Guide de configuration de Webex pour Cisco BroadWorks

Publier 45.10

Version du document 3

Table des matières

1 Résumé des changements 1
1.1 Modifications de la version 45.10, octobre 2025 1
1.2 Modifications pour la version 45.9, septembre 2025 1
1.3 Modifications pour la version 45.8, août 2025 1
1.4 Modifications pour la version 45.7, juillet 2025 2
1.5 Modifications de la version 45.6, juin 2025 2
1.6 Modifications de la version 45.5, mai 2025 2
1.7 Modifications de la version 45.4, avril 2025 2
1.8 Modifications de la version 45.3, mars 2025 2
1.9 Modifications de la version 45.2, février 2025 2
1.10 Changements pour la version 45.1, janvier 2025 2
1.11 Changements pour la version 44.12, décembre 2024 2
1.12 Modifications pour la version 44.11, novembre 2024 3
1.13 Modifications de la version 44.10, octobre 2024 3
1.14 Modifications pour la version 44.9, septembre 2024 3
1.15 Modifications pour la version 44.8, août 2024 3
1.16 Modifications pour la version 44.7, juillet 2024 3
1.17 Modifications de la version 44.6, juin 2024 3
1.18 Modifications de la version 44.5, mai 2024 3
1.19 Modifications de la version 44.4, avril 2024 3
1.20 Modifications de la version 44.3, mars 2024 4
1.21 Modifications de la version 44.2, février 2024 4
1.22 Modifications de la version 44.1, janvier 2024 4
2 Modifications des fichiers de configuration 5
2.1 Modifications des fichiers de configuration de la version 45.10 5
2.2 Modifications des fichiers de configuration de la version 45.9 6
2.3 Modifications des fichiers de configuration de la version 45.8 6
2.4 Modifications des fichiers de configuration de la version 45.7 6
2.5 Modifications des fichiers de configuration de la version 45,6 7
2.6 Modifications des fichiers de configuration de la version 45,5 7
2.7 Modifications des fichiers de configuration de la version 45,4 8
2.8 Modifications des fichiers de configuration de la version 45,3 8
2.9 Modifications des fichiers de configuration de la version 45,2 8
2.10 Modifications des fichiers de configuration de la version 45,1 8
2.11 Modifications des fichiers de configuration de la version 44,12 8
2.12 Modifications des fichiers de configuration de la version 44,11 8
2.13 Modifications des fichiers de configuration de la version 44,1 9
2.14 Modifications des fichiers de configuration de la version 44.9 9
2.15 Modifications des fichiers de configuration de la version 44.8 9

Confidentiel à Cisco

2.16 Modifications des fichiers de configuration de la version 44.7 9
2.17 Modifications des fichiers de configuration de la version 44.6 10
2.18 Modifications des fichiers de configuration de la version 44.5 10
2.19 Modifications des fichiers de configuration de la version 44,4 10
2.20 Modifications des fichiers de configuration de la version 44,3 11
2.21 Modifications des fichiers de configuration de la version 44,2 11
2.22 Modifications des fichiers de configuration de la version 44,1 13

3 Introduction 14

4 Installation 15
4.1 Téléchargement du client localisé 15
4.2 Client Android 15
4.3 Client iOS 15
4.4 Client de bureau 16

5 Gestion de l'appareil 17
5.1 Balises de gestion des périphériques 17
5.2 Amélioration de la correspondance partielle pour la sélection du type d'appareil 18
5.3 Configuration du client 19
5.4 Déploiement de config-wxt.xml 19
5.5 Fichier de configuration (config-wxt.xml) 19
5.6 Balises par défaut du système 20
5.7 Balises du système intégré dynamique Cisco BroadWorks 20

6 Balises personnalisées 23
6.1 Caractéristiques communes 40
6.1.1 Paramètres du serveur SIP 40
6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel 43
6.1.3 3GPP En-têtes SIP pour SRTP 45
6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou UDP 46
6.1.5 Délai d'expiration configurable pour l'ouverture du socket SIP 48
6.1.6 Détection dynamique du proxy SIP 49
6.1.7 Utilisation du port préféré pour SIP 54
6.1.8 SIP Failover et Failback 55
6.1.9 SIP SUBCSRIBE et REGISTER Refresh et SUBSCRIBE Retry 60
6.1.10 Utiliser les URI associés à P dans REGISTER 60
6.1.11 En-tête SIP P-Early Media (PEM) 61
6.1.12 Prise en charge de la MISE À JOUR SIP 62
6.1.13 FIR INFO SIP hérité 62
6.1.14 Gestion des ports SIP pour la traversée NAT 63
6.1.15 ID de session SIP 64
6.1.16 Comportement du rejet d'appel entrant 64
6.1.17 Plage de ports du protocole de transport en temps réel 65
6.1.18 Assistance ICE (Webex Calling uniquement) 66

Confidentiel à Cisco

6.1.19 MUX RTCP ... 66
6.1.20 Transfert ... 67
6.1.21 Conférences téléphoniques N-Way ... 68
6.1.22 Retirer un appel ... 69
6.1.23 Parquage d'appel/Récupérer ... 71
6.1.24 Statistiques de l'appel ... 72
6.1.25 Récupération automatique des appels / Transfert d'appel fluide ... 72
6.1.26 Enregistrement des appels ... 73
6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente ... 74
6.1.28 Transcription des messages vocaux pour Webex Calling ... 76
6.1.29 Paramètres des appels ... 77
6.1.30 Portail des paramètres et paramètres d'appel sur le Web ... 79
6.1.31 Connexion/déconnexion du centre d'appels/de la file d'attente des appels ... 83
6.1.32 Racines et chemins XSI ... 84
6.1.33 Chaîne d'événements XSI ... 84
6.1.34 Configuration des codecs ... 85
6.1.35 Numérotation SIP-URI ... 87
6.1.36 Historique des appels ... 88
6.1.37 Désactiver les appels vidéo ... 88
6.1.38 Appels d'urgence (911) - Création de rapports de localisation avec le fournisseur E911 ... 89
6.1.39 Le PAI en tant qu'identité ... 91
6.1.40 Désactiver le partage d'écran ... 91
6.1.41 Indication des appels indésirables ... 92
6.1.42 Suppression du bruit et extension de la bande passante pour les appels RTCP/mobiles ... 92
6.1.43 Marquage QoS DSCP ... 93
6.1.44 Profil primaire ... 94
6.1.45 Liste de blocage (Webex Calling uniquement) ... 95
6.1.46 Mise en œuvre de l'adaptation et de la résilience des médias (MARI) ... 96
6.1.47 Appels simultanés avec le même utilisateur ... 98
6.1.48 RTCP-XR ... 99
6.1.49 Informations sur le renvoi d'appel ... 99
6.1.50 ID de l'appelant ... 100
6.1.51 Multiligne ... 103
6.1.52 Autorisation SIP améliorée ... 105
6.1.53 Assistant personnel (Présence en absence) ... 105
6.2 Fonctionnalités du bureau uniquement ... 107
6.2.1 Déconnexion forcée ... 107
6.2.2 Prise d'appel ... 108
6.2.3 Assistance Boss-Admin (Cadre de direction-Assistant) ... 108
6.2.4 Transférer les appels SIP vers la réunion (Webex Calling uniquement) ... 109

Confidentiel à Cisco

6.2.5 Appels de contrôle du téléphone de bureau – Réponse automatique 109
6.2.6 Réponse automatique avec notification de tonalité 110
6.2.7 Contrôle du téléphone de bureau - Contrôle des appels intermédiaires - Conférence 110
6.2.8 Notifications de prise d'appel 111
6.2.9 Pack d'événements de contrôle à distance..... 113
6.2.10 Passerelle de survivabilité (Webex Calling uniquement) 114
6.2.11 Pack d'événements pour le contrôle de la coupure du son à distance (Webex Calling uniquement) 114
6.2.12 Déplacer l'appel 115
6.3 Fonctionnalités mobiles uniquement 118
6.3.1 Appels d'urgence 118
6.3.2 Notifications Push pour les appels..... 119
6.3.3 Alerte unique 122
6.3.4 Cliquer pour composer (Rappeler) 122
6.3.5 Prise en charge MNO..... 123
6.3.6 ID de l'appelant entrant 128
7 Caractéristiques des premiers essais sur le terrain (BETA) 130
7.1 Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration 130
7.2 Historique unifié des appels pour les lignes secondaires (Webex Calling uniquement) 134
7.3 Chiffrement de bout en bout (Webex Calling uniquement)..... 134
Mappage des balises personnalisées entre Webex pour Cisco BroadWorks et UC-One . 136
8 Annexe A : Chiffrements TLS..... 144
9 Annexe B : Script d'approvisionnement en étiquettes DM..... 145
9.1 Bureau..... 146
9.2 Portable..... 149
9.3 Tablette 152
9.4 Balises du système..... 155
10 Acronymes et abréviations..... 156

Confidentiel à Cisco

1 Résumé des changements

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

1.1 Modifications de la version 45.10, octobre 2025

Cette version du document inclut les modifications suivantes :

- Mise à jour de la section *6.1.21 Conférences téléphoniques N-Way* – a fusionné la section BÊTA *Amélioration des conférences téléphoniques N-Way (Webex Calling uniquement)*.
- Mise à jour de la section *6.1.22 Retirer un* appel – a fusionné la section BÊTA *Améliorations de renvoi d'appels*.
- [**Important**] Ajout de la section *Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration* en BÊTA.
    - Version du document 3 : des détails supplémentaires ont été inclus concernant la disponibilité du service d'informations de localisation d'urgence Cisco exclusivement pour le type de déploiement de Webex Calling.
- Ajout de la section *Historique unifié des appels pour les lignes secondaires (Webex Calling uniquement)* en BÊTA.
- Mise à jour de la section *6.1.36 Historique des appels* – ajout de la clarification selon laquelle l'historique des appels est synchronisé sur tous les périphériques uniquement pour la ligne principale de l'utilisateur.
- Ajout de la section *Chiffrement de bout en bout (Webex Calling uniquement)* en BÊTA.

1.2 Modifications pour la version 45.9, septembre 2025

Cette version du document inclut les modifications suivantes :

- Mise à jour de la section *Améliorations de la fonction d'extraction d'appel* – ajout de plus de détails.
- Mise à jour de la section *6.1.22 Retirer un* appel – ajout de plus de détails concernant la dépendance de la fonctionnalité sur la configuration du service côté serveur.
- Mise à jour de la section *6.1.25 Récupération automatique des appels / Transfert d'appel fluide* – ajout de plus de détails concernant la dépendance de la fonctionnalité par rapport à la fonction d'extraction d'appel et la tonalité lue pendant la récupération d'appel.

1.3 Modifications pour la version 45.8, août 2025

Cette version du document inclut les modifications suivantes :

- Mise à jour de la section *6.1.34 Configuration des codecs* – ajout de détails sur la résolution vidéo maximale H.264 par plateforme et la mise à jour de la version de bureau de l'application Webex.

Confidentiel à Cisco

1.4 Modifications pour la version 45.7, juillet 2025

Cette version du document inclut les modifications suivantes :

- Ajout de la section *Amélioration des conférences téléphoniques à n voies (Webex Calling uniquement)* en BÊTA.
- Ajout de la section *Améliorations de la fonction d'extraction d'appel* en BÊTA.

1.5 Modifications de la version 45.6, juin 2025

Aucune modification n'a été apportée à ce document pour cette version.

1.6 Modifications de la version 45.5, mai 2025

Cette version du document inclut les modifications suivantes :

- Suppression de la section Sélection CLID de l'agent de la file d'attente des appels – obsolète par *6.1.50.1 ID de l'appelant sortant*.
- Suppression des balises et attributs obsolètes.

1.7 Modifications de la version 45.4, avril 2025

Cette version du document inclut les modifications suivantes :

- Section déplacée *6.1.34.1 Codec AI* – hors BÊTA.
- Ajout de la section *6.1.51 Multiligne* – a combiné les sections BÊTA pour ordinateur de bureau uniquement et mobile.
- Section déplacée *6.1.52 Autorisation SIP améliorée* – hors BÊTA.
- Section déplacée *6.1.53 Assistant personnel (Présence en* absence) comme commun pour les ordinateurs de bureau et les périphériques mobiles

1.8 Modifications de la version 45.3, mars 2025

Aucune modification n'a été apportée à ce document pour cette version.

1.9 Modifications de la version 45.2, février 2025

Cette version du document inclut les modifications suivantes :

- Ajout de la section *Autorisation SIP améliorée* en version BÊTA.

1.10 Changements pour la version 45.1, janvier 2025

Cette version du document inclut les modifications suivantes :

- La section *Assistant personnel (Présence en* absence) a été déplacée hors BÊTA.
- Section déplacée *6.3.2.3 Mode de livraison (Webex Calling uniquement)* hors BÊTA.

1.11 Changements pour la version 44.12, décembre 2024

Aucune modification n'a été apportée à ce document pour cette version.

Confidentiel à Cisco

1.12 Modifications pour la version 44.11, novembre 2024

Cette version du document inclut les modifications suivantes :

- Ajout de la section *Mobile (Webex Calling uniquement)* en BÊTA.

1.13 Modifications de la version 44.10, octobre 2024

Cette version du document inclut les modifications suivantes :

- Ajout de la section *Assistant personnel (Présence en absence)* en version BÊTA.
- Ajout de la section *Mode de livraison (Webex Calling uniquement)* en BÊTA.

1.14 Modifications pour la version 44.9, septembre 2024

Aucune modification n'a été apportée à ce document pour cette version.

1.15 Modifications pour la version 44.8, août 2024

Cette version du document inclut les modifications suivantes :

- Mise à jour de la section *6.1.34 Configuration des* codecs - ajout de précisions sur les DTMF et les mécanismes de transmission pris en charge.

1.16 Modifications pour la version 44.7, juillet 2024

Cette version du document inclut les modifications suivantes :

- Ajout de la section *Codec AI* en BETA.
- Mise à jour de la section *6.1.641P44mary Profile* – suppression des détails sur le comportement de l'application Webex avant la Version 43,2.

1.17 Modifications de la version 44.6, juin 2024

Cette version du document inclut les modifications suivantes :

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

1.18 Modifications de la version 44.5, mai 2024

Cette version du document inclut les modifications suivantes :

- Section mise à jour *6.1.18 Assistance ICE (Webex Calling uniquement)* – IPv6 assistance ajoutée via NAT64.
- Mise à jour de la section *6.1.50 ID de* l'appelant - ajout de la sous-section *6.1.50.2 Nom de l'ID de* l'appelant distant.

1.19 Modifications de la version 44.4, avril 2024

Cette version du document inclut les modifications suivantes :

- Mise à jour de la section *6.1.50.1 ID de l'appelant sortant*.
- Section mise à jour *Modifications des fichiers de configuration de la version 44,3* – ajout de détails sur les mises à jour keepalive dans 44,3.

Confidentiel à Cisco

1.20 Modifications de la version 44.3, mars 2024

Cette version du document inclut les modifications suivantes :

- Section mise à jour *6.3.6. ID de l'appelant* entrant
    - La section *6.1.50.1 ID de l'appelant sortant* a été déplacée comme commune pour le bureau et le périphérique mobile et a été mise à jour avec plus de détails.
- Mise à jour de la section *6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou* UDP - ajout de détails sur les keepalives configurables à l'aide de balises personnalisées.

1.21 Modifications de la version 44.2, février 2024

Cette version du document inclut les modifications suivantes :

- Ajout de la section *6.3.6 ID de l'appelant entrant*
- Mise à jour de la section *6.2.8 Notifications de prise d'appel*
    - Ajout de la sous-section *6.2.8.1 Voyant d'occupation de* ligne - les spécificités du BLF y sont déplacées.
    - Ajout de la sous-section *6.2.8.2 Groupe de prise d'appel (Webex Calling uniquement)*.
- Ajout de la section *6.1.49 Informations sur le* renvoi d'appel.
- Mise à jour de la section *6.1.8.3 Renforcer la version* IP - ajout de détails sur le nouveau mode *nat64* .
- Mise à jour de la section *6.1.42 Suppression du bruit et extension de la bande passante* pour les appels RTCP/mobiles - ajout de détails sur la nouvelle prise en charge de l'extension de la bande passante et sur les mises à jour de la suppression du bruit. La section *Amélioration de la qualité de la parole pour les appels RTPC* est supprimée de la version BETA.

1.22 Modifications de la version 44.1, janvier 2024

Aucune modification n'a été apportée à ce document pour cette version.

Confidentiel à Cisco

2 Modifications des fichiers de configuration

2.1 Modifications des fichiers de configuration de la version 45.10

- [Webex Calling uniquement] La balise dans la section contrôle maintenant une fonctionnalité officielle.

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

- Le mode et les attributs par défaut-active-move-option (Bureau uniquement) dans la balise contrôlent maintenant une fonctionnalité officielle.

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

- [Important] [Fonctionnalité BÊTA] [Bureau et tablette uniquement] Ajout de la section sous , supprimant la section .

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


Confidentiel à Cisco

- [Webex Calling uniquement] Ajout d'une balise dans la section .

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

Les %TAG%s suivants ont été ajoutés :

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

Les %TAG%s suivants ont été obsolètes :

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

Pour plus d'informations, consultez *Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration*.

2.2 Modifications des fichiers de configuration de la version 45.9

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.3 Modifications des fichiers de configuration de la version 45.8

- [Desktop uniquement] Mise à jour de la résolution vidéo H.264 vers WIDE_FULL_HD – ajout des attributs de résolution, de cadence et de débit dans la balise pour le codec H.264 sous la section .<video>

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

2.4 Modifications des fichiers de configuration de la version 45.7

- [fonctionnalité BÊTA] [Webex Calling uniquement] Ajout de la balise dans la section .

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


Confidentiel à Cisco

- [Fonctionnalité BÊTA]Ajout des attributs du mode et de l'option de déplacement actif par défaut (Bureau uniquement) dans la balise .

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

Les %TAG%s suivants ont été ajoutés :

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

2.5 Modifications des fichiers de configuration de la version 45,6

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.6 Modifications des fichiers de configuration de la version 45,5

Les sections/balises suivantes ont été supprimées :

- [D/M]
  - Obsolète avec la version 42,12
  - Remplacé par les pour chaque ligne sous
- [D]
  - Remplacé par le pour chaque ligne sous les
- [D/M]
  - Obsolète avec la version 43,11
  - Remplacé par la dans
- [D/M] <service-uri>
  - Obsolète avec la version 42,12
  - Remplacé par le. pour chaque ligne sous
- [D/M] <suppression du bruit>
  - Obsolète avec la version 43,12
  - Remplacé par les < services>< calls>< speech-enhancements>
- [D/M] <numéro de centre>
  - Obsolète avec la version 42,12
  - Remplacé par le pour chaque ligne sous
- [D]

Confidentiel à Cisco

- Obsolète avec la version 44,3
- Remplacé par le

Les attributs suivants ont été supprimés :

- [D/M] url attribut sous
- [D/M] attribut avec marquage sous

Les %TAG%s suivants ont été supprimés :

- [D] %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%

2.7 Modifications des fichiers de configuration de la version 45,4

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.8 Modifications des fichiers de configuration de la version 45,3

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.9 Modifications des fichiers de configuration de la version 45,2

- [Fonctionnalité BÊTA] Ajout de la balise sous la section .

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

Le %TAG% suivant a été ajouté :

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.10 Modifications des fichiers de configuration de la version 45,1

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.11 Modifications des fichiers de configuration de la version 44,12

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.12 Modifications des fichiers de configuration de la version 44,11

- [Fonctionnalité BÊTA] [Mobile only] [Webex Calling only]Ajout de l'attribut multi-lignes dans la balise .

  Ajout de sections et pour les lignes secondaires sous la section .

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


Confidentiel à Cisco

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

2.13 Modifications des fichiers de configuration de la version 44,1

- [Fonctionnalité BÊTA] Ajout de la balise sous la section .

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

- [Fonctionnalité BÊTA] [Mobile uniquement] [Webex Calling uniquement]Ajout de l'attribut mode de livraison sous la balise .

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

Les %TAG%s suivants ont été ajoutés :

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.14 Modifications des fichiers de configuration de la version 44.9

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.15 Modifications des fichiers de configuration de la version 44.8

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.16 Modifications des fichiers de configuration de la version 44.7

- [Fonctionnalité BÊTA]
  Ajout du codec IA (xCodec) sous la section .<audio>

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


Confidentiel à Cisco

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

2.17 Modifications des fichiers de configuration de la version 44.6

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

2.18 Modifications des fichiers de configuration de la version 44.5

- [Webex Calling uniquement] Ajout de l'attribut enable-ipv6-support à la balise .

```
<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 a été ajoutée dans la section avec 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%

2.19 Modifications des fichiers de configuration de la version 44,4

- [Bureau uniquement] [Webex Calling uniquement] Ajout de balises , et sous la section .

```
<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>
```


Confidentiel à Cisco

2.20 Modifications des fichiers de configuration de la version 44,3

- [Bureau uniquement] [Webex Calling uniquement] Ajout de sous la nouvelle section , avec 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 Keep Alive activée codée en dur pour chaque transport sous .

```
<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%
- %TCP_KEEPALIVE_ENABLED_WXT%
- %TLS_KEEPALIVE_ENABLED_WXT%

2.21 Modifications des fichiers de configuration de la version 44,2

- [Mobile uniquement] Ajout de la section sous .
  Ajout de sous-balises et , avec une nouvelle sous-balise 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>
```


Confidentiel à Cisco

- [Mobile uniquement] [Webex Calling uniquement] Ajout de sous la nouvelle section .

```
<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 dans la section .

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

- [Bureau uniquement] [Webex Calling uniquement] Ajout de la section sous , avec et comme sous-balises.
  La balise a également été ajoutée sous chaque balise dans la section .

```
<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>
    …
```

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%

Confidentiel à Cisco

- %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 obsolète :

- %ENABLE_NOISE_REMOVAL_WXT%

2.22 Modifications des fichiers de configuration de la version 44,1

Il n'y a pas eu de mise à jour des fichiers de configuration pour cette version.

Confidentiel à Cisco

3 Introduction

L'objectif de ce document est de fournir une description de la configuration de Webex pour le client 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 en utilisant une configuration qui n'est pas visible par l'utilisateur final. Le *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 lorsqu'il démarre, après avoir été récupérés à partir de Gestion des périphériques. Les informations des fichiers de configuration sont stockées chiffrées, ce qui la rend invisible et inaccessible pour l'utilisateur final.

REMARQUE : Les propriétés XML ne doivent pas contenir d'espaces (par exemple, au lieu de).

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 du client localisé

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 son espace privé.

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

Lorsque la nouvelle version est téléchargée, l'ancien logiciel est écrasé ; toutefois, les données de l'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 de l'appareil

5.1 Balises de gestion des périphériques

Webex pour Cisco BroadWorks utilise les *Jeux de balises de gestion des périphériques* illustrés dans la figure suivante. Le site *System Default* et les jeux de balises personnalisés sont nécessaires pour définir les paramètres spécifiques des périphériques/clients. Ce jeu de balises permet de gérer avec souplesse les paramètres de connectivité du réseau/service du client ainsi que les contrôles d'activation des fonctionnalités.

Ce jeu de balises personnalisé est fourni par un administrateur système via l'option *System → Resources → Device Management Tag Sets* . L'administrateur doit ajouter de nouveaux jeux de balises :

- Cellulaire : Connect_Tags
- Tablette : ConnectTablet_Tags
- Bureau : BroadTouch_Tags

Créez chaque balise individuelle et définissez sa valeur. Les références des sections fournissent des descriptions détaillées pour chaque balise. Les balises personnalisées sont réparties en groupes en fonction de leur fonctionnalité et sont abordées plus loin dans ce document.

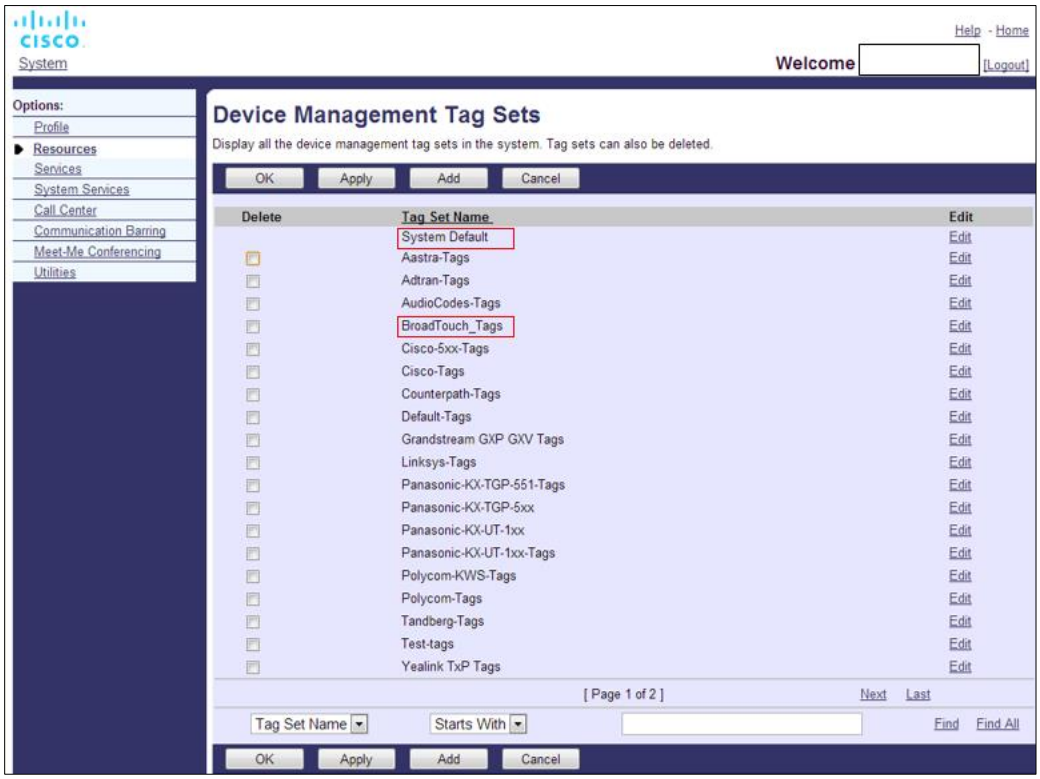


Figure 1 Desktop Device Management Tag Sets (ensembles de balises de gestion des dispositifs de bureau)

Confidentiel à Cisco

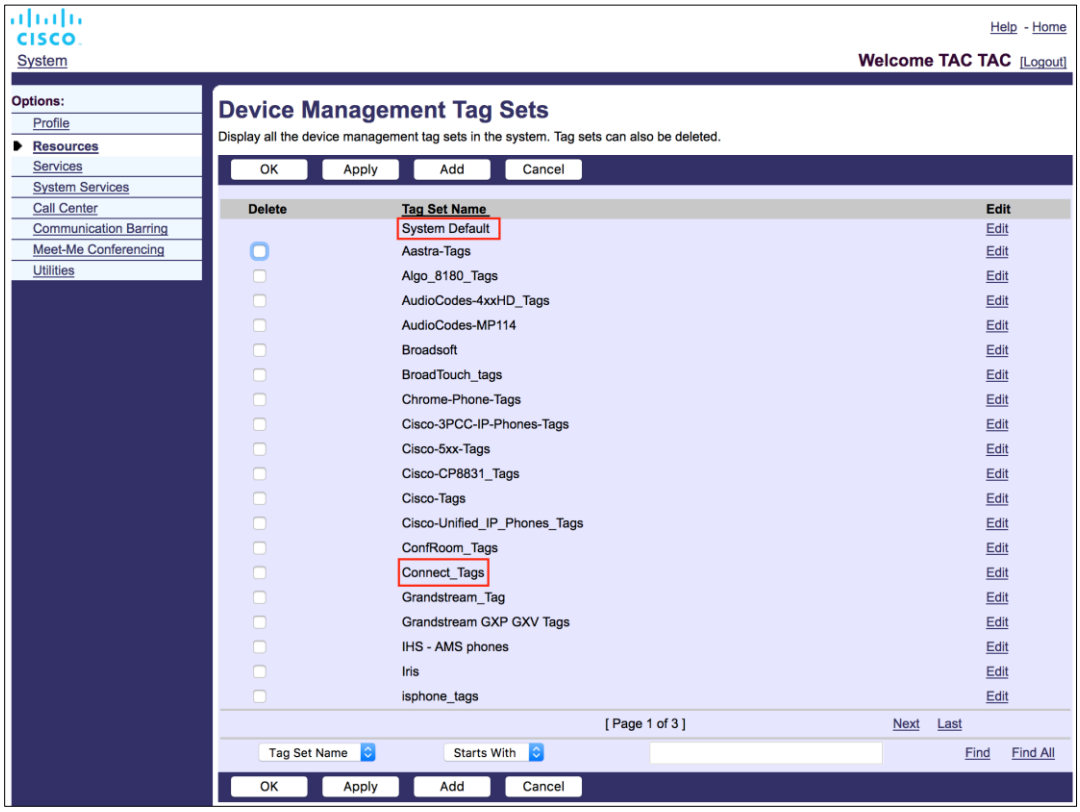


Figure 2 Jeux de balises pour la gestion des périphériques mobiles

5.2 Amélioration de la correspondance partielle pour la sélection du type d'appareil

Pour permettre une plus grande flexibilité lors de la sélection des ensembles de fonctionnalités pour les groupes d'utilisateurs ou les utilisateurs individuels, le type de profil d'appareil est sélectionné sur la base d'une (première) correspondance partielle. Cela permet aux clients d'utiliser différents types d'appareils.

La procédure générale de gestion des périphériques spécifie que le serveur d'applications Cisco BroadWorks fournit un type de profil de périphérique. Il s'appelle "Business Communicator - PC" pour les ordinateurs de bureau, "Connect - Mobile" pour les téléphones portables et "Connect - Tablet" pour les tablettes. Un profil d'appareil peut être créé et attribué à l'utilisateur. Le serveur d'application crée ensuite un fichier de configuration et le stocke sur le serveur de profil.

Lors de la connexion, le client interroge la liste des appareils attribués via Xsi et recherche le profil de type d'appareil correspondant. Le client choisit le premier profil qui commence par le nom du type d'appareil correspondant. Les données de configuration du profil de l'appareil (fichier de configuration) associées à ce profil sont ensuite utilisées pour activer et désactiver diverses fonctions.

Cela permet d'utiliser le même exécutable client avec différents types de profils d'appareils, de sorte que le fournisseur de services peut modifier les ensembles de fonctionnalités pour des utilisateurs individuels ou des groupes d'utilisateurs en changeant simplement le type de profil d'appareil dans DM pour un utilisateur ou un groupe d'utilisateurs.

Confidentiel à Cisco

Par exemple, le fournisseur de services peut disposer d'un nombre quelconque de types de profils d'appareils basés sur les rôles des utilisateurs, 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 d'appareil qui leur est destiné.

Notez qu'il n'est pas prévu d'avoir plusieurs types de profils d'appareils correspondants dans la liste XML des appareils reçus, mais un seul.

5.3 Configuration du client

La version Webex pour Cisco BroadWorks du client utilise le fichier *config-wxt.xml* pour la configuration de 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 – Tablette » et « Business Communicator – PC ». Webex pour Cisco BroadWorks utilise les mêmes profils de périphérique que UC-One afin de faciliter son déploiement.

REMARQUE 1 : Un fichier de configuration doit exister pour chaque profil d'appareil.

NOTE 2: Il est VIVEMENT RECOMMANDÉ que les modèles soient tenus à jour avec la dernière version de l'application Webex

5.5 Fichier de configuration (config-wxt.xml)

Les 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, il y a encore quelques balises (système) qui sont 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, voir la section *5.7 Balises du système intégré dynamique Cisco* BroadWorks.

- %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 du système

En tant qu'administrateur système, vous pouvez accéder aux balises System Default via l'option *System → Resources → Device Management Tag Sets* . Les balises System Default suivantes doivent être provisionnées lorsque le paquet VoIP Calling est installé.

Étiquette	Description
%SBC_ADDRESS_WXT%	Il doit être configuré comme le nom de domaine complet (FQDN) ou l'adresse IP du contrôleur de session (SBC) déployé dans le réseau. Exemple : sbc.yourdomain.com
%SBC_PORT_WXT%	Si SBC_ADDRESS_WXT est une adresse IP, ce paramètre doit être réglé sur le port SBC. Si le SBC_ADDRESS_WXT est un FQDN, il peut être laissé vide. Exemple : 5075

5.7 Balises du système intégré dynamique Cisco BroadWorks

En plus des balises système par défaut et des balises personnalisées qui doivent être définies, il existe des balises système Cisco BroadWorks existantes qui sont généralement utilisées et font partie du fichier d'archive de type de périphérique recommandé (DTAF). Ces balises sont énumérées dans cette section. En fonction de la solution installée, toutes les balises système ne sont pas utilisées.

Étiquette	Description
%BWNETWORK-CONFERENCE-SIPURI-n%	Ceci est l'URI du serveur utilisée pour activer le 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.
%BWLINEPORT-n%	Nom d'utilisateur SIP utilisé dans la signalisation SIP, par exemple, dans l'inscription.

Confidentiel à Cisco

Étiquette	Description
%BWHOST-n%	Il s'agit de la partie du domaine du port de ligne provisionné pour le dispositif attribué à l'utilisateur. Il est extrait du profil de l'utilisateur. Généralement utilisé comme domaine SIP.
%BWAUTHUSER-n%	Il s'agit du nom de l'utilisateur d'authentification. Si l'abonné s'est vu attribuer une authentification, il s'agit de l'ID utilisateur provisionné sur la page Authentification, quel que soit le mode d'authentification sélectionné pour le type d'appareil. 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 une authentification a été attribuée à l'abonné, il s'agit du mot de passe fourni sur la page Authentification, quelle que soit la valeur de mode d'authentification sélectionnée pour le 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 famille de l'abonné dans le profil de l'utilisateur. Le nom et le prénom sont concaténés ensemble. Dans le cas d'une configuration multilignes, si aucune étiquette de ligne n'est configurée et si elle n'est pas vide, elle est utilisée comme nom d'affichage pour la ligne dans le sélecteur de ligne.
%BWEXTENSION-n%	L'extension de l'abonné est récupérée à partir de l'extension fournie dans le profil de l'utilisateur. Si un poste n'a pas été provisionné, la balise est remplacée par le numéro de téléphone de l'abonné (DN).
%BWAPPEARANCE-LABEL-n%	Il s'agit de l'étiquette de ligne configurée. Utilisé comme nom de ligne, s'il n'est pas vide.
%BWDISPLAYNAMELINEPORT%	Il s'agit de la ligne/du port de la première ligne privée, par opposition à une ligne partagée (Shared Call Appearance). Il s'agit du port de ligne mis à disposition sur le périphérique attribué 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 domaine du port de ligne provisionné. Il est extrait du profil de l'utilisateur.

Confidentiel à Cisco

Étiquette	Description
%BWE911-PRIMARY-HELDURL%	Spécifie l'URL de la plateforme de localisation d'urgence RedSky prenant en charge le protocole HELD.
%BWE911-CUSTOMERID%	L'identifiant du client (HeldOrgId, CompanyID) utilisé pour la requête HTTPS de RedSky.
%BWE911-SECRETKEY%	Le secret pour authentifier la requête HTTPS de 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 balises utilisé par le type de périphérique. La balise "reserved" 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. **NOTE :** 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 des balises réservées est 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 balises 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 en 911, 0911, 933
%BW-MEMBERTYPE-n%	Il s'agit du type de chaque ligne. Il peut s'agir d'un "profil virtuel", d'un "utilisateur" ou d'un "lieu".
%BWUSEREXTID-n%	Il s'agit de l'ID externe pour la ligne donnée (Webex Calling uniquement)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Fournit des informations si le 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 Desktop et Mobile/Tablette.

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

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_REJECT_WITH_486_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.16 Comportement du rejet d'appel entrant*
%REJECT_WITH_XSI_MODE_WXT%	N	Outlook 2007/ Exchange 2003	déclin_faux	*6.3.2 Notifications Push pour les appels*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	Outlook 2007/ Exchange 2003	occupé(e)	*6.3.2 Notifications Push pour les appels*
%ENABLE_TRANSFER_CALLS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.20 Transfert*
%ENABLE_CONFERENCE_CALLS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.21 Conférences téléphoniques N-Way*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.21 Conférences téléphoniques N-Way*
%MAX_CONF_PARTIES_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	10	*6.1.21 Conférences téléphoniques N-Way*
%ENABLE_CALL_STATISTICS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.24 Statistiques de* l'appel
%ENABLE_CALL_PULL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.22 Retirer un* appel

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.2 Notifications Push pour les appels*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.28 Transcription des messages vocaux pour Webex Calling*
%ENABLE_MWI_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente*
%MWI_MODE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente*
%ENABLE_VOICE_MAIL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente*
%ENABLE_VISUAL_VOICE_MAIL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur de message en attente*
%ENABLE_FORCED_LOGOUT_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.1 Déconnexion forcée*
%FORCED_LOGOUT_APPID_WXT%	Outlook 2007/ Exchange 2003	N	vide	*6.2.1 Déconnexion forcée*
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.1 Renvoi d'appel Toujours*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.29.3 BroadWorks Anywhere*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_EMERGENCY_DIALING_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.1 Appels d'urgence*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	Outlook 2007/ Exchange 2003	911, 112	*6.3.1 Appels d'urgence*
%ENABLE_USE_RPORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.14 Gestion des ports SIP pour la traversée NAT*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%RPORT_USE_LOCAL_PORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.14 Gestion des ports SIP pour la traversée NAT*
%USE_TLS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel*
%SBC_ADDRESS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide	*5.6 Balises par défaut du système*
%SBC_PORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	5060	*5.6 Balises par défaut du système*
%USE_PROXY_DISCOVERY_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.6 Détection dynamique du proxy SIP*
%USE_TCP_FROM_DNS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.6 Détection dynamique du proxy SIP*
%USE_UDP_FROM_DNS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.6 Détection dynamique du proxy SIP*
%USE_TLS_FROM_DNS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.6 Détection dynamique du proxy SIP*
%DOMAIN_OVERRIDE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide	*6.1.6 Détection dynamique du proxy SIP*
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.6 Détection dynamique du proxy SIP*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.6 Détection dynamique du proxy SIP*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	O (Windows uniquement)	N	faux	*6.1.6 Détection dynamique du proxy SIP*
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	5000	*6.1.5 Délai d'expiration configurable pour l'ouverture du socket SIP*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	10000	*6.1.5 Délai d'expiration configurable pour l'ouverture du socket SIP*
%SOURCE_PORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	5060	*6.1.7 Utilisation du port préféré pour SIP*
%SIP_FAILBACK_ENABLED_WXT%	Outlook 2007/ Exchange 2003	N	vrai	*6.1.8.2 Restauration SIP*
%SIP_FAILBACK_TIMEOUT_WXT%	Outlook 2007/ Exchange 2003	N	900	*6.1.8.2 Restauration SIP*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.1.8.2 Restauration SIP*
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	dns	*6.1.8.3. Renforcer la version IP*
%USE_ALTERNATIVE_IDENTITIES_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.10 Utiliser les URI associés à* P dans REGISTER
%TCP_SIZE_THRESHOLD_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	18000	*6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou UDP*
%SIP_REFRESH_ON_TTL_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.1.8.4 Gestion DNS TTL*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.12 Prise en charge* de la MISE À JOUR SIP
%ENABLE_PEM_SUPPORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.11 En-tête SIP P-Early Media (PEM)*
%ENABLE_SIP_SESSION_ID_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.15 ID de session SIP*
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.13 FIR INFO SIP hérité*
%SRTP_ENABLED_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel*
%SRTP_MODE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel*
%ENABLE_REKEYING_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.2 SIP sur TLS et protocole de transport sécurisé en temps réel*
%RTP_AUDIO_PORT_RANGE_START_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	8000	*6.1.17 Plage de ports du protocole de transport en temps réel*
%RTP_AUDIO_PORT_RANGE_END_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	8099	*6.1.17 Plage de ports du protocole de transport en temps réel*
%RTP_VIDEO_PORT_RANGE_START_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	8100	*6.1.17 Plage de ports du protocole de transport en temps réel*
%RTP_VIDEO_PORT_RANGE_END_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	8199	*6.1.17 Plage de ports du protocole de transport en temps réel*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_RTCP_MUX_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.19 MUX RTCP*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.33 Chaîne d'événements XSI*
%CHANNEL_HEARTBEAT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	10000	*6.1.33 Chaîne d'événements XSI*
%XSI_ROOT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide (utilise l'URL d'origine)	*6.1.32 Racines et chemins XSI*
%XSI_ACTIONS_PATH_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	/com.broadsoft.xsi-actions/	*6.1.32 Racines et chemins XSI*
%XSI_EVENTS_PATH_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	/com.broadsoft.xsi-events/	*6.1.32 Racines et chemins XSI*
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.25 Récupération automatique des appels / Transfert d'appel fluide*
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	Outlook 2007/ Exchange 2003	cs-only	*6.3.1 Appels d'urgence*
%ENABLE_CALL_PICKUP_BLIND_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.2 Prise d'appel*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.2 Prise d'appel*
%WEB_CALL_SETTINGS_URL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%USER_PORTAL_SETTINGS_URL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%ENABLE_CALL_CENTER_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.31 Connexion/déconnexion du centre d'appels/de la* file d'attente des appels
%WEB_CALL_SETTINGS_TARGET_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	externe	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.30 Portail des paramètres et paramètres d'appel sur le Web*
%USE_MEDIASEC_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.3 3GPP En-têtes SIP pour SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.4 Cliquer pour composer (Rappeler)*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%DIALING_CALL_BACK_TIMER_WXT%	N	Outlook 2007/ Exchange 2003	10	*6.3.4 Cliquer pour composer (Rappeler)*
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.3 Assistance Boss-Admin (Cadre de direction-Assistant)*
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	Outlook 2007/ Exchange 2003	35	*6.3.2 Notifications Push pour les appels*
%ENABLE_CALL_RECORDING_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.26 Enregistrement des* appels
%ENABLE_SINGLE_ALERTING_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.3 Alerte unique*
%ENABLE_CALL_PARK_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.23 Parquage d'appel/Récupérer*
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	10	*6.1.23 Parquage d'appel/Récupérer*
%ENABLE_RTP_ICE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.18 Assistance ICE (Webex Calling uniquement)*
%RTP_ICE_MODE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	icestun	*6.1.18 Assistance ICE (Webex Calling uniquement)*
%RTP_ICE_SERVICE_URI_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vide	*6.1.18 Assistance ICE (Webex Calling uniquement)*
%RTP_ICE_PORT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	3478	*6.1.18 Assistance ICE (Webex Calling uniquement)*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_RTP_ICE_IPV6_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.18 Assistance ICE (Webex Calling uniquement)*
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.1.8.4 Gestion DNS TTL*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.4 Transférer les appels SIP vers la réunion*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.5 Appels de contrôle du téléphone de bureau* – Réponse automatique
%ENABLE_DIALING_VOIP_WXT%	N	Outlook 2007/ Exchange 2003	vrai	*6.3.5 Prise en* charge MNO *Appeler avec le numéroteur natif*
%ENABLE_DIALING_NATIVE_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.5 Prise en* charge MNO *Appeler avec le numéroteur natif*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.35 Numérotation SIP-URI*
%ENABLE_SIP_VIDEOCALLS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.37 Désactiver les appels vidéo*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.37 Désactiver les appels vidéo*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	Bureau - vrai Mobile, Tablette - faux	*6.1.37 Désactiver les appels vidéo*
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	Y	Mobile – N Tablette – Y	faux	*6.1.38 Appels d'urgence (911) - Création de rapports de localisation avec le* fournisseur E911

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	Y	Mobile – N Tablette – Y	0	*6.1.38 Appels d'urgence (911) - Création de rapports de localisation avec le* fournisseur E911
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	Y	Mobile – N Tablette – Y	-1	*6.1.38 Appels d'urgence (911) - Création de rapports de localisation avec le* fournisseur E911
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	Y	Mobile – N Tablette – Y	une fois par connexion	*6.1.38 Appels d'urgence (911) - Création de rapports de localisation avec le* fournisseur E911
%ENABLE_AUTO_ANSWER_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.6 Réponse automatique avec notification de tonalité*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.41 Indication des appels indésirables*
%ENABLE_NOISE_REMOVAL_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.42 Suppression du bruit et extension de la bande passante pour les appels RTCP/mobiles*
%ENABLE_AUDIO_MARI_FEC_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.46.2 Correction des erreurs de renvoi (FEC) et retransmission des paquets* (RTX)
%ENABLE_AUDIO_MARI_RTX_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.46.2 Correction des erreurs de renvoi (FEC) et retransmission des paquets* (RTX)
%ENABLE_VIDEO_MARI_FEC_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.46.2 Correction des erreurs de renvoi (FEC) et retransmission des paquets* (RTX)
%ENABLE_VIDEO_MARI_RTX_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.46.2 Correction des erreurs de renvoi (FEC) et retransmission des paquets* (RTX)
%ENABLE_CALL_BLOCK_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.45 Liste de blocage (Webex Calling uniquement)*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	Outlook 2007/ Exchange 2003	vrai	*6.3.5.6 MNO Mobility - Widget en* cours d'appel
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	Outlook 2007/ Exchange 2003	vrai	*6.3.5.6 MNO Mobility - Widget en* cours d'appel
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	Outlook 2007/ Exchange 2003	vrai	*6.3.5.6 MNO Mobility - Widget en* cours d'appel
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.47 Appels simultanés avec le même utilisateur*
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.11 Pack d'événements pour le contrôle de la coupure du son à distance (Webex Calling uniquement)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.29.2 Transfert d'appel vers la messagerie vocale*
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.8.1 Basculement SIP*
%ENABLE_CALL_MOVE_HERE_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.12 Déplacer l'appel*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.42 Suppression du bruit et extension de la bande passante pour les appels RTCP/mobiles*
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	Outlook 2007/ Exchange 2003	vide	*6.3.5.1 Appeler avec le numéroteur natif*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.20 Transfert*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.6 ID de l'appelant entrant*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.6 ID de l'appelant entrant*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.1.50 ID de l'appelant* *ID de l'appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.1.50 ID de l'appelant* *ID de l'appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.1.50 ID de l'appelant* *ID de l'appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.1.50 ID de l'appelant* *ID de l'appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.1.50 ID de l'appelant* *ID de l'appelant sortant*
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.49 Informations sur le renvoi d'appel*
%ENABLE_BUSY_LAMP_FIELD_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.8.1 Voyant d'occupation de ligne*
%ENABLE_BLF_DISPLAY_CALLER_WXT%	Outlook 2007/ Exchange 2003	N	vrai	*6.2.8.1 Voyant d'occupation de ligne*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%BLF_NOTIFICATION_DELAY_TIME_WXT%	Outlook 2007/ Exchange 2003	N	0	*6.2.8.1 Voyant d'occupation de ligne*
%ENABLE_GCP_NOTIFICATIONS_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.8.2 Groupe de prise d'appel (Webex Calling uniquement)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	Outlook 2007/ Exchange 2003	N	faux	*6.2.8.2 Groupe de prise d'appel (Webex Calling uniquement)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	Outlook 2007/ Exchange 2003	N	120	*6.2.8.2 Groupe de prise d'appel (Webex Calling uniquement)*
%UDP_KEEPALIVE_ENABLED_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	vrai	*6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou UDP*
%TCP_KEEPALIVE_ENABLED_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou UDP*
%TLS_KEEPALIVE_ENABLED_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou UDP*
%ENABLE_MULTI_LINE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.51 Multiligne*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.2.4 Transférer les appels SIP vers la réunion (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.5.3 Identité de la ligne d'appel sortante (CLID) – Double* identité
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	Outlook 2007/ Exchange 2003	faux	*6.3.5.36.3.5.3 Identité de la ligne appelante sortante (CLID)*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	résolu(s)	*6.1.50.2 Nom de l'ID de l'appelant distant*
%PERSONAL_ASSISTANT_ENABLED_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.53 Assistant personnel (Présence en absence)*
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	Outlook 2007/ Exchange 2003	nps	*Mode de livraison (Webex Calling uniquement)*
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.52 Autorisation SIP améliorée*
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.21 Conférences téléphoniques N-Way*
%CALL_PULL_MODE_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	Masque de plongée	*6.1.22 Retirer un* appel
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	Outlook 2007/ Exchange 2003	N	déplacement_appel	*6.1.22 Retirer un* appel
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*6.1.36 Historique des appels*
%ENABLE_EMERGENCY_LOCATION_WXT%	Y	Mobile – N Tablette – Y	faux	*Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration*
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	Y	Mobile – N Tablette – Y	0	*Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration*
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	Y	Mobile – N Tablette – Y	-1	*Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration*

Confidentiel à Cisco

Étiquette	Utilisé dans les ordinateurs de bureau	Utilisé dans Mobile/ Tablette	Valeur par défaut	Section
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	Y	Mobile – N Tablette – Y	une fois par connexion	*Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration*
%ENABLE_CALLS_E2EE_WXT %	Outlook 2007/ Exchange 2003	Outlook 2007/ Exchange 2003	faux	*Chiffrement de bout en bout (Webex Calling uniquement)*

Pour plus d'informations sur le mappage des balises personnalisées utilisées dans Webex pour Cisco BroadWorks à celles utilisées par UC-One, voir la section *0 Mappage 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 est effectué en modifiant le fichier *config-wxt.xml* . En règle générale, les paramètres suivants doivent être modifiés :

- Domaine SIP. Il est utilisé comme partie du domaine de l'URI SIP propre (l'URI SIP propre est aussi parfois appelé port de ligne) en général dans les en-têtes SIP et dans les appels distants (XSI). La partie utilisateur de sa propre URI SIP provient de la configuration des informations d'authentification SIP (paramètre sous).
- URI du serveur SIP ou adresse IP du serveur proxy SIP en cas d'échec de la résolution DNS. Notez que pour utiliser TLS, les adresses IP ne peuvent pas être utilisées dans le paramètre proxy, car la validation du certificat TLS échouerait. Pour plus d'informations sur le port proxy, reportez-vous à la balise DM %SOURCE_PORT_WXT%. Notez que la fonction de gestion du TTL DNS ne peut pas être utilisée lorsqu'une adresse IP est utilisée dans le paramètre de l'adresse du 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 fonctions d'appel. Toutefois, les paramètres précédents permettent d'assurer une fonctionnalité de base pour les éléments suivants :

- S'inscrire sur le réseau SIP.
- Passer des appels audio ou vidéo.
- Découverte de proxy basée sur le DNS, ce 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, voir la section *6.1.27 Messagerie vocale, messagerie vocale visuelle, indicateur* de message en attente.

Notez que la configuration SIP de base est toujours nécessaire pour le MWI, même lorsque les appels SIP sont désactivés. Le 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 découverte du proxy DNS permet de prendre en charge de nombreux proxys, qui nécessitent une configuration correcte du DNS.

En outre, les temporisateurs 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 d'aller-retour sur le réseau.
- T2 - le délai maximal, en millisecondes, avant la retransmission des demandes de non-invitation et des réponses d'invitation.
- T4 - la durée maximale, en millisecondes, pendant laquelle un message reste dans le réseau.

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

L'exemple et le tableau suivants fournissent des informations sur les balises DM les plus courantes 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>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
              <credentials>
                     <username>%BWLINEPORT-1%</username>
                     <password>%BWAUTHPASSWORD-1%</password>
                     <auth>
                            <auth401>
                                   <default>
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </default>
                                   <realm id="%BWHOST-1%">
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </realm>
                            </auth401>
                            <auth407>
                                   <default>
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </default>
                                   <realm id="%BWHOST-1%">
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </realm>
                            </auth407>
                     </auth>
              </credentials>
       </line>
```


Confidentiel à Cisco

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%BWLINEPORT-n%	vide	String	Typiquement le nom d'utilisateur SIP. Pour plus d'informations, voir la section *5.7 Balises du système intégré dynamique Cisco* BroadWorks. Exemple : johndoe
%BWAUTHPASSWORD-n%	vide	String	Typiquement le mot de passe SIP. Pour plus d'informations, voir la section *5.7 Balises du système intégré dynamique Cisco* BroadWorks. Exemple : mot de passe secret
%BWE164-n%	vide	numéro de téléphone	Numéro de téléphone par défaut de l'utilisateur au format international. Pour plus d'informations, voir la section *5.7 Balises du système intégré dynamique Cisco* BroadWorks. Exemple : 12345678
%SBC_ADDRESS_WXT%	vide	String	Pour plus d'informations, voir la section *5.6 Balises par défaut du système*. Exemple : sbcexample.domain.com
%SBC_PORT_WXT%	5060	numéro	Pour plus d'informations, voir la section*5.6 Balises par défaut du système*. Exemple : 5060
%BWHOST-n%	vide	String	Généralement utilisé comme domaine SIP. Pour plus d'informations, voir la section *5.7 Balises du système intégré dynamique Cisco* BroadWorks. Exemple : exampledomain.com
%SOURCE_PORT_WXT%	5060	numéro	Généralement utilisé pour le paramètre *preferred-port* . Pour plus d'informations, voir la section *6.1.7 Utilisation du port préféré* pour SIP. Exemple : 5061
%BWUSEREXTID-n%	vide	String	(Webex Calling uniquement) Contient l'ID externe de la ligne Pour plus d'informations, consultez *6.1.51 Multiligne*. Exemple : 30f69bf7-710b-4cd0-ab4b-35ab393a1709

Confidentiel à Cisco

REMARQUE : Il est fortement recommandé que le port SIP soit différent de 5060 (par exemple, 5075) en raison des problèmes connus lors de l'utilisation du port SIP standard (5060) avec les appareils 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 le protocole de transport sécurisé en temps réel (SRTP) pour le cryptage des médias. Toutefois, ces fonctions doivent être activées dans la configuration, comme le montre l'exemple suivant. Notez également que lorsque la détection dynamique du proxy SIP est utilisée, les priorités DNS SRV priment sur les paramètres statiques tels que celui-ci (%USE_TLS_WXT%) et que 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, voir la section *6.1.6 Détection dynamique du proxy* SIP.

Lorsque la découverte dynamique de proxy n'est pas utilisée, l'activation de TLS pour SIP permet de l'utiliser.

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

Notez que le certificat utilisé doit être valide. En outre, la chaîne de certificats doit être intacte afin que le certificat intermédiaire soit également lié. Il est recommandé d'utiliser un certificat largement répandu qui soit déjà présent, par défaut, sur les appareils. Il est également possible d'ajouter des certificats localement sur l'ordinateur de bureau, soit manuellement, soit en utilisant l'approvisionnement en masse, bien que cela ne se fasse généralement pas.

Un paramètre distinct permet d'activer le protocole SRTP pour le cryptage des médias.

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

Pour les algorithmes de chiffrement SIP/TLS, voir *Annexe A : Chiffrements TLS.*

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

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

La version actuelle du cadre média prend en charge l'AES 128 Counter Mode pour la protection et le HMAC (Hash Message Authentication Code) -SHA-1 pour l'authentification. La taille de la clé principale est de 16 octets et celle du sel principal de 14 octets.

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

Confidentiel à Cisco

SRTP peut être activé à l'aide de la configuration présentée dans l'exemple suivant. L'implémentation actuelle utilise uniquement le profil RTP sécurisé SDP et prend en charge le SDP multiligne pour Audio Visual Profile (AVP) et Secure Audio Visual profile (SAVP) entries. 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 ne prennent en charge que le cryptage 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 m-lignes sont toujours utilisées. Des lignes m distinctes sont utilisées pour l'AVP et la SAVP.

Il convient toutefois d'accorder une attention particulière à la configuration du SBC, en veillant notamment 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 de réseau différentes sont toutefois possibles : dans certains déploiements, le SBC n'est pas impliqué dans le trafic média, tandis que dans d'autres déploiements, chaque segment de média RTP du client vers le SBC est crypté séparément et négocié via le SBC. Dans certains déploiements, le SBC n'autorise pas les lignes SDP multiples.

Le SBC peut également modifier l'ordre des m-lignes SDP lors de l'établissement 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 fonctionnelle sont amenés à préférer le trafic crypté ou non crypté. Les différentes options de configuration de SRTP sont les suivantes :

- Obligatoire - Lors de l'établissement de l'appel, le SDP initial ne comprend 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, de sorte que seuls les appels SRTP sont possibles.
- Preferred - Lors de l'établissement de l'appel, le SDP initial comprend à la fois les lignes m AVP et SAVP, mais SAVP est en premier lors de l'offre, ce qui indique l'ordre de préférence. Lorsqu'il répond, 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. Lorsqu'il répond, le client sélectionne la première ligne m, AVP ou SAVP.
- SRTP non activé - Il n'y a pas de ligne SAVP m dans le SDP initial lors de l'offre. Lors de la réponse, la fonction SAVP n'est pas acceptée et seuls les appels RTP sont possibles.
- Transport - Sélectionne 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 les mêmes.

```
<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 le protocole SRTP est activé.

Dans certains déploiements, la recomposition des clés pour SRTP n'est pas prise en charge. Il existe donc un paramètre de configuration permettant d'activer/désactiver la recomposition SRTP. Toutefois, les nouvelles clés sont toujours prises en compte lorsqu'elles sont reçues dans un SDP mis à jour conformément à la norme rfc3264. La configurabilité ne concerne que l'envoi de nouvelles clés.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USE_TLS_WXT%	false	vrai, faux	Si la valeur est "false", le protocole SIP TLS est désactivé. Lorsqu'il est défini sur « vrai », SIP TLS est activé. Veuillez noter que si *6.1.6 Détection dynamique du proxy* SIP est utilisé, ce paramètre est ignoré.
%SRTP_ENABLED_WXT%	false	vrai, faux	Lorsqu'il est défini sur « false », SRTP est désactivé. Lorsqu'il est défini sur « vrai », SRTP est activé.
%SRTP_MODE_WXT%	facultatif	obligatoire, préférée, facultative, transport	Définit la préférence accordée à SRTP lors de l'établissement de l'appel. La valeur par défaut est "optional".
%ENABLE_REKEYING_WXT%	vrai	vrai, faux	Active la recomposition des clés SIP (SDP) pour SRTP.

NOTE: Si la prise en charge d'ICE est activée (voir *6.1.18 Assistance ICE (Webex Calling uniquement)*), la réinitialisation sera toujours effectuée (la valeur%ENABLE_REKEYING_WXT% de la configuration est ignorée).

6.1.3 3GPP En-têtes SIP pour SRTP

Les spécifications 3GPP les plus récentes exigent des en-têtes SIP supplémentaires pour utiliser le protocole de transport sécurisé en temps réel (SRTP). Pour plus d'informations, voir *3GPP TS 24.229* ainsi que les documents suivants :

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

Les en-têtes requis par cette spécification peuvent interrompre les appels SIP dans les déploiements où cette spécification n'est pas utilisée. Il est donc recommandé de n'utiliser ces en-têtes que dans les environnements où le serveur les prend en charge.

Confidentiel à Cisco

Seule l'activation de l'utilisation des en-têtes est configurable. Il n'existe pas d'autres possibilités de configuration 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.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USE_MEDIASEC_WXT%	false	vrai, faux	Active les en-têtes SIP 3GPP pour la négociation SRTP.

6.1.4 Forcer l'utilisation et les keepalives TCP, TLS ou UDP

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

L'exemple suivant illustre ce nœud de configuration.

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

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs prises en charge (Octets)	Description
%TCP_SIZE_THRESHOLD_WXT%	0	0	Force l'utilisation de TCP. La décision d'utiliser TCP ou UDP pour le client appartient au fournisseur de services ; toutefois, il est recommandé d'utiliser TCP avec la valeur par défaut "0".
	0	1 - 99,000	Force l'utilisation de UDP 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	100000	Force l'utilisation du protocole UDP.

Confidentiel à Cisco

Le même nœud de configuration comporte également des paramètres pour UDP, TCP et TLS keepalive, comme le montre l'exemple suivant.

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

Les paramètres possibles sont les suivants :

- Activation du keepalive TCP ou TLS, valeurs possibles - true/false, la valeur par défaut est "false" si le nœud est manquant. Notez que lorsque cette fonction est activée, les keepalives TCP sont envoyés même si le transport UDP est utilisé pour le SIP.
- Activation de la clé UDP keepalive, 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 envoyées même si le transport TCP est utilisé pour SIP. En outre, même si TCP est utilisé pour SIP, le client accepte également le trafic sur UDP conformément à *RFC 3261*.
- Timeout spécifie le temps maximum d'inactivité en secondes après lequel le message keepalive est envoyé. L'absence de valeur signifie que le keepalive est désactivé pour le protocole.
- Charge utile pour les messages keepalive, valeurs possibles (aucune valeur signifie que keepalive est désactivé pour le protocole) :
  - Crlf
  - Nul (à ne pas utiliser)
  - Chaîne personnalisée (**à ne pas utiliser**)

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

Confidentiel à Cisco

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%UDP_KEEPALIVE_ENABLED_WXT%	vrai	vrai, faux	Contrôle si les paquets "keep-alive" doivent être envoyés pour le transport UDP.
%TCP_KEEPALIVE_ENABLED_WXT%	false	vrai, faux	Contrôle si les paquets de maintien de connexion doivent être envoyés pour le transport TCP.
%TLS_KEEPALIVE_ENABLED_WXT%	false	vrai, faux	Contrôle si les paquets de maintien de connexion doivent être envoyés pour le transport TLS.

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

Auparavant, le délai d'ouverture d'une socket SIP était codé en dur à 5 secondes pour TCP et 10 secondes pour TLS. Ces délais sont désormais 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 de connexion au socket (en millisecondes).

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	- le délai d'expiration en millisecondes	Le délai de connexion à la socket lorsque le transport TCP est utilisé.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	- le délai d'expiration en millisecondes	Le délai d'attente de la connexion du socket lorsque le transport TLS est utilisé.

6.1.6 Détection dynamique du proxy SIP

Pour activer la fonctionnalité de découverte de proxy dynamique SIP, voir 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 quels protocoles de transport les entrées DNS SRV sont utilisées lorsque plusieurs sont disponibles, en suivant les procédures décrites dans cette section.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USE_PROXY_DISCOVERY_WXT%	false	vrai, faux	Permet la découverte dynamique de proxy SIP pour les appels audio et vidéo. La valeur recommandée est "true".
%SBC_ADDRESS_WXT%	vide	Chaine de caractères	Cette balise Cisco BroadWorks est généralement utilisée pour le paramètre de nom d’enregistrement. Il doit s'agir d'une URL valide, et non d'une adresse IP. Pour plus d'informations, voir la section*5.6 Balises par défaut du système*. Exemple : sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	vide	Chaine de caractères	Cette balise personnalisée est utilisée pour la substitution de domaine. Pour plus d'informations, reportez-vous à la section suivante. Exemple : other.domain.com

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USE_TCP_FROM_DNS_WXT%	vrai	vrai, faux	Si la valeur de ce paramètre est "false", les résultats des DNS SRV pour ce protocole de transport (TCP) sont rejetés. Si "true", les résultats du DNS SRV pour ce protocole de transport (TCP) sont utilisés. En fonction des priorités SRV, un autre transport peut encore être élu.
%USE_UDP_FROM_DNS_WXT%	vrai	vrai, faux	Si la valeur de ce paramètre est « false » (faux), les résultats DNS SRV pour ce protocole de transport (UDP) sont ignorés. Si « vrai », alors les résultats de DNS SRV pour ce protocole de transport (UDP) sont utilisés. En fonction des priorités SRV, un autre transport peut encore être élu.
%USE_TLS_FROM_DNS_WXT%	vrai	vrai, faux	Si la valeur de ce paramètre est « false » (faux), les résultats DNS SRV pour ce protocole de transport (TLS) sont ignorés. Si « vrai », alors les résultats du DNS pour ce protocole de transport (TLS) sont utilisés. En fonction des priorités 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. Il n'est pris en compte que lorsque la découverte de services SRV/NAPTR est activée.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	vrai, faux	vrai	Si la valeur est "true" et que la recherche de services NAPTR échoue ou ne donne aucun résultat, la recherche de services SRV est effectuée pour l'hôte configuré. Si la valeur est "false", aucune recherche SRV n'est effectuée.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	vrai, faux	faux	Permet de contourner le cache DNS du système d'exploitation.

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

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

1. Effectuez une requête NAPTR en utilisant le champ ci-dessus pour obtenir les URI du serveur avec les protocoles de transport s'ils existent. La valeur du paramètre doit être le domaine complet que DNS doit résoudre et ne peut pas être une adresse IP.

Confidentiel à Cisco

2. Résoudre les éléments trouvés dans la requête NAPTR à l'aide d'une requête SRV pour obtenir l'URI et le port du serveur final. La partie du domaine utilisée dans la requête SRV est tirée du résultat de la requête NAPTR pour trouver l'URI (et le port) du serveur final. Le port reçu de DNS SRV-query 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 résolus à l'aide de SRV. Voir les exemples suivants pour l'utilisation des différents noms d'enregistrement.

   Si aucun NAPTR n'est trouvé, alors le client tente une requête SRV avec le nom d'enregistrement pris du paramètre sauf s'il y a un paramètre présent auquel cas 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 de transmission de contrôle de flux (SCTP) n'est pas pris en charge. Si les requêtes SRV ne donnent aucun résultat, la découverte du proxy échoue et l'utilisateur final reçoit un message d'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 solution de secours, le client vérifie toujours si le proxy statique configuré fonctionne, uniquement avec des requêtes A vers l'URI spécifié dans l' afin de voir s'il fournit une adresse IP qui fournit un enregistrement SIP opérationnel. Le port et le transport dans ce cas de dernier recours proviennent des paramètres tcp-threshold et .

3. Résoudre les URI trouvés à l'aide de la requête A-record. Les adresses IP finales reçues sont essayées dans l'ordre dans lequel elles ont été reçues afin d'obtenir une connexion fonctionnelle au proxy SIP. Cet ordre peut être défini par le fournisseur de services dans le DNS. Le premier URI de proxy SIP, dont la consultation de l'enregistrement A a réussi, est sélectionné et utilisé jusqu'à ce qu'il ne fonctionne plus ou que le client se déconnecte. Dans l'étape 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

REMARQUE 1 : Si la recherche de proxy DNS entraîne la sélection d'un protocole de transport dans l'étape SRV en recevant un URI de proxy SIP fonctionnel pour un protocole de transport, elle remplace le paramètre *tcp-threshold* généralement utilisé pour sélectionner UDP ou TCP dans le fichier de configuration. Il en va de même pour la configuration de SIP/TLS. TCP ou UDP est utilisé en fonction de la priorité dans le DNS.

NOTE 2: Les éléments reçus via SRV sont prioritaires sur le proxy statique dans le fichier de configuration. L'ordre NAPTR n'est pas pris en compte ; seule la priorité SRV compte. Lorsque SRV aboutit à plusieurs éléments ayant le même protocole de transport, la même priorité et le même poids, l'un d'entre eux est sélectionné au hasard. Les pondérations NAPTR ne sont pas prises en charge dans cette version, mais les pondérations SRV le sont. La priorité SRV est examinée en premier lieu et, pour les éléments de même priorité, le poids est examiné pour déterminer la probabilité qu'un serveur donné soit essayé ensuite.

NOTE 3: Le paramètre facultatif *domain-override* permet de résoudre par SRV un nom d'enregistrement A autre que celui indiqué dans le paramètre de configuration du domaine SIP lorsque les résultats NAPTR sont omis. Les exemples suivants illustrent l'utilisation du paramètre *domain-override* .

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

Confidentiel à Cisco

NOTE 5: Le type de 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 ne prend en charge que certains préfixes pour les services NAPTR. Les préfixes pris en charge sont énumérés ci-dessous :

SIP+D2U -> _sip._udp

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

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

Exemple 1 : Utilisation de la découverte de proxy DNS sans paramètre de configuration domain-override

Voici un exemple de configuration utilisant la découverte de proxy SIP lorsque seul le protocole SIP over TCP est utilisé et que la requête NAPTR de l'étape 1 renvoie des 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>
```

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

Par conséquent, l'enregistrement SIP s'effectue via TCP sur le port 5061 (reçu lors de l'étape SRV) et vers l'adresse IP 1.2.3.4.

Exemple 2 : **Utilisation du paramètre domain-override dans le fichier de configuration**

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

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


Confidentiel à Cisco

```
<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, 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 s'effectue sur UDP à l'aide du port 5061 (reçu à l'étape SRV) et vers l'adresse IP 4.3.2.1.

Exemple 3 : **Utilisation des priorités SRV**

Voici 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 que plusieurs enregistrements NAPTR et SRV avec des priorités différentes sont reçus. Dans ce cas, seule la priorité SRV compte dans cet événement de libération, 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 s'effectue sur TCP à l'aide du port 5061 (reçu à l'étape SRV) et vers l'adresse IP 1.2.3.4 qui prendrait en charge à la fois UDP et TCP.

Confidentiel à Cisco

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

Voici 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 des 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>
```

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._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 s'effectue via TCP sur le port 5061 (reçu lors de l'étape SRV) et vers l'adresse IP 1.2.3.4.

6.1.7 Utilisation du port préféré pour SIP

Dans certains cas, un autre logiciel fonctionnait sur la même machine que le client et occupait le port SIP par défaut. Pour configurer le client afin qu'il utilise un autre port pour SIP, le paramètre *preferred-port* peut être utilisé. Le client essaie d'utiliser la valeur de port configurée spécifiée dans le paramètre *preferred-port* , mais si elle est prise, le client essaie 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 essaie 6001, 6002, 6003, et ainsi de suite jusqu'à ce qu'il trouve un port inutilisé. Lorsqu'un port inutilisé est trouvé, il l'utilise pour sa propre communication SIP.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SOURCE_PORT_WXT%	5060	numéro	Spécifie le port SIP local préféré pour la communication. Exemple : 5060

Confidentiel à Cisco

6.1.8 SIP Failover et Failback

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

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

- La découverte de proxy SIP est activée et le serveur DNS possède des enregistrements NAPTR et/ou SRV pour le FQDN du SBC (voir la section *6.1.6 Détection dynamique du proxy* SIP), OU
- L'adresse du proxy SIP est fournie sous la forme d'un FQDN et est résolue en plusieurs adresses IP (voir la section *6.1.1 Paramètres 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
pour le nombre maximum d'adresses IP dans la liste.

Lors de la connexion, si plusieurs adresses IP sont résolues, elles sont classées par ordre de 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 requête ou une réponse d'erreur définitive du serveur, comme suit :

- Erreur de socket - si le socket entre le client et le serveur est rompu ou fermé, comme dans le cas d'une perte de connectivité réseau, le client réagit immédiatement et déclenche un basculement.
- Délai d'attente (par exemple, lorsque le SBC se bloque) - basé sur le SIP T1 :
  - SIP INVITE - si la demande INVITE n'aboutit pas, le client s'enregistre auprès du prochain SBC disponible (IP) et réessaie l'INVITE.
  - Autre demande SIP - le client tente de s'enregistrer auprès du prochain SBC disponible (IP).
- Réponse d'erreur définitive reçue du serveur :
  - Les réponses d'erreur SIP suivantes du serveur à un SIP REGISTER déclenchent un basculement :
    - 5xx
    - 6xx
  - Les réponses SIP *4xx* suivantes à SIP REGISTER ne provoquent pas de basculement :
    - 401 Non autorisé
    - 403 Interdit
    - 404 Non trouvé
    - Authentification du 407 proxy requise
    - 423 Intervalle trop court

Confidentiel à Cisco

- En outre, les réponses d'erreur *4xx* à SIP INVITE ne déclenchent pas de basculement, mais *5xx* et *6xx* le font.

Lorsqu'un basculement est déclenché, le client prend la prochaine adresse IP disponible de la liste. La minuterie SIP T1 définit la durée d'essai d'un proxy de la liste avant de passer au suivant. La valeur utilisée est généralement de 32 secondes (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 lorsque le basculement se produit, l'appel est interrompu.

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

- Temporisateurs de basculement SIP - Les temporisateurs 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 d'aller-retour sur le réseau.
  - T2 - le délai maximal, en millisecondes, avant la retransmission des demandes de non-invitation et des réponses d'invitation.
  - T4 - la durée maximale, en millisecondes, pendant laquelle un message reste dans le réseau.
- Adresse du proxy SIP et découverte du proxy SIP
  - Voir la section *6.1.1 Paramètres du serveur SIP*.
  - Voir la section *6.1.6 Détection 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 du nouveau périphérique. L'en-tête Contact de l'ancienne session est inclus pour informer le SBC de nettoyer les données. Cet en-tête comprend expires=0 et q=0.5.

L'en-tête du contact avec les informations du nouveau périphérique a également une valeur q, qui est lue à partir de la balise . La valeur de la balise est utilisée pour indiquer la préférence ou la priorité d'une adresse de contact particulière. Il va de 0 à 1,0, 1,0 étant la préférence la plus élevée et 0 la plus basse. Cette balise n'a pas de balise personnalisée pour contrôler la valeur - elle est codée en dur à 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 une priorité maximale.

Confidentiel à Cisco

À partir de la version 42,11, une nouvelle section est introduite dans le modèle de configuration. Un nouveau paramètre configurable a été ajouté pour contrôler si l'application enverra l'en-tête Contact pour nettoyer les informations de l'ancien périphérique ou non. Certains SBC nettoient l'ancienne session immédiatement lors de la déconnexion de la socket, 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.

Pour plus de cohérence, la balise est également déplacée sous la même section .

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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	vrai	vrai, faux	Contrôle le nettoyage des informations sur les anciens appareils 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'IP ayant la priorité la plus élevée. Le délai de reprise est basé sur la configuration de la gestion du TTL du DNS (voir la section *6.1.8.4 Gestion DNS TTL*). Si un appel est en cours lorsque le délai de reprise est atteint, le client attend que tous les appels soient terminés et déclenche la procédure de reprise. Notez que ceci n'est valable que pour les clients de bureau puisque la connexion SIP n'est active que lors d'un appel sur mobile.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SIP_FAILBACK_ENABLED_WXT%	vrai	vrai, faux	Active/désactive la reprise sur défaillance SIP.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Plus de 60 ans	Le délai d'attente pour la reprise SIP en secondes.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	vrai, faux	Ajoute une période aléatoire [0-10]% de la reprise SIP.

Confidentiel à Cisco

6.1.8.3 Renforcer 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 de IPv6
- ipv6 - filtre les adresses de IPv4
- prefer-ipv4 : commande les adresses IPv4 avant le IPv6 (version 42,9)
- prefer-ipv6 : commande les adresses IPv6 avant le IPv4 (version 42,9)
- nat64 : ignore les adresses IPv6, commande les adresses IPv4 (version 44,2)

Il est recommandé d'utiliser la valeur par défaut (dns), à moins que la configuration de l'environnement/du réseau n'exige un mode différent.

Avec la configuration « dns », les adresses IPv4 sont prioritaires par rapport aux adresses IPv6, pour un hôte donné. S'il y a deux hôtes avec des adresses IPv4 et IPv6, l'ordre est IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

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

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

Avec le mode « prefer-ipv6 », l'ordre est inverse : 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(s) préfixe(s) IPv6 est/sont découvert(s). 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), Pref64(2)::IPv4(host2)::Suff64(2), IPv4(host2)::Suff64(3).

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	dns	ipv4 ipv6 dns prefer-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 DNS TTL

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

Une fois la résolution DNS effectuée, ce paramètre oblige également le client à se reconnecter au serveur prioritaire reçu s'il est différent du serveur actuellement utilisé, même dans le cas où la connexion actuelle fonctionne parfaitement. Toutefois, la reconnexion n'est effectuée qu'après la fin des appels en cours.

Si les TTL des serveurs A et des enregistrements SRV sont différents, c'est la plus petite valeur qui est retenue.

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

Ce paramètre ne fonctionne que pour SIP.

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

> **REMARQUE** : Il s'agit d'une fonction réservée aux ordinateurs de bureau, car les clients mobiles ne disposent d'une connexion SIP que lorsqu'ils sont en cours d'appel.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SIP_REFRESH_ON_TTL_WXT%	false (faux)	faux, vrai	Si la valeur est "false", la gestion du TTL du DNS est désactivée pour SIP. Lorsqu'elle est définie sur « vrai », la gestion DNS TTL est activée pour SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	faux	faux, vrai	Si cette option est activée, elle ajoute a une période aléatoire comprise entre 0 et 10 % au TTL du DNS.

REMARQUE : Il est fortement recommandé d'activer le facteur aléatoire TTL du DNS afin d'éviter les pics de requêtes au DNS et potentiellement les pics de tentatives de reconnexion au serveur d'application.

6.1.9 SIP SUBCSRIBE et REGISTER Refresh et SUBSCRIBE Retry

Communicator permet de configurer les intervalles de rafraîchissement pour SIP SUBSCRIBE et REGISTER. Pour SIP SUBSCRIBE, il existe un paramètre distinct pour l'intervalle de rafraîchissement (en secondes) et pour la durée d'attente avant que le client ne réessaie SIP SUBSCRIBE en cas d'erreur (en secondes). La valeur maximale recommandée pour la variable *subscription-retry-interval* est de 2000000 secondes, tandis que toute valeur négative, 0 ou vide entraîne l'utilisation de 1800 secondes. Toute valeur négative dans le champ subscribe refresh ne tient pas compte de l'en-tête *Expires* et crée donc un SUBSCRIBE unique.

Le délai de rafraîchissement de SIP REGISTER proposé par le client peut être configuré en secondes, mais selon les spécifications SIP, le serveur peut remplacer cette valeur. Actuellement, le client se souvient de la valeur proposée par le serveur pour les actualisations suivantes au lieu de toujours utiliser la valeur configurée.

Enfin, la valeur d'expiration des 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 associés à P dans REGISTER

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

Si la valeur de ce paramètre est "false", le client n'utilise pas l'adresse *P-Associated-URI* et utilise à la place l'identité de son propre URI SIP.

Confidentiel à Cisco

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

Si la valeur de ce paramètre est "true", le client prend sa propre identité dans le dernier en-tête *P-Associated-URI* pour toutes les demandes SIP sortantes (INVITE, SUBSCRIBE, CANCEL, INFO et REFER) à partir de la réponse *200 OK* dans le REGISTER. En outre, ces URI ne figurent pas dans la liste des contacts.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	vrai, faux	Permet l'utilisation d'identités alternatives dans SIP REGISTER. Si la valeur est "true", le client prend sa propre identité dans le dernier en-tête *P-Associated-URI* pour les requêtes SIP sortantes. Si la valeur est "false", sa propre identité pour les requêtes SIP sortantes est tirée 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 les environnements IMS à l'intérieur d'un domaine de confiance pour permettre au réseau d'autoriser plusieurs dialogues SIP sur les médias précoces, par exemple dans les cas où un autre réseau autorise tous les médias précoces.

Ce paramètre de configuration permet d'activer la prise en charge de la publicité PEM dans la signalisation SIP. La logique de traitement des premiers médias 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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_PEM_SUPPORT_WXT%	false	vrai, faux	La valeur "true" permet d'activer la prise en charge de la publicité PEM du client dans la signalisation SIP. Définissez sur « false » (faux) pour désactiver la prise en charge PEM de la publicité du client dans la signalisation SIP.

Confidentiel à Cisco

6.1.12 Prise en charge de la MISE À JOUR SIP

SIP UPDATE est nécessaire, par exemple, dans certains déploiements IMS, au lieu de l'alternative re-INVITE. Il permet à un client de mettre à jour les paramètres d'une session, tels que l'ensemble des flux de médias et leurs codecs, mais n'a aucun impact sur l'état d'un dialogue SIP.

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

SIP UPDATE n'est actuellement pris en charge que lorsqu'il est reçu dans des cas d'utilisation préalables au dialogue (early media) et non pendant un dialogue actif, par exemple pour la mise en attente/reprise d'un appel où le re-INVITE est toujours utilisé.

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

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	vrai, faux	Si la valeur est "false", la prise en charge de SIP UPDATE est désactivée. Lorsqu'elle est définie sur « vrai », la prise en charge de la mise à jour SIP est activée.

6.1.13 FIR INFO SIP hérité

Ce client prend en charge l'ancienne méthode de demande d'images clés vidéo via la demande de contrôle de média SIP INFO. Cela est nécessaire car certains appareils ont des problèmes pour répondre au RTCP-FB FIR et, parfois, le RTCP n'arrive pas jusqu'à l'extrémité distante, ce qui peut conduire à une absence de vidéo ou à une vidéo à sens unique. Pour plus d'informations, voir *RFC 5168*.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false	vrai, faux	Lorsqu'elle est définie sur « faux », la prise en charge de SIP INFO FIR est désactivée. Lorsqu'elle est définie sur « vrai », la prise en charge de SIP INFO FIR est activée.

6.1.14 Gestion des ports SIP pour la traversée NAT

Le client peut être configuré pour utiliser le mécanisme SIP rport pour la traversée du NAT. Il convient de noter qu'en règle générale, il ne peut s'agir de la seule solution pour la traversée de la NAT et que le SBC est principalement utilisé à cette fin. Pour une description de la spécification rport, voir *RFC 3581*.

Pour plus d'informations sur le port SIP et les recommandations de protocole de transport lorsque des passerelles de couche d'application (ALG) SIP sont utilisées dans le réseau, voir 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. Ce 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 cette fonction est activée, les valeurs des en-têtes "received" et "rport" sont utilisées dans l'en-tête SIP Contact des requêtes SIP (même si l'en-tête "received" est absent de la réponse REGISTER).

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

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

> **NOTE**: Dans IPv6 les environnements, toutes les adresses sont réelles et le SBC essaie d'établir une connexion avec l'adresse du client qui 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%"/>
```


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_USE_RPORT_WXT%	false	vrai, faux	Active la fonction rport pour les appels audio et vidéo.
%RPORT_USE_LOCAL_PORT_WXT%	false	vrai, faux	Contrôle si le port local du socket du client doit être ajouté dans l'en-tête SIP *Contact* .

6.1.15 ID de session SIP

Lorsque cette option est activée, un identifiant de session local est généré lors de l'enregistrement initial. L'identifiant de session est utilisé pendant toute la durée de la connexion/session pour ce dispositif, pour tous les dialogues hors appel, REGISTER, SUBSCRIBE, NOTIFY, etc. Le même identifiant 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 identifiant de session local est généré.

La valeur de l'ID de session peut être utilisée pour trouver l'ensemble des dialogues associés à ce dispositif.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SIP_SESSION_ID_WXT%	false	vrai, faux	Contrôle l'utilisation de l'identifiant de session SIP.

6.1.16 Comportement du rejet d'appel entrant

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

Notez que si le client est configuré pour rejeter un appel avec *603 Decline*, les services Call Forward Busy et Call Forward No Answer peuvent ne pas fonctionner comme prévu.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_REJECT_WITH_486_WXT%	vrai	vrai, faux	Contrôle le code d'erreur SIP et la raison utilisés pour rejeter les appels SIP entrants. Si cette option est activée, *486 Temporarily Unavailable* est utilisé. Sinon, *603 Decline* est utilisé.

6.1.17 Plage de ports du 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), ce qui s'applique également à SRTP. Cette configuration s'effectue en définissant les valeurs limites de la 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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	numéro	Début de la plage de ports audio.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	numéro	Fin de la plage des 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 ce qu'elles ne se chevauchent jamais.

Confidentiel à Cisco

6.1.18 Assistance ICE (Webex Calling uniquement)

Le client prend en charge la négociation de l'établissement de la connectivité interactive (ICE), qui permet d'optimiser le trajet des médias entre les points d'extrémité (d'égal à égal). Cela permet de réduire la latence des données, de diminuer la perte de paquets et de réduire les coûts opérationnels du déploiement de l'application.

Notez que la mise en œuvre actuelle prend en charge le serveur STUN, alors que TURN n'est pas pris en charge.

Lorsque la prise en charge de l'ICE est activée, la recomposition de la clé pour SRTP est toujours effectuée (voir la section *6.1.2 SIP 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 à l'aide de 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_RTP_ICE_WXT%	false	vrai, faux	Activer / désactiver la prise en charge de l'ICE.
%RTP_ICE_MODE_WXT%	icestun	icestun	Mode de prise en charge ICE. Actuellement, la seule valeur prise en charge est "icestun".
%RTP_ICE_SERVICE_URI_WXT%	(vide)	URI valide du serveur STUN ou (vide)	URI du serveur STUN.
%RTP_ICE_PORT_WXT%	3478	Numéro (0-65535)	Port du serveur STUN.
%ENABLE_RTP_ICE_IPV6_WXT%	false	vrai, faux	Active ICE sur IPv6.

6.1.19 MUX RTCP

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

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

Confidentiel à Cisco

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

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

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_RTCP_MUX_WXT%	vrai	vrai, faux	Pour activer le RTPC MUX, mettre à "true". Pour désactiver le MUX RTCP, mettre à "false".

6.1.20 Transfert

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 le destinataire distant. Le bouton d'achèvement semi-consultatif n'est activé pour l'appelant que lorsque la sonnerie est lancée du côté de l'appelant et que la notification SIP correspondante (*180 Ringing*) est reçue du côté de l'appelant. Le transfert en aveugle est appelé "Transférer maintenant" dans l'interface utilisateur.

> **NOTE**: La sonnerie *180 SIP* ne peut pas être déclenchée dans certains environnements, pour certains numéros, ou dans certains scénarios de communication entre serveurs.

La version 43,9 de l'application Webex introduit le transfert vers un autre appel autonome en cours du même type. Les appels terminés dans l'application Webex peuvent être transférés vers d'autres appels terminés dans le point de terminaison local. Les appels terminés sur un appareil distant peuvent être transférés vers des appels terminés sur un point d'extrémité distant. Cette fonction n'a 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 de menu Transférer est sélectionné. Ce comportement est contrôlé par le nouvel attribut *auto-hold* . Par défaut, la fonction de maintien 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%"/>
```


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_TRANSFER_CALLS_WXT%	false	vrai, faux	Lorsque la valeur est "true", le transfert d'appel est activé. Lorsqu'il est défini sur « faux », le transfert d'appel est désactivé.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false	vrai, faux	Active les options de transfert pour les appels distants (XSI) terminés sur un autre site.
%TRANSFER_CALL_TYPE_WXT%	complet	parler d'abord, aveugle, complet	Spécifie les types de transfert disponibles pour l'utilisateur dans la configuration BroadWorks.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	vrai, faux	Contrôle si l'appel actif sera automatiquement mis en attente lorsque l'utilisateur sélectionne l'option Transfert dans le menu de l'écran d'appel.

6.1.21 Conférences téléphoniques N-Way

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. En outre, le propriétaire du N-way peut voir la liste complète des participants via SIP SUBSCRIBE/NOTIFY et le paquet d'événements de conférence. Le client du propriétaire connaît l'URI à laquelle envoyer le SIP SUBSCRIBE via l'en-tête SIP *Contact* du message *200 OK* envoyé en réponse à l'INVITE à l'URI de la conférence, tandis que pour les participants, les mêmes informations se trouvent dans un NOTIFY d'informations d'appel précédent.

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

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

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

Example output:
maxConferenceParties = 6
conferenceURI =
```

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

Confidentiel à Cisco

Avec la version 45,7, pour le déploiement exclusif de Webex Calling, l'application Webex introduit la prise en charge de la transition automatique d'une conférence téléphonique ad-hoc N-Way à une session d'appel 1:1, à condition que l'hôte et un participant supplémentaire restent dans l'appel. Une nouvelle option configurable (conférence à deux parties) a été ajoutée pour contrôler l'activation de cette amélioration.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CONFERENCE_CALLS_WXT%	false	vrai, faux	Contrôle si l'option Conférence doit être activée pour l'utilisateur.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	false	vrai, faux	La valeur "true" permet d'activer la liste des participants propriétaires de N-way. Configurer la valeur « false » (faux) pour désactiver la liste des participants du propriétaire N-way.
%MAX_CONF_PARTIES_WXT%	10	Nombre compris entre 4 et 15 (vide)	Spécifie le nombre maximum de participants à N-voies, appliqué par le client, par exemple 10. Le côté serveur a ses propres limites. Une valeur vide désactive l'application côté client de la limite de participants à N voies.
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	false	vrai, faux	Contrôle si la conférence téléphonique ad hoc doit être convertie en session d'appel 1:1, uniquement si deux participants restent dans la conférence téléphonique.

6.1.22 Retirer un appel

L'application Webex prend en charge la fonction Call Pull, qui permet aux utilisateurs de déplacer les appels à distance qui sont terminés sur leurs périphériques vers le périphérique actuel. Il existe une option d'extraction d'appel statique (aveugle) que les utilisateurs peuvent utiliser même lorsqu'il n'y a pas d'appel en cours.

La version 45,1 de l'application Webex améliore la fonctionnalité en ajoutant une surveillance active des appels et en offrant la possibilité de récupérer l'appel distant sur le périphérique actuel à partir de l'appel lui-même. Cette fonction n'est disponible que lorsqu'un seul appel est en cours pour l'utilisateur, qui est terminé sur un autre périphérique appartenant à l'utilisateur.

Confidentiel à Cisco

Dans l'application de bureau, une nouvelle option configurable est exposée dans les paramètres d'appel de l'application Webex, permettant une gestion différente des appels à distance :

- Contrôle des appels à distance - il s'agit du comportement actuel de l'application Webex, où les appels à distance sont affichés avec un minuteur dans la liste des appels. Lorsque le minuteur est sélectionné, l'utilisateur peut voir l'écran de contrôle des appels. Grâce à cette nouvelle amélioration, l'utilisateur pourra utiliser la nouvelle option « Déplacer l'appel vers l'ordinateur » dans le menu Plus, pour lancer une recherche d'appel
- Déplacement d'appel - lorsque cette option est sélectionnée, l'utilisateur ne pourra pas ouvrir l'écran de contrôle des appels pour les appels à distance. L'utilisateur ne voit une option de déplacement de l'appel que lorsqu'il y a un seul appel à distance, terminé sur un périphérique appartenant à l'utilisateur. Lorsque l'option Déplacer est sélectionnée, l'utilisateur voit une boîte de dialogue de confirmation, avant que l'application Webex ne lance l'extraction d'appel.
- Toujours demander - dans ce type de configuration, l'utilisateur voit le minuteur de l'appel à distance dans la liste des appels, et lorsqu'il est sélectionné, il lui est demandé comment procéder - si le contrôle d'appel à distance doit être affiché, si la commande d'appel à distance doit être lancée (le cas échéant) ou si l'opération doit être annulée

La version 45,1 améliore également l'application mobile. Si le mode d'extraction d'appel actif est activé, elle affiche tous les appels à distance pour l'utilisateur, ce qui permet la surveillance active des appels et offre la possibilité de déplacer les appels dans certaines situations. Si un seul appel est terminé sur un périphérique distant (appartenant à l'utilisateur), l'option de déplacement sera disponible pour cet appel. Toutefois, s'il y a plusieurs appels pour l'utilisateur, ou si l'appel est terminé sur un périphérique partagé, les appels seront toujours visibles, mais uniquement à titre d'information – il n'y aura aucune option pour déplacer ou contrôler l'appel à distance.

Pour contrôler la fonctionnalité, il existe plusieurs options configurables - une pour contrôler la disponibilité et deux autres - le *mode* et *l'option de déplacement actif par défaut* (Bureau uniquement), pour contrôler le comportement de la fonctionnalité. Le *mode* peut être configuré sur l'une des options suivantes :

- Masque de plongée
    - le mode par défaut
    - Bureau : un bouton d'extraction d'appel dans le clavier de numérotation
    - Mobile – une option de renvoi d'appel dans l'onglet Calling (Appel)
- actif(s)
    - Ordinateur de bureau
        - aucun bouton d'extraction d'appel dans le clavier de numérotation
        - permet la récupération d'un appel activement surveillé
        - permet la configurabilité de l'action lorsqu'un appel est sélectionné
    - Mobile
        - aucune option de renvoi d'appel dans les options de l'onglet Appel
        - permet la surveillance active de tous les appels à distance de l'utilisateur

Confidentiel à Cisco

- permet la récupération d'un appel activement surveillé

- full : combine le mode aveugle et actif

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_PULL_WXT%	false	vrai, faux	Active le tirage d'appel.
%CALL_PULL_MODE_WXT%	Masque de plongée	aveugle, actif, complet	Contrôle les options d'extraction d'appel disponibles pour l'utilisateur - il peut s'agir de l'une des options d'extraction d'appel aveugle actuelles, d'une option d'extraction d'appel basée sur la surveillance active ou des deux.
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	déplacement_appel	contrôle_appel, déplacement_appel, toujours_demander	Ordinateur de bureau uniquement Si le déplacement actif est disponible (le mode actif ou plein est configuré), ce paramètre spécifie l'action par défaut activée pour l'utilisateur dans la liste des appels

REMARQUE : Cette fonctionnalité nécessite que le service de récupération d'appel d'apparence d'appel partagée soit activé pour l'utilisateur, en activant la case à cocher « Autoriser la récupération d'appel à partir d'un autre emplacement » à partir de la page de configuration de l'apparence d'appel partagée dans le portail CommPilot.

6.1.23 Parquage d'appel/Récupérer

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

L'utilisateur peut récupérer l'appel en le mettant en attente dans la boîte de dialogue pendant un nombre de secondes configurable, immédiatement après avoir mis l'appel en attente. L'appel parqué peut également être récupéré par l'utilisateur ou un autre utilisateur en sélectionnant l'option de récupération d'appel et en saisissant le numéro ou le poste.

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


Confidentiel à Cisco

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_PARK_WXT%	false	vrai, faux	Active le parcage/la récupération des appels.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Numéro entre 5 et 30	Spécifie le nombre de secondes pendant lesquelles la boîte de dialogue "Appel parqué réussi" reste visible pour l'utilisateur avant d'être fermée automatiquement.

6.1.24 Statistiques de l'appel

Rapport sur les statistiques de fin d'appel dans le protocole d'initiation de session (SIP) Le message BYE permet d'envoyer des statistiques d'appel à une extrémité distante 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 du délai, le délai aller-retour et la durée de l'appel.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_STATISTICS_WXT%	false	vrai, faux	La valeur "true" permet d'activer la capture des métriques d'appel. Définissez la valeur sur « false » (faux) pour désactiver la capture des métriques d'appels.

6.1.25 Récupération automatique des appels / Transfert d'appel fluide

Le client prend en charge la récupération automatique des appels en cas de changement de réseau alors que l'utilisateur a un appel VoIP en cours. La récupération automatique des appels fonctionne dans les deux sens - données cellulaires vers WiFi et WiFi vers données cellulaires, ainsi que lors du passage d'un réseau WiFi à un autre. L'appel tente d'être récupéré dans un délai d'une minute, puis s'arrête. Si plusieurs appels VoIP sont en cours, seul l'appel actif est récupéré.

Confidentiel à Cisco

Dans le cas d'une transition des données cellulaires vers le Wi-Fi, le client conserve les appels VoIP en cours sur les données cellulaires jusqu'à ce qu'il y soit mis fin ou que le réseau de données cellulaires soit perdu.

En cas de récupération automatique d'appel en raison d'un changement de réseau, une indication de tonalité est émise à l'utilisateur, lors de la tentative de reconnexion d'appel.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false	vrai, faux	Contrôle si le mécanisme de récupération automatique doit être activé pour l'utilisateur.

NOTE: Cette fonction dépend de l'activation de la fonction Appel Pull pour l'utilisateur. Pour plus d'informations, consultez la section *6.1.22 Retirer un* appel.

6.1.26 Enregistrement des appels

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

Si la fonction est désactivée, l'utilisateur ne dispose d'aucun bouton d'enregistrement ni d'aucune option. Notez que l'enregistrement des appels fonctionne 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 en cours d'enregistrement. Les modes d'enregistrement d'appel suivants sont pris en charge par Cisco BroadWorks :

Toujours

- L'enregistrement des appels est lancé automatiquement lors de l'établissement de l'appel.
- L'utilisateur est **NOT** en mesure d'arrêter/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 suspendre et reprendre l'appel.
- Interactions possibles avec les utilisateurs :

Confidentiel à Cisco

- L'enregistrement est en cours - **Pause** Action d'enregistrement.
- L'enregistrement est en pause – **Reprendre** l'action de l'enregistrement.

Sur demande

- Une fois l'appel établi, l'enregistrement de l'appel commence sur le serveur.
- Si l'utilisateur appuie sur l'option Démarrer l'enregistrement pendant l'appel, l'enregistrement de l'appel sera stocké et conservera l'appel depuis son démarrage. Dans le cas contraire, si aucun enregistrement de départ n'est initié par l'utilisateur, l'enregistrement de l'appel sera supprimé sur le serveur.
- Interactions possibles avec les utilisateurs :
  - Aucun enregistrement n'a encore commencé - **Démarrer** Action d'enregistrement.
  - L'enregistrement est en cours - **Pause** Action d'enregistrement.
  - L'enregistrement est en pause – **Reprendre** l'action de l'enregistrement.

À la demande avec démarrage à l'initiative de l'utilisateur

- L'utilisateur peut démarrer, arrêter, mettre en pause et reprendre l'enregistrement d'un appel à tout moment, ou plusieurs fois au cours d'un appel.
- Il y aura des enregistrements d'appels distincts pour chaque démarrage d'enregistrement d'appel.
- Interactions possibles avec les utilisateurs :
  - Aucun enregistrement n'a encore commencé - **Démarrer** Action d'enregistrement.
  - L'enregistrement est en cours – **Arrêter** et **Mettre en pause** l'action de l'enregistrement.
  - L'enregistrement est en pause – **Arrêter** et **reprendre** l'action de l'enregistrement.

Le mode d'enregistrement des appels attribué à l'utilisateur peut être sélectionné à partir du centre de contrôle.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_RECORDING_WXT%	false	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.

Confidentiel à Cisco

La messagerie vocale visuelle (VVM) est prise en charge pour l'audio uniquement. Les formats pris en charge sont wav, ulaw et mov contenant de la vidéo H264 (jouée en tant qu'audio uniquement). Il permet aux utilisateurs d'afficher les messages vocaux entrants sous forme de liste et de les écouter individuellement. Cette fonction est basée sur Xsi, mais les notifications de nouveaux messages vocaux 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 le MWI doit être activé pour que la messagerie vocale visuelle fonctionne. Pour plus d'informations sur la configuration SIP, voir la section *6.1.1 Paramètres du serveur SIP*.

Pour connaitre la version de Cisco BroadWorks et la configuration minimale requise pour la messagerie vocale visuelle, voir le
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 disposer de la messagerie vocale visuelle :

- Messagerie vocale activée
- L'option "Lorsque le message arrive, utiliser la messagerie unifiée" est activée.
- Option "Utiliser l'indicateur de message en attente du téléphone" activée

Le fait de ne pas avoir le service de messagerie vocale visuelle attribué du côté de Cisco BroadWorks pour l'utilisateur désactive automatiquement la configuration du service.

Notez que la désactivation de l'enregistrement SIP désactive également le MWI pour les nouveaux messages vocaux. Voir le tableau suivant pour plus d'informations sur l'activation du MWI.

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

Notez que si l'abonnement SIP au paquet 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 relance SIP SUBSCRIBE, voir la section *6.1.9 SIP SUBCSRIBE et REGISTER Refresh et SUBSCRIBE Retry.*

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_MWI_WXT%	false	vrai, faux	La valeur "true" permet d'activer le MWI. Régler sur "false" pour désactiver le MWI.
%MWI_MODE_WXT%	vide	implicite, explicite	Réglé sur "explicite" pour envoyer SIP SUBSCRIBE pour le paquet d'événements MWI lorsque le MWI est activé. L'utilisation de « implicite » n'envoie pas un pack d'événement SIP SUBSCRIBE pour MWI lorsque MWI est activé. S'il est laissé vide, le MWI est désactivé.
%ENABLE_VOICE_MAIL_WXT%	false	vrai, faux	La valeur "true" permet d'activer la prise en charge de la messagerie vocale. Configurer la valeur « false » (faux) pour désactiver la prise en charge de la messagerie vocale.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	vrai, faux	Lorsqu'il est défini sur « faux », VVM est désactivé. Lorsqu'il est défini sur « vrai », VVM est activé. Notez que l'option voice-mail enabled=false avant l'attribut VVM est toujours utilisée pour des raisons de compatibilité ascendante.

6.1.28 Transcription des messages vocaux 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 mobiles et de bureau Webex Calling.

La fonction 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 fonction de messagerie vocale visuelle est activée pour l'utilisateur.
3. La fonctionnalité est activée dans la configuration (l'attribut activé dans la balise < services>< voice-mail>< transcription> doit être configuré sur « true »).

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	false	vrai, faux	[Webex Calling Only] Contrôle la disponibilité de la transcription des messages vocaux 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 Toujours renvoi d'appel Cisco BroadWorks dans le client Webex pour Cisco BroadWorks.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	vrai, faux	Contrôle la disponibilité du service de renvoi d'appel toujours. Par défaut, la fonction est désactivée.

REMARQUE : Le renvoi permanent d'appel et le renvoi d'appel vers la messagerie vocale (*6.1.29.2 Transfert 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 offre une option permettant de contrôler la disponibilité du transfert vers la messagerie vocale. Par défaut, la fonction 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%"/>
```


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	vrai	vrai, faux	Contrôle la disponibilité du transfert vers la messagerie vocale. Par défaut, la fonctionnalité est activée.

REMARQUE 1 : Cette fonction dépend de l'un des services "Utilisateur de messagerie vocale" ou "Support de messagerie vocale tiers" à attribuer à l'utilisateur.

NOTE 2: Le renvoi d'appel vers la messagerie vocale et le renvoi d'appel toujours (*6.1.29.1 Renvoi 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 (Single Number Reach)

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 fonction dans le client est *Manage My Numbers*.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_BROADWORKS_ANYWHERE_WXT%	false	vrai, faux	Active BroadWorks Anywhere (BWA) au niveau de la configuration.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	vrai	vrai, faux	Contrôle si la description de la localisation BWA doit être disponible pour l'utilisateur.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	vrai, faux	La valeur "true" permet à l'utilisateur d'accéder à la fonction "Alert All Locations" pour le service BWA. Configurez la valeur « false » (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	vrai, faux	Contrôle si l'application doit activer l'état "Alerter tous les emplacements" lors de l'ajout d'un deuxième emplacement BWA ou de chaque nouvel emplacement suivant.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	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	vrai, faux	Contrôle l'état par défaut du contrôle d'appel pour la localisation BWA.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	vrai, faux	Contrôle si l'inhibiteur de diversion de l'emplacement BWA doit être disponible pour l'utilisateur.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	vrai, faux	Contrôle l'état par défaut de l'inhibiteur de diversion de l'emplacement BWA.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false	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	vrai, faux	Contrôle l'état par défaut de la confirmation de réponse de l'emplacement BWA.

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

Le client Webex pour Cisco BroadWorks permet d'accéder à un portail de paramètres (Self Care), où l'utilisateur peut configurer certains paramètres de l'application et du service.

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

NOTE: Il est conseillé de masquer les paramètres qui sont déjà visibles dans l'application comme Call Center (voir section *6.1.31 Connexion/déconnexion du centre d'appels/de la* file d'attente des appels) et

Confidentiel à Cisco

BroadWorks Anywhere (voir section *6.1.29.3 BroadWorks Anywhere*). Il est également conseillé de masquer le service Remote Office car le service BroadWorks Anywhere lui a succédé.

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 de configuration 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%"/>
   <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>
```


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%WEB_CALL_SETTINGS_TARGET_WXT%	externe	externe, csw	Contrôle le mode du portail d'administration. Régler sur "externe" pour ouvrir l'URL du portail de configuration configuré dans un navigateur externe. Définir sur « csw » pour ouvrir le portail CSW dans un navigateur intégré en utilisant la section paramètres supplémentaires pour former la demande POST.
%WEB_CALL_SETTINGS_URL_WXT%	vide	Chaîne URL	URL du portail de configuration. Exemple : https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Renvoi d'appel toujours doit être visible pour l'utilisateur dans les paramètres basés sur le web.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Ne pas déranger (NPD) doit être visible par 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 par 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 par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de renvoi d'appels non joignable (CFNR) doit être visible par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option de renvoi d'appel sans réponse (CFNA) doit être visible par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Sonnerie simultanée personnelle (SIMRING) doit être visible par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Sonnerie séquentielle (SEQRING) doit être visible par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Bureau à distance (RO) doit être visible par 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 par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Appel en attente (CW) doit être visible par l'utilisateur dans les paramètres Web.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option CLIDB (Calling Line ID Delivery Blocking) doit être visible par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Assistant personnel (AP) doit être visible par 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 par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option Call Center doit être visible par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si l'option BroadWorks Mobility (BWM) doit être visible par l'utilisateur dans les paramètres 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 par l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false	vrai, faux	Contrôle l'utilisation ou non de la nouvelle image de marque de la WebView des paramètres d'appel. Activé si la version de CSWV côté serveur est 1.8.6 ou supérieure. Dans le cas contraire, gardez-le faux.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	vrai	vrai, faux	Contrôle si les options de messages électroniques et vocaux sont visibles dans les paramètres basés sur le web.
%USER_PORTAL_SETTINGS_URL_WXT%	vide	Chaîne 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.
%USER_PORTAL_SETTINGS_TARGET_WXT%	externe	externe, interne	Spécifie si l'URL doit être ouvert dans un navigateur intégré ou externe.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false	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 BroadWorks à durée de vie courte est ajouté dans le BODY. Lorsqu'il est désactivé, l'URL est ouvert avec HTTP GET.

REMARQUE 1 : L'URL de la WebView des paramètres d'appel doit toujours être configurée avec un "/" à la fin. Par exemple : http(s):////

NOTE 2: La version minimale de l'application Call Settings WebView prise en charge est 1.7.5.

Pour l'installation sur la version 21Cisco BroadWorks, consultez les étapes supplémentaires décrites dans le *Guide de la solution Webex pour Cisco BroadWorks*.

6.1.31 Connexion/déconnexion du centre d'appels/de la file d'attente des 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'appel, cette fonction lui permet de se connecter à un centre d'appel et de visualiser les files d'attente disponibles, ainsi que de rejoindre/déjoindre les files d'attente et de définir l'état de la distribution automatique des appels (DAA).

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 l'affichage Web des paramètres d'appel (voir la section *6.1.30 Portail des paramètres et paramètres d'appel 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 des paramètres de l'application mobile Webex.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_CENTER_WXT%	false	vrai, faux	Active le support du centre d'appel.

Confidentiel à Cisco

6.1.32 Racines 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 modifier la racine XSI est de mettre en œuvre l'équilibrage de charge au niveau de la configuration, bien qu'il soit recommandé d'utiliser plutôt l'équilibrage de charge au niveau de la couche HTTP.

Les chemins d'accès aux événements et aux actions sont généralement modifiés pour des raisons de stratégie de marque, afin de supprimer la référence au domaine *com.broadsoft* des chemins d'accès 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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%XSI_ROOT_WXT%	Continue d'utiliser l'original utilisé pour la récupération de la configuration.	Chaîne URL	La racine XSI pour toutes les opérations XSI. Exemple : https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	String	Spécifie le chemin d'accès aux actions XSI. Il doit commencer et se terminer par "/" et ne contenir que le contexte de l'action. Exemple : /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	String	Spécifie le chemin d'accès XSI Events. Il doit commencer et se terminer par « / » et ne contenir que le contexte des événements. Exemple : /com.domain.xsi-events/

6.1.33 Chaîne d'événements XSI

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

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

Confidentiel à Cisco

- Enregistrement des appels

Le battement de cœur de XSI Events est utilisé pour maintenir le canal XSI Event ouvert et l'intervalle de battement de cœur 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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_XSI_EVENT_CHANNEL_WXT%	vrai	vrai, faux	Contrôle si le canal XSI Event est activé. Il doit être réglé sur "true" pour recevoir, par exemple, des événements liés au service de contrôle en milieu d'appel. La valeur recommandée est "true".
%CHANNEL_HEARTBEAT_WXT%	10000	numéro	Il s'agit du rythme cardiaque du canal XSI Event (en millisecondes). La valeur par défaut est "10000".

6.1.34 Configuration des codecs

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 *video/codecs* . La priorité de chaque codec peut être modifiée via l'attribut XML priority , qui est une valeur comprise entre 0,0 (la plus faible) et 1,0 (la plus élevée).

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

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

Confidentiel à Cisco

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

Le client prend en charge le codec vidéo H.264. L'attribut de résolution vidéo, indiquant la résolution vidéo maximale publiée par l'application, peut être défini sur l'une des valeurs disponibles suivantes : SUBQCIF, QCIF, CIF, 4CIF, VGA, HD et WIDE_FULL_HD.

À partir de la version 45,8, la résolution vidéo maximale utilisée par l'application de bureau est mise à jour de la HD par défaut à WIDE_FULL_HD, et celle des applications mobiles et tablettes reste 4CIF.

Si le débit n'est pas indiqué dans la configuration, les valeurs de débit par défaut sont utilisées. Les valeurs de débit par défaut, en fonction de la résolution et de la fréquence d'images, sont indiquées dans le tableau suivant.

Résolution	Taille de la vidéo *	FPS (images par seconde)	Valeurs par défaut du débit binaire 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
WIDE_FULL_HD	1920 x 1080	30	4000000

***** Résolution vidéo maximale annoncée. La résolution vidéo réelle lors d'un appel entre deux clients Webex for Cisco BroadWorks dépend des capacités des deux clients - elle sera la plus faible des deux et sera la même sur les deux clients.

Confidentiel à Cisco

La résolution vidéo d'un appel vidéo est négociée lors de l'établissement de la session et est basée sur les capacités des deux terminaux. La résolution de l'appel vidéo est la même sur les deux points d'extrémité. Autrement dit, si les terminaux Webex pour Cisco BroadWorks ont des capacités différentes (et prennent donc en charge des résolutions différentes), alors la résolution inférieure est négociée pour l'appel. La résolution vidéo peut changer au cours d'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-interleaved (1). Le modèle utilise SingleNAL par défaut (< packet-mode>0).

La configuration des événements téléphoniques, simples ou multiples, est également possible. Pendant la négociation du codec, le client envoie tous les codecs configurés, y compris l'événement téléphonique. Une fois le codec audio sélectionné, il recherche l'événement téléphonique dans l'offre. Si l'offre comporte l'événement téléphonique avec la fréquence d'échantillonnage du codec audio négocié, cet événement téléphonique est sélectionné. Sinon, le premier événement téléphonique de la liste est utilisé.

S'il y a au moins un événement téléphonique négocié, les multifréquences à double tonalité (DTMF) sont envoyées sous forme de paquets RTP en utilisant le type de charge utile correspondant. Et si aucun événement téléphonique n'est négocié, les DTMF sont envoyés sous forme de paquets RTP avec le type de charge utile du codec audio négocié. Le mécanisme hors bande pour fournir des DTMF n’est pas pris en charge par l’application Webex.

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 une fréquence d'échantillonnage de 48kbps est négocié, l'événement téléphonique avec la charge utile 101 est utilisé.

6.1.34.1 Codec AI

À partir de la version 44,8, l'application Webex introduit la prise en charge d'un nouveau codec audio : codec IA (xCodec). Ce codec audio est utilisé dans des conditions de réseau défavorables pour obtenir une meilleure qualité d'appel. Le moteur de médias Webex dans l’application Webex vérifie les fonctionnalités du périphérique, suit la qualité des médias et le codec IA peut être utilisé s’il est pris en charge et activé par le biais du fichier de configuration.

Le codec AI ne fonctionne qu'en combinaison avec le codec Opus. Cela signifie que les codecs Opus et AI doivent être annoncés et négociés par les deux parties au cours de la négociation SDP.

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 de "Free Calling". Dans certains environnements, cela n'est pas souhaitable et ces appels doivent être bloqués.

Confidentiel à Cisco

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

La configuration suivante offre cette option.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	vrai	vrai, faux	Contrôle si le SIP-URI doit être acheminé par Locus (true) ou bloqué (false).

6.1.36 Historique des appels

L'application Webex prend en charge l'historique des appels pour suivre les appels de l'utilisateur. Pour la ligne principale de l'utilisateur, l'historique des appels est synchronisé sur tous les périphériques de l'utilisateur. Pour les lignes secondaires (partagées et virtuelles), l'application ne conserve qu'un enregistrement d'historique d'appels local.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	vrai, faux	Pour la ligne principale uniquement, contrôle si l'application doit utiliser l'historique des appels unifié ou 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 fonction pour les appels VoIP soutenus par BroadWorks et Locus (gratuits).

Lorsque la fonctionnalité est activée et que la balise de fonctionnalité est définie sur "false" :

- l'utilisateur ne verra pas le paramètre "Accepter les appels entrants avec ma vidéo allumée".
- tous les appels vidéo entrants, s'ils sont acceptés, seront des appels audio
- l'utilisateur ne pourra pas faire passer un appel à la vidéo et les appels à la vidéo seront automatiquement rejetés

Confidentiel à Cisco

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 fonction est activée pour les ordinateurs de bureau et désactivée pour les téléphones portables et les tablettes.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	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 Portable/tablette - faux	vrai, faux	Contrôle la valeur par défaut du paramètre "Accepter les appels entrants avec ma vidéo allumée".

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 E911 la création de rapports d'emplacement à l'aide de RedSky, Intrado ou un autre E911 fournisseur de localisation d'urgence pour le déploiement de Webex pour BroadWorks. Le fournisseur E911 fournit une assistance pour la localisation de chaque périphérique (pour les applications de bureau et de 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) des États-Unis, de ses territoires (Guam, Porto Rico et Îles Vierges) et du Canada uniquement. Le service est activé sur une base par emplacement.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	false	vrai, faux	Active la plate-forme de localisation d'urgence du fournisseur E911.
%BWE911-PRIMARY-HELDURL%	vide	String	Spécifie l'URL de la plate-forme d'emplacement d'urgence du fournisseur E911 prenant en charge le protocole HELD.
%BWE911-CUSTOMERID%	vide	String	L'ID du client (HeldOrgId, CompanyID) utilisé pour la demande HTTPS du fournisseur E911.
%BWE911-SECRETKEY%	vide	String	Le code secret permettant d'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.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (l'utilisateur ne sera plus invité à répondre)	numéro [0 - 43200]	Le délai d'attente en minutes qui sera utilisé pour rappeler à l'utilisateur de mettre à jour l'emplacement d'urgence si l'emplacement d'urgence actuel n'est pas saisi ou n'est pas valide. Valeur suggérée si l'on décide de l'activer : 1440 (un jour).
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (l'utilisateur peut toujours annuler le dialogue)	numéro [-1 - 100]	Les fois où 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 le dialogue - emplacement obligatoire toujours) ▪ N > 0 (l'utilisateur est autorisé à annuler le dialogue N fois avant qu'il ne devienne obligatoire)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	agressif, une fois par connexion	une fois par connexion	Définit le comportement de l'invite d'emplacement E911. La valeur "agressif" affichera la boîte de dialogue à l'utilisateur à chaque changement de réseau vers un emplacement inconnu, tandis que la valeur "once_per_login" n'affichera la boîte de dialogue qu'une seule fois, évitant ainsi à l'utilisateur d'autres fenêtres contextuelles et distractions.

REMARQUE 1 : Les balises BWE911-*** sont des "balises système intégrées dynamiques". Pour plus d'informations, voir la section *5.7 Balises du système intégré dynamique Cisco* BroadWorks.

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 uniquement.

Confidentiel à Cisco

6.1.39 Le PAI en tant qu'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 la ligne appelante. Si un en-tête X-BroadWorks-Remote-Party-Info est présent dans le message SIP INVITE entrant, il est utilisé en priorité par rapport aux 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 De 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 « vrai », l'en-tête PAI est utilisé avec la priorité sur l'en-tête De. L'identité de l'appelant est utilisée pour résoudre le contact et le présenter à l'utilisateur.

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.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	vrai, faux	Contrôle si l'identité de l'appelant, présentée à l'utilisateur, doit être tirée des en-têtes SIP From ou SIP P-Asserted-Identity. La valeur "true" permet d'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 d'initier le partage d'écran dans les appels 1-1
- les demandes de partage d'écran entrantes sont rejetées et l'utilisateur reçoit un message d'information

Cette fonctionnalité est activée par défaut.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SCREEN_SHARE_WXT%	vrai	vrai, faux	Spécifie si le partage d'écran doit être activé pour l'utilisateur.

Confidentiel à Cisco

6.1.41 Indication des appels indésirables

Lorsque le bouton 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 de nouvel appel ou des enregistrements de l'historique des appels.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	vrai, faux	Contrôle la disponibilité de l'indication d'appel indésirable dans l'écran d'appel entrant et dans l'historique des appels pour Webex Calling uniquement.

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 qui appellent lorsqu'ils parlent à des utilisateurs qui ne font pas partie de Webex sur le réseau RTCP ou des périphériques 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 des médias audio entrants pour les appels RTCP à bande étroite.

- Un nouvel algorithme d'extension de la bande passante est ajouté pour améliorer la qualité audio en étendant la bande passante du spectre RTPC à bande étroite et en supprimant le bruit. La largeur de bande étendue augmente l'intelligibilité et réduit la fatigue d'écoute.
- L'algorithme de suppression du bruit déjà existant est amélioré, supprimant les limitations pour la musique d'attente et d'autres tonalités audio (par exemple, les signaux sonores).
- Lorsque cette fonction est activée, l'utilisateur voit l'indicateur "Smart audio - external" et peut contrôler les améliorations Speech AI pour le média audio entrant.

Par défaut, ces améliorations vocales sont activées. L'utilisateur peut contrôler l'état initial par le biais des paramètres audio intelligents dans les préférences audio.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	false	vrai, faux	Active les améliorations vocales pour les médias externes (entrants).

NOTE : La suppression du bruit fait maintenant partie des améliorations vocales supplémentaires, et la balise a été obsolète par la nouvelle balise . La balise personnalisée de suppression du bruit %ENABLE_NOISE_REMOVAL_WXT% est également obsolète.

6.1.43 Marquage QoS DSCP

Le marquage QoS DSCP est pris en charge par les paquets RTP de média d'appel de l'application Webex (audio et vidéo). Le DSCP détermine la classification du trafic pour les données du réseau. Cela permet de déterminer quel trafic réseau nécessite une plus grande largeur de bande, a une priorité plus élevée et est plus susceptible de laisser tomber des paquets.

REMARQUE : Les versions récentes du système d'exploitation Microsoft Windows n'autorisent pas les applications à configurer directement DSCP ou UP sur les paquets sortants, nécessitant au lieu de cela le déploiement d'objets de stratégie de groupe (GPO) pour définir les politiques de marquage DSCP basées sur les plages de ports UDP.

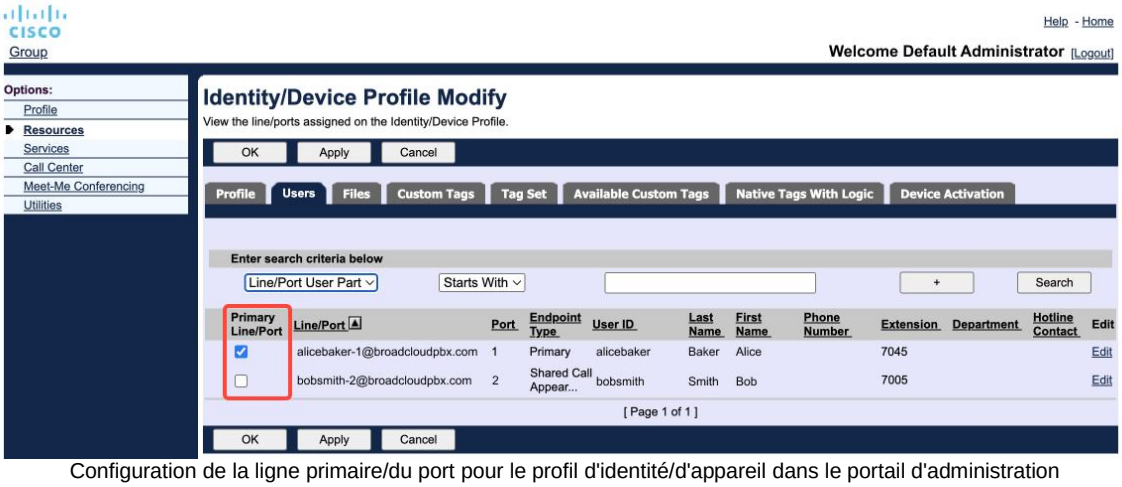
Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_AUDIO_QOS_WXT%	vrai	vrai, faux	Active la qualité de service pour les appels audio.
%AUDIO_QOS_VALUE_WXT%	46	0-63	Spécifie la valeur de QoS pour le type de QoS sélectionné pour les appels audio. Remarque : La valeur par 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 qualité de service pour les appels vidéo

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%VIDEO_QOS_VALUE_WXT%	34	0-63	Spécifie la valeur QoS du 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 primaire

Avec l'intégration des lignes partagées (*6.1.51.1 Bureau - Apparence de ligne partagée***Error! Reference source not found.**), si la ligne de l'utilisateur est partagée avec un autre utilisateur, il peut y avoir plusieurs profils du même type configurés pour l'utilisateur. Pour sélectionner le profil adéquat 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 de Cisco BroadWorks, cochez Drapeau du propriétaire dans la liste des périphériques pour prendre en charge les lignes partagées du client Webex.



Configuration de la ligne primaire/du port pour le profil d'identité/d'appareil 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/de port non principal pour se connecter aux services téléphoniques. Cette option de configuration s'applique à toutes les configurations, quel que soit le nombre de profils configurés pour l'utilisateur (**Si la restriction relative à la propriété des appareils est activée et qu'il n'y a pas d'appareil avec une ligne/un port primaire pour la plate-forme correspondante, les services téléphoniques ne se connecteront pas**).

Confidentiel à Cisco

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 qu'il possède. Cela empêche l'appariement avec les appareils 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	vrai	vrai, faux	Contrôle la restriction relative au propriétaire de l'appareil - si les services téléphoniques doivent utiliser le profil principal pour l'appareil donné.

NOTE : Il est recommandé d'activer la restriction du propriétaire. Si cette option est désactivée, les services téléphoniques utiliseront le premier profil trouvé pour se connecter. Des problèmes peuvent survenir si plusieurs profils du même type sont configurés pour l'utilisateur.

6.1.45 Liste de blocage (Webex Calling uniquement)

En commençant par 43,5 l'application Webex, vous trouverez la liste des numéros de téléphone bloqués définis par l'utilisateur. Si cette fonction est activée, l'utilisateur peut spécifier que les appels entrants provenant de numéros spécifiques seront bloqués du côté du serveur et ne seront pas transmis aux appareils 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 endroits : les préférences d'appel et l'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 comportent l'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 un enregistrement donné. L'option bloc est également disponible.

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

Format du numéro

- Le blocage des préférences d'appel applique la restriction du format E.164 localement dans l'application Webex
- Le blocage de l'historique des appels est autorisé pour tous les enregistrements Webex Calling

Confidentiel à Cisco

- 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 de l'utilisateur. Cette fonctionnalité fonctionne en même temps que 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 par le biais du Control Hub. Il n'y a AUCUN enregistrement de l'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 la liste de blocage STIR/SHAKEN, la liste de blocage définie par l'administrateur et les politiques de rejet des appels anonymes.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_BLOCK_WXT%	vrai	vrai, faux	Active la liste de blocs définie par l'utilisateur La valeur "true" permet d'afficher la liste des blocages dans les préférences d'appel et l'historique des appels.

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

6.1.46 Mise en œuvre de l'adaptation et de la résilience des médias (MARI)

6.1.46.1 Adaptation des taux

L'application Webex a déjà intégré des techniques de qualité média adaptative pour s'assurer que l'audio n'est affecté par aucune 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 de congestion.

L'adaptation du débit ou les ajustements dynamiques du débit binaire adaptent le débit d'appel à la largeur de bande variable disponible, en réduisant ou en augmentant le débit binaire vidéo en fonction de la condition de perte de paquets. Un point d'extrémité réduira le débit lorsqu'il recevra des messages du récepteur indiquant une perte de paquets ; une fois que la perte de paquets aura diminué, le débit augmentera.

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

Confidentiel à Cisco

6.1.46.2 Correction des erreurs de renvoi (FEC) et retransmission des 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 des erreurs de renvoi (FEC) et de la retransmission de paquets (RTX) à la fois pour les médias audio et vidéo.

Le FEC fournit une redondance aux informations transmises en utilisant un algorithme prédéterminé. La redondance permet au récepteur de détecter et de corriger un nombre limité d'erreurs, sans qu'il soit nécessaire de demander à l'expéditeur des données supplémentaires. Le FEC permet au récepteur de corriger les erreurs sans avoir besoin d'un canal inverse (tel que RTCP) pour demander la retransmission des données, mais cet avantage se fait au prix d'une bande passante fixe plus élevée pour le canal direct (plus de paquets envoyés).

Les points d'extrémité n'utilisent pas le FEC sur les bandes passantes inférieures à 768 kbps. En outre, la perte de paquets doit être d'au moins 1,5 % avant l'introduction du FEC. Les points finaux contrôlent généralement l'efficacité du FEC et si le FEC n'est pas efficace, il n'est pas utilisé.

Le FEC consomme plus de bande passante que la retransmission mais a moins de retard. RTX est utilisé lorsqu'un faible retard est autorisé et qu'il y a des contraintes de bande passante. En cas de retard important et de largeur de bande suffisante, le FEC est préférable.

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

Le 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>
```


Confidentiel à Cisco

```
            </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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_AUDIO_MARI_FEC_WXT%	false	vrai, faux	Active le FEC pour les appels audio
%ENABLE_AUDIO_MARI_RTX_WXT%	false	vrai, faux	Active RTX pour les appels audio (nécessite l'activation du FEC audio)
%ENABLE_VIDEO_MARI_FEC_WXT%	false	vrai, faux	Active le FEC pour les appels vidéo
%ENABLE_VIDEO_MARI_RTX_WXT%	false	vrai, faux	Active le protocole 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 appareil.

Cette fonction est utile pour certains déploiements, lorsque l'identité présentée pour l'appel n'est pas la même que l'identité connectée. Il en résulte l'impossibilité d'initier un transfert assisté vers la partie d'origine. En activant cette fonction, l'utilisateur pourra traiter plusieurs appels simultanés avec le même correspondant distant.

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


Confidentiel à Cisco

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false	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 a lieu pendant l'établissement de la session SIP INVITE. Si les deux terminaux prennent en charge les paquets RTCP-XR, le moteur de médias Webex commencera à échanger ces paquets et aidera le mécanisme adaptatif de qualité d'appel. Cette fonctionnalité est activée par défaut.

En outre, pour Webex Calling uniquement, ces mesures supplémentaires seront envoyées par le biais du protocole SIP BYE et seront ainsi exposées dans le Control Hub.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	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 renvoi 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'appels dans les écrans et l'historique des appels associés.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	vrai	vrai, faux	Contrôle la visibilité des informations relatives au renvoi et à la redirection d'appels. La valeur "true" permet d'afficher les informations dans les écrans relatifs aux appels et dans l'historique des appels.

6.1.50 ID de l'appelant

6.1.50.1 ID de l'appelant sortant

Les applications Webex Mobile (version 44,2) et Desktop (version 44,3) introduisent une nouvelle fonction permettant à l'utilisateur de choisir l'ID de l'appelant externe préféré pour les appels sortants. La liste des options disponibles comprend

- Ligne directe (par défaut)
- Numéro de l'emplacement
- Numéro personnalisé de la même organisation
- Files d'attente dont l'utilisateur fait partie, ce qui permet aux agents d'utiliser leur numéro d'identification de l'appelant.
    - Si des options DNIS sont configurées, elles pourront être sélectionnées
- Groupes de recherche dont l'utilisateur fait partie, ce qui permet aux agents d'utiliser leur numéro d'identification de l'appelant
- Masquer l'identité de l'appelant

Remarques :

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

Confidentiel à Cisco

La liste des options disponibles est configurable via le portail d'administration. Il existe également des balises personnalisées DMS 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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	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	vrai, faux	Contrôle la disponibilité des numéros supplémentaires configurés pour l'utilisateur.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	false	vrai, faux	Contrôle la disponibilité des numéros du centre d'appel (DNIS) configurés pour l'utilisateur.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	vrai, faux	Contrôle la disponibilité des numéros des groupes de recherche configurés pour l'utilisateur.
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	vrai, faux	Active le blocage de la remise de l'ID de l'appelant comme sélection pour les appels sortants.

NOTE : La version de l'application de bureau 44,3 ne prend en charge que le CLID du centre d'appels et 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. Dans le même temps, l'application Webex commence à résoudre les contacts à partir de plusieurs sources, avec la priorité suivante :

- Identité commune (IC)
- Service de contact (contacts personnalisés)
- Contacts Outlook (bureau)

Confidentiel à Cisco

- Carnet d'adresses local (mobile)

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

La version 44,5 de l'application Webex ajoute une option configurable pour ignorer la résolution des contacts et conserver toujours le nom d'affichage Cisco BroadWorks pour les appels avec des espaces de travail ou des périphériques RoomOS utilisés pour l'appel 1:1 Cisco BroadWorks.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	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 appareils RoomOS. Utilisez "sip" pour ignorer la résolution du contact et utiliser le nom d'affichage reçu dans la session INVITE SIP.

Confidentiel à Cisco

6.1.51 Multiligne

L'utilisateur Webex peut avoir une ligne principale et jusqu'à 9 lignes secondaires. Les lignes secondaires peuvent être partagées ou virtuelles (Webex Calling uniquement). Pour le déploiement de Webex pour BroadWorks, l'application de bureau ne fonctionne qu'avec les lignes partagées et la fonctionnalité n'est pas prise en charge dans l'application mobile.

L'application Webex obtient la configuration de la ligne via le fichier de configuration DMS qui est téléchargé lors de la connexion et tous les 12h horaires. Si une mise à jour de la configuration de la ligne est détectée, l'utilisateur est invité à redémarrer l'application pour appliquer les modifications. La reconnexion de l'utilisateur détectera et appliquera immédiatement toutes les mises à jour de la configuration de la ligne.

Le tableau suivant décrit la section du modèle de configuration DMS relative à la prise en charge multi-lignes pour les ordinateurs de bureau et les périphériques mobiles.

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

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

Pour contrôler la fonction multiligne, utilisez la balise personnalisée dédiée.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_MULTI_LINE_WXT%	false	vrai, faux	Active la prise en charge de plusieurs lignes (si elle est configurée). Si elle est désactivée (définie à "false"), seule la première ligne configurée sera utilisée par l'application.

REMARQUE 1 : La fonctionnalité Prise en charge du boss-admin (Cadre de direction-Assistant) n'est pas disponible en combinaison avec la configuration multi-lignes.

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

6.1.51.1 Bureau - Apparence de ligne partagée

À partir de la version 42,12, l'application Webex ajoute la prise en charge des lignes partagées. L'administrateur doit configurer les apparences d'appel partagées pour chaque ligne partagée.

Dans la version 43,12, l'application Webex a été améliorée pour permettre de déplacer (reprendre localement) un appel en attente sur une ligne partagée ou virtuelle, traité par un autre utilisateur ou par le même utilisateur sur un autre périphérique. Pour plus d'informations, consultez *6.2.12 Déplacer l'appel*.

6.1.51.2 Bureau - 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 des lignes virtuelles. Sur le plan fonctionnel, la configuration avec des lignes virtuelles correspond à la multi-ligne utilisant les lignes partagées, avec la possibilité de voir les lignes virtuelles configurées pour l'utilisateur et de les utiliser pour les appels entrants et sortants.

La version 43,4 étend la prise en charge des lignes virtuelles, en ajoutant le parcage d'appels de groupe et la récupération de parcage d'appels.

Dans la version 43,12, l'application Webex a été améliorée pour permettre de déplacer (reprendre localement) un appel en attente sur une ligne partagée ou virtuelle, traité par un autre utilisateur ou par le même utilisateur sur un autre périphérique. Pour plus d'informations, consultez *6.2.12 Déplacer l'appel*.

6.1.51.3 Mobile (Webex Calling uniquement)

Pour le déploiement de Webex Calling uniquement, la version 45,4 ajoute la prise en charge de plusieurs lignes (partagées et virtuelles) dans la version mobile de l'application Webex. L'affectation de ligne s'applique à la fois à l'application Webex de bureau et à l'application Webex mobile.

Confidentiel à Cisco

En raison des spécificités de la plateforme Mobile, l'utilisateur peut avoir jusqu'à deux appels simultanés sur n'importe quelle ligne.

> **REMARQUE 1** : Si l'appel avec le numéroteur natif est activé (voir *6.3.5.1 Appeler avec le numéroteur natif*), la multiligne est désactivée.
>
> **NOTE 2**: La version multi-ligne pour tablette n'est pas prise en charge.

6.1.52 Autorisation SIP améliorée

La version 45,4 de l'application Webex fournit une option configurable pour optimiser la communication SIP, en partageant l'autorisation entre toutes les sessions SIP. L'application stocke l'autorisation et la réutilise jusqu'à ce qu'elle soit toujours valide.

Cette fonctionnalité accélère la communication SIP entre le serveur et l'application Webex, réduit le trafic, réduit la durée de connexion des appels et améliore les performances globales de l'application Webex.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	vrai, faux	Lorsqu'elle est définie sur « vrai », l'amélioration de l'autorisation SIP est activée.

> **REMARQUE 1** : Certains SBC peuvent nécessiter une nouvelle autorisation SIP sur chaque session, donc cette fonctionnalité doit être utilisée en fonction des détails du déploiement.
>
> **NOTE 2**: Même si cette fonctionnalité est activée, si l'application Webex reçoit 401 Non autorisé, la nouvelle autorisation sera utilisée dans la demande SIP suivante.

6.1.53 Assistant personnel (Présence en absence)

Avec la version 44,11, l'application Webex mobile et la version 45,3, l'application Webex de bureau, ajoutent une intégration avec le service d'assistant personnel (PA) Cisco BroadWorks. Il fonctionne en combinaison avec la présence Absent de l'utilisateur et nécessite la synchronisation de l'état du PA avec la présence Webex sur le Cloud.

Le service PA offre à l'utilisateur la possibilité d'informer les appelants de la raison pour laquelle l'appelé n'est pas disponible, en fournissant éventuellement des informations sur la date de retour de l'appelé et sur la présence éventuelle d'un préposé pour traiter l'appel.

Confidentiel à Cisco

Si l'AP est activé, l'option de présence absente sera disponible pour l'utilisateur. Il peut être utilisé pour configurer le PA du côté de Cisco BroadWorks. Lorsque la fonction est activée, les utilisateurs verront la présence en attente de l'utilisateur en combinaison avec l'état de l'AP et la durée configurée.

L'utilisateur peut configurer uniquement la configuration manuelle du PA. Si des horaires affectent le service de l'assistant personnel, la présence sera mise à jour par le biais de la synchronisation de l'état de l'assistant personnel. Cependant, l'application Webex n'expose pas la configuration des horaires et les horaires qui affectent le PA.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	vrai, faux	Contrôle si la fonction de présence Absent est disponible pour l'utilisateur.

REMARQUE 1 : Cette fonction nécessite que la synchronisation du statut de l'assistant personnel soit activée à partir du hub partenaire.

NOTE 2: Le routage des appels de l'assistant personnel standard ne prendra pas effet lorsque les services NPD, Renvoi automatique d'appels ou Renvoi sélectif d'appels sont actifs.

NOTE 3: Les états de présence "Ne pas déranger" et "Occupé" ont une priorité plus élevée que "Absent". Lorsque le manuel de l'utilisateur active l'un de ces états de présence, l'activation de l'assistant personnel n'entraîne pas le passage de votre état de présence à l'état Absent.

Confidentiel à Cisco

6.2 Fonctionnalités du bureau uniquement

6.2.1 Déconnexion forcée

Cette fonctionnalité permet à Cisco BroadWorks de suivre les instances de clients en ligne avec le même type de périphérique et ne permet à l'une d'entre elles d'être en ligne qu'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 en ligne en même temps, ce qui entraîne des effets secondaires. Un exemple est celui d'un utilisateur disposant d'un ordinateur 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 SUBSCRIBE SIP au paquet d'événements *call-info* avec une valeur appid spéciale dans l'en-tête *From* , indépendamment de la valeur du paramètre *bsoft-call-info* . Lorsque Cisco BroadWorks détecte plusieurs instances client en ligne avec le même *appid*, il envoie un SIP NOTIFY spécial à l'instance client plus ancienne, ce qui la déconnecte. Par exemple, les clients Desktop auront un identifiant identique *appid-value* bien qu'il n'y ait aucune restriction quant à l'utilisation de cet identifiant du côté du client. La valeur de l'appid est configurée par le fournisseur de services.

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

Pour plus d'informations sur les correctifs et les versions Cisco BroadWorks nécessaires pour cette fonctionnalité, voir la section sur les exigences logicielles Cisco BroadWorks dans le *Guide de la solution Webex pour Cisco BroadWorks*.

Voir l'exemple suivant pour les détails de la 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_FORCED_LOGOUT_WXT%	false	vrai, faux	Active la déconnexion forcée.
%FORCED_LOGOUT_APPID_WXT%	vide	String	Appid utilisé côté serveur pour la corrélation. Il peut s'agir de n'importe quelle chaîne de caractères. Exemple : "123abc"

Confidentiel à Cisco

6.2.2 Prise d’appel

La prise d'appel est un service multi-utilisateurs qui permet à des utilisateurs sélectionnés de répondre à n'importe quelle ligne qui sonne au sein de leur groupe de prise d'appel. Un groupe de prise d'appel est défini par l'administrateur et constitue un sous-ensemble d'utilisateurs du groupe qui peuvent prendre les appels les uns des autres.

Les cas de ramassage suivants sont pris en charge :

- Prise d'appel aveugle
- le décrochage dirigé (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 fonction concernée 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	vrai, faux	La valeur "true" permet d'activer la prise d'appel en aveugle.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	vrai, faux	Définissez la valeur sur « true » (vrai) pour activer la prise d’appel dirigée.

6.2.3 Assistance Boss-Admin (Cadre de direction-Assistant)

Le Boss-Admin, connu sous le nom de fonctionnalité Cadre de direction-Assistant de Cisco BroadWorks, permet à un assistant d’agir pour le compte d’un cadre de direction pour filtrer, répondre et passer des appels en tant que « cadre ». Un assistant peut avoir plusieurs cadres et c'est possible :

- Sélectionnez le rôle souhaité lors d'un appel.
- Répondre à un appel entrant au nom d'un cadre et transférer l'appel au cadre. En outre, toutes les options habituelles de gestion des appels sont disponibles.
- S'assurer qu'un appel entrant est bien destiné au dirigeant.

Exécutif et Exécutif-Assistant sont deux services Cisco BroadWorks interconnectés qui offrent ensemble les fonctionnalités suivantes :

- Un utilisateur disposant du service Executive peut définir un pool d'assistants qui gèrent ses appels. Les assistants doivent être sélectionnés parmi les utilisateurs du même groupe ou de la même entreprise auxquels le service Executive-Assistant a été attribué.
- Un utilisateur disposant du service Executive-Assistant peut répondre et initier des appels au nom de ses cadres.

Confidentiel à Cisco

- Le cadre et ses assistants peuvent spécifier quels appels doivent être transférés aux assistants, comment les assistants doivent être avertis des appels entrants et lesquels des appels transférés aux assistants doivent être présentés au cadre pour être filtrés.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	vrai, faux	La valeur "true" permet d'activer la fonction Boss-Admin.

REMARQUE : La fonction Boss-Admin (assistant de direction) n'est pas disponible en combinaison avec les lignes partagées.

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

Le client fournit la fonctionnalité pour escalader un appel SIP en cours vers 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 pendant la réunion.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	vrai, faux	Définissez la valeur sur « true » (vrai) pour activer l'option du menu Escalader vers la réunion Webex.

6.2.5 Appels de contrôle du téléphone de bureau – Réponse automatique

La réponse automatique permet à l'utilisateur d'utiliser Desk Phone Control (DPC) pour les appels sortants sur le client afin de gérer les téléphones MPP avec une réponse sans contact.

Le téléphone MPP sélectionné transmettra l'audio/vidéo de l'appel DPC sortant.

La réponse automatique peut fonctionner sur les appareils provisionnés primaires et non primaires. Si l'utilisateur a plus d'un téléphone de bureau enregistré avec lequel il peut être jumelé, seul l'appareil sélectionné/jumelé répondra automatiquement.

Confidentiel à Cisco

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	vrai	vrai, faux	La valeur "true" permet d'activer la réponse automatique du contrôle du téléphone de bureau.

REMARQUE : La réponse automatique n'affecte 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 fonction permet de répondre automatiquement aux appels entrants pour les appareils locaux, si cela est indiqué dans la demande d'appel entrant.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_AUTO_ANSWER_WXT%	false	vrai, faux	La valeur "true" permet de répondre automatiquement aux appels entrants si cela est demandé par le backend.

6.2.7 Contrôle du téléphone de bureau - Contrôle des appels intermédiaires - Conférence

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	vrai, faux	Lorsqu'il est défini sur « vrai », active les options de conférence et de fusion pour les appels distants (XSI), terminés sur un autre emplacement.

Confidentiel à Cisco

6.2.8 Notifications de prise d'appel

Les notifications de prise d'appel permettent à l'utilisateur de savoir si un appel entrant est destiné à un utilisateur qu'il est configuré pour surveiller. Les notifications de prise d'appel peuvent être reçues pour les listes de surveillance configurées par le biais des services Groupe de prise d'appel et Champ de lampe occupée.

Les notifications de prise d'appel 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

L'application de bureau Webex affiche une notification si un membre de sa liste de surveillance de voyant d'occupation de ligne (FLO) a un appel entrant à l'état d'alerte. La notification contient des informations sur l'appelant et l'utilisateur qui a reçu l'appel entrant, ainsi que des options permettant de répondre à l'appel, de réduire au silence ou d'ignorer la notification. La réponse de l'utilisateur à l'appel entrant déclenche la prise d'appel dirigée.

À partir de la version 43,4, la liste des utilisateurs surveillés par un voyant d'occupation de ligne est disponible dans la fenêtre d'appels multiples (MCW) pour l'appel (disponible uniquement pour Windows). L'intégration de la liste des BLF 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 de la BLF.

Surveiller la présence des utilisateurs – la présence riche est disponible uniquement pour les utilisateurs disposant de l'autorisation Webex Cloud. La présence de base (téléphonie) n'est disponible que pour les utilisateurs de BroadWorks uniquement.

Commencer un appel avec un utilisateur BLF.

Démarrer une conversation instantanée avec un utilisateur FLO – disponible uniquement pour les utilisateurs disposant de Webex Cloud.

Ajouter un utilisateur FLO comme 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	vrai, faux	Active la surveillance du champ de la lampe occupée et la notification de la sonnerie pour les autres utilisateurs ayant la possibilité de prendre les appels.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_BLF_DISPLAY_CALLER_WXT%	vrai	vrai, faux	Permet d'afficher le nom/numéro de l'appelant dans la notification de sonnerie.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Contrôle le nombre de secondes pendant lesquelles la notification de sonnerie doit être retardée avant d'être affichée à l'utilisateur.

REMARQUE : Cette fonction dépend du service de prise d'appel dirigée.

6.2.8.2 Groupe de prise d'appel (Webex Calling uniquement)

À partir de la version 44,2, l'application Webex ajoute la prise en charge des notifications de prise d'appels de groupe (GCP) pour le déploiement de Webex Calling. Il permet aux utilisateurs d'être avertis des appels entrants pour n'importe quel utilisateur surveillé par le groupe de prise d'appel.

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

En cas d'appels multiples au sein d'un même groupe de prise d'appel, ils sont traités de manière séquentielle en fonction de l'heure à laquelle ils ont été reçus. La notification de l'appel le plus ancien est d'abord transmise au groupe et, une fois qu'elle a été traitée, la notification suivante est transmise au groupe.

Les notifications peuvent être audio uniquement, visuelles uniquement ou audio et visuelles en fonction de la configuration dans le portail d'administration du Control Hub. S'il y a une notification visuelle GCP, l'utilisateur peut prendre l'appel à l'aide de la fonction de prise d'appel. 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 manuellement le code FAC (*98) et le numéro de poste.

L'utilisateur peut mettre en sourdine la notification GCP par le biais des paramètres de l'application. Ce paramètre s'applique à toutes les notifications de prise d'appel (BLF et GCP) et, par défaut, les notifications sont mises en sourdine.

La fonction fonctionne pour les lignes primaires et pour les lignes partagées ou virtuelles attribuées à l'utilisateur.

Confidentiel à Cisco

```
<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>
        ...
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	vrai, faux	Active les notifications de prise d'appel 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	5-120	Définit la durée maximale pendant laquelle une notification BPC est disponible pour l'utilisateur.
%BWGROUP-CALL-PICKUP-BOOL-n%	false	vrai, faux	Indique si la ligne correspondante a un groupe de prise d'appel configuré

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

NOTE 2: Cette fonction dépend du groupe de prise d'appel 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 appelant, l'application Webex respecte désormais le pack d'événements de contrôle à distance lors de la réception d'un appel ou du traitement de la mise en attente/reprise.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false	vrai, faux	La valeur "true" indique que la télécommande doit être activée pour l'utilisateur.

6.2.10 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 au Cloud Webex, l'application Webex peut fonctionner en mode de survivabilité. Dans ce mode, l'utilisateur dispose d'une fonctionnalité d'appel limitée.

La passerelle de survie locale est déployée par le client.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	vrai, faux	Active la prise en charge du mode de survie.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Spécifie le temps de repli (passerelle de survivabilité vers SSE)

NOTE : Cette caractéristique permet de passer en toute confiance des solutions d'appel sur site aux solutions d'appel en nuage.

6.2.11 Pack d'événements pour le contrôle de la 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 de mise en sourdine à distance du flux de médias audio. Cela permet de couper/rétablir le 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 appelant.

Confidentiel à Cisco

La fonctionnalité dépend du nouveau paquet SIP *x-cisco-mute-status* info. Si l'en-tête *Recv-Info :x-cisco-mute-status* est reçu au cours de l'établissement de la session d'appel SIP INVITE, puis chaque fois qu'il y a une mise à jour (locale ou distante) vers l'état de coupure du son 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 muted représente l'état mis à jour du flux de médias audio.

La mise en sourdine ou le rétablissement du son peut être déclenché localement ou à distance. La mise à jour à distance déclenche un événement SIP NOTIFY avec *: couper le son* (ou *rétablir le son*) pour être envoyé à l'application Webex à partir du serveur d'applications. L'application Webex honore la demande distante 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false	vrai, faux	Lorsqu'il est défini sur « vrai », le contrôle de mise en sourdine à distance est activé pour l'utilisateur.

6.2.12 Déplacer l'appel

L'application Webex fournit la surveillance des appels et le contrôle des appels VoIP terminés sur un autre emplacement. Cette fonction n'est actuellement disponible que 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 des appels en cours à titre d'information et sans possibilité de les contrôler. Ce n'est que si un tel appel est mis en attente que l'utilisateur pourra le déplacer vers l'appareil local en le sélectionnant et en le reprenant à partir de l'écran d'appel. Ce mécanisme est utile si l'appel a été traité par le même utilisateur sur un autre site 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 apparié à un appareil, il doit d'abord se déconnecter, puis il peut reprendre l'appel en cours localement.

La surveillance des appels pour les lignes partagées et virtuelles dépend du paquet d'événements SIP call-info.

Confidentiel à Cisco

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

- 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 est en communication avec Charlie via le téléphone de bureau - Alice peut voir l'appel en cours dans l'application Bureau.
    c. Alice met l'appel en attente à partir du téléphone de bureau - Alice peut reprendre l'appel à partir de l'application de bureau.
- 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.
- Cas d'utilisation 3 :
    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 Desktop.
    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 Desktop du téléphone de bureau - Alice peut reprendre l'appel avec Charlie à partir de l'application Desktop.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALL_MOVE_HERE_WXT%	false	vrai, faux	Permet le déplacement d'appel sur l'appareil local. Utilisé pour la mise en attente/reprise à travers les lieux/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 les appels d'urgence natifs.

Lorsque la fonction 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. Elle est configurable à l'aide de la balise *dial-sequence* .

Les modes pris en charge sont les suivants :

- cs-uniquement : le client ne passe des appels d'urgence que via le réseau cellulaire si le réseau est disponible.
- cs-first - Lorsqu'il lance un appel d'urgence, le client vérifie le type de réseau auquel l'appareil actuel est connecté. Si le réseau cellulaire est disponible, le client passe l'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 via le réseau cellulaire, le client suggère à l'utilisateur de réessayer l'appel d'urgence en tant que VoIP.
- VoIP uniquement : le client ne passe des appels d'urgence que en tant que VoIP si le réseau WiFi/données cellulaires est disponible.
- cs-voip - Le client analyse si l'appareil peut l'initier en tant qu'appel à commutation de circuits (CS) natif (sans tenir compte du fait que le réseau CS est disponible ou non). Si l'appareil peut démarrer un appel natif, le numéro d'urgence est composé comme un appel CS d'urgence. 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 uniquement.

Un message d'avertissement concernant les appels d'urgence est affiché à l'utilisateur lors de la connexion. Il n'est pas contrôlé par les options de configuration.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_EMERGENCY_DIALING_WXT%	false	vrai, faux	La valeur "true" permet d'activer la détection des appels d'urgence. La valeur par défaut est vide.

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	cs-only	cs-uniquement, cs-d'abord, voip uniquement, cs-voip	Contrôle le mode de séquence de numérotation pour les appels d'urgence.
%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'il reçoit un appel entrant, 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. Lorsque la notification push est reçue, OU
2. Lorsque l'appel est accepté par l'utilisateur.

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

Selon les exigences d'iOS13 , les PN VoIP ne doivent être utilisés que pour les appels entrants. Les autres événements liés à l'appel doivent utiliser des PN ordinaires.

Pour répondre à cette exigence, une nouvelle API d'enregistrement des PN est introduite et nécessite l'application du correctif correspondant sur le serveur d'application. Si le backend n'est pas configuré pour prendre en charge les PN d'iOS13 , le paramètre de configuration peut être utilisé pour forcer l'utilisation des notifications push héritées, où tous les événements liés aux appels sont transmis via les PN de la VoIP.

Une notification push est envoyée par le serveur d'application (AS) lorsqu'un appel sonnant est accepté par l'appelant sur un autre site, fermé par l'appelant ou, par exemple, redirigé vers la messagerie vocale. Avec iOS 13, ce type de notification Push est désormais normal et comporte certaines restrictions. Elle peut être retardée par le service de notification push d'Apple (APNS) ou même ne pas être délivrée du tout. Pour gérer les PN de mise à jour d'appel manquants ou retardés, un délai de sonnerie configurable est ajouté pour contrôler la durée maximale de la sonnerie. Si la durée maximale de sonnerie est atteinte, la sonnerie est interrompue pour le destinataire de l'appel et l'appel est considéré comme manqué. Du côté de l'appelant, l'appel peut rester en état de sonnerie jusqu'à ce que la politique de non-réponse configurée sur le serveur d'application (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 distincte a été ajoutée pour spécifier le comportement de refus d'appel lorsqu'un appel entrant est reçu sous la forme d'une 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 des appels Cisco BroadWorks attribués seront appliqués. Si "decline_false" est configuré, l'appel continue de sonner jusqu'à ce que le demandeur abandonne ou que le délai de non-réponse expire, et les services de traitement des appels associés démarrent. Si "decline_true" est configuré, le motif de déclin spécifie le traitement de l'appel. Si le motif de refus est "occupé", le serveur force immédiatement le service de traitement occupé. Si "temp_unavailable" est configuré, le service de traitement des indisponibilités temporaires 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	vrai, faux	Contrôle le moment où la session SIP REGSITER est établie - lors de la réception d'une notification push pour un appel entrant ou lors de son acceptation.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Contrôle la durée maximale de la sonnerie des appels entrants pour les appels reçus par PN. Si aucun PN CallUpd n'est reçu dans le délai imparti, l'appel sera considéré comme manqué.
%REJECT_WITH_XSI_MODE_WXT%	decline_false (faux)	ignorer, décliner_vrai, décliner_faux	Spécifie le comportement de refus d'appel.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	occupé(e)	busy, temp_unavailable	Spécifie la raison du refus de l'appel, si le mode de rejet est réglé sur "decline_true".

6.3.2.1 indicateur de message (MWI)

Avec la fonctionnalité MWI activée, le client Webex mobile s'abonne à la notification MWI Push pour recevoir des mises à jour avec la messagerie vocale de l'utilisateur et l'informer.

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

Confidentiel à Cisco

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

6.3.2.2 Sonnerie d'avertissement

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

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_RING_SPLASH_WXT%	false	vrai, faux	Active Ring Splash dans la configuration BroadWorks.

6.3.2.3 Mode de livraison (Webex Calling uniquement)

L'application Webex utilise le serveur Push de notification (NPS) pour envoyer les notifications push pour les appels à APNS/FCM. La version 45,2 de l'application Webex prend maintenant en charge trois modes de transmission différents pour configurer la manière dont les notifications push liées aux appels doivent être transmises à APNS/FCM :

- SNP - Mécanisme actuel, utilisant le SNP
- Cloud - mécanisme amélioré, utilisant le microservice Cisco Webex Cloud
- externe - un mécanisme qui utilise un système tiers. Elle nécessite l'intégration du système tiers avec le moteur Cisco WebHooks.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	nps	nps, cloud, externe	Spécifie le mode de livraison des notifications push pour les appels.

Confidentiel à Cisco

6.3.3 Alerte unique

La fonction Mobile Single Alert est destinée aux déploiements de convergence fixe-mobile (FMC) / opérateurs de réseaux mobiles (MNO) qui exploitent 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 cette fonction est activée, l'application désactive l'alerte de mobilité 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 l'utilisation de cette fonction est que l'utilisateur ait le service BroadWorks Mobility assigné et exactement un emplacement configuré.

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_SINGLE_ALERTING_WXT%	false	vrai, faux	La valeur "true" permet d'activer l'alerte unique.

6.3.4 Cliquer pour composer (Rappeler)

Le Click to Dial sortant permet à l'utilisateur final d'avoir un appel sur son téléphone mobile personnel à commutation de circuits et de fournir son numéro d'entreprise comme identifiant de la ligne d'appel.

Le client Webex mobile prend en charge les appels Click to Dial (Rappel) en utilisant le service BroadWorks Anywhere. Les emplacements BroadWorks Anywhere dans l'application Webex sont appelés emplacements Portée du numéro individuel (SNR).

Lorsque la fonction est activée, les utilisateurs peuvent sélectionner l'emplacement du SNR dans le menu d'appairage de l'appareil. Lorsqu'il est associé à la localisation SNR, tous les appels sortants sont initiés par des appels Click to Dial (Call Back). Pour éviter les doubles alertes, les notifications push pour les appels entrants sont désactivées.

Lorsqu'un utilisateur lance un appel Click to Dial, il voit apparaître l'écran d'appel sortant avec des informations sur l'attente d'un appel entrant sur le site SNR sélectionné. Cet écran est fermé automatiquement en fonction d'un délai configurable.

Lors de la déconnexion d'un site SNR, l'application s'enregistre à nouveau pour recevoir des notifications push en cas d'appels entrants.

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


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_DIALING_CALL_BACK_WXT%	false	vrai, faux	La valeur "true" permet d'activer les appels Click to Dial (Call Back).
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Contrôle le nombre de secondes avant la fermeture automatique de l'écran de rappel.

6.3.5 Prise en charge MNO

6.3.5.1 Appeler avec le numéroteur natif

Cette fonctionnalité ajoute la prise en charge des déploiements des opérateurs de réseaux mobiles (ORM) qui exploitent le service BroadWorks Mobility (BWM). On suppose que le service BroadWorks Mobility a été attribué à l'utilisateur et qu'au moins un emplacement a été configuré.

La capacité de l'utilisateur à lancer des appels via le composeur natif est contrôlée par la balise de configuration **native** . Si cette option est activée, l'application lancera le composeur 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 qu'il souhaite utiliser.

Le < mode de numérotation> contrôle si les utilisateurs peuvent sélectionner la manière dont les appels entrants et sortants doivent être démarrés/reçus. Les appels natifs et les appels VoIP doivent être activés.

À partir de la version 43,12, la configuration de numérotation d'origine 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'applications Cisco BroadWorks intégré, les codes FAC peuvent être traités par le serveur d'applications Telecom. Une nouvelle balise est ajoutée sous la section 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%"/>
```


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_DIALING_VOIP_WXT%	vrai	vrai, faux	La valeur "true" permet d'activer l'option d'appel VoIP.
%ENABLE_DIALING_NATIVE_WXT%	false	vrai, faux	Définissez la valeur sur « true » (vrai) pour activer l'option d'appel d'origine.
%ENABLE_DIALING_MODE_WXT%	false	vrai, faux	Permet à l'utilisateur de sélectionner le mode d'appel par le biais des paramètres d'appel dans les préférences.
%DIALING_MODE_DEFAULT_WXT%	voip	voip, native	Spécifie le mode d'appel par défaut sélectionné.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false	vrai, faux	Contrôle si la disponibilité de l'appel natif doit dépendre de l'affectation du service BroadWorks Mobility et de l'emplacement de mobilité configuré pour l'utilisateur.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*vide*	String	Spécifie un préfixe qui doit être ajouté si l'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.

REMARQUE 1 : Au moins un des appels **voip** et **native** 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 **native** et **voip** sont activés, dans les déploiements MNO, il est recommandé d'activer l'alerte unique pour éviter les doubles alertes.

6.3.5.2 Commandes en cours d'appel

Cette fonctionnalité permet au client mobile Webex de contrôler via les appels natifs XSI sur le périphérique mobile qui sont ancrés sur Cisco BroadWorks. La commande d'appel XSI n'est disponible que si :

- Le service BroadWorks Mobility (BWM) est attribué à l'utilisateur,
- Il n'y a qu'une seule identité mobile BMW configurée,
- Le mode d'appel natif est sélectionné par l'utilisateur (pour plus d'informations, voir la section *6.3.5.1 Appeler avec le numéroteur* natif*),*
- Il y a un appel ancré sur BroadWorks, qui passe par le service BMW,
- Un appel cellulaire est en cours sur l'appareil mobile.

Confidentiel à Cisco

La version 43,1 ajoute une meilleure gestion du transfert consultatif, créant une association entre les deux appels cellulaires présentés dans l'application Webex et offrant à l'utilisateur une option pour terminer le transfert. En outre, si l'utilisateur a deux appels cellulaires indépendants sur le même appareil, le menu de transfert est amélioré pour permettre le transfert de l'un à l'autre, même si aucune association n'a été créée entre eux.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_XSI_CALL_CONTROL_WXT%	false	vrai, faux	Active le contrôle des appels XSI pour l'environnement MNO.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Contrôle le type de déploiement XSI MNO utilisé par l'application. Les valeurs possibles sont : ▪ MNO_Access - montre tous les appels à distance (XSI) avec les types de dispositifs définis dans le nœud ci-dessous. ▪ MNO_Network - affiche tous les appels à distance (XSI).
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	String	Le(s) nom(s) du type d'appareil à utiliser dans le type de déploiement MNO_Access.
%ENABLE_XSI_HOLD_CALLS_WXT%	vrai	vrai, faux	Contrôle si l'action de mise en attente de l'appel doit être disponible pour l'utilisateur pour les appels mobiles XSI.

6.3.5.3 Identité de la ligne d’appel sortante (CLID) – Double identité

Avec la version mobile 42,12, l'application Webex permet aux utilisateurs de sélectionner l'identité de leur ligne appelante (CLID) présentée à l'interlocuteur distant lors de l'initiation d'un appel sortant.

Si l'utilisateur est configuré avec Cisco BroadWorks Mobility, si la configuration typique des déploiements MNO (Mobile Network Operator) et si 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 existe également une option permettant de masquer sa propre identité et de présenter l'appel comme anonyme.

Pour les appels VoIP, l'utilisateur a également la possibilité de contrôler son CLID. L'option disponible dans ce cas consiste uniquement à contrôler si son identité est cachée ou non.

Confidentiel à Cisco

La gestion des personnes et le blocage du 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%"/>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	false	vrai, faux	Active le blocage de la transmission de l'ID de la ligne appelante. Il s'applique à tous les types d'appels sortants de l'utilisateur.
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	false	vrai, faux	Active la gestion personnelle pour les 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 MNO, cette fonctionnalité ajoute une bannière de notification pour les appels d'origine, qui peuvent être contrôlés via l'application Webex. Cette notification repose sur la notification Push, envoyée par le serveur d'applications une fois l'appel établi.

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	vrai	vrai, faux	Active l'abonnement à la notification push MOBILE_CALL_INFO.

6.3.5.5 Déplacer un appel natif vers une réunion convergente

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

Confidentiel à Cisco

- Lancer Webex dans une réunion Chat
- Ajouter une vidéo (l'audio continuera dans l'appel natif)
- Partager l'écran / le contenu
- Déclencher l'enregistrement des réunions

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	vrai, faux	Active la mise sous tension (actions Invite and Meet, Video Meet).

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 d'appel (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'affichera au-dessus de l'interface utilisateur native et permettra à l'utilisateur d'effectuer les actions suivantes :

- Attente/Reprise
- Transfert sans suivi/consultatif : place l'utilisateur dans la boîte de dialogue de transfert de l'application Webex.
- Effectuer le transfert : permet de terminer le transfert consultatif (version 43,1)
- Réunion vidéo – déplace les parties dans une réunion Webex.
- Raccrocher

```
<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%"/>
```


Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_WIDGET_HOLD_CALLS_WXT%	vrai	vrai, faux	Contrôle la disponibilité de l'action Hold dans le Call Widget.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	vrai	vrai, faux	Contrôle la disponibilité des actions Transférer et Terminer le transfert dans le widget Appel.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	vrai	vrai, faux	Contrôle la disponibilité de l'action Réunion vidéo dans le widget Appel.

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 manqué.

6.3.6.1 Écran d'appel entrant

Il existe des différences de plateforme entre Android et iOS en ce qui concerne l'affichage des données dans l'écran d'appel entrant. L'expérience native de l'affichage des informations relatives à un appel entrant est la suivante :

Android : il y a deux champs distincts dans l'écran de l'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 Webex iOS affichera le numéro dans l'écran d'appel à côté du nom (format : *Nom (numéro)*). Le comportement de l'application Android Webex 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'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 elle est activée et que le nom et le numéro sont disponibles, l'application Webex ajoute le numéro à côté du nom (format : *Nom (numéro)*). Ce comportement de l'application Webex s'applique 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'appels manqués. Il peut être utilisé pour contrôler les informations sur le correspondant distant, comme pour les notifications d'appels entrants, ce qui permet d'ajouter le numéro au nom d'affichage de l'utilisateur distant et de le présenter dans la notification d'appel manqué. Ce comportement de l'application Webex s'applique 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>
```

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false	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	vrai, faux	Contrôle si le numéro doit être ajouté au nom dans la notification d'appel manqué.

REMARQUE : Si le numéro est fourni comme nom d'affichage ou si le nom d'affichage se termine par le numéro, l'application Webex évitera la duplication et n'affichera le numéro qu'une seule fois.

Confidentiel à Cisco

7 Caractéristiques des premiers essais sur le terrain (BETA)

7.1 Appel d'urgence (911) - Service d'information de localisation d'urgence Cisco (Webex Calling uniquement) et nettoyage de la configuration

L'application Webex prend déjà en charge la localisation d'urgence pour les appels d'urgence, en utilisant des fournisseurs tiers, comme décrit dans 6.1.36 1x38d="1" />*6.1.38*.Appels d'urgence (911) - Création de rapports de localisation avec le fournisseur E911 Cette fonctionnalité s'applique aux appels d'urgence vers les centres de réponse de la sécurité publique (PSAP) des États-Unis, de ses territoires (Guam, Porto Rico et îles Vierges) et du Canada uniquement.

Pour le déploiement exclusif de Webex Calling, Cisco a ajouté son propre service d'informations de localisation d'urgence pour gérer et stocker les interactions HELD/HELD+, gérer les cartes filaires créées par l'entreprise et les utilisateurs, stocker les adresses avec leurs attributs PIDF-LO et envoyer les informations de localisation pour les appels d'urgence.

La version 45,1 de l'application Webex ajoute une intégration avec le service de localisation d'urgence de Cisco. Le modèle de configuration DMS est mis à jour, pour ajouter la prise en charge de différents fournisseurs de localisation d'urgence :

- La section actuelle sous du modèle de configuration DMS est obsolète. Une nouvelle section est ajoutée à la place et sera utilisée par l'application Webex à partir de maintenant.
- Une nouvelle option de *fournisseur* est maintenant disponible dans la nouvelle section, permettant le contrôle du fournisseur d'emplacement d'urgence que l'application Webex doit utiliser. Les options disponibles comprennent *redsky*, *intrado*, *9line* et *webex*. Les trois premières options sont disponibles pour le déploiement de Webex pour BroadWorks et sont principalement utilisées à des fins de suivi, en utilisant le protocole HELD+ pour la communication avec des fournisseurs tiers. L'option *Webex* n'est disponible que pour le déploiement de Webex Calling et permet à l'application d'utiliser le service d'informations de localisation d'urgence de Cisco, avec un plan filaire amélioré et une prise en charge PIDF-LO pour les appels d'urgence.
- De nouvelles balises personnalisées ont été ajoutées qui nécessitent leur configuration manuelle, pour correspondre à la configuration actuelle (si la fonctionnalité est déjà utilisée). Sans être configurées, les valeurs par défaut seront utilisées, ce qui peut désactiver la fonction ou modifier le comportement
- Il n'y a aucune mise à jour dans les balises système utilisées pour les , , et .
- [**Important**] Empêchez la fonctionnalité d'emplacement d'urgence d'être désactivée en raison d'une mauvaise configuration, assurez-vous que la nouvelle balise personnalisée contrôlant la disponibilité de la fonctionnalité d'emplacement d'urgence (%ENABLE_EMERGENCY_LOCATION_WXT%) est définie de la même manière que la balise existante (%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%).

Confidentiel à Cisco

- [**Important**] Pour éviter de perdre cette fonctionnalité critique en raison d'une mauvaise configuration, une logique de compatibilité ascendante a été ajoutée à l'application Webex. Si la nouvelle section de configuration est manquante dans le modèle ou si la nouvelle balise personnalisée (%ENABLE_EMERGENCY_LOCATION_WXT%) n'est pas configurée, ce qui conduit à configurer l'attribut activé sur « faux », l'application Webex tentera de lire la section de configuration existante () et d'appliquer ses valeurs.
- Si la fonction est désactivée, les appels d'urgence seront acheminés pour être triés par le ERC (Emergency Relay Center) afin de valider la localisation de l'appelant avant d'être acheminés vers un PSAP approprié, ce qui peut entraîner des frais supplémentaires.

L'extrait suivant affiche les modifications apportées au modèle de configuration DMS :

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

Le tableau suivant répertorie le mappage entre les nouvelles balises personnalisées et les anciennes :

Option de configuration	Balise personnalisée obsolète	Nouvelle balise personnalisée
L'attribut activé dans la balise par rapport au même dans l'ancienne balise	%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	%ENABLE_EMERGENCY_LOCATION_WXT%
Balise	%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%

Confidentiel à Cisco

Balise	%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%
Balise	%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_EMERGENCY_LOCATION_WXT%	false	vrai, faux	Active l'utilisation de la plateforme de localisation d'urgence.
%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%	ciel rouge	redsky, intrado, 9ligne, webex	Indique quel fournisseur de localisation d'urgence doit être utilisé. « webex » s'applique uniquement au déploiement de Webex Calling et doit être configuré pour utiliser le service d'information de localisation d'urgence de Cisco.
%BWE911-PRIMARY-HELDURL%	vide	String	Spécifie l'URL du fournisseur E911 prenant en charge le protocole HELD.
%BWE911-CUSTOMERID%	vide	String	L'ID du client (HeldOrgId, CompanyID) utilisé pour la demande HTTPS du fournisseur E911.
%BWE911-SECRETKEY%	vide	String	Le code secret permettant d'authentifier la demande HTTPS du fournisseur E911. Non utilisé (vide) avec « webex » comme E911 fournisseur
%BWE911-EMERGENCY-NUMBER-LIST%	vide	Chaîne CSV	La liste des numéros d'urgence pris en charge par le fournisseur E911.
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	0 (l'utilisateur ne sera plus invité à répondre)	numéro [0 - 43200]	Le délai d'attente en minutes qui sera utilisé pour rappeler à l'utilisateur de mettre à jour l'emplacement d'urgence si l'emplacement d'urgence actuel n'est pas saisi ou n'est pas valide. Valeur suggérée si l'on décide de l'activer : 1440 (un jour).

Confidentiel à Cisco

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	-1 (l'utilisateur peut toujours annuler le dialogue)	numéro [-1 - 100]	Les fois où 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 le dialogue - emplacement obligatoire toujours) N > 0 (l'utilisateur est autorisé à annuler le dialogue N fois avant qu'il ne devienne obligatoire)
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	une fois par connexion	agressif, une fois par connexion	▪ Définit le comportement de l'invite d'emplacement E911. La valeur "agressif" affichera la boîte de dialogue à l'utilisateur à chaque changement de réseau vers un emplacement inconnu, tandis que la valeur "once_per_login" n'affichera la boîte de dialogue qu'une seule fois, évitant ainsi à l'utilisateur d'autres fenêtres contextuelles et distractions.

7.2 Historique unifié des appels pour les lignes secondaires (Webex Calling uniquement)

L'application Webex prend en charge l'historique des appels synchronisés sur tous les périphériques pour la ligne principale de l'utilisateur, comme décrit dans la section *6.1.36 Historique des appels*.

Pour le déploiement exclusif de Webex Calling, la version 45,1 étend la fonctionnalité aux lignes secondaires (partagées et virtuelles).

7.3 Chiffrement de bout en bout (Webex Calling uniquement)

À partir de la version 45,1, pour le déploiement de Webex Calling uniquement, cette application Webex ajoute la prise en charge du chiffrement de bout en bout (E2EE) pour les médias audio et vidéo, pour les appels 1-on-1 au sein de la même organisation. Le E2EE garantit que seuls les participants à la communication peuvent déchiffrer le contenu.

Que les appels commencent par le chiffrement SRTP standard, avec les clés échangées pendant la négociation SDP. Si les deux parties prennent en charge E2EE, un nouvel ensemble de clés, que seuls les deux participants connaissent, est utilisé pour chiffrer le média.

Confidentiel à Cisco

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

Étiquette	Valeur par défaut en cas d'omission	Valeurs supportées	Description
%ENABLE_CALLS_E2EE_WXT%	false	vrai, faux	Contrôle si le E2EE doit être activé pour les appels 1:1.

Confidentiel à Cisco

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 héritées pour UC-One.

Balise Webex pour Cisco BroadWorks	Étiquette de l'héritage du bureau	Étiquette d'héritage mobile
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	S/O	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	S/O	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ACTIVER_TRANSFÉRER_APPELS%	%ACTIVER_TRANSFÉRER_APPELS_MOBILES%
%ENABLE_CONFERENCE_CALLS_WXT%	S/O	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	S/O
%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%	S/O	%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%	%MODE_MWI_DU BUREAU%	%MWI_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	N/A	N/A
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	S/O
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	S/O
%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	Étiquette de l'héritage du bureau	Étiquette d'héritage 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%	S/O	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	S/O
%SBC_ADDRESS_WXT%	%SBC_ADDRESS%	%SBC_ADDRESS%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILE %
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	S/O
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	N/A

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Étiquette de l'héritage du bureau	Étiquette d'héritage 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	Étiquette de l'héritage du bureau	Étiquette d'héritage 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_BLI ND_WXT%	N/A	N/A
%ENABLE_CALL_PICKUP_ DIRECTED_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_URL _WXT%	N/A	%WEB_CALL_SETTINGS_URL %
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP %
%ENABLE_CALL_CENTER_ WXT%	%ENABLE_CALL_CENTER_ DESKTOP%"	N/A
%WEB_CALL_SETTINGS_TAR GET_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_CFA _ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFA _VISIBLE%
%WEB_CALL_SETTINGS_DN D_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_DN D_VISIBLE%
%WEB_CALL_SETTINGS_AC R_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_AC R_VISIBLE%
%WEB_CALL_SETTINGS_CFB _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFB _VISIBLE%
%WEB_CALL_SETTINGS_CFN R_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFN R_VISIBLE%
%WEB_CALL_SETTINGS_CFN A_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFN A_VISIBLE%
%WEB_CALL_SETTINGS_SIM RING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SIM RING_VISIBLE%
%WEB_CALL_SETTINGS_ SEQRING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SE QRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_RO_ VISIBLE%
%WEB_CALL_SETTINGS_ACB _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_ACB _VISIBLE%
%WEB_CALL_SETTINGS_CW _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CW _VISIBLE%
%WEB_CALL_SETTINGS_CLI DB_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CLI DB_VISIBLE%
%WEB_CALL_SETTINGS_PA_ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_PA_ VISIBLE%

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Étiquette de l'héritage du bureau	Étiquette d'héritage 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	Étiquette de l'héritage du bureau	Étiquette d'héritage 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	Étiquette de l'héritage du bureau	Étiquette d'héritage 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
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N/A	N/A
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	N/A	N/A
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	N/A	N/A

Confidentiel à Cisco

Balise Webex pour Cisco BroadWorks	Étiquette de l'héritage du bureau	Étiquette d'héritage mobile
%CALL_PULL_MODE_WXT%	N/A	N/A
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	N/A	N/A
%ENABLE_EMERGENCY_LOCATION_WXT%	N/A	N/A
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	N/A	N/A
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	N/A	N/A
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	N/A	N/A
%ENABLE_CALLS_E2EE_WXT%	N/A	N/A

REMARQUE : N/A indique qu'il n'y a pas de balise personnalisée correspondante contrôlant la fonctionnalité dans UC-One. Avoir N/A pour les balises héritées 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

8 Annexe A : Chiffrements TLS

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

Confidentiel à Cisco

9 Annexe B : Script d'approvisionnement en étiquettes DM

Le nombre d'étiquettes DM personnalisées a augmenté avec chaque version, car de nombreux clients préfèrent les étiquettes pour les nouveaux paramètres de configuration. Pour faciliter le provisionnement de ces étiquettes DM personnalisées, cette section contient un script qui peut être exécuté du côté du serveur d'application (AS) pour attribuer des valeurs aux étiquettes 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 valable que pour les nouveaux déploiements où des étiquettes DM personnalisées sont créées. Pour modifier des balises DM personnalisées existantes, la commande du script suivant doit être remplacée par "set" au lieu de "add".

Modèle de script avec seulement quelques balises personnalisées (dans un déploiement réel, vous devriez remplir une liste plus importante de balises personnalisées). Notez que l'exemple suivant concerne les téléphones portables. Pour les ordinateurs de bureau, utilisez le jeu de balises BroadTouch_tags au lieu de Connect_Tags. Pour les tablettes, 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
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------------------------------------------------------------------------------------------------------------
%% Step 4: Verify custom tags have been correctly defined and set
%% ----------------------------------------------------------------------------------------------------------------
```


Confidentiel à Cisco

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

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

9.1 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
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
```


Confidentiel à Cisco

```
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
```


Confidentiel à Cisco

```
add tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PARK_WXT% false
add tagSetName BroadTouch_tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
add tagSetName BroadTouch_tags %RTP_ICE_PORT_WXT% 3478
add tagSetName BroadTouch_tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName BroadTouch_tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID_WXT% true
add tagSetName BroadTouch_tags %XSI_ROOT_WXT% true
add tagSetName BroadTouch_tags %SBC_ADDRESS_WXT% true
add tagSetName BroadTouch_tags %SBC_PORT_WXT% true
add tagSetName BroadTouch_tags %MWI_MODE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName BroadTouch_tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUTO_ANSWER_WXT% false
add tagSetName BroadTouch_tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName BroadTouch_tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName BroadTouch_tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName BroadTouch_tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName BroadTouch_tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REMOTE_MUTE_CONTROL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName BroadTouch_tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_MOVE_HERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_NOTIFICATIONS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_DISPLAY_CALLER_WXT% false
add tagSetName BroadTouch_tags %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% 120
add tagSetName BroadTouch_tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName BroadTouch_tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName BroadTouch_tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT% false
add tagSetName BroadTouch_tags %CALL_PULL_MODE_WXT% false
add tagSetName BroadTouch_tags %CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT% call_move
add tagSetName BroadTouch_tags %ENABLE_EMERGENCY_LOCATION_WXT% false
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_PROVIDER_NAME_WXT% redsky
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
```


Confidentiel à Cisco

```
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName BroadTouch_tags %ENABLE_CALLS_E2EE_WXT% false
```

9.2 Portable

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


Confidentiel à Cisco

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


Confidentiel à Cisco

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


Confidentiel à Cisco

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

9.3 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
```


Confidentiel à Cisco

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


Confidentiel à Cisco

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

9.4 Balises du 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

10 Acronymes et abréviations

Cette section énumère les acronymes et les abréviations utilisés dans le présent document. Les acronymes et abréviations sont classés par ordre alphabétique avec leur signification.

ACB	Rappel automatique
ACD	Distribution automatique des appels
ACR	Rejet d'appel anonyme
AES	Norme de chiffrement avancée
ALG	Passerelle de la couche d'application
API	Application Programming Interface
APK	Dossier de candidature
APNS (Réseaux d'équipe)	Apple Push Notification Service
ARS	Sélection automatique du débit binaire
AS	Serveur d'applications (Cisco BroadWorks)
MOY	Profil audio visuel
bande passante	BroadWorks
BWA	BroadWorks Anywhere
BWKS	BroadWorks
BWM	BroadWorks Mobility
BOYD	Apportez votre propre périphérique
CC	Centre d'appels
CFB	Renvoi d'appel Occupé
CFNA	Renvoi d'appel Aucune réponse
CFNR	Renvoi d'appel non joignable
CAF	Format intermédiaire commun
CLI	Interface de la ligne de commande
CLID	Identité de la ligne appelante
Base de données CLIDB	Blocage de la transmission de l'ID de la ligne appelante
CRLF	Alimentation de ligne de retour de chariot

Confidentiel à Cisco

CS	Circuit commuté
CSWV	Vue Web des paramètres d'appel
CW	Appel en attente
DB	Base de données
MD	Gestion de l'appareil
DND	Ne pas déranger
DNS	Système de noms de domaine
DPC	Contrôle du téléphone de bureau
DTAF	Fichier d'archive 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
Émulateur connecté	Établissement de la connectivité interactive
iLBC	Codec Internet à faible débit binaire
MI	Messagerie instantanée
MI&P	Messagerie instantanée et Présence
OT	Tests d'interopérabilité
Dst.	Protocole Internet
JID (Id JID)	Identificateur Jabber
H/S	Obligatoire/Facultatif
MNO	Opérateur de réseau mobile
MTU	Unité de transmission maximale
MUC	Chat multi-utilisateurs
indicateur de message (MWI)	Indicateur de message en attente
NAL	Couche d'abstraction réseau
NAPTR	Pointeur d'autorité de nommage

Confidentiel à Cisco

NAT	Traduction d’adresses de réseau
Ott	En haut de la page
AP	Assistant personnel
IAP	P-Asserted-Identity
PEM	P-Early Media
PLI	Indication de perte d'image
PLMN	Réseau mobile sur site public
PN	Notification Push
QCIF	Format intermédiaire commun quart
QDS	Qualité de service
RO	Bureau à distance
RTCP	Protocole de contrôle en temps réel
RTP	Protocole en temps réel
SaaS	Logiciel en tant que service
SAN	Nom alternatif de l'objet
SASL	Authentification simple et couche de sécurité
SAVP	Profil audio et vidéo sécurisé
SBC	Contrôleur de limites de session
SCA	Apparence partagée des appels
SCF	Fonction de continuité de session
SCTP	Protocole de transmission de contrôle de flux
SDP	Protocole de définition de session
Sonnerie PERMANENTE	
Sonnerie RAPIDE	
SIP	Protocole d’initiation de session
RSB (Rapport signal sur bruit)	Rapport signal/bruit
RSB (Rapport signal sur bruit)	Numéro unique
SRTCP	Protocole de contrôle sécurisé en temps réel

Confidentiel à Cisco

SRTP	Protocole de transport sécurisé en temps réel
SSL	Secure Sockets Layer
STUN	Utilitaires de traversée de session pour NAT
SUBQCIF	
TCP	Protocole de contrôle de la transmission
TLS	Sécurité de la couche de transport
TTL	Durée de vie
TOURNER	Traversée à l'aide de NAT Relay
UDP	Protocole de datagramme de l'utilisateur
IU	Interface utilisateur
UMS	Serveur de messagerie (Cisco BroadWorks)
URI	Identifiant uniforme des ressources
UVS	Serveur vidéo (Cisco BroadWorks)
VGA	Tableau de graphiques vidéo
VoIP	Voix sur IP
VVM	Messagerie vocale visuelle
WXT	Webex
XMPP	Protocole extensible de présence et de messagerie
XR	Rapport étendu
Xsp	Plateforme de services étendus
xsi	Interface des services étendus

Confidentiel à Cisco