Un nouveau paramètre configurable <*registration-cleanup*> a été ajouté pour contrôler si l'application enverra l'en-tête Contact pour nettoyer ou non les anciennes informations du périphérique. Certains SBC nettoient l'ancienne session immédiatement à la déconnexion de la prise, de sorte que l'existence de l'en-tête Contact pour l'ancienne session n'est pas nécessaire. Par défaut, la logique de nettoyage de l'enregistrement est activée.

Confidentiel à Cisco

Par souci de cohérence, la balise *<q-value>* est également déplacée sous la même section *<register-failover>*.

Exemple :

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	vrai	vrai, faux	Contrôle le nettoyage des informations des anciens périphériques en cas de basculement SIP.

6.1.8.2 Restauration SIP

Si le client est connecté à un proxy qui n'est pas prioritaire, il tente de se reconnecter à l'adresse IP avec la priorité la plus élevée. Le délai de restauration est basé sur la configuration de gestion du TTL DNS (voir section *6.1.8.4Gestion du TTL* DNS). Si un appel est en cours lorsque le minuteur de restauration est atteint, le client attend que tous les appels soient terminés et déclenche la procédure de restauration. Notez que ceci n'est valide que pour les clients de bureau puisque la connexion SIP est active uniquement lors d'un appel sur mobile.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SIP_FAILBACK_ENABLED_WXT%	vrai	vrai, faux	Active/désactive la restauration SIP.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Plus de 60 ans	Le délai d'expiration de la restauration SIP en secondes.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false (faux)	vrai, faux	Ajoute une période aléatoire [0-10] % de la restauration SIP.

6.1.8.3 Appliquer la version IP

Le client Webex peut être configuré pour commander la liste des hôtes résolus via le DNS, puis pour itérer via eux en cas de basculement SIP. Dans tous les modes, la priorité et le poids sont respectés.

Les configurations prises en charge sont :

- dns - utilise toutes les adresses renvoyées par les requêtes DNS
- ipv4 - filtre les adresses IPv6
- ipv6 - filtre les adresses IPv4

Confidentiel à Cisco

- prefer-ipv4 – commande les adresses IPv4 avant l'IPv6 (version 42.9)
- prefer-ipv6 – commande les adresses IPv6 avant l'IPv4 (version 42.9)
- nat64 – ignore les adresses IPv6, commande celles IPv4 (version 44.2)

Il est recommandé d'utiliser la valeur par défaut (dns), sauf si la configuration de l'environnement/du réseau nécessite un mode différent.

Avec la configuration « dns », les adresses IPv4 sont priorisées sur celles IPv6, pour un hôte donné. S'il y a deux hôtes avec les adresses IPv4 et IPv6, l'ordre sera IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

En mode « prefer-ipv4 », les adresses IPv4 sont classées avant les adresses IPv6 (l'ordre dans les groupes IPv4 et IPv6 reste)

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

Avec le mode « prefer-ipv6 », l'ordre est le contraire : les adresses IPv6 sont placées avant les adresses IPv4

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

Avec le mode « nat64 » - les adresses IPv6 sont ignorées, l'ordre IPv4 est respecté. Le ou les préfixes IPv6 sont découverts. Pour chaque adresse IPv4, une combinaison avec chaque préfixe et/ou suffixe Pref64 est créée.

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

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	dns	ipv4 ipv6 dns préférer ipv4 préférer ipv6 nat64	Contrôle l'ordre des adresses IPv4/IPv6 utilisées par le client Webex pour connecter la session SIP.

6.1.8.4 Gestion du TTL DNS

Un paramètre de configuration distinct a été ajouté pour gérer la façon dont la résolution DNS est refaite lorsque le TTL de l'enregistrement DNS du serveur actuellement utilisé expire. Le paramètre dans le tableau suivant, lorsqu'il est activé, force le client à refaire des opérations DNS une fois que le TTL du DNS SRV ou l'enregistrement A du serveur actuellement utilisé expire.

Confidentiel à Cisco

Une fois la résolution DNS reeffectuée, ce paramètre force également le client à se reconnecter au serveur de priorité supérieure reçu s'il est différent du serveur actuellement utilisé, même dans le cas où la connexion actuelle fonctionne entièrement. Cependant, la reconnexion n'est effectuée qu'après la fin des appels en cours.

Si les TTL des enregistrements des serveurs A et SRV sont différents, la valeur la plus petite est choisie.

Lorsque ce paramètre est désactivé, les opérations DNS ne sont pas renouvelées à l'expiration du TTL, mais plutôt toutes les 15 minutes.

Ce paramètre ne fonctionne que pour SIP.

Notez que la fonction de gestion DNS TTL ne peut pas être utilisée lorsqu'une adresse IP est utilisée dans le paramètre d'adresse proxy.

> **REMARQUE :** Il s'agit d'une fonctionnalité de bureau uniquement, car les clients mobiles n'ont de connexion SIP que lorsqu'ils sont en communication.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SIP_REFRESH_ON_TTL_WXT%	false (faux)	faux, vrai	Lorsque ce paramètre est défini sur « faux », la gestion du TTL DNS est désactivée pour SIP. Lorsque ce paramètre est défini sur « vrai », la gestion DNS TTL est activée pour SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	false (faux)	faux, vrai	Si cette option est activée, ajoute a une période aléatoire comprise entre 0 et 10 % au TTL DNS DNS.

> **REMARQUE :** Il est fortement recommandé d'activer le facteur aléatoire DNS TTL pour empêcher les pics de requêtes vers le DNS et potentiellement les pics de tentatives de reconnexion vers le serveur d'applications.

Confidentiel à Cisco

6.1.9 SIP SUBCSRIBE et REGISTER Actualiser et S'ABONNER Réessayer

Communicator prend en charge la configuration des intervalles d'actualisation pour SIP SUBSCRIBE et REGISTER. Pour SIP SUBSCRIBE, il existe un paramètre distinct pour l'intervalle d'actualisation (en secondes) et la durée pendant laquelle le client attend avant de retenter SIP SUBSCRIBE en cas d'erreurs (en secondes). La valeur maximale recommandée pour l'*intervalle abonnement-nouvelle tentative* est de 2000000 secondes alors que toute valeur négative, 0 ou vide entraîne l'utilisation de 1800 secondes. Toute valeur négative dans l'actualisation des abonnements ne tient pas compte de l'en-tête *Expires* et crée ainsi une SUBSCRIBE unique.

Le minuteur d'actualisation SIP REGISTER proposé par le client peut être configuré en secondes, mais selon les spécifications SIP, le serveur peut remplacer la valeur. Actuellement, le client se souvient de la valeur proposée par le serveur pour les actualisations ultérieures au lieu d'utiliser toujours la valeur configurée.

Enfin, la valeur d'expiration pour les sessions SIP (pour SIP INVITE et SUBSCRIBE) peut également être configurée (en secondes).

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

6.1.10 Utiliser les URI P-Associated dans REGISTER

Le paramètre suivant est utilisé lors de l'enregistrement et du traitement de la réponse *200 OK* correspondante.

Si le paramètre est défini sur « false », alors le client n'utilise pas l'*URI P-Associated* et utilise l'identité de son propre URI SIP à la place.

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

Si le paramètre est défini sur « true », le client prend sa propre identité à partir du dernier en-tête *P-Associated-URI* pour toutes les requêtes SIP sortantes (INVITE, SUBSCRIBE, CANCEL, INFO et REFER) de la réponse *200 OK* dans REGISTER. De plus, ces URI ne sont pas affichées en tant que contacts dans la liste des contacts.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USE_ALTERNATIVE_IDENTITIES_WXT%	false (faux)	vrai, faux	Active l'utilisation d'identités alternatives dans SIP REGISTER. S'il est défini sur « true », le client prend sa propre identité à partir du dernier en-tête *P-Associated-URI* pour les demandes SIP sortantes. Si défini sur « faux », alors sa propre identité pour les demandes SIP sortantes est prise à partir de son propre URI SIP.

6.1.11 En-tête SIP P-Early Media (PEM)

L'en-tête SIP *P-Early Media* (PEM) peut être utilisé, par exemple, dans des environnements IMS à l'intérieur d'un domaine de confiance pour permettre au réseau d'autoriser plusieurs boîtes de dialogue de médias précoces SIP, par exemple dans les cas où un autre réseau autorise tous les médias précoces.

Le paramètre de configuration active la prise en charge PEM publicitaire dans la signalisation SIP. La logique réelle de traitement des médias précoces est la même pour les cas PEM et non-PEM, agissant sur les valeurs d'en-tête PEM prises en charge.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_PEM_SUPPORT_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer la prise en charge PEM de la publicité client dans la signalisation SIP. Définissez sur « faux » pour désactiver la prise en charge PEM publicitaire du client dans la signalisation SIP.

6.1.12 Prise en charge de la MISE À JOUR SIP

La MISE À JOUR SIP est nécessaire, par exemple, dans certains déploiements IMS, au lieu de réinviter l'autre. Il permet à un client de mettre à jour les paramètres d'une session tels que l'ensemble des flux média et leurs codecs mais n'a pas d'impact sur l'état d'une boîte de dialogue SIP.

Les cas d'utilisation typiques sont liés aux médias précoces lorsque, par exemple, la tonalité de retour d'appel et la pré-alerte sont utilisés simultanément.

Confidentiel à Cisco

La MISE À JOUR SIP n'est actuellement prise en charge que lorsqu'elle est reçue dans les cas d'utilisation de pré-dialogue (média précoce) et non pendant la boîte de dialogue active, par exemple, pour la mise en attente/reprise d'appel où re-INVITE est toujours utilisée.

Il n'est pas possible d'ajouter de la vidéo à l'audio en utilisant SIP UPDATE (changement de média) dans cette version. En outre, le client ne prend pas en charge le flux d'appels longs IMS complet avec réservation de ressources.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false (faux)	vrai, faux	Lorsque cette option est définie sur « faux », la prise en charge de la MISE À JOUR SIP est désactivée. Lorsque ce paramètre est défini sur « vrai », la prise en charge de la MISE À JOUR SIP est activée.

6.1.13 Ancien SIP INFO FIR

Ce client prend en charge la manière existante de demander des images clés vidéo via la demande de contrôle de média SIP INFO. Cela est nécessaire car certains des périphériques ont des problèmes de réponse au RTCP-FB FIR et parfois le RTCP n'arrive pas jusqu'au point de terminaison distant, ce qui peut conduire à l'absence de vidéo ou à la vidéo unidirectionnelle. Pour plus d'informations, reportez-vous à la *RFC 5168*.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « faux », la prise en charge de SIP INFO FIR est désactivée. Lorsque ce paramètre est défini sur « vrai », la prise en charge de SIP INFO FIR est activée.

6.1.14 Gestion du port SIP pour la traversée NAT

Le client peut être configuré pour utiliser le mécanisme de rport SIP pour la traversée NAT. Notez que, généralement, il ne peut pas être la seule solution pour la traversée NAT et SBC est principalement utilisé à cette fin. Pour une description de la spécification rport, voir *RFC 3581*.

Confidentiel à Cisco

Pour plus d'informations sur les recommandations de port SIP et de protocole de transport lorsque des passerelles de couche d'application SIP (ALG) sont utilisées sur le réseau, consultez le *Guide de la solution Webex pour Cisco BroadWorks*.

Notez que la chaîne « rport » est toujours présente dans les requêtes SIP sortantes quelle que soit la configuration. Le paramètre n'affecte que l'utilisation de l'adresse IP et du port reçus du serveur dans les en-têtes SIP « received » et « rport ». Lorsque la fonctionnalité est activée, les valeurs des en-têtes « received » et « rport » sont utilisées dans l'en-tête SIP Contact des requêtes SIP (même lorsque l'en-tête « received » est manquant dans la réponse REGISTER).

Le paramètre *Port préféré* est lié en ce qu'il définit autrement le port utilisé dans l'en-tête SIP Contact. Pour plus d'informations sur l'allocation des ports SIP, voir section *6.1.7Utilisation du port préféré* pour SIP.

Il existe un paramètre de configuration distinct *use-local-port* qui force le port local du socket client à définir dans l'en-tête *Contact*. Ceci est utilisé pour certains SBC qui détectent que le client a une adresse IP réelle (à partir de l'en-tête *Contact*) et le SBC tente d'établir un socket distinct pour le client pour ses demandes. Dans la plupart des cas, un pare-feu se trouve entre le SBC et le client, et il refuse les connexions entrantes au client.

REMARQUE : Dans les environnements IPv6, toutes les adresses sont réelles et le SBC tente d'établir une connexion avec l'adresse du client d'écoute (à partir de l'en-tête *Contact*).

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_USE_RPORT_WXT%	false (faux)	vrai, faux	Active le rport pour les appels audio et vidéo.
%RPORT_USE_LOCAL_PORT_WXT%	false (faux)	vrai, faux	Contrôle si le port local du socket du client doit être ajouté dans l'en-tête *Contact* SIP.

6.1.15 ID de session SIP

Lorsque cette option est activée, lors de la première inscription, un ID de session local est généré. L'ID de session est utilisé pendant la durée de vie de la connexion/session pour ce périphérique, pour toutes les boîtes de dialogue hors appel, REGISTER, SUBSCRIBE, NOTIFY, etc. Le même ID de session est utilisé jusqu'à ce que la liaison soit perdue. Lorsque la liaison d'enregistrement est perdue (recherche DNS, réinitialisation de la connexion, réinitialisation du téléphone, etc.), un nouvel ID de session local est généré.

La valeur de l'ID de session peut être utilisée pour trouver l'ensemble complet des boîtes de dialogue associées à ce périphérique.

Confidentiel à Cisco

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SIP_SESSION_ID_WXT%	false (faux)	vrai, faux	Contrôle l'utilisation de l'ID de session SIP.

6.1.16 Comportement de rejet d'appel entrant

Le client offre la flexibilité de rejeter un appel avec *486* ou *603*.

Notez que si le client est configuré pour rejeter un appel avec *603 Refuser*, alors les services Renvoi d'appel si occupé et Renvoi d'appel sans réponse peuvent ne pas fonctionner comme prévu.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_REJECT_WITH_486_WXT%	vrai	vrai, faux	Contrôle le code d'erreur SIP et la raison utilisée pour rejeter les appels SIP entrants. Si cette option est activée, *486 Temporairement indisponible* est utilisée. Sinon, *603 Refuser* est utilisé.

6.1.17 Plage de ports de protocole de transport en temps réel

Le client peut être configuré pour utiliser une plage de ports définie pour les flux RTP (Real-Time Transport Protocol), qui s'applique également pour SRTP. Cette configuration est effectuée en définissant les valeurs limites de plage de ports pour les flux audio et vidéo avec les balises indiquées dans l'exemple suivant.

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	numéro	Démarrage de la plage de ports audio.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	numéro	Fin de la plage de ports audio.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	numéro	Début de la plage de ports vidéo.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	numéro	Fin de la plage de ports vidéo.

REMARQUE : Les plages de ports doivent être définies de manière à ne jamais se chevaucher.

6.1.18 Prise en charge ICE (Webex Calling uniquement)

Le client prend en charge la négociation Interactive Connectivity Establishment (ICE) qui permet l'optimisation du chemin média entre les terminaux (de manière peer-to-peer). Ceci est fait pour réduire la latence des données, réduire la perte de paquets et réduire les coûts opérationnels du déploiement de l'application.

Notez que l'implémentation actuelle prend en charge le serveur STUN, tandis que TURN n'est pas pris en charge.

Lorsque la prise en charge ICE est activée, une nouvelle saisie pour SRTP sera toujours effectuée (voir section *6.1.2SIP sur TLS et protocole de transport sécurisé* en temps réel).

À partir de la version 44.5, l'application Webex ajoute la prise en charge d'ICE sur IPv6 en utilisant NAT64.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_RTP_ICE_WXT%	false (faux)	vrai, faux	Activer/désactiver la prise en charge ICE.
%RTP_ICE_MODE_WXT%	ictère	ictère	Mode de prise en charge du ICE. Actuellement, la seule valeur prise en charge est « icestun ».

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%RTP_ICE_SERVICE_URI_WXT%	(vide)	URI du serveur STUN valide ou (vide)	URI du serveur STUN.
%RTP_ICE_PORT_WXT%	3478	Numéro (0-65535)	Port du serveur STUN.
%ENABLE_RTP_ICE_IPV6_WXT%	false (faux)	vrai, faux	Active ICE sur IPv6.

6.1.19 MUX RTCP

RTCP MUX est configurable. Cette fonctionnalité permet au client d'utiliser le même port pour RTP et RTCP. Au niveau de signalisation SIP/SDP, la ligne a=rtcp-mux est ajoutée au SDP. De plus, différents modes sont possibles :

- Mode rétrocompatibilité (c'est-à-dire que la ligne a=rtcp-mux n'apparaît pas dans SDP)
- Mode multiplexage (la ligne a=rtcp-mux apparaîtra deux fois dans le SDP : une fois dans la section m=audio, et une seconde fois dans la section m=vidéo)

La vidéo et l'audio n'utilisent pas le même port.

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

Notez que RTCP MUX ne peut pas être utilisé avec les appels SRTP.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_RTCP_MUX_WXT%	vrai	vrai, faux	Pour activer RTPC MUX, définissez sur « vrai ». Pour désactiver RTCP MUX, définissez sur « false ».

6.1.20 Transférer

Le client Webex pour Cisco BroadWorks prend en charge le transfert d'appel assisté (consultatif), semi-consultatif et Direct (aveugle).

Le transfert d'appel semi-consultatif permet à l'appelant de terminer le transfert avant que l'appel ne soit pris par l'appelé distant. Le bouton de fin semi-consultatif n'est activé pour l'appelant qu'une fois que la sonnerie a démarré du côté de l'appelé et que la notification SIP correspondante (*sonnerie 180*) est reçue du côté de l'appelant. Le transfert aveugle est appelé « Transférer maintenant » dans l'interface utilisateur.

Confidentiel à Cisco

REMARQUE : La sonnerie SIP *180* peut ne pas être déclenchée dans certains environnements, pour certains numéros ou dans certains scénarios de communication inter-serveurs.

La version 43.9 de l'application Webex introduit le transfert vers un autre appel en cours autonome du même type. Les appels terminés dans l'application Webex peuvent être transférés vers d'autres appels terminés dans le point de terminaison local. Et les appels terminés sur un périphérique distant peuvent être transférés vers des appels terminés sur un point de terminaison distant. Cette fonctionnalité ne comporte pas d'options configurables.

À partir de la version 43.12, l'application Webex ajoute une option de configuration pour contrôler si l'appel en cours doit être automatiquement mis en attente lorsque l'élément du menu Transférer est sélectionné. Ce comportement est contrôlé par le nouvel attribut *auto-hold*. Par défaut, la mise en attente automatique est désactivée.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_TRANSFER_CALLS_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « vrai », le transfert d'appel est activé. Lorsque ce paramètre est défini sur « faux », le transfert d'appel est désactivé.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false (faux)	vrai, faux	Active la ou les options de transfert pour les appels distants (XSI) terminés sur un autre emplacement.
%TRANSFER_CALL_TYPE_WXT%	complet	parler d'abord, aveugle, plein	Spécifie les types de transfert disponibles pour l'utilisateur dans la configuration BroadWorks.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false (faux)	vrai, faux	Contrôle si l'appel actif sera mis en attente automatiquement lorsque l'utilisateur sélectionne l'option de transfert dans le menu de l'écran d'appel.

Confidentiel à Cisco

6.1.21 Conférences téléphoniques à N-Way et participants

La balise personnalisée suivante peut être utilisée pour contrôler la disponibilité de la conférence téléphonique ad hoc (N-Way) via SIP dans le client Webex pour Cisco BroadWorks. De plus, le propriétaire de N-way peut voir la liste complète des participants via SIP SUBSCRIBE/NOTIFY et le pack d'événements de la conférence. Le client du propriétaire apprend l'URI à laquelle envoyer le SIP SUBSCRIBE via l'en-tête SIP *Contact* précédent du message *200 OK* envoyé en réponse à l'INVITE à l'URI de la conférence alors que pour les participants, les mêmes informations se trouvent dans un appel-info précédent NOTIFY.

Le paramètre système Cisco BroadWorks (*maxConferenceParties)* est utilisé pour définir le nombre maximum de parties de conférence. Pour un appel donné, il indique le nombre de parties simultanées actives qu'un utilisateur peut avoir ou ajouter via l'option de contrôle de mi-appel « Ajouter des participants » ou via la fonction d'appel à n-way de Cisco BroadWorks.

Ces informations sont récupérées à partir du serveur d'applications (AS) à l'aide de la commande d'interface de ligne de commande (CLI) suivante.

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

Example output:
maxConferenceParties = 6
conferenceURI =
```

Une fois la valeur obtenue pour *maxConferenceParties* (qui a une plage de 4 à 15), la balise %MAX_CONF_PARTIES_WXT% doit être définie en conséquence.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CONFERENCE_CALLS_WXT%	false (faux)	vrai, faux	Contrôle si l'option Conférence doit être activée pour l'utilisateur.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer la liste des participants propriétaires N-way. Définissez sur « faux » pour désactiver la liste des participants propriétaires N-way.
%MAX_CONF_PARTIES_WXT%	10	Nombre compris entre 4 et 15 (vide)	Indique le nombre maximum de participants à N voies, exigé par le client, par exemple 10. Côté serveur a ses propres limites. La valeur vide désactive l'application par le client de la limite des participants à N voies.

Confidentiel à Cisco

6.1.22 Call Pull (Transfert d'appel)

La fonction d'extraction d'appel peut être activée à l'aide d'un seul paramètre de configuration, comme illustré dans l'exemple suivant.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_PULL_WXT%	false (faux)	vrai, faux	Active l'extraction d'appel.

6.1.23 Parcage/Récupération d'appels

La fonctionnalité de parcage d'appels de groupe permet de transférer les appels VoIP en cours vers un serveur de parcage d'appels, ce qui permet à l'appelant de faire autre chose et d'être récupéré par le même utilisateur ou un autre utilisateur. Un appel en cours sera parqué sur le premier poste disponible dans le groupe de parcage d'appels.

La récupération d'appel peut être effectuée par l'utilisateur qui parait l'appel dans la boîte de dialogue pendant un nombre de secondes configurable immédiatement après le parcage de l'appel. Ou l'appel parqué peut être récupéré par l'utilisateur ou un autre utilisateur en sélectionnant l'option de récupération d'appel et en saisissant le numéro ou le numéro de poste.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_PARK_WXT%	false (faux)	vrai, faux	Active le parcage/la récupération d'appels.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Nombre compris entre 5 et 30	Indique le nombre de secondes pendant lesquelles la boîte de dialogue de parcage d'appel réussie est visible par l'utilisateur avant d'être fermée automatiquement.

Confidentiel à Cisco

6.1.24 Stat. appels

La création de rapports statistiques de fin d'appel dans le protocole SIP (Session Initiation Protocol) permet d'envoyer des statistiques d'appel à un terminal distant lorsqu'un appel se termine. Les statistiques d'appel sont envoyées en tant que nouvel en-tête dans le message SIP BYE ou dans la réponse *200 OK* correspondante au message BYE. Les statistiques comprennent les paquets RTP (Real-time Transport Protocol) envoyés ou reçus, le nombre total d'octets envoyés ou reçus, le nombre total de paquets perdus, la gigue de délai, le délai aller-retour et la durée d'appel.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_STATISTICS_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour permettre la capture des métriques d'appel. Définissez sur « faux » pour désactiver la capture des métriques d'appel.

6.1.25 Récupération automatique des appels / Transfert d'appel fluide

Le client prend en charge la récupération automatique d'appel au niveau de réseaux de commutation alors que l'utilisateur a un appel VoIP en cours. La récupération automatique d'appel fonctionne dans les deux sens - Données cellulaires-vers-WiFi et WiFi-vers-Données cellulaires, ainsi que lors de la commutation entre les réseaux WiFi. L'appel est tenté pour être récupéré dans un délai d'une minute, puis s'arrête. S'il y a plus d'un appel VoIP en cours, seul l'appel actif est récupéré.

Lors de la transition de données cellulaires vers le WiFi, le client conserve les appels VoIP en cours sur les données cellulaires jusqu'à ce qu'ils soient terminés ou que le réseau de données cellulaires soit perdu.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false (faux)	vrai, faux	Contrôle si le mécanisme de récupération automatique doit être activé pour l'utilisateur.

Confidentiel à Cisco

6.1.26 Enregistrement des appels

La fonctionnalité d'enregistrement des appels est prise en charge par le client et dépend de la disponibilité de la fonctionnalité côté serveur, ainsi que de l'option de configuration. La fonctionnalité dépend du canal d'événement XSI activé (voir section *6.1.33Canal d'événement XSI*) et du serveur d'applications (AS) configuré pour envoyer l'en-tête SIP *X-BroadWorks-Correlation-Info* (voir le *Guide de la solution Webex pour Cisco BroadWorks*).

Si la fonctionnalité est désactivée, il n'y a pas de boutons et d'options d'enregistrement pour l'utilisateur. Notez que l'enregistrement des appels fonctionne sur une base par utilisateur, et non par appel. Cela signifie que si l'un des participants à un appel prend en charge l'enregistrement des appels, l'appel peut être enregistré.

Si la fonction d'enregistrement des appels est activée, il y a toujours une indication visuelle lorsque l'appel est enregistré. Les modes d'enregistrement des appels suivants sont pris en charge par Cisco BroadWorks :

Toujours

- L'enregistrement des appels sera démarré automatiquement à l'établissement de l'appel.
- L'utilisateur ne peut **PAS** arrêter/mettre en pause l'enregistrement de l'appel.

Toujours avec prise en charge de la pause/reprise

- L'enregistrement de l'appel sera démarré automatiquement à l'établissement de l'appel, mais l'utilisateur pourra mettre l'appel en pause et le reprendre.
- Interactions possibles avec les utilisateurs :
  - L'enregistrement est en cours – **Pause** de l'action d'enregistrement.
  - L'enregistrement est en pause – **Reprendre** l'action d'enregistrement.

Sur demande

- Une fois l'appel établi, l'enregistrement des appels démarre sur le serveur.
- Si l'utilisateur appuie sur l'option Démarrer l'enregistrement pendant l'appel, l'enregistrement de l'appel sera stocké et il gardera l'appel à partir de son démarrage. Sinon, si aucun enregistrement de démarrage n'est initié à partir de l'utilisateur, l'enregistrement d'appel sera supprimé sur le serveur.
- Interactions possibles avec les utilisateurs :
  - Aucun enregistrement n'a encore démarré – action **Démarrer** l'enregistrement.
  - L'enregistrement est en cours – **Pause** de l'action d'enregistrement.
  - L'enregistrement est en pause – **Reprendre** l'action d'enregistrement.

À la demande avec démarrage initié par l'utilisateur

- L'utilisateur peut démarrer, arrêter, mettre en pause et reprendre l'enregistrement des appels à tout moment, plusieurs fois au cours d'un appel.
- Il y aura des enregistrements d'appels séparés pour chaque démarrage d'enregistrement d'appel.

Confidentiel à Cisco

- Interactions possibles avec les utilisateurs :
  - Aucun enregistrement n'a encore démarré – action **Démarrer** l'enregistrement.
  - L'enregistrement est en cours – action **Arrêter** et **Mettre en pause** l'enregistrement.
  - L'enregistrement est en pause – **Arrêter** et **Reprendre** l'action d'enregistrement.

Le mode d'enregistrement des appels attribué à l'utilisateur peut être sélectionné à partir du Control Hub.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_RECORDING_WXT%	false (faux)	vrai, faux	Active les commandes d'enregistrement des appels.

6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente

Les balises personnalisées suivantes peuvent être utilisées pour contrôler la disponibilité de la messagerie vocale Cisco BroadWorks et de la messagerie vocale visuelle dans le client Webex pour Cisco BroadWorks. Notez qu'une balise système Cisco BroadWorks (%BWVOICE-PORTAL-NUMBER-1%) est utilisée avec la messagerie vocale.

La messagerie vocale visuelle (VVM) est prise en charge uniquement pour l'audio. Les formats pris en charge sont wav, ulaw et mov contenant la vidéo H264 (lue en audio uniquement). Il permet aux utilisateurs d'afficher les messages vocaux entrants dans une vue de liste et des éléments individuels peuvent être lus. Cette fonctionnalité est basée sur Xsi, mais les notifications de nouvelle messagerie vocale sont fournies via SIP ; par conséquent, SIP doit être activé pour que les notifications fonctionnent. En outre, la configuration SIP SUBSCRIBE pour l'indicateur de message en attente (MWI) est nécessaire pour que les notifications arrivent et MWI doit être activé pour que la messagerie vocale visuelle fonctionne. Pour plus d'informations sur la configuration SIP, reportez-vous à la section*6.1.1Paramètres du serveur* SIP.

Pour les exigences de version et de patch de Cisco BroadWorks pour la messagerie vocale visuelle, reportez-vous au
Guide de la solution Webex pour Cisco BroadWorks.

La messagerie vocale visuelle doit être activée séparément dans la configuration.

Les paramètres suivants sont nécessaires sur le portail CommPilot pour avoir la messagerie vocale visuelle :

- Messagerie vocale activée
- Option « Lorsque le message arrive, utiliser la messagerie unifiée » activée
- Option « Utiliser l'indicateur de message téléphonique en attente » activée

Confidentiel à Cisco

Ne pas avoir le service de messagerie vocale visuelle affecté du côté Cisco BroadWorks pour l'utilisateur désactive automatiquement la configuration du service.

Notez que la désactivation de l'enregistrement SIP désactive également MWI pour les nouveaux messages vocaux. Reportez-vous au tableau suivant pour plus d'informations sur l'activation de MWI.

Pour afficher les informations des messages vocaux dans l'interface utilisateur, le client doit recevoir des notifications SIP MWI du serveur (c'est-à-dire le pack d'événements de messagerie vocale). Reportez-vous au tableau ci-dessous pour les options d'abonnement. Notez également que MWI est nécessaire pour que les notifications de messagerie vocale visuelle fonctionnent.

Notez que si l'abonnement SIP au pack d'événements de messagerie vocale échoue, le client continue de réessayer lorsqu'il est configuré pour le faire. Pour plus d'informations sur la configuration de la nouvelle tentative SIP SUBSCRIBE, voir la section*6.1.9SIP SUBCSRIBE et REGISTER Actualiser et S'ABONNER Réessayer.*

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_VOICE_MAIL_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer la prise en charge de la messagerie vocale. Définissez sur « faux » pour désactiver la prise en charge de la messagerie vocale.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « faux », VVM est désactivé. Lorsque ce paramètre est défini sur « vrai », VVM est activé. Notez que la messagerie vocale activée = faux avant l'attribut VVM actuel est toujours utilisée pour la compatibilité ascendante.
%BWVOICE-PORTAL-NUMBER-1%	vide	numéro	Le client appelle ce numéro généralement spécifié à l'aide d'une balise système Cisco BroadWorks existante lors de la composition de la messagerie vocale.
%ENABLE_MWI_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer MWI. Définissez sur « faux » pour désactiver MWI.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%MWI_MODE_WXT%	vide	implicite, explicite	Définissez sur « explicite » pour envoyer SIP SUBSCRIBE au pack d'événements MWI lorsque MWI est activé. L'utilisation de « implicit » n'envoie pas un pack d'événements SIP SUBSCRIBE pour MWI lorsque MWI est activé. S'il reste vide, MWI est désactivé.

6.1.28 Transcription de la messagerie vocale pour Webex Calling

Grâce à cette fonctionnalité, les messages vocaux sont convertis en texte et affichés dans l'affichage visuel des messages vocaux dans les applications de bureau et mobiles Webex Calling.

La fonctionnalité ne doit être activée pour un utilisateur que si :

1. L'application est en cours d'exécution dans le déploiement de Webex Calling.
2. La fonctionnalité de messagerie vocale visuelle est activée pour l'utilisateur.
3. La fonctionnalité est activée dans la configuration (l'attribut activé dans la balise <services><messagerie vocale><transcription> doit être défini sur « true »).

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	false (faux)	vrai, faux	[Webex Calling uniquement] Contrôle la disponibilité de la transcription de la messagerie vocale uniquement si la messagerie vocale visuelle est activée.

6.1.29 Paramètres des appels

6.1.29.1 Renvoi d'appel Toujours

La balise personnalisée suivante peut être utilisée pour contrôler la disponibilité du service de toujours transfert d'appel Cisco BroadWorks dans le client Webex pour Cisco BroadWorks.

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false (faux)	vrai, faux	Contrôle la disponibilité du service Toujours renvoi d'appel. Par défaut, la fonctionnalité est désactivée.

REMARQUE : Le renvoi automatique d'appel et le renvoi d'appel vers la messagerie vocale (*6.1.29.2Transfert d'appel vers* la messagerie vocale) peuvent être utilisés ensemble pour afficher ou masquer le paramètre « Renvoi d'appel » dans les applications Webex. Lorsque les deux balises sont désactivées, le paramètre « Renvoi d'appel » dans les applications Webex est masqué.

6.1.29.2 Transfert d'appel vers la messagerie vocale

À partir de la version 43.9, l'application Webex fournit une option pour contrôler la disponibilité du transfert vers la messagerie vocale. Par défaut, la fonctionnalité est activée et l'option de configuration suivante peut être utilisée pour la désactiver.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	vrai	vrai, faux	Contrôle la disponibilité du transfert vers la messagerie vocale. Par défaut, la fonctionnalité est activée.

NOTA 1 : Cette fonctionnalité dépend de l'un des services « Utilisateur de messagerie vocale » ou « Prise en charge de la messagerie vocale par un tiers » à attribuer à l'utilisateur.

NOTE 2 : Le renvoi d'appel vers la messagerie vocale et le renvoi d'appel toujours (*6.1.29.1Renvoi d'appel* Toujours) peuvent être utilisés ensemble pour afficher ou masquer le paramètre « Renvoi d'appel » dans les applications Webex. Lorsque les deux balises sont désactivées, le paramètre « Renvoi d'appel » dans les applications Webex est masqué.

6.1.29.3 BroadWorks Anywhere (numéro d'appel unique)

Les balises personnalisées suivantes contrôlent la disponibilité de BroadWorks Anywhere et la disponibilité de ses paramètres dans le client Webex pour Cisco BroadWorks. Notez que le nom de cette fonctionnalité à l'intérieur du client est *Gérer mes numéros*.

```
<config>
```


Confidentiel à Cisco

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_BROADWORKS_ANYWHERE_WXT%	false (faux)	vrai, faux	Active BroadWorks Anywhere (BWA) au niveau de la configuration.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	vrai	vrai, faux	Contrôle si la Description de l'emplacement BWA doit être disponible pour l'utilisateur.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false (faux)	vrai, faux	Définissez sur « true » pour rendre Alert All Locations du service BWA disponible pour l'utilisateur. Définissez sur « faux » pour rendre l'alerte de tous les emplacements pour le service BWA indisponible pour l'utilisateur.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	false (faux)	vrai, faux	Contrôle si l'application doit activer l'état Alert All Locations, lors de l'ajout de deuxième ou de chaque nouvel emplacement BWA ultérieur.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false (faux)	vrai, faux	Contrôle si le contrôle d'appel de l'emplacement BWA doit être disponible pour l'utilisateur.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	false (faux)	vrai, faux	Contrôle l'état par défaut du contrôle d'appel pour l'emplacement BWA.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false (faux)	vrai, faux	Contrôle si l'inhibiteur de dérivation de l'emplacement BWA doit être disponible pour l'utilisateur.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false (faux)	vrai, faux	Contrôle l'état par défaut de l'inhibiteur de dérivation de l'emplacement BWA.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false (faux)	vrai, faux	Contrôle si la confirmation de réponse de l'emplacement BWA doit être disponible pour l'utilisateur.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	false (faux)	vrai, faux	Contrôle l'état par défaut de la confirmation de réponse de l'emplacement BWA.

Confidentiel à Cisco

6.1.30 Portail des paramètres et paramètres d'appel basés sur le Web

Le client Webex pour Cisco BroadWorks donne accès à un portail de paramètres (Self Care), dans lequel l'utilisateur peut configurer certains paramètres de l'application et du service.

En outre, le client offre la possibilité d'utiliser l'affichage Web des paramètres d'appel (CSWV) à la place. Cela permet à l'utilisateur de contrôler davantage de paramètres d'appel basés sur le serveur. Des balises séparées peuvent être utilisées pour contrôler si des services spécifiques doivent être visibles dans les paramètres d'appel basés sur le Web.

> **REMARQUE :** Il est conseillé de masquer les paramètres qui sont déjà visibles dans l'application comme Call Center (voir section *6.1.31Connexion/déconnexion du centre d'appels/de* la file d'attente d'appels) et BroadWorks Anywhere (voir section*6.1.29.3BroadWorks Anywhere*). Il est également conseillé de masquer le service Remote Office car il a été remplacé par le service BroadWorks Anywhere.

La balise personnalisée suivante peut être utilisée pour configurer l'URL du portail des paramètres (Self Care ou CSWV). Si la balise est vide, le lien vers le portail des paramètres n'est pas visible pour l'utilisateur dans l'application.

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


Confidentiel à Cisco

```
   <service name="Voice Messaging User"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
</web-call-settings>
```

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%WEB_CALL_SETTINGS_TARGET_WXT%	extérieur	externe, CSW	Contrôle le mode du portail d'administration. Définissez sur « externe »pour ouvrir l'URL du portail de configuration configuré dans un navigateur externe. Définissez sur « csw » pour ouvrir le portail CSW dans un navigateur intégré en utilisant la section paramètres supplémentaires <services><web-call-settings> pour former la demande POST.
%WEB_CALL_SETTINGS_URL_WXT%	vide	chaîne d'URL	URL du portail des paramètres. Exemple : https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Toujours renvoi d'appel doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Ne pas déranger (NPD) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de rejet d'appel anonyme (ACR) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de renvoi d'appel occupé (CFB) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de renvoi d'appel non accessible (CFNR) doit être visible pour l'utilisateur dans les paramètres basés sur le Web.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de renvoi d'appel sans réponse (CFNA) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Sonnerie personnelle simultanée (SIMRING) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de sonnerie séquentielle (SEQRING) doit être visible pour l'utilisateur dans les paramètres Web.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Remote Office (RO) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de rappel automatique (ACB) doit être visible pour l'utilisateur dans les paramètres basés sur le Web.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option d'appel en attente (CW) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option CLIDB (Calling Line ID Delivery Blocking) doit être visible pour l'utilisateur dans les paramètres basés sur le Web.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Assistant personnel (PA) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option BroadWorks Anywhere (BWA) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Call Center doit être visible pour l'utilisateur dans les paramètres basés sur le Web.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option BroadWorks Mobility (BWM) doit être visible pour l'utilisateur dans les paramètres basés sur le Web. Actuellement, la valeur recommandée est « faux » en raison de problèmes d'interopérabilité entre Webex pour Cisco BroadWorks et BroadWorks Mobility.
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de gestion vocale (VM) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false (faux)	vrai, faux	Contrôle si vous souhaitez utiliser la nouvelle charte graphique WebView des paramètres d'appel. Activez si la version CSWV côté serveur est 1.8.6 ou version plus récente. Sinon, gardez-le faux.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si les options des messages électroniques/vocaux sont visibles dans les paramètres basés sur le Web.
%USER_PORTAL_SETTINGS_URL_WXT%	vide	chaîne d'URL	Spécifie l'URL du portail des paramètres utilisateur. Pour activer la fonctionnalité et présenter le bouton Accéder au portail utilisateur dans l'interface utilisateur, cette balise personnalisée ne doit pas être vide. Par exemple : https://settings.webex.com.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USER_PORTAL_SETTINGS_TARGET_WXT%	extérieur	externe, interne	Indique si l'URL doit être ouverte dans un navigateur intégré ou externe.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false (faux)	vrai, faux	Applicable uniquement lorsque le navigateur intégré est configuré (USER_PORTAL_SETTINGS_TARGET_WXT=internal). Lorsque cette option est activée, la requête HTTP POST est utilisée et le jeton de courte durée BroadWorks est ajouté dans le cadre du CORPS. Lorsque cette option est désactivée, l'URL est ouverte avec HTTP GET.

NOTE 1 : L'URL des paramètres d'appel WebView doit toujours avoir un « / » de suite configuré. Par exemple : http(s)://<XSP-FQDN>/<CSW-Context-Path>/

NOTE 2 : La version minimum de l'application WebView Paramètres d'appel qui est prise en charge est 1.7.5.

Pour l'installation sur Cisco BroadWorks version 21.0, reportez-vous aux étapes supplémentaires décrites dans le *Guide de la solution Webex Pour CiscoBroadWorks*.

6.1.31 Connexion/déconnexion du centre d'appels/de la file d'attente d'appels

L'application Webex permet d'accéder aux paramètres de l'agent du centre d'appels (file d'attente d'appels). Si un utilisateur est provisionné pour le centre d'appels, cette fonctionnalité lui permet de se connecter à un centre d'appels et d'afficher les files d'attente d'appels disponibles, ainsi que de rejoindre/quitter les files d'attente et de définir l'état de distribution automatique des appels (ACD).

À partir de la version de bureau 42.8 et de la version mobile 42.12, l'agent du centre d'appels (file d'attente d'appels) n'est plus basé sur la vue Web des paramètres d'appel (voir section *6.1.30Portail des paramètres et paramètres d'appel* basés sur le Web). La configuration de l'agent du centre d'appels (file d'attente d'appels) est accessible via le pied de page du bureau et les paramètres de l'application Webex mobile.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_CENTER_WXT%	false (faux)	vrai, faux	Active la prise en charge du centre d'appels.

Confidentiel à Cisco

6.1.32 Racine et chemins XSI

Le client Webex pour Cisco BroadWorks utilise les balises suivantes pour contrôler le chemin XSI Root, Actions et Events s'ils doivent être configurés pour différer de ceux utilisés pour la connexion.

La principale raison de changer la racine XSI est de mettre en œuvre l'équilibrage de charge au niveau de la configuration, bien qu'il soit recommandé d'utiliser l'équilibrage de charge au niveau de la couche HTTP à la place.

Les chemins Events et Actions sont généralement modifiés en raison des exigences de charte graphique afin de supprimer la référence du domaine *com.broadsoft* des chemins URL des requêtes HTTP XSI effectuées par le client.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%XSI_ROOT_WXT%	Continue d'utiliser celui d'origine utilisé pour la récupération de la configuration.	chaîne d'URL	La racine XSI pour toutes les opérations XSI. Exemple : https://domaine.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	chaîne de caractères	Spécifie le chemin d'accès des actions XSI. Il doit commencer et se terminer par « / » et contenir uniquement le contexte des actions. Exemple : /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	chaîne de caractères	Spécifie le chemin d'accès des événements XSI. Il doit commencer et se terminer par « / » et contenir uniquement le contexte des événements. Exemple : /com.domain.xsi-events/

6.1.33 Canal d'événement XSI

Le canal XSI Event est utilisé pour divers services tels que :

- Commandes en cours d'appel XSI
- Notifications d'état des paramètres d'appel

Confidentiel à Cisco

- Enregistrement des appels

Le battement de cœur XSI Events est utilisé pour garder le canal d'événement XSI ouvert et l'intervalle de battement peut être spécifié à l'aide du paramètre suivant.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_XSI_EVENT_CHANNEL_WXT%	vrai	vrai, faux	Contrôle si la chaine XSI Event est activée. Il doit être défini sur « vrai » pour recevoir, par exemple, les événements liés au service de contrôle en cours d'appel. La valeur recommandée est « vrai ».
%CHANNEL_HEARTBEAT_WXT%	10 000	numéro	Ceci est le battement du canal XSI Event (en millisecondes). La valeur par défaut est « 10000 ».

6.1.34 Configuration du codec

Webex pour Cisco BroadWorks offre une variété de codecs audio et vidéo. Les listes respectives de codecs se trouvent sous *config/services/calls/* dans les sections *audio/codecs* et *vidéo/codecs*. La priorité de chaque codec peut être modifiée via la *priorité de l'attribut XML*,qui est une valeur comprise entre 0.0 (la plus basse) et 1.0 (la plus haute).

L'application Webex prend officiellement en charge les codecs suivants :

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

Confidentiel à Cisco

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

Le client prend en charge H.264 en tant que codec vidéo. L'attribut de résolution vidéo peut être utilisé pour définir l'une des valeurs disponibles suivantes : SUBQCIF, QCIF, CIF, 4CIF, VGA et HD.

Si le débit binaire n'est pas saisi dans la configuration, les valeurs de débit binaire par défaut sont utilisées. Les valeurs de débit binaire par défaut, par résolution et par fréquence d'images, sont répertoriées dans le tableau suivant.

Résolution	Taille de la vidéo *	IPS (images par seconde)	Valeurs de débit binaire par défaut par résolution et 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

***** Résolution vidéo maximale publiée. La résolution vidéo réelle au cours d'un appel entre deux clients Webex pour Cisco BroadWorks dépend des capacités des deux clients – elle sera la plus faible des deux et sera la même pour les deux clients.

La résolution vidéo pour un appel vidéo est négociée pendant la configuration de la session et est basée sur les capacités des deux terminaux. La résolution des appels vidéo est la même sur les deux terminaux. Autrement dit, si les points de terminaison Webex pour Cisco BroadWorks ont des capacités différentes (et prennent donc en charge des résolutions différentes), alors la résolution la plus faible est négociée pour l'appel. La résolution vidéo peut changer pendant un appel si les conditions du réseau se détériorent. Dans ce cas, les deux terminaux mobiles peuvent utiliser des résolutions vidéo différentes.

Le mode de mise en paquets peut être configuré pour être SingleNAL (0) ou Non entrelacé (1). Le modèle utilise SingleNAL par défaut (<packet-mode>0</packet-mode>).

La configuration de plusieurs événements téléphoniques est également prise en charge. Pendant la négociation de codec, le client envoie tous les codecs configurés, y compris plusieurs événements téléphoniques. Une fois le codec audio sélectionné, il recherche les événements téléphoniques dans l'offre. Si l'offre comporte l'événement téléphonique avec le taux d'échantillonnage du codec audio négocié, alors cet événement téléphonique est sélectionné. Sinon, le premier événement téléphonique de la liste est utilisé. S'il n'y a aucun événement téléphonique dans l'offre, des multifréquences bi-tonalités (DTMF) intra-bande sont utilisées.

Exemple de codecs configurés :

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

Si un codec audio avec un taux d'échantillonnage de 48 kbps est négocié, l'événement téléphonique avec charge utile 101 est utilisé.

6.1.35 Numérotation SIP-URI

Actuellement, la numérotation SIP-URI via BroadWorks n'est pas disponible et par défaut tous les appels SIP-URI sont acheminés via Locus, également connu sous le nom d'« appel gratuit ». Dans certains environnements, ce n'est pas souhaitable et ces appels doivent être bloqués.

REMARQUE : Ceci s'applique uniquement si l'appel Locus est désactivé. Ce n'est que dans ce cas que le blocage de la numérotation URI SIP fonctionne.

La configuration suivante fournit cette option.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	vrai	vrai, faux	Contrôle si l'URI SIP doit être acheminé via Locus (vrai) ou bloqué (faux).

6.1.36 Historique des appels sur tous les périphériques

Le client offre la possibilité de stocker et de récupérer l'historique des appels à partir du serveur au lieu de le stocker localement. De cette manière, l'historique des appels est unifié sur tous les périphériques.

REMARQUE : L'historique unifié des appels doit être activé en même temps côté client et serveur afin d'éviter l'absence d'historique des appels ou les enregistrements dupliqués.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false (faux)	vrai, faux	Contrôle si l'application doit utiliser l'historique des appels unifiés ou un appel côté client (local).

6.1.37 Désactiver les appels vidéo

La version 41.9 a ajouté la possibilité de désactiver les appels vidéo. Il existe des options de configuration distinctes pour contrôler cette fonctionnalité pour les appels VoIP BroadWorks et Locus (gratuits).

Lorsque la fonctionnalité est activée et que la balise de la fonctionnalité est définie sur « faux » :

- l'utilisateur ne verra pas le paramètre « Accepter les appels entrants avec ma vidéo activée »
- tous les appels vidéo entrants s'ils sont acceptés, seront des appels audio
- l'utilisateur ne pourra pas escalader un appel vidéo et les escalades vidéo seront automatiquement rejetées

Lorsque les appels vidéo sont activés, une nouvelle propriété de configuration est ajoutée pour contrôler la valeur par défaut du paramètre « Accepter les appels entrants avec ma vidéo activée ». Par défaut, cette fonctionnalité est activée pour Bureau et désactivée pour Mobile et Tablette.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SIP_VIDEOCALLS_WXT%	vrai	vrai, faux	Contrôle la disponibilité des appels vidéo SIP via BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	vrai	vrai, faux	Contrôle la disponibilité des appels vidéo Locus (gratuits).
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Bureau - vrai Mobile / Tablette - faux	vrai, faux	Contrôle la valeur par défaut du paramètre « Accepter les appels entrants avec ma vidéo activée ».

Confidentiel à Cisco

6.1.38 Appels d’urgence (911) - Création de rapports de localisation avec le fournisseur E911

Le client Webex de bureau et de tablette prend en charge la création de rapports de localisation E911 en utilisant RedSky, Intrado ou la bande passante comme fournisseur d’appel d’urgence E911 pour le déploiement Webex for BroadWorks. Le fournisseur E911 fournit une prise en charge de la localisation par périphérique (pour les applications de bureau et tablettes Webex et les périphériques MPP compatibles HELD) et un réseau qui achemine les appels d’urgence vers les centres de réponse de sécurité publique (PSAP) autour des États-Unis, de ses territoires (Guam, Porto Rico et les îles Vierges) et du Canada uniquement. Le service est activé sur une base par emplacement.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%EMERGENCY_DIALING_ ENABLE_REDSKY_WXT%	false (faux)	vrai, faux	Active la plateforme de localisation d’urgence du fournisseur E911.
%BWE911-PRIMARY-HELDURL%	vide	chaîne de caractères	Spécifie l'URL de la plateforme de localisation d'urgence du fournisseur E911 prenant en charge le protocole HELD.
%BWE911-CUSTOMERID%	vide	chaîne de caractères	L’ID du client (HeldOrgId, CompanyID) utilisé pour la demande HTTPS du fournisseur E911.
%BWE911-SECRETKEY%	vide	chaîne de caractères	Le secret pour authentifier la demande HTTPS du fournisseur E911.
%BWE911-EMERGENCY-NUMBER-LIST%	vide	Chaîne CSV	La liste des numéros d'urgence pris en charge par le fournisseur E911.
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (l’utilisateur ne sera pas invité à nouveau)	numéro [0 - 43200]	Délai d'expiration en minutes qui sera utilisé pour rappeler à l'utilisateur de mettre à jour l'emplacement d'urgence si l'emplacement actuel n'est pas saisi ou n'est pas valide. La valeur suggérée si vous décidez d'activer : 1440 (un jour).

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (l'utilisateur peut toujours annuler la boîte de dialogue)	nombre [-1 - 100]	Les heures auxquelles l'utilisateur est autorisé à fermer la boîte de dialogue d'emplacement avant que l'emplacement ne devienne obligatoire (c'est-à-dire qu'il ne peut pas fermer la fenêtre d'emplacement). Valeurs possibles : ▪ N = -1 (l'utilisateur peut toujours annuler la boîte de dialogue) ▪ N = 0 (l'utilisateur n'est pas autorisé à annuler la boîte de dialogue - emplacement obligatoire toujours) ▪ N > 0 (l'utilisateur est autorisé à annuler la boîte de dialogue N fois avant qu'elle ne devienne obligatoire)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	agressif, once_per_login	once_par_connexion	Définit le comportement d'incitation de l'emplacement E911. La valeur « agressive » affichera la boîte de dialogue à l'utilisateur sur chaque changement de réseau vers un emplacement inconnu, tandis que la valeur « once_per_login » affichera la boîte de dialogue une seule fois, évitant ainsi d'autres fenêtres contextuelles et distractions pour l'utilisateur.

NOTE 1 : Les balises BWE911-*** sont « Dynamic Built-in System Tags ». Pour plus d'informations, reportez-vous à la section *5.7Balises système intégré Cisco BroadWorks Dynamic*.

NOTE 2 : Si l'appel VOIP est désactivé, la seule valeur significative pour la séquence de numérotation d'urgence (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) est cs-only.

6.1.39 PAI comme identité

Pour les **appels entrants**, ce nouveau paramètre contrôle la priorité des en-têtes SIP From et P-Asserted-Identity (PAI), et ce qui doit être utilisé comme identité de ligne d'appel. S'il y a un en-tête X-BroadWorks-Remote-Party-Info dans le SIP INVITE entrant, il est utilisé avec priorité sur les en-têtes SIP From et PAI. S'il n'y a pas d'en-tête X-BroadWorks-Remote-Party-Info dans le SIP INVITE entrant, ce nouveau paramètre détermine si l'en-tête SIP From est prioritaire sur l'en-tête PAI ou vice versa.

Si l'attribut activé de la balise <use-pai-as-calling-identity> est défini sur « true », l'en-tête PAI est utilisé avec priorité sur l'en-tête De. Cette identité de l'appelant est utilisée pour résoudre le contact et le présenter à l'utilisateur.

Confidentiel à Cisco

Pour les **appels sortants**, cette logique n'est pas appliquée. Dans les réponses 18X, 200 OK, l'identité de la ligne connectée est reçue, de sorte que l'application Webex utilise toujours l'en-tête SIP PAI avec priorité.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false (faux)	vrai, faux	Contrôle si l'identité d'appel, présentée à l'utilisateur doit être extraite des en-têtes SIP From ou SIP P-Asserted-Identity. Définissez sur « true » pour utiliser l'en-tête PAI avec priorité.

6.1.40 Désactiver le partage d'écran

La version 42.5 ajoute la possibilité de contrôler la disponibilité du partage d'écran. Lorsque le partage d'écran est désactivé :

- l'utilisateur ne verra pas l'option permettant d'initier le partage d'écran lors des appels 1 à 1
- les demandes de partage d'écran entrantes sont rejetées et l'utilisateur verra un message d'information

Par défaut, cette fonctionnalité est activée.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SCREEN_SHARE_WXT%	vrai	vrai, faux	Indique si le partage d'écran doit être activé pour l'utilisateur.

6.1.41 Indication d'appel de spam

Lorsque le commutateur de fonctionnalité (par type de déploiement) est activé et que la fonctionnalité est activée dans le fichier de configuration, l'application Webex traite le nouveau paramètre indiquant l'état de vérification des appels indésirables, s'ils sont reçus dans le cadre de la notification push NewCall ou des enregistrements de l'historique des appels.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false (faux)	vrai, faux	Contrôle la disponibilité de l'indication d'appel indésirable dans l'écran d'appel entrant et l'historique des appels pour Webex Calling uniquement.

Confidentiel à Cisco

6.1.42 Suppression du bruit et extension de la bande passante pour les appels RTCP/mobiles

La suppression du bruit offre une meilleure expérience d'appel aux utilisateurs appelants lorsqu'ils parlent à des utilisateurs non-Webex sur des périphériques RTCP ou mobiles. Avec la version 43.12, la suppression du bruit est activée par défaut.

La version 44.2 de l'application Webex introduit de nouvelles améliorations de l'IA vocale pour les médias audio entrants pour les appels RTCP à bande étroite.

- Un nouvel algorithme d'extension de bande passante est ajouté pour améliorer la qualité audio en étendant la bande passante du spectre RTCP à bande étroite et en supprimant le bruit. La bande passante étendue augmentera l'intelligibilité et diminuera la fatigue d'écoute.
- L'algorithme de suppression du bruit déjà existant a été amélioré, supprimant les limites pour la musique d'attente et les autres tonalités audio (par ex. les signaux sonores).
- Lorsque cette fonctionnalité est activée, les utilisateurs voient l'indicateur « Audio intelligent – externe » et peuvent contrôler les améliorations de l'IA vocale pour les médias audio entrants.

Par défaut, ces améliorations vocales sont activées et activées. L'utilisateur peut contrôler l'état initial via les paramètres audio intelligents dans les préférences audio.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	false (faux)	vrai, faux	Active les améliorations vocales pour les médias externes (entrants).

REMARQUE : La suppression du bruit fait maintenant partie des améliorations vocales supplémentaires, et la balise <noise-removal> a été obsolète par la nouvelle balise <speech-enhancements>. La balise personnalisée de suppression du bruit %ENABLE_NOISE_REMOVAL_WXT% est également obsolète.

6.1.43 Marquage DSCP QoS

Le marquage DSCP QoS est pris en charge avec les paquets RTP média d'appel de l'application Webex (audio et vidéo). DSCP détermine la classification du trafic pour les données réseau. Cela peut être utilisé pour déterminer quel trafic réseau nécessite une bande passante plus élevée, a une priorité plus élevée et est plus susceptible de supprimer des paquets.

Confidentiel à Cisco

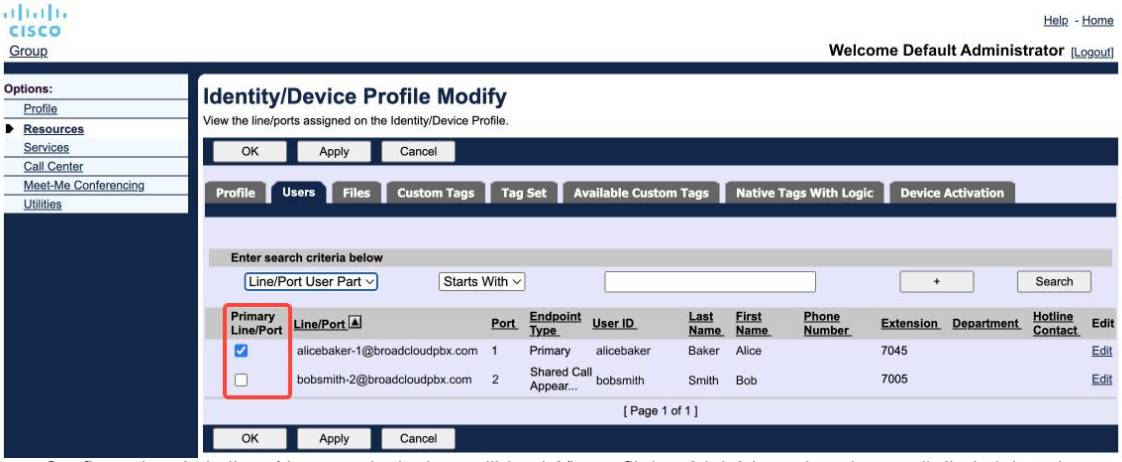
REMARQUE : Les versions récentes du système d'exploitation Microsoft Windows ne permettent pas aux applications de configurer directement DSCP ou UP sur les paquets sortants, nécessitant plutôt le déploiement d'objets de stratégie de groupe (GPO) pour définir des politiques de marquage DSCP basées sur les plages de ports UDP.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_AUDIO_QOS_WXT%	vrai	vrai, faux	Active la QoS pour les appels audio.
%AUDIO_QOS_VALUE_WXT%	46	0 à 63	Spécifie la valeur QoS pour le type QoS sélectionné pour les appels audio. Remarque : La valeur par défaut est utilisée, si aucune valeur n'est fournie, ou si la valeur n'a pas pu être analysée avec succès.
%ENABLE_VIDEO_QOS_WXT%	vrai	vrai, faux	Active la QoS pour les appels vidéo
%VIDEO_QOS_VALUE_WXT%	34	0 à 63	Spécifie la valeur QoS pour le type QoS sélectionné pour les appels vidéo. Remarque : La valeur par défaut est utilisée, si aucune valeur n'est fournie, ou si la valeur n'a pas pu être analysée avec succès.

6.1.44 Profil principal

Avec l'intégration des lignes Partagées (*6.2.12Multiligne - Apparence de* ligne partagée), si la ligne de l'utilisateur est partagée avec un autre utilisateur, il peut y avoir plusieurs profils de même type configurés pour l'utilisateur. Pour sélectionner le profil correct pour se connecter aux services téléphoniques, Cisco BroadWorks a été amélioré pour indiquer si un utilisateur possède un périphérique, c'est-à-dire qu'il se voit attribuer la ligne/le port principal d'un périphérique - pour plus d'informations sur la mise à jour Cisco BroadWorks, consultez Indicateur de propriétaire dans la liste des périphériques pour prendre en charge les lignes partagées du client Webex.

Confidentiel à Cisco



Configuration de la ligne/du port principal pour l'identité/le profil du périphérique dans le portail d'administration

À partir de la version 43.2, une nouvelle option de configuration (*device-owner-restriction*) est ajoutée pour contrôler si la restriction du profil principal doit être appliquée. Il peut être utilisé pour permettre à l'application Webex d'utiliser un profil de ligne/port non principal pour se connecter aux services téléphoniques. Cette option de configuration est appliquée à toutes les configurations, quel que soit le nombre de profils configurés pour l'utilisateur (**si la restriction de propriété du périphérique est activée et qu'il n'y a pas de périphérique avec ligne/port principal pour la plate-forme correspondante, les services téléphoniques ne se connecteront pas**).

La même restriction s'applique aux périphériques avec lesquels l'utilisateur peut s'appairer dans l'application de bureau Webex. L'utilisateur ne peut voir et s'appairer qu'avec les périphériques dont il est propriétaire. Ceci empêche l'appairage avec les périphériques d'un autre utilisateur auquel une ligne partagée ou virtuelle a été attribuée. La valeur du même paramètre de configuration s'applique également à cette restriction.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	vrai	vrai, faux	Contrôle la restriction du propriétaire du périphérique – si les services téléphoniques doivent utiliser le profil principal du périphérique donné

REMARQUE : Il est recommandé d'activer la restriction du propriétaire. S'ils sont désactivés, les services téléphoniques utilisent le premier profil trouvé pour se connecter et certains problèmes peuvent se produire s'il existe plusieurs profils configurés pour l'utilisateur du même type.

Confidentiel à Cisco

6.1.45 Liste de blocage (Webex Calling uniquement)

À partir de la version 43.5, l'application Webex introduit la liste de blocage des numéros de téléphone définie par l'utilisateur. Si la fonctionnalité est activée, l'utilisateur peut spécifier que les appels entrants provenant de numéros spécifiques doivent être bloqués côté serveur et ne pas être livrés sur l'un des périphériques de l'utilisateur. L'utilisateur peut voir ces appels bloqués dans l'historique des appels.

L'utilisateur peut configurer la liste de blocage à partir de deux emplacements : Préférences d'appel et Historique des appels. Dans les Préférences, l'utilisateur peut voir la liste des numéros bloqués et la modifier. Dans l'historique des appels, l'utilisateur peut voir les enregistrements de l'historique des appels bloqués par la liste de blocage définie par l'utilisateur. Ces enregistrements ont une indication Bloqué si le numéro figure dans la liste de blocage définie par l'utilisateur et l'utilisateur aura la possibilité de débloquer le numéro directement pour l'enregistrement donné. L'option Bloquer est également disponible.

Règles pour les numéros ajoutés à la liste de blocage définie par l'utilisateur :

- Format du numéro
  - Le blocage à partir des préférences d'appel applique la restriction du format E.164 localement dans l'application Webex
  - Le blocage dans l'historique des appels est autorisé pour tous les enregistrements Webex Calling
  - Cisco BroadWorks peut autoriser ou rejeter les demandes de nouveaux numéros ajoutés dans la liste de blocage en fonction du format des numéros
- Numéros internes : les appels entrants provenant de numéros internes seront transmis à l'utilisateur, même s'ils font partie de la liste de blocage définie par l'utilisateur

La liste de blocage définie par l'utilisateur est configurée sur Cisco BroadWorks et est appliquée à tous les périphériques WxC pour l'utilisateur. Cette fonctionnalité fonctionne avec la liste de blocage définie par l'administrateur, qui n'est pas configurable par l'utilisateur et ne peut être contrôlée que par les administrateurs via le Control Hub. Il n'y a AUCUN enregistrement d'historique des appels pour les appels entrants bloqués par la liste de blocage définie par l'administrateur.

La liste de blocage définie par l'utilisateur est appliquée après STIR/SHAKEN, la liste de blocage définie par l'administrateur et les politiques de rejet d'appel anonyme.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_BLOCK_WXT%	vrai	vrai, faux	Active la liste de blocage définie par l'utilisateur Définissez sur « vrai », pour afficher la liste de blocage dans les préférences d'appel et l'historique des appels

Confidentiel à Cisco

REMARQUE : Cette fonctionnalité dépend du service de blocage d'appels Cisco BroadWorks attribué à l'utilisateur.

6.1.46 Adaptation des médias et mise en œuvre de la résilience (MARI)

6.1.46.1 Adaptation du tarif

L’application Webex a déjà intégré des techniques adaptatives de qualité média pour s’assurer que l’audio n’est pas affecté par une perte de paquets vidéo, et pour s’assurer que la vidéo peut tirer parti de l’adaptation du débit vidéo pour gérer la quantité de bande passante utilisée pendant les périodes d’encombrement.

L'adaptation de débit ou les ajustements de débit binaire dynamique permettent d'adapter le débit d'appel à la largeur de bande variable disponible, d'abaisser ou d'augmenter le débit binaire vidéo en fonction de la condition de perte de paquets. Un terminal réduit le débit binaire lorsqu'il reçoit des messages du récepteur indiquant qu'il y a une perte de paquets; et une fois que la perte de paquets a diminué, le débit binaire augmente.

Il n'y a pas de paramètres configurables pour contrôler l'utilisation du mécanisme d'adaptation de taux.

6.1.46.2 Correction d’erreur directe (FEC) et retransmission de paquets (RTX)

À partir de la version 43.4, l’application Webex ajoute au mécanisme d’adaptation des médias la prise en charge de la correction d’erreur directe (FEC) et de la retransmission de paquets (RTX) pour les médias audio et vidéo.

FEC assure la redondance des informations transmises au moyen d'un algorithme prédéterminé. La redondance permet au récepteur de détecter et de corriger un nombre limité d'erreurs, sans avoir à demander des données supplémentaires à l'expéditeur. FEC donne au récepteur la possibilité de corriger les erreurs sans avoir besoin d'un canal inverse (tel que RTCP) pour demander la retransmission de données, mais cet avantage se fait au prix d'une bande passante supérieure fixe (plus de paquets envoyés).

Les terminaux n'utilisent pas FEC sur des largeurs de bande inférieures à 768 Kbps. En outre, il doit également y avoir une perte de paquets d'au moins 1,5 % avant l'introduction du FEC. Les critères d’évaluation surveillent généralement l’efficacité du FEC et si le FEC n’est pas efficace, il n’est pas utilisé.

FEC consomme plus de bande passante que la retransmission mais a moins de délai. Le RTX est utilisé lorsqu’un petit délai est autorisé et qu’il existe des contraintes de bande passante. En cas de retard important et de bande passante suffisante, FEC est préférable.

L’application Webex sélectionne dynamiquement RTX ou FEC en fonction de la bande passante négociée et de la tolérance de délai pour un flux média donné. Le FEC entraîne une utilisation plus élevée de la bande passante en raison de données vidéo redondantes, mais il n’introduit pas de délai supplémentaire pour récupérer les paquets perdus. Alors que RTX ne contribue pas à une utilisation plus élevée de la bande passante, car les paquets RTP sont retransmis uniquement lorsque le récepteur indique une perte de paquets dans le canal de retour RTCP. Le RTX introduit un délai de récupération de paquets en raison du temps nécessaire pour que le paquet RTCP atteigne le récepteur depuis l'expéditeur et pour que le paquet retransmis atteigne le récepteur depuis l'expéditeur.

FEC doit être activé pour que le RTX soit activé.

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_AUDIO_MARI_FEC_WXT%	false (faux)	vrai, faux	Active FEC pour les appels audio
%ENABLE_AUDIO_MARI_RTX_WXT%	false (faux)	vrai, faux	Active le RTX pour les appels audio (nécessite un FEC audio activé)
%ENABLE_VIDEO_MARI_FEC_WXT%	false (faux)	vrai, faux	Active FEC pour les appels vidéo
%ENABLE_VIDEO_MARI_RTX_WXT%	false (faux)	vrai, faux	Active le RTX pour les appels vidéo (nécessite l'activation du FEC vidéo)

6.1.47 Appels simultanés avec le même utilisateur

Ajout de la prise en charge des appels simultanés avec le même utilisateur sur un seul périphérique.

Cette fonctionnalité est utile pour certains déploiements, où l'identité présentée de l'appel n'est pas la même que l'identité connectée. Cela conduit à l'impossibilité d'initier un transfert assisté vers la partie initiale. En activant cette fonctionnalité, l'utilisateur sera en mesure de traiter plusieurs appels simultanés avec le même interlocuteur distant.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false (faux)	vrai, faux	Indique si l'application Webex peut avoir un seul ou plusieurs appels WxC avec le même utilisateur.

6.1.48 RTCP-XR

À partir de la version 43.8, l'application Webex ajoute la négociation pour l'échange de paquets RTCP-XR au cours d'un appel. La négociation se déroule pendant l'établissement de la session SIP INVITE. Si les deux terminaux prennent en charge les paquets RTCP-XR, le moteur média Webex commencera à échanger ces paquets et aidera le mécanisme adaptatif de qualité d'appel. Cette fonction est activée par défaut.

Confidentiel à Cisco

En outre, pour Webex Calling uniquement, ces mesures supplémentaires seront envoyées via le SIP BYE et exposées de cette manière dans le Control Hub.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	vrai	vrai, faux	Permet la négociation RTCP-XR et l'échange de paquets pour une meilleure qualité d'appel. Option activée par défaut.

6.1.49 Informations sur le transfert d'appel

La version 44.2 de l'application Webex introduit une option configurable pour contrôler la visibilité des informations de transfert et de redirection d'appel dans les écrans et l'historique des appels liés aux appels.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	vrai	vrai, faux	Contrôle la visibilité des informations de transfert et de redirection d'appel. Définissez sur « vrai » pour afficher les informations dans les écrans relatifs aux appels et l'historique des appels.

REMARQUE : Cette fonctionnalité nécessite que les informations de redirection (Diversion ou History-Info) soient activées du côté de Cisco BroadWorks.

6.1.50 ID de l'appelant

6.1.50.1 ID de l'appelant sortant (Webex Calling uniquement)

Les applications Webex Mobile (version 44.2) et Desktop (version 44.3) introduisent une nouvelle fonction permettant à l'utilisateur de choisir l'ID d'appelant externe préféré pour les appels sortants. La liste des options disponibles comprend :

- Ligne directe (valeur par défaut)

Confidentiel à Cisco

- Numéro de l'emplacement
- Numéro personnalisé de la même organisation
- Listes des appels en attente dont fait partie l'utilisateur, ce qui permet aux agents d'utiliser leur numéro d'identification de l'appelant
- Groupes de recherche dont l'utilisateur fait partie, ce qui permet aux agents d'utiliser leur numéro d'identification de l'appelant
- Masquer l'ID de l'appelant

Remarques :

- Webex Calling uniquement
- La liste des options dépend de la ligne :
  - Ligne principale – ensemble complet d'options
  - Lignes partagées – non disponible
  - Lignes virtuelles – uniquement les options de file d'attente d'appels
- Si l'identité déjà sélectionnée n'est plus disponible, l'ID appelant par défaut de l'utilisateur est utilisé
- Les appels d'urgence utilisent toujours le numéro de rappel d'urgence de l'utilisateur
- Déprécie la balise <appels sortants> sous la section <services><call-center-agent>

La liste des options disponibles est configurable via le portail d'administration. Il existe également des balises DMS personnalisées distinctes pour contrôler la disponibilité de ces améliorations dans l'application Webex.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false (faux)	vrai, faux	Active la sélection du numéro d'identification de la ligne appelante pour les appels sortants.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	false (faux)	vrai, faux	Contrôle la disponibilité des numéros supplémentaires configurés pour l'utilisateur.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	false (faux)	vrai, faux	Contrôle la disponibilité des numéros du centre d'appel (DNIS) configurés pour l'utilisateur.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false (faux)	vrai, faux	Contrôle la disponibilité des numéros de groupe de recherche configurés pour l'utilisateur.
"%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false (faux)	vrai, faux	Active le blocage de la transmission de l'ID de l'appelant en tant que sélection pour les appels sortants.

REMARQUE : La version 44.3 de l'application de bureau prend en charge uniquement Call Center CLID et la version 44.4 ajoute la prise en charge du reste des options.

6.1.50.2 Nom de l'ID de l'appelant distant

Lors de la réception/du lancement d'un appel, Cisco BroadWorks envoie le nom d'affichage de l'interlocuteur distant dans l'INVITE SIP. Elle est utilisée par défaut par l'application Webex. En même temps, l'application Webex démarre la résolution des contacts par rapport à plusieurs sources, avec la priorité suivante :

- Identité commune (IC)
- Service de contact (contacts personnalisés)
- Contacts Outlook (Bureau)
- Carnet d'adresses local (Mobile)

En cas de résolution de contact réussie par rapport à l'une des sources de recherche, le nom d'affichage de l'interlocuteur distant est mis à jour. De plus, si le contact est trouvé dans CI, la session d'appel est liée aux services du Cloud Webex du même utilisateur, ce qui offre l'option de voir l'avatar et la présence de l'interlocuteur distant, d'avoir une conversation instantanée, de partager l'écran, l'option de transfert vers une réunion du Cloud Webex, etc.

La version 44.5 de l'application Webex ajoute une option configurable pour ignorer la résolution des contacts et toujours conserver le nom d'affichage Cisco BroadWorks pour les appels avec des espaces de travail ou des périphériques RoomOS utilisés pour un appel 1:1 Cisco BroadWorks.

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	résolu(s)	résolu, sip	Contrôle le nom d'affichage de la partie distante pour les espaces de travail et les périphériques RoomOS. Utilisez « sip » pour ignorer la résolution des contacts et utiliser le nom d'affichage reçu lors de la session SIP INVITE.

Confidentiel à Cisco

6.2 Fonctionnalités du bureau uniquement

6.2.1 Déconnexion forcée

Cette fonctionnalité permet à Cisco BroadWorks de suivre les instances des clients en ligne avec le même type de périphérique et de n'autoriser qu'une seule d'entre elles à être en ligne à la fois. Lorsque Cisco BroadWorks notifie au client de se déconnecter, la connexion SIP est interrompue et le client indique que l'appel n'est pas connecté.

Cette fonctionnalité est nécessaire dans certains déploiements où des clients similaires peuvent être autrement en ligne en même temps, causant des effets secondaires. Un exemple est un utilisateur avec une machine de bureau au travail et à la maison, où les appels entrants ne seraient reçus que par l'un des clients, en fonction de l'enregistrement SIP actif.

La déconnexion forcée est basée sur SIP, le client envoie un SIP SUBSCRIBE au package d'événements *call-info* avec une *appid-value* spéciale dans l'en-tête *De*, quelle que soit la valeur du paramètre *bsoft-call-info*. Lorsque Cisco BroadWorks détecte plusieurs instances client en ligne avec le même *appid*, il envoie une notification SIP NOTIFY spéciale à l'ancienne instance client, ce qui provoque sa déconnexion. Par exemple, les clients de bureau auraient une *valeur appid* identique bien qu'il n'y ait aucune restriction concernant l'utilisation de cet identifiant côté client. La *valeur appid* est configurée par le fournisseur de services.

Notez que pour utiliser la déconnexion forcée, l'abonnement SIP *Info-appel* doit être activé.

Pour plus d'informations sur les correctifs et versions Cisco BroadWorks nécessaires pour cette fonctionnalité, reportez-vous à la section sur la configuration minimale du logiciel Cisco BroadWorks requise dans le *Guide de la solution Webex pour Cisco BroadWorks*.

Voir l'exemple suivant pour les détails de configuration (SIP est le seul protocole de contrôle pris en charge dans cette version).

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_FORCED_ LOGOUT_WXT%	false (faux)	vrai, faux	Active la déconnexion forcée.
%FORCED_LOGOUT_ APPID_WXT%	vide	chaîne de caractères	Appid utilisé côté serveur pour la corrélation. Cela peut être n'importe quelle chaîne. Exemple : “123abc”

6.2.2 Prise d’appel

L’interception d’appels est un service multi-utilisateurs qui permet aux utilisateurs sélectionnés de répondre à n’importe quelle ligne de sonnerie dans leur groupe d’interception d’appels. Un groupe de prise d’appels est défini par l’administrateur et est un sous-ensemble des utilisateurs du groupe qui peuvent prendre les appels des autres.

Confidentiel à Cisco

Les cas de prise en charge suivants sont pris en charge :

- Interception d'appels aveugle
- Interception d'appels dirigée (qui permet à un utilisateur de répondre à un appel dirigé vers un autre téléphone de son groupe en composant le code d'accès à la fonctionnalité respective, suivi du numéro de poste du téléphone qui sonne).

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_PICKUP_BLIND_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer l'interception d'appels aveugle.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer l'interception d'appels dirigée.

6.2.3 Prise en charge Boss-Admin (Cadre de direction-Assistant)

La fonctionnalité Boss-Admin, connue sous le nom de Cadre de direction-Assistant sur Cisco BroadWorks, permet à unassistant de fonctionner pour le compte d'un cadre de direction pour filtrer, répondre et passer des appels en tant que « cadre de direction ». Un assistant peut avoir plusieurs cadres et il est possible de :

- Sélectionnez le rôle souhaité lorsque vous passez un appel.
- Répondre à un appel entrant pour le compte d'un cadre de direction, puis transmettre l'appel au cadre de direction. En outre, toutes les options habituelles de gestion des appels sont disponibles.
- Vérifiez qu'un appel entrant est en fait destiné au cadre de direction.

Cadre de direction et Cadre de direction-Assistant sont deux services Cisco BroadWorks interdépendants qui fournissent ensemble les fonctionnalités suivantes :

- Un utilisateur disposant du service Cadre de direction peut définir un groupe d'assistants qui gèrent leurs appels. Les assistants doivent être sélectionnés parmi les utilisateurs du même groupe ou de la même entreprise auxquels le service Cadre de direction-Assistant a été attribué.
- Un utilisateur disposant du service Cadre de direction-Assistant peut répondre et lancer des appels pour le compte de ses cadres de direction.
- Le cadre de direction et ses assistants peuvent spécifier quels appels doivent être transférés aux assistants, comment les assistants doivent être alertés sur les appels entrants et lesquels des appels transférés aux assistants doivent être présentés au cadre de direction pour vérification.

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


Confidentiel à Cisco

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer la fonctionnalité Boss-Admin.

REMARQUE : La prise en charge de la fonctionnalité Boss-Admin (Cadre de direction-Assistant) n'est pas disponible en combinaison avec les lignes partagées.

6.2.4 Transférer les appels SIP vers une réunion (Webex Calling uniquement)

Le client fournit la fonctionnalité pour faire remonter un appel SIP en cours à une réunion via Webex Calling. En utilisant cette fonctionnalité au lieu d'une conférence ad hoc standard, l'utilisateur pourra utiliser la vidéo ainsi que le partage d'écran au cours de la réunion.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer l'option du menu Escalader vers la réunion Webex.

6.2.5 Appel de contrôle du téléphone de bureau – Réponse automatique

La fonction de réponse automatique permet à l'utilisateur d'utiliser le contrôle du téléphone de bureau (DPC) pour les appels sortants sur le client afin de gérer les téléphones MPP avec une réponse sans contact.

Le téléphone MPP sélectionné transportera l'audio/vidéo pour l'appel DPC sortant.

La réponse automatique peut fonctionner sur les périphériques mis à disposition principaux et non principaux. Si l'utilisateur dispose de plusieurs téléphones de bureau enregistrés qui peuvent être appairés, seul le périphérique sélectionné/appairé répond automatiquement.

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	vrai	vrai, faux	Lorsque ce paramètre est défini sur « vrai », active la fonction de réponse automatique du contrôle du téléphone de bureau.

REMARQUE : La réponse automatique n'affectera pas les appels entrants en mode DPC, de sorte que le téléphone de bureau sonne pour les appels entrants.

6.2.6 Réponse automatique avec notification de tonalité

Cette fonctionnalité permet la prise en charge automatique de la réponse aux appels entrants pour les périphériques locaux, si cela est indiqué dans la demande d'appel entrant.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_AUTO_ANSWER_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « vrai », active la réponse automatique aux appels entrants si elle est demandée par le serveur principal.

6.2.7 Contrôle du téléphone de bureau – Commandes en cours d'appel – Conférence

Cette fonctionnalité active les options de conférence et de fusion pour les appels distants (XSI), terminés sur un autre emplacement.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « vrai », active les options de conférence et de fusion pour les appels distants (XSI), terminés sur un autre emplacement.

6.2.8 Notifications d’interception d’appels

Les notifications d’interception d’appels permettent à l’utilisateur de savoir quand il y a un appel entrant vers un utilisateur qu’il est configuré pour surveiller. Des notifications d’interception d’appels peuvent être reçues pour les listes de surveillance configurées par le biais du groupe d’interception d’appels et des services de voyant d’occupation de ligne (BLF).

Confidentiel à Cisco

Les notifications d'interception d'appels sont utiles lorsque les utilisateurs surveillés ne sont pas physiquement proches les uns des autres et ne peuvent pas entendre la sonnerie du téléphone de leur collègue.

6.2.8.1 Voyant d'occupation de ligne (BLF)

L'application de bureau Webex affiche une notification si un membre de sa liste de surveillance FLO (Busy Lamp Field) a un appel entrant en état d'alerte. La notification contient des informations sur l'appelant et l'utilisateur qui a reçu l'appel entrant, avec les options permettant de prendre l'appel, de couper le son ou d'ignorer la notification. Répondre à l'appel entrant par l'utilisateur initie une interception d'appel dirigée.

À partir de la version 43.4, la liste des utilisateurs surveillés par FLO est disponible dans la fenêtre d'appel multiple (MCW) pour Calling (disponible uniquement pour Windows). L'intégration de la liste FLO dans le MCW comprend :

- Surveillez les appels entrants avec la possibilité de prendre l'appel ou d'ignorer l'alerte.
- Voir la liste complète des utilisateurs FLO.
- Surveillez la présence des utilisateurs – une présence riche est disponible uniquement pour les utilisateurs disposant d'un droit Webex Cloud. La présence de base (téléphonie) n'est disponible que pour les utilisateurs BroadWorks uniquement.
- Démarrer un appel avec un utilisateur FLO.
- Démarrer une conversation instantanée avec un utilisateur FLO – disponible uniquement pour les utilisateurs disposant d'un droit Webex Cloud.
- Ajouter un utilisateur FLO en tant que contact.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_BUSY_LAMP_FIELD_WXT%	false (faux)	vrai, faux	Active la surveillance du voyant d'occupation de ligne (BLF) et la notification de sonnerie pour les autres utilisateurs avec la possibilité de prendre les appels.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	vrai	vrai, faux	Permet d'afficher le nom/le numéro d'affichage de l'appelant dans la notification de sonnerie.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0 à 60	Contrôle le nombre de secondes pendant lesquelles la notification de sonnerie doit être retardée avant qu'elle ne soit affichée à l'utilisateur.

Confidentiel à Cisco

REMARQUE : Cette fonctionnalité dépend du service d'interception d'appels dirigée.

6.2.8.2 Groupe d'interception d'appels (Webex Calling uniquement)

À partir de la version 44.2, l'application Webex ajoute la prise en charge des notifications d'interception d'appels de groupe (GCP) pour le déploiement de Webex Calling. Il permet aux utilisateurs d'être informés des appels entrants pour tous les utilisateurs surveillés via le groupe d'interception d'appels.

En cas d'appel entrant pour un utilisateur faisant partie d'un groupe d'interception d'appels, l'appelé a la possibilité de répondre à l'appel. Il existe un délai de notification GCP configurable via le Control Hub. Si l'appelé ne traite pas l'appel dans le délai configuré, une notification GCP est envoyée au groupe.

En cas de plusieurs appels dans le même groupe d'interception d'appels, ils sont traités séquentiellement en fonction de l'heure de réception. La notification de l'appel le plus ancien est initialement transmise au groupe et une fois qu'il est traité, la notification suivante en ligne est transmise au groupe.

Les notifications peuvent être audio uniquement, visuelles uniquement ou audio et visuelles en fonction de la configuration du portail d'administration du Control Hub. S'il y a une notification visuelle GCP, l'utilisateur peut intercepter l'appel à l'aide de la fonctionnalité d'interception d'appels. Si la notification audio uniquement est configurée, l'utilisateur ne voit pas de notification visuelle pour l'appel entrant, entend une sonnerie spécifique et peut prendre l'appel à partir du menu Prise d'appel disponible dans l'application Webex, ou en composant le code FAC (*98) et le numéro de poste manuellement.

L'utilisateur peut couper le son de la notification GCP via les paramètres de l'application. Ce paramètre s'applique à toutes les notifications d'interception d'appels (FLO et GCP) et par défaut, le son des notifications est coupé.

La fonctionnalité fonctionne pour les lignes principales et pour les lignes partagées ou virtuelles attribuées à l'utilisateur.

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_GCP_NOTIFICATIONS_WXT%	false (faux)	vrai, faux	Active les notifications d'interception d'appels de groupe
%ENABLE_GCP_DISPLAY_CALLER_WXT%	vrai	vrai, faux	Permet d'afficher le nom/le numéro d'affichage de l'appelant dans la notification de sonnerie
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5 à 120	Définit la durée maximale pendant laquelle une notification GCP est disponible pour l'utilisateur
%BWGROUP-CALL-PICKUP-BOOL-n%	false (faux)	vrai, faux	Indique si la ligne correspondante a un groupe d'interception d'appels configuré

NOTA 1 : Il s'agit d'une fonctionnalité Webex Calling uniquement.

NOTE 2 : Cette fonctionnalité dépend du groupe d'interception d'appels configuré pour l'utilisateur.

6.2.9 Pack d'événements de contrôle à distance

Pour les clients Click to Dial tels que le client léger BroadWorks Receptionist et l'intégrateur Go où l'application Webex est le périphérique d'appel, lorsque vous recevez un appel ou que vous traitez la mise en attente/reprise, l'application Webex honore désormais l'ensemble des événements de contrôle à distance.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « vrai », indique que la télécommande doit être activée pour l'utilisateur.

6.2.10 Sélection CLID de l'agent de la file d'attente d'appels

Lorsque les agents passent des appels à leurs clients, ils souhaitent que les clients voient l'ID de ligne d'appel approprié (CLID) plutôt que leur CLID personnel/d'entreprise. Par exemple, si l'agent Mary Smith est joint à la file d'attente d'appels de l'assistance technique, alors lors de l'appel des clients, Mary souhaite que les clients voient son CLID comme l'assistance technique, et non comme Mary Smith.

Les administrateurs de Control Hub ou CommPilot peuvent spécifier pour une file d'attente d'appels un ou plusieurs numéros DNIS à utiliser pour le CLID sortant. Les agents ont ensuite la possibilité de sélectionner l'un des numéros DNIS à utiliser comme CLID lorsqu'ils effectuent des appels sortants. L'application Webex permet aux agents de sélectionner le DNIS à utiliser comme CLID.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%	false (faux)	vrai, faux	Active les appels sortants (sélection CLID) pour le compte de la file d'attente du centre d'appels.

6.2.11 Passerelle de survivabilité (Webex Calling uniquement)

À partir de la version 43.2, l'application Webex ajoute la prise en charge du mode d'appel de survivabilité. Si la fonctionnalité est activée et qu'il n'y a pas de connectivité Webex Cloud, l'application Webex peut fonctionner en mode de survivabilité. Dans ce mode, les fonctionnalités d'appel disponibles pour l'utilisateur sont limitées.

La passerelle de survivabilité locale est déployée par le client.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false (faux)	vrai, faux	Active la prise en charge du mode de survivabilité.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Spécifie le temps de secours (passerelle de survivabilité vers SSE)

REMARQUE : Cette fonctionnalité fournit une confiance dans la migration des solutions d'appels sur site vers le Cloud.

6.2.12 Multiligne - Apparence de ligne partagée

À partir de la version 42.12, l'application Webex ajoute la prise en charge de plusieurs lignes. Un utilisateur Webex peut avoir une ligne principale et jusqu'à 9 lignes de partage avec d'autres utilisateurs.

L'administrateur doit configurer les apparences d'appels partagés pour chaque ligne partagée.

Le client Webex détectera les mises à jour de la configuration de la ligne dans les 12 heures et demandera à l'utilisateur de redémarrer l'application. La reconnexion de l'utilisateur appliquera immédiatement les mises à jour de la ligne.

Confidentiel à Cisco

À partir de la version 43.12, l'application Webex est améliorée pour permettre le déplacement (reprise locale) d'un appel en attente sur une ligne partagée, traité par un autre utilisateur ou par le même utilisateur sur un autre périphérique. Pour plus d'informations, consultez *6.2.15Déplacer l'appel*.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_MULTI_LINE_WXT%	false (faux)	vrai, faux	Permet la prise en charge de plusieurs lignes (si configurées). Si cette option est désactivée (définie sur « false »), seule la première ligne configurée sera utilisée par l'application.

NOTE 1 : La fonctionnalité Prise en charge du boss-admin (Assistant de direction) n'est pas disponible en combinaison avec les lignes partagées.

NOTE 2 : Voir « Apparence de ligne partagée » dans le Guide de la solution Webex-pour-Cisco-BroadWorks pour des exigences supplémentaires de BroadWorks.

6.2.13 Multi-lignes - Lignes virtuelles (Webex Calling uniquement)

Pour le déploiement de Webex Calling uniquement, l'application Webex prend en charge la configuration multi-lignes à l'aide de lignes virtuelles. Fonctionnellement, la configuration avec les lignes virtuelles correspond à la multiligne utilisant des lignes partagées – ayant la possibilité de voir les lignes virtuelles configurées pour l'utilisateur et de les utiliser pour les appels entrants et sortants. Un maximum de 10 lignes virtuelles combinées et lignes partagées peuvent être configurées.

La version 43.4 étend la prise en charge des lignes virtuelles et ajoute le parcage d'appels et le parcage d'appels récupérés.

À partir de la version 43.12, l'application Webex est améliorée pour permettre le déplacement (reprise locale) d'un appel en attente sur une ligne virtuelle, traité par un autre utilisateur ou par le même utilisateur sur un autre périphérique. Pour plus d'informations, consultez *6.2.15Déplacer l'appel*.

Ce qui suit décrit les modifications du modèle de configuration liées à la prise en charge des lignes virtuelles.

Confidentiel à Cisco

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

6.2.14 Pack d’événements de contrôle de coupure du son à distance (Webex Calling uniquement)

À partir de la version 43.9, l’application Webex ajoute la prise en charge du contrôle à distance des appels de coupure du son du flux audio. Cela permet de déclencher le son/rétablissement du son d’un appel en cours à partir d’un autre emplacement tel que le client léger BroadWorks Receptionist, où l’application Webex est le périphérique d’appel.

La fonctionnalité dépend du nouveau pack d'informations SIP *x-cisco-mute-status*. Si l'en-tête *Recv-Info:x-cisco-mute-status* est reçu au cours de l'établissement de la session d'appel SIP INVITE, alors chaque fois qu'il y a une mise à jour (locale ou distante) vers l'état muet de la session d'appel audio, l'application Webex renvoie SIP INFO avec le *Info-Package:x-cisco-mute-status;muted=true* (ou *muted=false*), où le paramètre muté représente l'état mis à jour du flux de média audio.

Couper ou rétablir le son peut être déclenché localement ou à partir d’un emplacement distant. La mise à jour à distance déclenche un SIP NOTIFY avec *Event : couper le son* (ou *rétablir le son*) pour être envoyé à l’application Webex à partir du serveur d’applications. L’application Webex répond à la demande à distance et après la mise à jour de l’état du flux de média audio, renvoie un SIP NOTIFY avec le *Info-Package:x-cisco-mute-status;muted=true* (ou *muted=false*).

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


Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false (faux)	vrai, faux	Lorsque ce paramètre est défini sur « vrai », le contrôle d'appel à distance de coupure du son est activé pour l'utilisateur.

6.2.15 Déplacer l'appel

L'application Webex fournit la surveillance des appels et le contrôle des appels VoIP terminés sur un autre emplacement. Ceci est actuellement disponible uniquement pour la ligne principale de l'utilisateur.

À partir de la version 43.12, l'application Webex est améliorée pour afficher les appels terminés sur un autre emplacement également pour les lignes partagées et virtuelles. Ces appels sont visibles dans la zone appels en coursà titre indicatif et sans possibilité de les contrôler. Uniquement si un tel appel est mis en attente, l'utilisateur pourra le déplacer vers le périphérique local en le sélectionnant et le reprendre à partir de l'écran d'appel. Ce mécanisme est utile si l'appel a été traité par le même utilisateur sur un autre emplacement ou par un autre utilisateur utilisant la même ligne.

Notez qu'il n'est pas possible pour l'application Webex de déplacer un appel en attente vers un périphérique appairé. Si l'utilisateur est appairé à un périphérique, il doit d'abord se déconnecter, puis il peut reprendre l'appel en attente localement.

La surveillance des appels pour la ligne partagée et virtuelle dépend du pack d'événements d'infos d'appel SIP.

La surveillance des appels pour la ligne principale de l'utilisateur dépend des événements XSI (pack d'événements d'appel avancé) et le déplacement d'un appel vers le périphérique local n'est pas disponible pour ces appels. Pour ce type d'appels, l'utilisateur peut utiliser la fonction Call Pull (*6.1.22Call Pull* (Transfert d'appel)). L'extraction d'appel ne fonctionne que pour les derniers appels actifs de l'utilisateur, tandis que le mécanisme des lignes partagées et virtuelles fonctionne pour tous les appels de l'utilisateur qui sont mis en attente.

1. Cas d'utilisation 1 :
    a. La ligne de Bob est attribuée à Alice pour les profils de téléphone de bureau et de bureau.
    b. Alice a un appel avec Charlie via le téléphone de bureau – Alice peut voir l'appel en cours dans l'application de bureau.
    c. Alice met l'appel en attente du téléphone de bureau – l'appel peut être repris par Alice à partir de l'application de bureau.
2. Cas d'utilisation 2 :
    a. La ligne de Bob est attribuée à Alice pour les profils de téléphone de bureau et de bureau.
    b. Bob a un appel avec Charlie – Alice peut voir l'appel en cours dans l'application de bureau.
    c. Bob met l'appel avec Charlie en attente – Alice peut reprendre l'appel avec Charlie à partir de l'application de bureau.
3. Cas d'utilisation 3 :

Confidentiel à Cisco

a. La ligne de Bob est attribuée à Alice pour les profils de téléphone de bureau et de bureau.

b. Alice est jumelée à son téléphone de bureau à partir de l'application de bureau.

c. Bob a un appel avec Charlie – Alice peut voir l'appel en cours dans l'application de bureau.

d. Bob met l'appel avec Charlie en attente – Alice ne peut pas reprendre l'appel avec Charlie à partir de l'application de bureau.

e. Alice déconnecte l'application de bureau du téléphone de bureau – Alice peut reprendre l'appel avec Charlie à partir de l'application de bureau.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALL_MOVE_HERE_WXT%	false (faux)	vrai, faux	Permet le transfert d'appel sur le périphérique local. Utilisé pour la mise en attente/reprise entre les sites/utilisateurs dans le cas d'utilisation multi-lignes.

Confidentiel à Cisco

6.3 Fonctionnalités mobiles uniquement

6.3.1 Appels d’urgence

Webex pour Cisco BroadWorks prend en charge l’appel d’urgence natif.

Lorsque la fonctionnalité est activée, lors de l'initiation d'un appel VoIP sortant, l'application analyse le numéro composé et le compare à la liste des numéros d'urgence configurés. Si le numéro est identifié comme un numéro d'urgence, l'application exécute le comportement de numérotation configuré. Il est configurable à l'aide de la balise *séquence de numérotation*.

Les modes pris en charge sont :

- *cs-only* – Le client passe des appels d'urgence uniquement via le réseau cellulaire si le réseau est disponible.
- *cs-first* – Lors de l'émission d'un appel d'urgence, le client vérifie le type de réseau auquel le périphérique actuel est connecté. Si le réseau cellulaire est disponible, le client passe cet appel sur le réseau cellulaire. Si le réseau cellulaire n'est pas disponible mais qu'un réseau de données cellulaires/WiFi est disponible, le client passe l'appel sur le réseau de données cellulaires/WiFi en tant qu'appel VoIP. De plus, si l'appel d'urgence est passé par le réseau cellulaire, le client suggère à l'utilisateur de réessayer l'appel d'urgence en tant que VoIP.
- *voip-only* – Le client passe des appels d’urgence uniquement en tant que VoIP si le réseau de données cellulaires/WiFi est disponible.
- *cs-voip* – Le client analyse si le périphérique peut l'initier en tant qu'appel CS natif (sans tenir compte de la disponibilité ou non du réseau CS). Si le périphérique peut démarrer un appel natif, le numéro d'urgence est composé en tant qu'appel d'urgence CS. Sinon, l'appel est composé en tant que VoIP.

> **REMARQUE :** Si l'appel VOIP est désactivé, la seule valeur significative pour la séquence de numérotation d'urgence (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) est cs-only.

Un message de non-responsabilité des appels d’urgence s’affiche à l’utilisateur lors de la connexion. Il n’est pas contrôlé par les options de configuration.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_EMERGENCY_DIALING_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer la détection des appels d'urgence. La valeur par défaut est vide.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	uniquement cs	cs uniquement, cs-first, voip uniquement, cs-voip	Contrôle le mode de séquence de numérotation pour les appels d'urgence.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%EMERGENCY_DIALING_NUMBERS_WXT%	« 911,112 »	Liste CSV	Liste CSV des numéros d'urgence. Exemple : 911 112

6.3.2 Notifications push pour les appels

Lorsqu'un appel entrant est reçu, le client mobile reçoit d'abord une notification push (PN). Il existe un paramètre de configuration qui peut être utilisé pour contrôler quand la session SIP REGISTER doit être établie :

1. Lors de la réception de la notification push, OU
2. Lorsque l'appel est accepté par l'utilisateur.

La deuxième approche est recommandée. Cependant, par rapport au premier cas, cela ajoute un certain délai avant que l'appel ne soit établi.

Selon les exigences d'iOS 13, les PN VoIP doivent être utilisés uniquement pour les appels entrants. Le reste des événements liés à l'appel doit utiliser des PN réguliers.

Pour répondre à cette exigence, une nouvelle API d'enregistrement de PN est introduite et elle nécessite l'application du patch correspondant sur le serveur d'applications. Si le backend n'est pas configuré pour prendre en charge les numéros d'appel iOS 13, le paramètre de configuration peut être utilisé pour imposer l'utilisation des notifications push existantes, où tous les événements liés à l'appel sont livrés via les numéros d'appel VoIP.

Il y a une notification push envoyée par le serveur d'applications (AS) lorsqu'un appel qui sonne est accepté par l'appelé sur un autre emplacement, clôturé par l'appelant ou, par exemple, redirigé vers la messagerie vocale. Avec l'iOS 13, ce type de notification Push est maintenant un standard et il a quelques restrictions. Il peut être retardé par le service de notification push d'Apple (APNS) ou même ne pas être livré du tout. Pour gérer les PN de mise à jour des appels manquants ou retardés, un délai de sonnerie configurable est ajouté pour contrôler le temps de sonnerie maximum. Si le temps de sonnerie maximal est atteint, la sonnerie est arrêtée pour l'appelé et l'appel est traité comme en absence. Du côté de l'appelant, l'appel peut rester à l'état de sonnerie jusqu'à ce que la politique de sonnerie sans réponse configurée sur le serveur d'applications (AS) soit exécutée.

Pour que le comportement de l'application reste cohérent, le minuteur de sonnerie configurable s'applique à la fois à Android et iOS.

Confidentiel à Cisco

Une option de configuration séparée est ajoutée pour spécifier le comportement de refus d'appel lorsqu'un appel entrant est reçu en tant que notification push. Le client peut être configuré pour ignorer l'appel ou pour répondre au serveur via Xsi avec le refus défini sur « vrai » ou « faux », auquel cas les services de traitement d'appel Cisco BroadWorks attribués seront appliqués. Si « decline_false » est configuré, l'appel continue à sonner jusqu'à ce que l'expéditeur abandonne ou que le temporisateur de non-réponse expire et que les services de traitement d'appel associés commencent. Si « decline_true » est configuré, la raison du déclin spécifie le traitement des appels. Si le motif de refus est défini sur « occupé », le serveur force immédiatement le service de traitement occupé. Si « temp_indisponible » est configuré, le service de traitement temporaire indisponible est appliqué.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false (faux)	vrai, faux	Contrôle lorsque la session SIP REGSITER est établie, lors de la réception d'une notification Push pour un appel entrant ou lors de l'acceptation de celui-ci.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0 à 180]	Contrôle la durée maximale de sonnerie des appels entrants pour les appels reçus via PN. Si aucun PN CallUpd n'est reçu dans la période donnée, l'appel sera traité comme en absence.
%REJECT_WITH_XSI_MODE_WXT%	refuser_faux	ignorer, decline_true, decline_false	Spécifie le comportement de refus d'appel.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	occupé	occupé, temp_indisponible	Indique la raison du refus d'appel, si le mode de rejet est défini sur « decline_true ».

6.3.2.1 MWI

Lorsque la fonctionnalité MWI est activée, le client Webex mobile s'abonne à la notification push MWI pour recevoir des mises à jour avec la messagerie vocale de l'utilisateur et l'avertir.

Pour réduire le nombre de notifications et éviter toute distraction inutile, les notifications push MWI sont supprimées dans certains cas. Par exemple, lorsque l'utilisateur écoute les messages vocaux ou les marque comme lus à partir du client mobile Webex (le nombre de messages non lus diminue). Il n'y a pas d'option configurable pour le contrôler.

Pour plus d'informations sur MWI, consultez la section *6.1.27Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente.

Confidentiel à Cisco

6.3.2.2 Sonnerie Splash

Les services BroadWorks (comme NPD) peuvent envoyer des rappels de sonnerie lorsque les appels entrants sont redirigés. Le client Webex Mobile peut être configuré pour activer les notifications push Ring Splash et les présenter à l'utilisateur lorsqu'elles sont déclenchées par BroadWorks.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_RING_SPLASH_WXT%	false (faux)	true, faux	Active Ring Splash dans la configuration BroadWorks.

6.3.3 Alerte unique

La fonctionnalité d'alerte unique mobile est destinée aux déploiements de convergence fixe-mobile (FMC) / opérateur de réseau mobile (MNO) exploitant le service BroadWorks Mobility. Sans cela, lorsqu'il est connecté au client Webex et reçoit un appel entrant, l'utilisateur reçoit simultanément deux appels : un appel natif et un appel de notification push (VoIP). Lorsque la fonctionnalité est activée, l'application désactive l'alerte Mobility sur l'emplacement BroadWorks Mobility de l'utilisateur lors de la connexion et active l'alerte lors de la déconnexion. Une condition préalable importante pour utiliser cette fonctionnalité est que l'utilisateur ait attribué le service BroadWorks Mobility et qu'un emplacement exactement soit configuré.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_SINGLE_ALERTING_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer l'alerte unique.

6.3.4 Cliquer pour composer (Rappel)

Le bouton sortant Click to Dial garantit que l'utilisateur final peut avoir un appel sur son téléphone mobile personnel à commutation de circuit et fournir son ND professionnel comme ID de la ligne appelante.

Le client Webex mobile prend en charge les appels Click to Dial (Rappel) à l'aide du service BroadWorks Anywhere. Les emplacements BroadWorks Anywhere dans l'application Webex sont appelés emplacements SNR (Single Number Reach).

Confidentiel à Cisco

Lorsque la fonctionnalité est activée, les utilisateurs peuvent sélectionner l'emplacement SNR dans le menu de jumelage du périphérique. Lorsqu'ils sont appairés à l'emplacement SNR, tous les appels sortants sont initiés à l'aide des appels Cliquer pour composer (Rappel). Pour éviter une double alerte, les notifications push pour les appels entrants sont désactivées.

Lorsqu'un utilisateur initie un appel Cliquer pour composer, il voit l'écran d'appel sortant avec des informations pour s'attendre à un appel entrant sur l'emplacement SNR sélectionné. Cet écran est fermé automatiquement en fonction du temporisateur configurable.

Lors de la déconnexion d'un emplacement SNR, l'application s'enregistre à nouveau pour les notifications push pour les appels entrants.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_DIALING_CALL_BACK_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer les appels Click to Dial (Rappel).
%DIALING_CALL_BACK_TIMER_WXT%	10	[3 à 20]	Contrôle le nombre de secondes avant la fermeture automatique de l'écran de rappel.

6.3.5 Prise en charge du MNO

6.3.5.1 Appel avec numéroteur natif

Cette fonctionnalité ajoute la prise en charge des déploiements d'opérateurs de réseau mobile (MNO) exploitant le service BroadWorks Mobility (BWM). Il est supposé que le service BroadWorks Mobility de l'utilisateur lui est attribué et qu'au moins un emplacement est configuré.

La capacité de l'utilisateur à lancer des appels via le numéroteur natif est contrôlée par la balise de configuration **native**. Si cette option est activée, l'application lancera le numéroteur natif et passera l'appel. En outre, la disponibilité des appels VoIP est contrôlée par la balise **voip** – en fonction des exigences de déploiement, les appels VoIP peuvent être activés ou désactivés.

Si la VoIP et l'appel natif sont activés, l'utilisateur pourra choisir l'option à utiliser.

La balise <mode de numérotation> contrôle si les utilisateurs peuvent sélectionner la manière dont les appels entrants et sortants doivent être démarrés/reçus. Nécessite l'activation de l'appel natif et VoIP.

À partir de la version 43.12, la configuration de la numérotation native est étendue, offrant la possibilité d'ajouter un préfixe personnalisé au numéro d'appel sortant. Ceci s'applique aux appels cellulaires initiés à partir de l'application Webex, uniquement si le numéro composé commence par un code FAC.

Cette fonctionnalité est utile pour les clients utilisant des déploiements MNO, où les appels au lieu d'être redirigés vers le serveur d'application Cisco BroadWorks intégré, les codes FAC peuvent être traités par le backend Telecom. Une nouvelle balise <fac-prefix> est ajoutée dans la section <numérotation><native> et les télécoms peuvent l'utiliser pour résoudre ce problème.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_DIALING_VOIP_WXT%	vrai	vrai, faux	Définissez sur « vrai » pour activer l'option d'appel VoIP.
%ENABLE_DIALING_NATIVE_WXT%	false (faux)	vrai, faux	Définissez sur « vrai » pour activer l'option d'appel native.
%ENABLE_DIALING_MODE_WXT%	false (faux)	vrai, faux	Active la sélection du mode de numérotation par l'utilisateur, via les paramètres d'appel dans Préférences.
%DIALING_MODE_DEFAULT_WXT%	voip	voip, natif	Spécifie le mode de numérotation par défaut sélectionné lorsque le mode de numérotation est activé dans Préférences.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false (faux)	vrai, faux	Contrôle si la disponibilité de l'appel natif doit dépendre de l'attribution du service BroadWorks Mobility et de l'emplacement de mobilité configurés pour l'utilisateur.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*vide*	chaîne de caractères	Indique un préfixe qui doit être ajouté si un appel sortant vers un numéro commençant par un code FAC est lancé en tant qu'appel cellulaire. Par défaut, aucun préfixe FAC n'est défini et la balise est vide.

NOTE 1 : Au moins un appel **voip** et **natif** doit être activé.

NOTE 2 : Si seul l'appel **natif** est activé, dans les déploiements MNO, il est recommandé de désactiver l'alerte unique pour empêcher le client de désactiver l'alerte BWM.

NOTE 3 : Si les appels **natifs** et **voip** sont activés, dans les déploiements MNO, il est recommandé d'activer l'alerte unique pour éviter la double alerte.

Confidentiel à Cisco

6.3.5.2 Commandes en cours d'appel

Cette fonctionnalité permet au client Webex mobile de contrôler via les appels natifs XSI sur le périphérique mobile qui sont ancrés sur Cisco BroadWorks. Les commandes d'appel XSI sont disponibles uniquement si :

- Le service BroadWorks Mobility (BWM) est attribué à l'utilisateur,
- Une seule identité mobile BMW est configurée,
- Le mode de numérotation natif est sélectionné par l'utilisateur (pour plus d'informations, consultez la section *6.3.5.1Appel avec numéroteur natif),*
- Il y a un appel basé sur BroadWorks, qui passe par le service BMW,
- Il y a un appel cellulaire en cours sur le périphérique mobile.

La version 43.10 améliore la gestion du transfert consultatif, créant une association entre les deux appels cellulaires présentés dans l'application Webex et fournissant une option à l'utilisateur pour effectuer le transfert. En outre, si l'utilisateur a deux appels cellulaires indépendants sur le même périphérique, le menu de transfert est amélioré pour permettre le transfert de l'un vers l'autre même s'il n'y a pas d'association créée entre eux.

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_XSI_CALL_CONTROL_WXT%	false (faux)	vrai, faux	Active le contrôle d'appel XSI pour l'environnement MNO.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	Accès_MNO	MNO_Access, MNO_Network	Contrôle le type de déploiement XSI MNO utilisé par l'application. Les valeurs possibles sont : ▪ MNO_Access – affiche tous les appels distants (XSI) avec les types de périphériques définis dans le nœud ci-dessous. ▪ MNO_Network - affiche tous les appels distants (XSI).
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	""	chaîne de caractères	Le ou les noms de type de périphérique qui doivent être utilisés dans le type de déploiement MNO_Access.
%ENABLE_XSI_HOLD_CALLS_WXT%	vrai	vrai, faux	Contrôle si l'action de mise en attente d'appel doit être disponible pour l'utilisateur pour les appels mobiles XSI.

Confidentiel à Cisco

6.3.5.3 Identité de la ligne d'appel sortante (CLID) – Double personnalité

Avec la version mobile 42.12, l'application Webex permet aux utilisateurs de sélectionner leur identité de ligne d'appel (CLID) présentée à l'interlocuteur distant lors de l'initiation d'un appel sortant.

Si l'utilisateur est configuré avec Cisco BroadWorks Mobility, la configuration typique des déploiements des opérateurs de réseau mobile (MNO) et que l'appel natif est activé, l'utilisateur peut sélectionner l'identité à présenter aux personnes qu'il appelle. L'utilisateur peut choisir son identité professionnelle ou personnelle. Il y a également une option pour masquer sa propre identité et l'appel à être présenté comme anonyme.

Pour les appels VoIP, l'utilisateur a également une option pour contrôler son CLID. L'option disponible dans ce cas est seulement de contrôler s'il faut cacher son identité ou non.

La gestion des persona et le blocage CLID sont contrôlés par des options de configuration distinctes.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	false (faux)	vrai, faux	Active le blocage de la distribution de l'ID de la ligne appelante. Il s'applique à tous les types d'appels sortants pour l'utilisateur.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	false (faux)	vrai, faux	Active la gestion personnelle des appels natifs lorsque le type de déploiement est configuré comme MNO_Access ou MNO_Network. (BroadWorks Mobility est utilisé pour les appels natifs et tous les appels natifs sont ancrés sur BroadWorks)

6.3.5.4 Notification pour les appels natifs

Pour les utilisateurs déployés avec le MNO, cette fonctionnalité ajoute une bannière de notification pour les appels natifs, qui peut être contrôlée via l'application Webex. Cette notification repose sur une notification push, envoyée par le serveur d'applications une fois l'appel établi.

Confidentiel à Cisco

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	vrai	true, faux	Active l'abonnement à la notification push MOBILE_CALL_INFO.

6.3.5.5 Déplacer l'appel d'origine vers une réunion convergée

Pour les utilisateurs déployés avec MNO, cette fonctionnalité permet qu'un appel vocal natif soit transféré à une réunion pour les deux parties d'un appel 1 à 1 (même si l'autre partie n'est pas un utilisateur de Webex). Si l'utilisateur distant est un utilisateur Webex, une fois au cours d'une réunion, les parties auront la possibilité de :

- Lancer Webex dans le Chat de la réunion
- Ajouter la vidéo (notez que l'audio continuera dans l'appel d'origine)
- Partager l'écran/le contenu
- Déclencher l'enregistrement des réunions

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false (faux)	vrai, faux	Active la mise sous tension (Inviter et se rencontrer, actions de rencontre vidéo).

6.3.5.6 MNO Mobility - Widget en cours d'appel

La version 43.7 de l'application Webex pour Android (mobile et tablette) introduit officiellement un nouveau widget de contrôle des appels (bulle), fournissant un contrôle d'appel supplémentaire pour les appels natifs ancrés sur Cisco BroadWorks, à l'aide du service de mobilité. Le widget s'affiche en haut de l'interface utilisateur native et permet à l'utilisateur les actions suivantes :

- Attente/Reprise
- Transfert aveugle/consultatif– place l'utilisateur dans la boîte de dialogue de transfert dans l'application Webex.
- Complete Transfer – offre la possibilité d'effectuer le transfert consultatif (version 43.10)
- Réunion vidéo – déplace les parties dans une réunion Webex.
- Mettre fin à l'appel

```
<config>
<services><calls>
       <hold xsi-enabled="%ENABLE_XSI_HOLD_CALLS_WXT%" widget-
enabled="%ENABLE_WIDGET_HOLD_CALLS_WXT%"/>
```


Confidentiel à Cisco

```
      <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%"/>
```

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_WIDGET_HOLD_CALLS_WXT%	vrai	vrai, faux	Contrôle la disponibilité de l'action Attente dans le widget Appel.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	vrai	vrai, faux	Contrôle la disponibilité des actions Transférer et Terminer le transfert dans le widget Appeler.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	vrai	vrai, faux	Contrôle la disponibilité de l'action Réunion vidéo dans le widget Appeler.

6.3.6 ID de l'appelant entrant

La version 44.2 ajoute la possibilité de contrôler les informations de contact présentées à l'utilisateur en fonction du nom et du numéro. Deux options de configuration ont été ajoutées pour contrôler les informations présentées à l'utilisateur dans l'écran d'appel entrant et la notification d'appel entrant, ainsi que les notifications d'appel en absence.

6.3.6.1 Écran des appels entrants

Il existe des différences de plateforme entre Android et iOS lorsqu'il s'agit d'afficher les données dans l'écran d'appel entrant. L'expérience native d'affichage des informations pour les appels entrants est la suivante :

- Android - il y a deux champs séparés dans l'écran d'appel entrant pour afficher à la fois le nom et le numéro
- iOS - il n'y a qu'un seul champ pour afficher le nom ou le numéro - si les deux sont disponibles, le nom est prioritaire

La nouvelle option de configuration pour les appels entrants peut être utilisée pour vous assurer que l'application iOS Webex affiche le numéro sur l'écran d'appel à côté du nom (format : *Nom (Numéro)*). Le comportement de l'application Webex Android n'est pas affecté.

6.3.6.2 Notification d'appel entrant

Dans certains cas, l'appel entrant est présenté à l'utilisateur sous forme de notification. En raison de l'espace limité, le numéro n'y est pas toujours affiché.

La nouvelle option de configuration pour les appels entrants contrôle également les informations affichées dans les notifications d'appels entrants. Si cette option est activée et que le nom et le numéro sont disponibles, l'application Webex ajoutera le numéro à côté du nom (format : *Nom (Numéro)*). Ce comportement de l'application Webex est applicable à la fois à Android et iOS.

Confidentiel à Cisco

6.3.6.3 Notification d’appel manqué

Un paramètre de configuration supplémentaire a été ajouté pour les notifications d'appel en absence. Il peut être utilisé pour contrôler les informations de l'interlocuteur distant, comme pour les notifications d'appel entrant, permettant d'ajouter le numéro au nom d'affichage de l'utilisateur distant et de le présenter dans la notification d'appel en absence. Ce comportement de l’application Webex est applicable à la fois à Android et iOS.

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

Balise	Valeur par défaut si Omis	Valeurs prises en charge	Description
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false (faux)	vrai, faux	Contrôle si le numéro doit être ajouté au nom dans l'écran d'appel entrant (iOS uniquement) et les notifications.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	false (faux)	vrai, faux	Contrôle si le numéro doit être ajouté au nom dans la notification d'appel en absence.

REMARQUE : Si le numéro est fourni en tant que nom d’affichage ou si le nom d’affichage se termine par le numéro, l’application Webex évitera la duplication et affichera le numéro une seule fois.

Confidentiel à Cisco

7 Fonctionnalités de l'essai précoce sur le terrain (BÊTA)

7.1 Codec IA

À partir de la version 44.7, l'application Webex introduit la prise en charge d'un nouveau codec audio : le codec AI (xCodec). Ce codec audio est utilisé dans des conditions réseau défavorables pour obtenir une meilleure qualité d'appel. Le moteur média Webex de l'application Webex vérifie les capacités du périphérique, suit la qualité du média et le codec AI peut être utilisé s'il est pris en charge et activé via le fichier de configuration.
Le codec AI ne fonctionne qu'en combinaison avec le codec Opus. Cela signifie que le codec Opus et AI doivent être annoncés et négociés par les deux parties au cours de la négociation SDP.

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


Confidentiel à Cisco

8 Mappage des balises personnalisées entre Webex pour Cisco BroadWorks et UC-One

Le tableau suivant répertorie les balises personnalisées Webex pour Cisco BroadWorks, correspondant à leurs balises personnalisées existantes pour UC-One.

Balise Webex pour Cisco BroadWorks	Balise existante du bureau	Étiquette existante mobile
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	N/A	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N/A	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	N/A	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	N/A
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	N/A
%ENABLE_CALL_STATISTICS_WXT%	N/A	N/A
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N/A	%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%MWI_MODE_WXT%	%DESKTOP_MWI_MODE%	%MWI_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	N/A	N/A
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	N/A
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	N/A
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	N/A
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_WXT%	N/A	N/A

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Balise existante du bureau	Étiquette existante mobile
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	N/A	N/A
%ENABLE_EMERGENCY_DIALING_WXT%	N/A	N/A
%EMERGENCY_DIALING_NUMBERS_WXT%	N/A	N/A
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	N/A	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	N/A
%SBC_ADDRESS_WXT%	%SBC_ADRESSE%	%SBC_ADRESSE%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILE%
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	N/A
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	N/A

Confidentiel à Cisco

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

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Balise existante du bureau	Étiquette existante mobile
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	N/A	%ENABLE_CALLS_AUTO_RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N/A	%EMERGENCY_CALL_DIAL_SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLIND_WXT%	N/A	N/A
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_URL_WXT%	N/A	%WEB_CALL_SETTINGS_URL%
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP%
%ENABLE_CALL_CENTER_WXT%	%ENABLE_CALL_CENTER_DESKTOP% »	N/A
%WEB_CALL_SETTINGS_TARGET_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFA_VISIBLE%
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_DND_VISIBLE%
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_ACR_VISIBLE%
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFB_VISIBLE%
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFNR_VISIBLE%
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFNA_VISIBLE%
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SIMRING_VISIBLE%
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SEQRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_RO_VISIBLE%
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_ACB_VISIBLE%
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CW_VISIBLE%
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CLIDB_VISIBLE%
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_PA_VISIBLE%

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Balise existante du bureau	Étiquette existante mobile
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_BWA_VISIBLE%
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	N/A	%WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE%
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_BWM_VISIBLE%
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_VM_VISIBLE%
%ENABLE_DIALING_CALL_BACK_WXT%	N/A	N/A
%DIALING_CALL_BACK_TIMER_WXT%	N/A	N/A
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	N/A
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N/A	%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_MOBILE%
%ENABLE_CALL_RECORDING_WXT%	%ENABLE_CALL_RECORDING_DESKTOP%	%CALL_RECORDING_MOBILE%
%ENABLE_SINGLE_ALERTING_WXT%	N/A	%ENABLE_SINGLE_ALERTING%
%ENABLE_CALL_PARK_WXT%	%ENABLE_CALL_PARK_DESKTOP%	N/A
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	N/A	N/A
%ENABLE_RTP_ICE_WXT%	N/A	N/A
%RTP_ICE_MODE_WXT%	N/A	N/A
%RTP_ICE_SERVICE_URI_WXT%	N/A	N/A
%RTP_ICE_PORT_WXT%	N/A	N/A
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	N/A	N/A
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/A	N/A
%ENABLE_DIALING_VOIP_WXT%	N/A	N/A
%ENABLE_DIALING_NATIVE_WXT%	N/A	N/A
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	N/A	N/A
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	N/A	N/A

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Balise existante du bureau	Étiquette existante mobile
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	N/A	N/A
%USER_PORTAL_SETTINGS_URL_WXT%	N/A	N/A
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	N/A	N/A
%ENABLE_AUDIO_MARI_FEC_WXT%	N/A	N/A
%ENABLE_AUDIO_MARI_RTX_WXT%	N/A	N/A
%ENABLE_VIDEO_MARI_FEC_WXT%	N/A	N/A
%ENABLE_VIDEO_MARI_RTX_WXT%	N/A	N/A
%ENABLE_CALL_BLOCK_WXT%	N/A	N/A
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N/A	N/A
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N/A	N/A
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/A	N/A
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	N/A	N/A
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	N/A	N/A
%ENABLE_CALL_MOVE_HERE_WXT%	N/A	N/A
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	N/A	N/A
%DIALING_NATIVE_FAC_PREFIX_WXT%	N/A	N/A
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	N/A	N/A
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	N/A	N/A
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N/A	N/A

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Balise existante du bureau	Étiquette existante mobile
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N/A	N/A
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	N/A	N/A
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	N/A
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	N/A
%BLF_NOTIFICATION_DELAY_TIME_WXT%	N/A	N/A
%ENABLE_GCP_NOTIFICATIONS_WXT%	N/A	N/A
%ENABLE_GCP_DISPLAY_CALLER_WXT%	N/A	N/A
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	N/A	N/A
%UDP_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%TCP_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%TLS_KEEPALIVE_ENABLED_WXT%	N/A	N/A

REMARQUE : N/A indique qu'il n'y avait aucune balise personnalisée correspondante contrôlant la fonctionnalité dans UC-One. Avoir N/A pour les balises existantes de bureau et mobiles indique que la balise Webex pour Cisco BroadWorks est nouvelle et contrôle soit une nouvelle fonctionnalité, soit une fonctionnalité existante, qui n'a pas été contrôlée par une balise personnalisée dans UC-One.

Confidentiel à Cisco

9 Annexe A : Codes de chiffrement TLS

Le client Webex pour BroadWorks utilise CiscoSSL, qui est basé sur OpenSSL avec un renforcement de sécurité supplémentaire.

Confidentiel à Cisco

10 Annexe B : Script de mise à disposition de la balise DM

Le nombre de balises DM personnalisées a augmenté à chaque version, car de nombreux clients préfèrent les balises pour les nouveaux paramètres de configuration. Pour offrir des mécanismes de mise à disposition plus facile de ces balises DM personnalisées, cette section contient un script qui peut être exécuté du côté du serveur d'applications (AS) pour affecter des valeurs aux balises DM personnalisées. Ce script est particulièrement destiné aux nouveaux déploiements où la plupart des balises DM personnalisées sont destinées à être utilisées.

Notez que ce script n'est valide que pour les nouveaux déploiements où des balises DM personnalisées sont créées. Pour modifier les balises DM personnalisées existantes, la commande dans le script suivant doit être modifiée de « ajouter » à « définir ».

Modèle de script avec seulement quelques balises personnalisées (dans un déploiement réel, vous devez remplir une liste plus grande de balises personnalisées). Notez que l'exemple suivant est pour mobile. Pour le bureau, utilisez le jeu de balises BroadTouch_tags au lieu de Connect_Tags. Pour la tablette, utilisez le jeu de balises ConnectTablet_Tags au lieu de Connect_Tags.

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


Confidentiel à Cisco

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

La liste suivante répertorie toutes les balises personnalisées utilisées par Webex pour Cisco BroadWorks, avec des exemples de valeurs (par défaut ou recommandées). Notez que certaines balises nécessitent des valeurs spécifiques au déploiement correspondant (comme les adresses de serveur). C'est pourquoi ces balises sont ajoutées à la fin du script mais laissées vides, et des commandes d'ensemble supplémentaires doivent être ajoutées pour les spécifier.

10.1 Bureau

```
add tagSetName BroadTouch_tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_WXT% true
add tagSetName BroadTouch_tags %BLF_NOTIFICATION_DELAY_TIME_WXT% 0
add tagSetName BroadTouch_tags %ENABLE_REMOTE_CONTROL_EVENTS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName BroadTouch_tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName BroadTouch_tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName BroadTouch_tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PULL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MWI_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%
false
add tagSetName BroadTouch_tags
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%
false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%
false
add tagSetName BroadTouch_tags
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% false
add tagSetName BroadTouch_tags
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_USE_RPORT_WXT% false
add tagSetName BroadTouch_tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName BroadTouch_tags %USE_TLS_WXT% false
add tagSetName BroadTouch_tags %SBC_PORT_WXT% 5075
```


Confidentiel à Cisco

```
add tagSetName BroadTouch_tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName BroadTouch_tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName BroadTouch_tags %SOURCE_PORT_WXT% 5060
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName BroadTouch_tags %SIP_FAILBACK_ENABLED_WXT% true
add tagSetName BroadTouch_tags %SIP_FAILBACK_TIMEOUT_WXT% 900
add tagSetName BroadTouch_tags %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName BroadTouch_tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_WXT% false
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName BroadTouch_tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName BroadTouch_tags %SRTP_ENABLED_WXT% false
add tagSetName BroadTouch_tags %SRTP_MODE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REKEYING_WXT% true
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName BroadTouch_tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName BroadTouch_tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName BroadTouch_tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName BroadTouch_tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName BroadTouch_tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName BroadTouch_tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName BroadTouch_tags %USE_MEDIASEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_URL_WXT%
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
```

```
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_BLIND_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_DIRECTED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% true
add tagSetName BroadTouch_tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PARK_WXT% false
add tagSetName BroadTouch_tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
add tagSetName BroadTouch_tags %RTP_ICE_PORT_WXT% 3478
add tagSetName BroadTouch_tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName BroadTouch_tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID_WXT% true
add tagSetName BroadTouch_tags %XSI_ROOT_WXT% true
add tagSetName BroadTouch_tags %SBC_ADDRESS_WXT% true
add tagSetName BroadTouch_tags %SBC_PORT_WXT% true
add tagSetName BroadTouch_tags %MWI_MODE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName BroadTouch_tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUTO_ANSWER_WXT% false
add tagSetName BroadTouch_tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MULTI_LINE_WXT%false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName BroadTouch_tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName BroadTouch_tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName BroadTouch_tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName BroadTouch_tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REMOTE_MUTE_CONTROL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName BroadTouch_tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_MOVE_HERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_NOTIFICATIONS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_DISPLAY_CALLER_WXT% false
add tagSetName BroadTouch_tags %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% 120
add tagSetName BroadTouch_tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% false
```


Confidentiel à Cisco

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

10.2 Mobile

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


Confidentiel à Cisco

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


Confidentiel à Cisco

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


Confidentiel à Cisco

```
add tagSetName Connect_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
```

10.3 Tablette

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


Confidentiel à Cisco

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


Confidentiel à Cisco

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

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

10.4 Balises système

La liste suivante répertorie les balises système utilisées par Webex pour BroadWorks.

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


Confidentiel à Cisco

11 Acronymes et abréviations

Cette section répertorie les acronymes et abréviations trouvés dans ce document. Les acronymes et abréviations sont listés par ordre alphabétique avec leurs significations.

ACB	Rappel automatique
ACD	Distribution automatique des appels
ACR	Rejet d'appel anonyme
AES	Norme de chiffrement avancée
ALG	Passerelle de couche applicative
API	Interface de programmation d'application
APK	Dossier de demande
APNS	Service de notification Push Apple
ARS	Sélection automatique du débit binaire
AS	Serveur d'applications (Cisco BroadWorks)
AVP	Profil audio-visuel
BW	BroadWorks
BWA	BroadWorks Anywhere
BWKS	BroadWorks
BWM	Mobilité BroadWorks
BYOD	Apportez votre propre appareil
CC	Centre d'appel
CFB	Renvoi d'appel occupé
CFNA	Renvoi d'appel sans réponse
CFNR	Renvoi d'appel non accessible
CIF	Format intermédiaire commun
CLI	Interface de ligne de commande
CLID	Identité de la ligne appelante
CLIDB	Blocage de la distribution de l'ID de la ligne appelante
CRLF	Alimentation de la ligne de retour chariot
CS	Circuit commuté
CSWV	Vue Web des paramètres d'appel
CW	Appel en attente
DB	Base de données
DM	Gestion des périphériques
NPD	Ne pas déranger
DNS	Système de noms de domaine

Confidentiel à Cisco

DPC	Contrôle du téléphone de bureau
DTAF	Fichier d’archivage du type de périphérique
ECACS	Service de changement d'adresse d'appel d'urgence
FMC	Convergence fixe-mobile
FDQN	Nom de domaine entièrement qualifié
HMAC	Code d'authentification du message de hachage
ICE	Établissement de la connectivité interactive
iLBC	Codec internet à faible débit binaire
IM	Messagerie instantanée
IM&P	Messagerie instantanée et présence
IOT	Tests d’interopérabilité
IP	Protocole Internet
JID	Identifiant Jabber
M/O	Obligatoire/Optionnel
MNO	Opérateur de réseau mobile
BTM	Unité de transmission maximale
MUC	Conversation multi-utilisateurs
MWI	Indicateur de message en attente
NAL	Couche d'abstraction réseau
NAPTR	Pointeur d'autorité de nommage
NAT	Traduction des adresses réseau
OTT	Over The Top
PA	Assistant personnel
PAI	Identité revendiquée
PEM	P-Early Media
PLI	Indication de perte d'image
PLMN	Réseau mobile terrestre public
PN	Notification push
QCIF	Format intermédiaire commun du trimestre
QoS	Qualité de service
RO	Bureau distant
RTCP	Protocole de contrôle en temps réel
RTP	Protocole en temps réel
SaaS	Software as a Service
SAN	Nom alternatif de l'objet
SASL	Couche d'authentification simple et de sécurité

Confidentiel à Cisco

SAVP	Profil audio vidéo sécurisé
SBC	Contrôleur de limites de session
SCA	Apparence des appels partagés
SCF	Fonction de continuité de session
SCTP	Protocole de transmission de contrôle de flux
SDP	Protocole de définition de session
SEQRING	Anneau séquentiel
SIMRING	Sonnerie simultanée
SIP	Protocole d'initiation de session
SNR	Rapport signal/bruit
SNR	Numéro d'appel unique
SRTCP	Protocole de contrôle sécurisé en temps réel
SRTP	Protocole de transport sécurisé en temps réel
SSL	Secure Sockets Layer
STUN	Session Traversal Utilities for NAT
SUBQCIF	Sous-trimestre CIF
TCP	Protocole de contrôle de transmission
TLS	Sécurité de la couche transport
TTL	Durée de vie
TURN	Traversée à l'aide du relais NAT
UDP	Protocole de datagramme utilisateur
UI	Interface utilisateur
UMS	Serveur de messagerie (Cisco BroadWorks)
URI	Identificateur uniforme de ressource
Serveur vidéo UVS	(Cisco BroadWorks)
VGA	Video Graphics Array (réseau graphique vidéo)
VoIP	Voix sur IP
VVM	Messagerie vocale visuelle
WXT	Webex
XMPP	Protocole extensible de messagerie et de présence
XR	Rapport étendu
Plateforme de services Xsp	Xtended
Xsi	Xtended Services Interface

Confidentiel à Cisco