Webex du Guide de configuration de Cisco BroadWorks

Version 45.4

Version du document 1

Table des matières

1 Résumé des changements 1
1.1 Modifications pour la version 45.4, avril 2025 1
1.2 Modifications apportées à la version 45.3, mars 2025 1
1.3 Modifications pour la version 45.2, février 2025 1
1.4 Modifications pour la version 45.1, janvier 2025 1
1.5 Modifications pour la version 44.12, décembre 2024 1
1.6 Modifications pour la version 44.11, novembre 2024 1
1.7 Modifications pour la version 44.10, octobre 2024 1
1.8 Modifications pour la version 44.9, septembre 2024 2
1.9 Modifications pour la version 44.8, août 2024 2
1.10 Modifications pour la version 44.7, juillet 2024 2
1.11 Modifications pour la version 44.6, juin 2024 2
1.12 Modifications pour la version 44.5, mai 2024 2
1.13 Modifications pour la version 44.4, avril 2024 2
1.14 Modifications pour la version 44.3, mars 2024 2
1.15 Modifications pour la version 44.2, février 2024 3
1.16 Modifications pour la version 44.1, janvier 2024 3
2 Modifications apportées aux fichiers de configuration 4
2.1 Modifications apportées aux fichiers de configuration de la version 45.4 4
2.2 Modifications apportées aux fichiers de configuration pour la version 45.3 4
2.3 Modifications apportées aux fichiers de configuration pour la version 45.2 4
2.4 Mises à jour pour les fichiers de configuration pour la version 45.1 4
2.5 Modifications apportées aux fichiers de configuration de la version 44.12 4
2.6 Modifications apportées aux fichiers de configuration de la version 44.11 4
2.7 Modifications apportées aux fichiers de configuration de la version 44.10 5
2.8 Modifications apportées aux fichiers de configuration de la version 44.9 5
2.9 Modifications apportées aux fichiers de configuration de la version 44.8 5
2.10 Modifications apportées aux fichiers de configuration de la version 44.7 5
2.11 Modifications apportées aux fichiers de configuration de la version 44.6 5
2.12 Modifications apportées aux fichiers de configuration pour la version 44.5 6
2.13 Modifications apportées aux fichiers de configuration pour la version 44.4 6
2.14 Modifications apportées aux fichiers de configuration pour la version 44.3 6
2.15 Modifications apportées aux fichiers de configuration pour la version 44.2 7
2.16 Modifications apportées aux fichiers de configuration pour la version 44.1 9
3 Introduction 10
4 Installation 11
4.1 Téléchargement du client localisé 11
4.2 Android Client 11
4.3 Client iOS 11

Informations confidentielles de Cisco

4.4 Client du bureau 12
5 Gestion des périphériques 13
5.1 Balises de gestion des périphériques 13
5.2 Améliorations de la correspondance partielle pour la sélection du type de périphérique 14
5.3 Client Configuration 15
5.4 Déploiement de config-wxt.xml 15
5.5 Fichier de configuration (config-wxt.xml) 15
5.6 Balises par défaut système 16
5.7 Balises système intégrées dynamiques Cisco BroadWorks 16
6 Balises personnalisées 19
6.1 Fonctionnalités communes 31
6.1.1 Paramètres du serveur SIP 31
6.1.2 SIP Over TLS et protocole de transport en temps réel sécurisé 34
6.1.3 En-têtes SIP 3GPP pour SRTP 37
6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les souvenirs 37
6.1.5 Délai d'expiration configurable pour l'ouverture d'un socket SIP 39
6.1.6 Détection dynamique du proxy SIP 40
6.1.7 Utilisation du port préféré pour SIP 45
6.1.8 Basculement et restauration automatique SIP 46
6.1.9 SIP SUBCSRIBE et REGISTER Actualiser et SUBSCRIBE Réessayer 51
6.1.10 Utiliser des URI associés à P dans REGISTER 51
6.1.11 En-tête SIP P-Early Media (PEM) 52
6.1.12 Prise en charge de SIP UPDATE 53
6.1.13 Ancien SIP INFO FIR 53
6.1.14 Gestion de l'acheminement SIP pour la traversée NAT 54
6.1.15 ID de la session SIP 55
6.1.16 Comportement du rejet de l'appel entrant 55
6.1.17 Plage de ports du protocole de transport en temps réel 55
6.1.18 Prise en charge ICE (Webex Calling uniquement) 56
6.1.19 RTCP MUX 57
6.1.20 Transfert 57
6.1.21 Conférences téléphoniques N-Way et participants 59
6.1.22 Extraction d'appel 60
6.1.23 Parquer/Récupérer un appel 60
6.1.24 Statistiques d'appel 60
6.1.25 Récupération automatique de l'appel / Transfert transparent d'appel 61
6.1.26 Enregistrement d'appel 61
6.1.27 Messagerie vocale, Messagerie vocale visuelle, indicateur de message en attente 63
6.1.28 Transcription des messages vocaux pour Webex Calling 64
6.1.29 Paramètres d'appel 65
6.1.30 Paramètres du portail et des appels Web 67

Informations confidentielles de Cisco

6.1.31 Connexion/déconnexion au centre d'appels / File d'attente d'appels 71
6.1.32 Racine XSI et chemins d'accès 72
6.1.33 Canal d'événements XSI 72
6.1.34 Configuration des codecs 73
6.1.35 Composition SIP-URI 75
6.1.36 Historique des appels sur tous les périphériques 76
6.1.37 Désactivation des appels vidéo 76
6.1.38 Appel d'urgence (911) - Établissement de rapports de localisation avec le fournisseur E911 77
6.1.39 PAI comme identité 78
6.1.40 Désactiver le partage d'écran 79
6.1.41 Indication d'appel de spam 79
6.1.42 Suppression du bruit et extension de bande passante pour les appels PSTN/mobiles 79
6.1.43 Marquage de l'DSCP QoS 80
6.1.44 Profil principal 81
6.1.45 Liste de contacts bloqués (Webex Calling seulement) 82
6.1.46 Mise en œuvre de l'adaptation et de la résilience des médias (MARI) 83
6.1.47 Appels simultanés avec le même utilisateur 85
6.1.48 RTCP-XR 86
6.1.49 Informations sur le renvoi d'appels 87
6.1.50 Afficher l'ID de l'appelant 87
6.1.51 Multiligne 90
6.1.52 Autorisation SIP étendue 91
6.1.53 Assistant personnel (absent) 92
6.2 Fonctionnalités du bureau uniquement 94
6.2.1 Déconnexion forcée 94
6.2.2 Interception d'appel 94
6.2.3 Support Boss-Admin (assistante de direction) 95
6.2.4 Transfert des appels SIP à la réunion (Webex Calling uniquement) 96
6.2.5 Contrôle du téléphone de bureau - Réponse automatique 96
6.2.6 Réponse automatique avec notification par tonalité 97
6.2.7 Contrôle de téléphone de bureau - Contrôles à mi-appel - Conférence 97
6.2.8 Notifications d'interception d'appels 97
6.2.9 Forfait d'événements télécommandés 100
6.2.10 Sélection CLID de l'agent de la file d'attente d'appels 101
6.2.11 Survivability Gateway (Webex Calling seulement) 101
6.2.12 Package d'événements de contrôle à distance du mode silencieux (Webex Calling uniquement) 102
6.2.13 Déplacer l'appel 103
6.3 Fonctionnalités réservées aux appareils mobiles 105
6.3.1 Appel d'urgence 105
6.3.2 Notifications push pour les appels 106

Informations confidentielles de Cisco

6.3.3 Alerte unique 108
6.3.4 Cliquez pour composer (rappel) 109
6.3.5 Prise en charge des ORM 109
6.3.6 ID appelant entrant 115

7 Fonctionnalités Early Field Trial (BETA) 117

8 Correspondance des balises personnalisées entre les Webex pour Cisco BroadWorks et UC-One 118

9 Annexe A : Chiffrements TLS 126

10 Annexe B : Script de mise à disposition des balises DM 127

10.1 Bureau 128
10.2 Mobile 131
10.3 Tablette 133
10.4 Balises système 136

11 Acronymes et abréviations 138

Informations confidentielles de Cisco

1 Résumé des changements

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

1.1 Modifications pour la version 45.4, avril 2025

Cette version du document comprend les modifications suivantes :

- Section déplacée *6.1.34.1 Codec IA* – hors de la version bêta.
- Ajout d'une section *6.1.51 Multiligne* – combinaison des sections Desktop Only et Mobile BETA.
- Section déplacée *6.1.52 Autorisation SIP étendue* – hors de la version bêta.
- Section *6.1.53 Assistant personnel (absent)* déplacée comme d'habitude pour les ordinateurs de bureau et les appareils mobiles

1.2 Modifications apportées à la version 45.3, mars 2025

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

1.3 Modifications pour la version 45.2, février 2025

Cette version du document comprend les modifications suivantes :

- Ajout d'une section *Autorisation SIP étendue**Error! Reference source not found.*** en version bêta.

1.4 Modifications pour la version 45.1, janvier 2025

Cette version du document comprend les modifications suivantes :

- Section déplacée *Assistant personnel (absent)* hors de BETA.
- Section déplacée *6.3.2.3 Mode de livraison (Webex Calling* seulement) hors de BETA.

1.5 Modifications pour la version 44.12, décembre 2024

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

1.6 Modifications pour la version 44.11, novembre 2024

Cette version du document comprend les modifications suivantes :

- Ajout d'une section *Mobile (Webex Calling uniquement)* en version bêta.

1.7 Modifications pour la version 44.10, octobre 2024

Cette version du document comprend les modifications suivantes :

- Ajout d'une section *Assistant personnel (absent)* en version bêta.***Error! Reference source not found.***
- Ajout d'une section *Mode de livraison (Webex Calling* seulement) en version bêta.

Informations confidentielles de Cisco

1.8 Modifications pour la version 44.9, septembre 2024

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

1.9 Modifications pour la version 44.8, août 2024

Cette version du document comprend les modifications suivantes :

- Section mise à jour *6.1.34 Configuration des* codecs – ajout de précisions sur les CGDT et les mécanismes de prestation pris en charge.

1.10 Modifications pour la version 44.7, juillet 2024

Cette version du document comprend les modifications suivantes :

- Ajout d'une section *Codec IA* en version bêta.
- Mise à jour de la section *6.1.44 Profil* principal – suppression des détails sur le comportement de l'application Webex a priori à la version 43.2.

1.11 Modifications pour la version 44.6, juin 2024

Cette version du document comprend les modifications suivantes :

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

1.12 Modifications pour la version 44.5, mai 2024

Cette version du document comprend les modifications suivantes :

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

1.13 Modifications pour la version 44.4, avril 2024

Cette version du document comprend les modifications suivantes :

- Section mise à jour *6.1.50.1 ID appelant sortant*.
- Section mise à jour *Modifications apportées aux fichiers de configuration pour* la version 44.3 – ajout de détails sur les mises à jour keepalive dans la version 44.3.

1.14 Modifications pour la version 44.3, mars 2024

Cette version du document comprend les modifications suivantes :

- Section mise à jour *6.3.6. ID appelant entrant*
    - Déplacé la section *6.1.50.1 ID appelant sortant* comme commun pour les ordinateurs de bureau et les appareils mobiles, et mise à jour avec plus de détails.
- Section mise à jour *6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les* souvenirs – ajout de détails sur les keepalives configurables à l'aide de balises personnalisées.

Informations confidentielles de Cisco

1.15 Modifications pour la version 44.2, février 2024

Cette version du document comprend les modifications suivantes :

- Section ajoutée *6.3.6 ID appelant entrant*
- Section mise à jour *6.2.8 Notifications d'interception d'appels*
  - Ajout d'une sous-section *6.2.8.1 Supervision de ligne* occupée - déplacée BLF les détails.
  - Ajout d'une sous-section *6.2.8.2 Groupe d'interception d'appels (Webex Calling uniquement)*.
- Section ajoutée *6.1.49 Informations sur le* renvoi d'appels.
- Section mise à jour *6.1.8.3 Appliquer IP version* – ajout de détails pour le nouveau *mode nat64* .
- Section Mise à jour *6.1.42 Suppression du bruit et extension de bande passante pour* les appels PSTN/mobiles : ajout de détails sur la prise en charge de la nouvelle extension de bande passante et les mises à jour de suppression du bruit. La section *Améliorations de la parole pour les appels* PSTN est supprimée de BETA.

1.16 Modifications pour la version 44.1, janvier 2024

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

Informations confidentielles de Cisco

2 Modifications apportées aux fichiers de configuration

2.1 Modifications apportées aux fichiers de configuration de la version 45.4

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

2.2 Modifications apportées aux fichiers de configuration pour la version 45.3

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

2.3 Modifications apportées aux fichiers de configuration pour la version 45.2

- [Fonction BETA]
  Ajout de la balise <autorisation étendue> dans la section <protocoles><sip>.

```
<config>
<protocoles>
  <gorgée>
    <autorisation étendue activée="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Le %TAG% suivant a été ajouté :

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.4 Mises à jour pour les fichiers de configuration pour la version 45.1

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

2.5 Modifications apportées aux fichiers de configuration de la version 44.12

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

2.6 Modifications apportées aux fichiers de configuration de la version 44.11

- [Fonction BETA] [Mobile uniquement] [Webex Calling seulement]
  Ajout d'un attribut multiligne activé dans la balise <protocols><sip><lines>.
  Ajout des sections <personnel> et <ligne> pour les lignes secondaires sous la section <protocoles><sip><lignes>.

```
<config>
<Protocols><SIP>
<lignes multilignes-enabled="%ENABLE_MULTI_LINE_WXT%">
   < personnel >
      <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
   </personnel >
   <line lineType="%BW-MEMBERTYPE-1 %">
      …
   </ligne>
   <line lineType="%BW-MEMBERTYPE-2 %">
      …
   </ligne>
   …
   <line lineType="%BW-MEMBERTYPE-10 %">
      …
   </ligne>
</lignes>
```


Informations confidentielles de Cisco

2.7 Modifications apportées aux fichiers de configuration de la version 44.10

- [Fonction BETA]
  Ajout de la balise <assistant-personnel> dans la section <services>.

```
<config>
<services>
   <assistant-personnel activé="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

- [Fonction BETA] [Mobile uniquement] [Webex Calling seulement]
  Ajout de l'attribut delivery-mode sous la balise <services><push-notifications-for-calls>.

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

Les %TAG%s suivants ont été ajoutés :

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.8 Modifications apportées aux fichiers de configuration de la version 44.9

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

2.9 Modifications apportées aux fichiers de configuration de la version 44.8

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

2.10 Modifications apportées aux fichiers de configuration de la version 44.7

- [Fonction BETA]
  Ajout du codec AI (xCodec) dans la section <services><appels><codec><audio>.

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

2.11 Modifications apportées aux fichiers de configuration de la version 44.6

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

Informations confidentielles de Cisco

2.12 Modifications apportées aux fichiers de configuration pour la version 44.5

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

```
<config>
<protocoles><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%"/>
```

- Le tag <nom-distant> a été ajouté dans la section <services><appels><id-appelant> avec <machine> comme sous-tag.

```
<config>
<services><appels>
   <id_appelant>
      <nom_distant>
         <mode machine="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Les %TAG%s suivants ont été ajoutés :

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.13 Modifications apportées aux fichiers de configuration pour la version 44.4

- [Bureau uniquement] [Webex Calling seulement]
  Ajout des balises <numéros supplémentaires>, <groupe-recherche> et <clid-delivery-blocking> sous la section <id-appelant><appels-sortants>.

```
<config>
<services><appels>
  <id_appelant>
    <appels-sortants activés="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <nombres-supplémentaires
activés="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <centre d'appels
activé="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <groupe-recherche
activé="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </appels sortants>
```

2.14 Modifications apportées aux fichiers de configuration pour la version 44.3

- [Bureau uniquement] [Webex Calling seulement]
  Ajout de <appels-sortants> sous la nouvelle section <id-appelant>, avec <centre d'appels> comme sous-tag.

```
<config>
<services><appels>
  <id_appelant>
    <appels-sortants activés="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
```


Informations confidentielles de Cisco

```
      <centre d'appels
activé="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
    </appels sortants>
```

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

```
<config>
<Protocols><SIP>
<transports>
  <udp>
    <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
      …
  </UDP>
  <tcp>
    <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
      …
  </tcp>
  <tls>
    <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
      …
  </tls>
```

Les %TAG%s suivants ont été ajoutés :

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

2.15 Modifications apportées aux fichiers de configuration pour la version 44.2

- [Mobile uniquement]
  Ajout de la section <id-appelant> sous <services><appels>. Ajout des sous-balises <appel entrant> et <appel manqué>, avec la nouvelle sous-balise <numéro additionnel> pour les deux.

```
<config>
<services><appels>
  <id_appelant>
    <Appels entrants>
      <append-number
enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
    </appels entrants>
    <appels en absence>
      <append-number
enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
    </appels manqués>
```

- [Mobile uniquement] [Webex Calling seulement]
  Ajout de la section <appels-sortants> dans la nouvelle section <id-appelant>.

```
<config>
<services><appels>
  <id_appelant>
    <appels-sortants activés="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
```


Informations confidentielles de Cisco

```
      <nombres-supplémentaires
activés="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <centre d'appels
activé="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <groupe-recherche
activé="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </appels sortants>
```

- Ajout du tag <call-forwarding-info> dans la section <services><calls>.

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

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

```
<config>
<services><appels>
  <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>
  <lignes>
    <ligne>
      <interception-appels-groupe>%INTERCEPTION D'APPELS-GROUPE-BOOL-
1 %</interception-appels-groupe>
      ...
    </ligne>
    <ligne>
      <interception d'appels-groupe>%INTERCEPTION D'APPELS-GROUPE-BOOL-
2 %</interception d'appels-groupe>
      ...
    </ligne>
    …
```

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%

Informations confidentielles de Cisco

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

Le %TAG% suivant est déconseillé :

- %ENABLE_NOISE_REMOVAL_WXT%

2.16 Modifications apportées aux fichiers de configuration pour la version 44.1

Il n'y a eu aucune mise à jour dans les fichiers de configuration de cette version.

Informations confidentielles de Cisco

3 Introduction

Ce document a pour objectif de fournir une description de la configuration du client Webex pour Cisco BroadWorks.

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

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

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

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

Informations confidentielles de Cisco

4 Installation

Le Webex pour les clients Cisco BroadWorks peut être installé à partir des éléments suivants :

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

4.1 Téléchargement du client localisé

Les versions localisées suivantes de l'Webex pour les clients Cisco BroadWorks peuvent être téléchargées à l'adresse suivante :

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

4.2 Android Client

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

Il existe un contrôle de version basé sur les procédures 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 utilisateur sont conservées par défaut.

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

4.3 Client iOS

Le client iOS est installé en tant qu'application, qui conserve les données relatives aux paramètres dans son "bac à sable" et les données du fichier de configuration sont stockées cryptées.

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

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

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

Informations confidentielles de Cisco

4.4 Client du bureau

Des informations sur l'installation et le contrôle de version du client de bureau (Windows et MacOS) peuvent être trouvées sur le suivant : https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade.

Informations confidentielles de Cisco

5 Gestion des périphériques

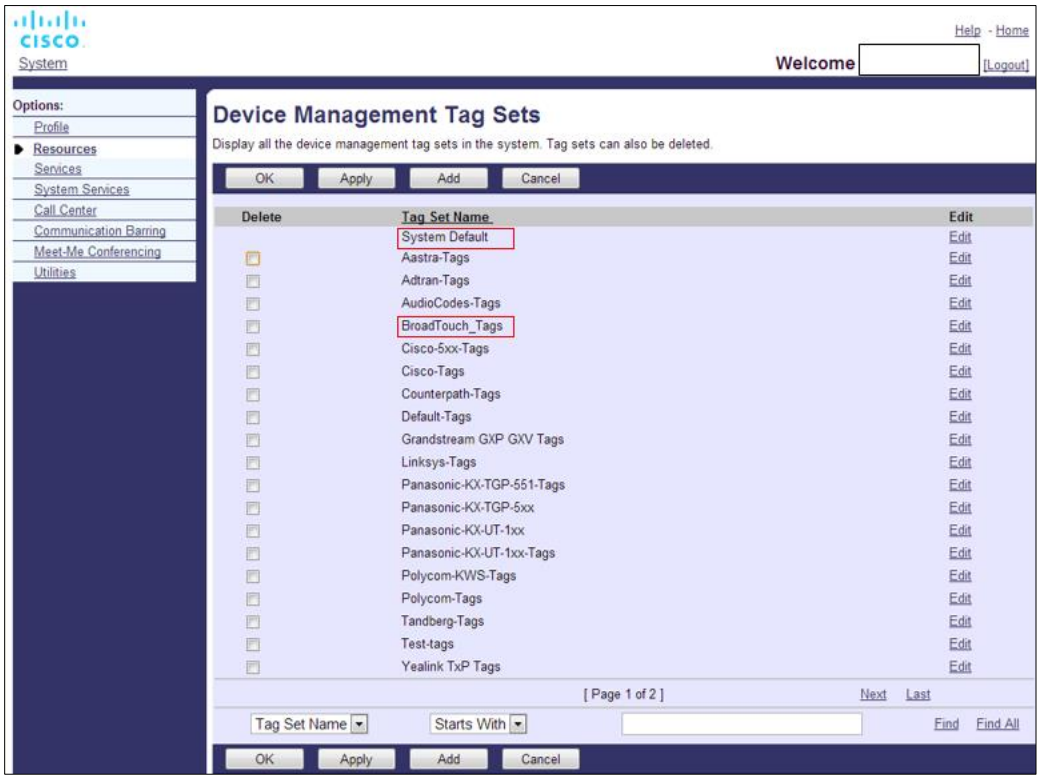
5.1 Balises de gestion des périphériques

Webex pour Cisco BroadWorks utilise le bouton *Ensembles* de balises de gestion des périphériques illustrés dans la figure suivante. Les *jeux de balises* système par défaut et personnalisés sont requis pour configurer des paramètres spécifiques de périphérique/client. Cet ensemble de balises offre une flexibilité dans la gestion des paramètres de connectivité réseau/service du client ainsi que des contrôles d'activation des fonctionnalités.

Cet ensemble de balises personnalisé est configuré par un administrateur système via l'option *System → Resources → Device Management Tag Sets* . L'administrateur doit ajouter de nouveaux jeux de tags :

- Portable : Connect_Tags
- Tablette : ConnectTablet_Tags
- Bureau : BroadTouch_Tags

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



Ensembles 1 de balises Figure Desktop Device Management

Informations confidentielles de Cisco

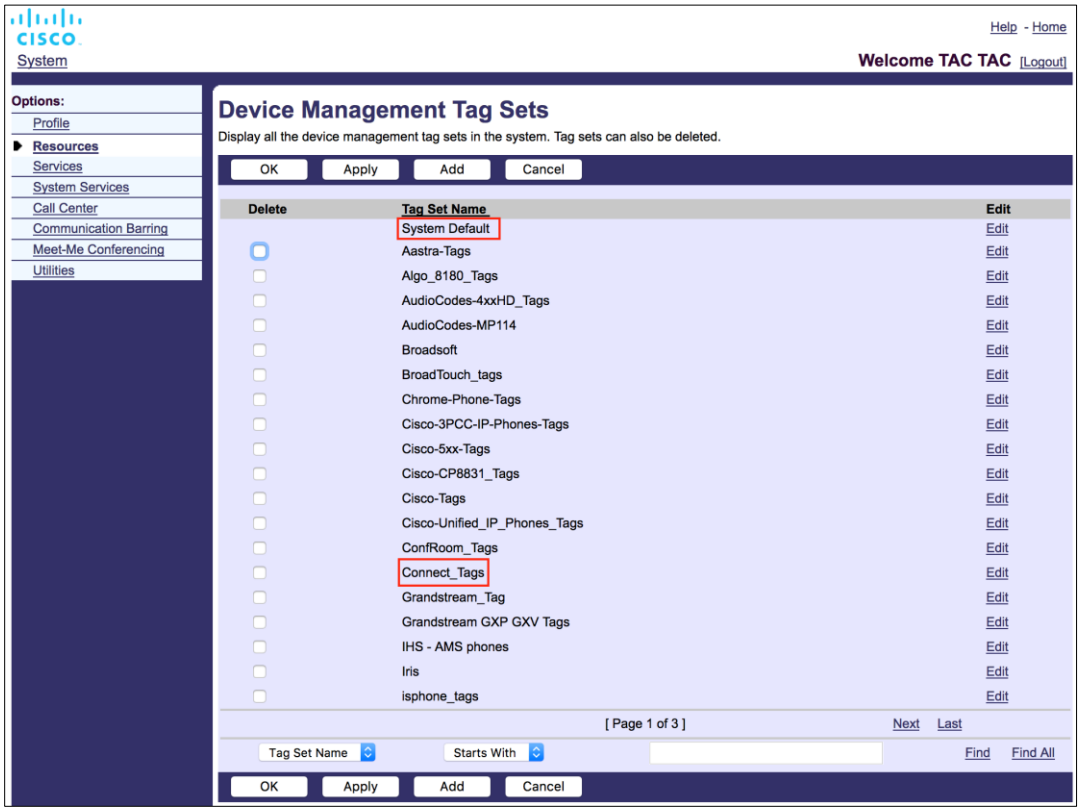


Figure 2 Jeux de balises de gestion des appareils mobiles

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

Pour permettre une flexibilité accrue lors de la sélection des packages de fonctionnalités pour les groupes d'utilisateurs ou les utilisateurs individuels, le type de profil de périphérique est sélectionné en fonction d'une (première) correspondance partielle. Cela permet aux clients d'utiliser différents types 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 est nommé "Business Communicator - PC" pour ordinateur de bureau, "Connect - Mobile" pour mobile et "Connect - Tablet" pour tablette. Un profil de périphérique peut être créé et attribué à l'utilisateur. Le serveur d'applications génère ensuite un fichier de configuration et le stocke sur le serveur de profils.

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

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

Informations confidentielles de Cisco

Par exemple, le fournisseur de services peut avoir un nombre illimité de types de profils d'appareil en fonction des rôles d'utilisateur, tels que "Business Communicator – PC Basic", "Business Communicator – PC Executive" ou "Business Communicator – PC Assistant", et modifier les fonctionnalités disponibles pour les utilisateurs individuels en modifiant le type de profil d'appareil pour eux.

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

5.3 Client Configuration

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

5.4 Déploiement de config-wxt.xml

Ajoutez le fichier de config-wxt.xml *correspondant* aux profils d'appareils "Connect – Mobile", "Connect – Tablet" et "Business Communicator – PC". Webex pour Cisco BroadWorks utilise les mêmes profils de périphériques que UC-One, ce qui facilite le déploiement.

REMARQUE 1 : Un fichier de configuration doit exister pour chaque profil de périphérique.

REMARQUE 2 : Il est HIHGLY RECOMMANDÉ les modèles à maintenir à jour avec la dernière version de l'application Webex

5.5 Fichier de configuration (config-wxt.xml)

De nouvelles balises personnalisées, avec **_WXT** suffixe, sont utilisées pour différencier la nouvelle Webex pour le déploiement de la configuration Cisco BroadWorks des clients hérités. Cependant, certaines balises (système) sont encore partagées entre UC-One et Webex.

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

- %BWNETWORK-CONFERENCE-SIPURI-n%
- %NOMBRE-PORTAIL-BWVOICE-n%
- %BWLINEPORT-n%
- %BWAUTHUSER-n%
- %BWAUTHPASSWORD-n%
- %BWE164-n%
- %BWHOST-n%
- %BWNAME-n%
- %BWEXTENSION-n%

Informations confidentielles de Cisco

- %BWAPPEARANCE-LABEL-n%
- %BWDISPLAYNAMELINEPORT%
- %BWLINEPORT-PRIMAIRE%
- %BWE911-PRIMAIRE-HELDURL%
- %BWE911-IDCLIENT% ;
- %BWE911-CLÉSECRÈTE%
- %BWE911-LISTE-DES-NUMÉROS-D'URGENCE%
- %BW-MEMBERTYPE-N%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (Webex Calling uniquement)

5.6 Balises par défaut système

En tant qu'administrateur système, vous pouvez accéder aux balises par défaut système via l'option *System → Resources → Device Management Tag Sets* . Les balises par défaut système suivantes doivent être configurées lorsque le package d'appel VoIP est installé.

Étiquette	Description
%SBC_ADDRESS_WXT%	Elle doit être configurée en tant que nom de domaine complet (FQDN) ou adresse IP du contrôleur de limites de session (SBC) déployé sur le réseau. Exemple : sbc.yourdomain.com
%SBC_PORT_WXT%	Si le SBC_ADDRESS_WXT est une adresse IP, ce paramètre doit être défini sur le port SBC. Si le SBC_ADDRESS_WXT est un nom de domaine complet, il peut être laissé non défini. Exemple : 5075

5.7 Balises système intégrées dynamiques Cisco BroadWorks

Outre les balises système par défaut et les balises personnalisées qui doivent être définies, il existe des balises système Cisco BroadWorks qui sont généralement utilisées et qui font partie du fichier d'archive de type de périphérique (DTAF) recommandé. Ces balises sont répertoriées dans cette section. Selon le package de solution installé, toutes les balises système ne sont pas utilisées.

Étiquette	Description
%BWNETWORK-CONFERENCE-SIPURI-n%	Il s'agit du serveur URI utilisé pour activer la conférence N-Way.
%NOMBRE-PORTAIL-BWVOICE-n%	Ce numéro est utilisé pour la messagerie vocale. Le client compose ce numéro lors de la récupération du message vocal.

Informations confidentielles de Cisco

Étiquette	Description
%BWLINEPORT-n%	Nom d'utilisateur SIP utilisé pour la signalisation SIP, par exemple lors de l'enregistrement.
%BWHOST-n%	Il s'agit de la partie domaine du port de ligne approvisionné pour le périphérique affecté à l'utilisateur. Il est récupéré à partir du profil de l'utilisateur. Généralement utilisé comme domaine SIP.
%BWAUTHUSER-n%	Il s'agit du nom d'utilisateur de l'authentification. Si l'authentification a été attribuée à l'abonné, il s'agit de l'ID utilisateur fourni sur la page Authentification, quel que soit le mode d'authentification sélectionné pour le type de périphérique. Le nom d'utilisateur SIP, généralement utilisé dans les signaux 401 et 407. Peut être différent du nom d'utilisateur SIP par défaut.
%BWAUTHPASSWORD-n%	Il s'agit du mot de passe d'authentification de l'utilisateur. Si l'authentification a été attribuée à l'abonné, il s'agit du mot de passe mis à disposition sur la page Authentification, quelle que soit la valeur du 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 l'abonné dans le profil de l'utilisateur. Le prénom et le nom sont concaténés. En cas de configuration sur plusieurs lignes, si aucun libellé de ligne n'est défini et s'il n'est pas vide, utilisé comme nom d'affichage de la ligne dans le sélecteur de ligne.
%BWEXTENSION-n%	Le poste de l'abonné est extrait du poste configuré dans le profil de l'utilisateur. Si aucun numéro de poste n'a été déployé, la balise est remplacée par le numéro de téléphone de l'abonné.
%BWAPPEARANCE-LABEL-n%	Il s'agit du libellé de ligne configuré. 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 configuré sur le périphérique affecté à l'utilisateur. Il est récupéré à partir du profil de l'utilisateur. Permet d'identifier la ligne principale de l'utilisateur.
%BWLINEPORT-PRIMAIRE%	Le port de ligne principale est configuré sur le périphérique affecté à l'utilisateur. Cette balise n'inclut pas la partie domaine du port de ligne approvisionné. Il est récupéré à partir du profil de l'utilisateur.

Informations confidentielles de Cisco

Étiquette	Description
%BWE911-PRIMAIRE-HELDURL%	Spécifie l'URL de la plate-forme de localisation d'urgence RedSky prenant en charge le protocole HELD.
%BWE911-IDCLIENT% ;	L'ID client (HeldOrgId, CompanyID) utilisé pour la demande HTTPS RedSky.
%BWE911-CLÉSECRÈTE%	Le secret pour authentifier la requête HTTPS RedSky.
%BWE911-LISTE-DES-NUMÉROS-D'URGENCE%	La liste des numéros d'urgence pris en charge par RedSky. Pour utiliser cette balise, la balise personnalisée réservée %RESERVEDBW911-EMERGENCY-NUMBER-LIST% doit être ajoutée au jeu 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. **REMARQUE :** le client Webex ne prend pas en charge les caractères génériques dans les numéros d'urgence ; par conséquent, seuls les numéros d'urgence exacts doivent être ajoutés à la balise personnalisée "réservé". L'exemple suivant montre comment la fonctionnalité de balise réservée est censée être utilisée : 1) La balise native %BWE911-EMERGENCY-NUMBER-LIST% est ajoutée au fichier de modèle du périphérique 2) La balise personnalisée réservée %RESERVEDBW911-EMERGENCY-NUMBER-LIST% est ajoutée au jeu 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%	Type de chaque ligne. Il peut s'agir de "Profil virtuel", "Utilisateur" ou "Lieu".
%BWUSEREXTID-n%	ID externe de la ligne donnée (Webex Calling uniquement)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Indique si un groupe d'interception d'appels est configuré pour la ligne correspondante. (Webex appel seulement)

Informations confidentielles de 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 plates-formes de bureau et mobiles / tablettes.

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

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_REJECT_WITH_486_WXT%	O	O	Vrai	*6.1.16 Comportement du rejet de* l'appel entrant
%REJECT_WITH_XSI_MODE_WXT %	N	O	decline_false	*6.3.2 Notifications push pour les* appels
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	O	occupé	*6.3.2 Notifications push pour les* appels
%ENABLE_TRANSFER_CALLS_WXT%	O	O	false	*6.1.20 Transfert*
%ENABLE_CONFERENCE_CALLS_WXT%	O	O	false	*6.1.21 Conférences téléphoniques N-Way et participants*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	O	O	false	*6.1.21 Conférences téléphoniques N-Way et participants*
%MAX_CONF_PARTIES_WXT%	O	O	10	*6.1.21 Conférences téléphoniques N-Way et participants*
%ENABLE_CALL_STATISTICS_WXT%	O	O	false	*6.1.24 Statistiques d'appel*
%ENABLE_CALL_PULL_WXT%	O	O	false	*6.1.22 Extraction d'appel*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	O	false	*6.3.2 Notifications push pour les* appels
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	O	O	false	*6.1.28 Transcription des messages vocaux pour* Webex Calling
%ENABLE_MWI_WXT%	O	O	false	*6.1.27 Messagerie vocale, Messagerie vocale visuelle, indicateur* de message en attente
%MWI_MODE_WXT %	O	O	vide	*6.1.27 Messagerie vocale, Messagerie vocale visuelle, indicateur* de message en attente

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_VOICE_MAIL_WXT%	O	O	false	*6.1.27 Messagerie vocale, Messagerie vocale visuelle, indicateur* de message en attente
%ENABLE_VISUAL_VOICE_MAIL_WXT%	O	O	false	*6.1.27 Messagerie vocale, Messagerie vocale visuelle, indicateur* de message en attente
%ENABLE_FORCED_LOGOUT_WXT%	O	N	false	*6.2.1 Déconnexion* forcée
%FORCED_LOGOUT_APPID_WXT%	O	N	vide	*6.2.1 Déconnexion* forcée
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	O	O	false	*6.1.29.1 Renvoi de tous* les appels
%ENABLE_BROADWORKS_ANYWHERE_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	O	O	Vrai	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	O	O	false	*6.1.29.3 BroadWorks Anywhere*

Informations confidentielles de Cisco

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

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	O (Windows uniquement)	N	false	*6.1.6 Détection dynamique du proxy* SIP
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	O	O	5000	*6.1.5 Délai d'expiration configurable pour l'ouverture d'un* socket SIP
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	O	O	10000	*6.1.5 Délai d'expiration configurable pour l'ouverture d'un* socket SIP
%SOURCE_PORT_WXT%	O	O	5060	*6.1.7 Utilisation du port préféré* pour SIP
%SIP_FAILBACK_ENABLED_WXT%	O	N	Vrai	*6.1.8.2 Restauration automatique* SIP
%SIP_FAILBACK_TIMEOUT_WXT%	O	N	900	*6.1.8.2 Restauration automatique* SIP
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	O	N	false	*6.1.8.2 Restauration automatique* SIP
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	O	O	Dns	*6.1.8.3. Appliquer IP version*
%USE_ALTERNATIVE_IDENTITIES_WXT%	O	O	false	*6.1.10 Utiliser des URI associés* à P dans REGISTER
%TCP_SIZE_THRESHOLD_WXT%	O	O	18000	*6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les* souvenirs
%SIP_REFRESH_ON_TTL_WXT%	O	N	false	*6.1.8.4 Gestion DNS TTL*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	O	O	false	*6.1.12 Prise en charge* de SIP UPDATE
%ENABLE_PEM_SUPPORT_WXT%	O	O	false	*6.1.11 En-tête SIP P-Early Media (PEM)*
%ENABLE_SIP_SESSION_ID_WXT%	O	O	false	*6.1.15 ID de la* session SIP
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	O	O	false	*6.1.13 Ancien SIP INFO FIR*
%SRTP_ENABLED_WXT%	O	O	false	*6.1.2 SIP Over TLS et protocole de transport en* temps réel sécurisé

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%SRTP_MODE_WXT%	O	O	false	*6.1.2 SIP Over TLS et protocole de transport en* temps réel sécurisé
%ENABLE_REKEYING_WXT%	O	O	Vrai	*6.1.2 SIP Over TLS et protocole de transport en* temps réel sécurisé
%RTP_AUDIO_PORT_RANGE_START_WXT%	O	O	8000	*6.1.17 Plage de ports du protocole* de transport en temps réel
%RTP_AUDIO_PORT_RANGE_END_WXT%	O	O	8099	*6.1.17 Plage de ports du protocole* de transport en temps réel
%RTP_VIDEO_PORT_RANGE_START_WXT%	O	O	8100	*6.1.17 Plage de ports du protocole* de transport en temps réel
%RTP_VIDEO_PORT_RANGE_END_WXT%	O	O	8199	*6.1.17 Plage de ports du protocole* de transport en temps réel
%ENABLE_RTCP_MUX_WXT%	O	O	Vrai	*6.1.19 RTCP MUX*
%ENABLE_XSI_EVENT_CHANNEL_WXT%	O	O	Vrai	*6.1.33 Canal d'événements XSI*
%CHANNEL_HEARTBEAT_WXT%	O	O	10000	*6.1.33 Canal d'événements XSI*
%XSI_ROOT_WXT%	O	O	vide (utilise l'URL d'origine)	*6.1.32 Racine XSI et chemins* d'accès
%XSI_ACTIONS_PATH_WXT%	O	O	/com.broadsoft.xsi-actions/	*6.1.32 Racine XSI et chemins* d'accès
%XSI_EVENTS_PATH_WXT%	O	O	/com.broadsoft.xsi-events/	*6.1.32 Racine XSI et chemins* d'accès
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	O	O	false	*6.1.25 Récupération automatique de l'appel / Transfert transparent* d'appel
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	O	CS uniquement	*6.3.1 Appel d'urgence*
%ENABLE_CALL_PICKUP_BLIND_WXT%	O	N	false	*6.2.2 Interception d'appel*

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	O	N	false	*6.2.2 Interception d'appel*
%WEB_CALL_SETTINGS_URL_WXT%	O	O	vide	*6.1.30 Paramètres du portail et des appels* Web
%USER_PORTAL_SETTINGS_URL_WXT%	O	O	vide	*6.1.30 Paramètres du portail et des appels* Web
%ENABLE_CALL_CENTER_WXT%	O	O	false	*6.1.31 Connexion/déconnexion au centre d'appels / File* d'attente d'appels
%WEB_CALL_SETTINGS_TARGET_WXT%	O	O	externe	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	O	O	Vrai	*6.1.30 Paramètres du portail et des appels* Web
%USE_MEDIASEC_WXT%	O	O	false	*6.1.3 En-têtes SIP 3GPP pour SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	O	false	*6.3.4 Cliquez pour composer (rappel)*
%DIALING_CALL_BACK_TIMER_WXT%	N	O	10	*6.3.4 Cliquez pour composer (rappel)*
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	O	N	false	*6.2.3 Support Boss-Admin (assistante* de direction)
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	O	35	*6.3.2 Notifications push pour les* appels
%ENABLE_CALL_RECORDING_WXT%	O	O	false	*6.1.26 Enregistrement d'appel*
%ENABLE_SINGLE_ALERTING_WXT%	N	O	false	*6.3.3 Alerte unique*
%ENABLE_CALL_PARK_WXT%	O	O	false	*6.1.23 Parquer/Récupérer un* appel
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	O	O	10	*6.1.23 Parquer/Récupérer un* appel

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_RTP_ICE_WXT%	O	O	false	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%RTP_ICE_MODE_WXT%	O	O	icestun	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%RTP_ICE_SERVICE_URI_WXT%	O	O	vide	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%RTP_ICE_PORT_WXT%	O	O	3478	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%ENABLE_RTP_ICE_IPV6_WXT%	O	O	faux	*6.1.18 Prise en charge ICE (Webex* Calling uniquement)
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	O	N	false	*6.1.8.4 Gestion DNS TTL*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	O	N	false	*6.2.4 Transfert des appels SIP à* la réunion
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	O	N	false	*6.2.5 Contrôle du téléphone de bureau - Réponse* automatique
%ENABLE_DIALING_VOIP_WXT%	N	O	Vrai	*6.3.5 Prise en* charge des ORM *Appel avec numéroteur natif*
%ENABLE_DIALING_NATIVE_WXT%	N	O	false	*6.3.5 Prise en* charge des ORM *Appel avec numéroteur natif*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	O	O	Vrai	*6.1.35 Composition SIP-URI*
%ENABLE_SIP_VIDEOCALLS_WXT%	O	O	Vrai	*6.1.37 Désactivation des appels* vidéo
%ENABLE_LOCUS_VIDEOCALLS_WXT%	O	O	Vrai	*6.1.37 Désactivation des appels* vidéo
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	O	O	Ordinateur de bureau - true Mobile, Tablette - faux	*6.1.37 Désactivation des appels* vidéo

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	O	O	false	*6.1.38 Appel d'urgence (911) - Établissement de rapports de localisation* avec le fournisseur E911
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	O	O	0	*6.1.38 Appel d'urgence (911) - Établissement de rapports de localisation* avec le fournisseur E911
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	O	O	-1	*6.1.38 Appel d'urgence (911) - Établissement de rapports de localisation* avec le fournisseur E911
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	O	O	once_per_login	*6.1.38 Appel d'urgence (911) - Établissement de rapports de localisation* avec le fournisseur E911
%ENABLE_AUTO_ANSWER_WXT%	O	N	false	*6.2.6 Réponse automatique avec notification par* tonalité
%ENABLE_CALLS_SPAM_INDICATION_WXT%	O	O	false	*6.1.41 Indication d'appel de* spam
%ENABLE_NOISE_REMOVAL_WXT%	O	O	false	*6.1.42 Suppression du bruit et extension de bande passante pour* les appels PSTN/mobiles
%ENABLE_AUDIO_MARI_FEC_WXT%	O	O	false	*6.1.46.2 Correction d'erreurs de renvoi (FEC) et RTX (Packets* Retransmission)
%ENABLE_AUDIO_MARI_RTX_WXT%	O	O	false	*6.1.46.2 Correction d'erreurs de renvoi (FEC) et RTX (Packets* Retransmission)
%ENABLE_VIDEO_MARI_FEC_WXT%	O	O	false	*6.1.46.2 Correction d'erreurs de renvoi (FEC) et RTX (Packets* Retransmission)
%ENABLE_VIDEO_MARI_RTX_WXT%	O	O	false	*6.1.46.2 Correction d'erreurs de renvoi (FEC) et RTX (Packets* Retransmission)
%ENABLE_CALL_BLOCK_WXT%	O	O	false	*6.1.45 Liste de contacts bloqués (Webex* Calling seulement)
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	O	Vrai	*6.3.5.6 Mobilité MNO - Widget d'appel*
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	O	Vrai	*6.3.5.6 Mobilité MNO - Widget d'appel*

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	O	Vrai	*6.3.5.6 Mobilité MNO - Widget d'appel*
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	O	O	false	*6.1.47 Appels simultanés avec le même* utilisateur
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	O	N	false	*6.2.12 Package d'événements de contrôle à distance du mode silencieux* (Webex Calling uniquement)
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	O	O	Vrai	*6.1.29.2 Renvoi d'appels vers la* messagerie vocale
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	O	O	Vrai	*6.1.8.1 Basculement SIP*
%ENABLE_CALL_MOVE_HERE_WXT%	O	N	false	*6.2.13 Déplacer l'appel*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	O	O	false	*6.1.42 Suppression du bruit et extension de bande passante pour* les appels PSTN/mobiles
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	O	vide	*6.3.5.1 Appel avec numéroteur natif*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	O	O	false	*6.1.20 Transfert*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	O	O	Vrai	*6.1.48 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	O	false	*6.3.6 ID appelant entrant*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	O	false	*6.3.6 ID appelant entrant*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	O	false	*6.1.50 Afficher l'ID* de l'appelant *ID appelant sortant*

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	O	false	*6.1.50 Afficher l'ID* de l'appelant *ID appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	O	false	*6.1.50 Afficher l'ID* de l'appelant *ID appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	O	false	*6.1.50 Afficher l'ID* de l'appelant *ID appelant sortant*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	O	false	*6.1.50 Afficher l'ID* de l'appelant *ID appelant sortant*
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	O	O	false	*6.1.49 Informations sur le* renvoi d'appels
%ENABLE_BUSY_LAMP_FIELD_WXT%	O	N	false	*6.2.8.1 Supervision de ligne* occupée
%ENABLE_BLF_DISPLAY_CALLER_WXT%	O	N	Vrai	*6.2.8.1 Supervision de ligne* occupée
%BLF_NOTIFICATION_DELAY_TIME_WXT%	O	N	0	*6.2.8.1 Supervision de ligne* occupée
%ENABLE_GCP_NOTIFICATIONS_WXT%	O	N	false	*6.2.8.2 Groupe d'interception d'appels (Webex Calling uniquement)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	O	N	false	*6.2.8.2 Groupe d'interception d'appels (Webex Calling uniquement)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	O	N	120	*6.2.8.2 Groupe d'interception d'appels (Webex Calling uniquement)*
%UDP_KEEPALIVE_ENABLED_WXT%	O	O	Vrai	*6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les* souvenirs
%TCP_KEEPALIVE_ENABLED_WXT%	O	O	false	*6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les* souvenirs
%TLS_KEEPALIVE_ENABLED_WXT%	O	O	false	*6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les* souvenirs
%ENABLE_MULTI_LINE_WXT%	O	O	false	*6.1.51 Multiligne*

Informations confidentielles de Cisco

Étiquette	Utilisé dans le bureau	Utilisé dans mobile/tablette	Valeur par défaut	Section
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	O	false	*6.2.4 Transfert des appels SIP à la réunion (Webex Calling)*
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	N	O	false	*6.3.5.3 Identité de la ligne appelante sortante (CLID)* – Dual Persona
%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%	N	O	false	*6.3.5.3 Identité de la ligne appelante sortante (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	O	O	résolu	*6.1.50.2 Nom de l'ID de* l'appelant distant
%PERSONAL_ASSISTANT_ENABLED_WXT%	O	O	false	*6.1.53 Assistant personnel (absent)**Error! Reference source not found.***
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	O	NPS	***Error! Reference source not found.*** *Mode de livraison (Webex Calling* seulement)
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	O	O	false	*6.1.52* ***Error! Reference source not found.****.*

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

Informations confidentielles de Cisco

6.1 Fonctionnalités communes

6.1.1 Paramètres du serveur SIP

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

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

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

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

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

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

La configuration des serveurs SIP suit le schéma de base suivant :

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

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

```
<config>
<protocoles>
<gorgée>
   < minuteries>
      <T1>500</T1>
      <T2>4000</T2>
```


Informations confidentielles de Cisco

```
        <T4>5000</T4>
    </minuteries>
```

- T1 – la durée, en millisecondes, d'un délai aller-retour réseau.
- T2 – temps maximum, en millisecondes, avant la retransmission des requêtes non-INVITE et des réponses d'invitation.
- T4 – la durée maximale, en millisecondes, pendant laquelle un message reste dans le réseau.

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

L'exemple et le tableau ci-dessous fournissent des informations sur les balises DM les plus courantes utilisées pour la configuration SIP.

```
<config>
<Protocols><SIP>
<lignes multilignes-enabled="%ENABLE_MULTI_LINE_WXT%">
       <ligne>
              <label>%BWAPPEARANCE-LABEL-1 %</label>
              <nom>%BWNAME-1 %</nom>
              <numéro de téléphone>%BWE164-1 %</numéro_de-téléphone>
              <extension>%BWEXTENSION-1 %</extension>
              <id-externe>%BWUSEREXTID-1 %</id-externe>
              <numéro-messagerie vocale>%BWNUMÉRO-PORTAIL-VOCAL-1 %</numéro-
messagerie-vocale>
              <URI-service-conférence>sip :%BWNETWORK-CONFERENCE-SIPURI-
1 %</service-conférence-URI>
              <domaine>%BWHOST-1 %</domaine>
              <informations d'identification>
                     <nom_utilisateur>%BWLINEPORT-1 %</nom_utilisateur>
                     <mot de passe>%BWAUTHPASSWORD-1 %</password>
                     <auth>
                            <auth401>
                                   <par défaut>
                                          <nom_utilisateur>%BWAUTHUSER-
1 %</nom_utilisateur>
                                          <mot de passe>%BWAUTHPASSWORD-
1 %</password>
                                   </par défaut>
                                   <realm id="%BWHOST-1 %">
                                          <nom_utilisateur>%BWAUTHUSER-
1 %</nom_utilisateur>
                                          <mot de passe>%BWAUTHPASSWORD-
1 %</password>
                                   </royaume>
                            </auth401>
                            <auth407>
                                   <par défaut>
                                          <nom_utilisateur>%BWAUTHUSER-
1 %</nom_utilisateur>
                                          <mot de passe>%BWAUTHPASSWORD-
1 %</password>
                                   </par défaut>
                                   <realm id="%BWHOST-1 %">
```


Informations confidentielles de Cisco

```
                                        <nom_utilisateur>%BWAUTHUSER-
1 %</nom_utilisateur>
                                        <mot de passe>%BWAUTHPASSWORD-
1 %</password>
                                  </royaume>
                            </auth407>
                      </auth>
               </informations d'identification>
       </ligne>
       …
</lignes>
<adresse proxy="%SBC_ADDRESS_WXT% » port="%SBC_PORT_WXT% » />
<Port préféré>%SOURCE_PORT_WXT%</Port préféré>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%BWLINEPORT-n%	vide	chaîne	Nom d'utilisateur généralement SIP. Pour plus d'informations, reportez-vous à la section *5.7 Balises système intégrées dynamiques Cisco BroadWorks*. Exemple : jeandurant
%BWAUTHPASSWORD-n%	vide	chaîne	Généralement un mot de passe SIP. Pour plus d'informations, reportez-vous à la section *5.7 Balises système intégrées dynamiques Cisco BroadWorks*. Exemple : secretpassword
%BWE164-n%	vide	Numéro de téléphone	Numéro de téléphone par défaut de l'utilisateur au format international. Pour plus d'informations, reportez-vous à la section *5.7 Balises système intégrées dynamiques Cisco BroadWorks*. Exemple : 12345678
%SBC_ADDRESS_WXT%	vide	chaîne	Pour plus d'informations, reportez-vous à la section *5.6 Balises par défaut* système. Exemple : sbcexample.domain.com
%SBC_PORT_WXT%	5060	nombre	Pour plus d'informations, reportez-vous à la section *5.6 Balises par défaut* système. Exemple : 5060
%BWHOST-n%	vide	chaîne	Généralement utilisé comme domaine SIP. Pour plus d'informations, reportez-vous à la section *5.7 Balises système intégrées dynamiques Cisco BroadWorks*. Exemple : exampledomain.com
%SOURCE_PORT_WXT%	5060	nombre	Généralement utilisé pour le *paramètre de port* préféré. Pour plus d'informations, reportez-vous à la section *6.1.7 Utilisation du port préféré* pour SIP. Exemple : 5061

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%BWUSEREXTID-n%	vide	chaîne	(Webex Calling uniquement) Contient l'ID externe de la ligne Pour plus d'informations, vérifiez *6.1.51 Multiligne*. Exemple : 30f69bf7-710b-4cd0-ab4b-35ab393a1709

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

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

Le client peut être configuré pour utiliser le signalement SIP sur TLS et le protocole de transport en temps réel sécurisé (SRTP) pour le chiffrement multimédia. Toutefois, ces fonctionnalités doivent être activées dans la configuration comme indiqué dans l'exemple suivant. Notez également que lorsque la détection de proxy SIP dynamique est utilisée, DNS priorités SRV remplacent les paramètres statiques tels que celui-ci (% USE_TLS_WXT %), et le transport non-TLS est utilisé s'il a une priorité plus élevée dans DNS SRV. Pour plus d'informations sur la détection dynamique du proxy SIP, reportez-vous à la section *6.1.6 Détection dynamique du proxy* SIP.

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

Pour plus d'informations sur les recommandations relatives aux ports SIP et aux protocoles de transport lorsque des ALG SIP sont utilisés dans le réseau, reportez-vous au *guide Webex pour Cisco BroadWorks Solution Guide*.

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 utilisé de telle sorte qu'il soit déjà présent, par défaut, sur les appareils. Il est également possible d'ajouter des certificats localement sur la machine de bureau, manuellement ou en utilisant la mise à disposition en masse, bien que cela ne soit généralement pas le cas.

Pour activer les SRTP associées pour le chiffrement multimédia, il existe un paramètre distinct.

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

Pour les chiffrements SIP/TLS, reportez-vous à *Annexe A : Chiffrements TLS.*

Le SRTP est utilisé pour assurer la sécurité du flux de médias sous trois aspects différents :

- Confidentialité (les données sont cryptées)
- Authentification (assurance de l'identité de l'autre ou des autres parties)

Informations confidentielles de Cisco

- Intégrité (mesures contre, par exemple, les attaques par relecture)

La version actuelle de l'infrastructure multimédia prend en charge le mode compteur AES 128 pour la protection et le code 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 est de 14 octets.

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

SRTP pouvez être activé en utilisant la configuration présentée dans l'exemple suivant. L'implémentation actuelle utilise uniquement le profil SDP Secure RTP et prend en charge les SDP multilignes pour les entrées AVP (Audio Visual Profile) et SAVP (Secure Audio Visual Profile). L'implémentation du SRTP a été testée avec succès dans sa configuration de déploiement habituelle avec différents SBC. Les tests d'interopérabilité (IOT) avec les terminaux qui prennent uniquement en charge le chiffrement à l'aide du profil AVP ne sont pas pris en charge.

Les procédures SDP multilignes liées à SRTP sont implémentées, de sorte que plusieurs lignes m sont toujours utilisées. Des lignes m distinctes pour AVP et SAVP sont utilisées.

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

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

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

- Obligatoire – Lors de la configuration de l'appel, le SDP initial inclut uniquement la ligne M SAVP lors de l'offre et le client n'accepte que la ligne M SAVP dans le SDP lorsqu'il répond, donc seuls SRTP appels sont possibles.
- Préféré – Lors de la configuration des appels, le SDP initial inclut à la fois les lignes M AVP et SARP, mais SAVP arrive en premier lors de l'offre, ce qui indique l'ordre de préférence. Lors de la réponse, le client sélectionne SAVP si disponible même s'il ne s'agit pas de la première ligne m (selon les spécifications SIP, l'ordre des lignes m n'est pas modifié lors de la réponse).
- Facultatif – Lors de la configuration des appels, le SDP initial inclut à la fois les lignes M SAVP et AVP lors de l'offre, mais AVP indique d'abord l'ordre de préférence. Lors de la réponse, le client sélectionne la première ligne m, AVP ou SAVP.
- SRTP’est pas activé – Il n'y a pas de ligne M SAVP dans le SDP initial lors de l'offre. En cas de réponse, le SAVP n'est pas accepté, par conséquent, seuls RTP appels sont possibles.

Informations confidentielles de Cisco

- Transport – Sélectionnez automatiquement le mode SRTP en fonction du protocole de transport. Si TLS est utilisé, le mode de SRTP obligatoire est activé. Si TCP ou UDP est utilisé, aucun SRTP n'est utilisé.

SRTP par rapport à 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>
< sécurisé > %USE_TLS_WXT %</sécurisé>
```

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

Le protocole SRTCP (Secure Real-Time Control Protocol) est également utilisé s SRTP est activé.

Dans certains déploiements, la nouvelle saisie d'informations SRTP n'est pas prise en charge. Par conséquent, il existe un paramètre de configuration pour activer/désactiver SRTP ressaisir. Cependant, les nouvelles clés sont toujours mises en service lorsqu'elles sont reçues dans un SDP mis à jour conformément à la norme rfc3264. La configurabilité concerne uniquement l'envoi de nouvelles clés.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%USE_TLS_WXT%	false	vrai, faux	Lorsque la valeur "false" est activée, l TLS SIP est désactivée. Lorsque la valeur true est activée, l'TLS SIP est activée. Veuillez noter que s'il *6.1.6 Détection dynamique du proxy* SIP est utilisé, ce paramètre est ignoré.
%SRTP_ENABLED_ WXT%	false	vrai, faux	Lorsque la valeur "false" est désactivée, SRTP est désactivée. Lorsque ce paramètre est défini sur "true", SRTP est activé.
%SRTP_MODE_ WXT%	optionnel	obligatoire, préféré, facultatif, transport	Permet de définir le degré de préférence des SRTP lors de la configuration d'appel. La valeur par défaut est "facultatif".
%ENABLE_REKEYI NG_WXT%	Vrai	vrai, faux	Permet d'activer la ressaisie SIP (SDP) pour les SRTP.

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

Informations confidentielles de Cisco

6.1.3 En-têtes SIP 3GPP pour SRTP

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

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

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

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

```
<config>
<Protocols><SIP>
<use-mediasec enabled="%USE_MEDIASEC_WXT%"/>
```

La balise suivante contrôle cette fonctionnalité.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%USE_MEDIASEC_WXT%	faux	Vrai, faux	Active les en-têtes SIP 3GPP pour la négociation SRTP.

6.1.4 Forcez TCP, TLS ou UDP l'utilisation et les souvenirs

L'Webex du client Cisco BroadWorks peut être configuré pour utiliser à la fois TCP, TLS ou UDP pour la signalisation SIP et les supports RTP. Notez que la valeur par défaut du client est TCP. Notez également que sans TCP keepalive, les connexions SIP TCP 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 contrôle si le client utilise TCP ou UDP.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge (octets)	Description
%TCP_SIZE_THRESHOLD_WXT%	0	0	Force TCP à utiliser. La décision d'utiliser TCP ou UDP pour le client appartient au fournisseur de services ; cependant, la recommandation est d'utiliser TCP avec la valeur par défaut "0".

Informations confidentielles de Cisco

	0	1 - 99,000	Force l'UDP à être utilisé lorsque la taille du message est inférieure à la valeur spécifiée ici. Par défaut, cette valeur 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 UDP être utilisée.

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

```
<config>
<Protocols><SIP>
<transports>
        …
        <udp>
                <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
                        <délai d'attente >20</délai d'attente>
                        <charge utile>crlf</charge utile>
                </keepalive>
        </UDP>
        <tcp>
                <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
                        <délai d'attente>0</délai d'attente>
                        <charge utile></charge utile>
                </keepalive>
        </tcp>
        <tls>
                <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
                        <délai d'attente>0</délai d'attente>
                        <charge utile></charge utile>
                </keepalive>
        </tls>
</transports>
```

Les paramètres possibles sont les suivants :

- En activant TCP ou TLS keepalive, valeurs possibles - true/false, la valeur par défaut est "false" si le nœud est manquant. Notez que lorsque cette fonctionnalité est activée, TCP keepalives sont envoyés même si UDP transport est utilisé pour SIP.
- Activation de UDP keepalive, valeurs possibles - true/false, la valeur par défaut est "true" si le nœud est manquant. Notez que lorsque cette fonctionnalité est activée, UDP keepalives sont envoyés même si TCP transport est utilisé pour SIP. En outre, même si TCP est utilisé pour SIP, le client accepte également le trafic sur UDP conformément à *la RFC 3261*.
- Timeout (délai d'inactivité) spécifie la durée d'inactivité maximale, en secondes, après laquelle le message de persistance de connexion est envoyé. Aucune valeur signifie que le keepalive est désactivé pour le protocole.
- Charge utile pour les messages keepalive, valeurs possibles (aucune valeur ne signifie que keepalive est désactivé pour le protocole) :
  - Crlf

Informations confidentielles de Cisco

- Null (à ne pas utiliser)
- Chaîne personnalisée (**à ne pas utiliser**)

Les keepalives peuvent être utilisés à des fins de traversée NAT pour garder les liaisons NAT ouvertes avec peu de trafic supplémentaire.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%UDP_KEEPALIVE_ENABLED_WXT%	Vrai	vrai, faux	Contrôle si les paquets de persistance de connexion doivent être envoyés pour le transport UDP.
%TCP_KEEPALIVE_ENABLED_WXT%	false	vrai, faux	Contrôle si les paquets de persistance de connexion doivent être envoyés pour le transport TCP.
%TLS_KEEPALIVE_ENABLED_WXT%	false	vrai, faux	Contrôle si les paquets de persistance de connexion doivent être envoyés pour le transport TLS.

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

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

```
<config>
    <protocoles>
        <gorgée>
            <transports>
                <udp>
                    …
                </UDP>
                <tcp>
                    …
                    <Délai d'expiration de
connexion>%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%</délai d'expiration de
connexion>
                </tcp>
                <tls>
                    <Délai d'expiration de
connexion>%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%</délai d'expiration de
connexion>
                </tcp>
            </transports>
```

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

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<entier> - délai d'expiration en millisecondes	Expiration de la connexion du socket lors de l'utilisation TCP transport.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	<entier> - délai d'expiration en millisecondes	Le délai de connexion du socket est expiré lors de TLS'utilisation du transport.

6.1.6 Détection dynamique du proxy SIP

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

```
<config>
<Protocols><SIP>
<proxy-discovery enabled="%USE_PROXY_DISCOVERY_WXT% » tcp="%USE_TCP_FROM_DNS_WXT% »
udp="%USE_UDP_FROM_DNS_WXT% » tls="%USE_TLS_FROM_DNS_WXT%">
    <nom_enregistrement>%SBC_ADDRESS_WXT%</nom_enregistrement>
     <domain-override>%DOMAIN_OVERRIDE_WXT%</domain-override>
</Proxy-discovery>
```

Il est possible de contrôler les entrées de protocoles de transport de DNS SRV qui sont utilisées lorsqu'il en existe de nombreuses en suivant les procédures fournies dans cette section.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%USE_PROXY_DISCOVERY_WXT%	faux	Vrai, faux	Permet la détection dynamique du proxy SIP pour les appels audio et vidéo. La valeur recommandée est "true".
%SBC_ADDRESS_WXT%	vide	Chaîne	Cette balise Cisco BroadWorks est généralement utilisée pour le paramètre record-name. Il doit s'agir d'une URL valide – et non d'une adresse IP. Pour plus d'informations, reportez-vous à la section *5.6 Balises par défaut* système. Exemple : sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	vide	Chaîne	Cette balise personnalisée est utilisée pour le domain-override. Pour plus d'informations, reportez-vous à la section suivante. Exemple : other.domain.com

Informations confidentielles de Cisco

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

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

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

1. Effectuez une requête NAPTR en utilisant le *champ* nom<enregistrement> ci-dessus pour obtenir les URI du serveur avec les protocoles de transport s'ils existent. La valeur du *paramètre nom<enregistrement>* doit correspondre au domaine complet que DNS doit résoudre. Il ne peut pas s'agir d'une adresse IP.

Informations confidentielles de Cisco

2. Résolvez les éléments trouvés dans la requête NAPTR à l'aide d'une requête SRV pour obtenir le URI et le port final du serveur. La partie domaine utilisée dans la requête SRV est prise à partir du résultat de la requête NAPTR pour trouver le URI (et le port) final du serveur. Le port reçu de DNS requête SRV est utilisé lorsque les entrées SRV DNS 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. Pour l'utilisation des différents noms d'enregistrement, reportez-vous aux exemples suivants.

   Si aucun NAPTR n'est trouvé, le client tente une requête SRV avec le nom d'enregistrement pris de <*domaine*> paramètre sauf s'il existe <*domaine*> paramètre d'override auquel cas <*domain-override* > est utilisé et essaie automatiquement de trouver des entrées distinctes pour TCP, UDP et TLS (*_sip_protocol* [UDP, TCP ou TLS]). Notez que le protocole SCTP (Stream Control Transmission Protocol) n'est pas pris en charge. Si les requêtes SRV ne donnent aucun résultat, la détection du proxy échoue et une erreur indiquant que les appels ne sont pas disponibles s'affiche. Dans ce cas, il n'y a pas d'enregistrement SIP. Cependant, même si toutes les requêtes SRV échouent ou si les serveurs qui y sont 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 au URI spécifiées dans <adresse proxy> afin de voir s'il génère une adresse IP qui fournit un enregistrement SIP fonctionnel. Dans ce dernier cas, le port et le transport proviennent des *paramètres tcp-threshold* et <*secure*> .

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

Remarques importantes

REMARQUE 1 : Si DNS détection de proxy entraîne la sélection d'un protocole de transport à l'étape SRV en recevant un URI 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 de DNS.

REMARQUE 2 : Les éléments reçus via SRV sont prioritaires par rapport au proxy statique dans le fichier de configuration. L'ordonnance NAPTR n'est pas examinée ; seule la priorité SRV compte. Lorsque SRV aboutit à plusieurs éléments avec le même protocole de transport, priorité et pondération, celui qui est reçu est sélectionné au hasard. Les poids NAPTR ne sont pas pris en charge dans cette version, mais les poids SRV le sont. La priorité SRV est examinée en premier, et pour les éléments de priorité égale, le poids est examiné pour déterminer la probabilité qu'un serveur donné soit essayé ensuite.

REMARQUE 3 : Le paramètre facultatif *domain-override* permet de résoudre un nom d'enregistrement autre que celui du paramètre de configuration de domaine SIP avec SRV lorsque les résultats NAPTR sont omis. Voir les exemples suivants pour l'utilisation du *paramètre domain-override* .

REMARQUE 4 : Le client utilise des primitives de système d'exploitation pour DNS opérations et, généralement, DNS réponses sont mises en cache pour honorer la durée de vie de la réponse DNS.

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

Informations confidentielles de Cisco

REMARQUE 6 : Le client ne prend en charge que certains préfixes pour les services NAPTR. La liste suivante répertorie les préfixes pris en charge :

SIP+D2U -> _sip._udp

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

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

Exemple 1 : utilisation d'DNS détection de proxy sans paramètre de configuration de remplacement de domaine

Voici un exemple de configuration utilisant la découverte de proxy SIP lorsque seul SIP sur le TCP est utilisé et qu'une requête NAPTR à l'étape 1 renvoie des résultats.

```
<config>
<Protocols><SIP>
<adresse proxy="domain.com » port="5060"/>
<proxy-discovery enabled="true" >
    <nom_enregistrement>record-domain.com</nom_enregistrement>
     <domain-override>override-domain.com</domain-override >
</Proxy-Discovery>
<domaine>sip-domain.com</domaine>
```

Il en résulte les étapes suivantes au niveau du protocole.

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

En conséquence, l'enregistrement SIP s'effectue sur TCP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 1.2.3.4.

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

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

```
<config>
<protocoles><SIP
<adresse proxy="domain.com » port="5060"/>
<proxy-discovery enabled="true">
    <nom_enregistrement>record-domain.com</nom_enregistrement>
     <domain-override>override-domain.com</domain-override>
</Proxy-Discovery>
```


Informations confidentielles de Cisco

```
<domaine>sip-domain.com</domaine>
```

Il en résulte les étapes suivantes au niveau du protocole.

```
1. Requête NAPTR pour record-domain.com, sans réponse.
2. Requête SRV pour _sip._tcp.override-domain.com (à partir du fichier de
configuration), réponse
_sip._tcp.override-domain.com. 28635 DANS SRV
10 10 5061 test.override-domain.com.
3. Requête d'enregistrement A pour test.override-domain.com, réponse :
test.sipgeooverride-domain.com. 16 EN UN 4.3.2.1
```

En conséquence, l'enregistrement SIP s'effectue sur UDP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 4.3.2.1.

Exemple 3 : **Utilisation des priorités SRV**

Voici un autre exemple de configuration utilisant la découverte de proxy SIP lorsque seul SIP sur le TCP est utilisé et que la requête NAPTR à l'étape 1 renvoie des 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 diffusion, bien que plusieurs enregistrements NAPTR avec des priorités différentes soient également reçus.

```
<config>
<Protocols><SIP>
<adresse proxy="domain.com » port="5060"/>
<proxy-discovery enabled="true">
    <nom_enregistrement>record-domain.com</nom_enregistrement>
     <domain-override>override-domain.com</domain-override >
</Proxy-Discovery>
<domaine>sip-domain.com</domaine>
```

Il en résulte les étapes suivantes au niveau du protocole.

```
1. Requête NAPTR pour record-domain.com, réponse :
record-domain.com.
28591 DANS 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. Requête SRV pour _sip._tcp.test.sip.record-domain.com (reçue dans la requête
NAPTR), réponse
_sip._tcp.test.sip.record-domain.com. 28635 DANS SRV
10 10 5061 test.sipgeo.record-domain.com.

Requête SRV pour _sip._udp.test.sip.record-domain.com (reçue dans la requête
NAPTR), réponse
_sip._udp.test.sip.record-domain.com. 28635 DANS SRV
20 10 5062 test.sipgeo.record-domain.com.

3. Requête d'enregistrement A pour test.sipgeo.record-domain.com, réponse :
test.sipgeo.record-domain.com. 16 EN UN 1.2.3.4
```

Par conséquent, l'enregistrement SIP s'effectue sur TCP en utilisant le 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.

Informations confidentielles de Cisco

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

Voici un exemple de configuration utilisant la découverte de proxy SIP lorsque SIP sur TCP et TLS est utilisé et qu'une requête NAPTR à l'étape 1 renvoie des résultats.

```
<config>
<Protocols><SIP>
<adresse proxy="domain.com » port="5060"/>
<proxy-discovery enabled="true" tcp="true" udp="false" tls="true">
    <nom_enregistrement>record-domain.com</nom_enregistrement>
     <domain-override>override-domain.com</domain-override>
</Proxy-Discovery>
<domaine>sip-domain.com</domaine>
```

Il en résulte les étapes suivantes au niveau du protocole.

```
1. Requête NAPTR pour record-domain.com, réponse :
record-domain.com.
28591 DANS NAPTR 100 10 "S" "SIPS+D2T" «  » _sip._tls.test.sip.record-
domain.com.
28591 DANS NAPTR 100 10 "S" "SIP+D2T" «  » _sip._tcp.test.sip.record-domain.com.

2. Pour le premier enregistrement, nous avons le type de service "SIPS + D2T" et
le préfixe est "sip._tls. ». Étant donné que ce préfixe ne correspond pas au
type de service (voir la note 6 ci-dessus), il sera ignoré.

3. Requête SRV pour _sip._tcp.test.sip.record-domain.com (reçue dans la requête
NAPTR), réponse
_sip._tcp.test.sip.record-domain.com. 28635 DANS SRV
10 10 5061 test.sipgeo.record-domain.com.

3. Requête d'enregistrement A pour test.sipgeo.record-domain.com, réponse :
test.sipgeo.record-domain.com. 16 EN UN 1.2.3.4
```

En conséquence, l'enregistrement SIP a lieu sur TCP en utilisant le port 5061 (reçu dans l'étape SRV) et vers l'adresse IP 1.2.3.4.

6.1.7 Utilisation du port préféré pour SIP

Dans certains cas, un autre progiciel s'est exécuté sur la même machine que le client, occupant le port SIP par défaut. Le paramètre preferred-port *peut être utilisé pour configurer le client afin qu'il utilise un autre port pour SIP* . Le client tente d'utiliser la valeur de port configurée spécifiée dans le *paramètre de port* préféré, mais si elle est prise, le client essaie de manière incrémentielle des valeurs de port supérieures à la valeur configurée. Par exemple, si la valeur du *port* préféré est "6000" et que ce port est utilisé, le client essaie 6001, 6002, 6003, et ainsi de suite jusqu'à ce qu'il trouve un port inutilisé. Une fois qu'un port inutilisé est trouvé, il l'utilise pour sa propre communication SIP.

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

Informations confidentielles de Cisco

6.1.8 Basculement et restauration automatique SIP

Le basculement et le retour arrière SIP suivent les procédures Cisco BroadWorks. Pour cela, plusieurs proxys (généralement le SBC) doivent être configurés.

Du côté client, le proxy doit être résolu en plusieurs adresses IP. Pour ce faire, vous pouvez :

- La détection de proxy SIP est activée et le serveur DNS possède des enregistrements NAPTR et/ou SRV pour le nom de domaine complet SBC (voir section *6.1.6 Détection dynamique du proxy* SIP), OU
- L'adresse proxy SIP est fournie en tant que nom de domaine complet et peut être transformée en plusieurs adresses IP (voir 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'existe pas de limite codée en dur pour le nombre maximal d'adresses de IP dans la liste.

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

6.1.8.1 Basculement SIP

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

- Erreur de socket – si le socket entre le client et le serveur est cassé ou fermé, comme dans le cas d'une perte de connectivité réseau, le client réagit immédiatement et déclenche un basculement.
- Délai expiré (par exemple, lorsque le SBC se bloque) – basé sur le SIP T1 :
  - SIP INVITE – si la requête INVITE expire, le client s'enregistre auprès du prochain SBC disponible (IP) et retente l'invite INVITE.
  - Autre requête SIP : le client tente de s'inscrire auprès du prochain SBC (IP) disponible.
- 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 <u>provoquent pas</u> de basculement :
    - 401 Non autorisé
    - 403 Interdit
    - 404 Introuvable
    - 407 Authentification du proxy requise
    - Intervalle 423 trop bref
  - De plus, *les réponses d'erreur 4xx* à SIP INVITE ne déclenchent pas le basculement, contrairement *aux modèles 5xx* et *6xx* .

Informations confidentielles de Cisco

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

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>
< minuteries>
   <T1>500</T1>
   <T2>4000</T2>
   <T4>5000</T4>
</minuteries>
```

  - T1 – la durée, en millisecondes, d'un délai aller-retour réseau.
  - T2 – temps maximum, en millisecondes, avant la retransmission des requêtes non-INVITE et des réponses d'invitation.
  - T4 – la durée maximale, en millisecondes, pendant laquelle un message reste dans le réseau.
- Adresse proxy SIP et détection de 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 du basculement (voir ci-dessous)

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

L'en-tête Contact contenant les informations sur le nouveau périphérique a également une valeur q, qui est lue à partir de la *balise <q-value>* . La *valeur de marque<q>* est utilisée pour indiquer la préférence ou la priorité d'une adresse de contact particulière. Il varie 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 contrôleur SBC utilisé dans le déploiement a une logique inverse et traite q=0,0 avec la priorité maximale.

Informations confidentielles de Cisco

À partir de la version 42.11, une nouvelle *section <register-failover>* est introduite dans le modèle de configuration. Un nouveau paramètre *configurable <registration-cleanup>* a été ajouté pour contrôler si l'application enverra ou non l'en-tête Contact pour nettoyer les informations sur l'ancien périphérique. Certains contrôleurs SBC nettoient l'ancienne session immédiatement à la déconnexion du 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.

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

Exemple :

```
<config>
<Protocols><SIP>
   <q-value>1.0</q-value> <!-- OBSOLÈTE -->
   <registre-basculement>
      <enregistrement-
nettoyage>%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%</nettoyage-
enregistrement>
      <q-value>1.0</q-value>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	Vrai	vrai, faux	Contrôle le nettoyage des informations sur l'ancien périphérique en cas de basculement SIP.

6.1.8.2 Restauration automatique SIP

Si le client est connecté à un proxy qui n'est pas le premier par priorité, il tente de se reconnecter au IP ayant la priorité la plus élevée. La durée de restauration automatique est basée sur la configuration DNS de la gestion TTL (voir section *6.1.8.4 Gestion DNS TTL*). Si un appel est en cours lorsque le temporisateur de restauration automatique est atteint, le client attend que tous les appels soient terminés et déclenche la procédure de restauration automatique. Notez que ceci n'est valable que pour les clients de bureau puisque la connexion SIP n'est active que pendant un appel sur mobile.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SIP_FAILBACK_ENABLED_WXT%	Vrai	vrai, faux	Active ou désactive le retour arrière SIP.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Plus de 60	Délai de restauration automatique SIP en secondes.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	vrai, faux	Ajoute une période aléatoire [0-10]% du retour arrière SIP.

Informations confidentielles de Cisco

6.1.8.3 Appliquer IP version

Webex client peut être configuré sur la manière de trier la liste des hôtes résolus via le DNS puis de les parcourir en cas de basculement SIP. Dans tous les modes, la priorité et le poids sont respectés.

Les configurations prises en charge sont les suivantes :

- DNS : utilise toutes les adresses renvoyées par les requêtes DNS
- ipv4 - filtre les adresses IPv6
- IPv6 - filtre les adresses IPv4
- prefer-ipv4 – commande les adresses IPv4 avant l'IPv6 (version 42.9)
- prefer-ipv6 – commande les adresses IPv6 avant le IPv4 (version 42.9)
- nat64 – ignore les adresses IPv6, ordonne les IPv4 (version 44.2)

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

Avec la configuration "dns", les adresses IPv4 sont prioritaires par rapport aux adresses IPv6, pour un hôte donné. S'il existe deux hôtes avec des adresses IPv4 et IPv6, l'ordre sera IPv4(hôte1), IPv6(hôte1), IPv4(hôte2), IPv6(hôte2).

En mode "prefer-ipv4", les adresses IPv4 sont classées avant les adresses IPv6 (l'ordre au sein des groupes IPv4 et IPv6 demeure)

Exemple : IPv4(hôte1), IPv4(hôte2), IPv6(hôte1), IPv6(hôte2).

Avec le mode "prefer-ipv6", l'ordre est inverse - les adresses IPv6 sont placées avant les adresses IPv4

Exemple : IPv6(hôte1), IPv6(hôte2), IPv4(hôte1), IPv4(hôte2).

Avec le mode "nat64" - les adresses IPv6 sont ignorées, l'ordre IPv4 est respecté. Les préfixes IPv6 sont détectés. 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>
<protocoles><sip><transports>
<enforce-ip-version>%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%</enforce-ip-version>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	Dns	IPv4 IPv6 Dns Préféré-IPv4 préférence-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 façon dont DNS résolution est refaite lorsque la durée de vie de l'enregistrement de DNS du serveur actuellement utilisé expire. Le paramètre du tableau suivant, lorsqu'il est activé, force le client à rétablir DNS opérations une fois que la durée de vie du SRV DNS ou de l'enregistrement A du serveur actuellement utilisé expire.

Une fois la résolution DNS refaite, ce paramètre force 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 en cours fonctionne pleinement. Toutefois, la reconnexion n'est effectuée qu'une fois les appels en cours terminés.

Si les durée de vie des enregistrements des serveurs A et SRV sont différentes, la valeur la plus petite est choisie.

Lorsque ce paramètre est désactivé, DNS opérations ne sont pas refaites lorsque la durée de vie expire, mais toutes les 15 minutes.

Ce paramètre ne fonctionne que pour SIP.

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

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

```
<config>
<Protocols><SIP>
<refresh-on-ttl enabled="%SIP_REFRESH_ON_TTL_WXT% »
  use-random-factor="%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SIP_REFRESH_ON_TTL_WXT%	false	faux, vrai	Lorsque la valeur "false" est activée", DNS gestion TTL est désactivée pour SIP. Lorsque la valeur "true" est activée, DNS gestion TTL est activée pour SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	false	faux, vrai	Si cette option est activée, ajoute une période aléatoire comprise entre 0 et 10 % à la durée de vie DNS.

REMARQUE : Il est fortement recommandé d'activer le facteur aléatoire TTL DNS pour éviter les pics de demandes au DNS et potentiellement les pics de tentatives de reconnexion au serveur d'applications.

6.1.9 SIP SUBCSRIBE et REGISTER Actualiser et SUBSCRIBE Réessayer

Office Communicator prend en charge la configuration des intervalles d'actualisation pour SIP SUBSCRIBE et REGISTER. Pour SIP SUBSCRIBE, il existe un paramètre distinct pour l'intervalle d'actualisation (en secondes) et la durée d'attente du client avant de retenter SIP SUBSCRIBE s'il y a des erreurs (en secondes). La valeur maximale recommandée pour l'intervalle *abonnement-nouvelle tentative* est 2000000 secondes, tandis que toute valeur négative, 0 ou vide entraîne l'utilisation de 1800 secondes. Toute valeur négative dans pour l'actualisation de l'abonnement omet l'en-tête *Expires* et crée ainsi un SUBSCRIBE unique.

Le temporisateur d'actualisation SIP REGISTER proposé par le client peut être configuré en quelques secondes, mais selon les spécifications SIP, le serveur peut remplacer la valeur. Actuellement, le client mémorise 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>
<intervalle-d'actualisation-abonnement>10800</intervalle-actualisation-abonnement>
<intervalle de nouvelle tentative d'abonnement>60</intervalle-réessayer-abonnement>
<intervalle d'actualisation-enregistrement>300</intervalle-actualisation-
enregistrement>
< session >
       <valeur_expire>3600</valeur_expire>
</session>
```

6.1.10 Utiliser des URI associés à P dans REGISTER

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

Si le paramètre est défini sur "false", le client n'utilise pas l'URI *associée à P* et utilise à la place l'identité de son propre URI SIP.

Informations confidentielles de Cisco

```
<config>
<Protocols><SIP>
<use-alternatives-identities>%USE_ALTERNATIVE_IDENTITIES_WXT%</use-alternative-
identities>
```

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	vrai, faux	Permet l'utilisation d'identités alternatives dans SIP REGISTER. Si ce paramètre est réglé sur true, le client prend sa propre identité à partir du dernier *en-tête P-Associated-URI* pour les requêtes SIP sortantes. Si ce paramètre est réglé par "false", sa propre identité pour les requêtes SIP sortantes est extraite de son propre URI SIP.

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

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

Le paramètre de configuration active la prise en charge du PEM publicitaire dans la signalisation SIP. La logique réelle de gestion 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 si omis	Valeurs prises en charge	Description
%ENABLE_PEM_SUPPORT_WXT%	faux	Vrai, faux	Défini sur "true" pour activer la prise en charge du PEM publicitaire client dans la signalisation SIP. Sélectionnez "false" pour désactiver la prise en charge du PEM publicitaire client dans la signalisation SIP.

Informations confidentielles de Cisco

6.1.12 Prise en charge de SIP UPDATE

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

Les cas d'utilisation typiques sont liés aux premiers médias lorsque, par exemple, l'utilisation simultanée de la tonalité de rappel et de la pré-alerte est utilisée.

Actuellement, SIP UPDATE n'est pris en charge que lorsqu'il est reçu dans les cas d'utilisation pré-dialogue (premiers médias) et non pendant la boîte de dialogue active, par exemple, pour les appels en attente/reprise où re-INVITE est toujours utilisé.

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

```
<config>
<Protocols><SIP>
<Support-Update enabled="%ENABLE_SIP_UPDATE_SUPPORT_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	vrai, faux	Lorsque la valeur "false" est sélectionnée, la prise en charge de SIP UPDATE est désactivée. Lorsque la valeur true est activée, la prise en charge de SIP UPDATE est activée.

6.1.13 Ancien SIP INFO FIR

Ce client prend en charge la méthode héritée de demande d'images clés vidéo via une demande de contrôle de média SIP INFO. Cela est nécessaire car certains périphériques ont des problèmes de réponse au RTCP-FB FIR et parfois RTCP ne passe pas par le terminal distant, ce qui peut conduire à l'absence de vidéo ou à la vidéo unidirectionnelle. Pour plus d'informations, consultez *RFC 5168*.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	faux	Vrai, faux	Lorsque "false" est sélectionné, la prise en charge de SIP INFO FIR est désactivée. Lorsque la valeur "true" est activée, la prise en charge de SIP INFO FIR est activée.

Informations confidentielles de Cisco

6.1.14 Gestion de l'acheminement SIP pour la traversée NAT

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

Pour plus d'informations sur les recommandations de port SIP et de protocole de transport lorsque des passerelles de couche d'application (ALG) SIP sont utilisées dans le réseau, reportez-vous *au guide Webex pour Cisco BroadWorks Solution Guide*.

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

Le *paramètre Preferred-port* est lié car il définit par ailleurs le port utilisé dans l'en-tête du Contact SIP. Pour plus d'informations sur l'attribution des ports SIP, reportez-vous à la section *6.1.7 Utilisation du port préféré* pour SIP.

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

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

```
<config>
<Protocols><SIP>
<use-rport enabled="%ENABLE_USE_RPORT_WXT% » use-local-
port="%RPORT_USE_LOCAL_PORT_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_USE_RPORT_WXT%	false	vrai, faux	Active le port pour les appels audio et vidéo.
%RPORT_USE_LOCAL_PORT_WXT%	false	vrai, faux	Indique si le port local du socket du client doit être ajouté dans l'en-tête du contact *SIP* .

Informations confidentielles de Cisco

6.1.15 ID de la session SIP

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

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

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_SIP_SESSION_ID_WXT%	faux	Vrai, faux	Contrôle l'utilisation de l'ID de session SIP.

6.1.16 Comportement du rejet de l'appel entrant

Le client offre la possibilité de refuser un appel au moyen *du 486* ou *du 603*.

Notez que si le client est configuré pour rejeter un appel avec *Refus* 603, les services Renvoi d'appel si occupé et Renvoi d'appel en l'absence de réponse risquent de ne pas fonctionner comme prévu.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_REJECT_WITH_486_WXT%	Vrai	vrai, faux	Contrôle le code d'erreur SIP et la raison utilisée pour rejeter les appels SIP entrants. Si cette option est activée,486 *l'option Non disponible* temporairement est utilisée. Sinon,603 *Déclin* 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 pour SRTP. Pour ce faire, définissez les valeurs limites de plage de ports pour les flux audio et vidéo avec les balises indiquées dans l'exemple suivant.

```
<config>
```


Informations confidentielles de Cisco

```
<protocoles><rtp>
<devenir-port-audio-préféré>%RTP_AUDIO_PORT_RANGE_START_WXT%</début-port-audio-
préféré>
<preferred audio-port-end>%RTP_AUDIO_PORT_RANGE_END_WXT%</preferred-audio-port-end>
<devenir-port-vidéo-préféré>%RTP_VIDEO_PORT_RANGE_START_WXT%</début-port-vidéo-
préféré>
<préféré-video-port-end>%RTP_VIDEO_PORT_RANGE_END_WXT%</preferred-video-port-end>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	nombre	Début de la plage de ports audio.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	nombre	Fin de la plage des ports audio.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	nombre	Début de la plage de ports vidéo.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	nombre	Fin de la plage des ports vidéo.

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

6.1.18 Prise en charge ICE (Webex Calling uniquement)

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

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

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

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

```
<config>
<protocoles><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%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_RTP_ICE_WXT%	false	vrai, faux	Activer/Désactiver la prise en charge 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)	serveur STUN valide URI ou (vide)	Le serveur STUN URI.
%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 RTCP MUX

RTCP MUX est configurable. Grâce à cette fonctionnalité, le client utilise le même port pour les RTP et RTCP. Au niveau de signalisation SIP/SDP, la ligne a=rtcp-mux est ajoutée au SDP. De plus, différents modes sont possibles :

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

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

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

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_RTCP_MUX_WXT%	Vrai	vrai, faux	Pour activer RTPC MUX, définissez la valeur "true". Pour désactiver RTCP MUX, définissez "false".

6.1.20 Transfert

Les Webex pour les clients Cisco BroadWorks prennent en charge les transferts d'appels assistés (consultatifs), semi-consultatifs et directs (aveugles).

Informations confidentielles de Cisco

Le transfert d'appel semi-consultatif permet à l'appelant d'effectuer le transfert avant que l'appel ne soit pris par l'appelé distant. Le bouton d'achèvement semi-consultatif n'est activé pour l'appelant qu'après le début de la sonnerie du côté de l'appelé et la réception de la notification SIP correspondante (*180 sonneries*) du côté de l'appelant. Le transfert aveugle est appelé "Transférer maintenant" dans l'interface utilisateur.

> **REMARQUE** : La sonnerie *SIP* 180 peut ne 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 sur le terminal local. En outre, les appels terminés sur un périphérique distant peuvent être transférés à des appels terminés sur un terminal distant. Cette fonctionnalité ne dispose 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 mis automatiquement en attente lorsque l'élément de menu Transfert est sélectionné. Ce comportement est contrôlé par le nouvel *attribut de mise en attente* automatique. Par défaut, la mise en attente automatique est désactivée.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_TRANSFER_CALLS_WXT%	false	vrai, faux	Lorsque la valeur "true" est activée, le transfert d'appels est activé. Lorsque la valeur "false" est sélectionnée, le transfert d'appels 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%	plein	Parlez d'abord, aveugle, plein	Spécifie les types de transfert disponibles pour l'utilisateur dans la configuration BroadWorks.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	vrai, faux	Indique si l'appel actif est mis en attente automatiquement lorsque l'utilisateur sélectionne l'option Transférer dans le menu de l'écran d'appel.

Informations confidentielles de Cisco

6.1.21 Conférences téléphoniques N-Way et participants

Le tag personnalisé suivant peut être utilisé pour contrôler la disponibilité de la conférence téléphonique ad hoc (N-Way) via SIP dans le Webex pour le client Cisco BroadWorks. En outre, le propriétaire N-way peut voir la liste complète des participants via SIP SUBSCRIBE/NOTIFY et le forfait événementiel de la conférence. Le client du propriétaire apprend le URI d'envoyer le message SIP SUBSCRIBE to via l'en-tête SIP *Contact* précédent du message 200 OK *envoyé en réponse à l'INVITE au URI de conférence, tandis que pour les participants les mêmes informations figurent dans un NOTIFY d'informations d'appel* précédent.

Le paramètre système Cisco BroadWorks (*maxConferenceParties)* permet de définir le nombre maximum de participants à la conférence. Pour un appel donné, il indique le nombre d'interlocuteurs simultanés actifs qu'un utilisateur peut avoir ou ajouter via l'option de contrôle "Ajouter des participants" ou via la fonction d'appel N-way de Cisco BroadWorks.

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

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

Exemple de sortie :
maxConferenceParties = 6
conferenceURI =
```

Une fois que la valeur de maxConferenceParties est obtenue (comprise entre 4 et 15), la balise %MAX_CONF_PARTIES_WXT% doit être définie en conséquence.

```
<config>
<services><appels>
<conférence activée="%ENABLE_CONFERENCE_CALLS_WXT%">
   <URI-SERVICE>sip_:%BWNETWORK-CONFERENCE-SIPURI-1 %</service-uri>
   <subscribe-conference-info enabled="%ENABLE_NWAY_PARTICIPANT_LIST_WXT%"/>
      <max-nway-participants>%MAX_CONF_PARTIES_WXT%</max-nway-participants>
</conférence>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	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	Définissez la valeur "true" pour activer la liste des participants des propriétaires N-way. Réglez sur "false" pour désactiver la liste des participants des propriétaires N-way.
%MAX_CONF_PARTIES_WXT%	10	Nombre entre 4 et 15 (vide)	Spécifie le nombre maximal de participants N-way, appliqué par le client, par exemple, 10. Le côté serveur a ses propres limites. La valeur vide désactive l'application côté client de la limite de participants N-way.

Informations confidentielles de Cisco

6.1.22 Extraction d'appel

La fonctionnalité Extraction d'appels peut être activée à l'aide d'un seul paramètre de configuration, comme illustré dans l'exemple suivant.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_PULL_WXT%	faux	Vrai, faux	Active l'extraction d'appel.

6.1.23 Parquer/Récupérer un appel

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

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

```
<config>
<services><appels>
<parcage d'appels activé="%ENABLE_CALL_PARK_WXT% »
timer="%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_PARK_WXT%	faux	Vrai, faux	Active le parcage/la récupération de l'appel.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Nombre entre 5 et 30	Spécifie le nombre de secondes pendant lesquelles la boîte de dialogue Appel parqué est visible par l'utilisateur avant d'être fermée automatiquement.

6.1.24 Statistiques d'appel

Création de rapports Statistiques de fin d'appel en Session Initiation Protocol (SIP) Le message BYE permet d'envoyer des statistiques d'appel à un interlocuteur distant lorsqu'un appel prend fin. Les statistiques d'appel sont envoyées sous forme de nouvel en-tête dans le message SIP BYE ou dans la *réponse correspondante 200 OK* au message BYE. Les statistiques incluent les paquets RTP en temps réel envoyés ou reçus, le nombre total d'octets envoyés ou reçus, le nombre total de paquets perdus, la gigue du retard, le délai aller-retour et la durée des appels.

Informations confidentielles de Cisco

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_STATISTICS_WXT%	false	vrai, faux	Défini sur "true" pour permettre la capture des métriques d'appel. Sélectionnez "false" pour désactiver la capture des mesures d'appel.

6.1.25 Récupération automatique de l'appel / Transfert transparent d'appel

Le client prend en charge la récupération automatique des appels sur les réseaux à commutation lorsque 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 de la commutation entre les réseaux WiFi. On tente de récupérer l'appel dans un délai d'une minute, puis il s'arrête. Si plusieurs appels VoIP sont en cours, seul le actif est récupéré.

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

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

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

6.1.26 Enregistrement d'appel

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

Si la fonction est désactivée, l'utilisateur n'a pas de boutons ni d'options d'enregistrement. Notez que l'enregistrement des appels fonctionne sur une base par utilisateur, pas par appel - cela signifie que si l'un des participants à un appel prend en charge l'enregistrement d'appel, alors l'appel peut être enregistré.

Informations confidentielles de Cisco

Si la fonction d'enregistrement des appels est activée, l'enregistrement de l'appel est toujours affiché visuellement. Les modes d'enregistrement des appels suivants sont pris en charge par Cisco BroadWorks :

Toujours

- L'enregistrement des appels sera lancé automatiquement lors de l'établissement de l'appel.
- L'utilisateur n'est **PAS** en mesure d'arrêter/mettre en pause l'enregistrement de l'appel.

Toujours avec pause / reprise de l'assistance

- L'enregistrement de l'appel sera lancé automatiquement lors de l'établissement de l'appel, mais l'utilisateur pourra mettre l'appel en pause et le reprendre.
- Interactions utilisateur possibles :
  - L'enregistrement est en cours – **Action Suspendre** l'enregistrement.
  - L'enregistrement est en pause – **Action Reprendre** l'enregistrement.

À la demande

- Une fois l'appel établi, l'enregistrement de l'appel démarre sur le serveur.
- Si l'utilisateur appuie sur l'option Démarrer l'enregistrement pendant l'appel, l'enregistrement de l'appel est stocké et l'appel est conservé depuis son démarrage. Sinon, si aucun démarrage d'enregistrement n'est lancé par l'utilisateur, l'enregistrement d'appel sera supprimé sur le serveur.
- Interactions utilisateur possibles :
  - Aucun enregistrement n'a encore démarré – **Action Démarrer l'enregistrement** .
  - L'enregistrement est en cours – **Action Suspendre** l'enregistrement.
  - L'enregistrement est en pause – **Action Reprendre** l'enregistrement.

À la demande avec démarrage initié par l'utilisateur

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

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

```
<config>
<services><appels>
<enregistrement activé="%ENABLE_CALL_RECORDING_WXT%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_RECORDING_WXT%	false	vrai, faux	Active les commandes 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 des messageries vocale et vocale visuelle Cisco BroadWorks dans l'Webex du client Cisco BroadWorks. Notez qu'un tag système Cisco BroadWorks (%BWVOICE-PORTAL-NUMBER-1 %) est utilisé avec la messagerie vocale.

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

Pour connaître la version de Cisco BroadWorks et les correctifs requis pour la messagerie vocale visuelle, reportez-vous au
Webex du Guide de solution Cisco BroadWorks.

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

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

- Messagerie vocale activée
- Option "Lorsque le message arrive, utilisez la messagerie unifiée" activée
- Option "Utiliser l'indicateur de messages en attente" activée

Si le service de messagerie vocale visuelle n'est pas affecté du côté de Cisco BroadWorks à l'utilisateur, la configuration du service est automatiquement désactivée.

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

Pour afficher les informations d'un message vocal dans l'interface utilisateur, le client doit recevoir des notifications de MWI SIP du serveur (c'est-à-dire du package d'événements de messagerie vocale). Reportez-vous au tableau qui suit pour connaître les options d'abonnement. Notez également qu'MWI est nécessaire pour que les notifications de messagerie vocale visuelle fonctionnent.

Informations confidentielles de Cisco

Notez que si l'abonnement SIP au package d'événements de messagerie vocale échoue, le client continue à réessayer lorsqu'il est configuré pour le faire. Pour plus d'informations sur la configuration des nouvelles tentatives SIP SUBSCRIBE, reportez-vous à la section *6.1.9 SIP SUBCSRIBE et REGISTER Actualiser et SUBSCRIBE Réessayer.*

```
<config>
<services><appels>
<MWI enabled="%ENABLE_MWI_WXT% » type="%MWI_MODE_WXT%"/>
<voice-mail enabled="%ENABLE_VOICE_MAIL_WXT% » visual-
voicemail="%ENABLE_VISUAL_VOICE_MAIL_WXT%">
   <numéro-centre>%NUMÉRO-PORTAIL-BWVOICE-1 %</numéro-centre>
</messagerie vocale >
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_VOICE_MAIL_WXT%	false	vrai, faux	Réglez la valeur "true" pour activer la prise en charge de la messagerie vocale. Sélectionnez "false" pour désactiver la prise en charge de la messagerie vocale.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	vrai,faux	Lorsque la valeur "false" est attribuée, la VVM est désactivée. Lorsque la valeur "true" est activée, VVM est activée. Notez que la messagerie vocale enabled=false avant l'attribut VVM réel est encore utilisé pour des raisons de compatibilité descendante.
%NOMBRE-PORTAIL-BWVOICE-1%	vide	nombre	Le client appelle ce numéro généralement spécifié à l'aide d'un tag système Cisco BroadWorks existant lors de la composition de la messagerie vocale.
%ENABLE_MWI_WXT%	false	vrai, faux	Défini sur "true" pour activer MWI. Sélectionnez "false" pour désactiver MWI.
%MWI_MODE_WXT%	vide	implicite, explicite	Défini sur "explicite" pour envoyer SIP SUBSCRIBE pour MWI package d'événements lorsque MWI est activé. Utiliser "implicit" n'envoie pas de package d'événements SIP SUBSCRIBE pour MWI lorsque MWI est activé. Si elle est laissée vide, MWI est désactivée.

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 de bureau et mobiles Webex Calling.

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

1. L'application est en cours d'exécution dans Webex Calling déploiement.

Informations confidentielles de Cisco

2. La fonctionnalité Messagerie vocale visuelle est activée pour l'utilisateur.
3. La fonctionnalité est activée dans la configuration (l'attribut enabled de la balise <services><voice-mail><transcription> doit être défini sur "true").

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

6.1.29 Paramètres d'appel

6.1.29.1 Renvoi de tous les appels

Le tag personnalisé suivant peut être utilisé pour contrôler la disponibilité du service Renvoi d'appel en continu Cisco BroadWorks dans la Webex du client Cisco BroadWorks.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	vrai, faux	Contrôle la disponibilité du service Renvoi automatique d'appel en permanence. Par défaut, la fonction est désactivée.

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

6.1.29.2 Renvoi d'appels vers la messagerie vocale

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

```
<config>
<services>
   <messagerie vocale>
      <transfert activé="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	Vrai	vrai, faux	Contrôle la disponibilité du transfert vers la messagerie vocale. La fonctionnalité est activée par défaut.

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

REMARQUE 2 : Renvoi d'appels vers la messagerie vocale et Renvoi d'appels Toujours (*6.1.29.1 Renvoi de tous* les appels) peuvent être utilisés ensemble pour afficher ou masquer le paramètre "Transfert d'appel" dans les applications Webex. Lorsque les deux balises sont désactivées, le paramètre "Transfert 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 ainsi que la disponibilité de ses paramètres dans l'Webex pour le client Cisco BroadWorks. Notez que le nom de cette fonctionnalité à l'intérieur du client est *Gérer mes numéros*.

```
<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%"/>
       <contrôle-appel activé="%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% »
default="%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%"/>
       <inhibiteur-de détournement
activé="%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% »
default="%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%"/>
       <confirmation-réponse
activée="%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% »
default="%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%"/>
</broadworks-n'importe où>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	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 l'emplacement BWA doit être disponible pour l'utilisateur.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	vrai, faux	Défini sur "true" pour rendre l'option Alert All Locations pour le service BWA disponible pour l'utilisateur. Réglez la valeur "false" pour rendre l'option Alerter tous les emplacements pour le service BWA non disponible 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, à l'ajout du deuxième emplacement ou à chaque nouvel emplacement BWA suivant.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	vrai, faux	Indique 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 l'emplacement BWA.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	vrai, faux	Contrôle si l'inhibiteur de dérivation de l'emplacement BWA doit être disponible pour l'utilisateur.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	vrai, faux	Contrôle l'état par défaut de l'inhibiteur de dérivation 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 Paramètres du portail et des appels Web

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

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

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

Informations confidentielles de Cisco

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

```
<config>
<services>
<web-call-settings target="%WEB_CALL_SETTINGS_TARGET_WXT% »
 <url>%WEB_CALL_SETTINGS_URL_WXT%</url>
<branding-enabled="%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%">
  <paramètres de service>
   <service name="Renvoi d'appels toujours"
visible="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <service name="Renvoi d'appels si occupé"
visible="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <service name="Renvoi d'appels non accessible"
visible="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
   <service name="Renvoi d'appel sans réponse"
visible="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <nom du service="Ne pas déranger"
visible="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
   <service name="Rejet d'appel anonyme"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="Sonnerie personnelle simultanée"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <nom de service="Sonnerie séquentielle"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <nom de service="Rappel automatique"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <nom de service="Appel en attente"
visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Blocage de la remise de l'ID de la ligne appelante"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <nom de service="Assistant personnel"
visible="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
   <service name="Centre d'appels - Standard"
visible="%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%"/>
   <nom de service="BroadWorks Anywhere"
visible="%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%"/>
   <service name="BroadWorks Mobility"
visible="%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <service name="Bureau distant" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Utilisateur de messagerie vocale"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 Paramètres de </service>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
Paramètres d'</web-call>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%WEB_CALL_SETTINGS_TARGET_WXT%	externe	externe, CSW	Contrôle le mode portail d'administration. Définissez la valeur "externe" pour ouvrir l'URL du portail configuré dans un navigateur externe. Réglez sur "csw" pour ouvrir le portail CSW dans un navigateur intégré en utilisant la section des paramètres supplémentaires <services><web-call-settings> à partir de la requête POST.
%WEB_CALL_SETTINGS_URL_WXT%	vide	Chaîne d'URL	URL du portail de paramètres. Exemple : https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'utilisateur doit voir l'option Toujours renvoyer les appels dans les paramètres Web.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Ne pas déranger (NPD) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option de rejet d'appel anonyme (ACR) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Renvoi d'appel si occupé (CFB) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	Vrai	vrai, faux	Contrôle si l'option Renvoi d'appel non joignable (CFNR) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Renvoi d'appel en l'absence de réponse (CFNA) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Sonnerie personnelle simultanée (SIMRING) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Sonnerie séquentielle (SEQRING) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Bureau distant (RO) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option de rappel automatique (ACB) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option d'appel en attente (CW) doit être visible pour l'utilisateur dans les paramètres Web.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%WEB_CALL_SETTINGS_ CLIDB_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'utilisateur doit voir l'option CLIDB (Calling Line ID Delivery Blocking) dans les paramètres Web.
%WEB_CALL_SETTINGS_PA _ VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Personal Assistant (PA) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_B WA_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option BroadWorks Anywhere (BWA) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_CC _ VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option Centre d'appels doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_ BWM_VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option BroadWorks Mobility (BWM) doit être visible pour l'utilisateur dans les paramètres Web. Actuellement, la valeur recommandée est "faux" en raison de problèmes d'interopérabilité entre Webex Cisco BroadWorks et BroadWorks Mobility.
%WEB_CALL_SETTINGS_VM _VISIBLE_WXT%	Vrai	vrai, faux	Indique si l'option de gestion vocale (VM) doit être visible pour l'utilisateur dans les paramètres Web.
%WEB_CALL_SETTINGS_BR ANDING_ENABLED_WXT%	false	vrai, faux	Contrôle l'utilisation des nouveaux paramètres d'appel WebView de la nouvelle marque. Activez si la version de CSWV côté serveur est 1.8.6 ou supérieure. Sinon, gardez-le faux.
%WEB_CALL_SETTINGS_EM AIL_VM_VISIBLE_WXT%	Vrai	vrai, faux	Indique si les options de messagerie vocale et de courrier électronique sont visibles dans les paramètres Web.
%USER_PORTAL_SETTINGS _URL_WXT%	vide	Chaîne d'URL	Indique l'URL d'accès au 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	Indique si l'URL doit être ouverte dans un navigateur incorporé ou externe.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	faux	Vrai, faux	Applicable uniquement lorsqu'un navigateur intégré est configuré (USER_PORTAL_SETTINGS_TARGET_WXT=interne). Lorsque cette option est activée, la requête HTTP POST est utilisée et le jeton de courte durée BroadWorks est ajouté dans le BODY. Lorsque cette option est désactivée, l'URL est ouverte avec HTTP GET.

REMARQUE 1 : L'URL de la WebView des paramètres d'appel doit toujours avoir un « / » de fin configuré. Par exemple : https://<XSP-FQDN>/<CSW-Context-Path>/

REMARQUE 2 : La version minimale de l'application Paramètres d'appel WebView prise en charge est 1.7.5.

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

6.1.31 Connexion/déconnexion au centre d'appels / File d'attente d'appels

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

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

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_CENTER_WXT%	false	vrai, faux	Active le support du centre d'appels.

Informations confidentielles de Cisco

6.1.32 Racine XSI et chemins d'accès

L'Webex du client Cisco BroadWorks utilise les balises suivantes pour contrôler la racine XSI, les actions et le chemin d'événements s'ils doivent être configurés différemment de ceux utilisés pour la connexion.

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

Les chemins d'accès aux événements et aux actions sont généralement modifiés en raison des exigences de personnalisation afin de supprimer la référence de *domaine com.broadsoft* des chemins d'URL des requêtes HTTP XSI effectuées par le client.

```
<config>
<Protocols><xsi>
       <chemins>
              <racine>%XSI_ROOT_WXT%</racine>
              <actions>%XSI_ACTIONS_PATH_WXT%</actions>
              <événements>%XSI_EVENTS_PATH_WXT%</événements>
       </chemins>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%XSI_ROOT_WXT%	Continue d'utiliser l'original utilisé pour la récupération de la configuration.	Chaîne d'URL	Racine XSI pour toutes les opérations XSI. Exemple : https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	chaîne	Spécifie le chemin d'accès des actions XSI. Il doit commencer et finir par « / » et contenir uniquement le contexte des actions. Exemple : /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	chaîne	Spécifie le chemin d'accès des événements XSI. Il doit commencer et finir par « / » et contenir uniquement le contexte des événements. Exemple : /com.domain.xsi-events/

6.1.33 Canal d'événements XSI

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

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

Informations confidentielles de Cisco

La pulsation des événements XSI est utilisée pour maintenir le canal d'événements XSI ouvert et l'intervalle de pulsation peut être spécifié à l'aide du paramètre suivant.

```
<config>
<Protocols><xsi>
<event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
    <Intervalle de battement > %CHANNEL_HEARTBEAT_WXT%</Intervalle de battement>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_XSI_EVENT_ CHANNEL_WXT%	Vrai	vrai, faux	Contrôle si le canal d'événements XSI est activé. Il doit être réglé sur "true" pour recevoir, par exemple, les événements de service de contrôle en cours d'appel. La valeur recommandée est "true".
%CHANNEL_HEARTBEAT_ WXT%	10000	nombre	Il s'agit du battement de cœur du canal d'événement XSI (en millisecondes). La valeur par défaut est "10 000".

6.1.34 Configuration des codecs

Webex pour Cisco BroadWorks propose 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 la priorité d'attribut *XML,* qui est une valeur comprise entre 0,0 (la plus basse) 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)
  - LPMC (G.711A)
  - iLBC
  - Codec IA
- Vidéo
  - H.264

Informations confidentielles de Cisco

```
<config>
<services><appels>
  <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"/>
    …
  <vidéo>
    <codecs>
      <codec name="H264" payload="109" resolution="CIF" framerate="25"
bitrate="768000" priority="1.0">
        <mode-paquet>0</mode-paquet>
```

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

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

Résolution	Taille de la vidéo *	FPS (images par seconde)	Valeurs de débit binaire par défaut par résolution et FPS
SUBQCIF	128 x 96	15	128000
Le	176 x 144	30	192000
CIF	352 x 288	15	384000
CIF	352 x 288	30	768000
VGA	640 x 460	15	2000000
4CIF	704 x 576	25	2000000
HD	960 x 720	30	2000000

***** Résolution vidéo maximale annoncée. La résolution vidéo réelle pendant un appel entre deux Webex pour les clients Cisco BroadWorks dépend des capacités des deux clients – elle sera la plus basse des deux et sera la même pour les deux clients.

La résolution vidéo d'un appel vidéo est négociée lors de la configuration de session et dépend des capacités des deux terminaux. La résolution d'appel vidéo est la même sur les deux terminaux. Ainsi, si les Webex des terminaux Cisco BroadWorks ont des capacités différentes (et prennent donc en charge des résolutions différentes), la résolution la plus basse est négociée pour l'appel. La résolution vidéo peut changer lors d'un appel si les conditions du réseau se détériorent. Dans ce cas, les deux terminaux mobiles peuvent utiliser des résolutions vidéo différentes.

Informations confidentielles de Cisco

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

La configuration d'événements téléphoniques, simples ou multiples, est également prise en charge. Lors de la négociation de codecs, 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 le taux d'échantillonnage du codec audio négocié, alors cet événement téléphonique est sélectionné. Sinon, le premier événement téléphonique de la liste est utilisé.

Si au moins un événement téléphonique est négocié, les multifréquences à deux tonalités (DTMF) sont envoyées sous forme de paquets RTP en utilisant le type de charge utile correspondant. Et s'il n'y a aucun événement téléphonique 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 48 kbps est négocié, l'événement téléphonique avec la charge utile 101 est utilisé.

6.1.34.1 Codec IA

À partir de la version 44.8, l'application Webex introduit la prise en charge d'un nouveau codec audio – AI Codec (xCodec). Ce codec audio est utilisé dans des conditions réseau défavorables pour obtenir une meilleure qualité d'appel. Le Webex Media Engine de l'application Webex vérifie les capacités de l'appareil, suit la qualité du support et le codec AI peut être utilisé s'il est pris en charge et activé via le fichier de configuration.

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

6.1.35 Composition 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, cette opération n'est pas souhaitable et ces appels doivent être bloqués.

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

Cette option est prévue dans la configuration suivante.

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


Informations confidentielles de Cisco

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	Vrai	vrai, faux	Indique si l'URI-SIP doit être acheminé via Locus (vrai) ou bloqué (false).

6.1.36 Historique des appels sur tous les périphériques

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

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	vrai, faux	Indique si l'application doit utiliser l'historique des appels unifié ou côté client (local).

6.1.37 Désactivation des appels vidéo

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

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

- l'utilisateur ne voit pas le paramètre "Accepter les appels entrants avec ma vidéo activée"
- Tous les appels vidéo entrants, s'ils sont acceptés, seront des appels audio
- L'utilisateur ne sera pas en mesure de faire remonter un appel en vidéo et les escalades vidéo seront automatiquement rejetées.

Lorsque les appels vidéo sont activés, une nouvelle propriété de configuration est ajoutée pour contrôler la valeur par défaut du paramètre "Accepter les appels entrants avec ma vidéo activée". Par défaut, cette fonctionnalité est activée pour les ordinateurs de bureau et désactivée pour les appareils mobiles et les tablettes.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_SIP_VIDEOCALLS_WXT%	Vrai	vrai, faux	Contrôle la disponibilité des appels vidéo SIP via BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	Vrai	vrai, faux	Contrôle la disponibilité des appels vidéo Locus (gratuits).
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Ordinateur de bureau - true Mobile / Tablette - faux	Vrai, faux	Contrôle la valeur par défaut du paramètre "Accepter les appels entrants avec ma vidéo activée".

6.1.38 Appel d'urgence (911) - Établissement de rapports de localisation avec le fournisseur E911

Le client de Webex de bureau et de tablette prend en charge les rapports de localisation E911 à l'aide de RedSky, Intrado ou Bandwidth comme fournisseur d'appels d'urgence E911 pour le déploiement de Webex pour BroadWorks. Le fournisseur E911 fournit une prise en charge de localisation par appareil (pour Webex applications de bureau et tablettes et les périphériques MPP compatibles HELD) et un réseau qui achemine les appels d'urgence vers les centres d'appels de la sécurité publique (PSAP) aux États-Unis, sur ses territoires (Guam, Porto Rico et îles Vierges) et au Canada uniquement. Le service est activé par emplacement.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	false	Vrai, faux	Active la plate-forme de localisation d'urgence du fournisseur E911.
%BWE911-PRIMAIRE-HELDURL%	vide	chaîne	Indique l'URL vers la plate-forme de localisation d'urgence du fournisseur E911 prenant en charge le protocole HELD.
%BWE911-IDCLIENT% ;	vide	chaîne	L'ID client (HeldOrgId, CompanyID) utilisé pour la requête HTTPS du fournisseur E911.
%BWE911-CLÉSECRÈTE%	vide	chaîne	Le secret pour authentifier la demande HTTPS du fournisseur E911.
%BWE911-LISTE-DES-NUMÉROS-D'URGENCE%	vide	CSV chaîne	Liste des numéros d'urgence pris en charge par le fournisseur E911.
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (l'utilisateur ne sera pas invité à nouveau)	nombre [0 - 43200]	Le délai en minutes qui sera utilisé pour rappeler à l'utilisateur de mettre à jour l'emplacement d'urgence si l'emplacement actuel n'est pas entré ou n'est pas valide. La valeur suggérée s'il est décidé d'activer : 1440 (un jour).

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (l'utilisateur peut toujours annuler la boîte de dialogue)	nombre [-1 - 100]	Heures pendant lesquelles l'utilisateur est autorisé à fermer la boîte de dialogue d'emplacement avant que l'emplacement ne devienne obligatoire (c'est-à-dire qu'il ne peut pas fermer la fenêtre d'emplacement). Valeurs possibles : ▪ N = -1 (l'utilisateur peut toujours annuler la boîte de dialogue) ▪ N = 0 (l'utilisateur n'est pas autorisé à annuler la boîte de dialogue - emplacement obligatoire toujours) ▪ N > 0 (l'utilisateur est autorisé à annuler la boîte de dialogue N fois avant qu'elle ne devienne obligatoire)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	agressif, once_per_login	once_per_login	Définit le comportement de l'invite de localisation E911. La valeur "agressif" montrera la boîte de dialogue à l'utilisateur sur 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 d'autres fenêtres contextuelles et distractions pour l'utilisateur.

REMARQUE 1 : Les balises BWE911-*** sont des "balises système intégrées dynamiques". Pour plus d'informations, reportez-vous à la section *5.7 Balises système intégrées dynamiques Cisco BroadWorks*.

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

6.1.39 PAI comme identité

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

Si l'attribut enabled de la balise <use-pai-as-calling-identity> est défini sur "true", l'en-tête PAI est utilisé avec priorité sur l'en-tête From. 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.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	vrai, faux	Indique si l'identité appelante présentée à l'utilisateur doit être extraite des en-têtes SIP De ou SIP P-Asserted-Identity. Définissez la valeur "true" pour utiliser l'en-tête PAI avec priorité.

6.1.40 Désactiver le partage d'écran

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

- L'utilisateur ne voit pas l'option permettant de lancer le partage d'écran lors des appels 1-1
- Les demandes entrantes de partage d'écran sont rejetées et un message d'information s'affiche.

Cette fonctionnalité est activée par défaut.

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

6.1.41 Indication d'appel de spam

Lorsque le basculement de la 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 en indiquant l'état de vérification des appels indésirables, s'ils sont reçus dans le cadre de la notification push NewCall ou des enregistrements de l'historique des appels.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	vrai, faux	Contrôle la disponibilité de l'indication d'appel de spam dans l'écran des appels entrants et l'historique des appels pour Webex Calling seulement.

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

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

Informations confidentielles de Cisco

La version 44.2 de l'application Webex introduit de nouvelles améliorations de Speech AI pour les appels PSTN à bande étroite.

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

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

```
<config>
   <services>
      <appels>
         <améliorations vocales activées="%ENABLE_SPEECH_ENHANCEMENTS_WXT%"/>
```

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

REMARQUE : la suppression du bruit fait désormais partie des améliorations vocales supplémentaires, et la balise <suppression du bruit> a été déconseillée par la nouvelle balise <améliorations de la parole>. La balise personnalisée Noise Removal %ENABLE_NOISE_REMOVAL_WXT% est également obsolète.

6.1.43 Marquage de l'DSCP QoS

Le marquage de la DSCP QoS est pris en charge par l'application Webex qui appelle des RTP des paquets multimédia (audio et vidéo). DSCP détermine la classification du trafic pour les données réseau. Ceci peut être utilisé pour déterminer quel trafic réseau nécessite une bande passante plus élevée, a une priorité plus élevée et est le plus susceptible de laisser tomber des paquets.

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

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	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 QoS pour le type QoS sélectionné pour les appels audio. Remarque : La valeur par défaut est utilisée, si aucune valeur n'est fournie ou si la valeur n'a pas pu être analysée correctement.
%ENABLE_VIDEO_QOS_WXT%	Vrai	Vrai, faux	Active la qualité de service pour les appels vidéo
%VIDEO_QOS_VALUE_WXT%	34	0-63	Spécifie la valeur QoS pour le type de Qualité de service (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 correctement.

6.1.44 Profil principal

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, plusieurs profils du même type peuvent être configurés pour l'utilisateur. Pour sélectionner le profil correct pour se connecter aux services téléphoniques, Cisco BroadWorks a été amélioré pour indiquer si un utilisateur possède un périphérique, c'est-à-dire si la ligne/le port principal d'un périphérique lui est affecté. Pour plus d'informations sur la mise à jour de Cisco BroadWorks, cochez la case Indicateur de propriétaire dans la liste des périphériques pour prendre en charge Webex lignes partagées client.

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

Informations confidentielles de Cisco

À partir de la version 43.2, une nouvelle option de configuration (*restriction* du propriétaire de l'appareil) est ajoutée pour contrôler si la restriction du profil principal doit être appliquée. Il permet à l'application Webex d'utiliser un profil de ligne/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 de propriété du périphérique est activée et qu'aucun périphérique n'est doté de la ligne/du port principal pour la plate-forme correspondante, les services téléphoniques ne se connecteront** pas).

La même restriction s'applique aux appareils que l'utilisateur peut associer dans l'application de bureau Webex. L'utilisateur ne peut voir et coupler qu'avec les appareils qu'il possède. Cela empêche le couplage avec les périphériques d'un autre utilisateur auquel une ligne partagée ou virtuelle est affectée. La valeur du même paramètre de configuration s'applique également à cette restriction.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	Vrai	vrai, faux	Contrôle la restriction du propriétaire de l'appareil – si les Services téléphoniques doivent utiliser le profil principal pour l'appareil donné

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

6.1.45 Liste de contacts bloqués (Webex Calling seulement)

À partir de 43.5, l'application Webex introduit une liste de blocs de numéros de téléphone définie par l'utilisateur. Si la fonctionnalité est activée, l'utilisateur peut spécifier les appels entrants provenant de numéros spécifiques à bloquer côté serveur et non à remettre sur ses périphériques. Les appels bloqués sont visibles dans l'historique des appels.

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

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

Informations confidentielles de Cisco

- Format de nombre
  - Le blocage à partir de l'application Préférences d'appel s'applique E.164 restriction de format localement dans l'application Webex
  - Le blocage à partir de l'historique des appels est autorisé pour tous les enregistrements de Webex Calling
  - Cisco BroadWorks peut autoriser ou rejeter les demandes de nouveaux numéros ajoutés à la liste des contacts bloqués en fonction du format du numéro
- 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 contacts bloqués définie par l'utilisateur est configurée sur Cisco BroadWorks et s'applique à tous les périphériques WxC de l'utilisateur. Cette fonctionnalité fonctionne avec la liste de blocage définie par l'administrateur, qui n'est pas configurable par l'utilisateur et ne peut être contrôlée que par les administrateurs via Control Hub. Il n'y a AUCUN enregistrement d'historique d'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 les stratégies STIR/SHAKEN, de liste de blocage définie par l'administrateur et de rejet d'appel anonyme.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_BLOCK_WXT%	Vrai	vrai, faux	Active la liste de contacts bloqués définie par l'utilisateur réglé sur "true", pour afficher la liste de blocage dans les préférences d'appel et l'historique des appels

REMARQUE : cette fonctionnalité dépend du service de blocage d'appel Cisco BroadWorks affecté à l'utilisateur.

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

6.1.46.1 Adaptation tarifaire

L'application Webex a déjà intégré des techniques de qualité multimédia adaptative pour garantir que l'audio n'est pas affecté par une perte de paquets vidéo et pour s'assurer que la vidéo peut tirer parti de l'adaptation du débit vidéo pour gérer la quantité de bande passante utilisée pendant les périodes de congestion.

Informations confidentielles de Cisco

L'adaptation du débit ou les ajustements dynamiques du débit binaire adaptent le débit d'appel à la bande passante variable disponible, en accélérant ou en accélérant le débit binaire vidéo en fonction de la condition de perte de paquets. Un point de terminaison réduit le débit binaire lorsqu'il reçoit des messages du récepteur indiquant qu'il y a une perte de paquets ; et une fois que la perte de paquets a diminué, une accélération du débit binaire se produit.

Il n'existe aucun paramètre configurable pour contrôler l'utilisation du mécanisme d'adaptation de débit.

6.1.46.2 Correction d'erreurs de renvoi (FEC) et RTX (Packets Retransmission)

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

FEC assure la redondance des informations transmises à l'aide d'un algorithme prédéterminé. La redondance permet au destinataire de détecter et de corriger un nombre limité d'erreurs, sans avoir besoin de demander à l'expéditeur des données supplémentaires. FEC donne au récepteur la possibilité 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 détriment d'une bande passante de canal de transfert fixe plus élevée (plus de paquets envoyés).

Les terminaux n'utilisent pas FEC sur des bandes passantes inférieures à 768 kbps. En outre, il doit également y avoir au moins 1,5 % de perte de paquets avant l'introduction du FEC. Les critères d'évaluation surveillent généralement l'efficacité de la FEC et si la FEC n'est pas efficiente, elle n'est pas utilisée.

FEC consomme plus de bande passante que la retransmission mais a moins de retard. RTX est utilisé lorsque de petits délais sont autorisés et qu'il existe des contraintes de bande passante. En cas de retard important et de bande passante suffisante, le FEC est préférable.

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

Le FEC doit être activé pour que RTX soit activé.

```
<config><services><appels>
<audio>
       <amélioration de la qualité audio>
              <Mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <charge utile>111</charge utile>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            < m>8</m>
                            <multi_ssrc>1</multi_ssrc>
                            <non_seq>1</non_seq>
```


Informations confidentielles de Cisco

```
                        < commentaires >0</commentaires>
                        <Commande>FEC_SRTP</Commande>
                </FEC>
                <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                        <mari-rtx>90000</mari-rtx>
                        <charge utile>112</charge utile>
                        <heure >180</heure>
                        <Flux de données>1</flux de données>
                        <Commande>RTX_SRTP</Commande>
                </rtx>
        </mari>
...
<vidéo>
        <amélioration de la qualité vidéo>
        <Mari>
                <fec enabled="%ENABLE_VIDEO_MARI_FEC_WXT%">
                        <x-ulpfecuc>8000</x-ulpfecuc>
                        <charge utile>111</charge utile>
                        <max_esel>1400</max_esel>
                        <max_n>255</max_n>
                        < m>8</m>
                        <multi_ssrc>1</multi_ssrc>
                        <non_seq>1</non_seq>
                        < commentaires >0</commentaires>
                        <Commande>FEC_SRTP</Commande>
                </FEC>
                <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                        <mari-rtx>90000</mari-rtx>
                        <charge utile>112</charge utile>
                        <heure >180</heure>
                        <Flux de données>1</flux de données>
                        <Commande>RTX_SRTP</Commande>
                </rtx>
        </mari>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_AUDIO_MARI_FEC_WXT%	false	vrai, faux	Active 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 FEC pour les appels vidéo
%ENABLE_VIDEO_MARI_RTX_WXT%	false	vrai, faux	Active RTX pour les appels vidéo (nécessite d'activer le FEC vidéo)

6.1.47 Appels simultanés avec le même utilisateur

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

Informations confidentielles de Cisco

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

```
<config>
   <services>
      <appels>
         <appels-simultanés-avec-le-même utilisateur
activé="%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%"/>
```

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

6.1.48 RTCP-XR

À partir de la version 43.8, Webex'application ajoute la négociation pour l'échange de paquets RTCP-XR pendant un appel. La négociation a lieu lors de l'établissement de la session SIP INVITE. Si les deux terminaux prennent en charge des paquets RTCP-XR, Webex Media Engine commencera à échanger ces paquets et contribuera au mécanisme adaptatif de qualité des appels. Cette fonctionnalité est activée par défaut.

De plus, pour Webex Calling uniquement, ces métriques supplémentaires seront envoyées via le SIP BYE et ainsi exposées dans Control Hub.

```
<config>
<Protocols><SIP>
   <rtcp-xr>
      <négociation activée="%ENABLE_RTCP_XR_NEGOTIATION_WXT%"/>
```

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

Informations confidentielles de Cisco

6.1.49 Informations sur le renvoi d'appels

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

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	Vrai	vrai, faux	Contrôle la visibilité des informations de renvoi et de redirection des appels. Réglez sur "true", pour afficher les informations dans les écrans liés aux appels et dans l'historique des appels.

6.1.50 Afficher l'ID de l'appelant

6.1.50.1 ID appelant sortant

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

- Ligne directe (par défaut)
- Numéro d'emplacement
- Numéro personnalisé de la même organisation
- Files d'attente d'appels dont fait partie l'utilisateur, ce qui permet aux agents d'utiliser le numéro d'identification de leur appelant.
- Groupes de recherche dont fait partie l'utilisateur, ce qui permet aux agents d'utiliser le numéro d'identification de leur appelant
- Masquer l'ID de l'appelant

Remarques :

- La liste des options dépend de la ligne :
  - Ligne principale – ensemble complet d'options
  - Lignes partagées – non disponibles
  - Lignes virtuelles – options de file d'attente d'appels uniquement
- Si l'identité déjà sélectionnée n'est plus disponible, l'ID d'appelant par défaut de l'utilisateur est utilisé
- 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>

Informations confidentielles de 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><appels>
   <id_appelant>
      <appels-sortants activés="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
         <nombres-supplémentaires activés="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
         <centre d'appels activé="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
         <groupe-recherche activé="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
         <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
      </appels sortants>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	vrai, faux	Permet d'activer 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 de centre d'appels (DNIS) configurés pour l'utilisateur.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	vrai, faux	Contrôle la disponibilité des numéros de groupe de recherche configurés pour l'utilisateur.
"%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	vrai, faux	Permet d'activer le blocage de la remise de l'ID de l'appelant comme sélection pour les appels sortants.

REMARQUE : la version 44.3 de l'application de bureau prend uniquement en charge la 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 ou du lancement d'un appel, Cisco BroadWorks envoie le nom d'affichage de l'interlocuteur distant dans SIP INVITE. Il est utilisé par défaut par l'application Webex. Dans le même temps, l'application Webex démarre la résolution des contacts par rapport à plusieurs sources, avec la priorité suivante :

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

Informations confidentielles de Cisco

Si le contact est parvenu à être résolu par l'une des sources de recherche, le nom d'affichage de l'interlocuteur distant est mis à jour. De plus, si le contact se trouve dans CI, la session d'appel est liée aux services cloud Webex du même utilisateur, offrant la possibilité de voir l'avatar et la présence de l'interlocuteur distant, d'avoir un chat, un partage d'écran, la possibilité de passer à une réunion cloud Webex, etc.

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

```
<config>
<services><appels>
   <id_appelant>
      <nom_distant>
         <mode machine="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	résolu	Résolu, SIP	Contrôle le nom d'affichage de l'interlocuteur distant pour les espaces de travail et les périphériques RoomOS. Utilisez "sip" pour ignorer la résolution du contact et utilisez le nom d'affichage reçu dans la session SIP INVITE.

Informations confidentielles de Cisco

6.1.51 Multiligne

L'utilisateur Webex peut disposer d'une ligne principale et de 9 lignes secondaires maximum. Les lignes secondaires peuvent être partagées ou virtuelles (Webex appel uniquement).

Webex'application obtient la configuration de la ligne via le fichier de configuration DMS qui est téléchargé à la connexion et toutes les 12 heures. Si une mise à jour de la configuration de ligne est détectée, l'utilisateur est invité à redémarrer l'application pour appliquer les modifications. La reconnexion de l'utilisateur détecte et applique immédiatement les mises à jour de configuration de ligne.

Ce qui suit décrit la section du modèle de configuration DMS relative à la prise en charge multiligne pour Desktop et Mobile.

```
<config>
<protocoles>
   <gorgée>
       <lignes multilignes-enabled="%ENABLE_MULTI_LINE_WXT%">
          < personnel >
             <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
          </personnel >
          <line lineType="%BW-MEMBERTYPE-1 %">
             <id-externe>%BWUSEREXTID-1 %</id-externe>
             ...
          </ligne>
          <line lineType="%BW-MEMBERTYPE-2 %">
             <id_externe>%BWUSEREXTID-2 %</id-externe>
             ...
          </ligne>
          ...
          <line lineType="%BW-MEMBERTYPE-10 %">
             <id_externe>%BWUSEREXTID-10 %</id-externe>
             ...
          </ligne>
```

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_MULTI_LINE_WXT%	faux	Vrai, faux	Active la prise en charge de plusieurs lignes (si configuré). S'il est désactivé (défini sur "false"), seule la première ligne configurée sera utilisée par l'application.

REMARQUE 1 : La fonction de support Boss-Admin (Executive-Assistant) n'est pas disponible en combinaison avec la configuration multiligne.

REMARQUE 2 : Voir 'Apparence de la ligne partagée' dans le Webex-for-Cisco-BroadWorks-Solution-Guide pour connaître les exigences supplémentaires de BroadWorks.

Informations confidentielles de Cisco

6.1.51.1 Bureau - Apparence de ligne partagée

À partir de la version 42.12, Webex application ajoute la prise en charge des lignes partagées. L'administrateur doit configurer les apparences d'appels partagés pour chaque ligne partagée.

Version 43.12, l'application Webex est améliorée pour permettre le déplacement (reprise localement) d'un appel en attente sur une ligne partagée ou virtuelle, traité par un autre utilisateur ou par le même utilisateur sur un autre appareil. Pour plus d'informations, vérifiez *6.2.13 Déplacer l'appel*.

6.1.51.2 Bureau - Lignes virtuelles (Webex Calling uniquement)

Pour Webex Calling déploiement uniquement, Webex application prend en charge la configuration multiligne à l'aide de lignes virtuelles. D'un point de vue fonctionnel, la configuration avec les lignes virtuelles correspond à celle des lignes partagées utilisant des lignes partagées – ayant la possibilité de voir les lignes virtuelles configurées pour l'utilisateur et de les utiliser pour les appels entrants et sortants.

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.

Version 43.12, l'application Webex est améliorée pour permettre le déplacement (reprise localement) d'un appel en attente sur une ligne partagée ou virtuelle, traité par un autre utilisateur ou par le même utilisateur sur un autre appareil. Pour plus d'informations, vérifiez *6.2.13 Déplacer l'appel*.

6.1.51.3 Mobile (Webex Calling uniquement)

Pour Webex Calling déploiement 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 est applicable aux applications de Webex de bureau et mobile.

En raison des spécificités de la plate-forme mobile, l'utilisateur peut avoir jusqu'à deux appels simultanés en même temps sur n'importe quelle ligne.

> **REMARQUE 1** : Si l'appel avec numéroteur natif est activé (voir *6.3.5.1 Appel avec numéroteur natif*), le multiligne est désactivé.
>
> **REMARQUE 2** : Multi-line pour la version tablette n'est pas pris en charge.

6.1.52 Autorisation SIP étendue

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 stockera l'autorisation et la réutilisera jusqu'à ce qu'elle soit encore valide.

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

Informations confidentielles de Cisco

```
<config>
<protocoles>
  <gorgée>
    <autorisation étendue activée="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	vrai, faux	Lorsque la valeur "true" est activée, l'amélioration de l'autorisation SIP est activée.

REMARQUE 1 : Certains SBC peuvent nécessiter une nouvelle autorisation SIP à chaque session, cette fonctionnalité doit donc être utilisée en fonction des spécificités du déploiement.

REMARQUE 2 : Même si cette fonctionnalité est activée, si l'application Webex reçoit 401 Non autorisé, une nouvelle autorisation sera utilisée dans la prochaine requête SIP.

6.1.53 Assistant personnel (absent)

Avec la version 44.11, l'application Mobile Webex et la version 45.3, l'application Desktop Webex, ajoute l'intégration avec le service Cisco BroadWorks Personal Assistant (PA). Il fonctionne en combinaison avec la présence Absent de l'utilisateur et nécessite la synchronisation de l'état PA avec la présence Webex Cloud.

Le service de sonorisation permet à l'utilisateur d'informer les appelants de la raison pour laquelle l'appelé n'est pas disponible, éventuellement de savoir quand l'appelé reviendra et s'il y a un Attendant pour traiter l'appel.

Si le sonorisation est activé, l'option de présence absente sera disponible pour l'utilisateur. Elle peut être utilisée pour configurer le PA côté Cisco BroadWorks. Lorsque la fonctionnalité est activée, les utilisateurs voient la présence Absent de l'utilisateur associée à l'état de sonorisation et à la durée configurée.

L'utilisateur ne peut configurer que la configuration manuelle de PA. Si des horaires affectent le service de sonorisation, l'état de présence sera mis à jour via la synchronisation de l'état de l'assistant personnel. Toutefois, l'application Webex n'expose pas la configuration des planifications et les planifications qui affectent l'AP.

```
<config>
<services>
  <assistant-personnel activé="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	vrai, faux	Contrôle si l'utilisateur peut disposer de la fonctionnalité Absent pour l'absence.

REMARQUE 1 : cette fonctionnalité nécessite que la synchronisation de l'état de Personal Assistant soit activée à partir du Partner Hub.

REMARQUE 2 : Le routage standard des appels de l'assistant personnel ne prendra pas effet tant que les services NPD, Renvoi d'appels toujours ou Renvoi d'appels sélectifs sont actifs.

REMARQUE 3 : Les états de présence manuels Ne pas déranger et Occupé ont une priorité plus élevée que Absent. Lorsque le manuel d'utilisation 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 Absent.

Informations confidentielles de 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 de n'autoriser que l'une d'entre elles à être en ligne à la fois. Lorsque Cisco BroadWorks notifie au client de se déconnecter, la connexion SIP est interrompue et le client indique que l'appel n'est pas connecté.

Cette fonctionnalité est nécessaire dans certains déploiements où des clients similaires peuvent être en ligne en même temps, ce qui provoque des effets secondaires. Par exemple, un utilisateur ayant un ordinateur de bureau au travail et à la maison, où les appels entrants ne sont reçus que par un seul client, selon l'enregistrement SIP actif.

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

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

Pour obtenir des informations sur les correctifs et versions Cisco BroadWorks nécessaires à cette fonctionnalité, reportez-vous à la section sur la configuration logicielle requise pour Cisco BroadWorks dans le *Webex du guide* de la solution Cisco BroadWorks.

Pour plus de détails sur la configuration, reportez-vous à l'exemple suivant (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 si omis	Valeurs prises en charge	Description
%ENABLE_FORCED_ LOGOUT_WXT%	false	vrai, faux	Active la déconnexion forcée.
%FORCED_LOGOUT_ APPID_WXT%	vide	chaîne	Appid utilisé côté serveur pour la corrélation. Il peut s'agir de n'importe quelle chaîne. Exemple : "123abc"

6.2.2 Interception d'appel

L'interception d'appels est un service multi-utilisateurs qui permet aux utilisateurs sélectionnés de répondre à n'importe quelle ligne qui sonne au sein de leur groupe d'interception d'appels. Un groupe d'interception d'appels est défini par l'administrateur et est un sous-ensemble des utilisateurs du groupe qui peuvent intercepter les appels des autres.

Informations confidentielles de Cisco

Les cas d'interception suivants sont pris en charge :

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

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	vrai, faux	Sélectionnez la valeur "true" pour activer l'interception aveugle des appels.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	vrai, faux	Réglez la valeur "true" pour activer l'interception d'appels dirigée.

6.2.3 Support Boss-Admin (assistante de direction)

La fonction Boss-Admin, connue sous le nom d'assistant exécutif sur Cisco BroadWorks, permet à un assistant d'agir pour le compte d'un cadre pour filtrer les appels, répondre et passer des appels en tant que "cadre". Un assistant peut avoir plusieurs cadres et il est possible de :

- Sélectionnez le rôle souhaité lors du passage d'un appel.
- Répondre à un appel entrant au nom d'un dirigeant, puis transmettre l'appel à l'exécutif. En plus de cela, toutes les options de gestion d'appel habituelles sont disponibles.
- Veillez à ce qu'un appel entrant soit en fait destiné à l'exécutif.

Executive et Executive-Assistant sont deux services Cisco BroadWorks interdépendants qui, ensemble, offrent les fonctionnalités suivantes :

- Un utilisateur doté du service exécutif peut définir un groupe d'assistants chargés de gérer ses appels. Les assistants doivent être sélectionnés parmi les utilisateurs d'un même groupe ou d'une même entreprise auxquels est affecté le service d'assistant exécutif.
- Un utilisateur doté du service Executive-Assistant peut répondre à des appels et passer des appels au nom de ses collaborateurs.
- Le cadre et leurs assistants peuvent spécifier quels appels doivent être transférés aux assistants, comment les assistants doivent être alertés des appels entrants et lesquels des appels transmis aux assistants doivent être présentés au cadre pour filtrage.

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


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	vrai, faux	Réglez sur "true" pour activer la fonctionnalité Boss-Admin.

REMARQUE : La fonction de support Boss-Admin (Executive-Assistant) n'est pas disponible en combinaison avec Shared-Lines.

6.2.4 Transfert des appels SIP à la réunion (Webex Calling uniquement)

Le client fournit la fonctionnalité permettant de faire remonter un appel SIP en cours vers une réunion via Webex Calling. En utilisant cette fonctionnalité à la place d'une conférence ad hoc standard, l'utilisateur sera en mesure d'utiliser la vidéo ainsi que le partage d'écran pendant la réunion.

```
<config>
<services><appels>
       <remonter-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	vrai, faux	Réglez la valeur "true" pour activer l'option de menu Passer à Webex réunion.

6.2.5 Contrôle du téléphone de bureau - Réponse automatique

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

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

La réponse automatique peut fonctionner sur les périphériques principaux et non principaux. Si l'utilisateur dispose de plusieurs téléphones de bureau enregistrés avec lesquels il peut être jumelé, seul le périphérique sélectionné ou jumelé doit répondre automatiquement.

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


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	Vrai	vrai, faux	Lorsque la valeur "true" est activée, cette option permet d'activer la réponse automatique du contrôle du téléphone de bureau.

REMARQUE : la réponse automatique n'affecte pas les appels entrants lorsque vous êtes en mode DPC, de sorte que le téléphone de bureau sonne pour les appels entrants.

6.2.6 Réponse automatique avec notification par tonalité

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_AUTO_ANSWER_WXT%	false	vrai, faux	Lorsque ce paramètre est réglé sur "true", active la réponse automatique aux appels entrants si cela est demandé au serveur principal.

6.2.7 Contrôle de téléphone de bureau - Contrôles à mi-appel - Conférence

Cette fonctionnalité active les options Conférence et Fusion pour les appels distants (XSI) terminés sur un autre site.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	vrai, faux	Lorsque la valeur "true" est activée, active les options Conférence et Fusion pour les appels distants (XSI), terminés à un autre emplacement.

6.2.8 Notifications d'interception d'appels

Les notifications d'interception d'appel permettent à l'utilisateur de savoir s'il y a un appel entrant pour un utilisateur qu'il est configuré pour surveiller. Les notifications d'interception d'appels peuvent être reçues pour les listes de surveillance configurées par le biais des services de groupe d'interception d'appels et de supervision de ligne occupée.

Informations confidentielles de Cisco

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

6.2.8.1 Supervision de ligne occupée

L'application Webex de bureau affiche une notification si un membre de sa liste de suivi de supervision de ligne occupée (BLF) a un appel entrant en état d'alerte. La notification contient des informations sur l'appelant et l'utilisateur qui a reçu l'appel entrant, avec des options pour intercepter l'appel, désactiver ou ignorer la notification. Si l'utilisateur répond à un appel entrant, cette personne intercepte l'appel dirigé.

Depuis la version 43.4, la liste des utilisateurs surveillés par FLO est disponible dans la fenêtre d'appels multiples (MCW) pour les appels (disponible uniquement pour Windows). L'intégration de la liste des BLF dans le MCW comprend :

- Surveillez les appels entrants en utilisant la possibilité de décrocher l'appel ou d'ignorer l'alerte.
- Voir la liste complète des utilisateurs du BLF.
- Surveillez la présence des utilisateurs – la présence riche n'est disponible que pour les utilisateurs disposant de Webex droit Cloud. La présence de base (téléphonique) n'est disponible que pour les utilisateurs de BroadWorks.
- Commencez un appel avec un utilisateur BLF.
- Démarrez une discussion avec un utilisateur BLF – disponible uniquement pour les utilisateurs disposant de droits Webex Cloud.
- Ajoutez un utilisateur BLF en tant que contact.

```
<config>
  <services>
    <appels>
      <occupé-lampe-champ enabled="%ENABLE_BUSY_LAMP_FIELD_WXT%">
        <display-caller enabled="%ENABLE_BLF_DISPLAY_CALLER_WXT%"/>
        <notification-delaytime="%BLF_NOTIFICATION_DELAY_TIME_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	vrai, faux	Permet d'activer la surveillance de l'affichage de ligne occupée et la notification de sonnerie pour les autres utilisateurs qui peuvent intercepter des appels.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	Vrai	vrai, faux	Permet d'afficher le nom/numéro affiché de l'appelant dans la notification qui sonne.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Contrôle le délai (en secondes) pendant lequel la notification de sonnerie doit être affichée à l'utilisateur.

Informations confidentielles de Cisco

REMARQUE : cette fonction dépend du service d'interception d'appels dirigé.

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

À partir de la version 44.2, Webex application ajoute la prise en charge des notifications d'interception d'appels de groupe (GCP) pour le déploiement de Webex Calling. Elle permet aux utilisateurs d'être avertis des appels entrants pour n'importe lequel des utilisateurs surveillés par l'intermédiaire du groupe d'interception d'appels.

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

Si plusieurs appels sont passés au sein du même groupe d'interception d'appels, ils sont traités de manière séquentielle en fonction de l'heure à laquelle ils sont reçus. La notification de l'appel le plus ancien est initialement transmise au groupe et, une fois traitée, la notification suivante en ligne est envoyée au groupe.

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

L'utilisateur peut désactiver le son de la notification GCP via les paramètres de l'application. Ce paramètre s'applique à toutes les notifications d'interception d'appels (BLF et GCP) et, par défaut, les notifications sont désactivées.

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

Informations confidentielles de Cisco

```
<config>
<services><appels>
    <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>
    <lignes>
        <ligne>
            <interception-appels-groupe>%INTERCEPTION D'APPELS-GROUPE-BOOL-
1 %</interception-appels-groupe>
            ...
        </ligne>
        <ligne>
            <interception d'appels-groupe>%INTERCEPTION D'APPELS-GROUPE-BOOL-
2 %</interception d'appels-groupe>
            ...
        </ligne>
        ...
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	vrai, faux	Active les notifications d'interception d'appels de groupe
%ENABLE_GCP_DISPLAY_CALLER_WXT%	Vrai	vrai, faux	Permet d'afficher le nom/numéro affiché de l'appelant dans la notification qui sonne
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5-120	Définit la durée maximale pendant laquelle une notification GCP est disponible pour l'utilisateur
%BWGROUP-CALL-PICKUP-BOOL-n%	false	vrai, faux	Indique si le groupe d'interception d'appels est configuré sur la ligne correspondante

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

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

6.2.9 Forfait d'événements télécommandés

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, lors de la réception d'un appel ou de la gestion de la mise en attente / reprise, l'application Webex honore désormais le package d'événements de contrôle à distance.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	faux	Vrai, faux	Lorsque ce paramètre est réglé sur "true", indique que la télécommande doit être activée pour l'utilisateur.

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

Lorsque des agents appellent leurs clients, ils souhaitent que ceux-ci voient l'ID de ligne appelante (CLID) approprié plutôt que leur CLID personnel/d'entreprise. Par exemple, si l'agent Mary Smith est joint à la file d'attente d'appels du support technique, lors de l'appel des clients, Marie souhaite que les clients voient sa CLID en tant que support technique, et non Marie Smith.

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%	faux	Vrai, faux	Active les appels sortants (sélection CLID) au nom de la file d'attente du centre d'appels.

6.2.11 Survivability Gateway (Webex Calling seulement)

À partir de la version 43.2, Webex'application ajoute la prise en charge du mode d'appel Survivability. si la fonctionnalité est activée et qu'il n'y a pas de connectivité Webex Cloud, l'application Webex peut fonctionner en mode de survie. Dans ce mode, la fonctionnalité d'appel disponible pour l'utilisateur est limitée.

Local Survivability Gateway est déployé par le client.

```
<config>
<protocoles>
<gorgée>
<survivability-gateway enabled="%ENABLE_SURVIVABILITY_GATEWAY_WXT% » fallback-
time="%SURVIVABILITY_FALLBACK_TIME_WXT%">%BWSURVIVABILITYGATEWAY%</survivability-
gateway>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	vrai, faux	Active la prise en charge du mode de survie.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Spécifie le temps de secours (passerelle de survie vers SSE)

REMARQUE : cette fonctionnalité vous donne confiance dans la migration des solutions d'appel sur site vers le Cloud.

6.2.12 Package d'événements de contrôle à distance du mode silencieux (Webex Calling uniquement)

Depuis la version 43.9, l'application Webex prend en charge le contrôle d'appel mis en sourdine à distance du flux multimédia audio. Cela permet de déclencher le mode silencieux/réactiver 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.

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

Le mode silencieux ou réactivé peut être déclenché localement ou à distance. La mise à jour à distance déclenche l'envoi d'un script SIP NOTIFY with *Event : mute* (ou *unmute*) 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 médias audio, renvoie un SIP NOTIFY avec Info-Package *:x-cisco-mute-status ; muted=true* (ou *muted=false*).

```
<config>
<services>
   <appels>
       <télécommande-sourdine activée="%ENABLE_REMOTE_MUTE_CONTROL_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	faux	Vrai, faux	Lorsque la valeur "true" est activée, le contrôle d'appel mis en sourdine à distance est activé pour l'utilisateur.

Informations confidentielles de Cisco

6.2.13 Déplacer l'appel

Webex'application permet de surveiller et de contrôler les appels des VoIP appels terminés à un autre endroit. Actuellement, cette option n'est disponible que pour la ligne principale de l'utilisateur.

À partir de la version 43.12, l'application Webex est améliorée pour afficher également les appels terminés à un autre emplacement 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 peut le déplacer vers le périphérique local en le sélectionnant et le reprendre à partir de l'écran d'appel. Ce mécanisme est utile si l'appel a été traité par le même utilisateur à un autre emplacement ou par un autre utilisateur utilisant la même ligne.

Remarque : il n'est pas possible dans l'application Webex de déplacer un appel en attente vers un périphérique associé. Si l'utilisateur est associé à un périphérique, il doit d'abord se déconnecter, puis il peut reprendre l'appel en attente localement.

La surveillance des appels des lignes partagée et virtuelle dépend du package d'événements d'informations d'appel SIP.

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

- Cas d'utilisation 1 :
    a. Alice a la ligne de Bob affectée aux profils de téléphone de bureau et de bureau.
    b. Alice a un appel avec Charlie via le téléphone de bureau - Alice peut voir l'appel en cours dans l'application de bureau.
    c. Alice met l'appel en attente à partir du téléphone de bureau – l'appel peut être repris par Alice à partir de l'application de bureau.
- Cas d'utilisation 2 :
    a. Alice a la ligne de Bob affectée aux 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 passe 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. Alice a la ligne de Bob affectée aux profils de téléphone de bureau et de bureau.
    b. Alice est jumelée avec son téléphone de bureau à partir de l'application Bureau.
    c. Bob a un appel avec Charlie – Alice peut voir l'appel en cours dans l'application de bureau.
    d. Bob met l'appel avec Charlie en attente – Alice ne peut pas reprendre l'appel avec Charlie à partir de l'application de bureau.

Informations confidentielles de Cisco

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

```
<config>
<services><appels>
    <Appeler-Déplacer>
         <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALL_MOVE_HERE_WXT%	faux	Vrai, faux	Active le déplacement de l'appel sur le périphérique local. Utilisé pour la mise en attente/reprise sur plusieurs sites/utilisateurs dans le cas d'utilisation multiligne.

Informations confidentielles de Cisco

6.3 Fonctionnalités réservées aux appareils mobiles

6.3.1 Appel d'urgence

Webex pour Cisco BroadWorks prend en charge les appels d'urgence natifs.

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

Les modes pris en charge sont les suivants :

- cs-only – Le client passe des appels d'urgence uniquement via le réseau cellulaire si le réseau est disponible.
- cs-first – Lors du lancement d'un appel d'urgence, le client vérifie le type de réseau auquel le périphérique actuel est connecté. Si le réseau cellulaire est disponible, le client passe 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. En outre, si l'appel d'urgence est passé via le réseau cellulaire, le client suggère à l'utilisateur de retenter l'appel d'urgence en tant que VoIP.
- VoIP uniquement – Le client ne passe les appels d'urgence que sous VoIP si le réseau de données cellulaires/WiFi est disponible.
- cs-voip – Le client analyse si le périphérique peut le lancer en tant qu'appel à commutation de circuits natif (CS) (sans tenir compte du fait que le réseau CS soit disponible ou non). Si l'appareil peut lancer un appel natif, le numéro d'urgence est composé en tant qu'appel CS d'urgence. Sinon, le numéro est composé comme VoIP.

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

Un message d'exclusion de responsabilité pour 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 si omis	Valeurs prises en charge	Description
%ENABLE_EMERGENCY_DIALING_WXT%	false	vrai, faux	Réglez la valeur "true" pour activer la détection des appels d'urgence. Aucune valeur par défaut n'est définie.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	CS uniquement	cs-only,cs-first,voip-only,cs-voip	Contrôle le mode séquence de numérotation pour les appels d'urgence.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	CSV liste	CSV liste des numéros d'urgence. Exemple : 911 112

6.3.2 Notifications push pour les appels

Lorsqu'un appel entrant est reçu, Mobile Client reçoit d'abord une notification Push (PN). Un paramètre config peut être utilisé pour contrôler le moment où 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. Cependant, par rapport au premier cas, cela ajoute un certain délai avant que l'appel ne soit établi.

Selon les exigences d'iOS 13, les NP de VoIP ne doivent être utilisés que pour les appels entrants. Les autres événements liés à l'appel doivent utiliser des NP ordinaires.

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

Une notification Push est envoyée par le serveur d'applications (AS) lorsqu'un appel en sonnerie est accepté par l'appelé sur un autre emplacement, fermé par l'appelant ou, par exemple, redirigé vers la messagerie vocale. Avec iOS 13, ce type de notification push est maintenant régulier et comporte certaines restrictions. Il peut être retardé par le service de notification push Apple (APNS) ou même ne pas être livré du tout. Pour traiter les PN de mise à jour d'appel manquants ou retardés, un délai de sonnerie configurable est ajouté pour contrôler la durée maximale de sonnerie. Si le temps de sonnerie maximum est atteint, la sonnerie de l'appelé est arrêtée et l'appel est traité comme en absence. Du côté de l'appelant, l'appel peut rester en sonnerie jusqu'à ce que la stratégie de sonnerie sans réponse configurée sur le serveur d'applications (AS) soit exécutée.

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

Une option de configuration distincte est ajoutée pour spécifier le comportement de refus d'appel lorsqu'un appel entrant est reçu en tant que notification Push. Le client peut être configuré pour ignorer l'appel ou pour répondre au serveur via Xsi avec le refus défini sur "true" ou "false", auquel cas les services de traitement d'appels Cisco BroadWorks affectés seront appliqués. Si decline_false est configuré, l'appel continue de sonner jusqu'à ce que l'expéditeur abandonne ou que le délai de non-réponse expire, et que les services de traitement des appels associés démarrent. Si "decline_true" est configuré, la raison du refus spécifie le traitement de l'appel. Si la raison du refus est définie sur "occupé", le serveur force immédiatement le service de traitement occupé. Si "temp_unavailable" est configuré, le service de traitement temporaire non disponible est appliqué.

Informations confidentielles de Cisco

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

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	vrai, faux	Contrôle la date d'établissement de la session SIP REGSITER – à 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 sonnerie des appels entrants reçus par l'intermédiaire de PN. Si aucun PN d'appel n'est reçu dans le délai imparti, l'appel sera considéré comme manqué.
%REJECT_WITH_XSI_MODE_WXT%	decline_false	ignorer, decline_true, decline_false	Spécifie le comportement de refus d'appel.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	occupé	occupé, temp_unavailable	Spécifie le motif du refus d'appel, si le mode de rejet est défini sur decline_true.

6.3.2.1 MWI

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

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

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 Accueil de la sonnerie

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

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


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_RING_SPLASH_WXT%	false	vrai, faux	Active Ring Splash dans la configuration BroadWorks.

6.3.2.3 Mode de livraison (Webex Calling seulement)

L'application Webex utilise le serveur NPS (Notification Push Server) pour fournir les notifications push pour les appels à APNS/FCM. La version 45.2 de l'application Webex prend désormais en charge trois modes de remise différents pour configurer la façon dont les notifications push liées aux appels doivent être envoyées à la FCM / APNS :

- nps - mécanisme actuel, à l'aide du NPS
- cloud - mécanisme amélioré, à l'aide Cisco Webex microservice Cloud
- externe - un mécanisme qui utilise un système tiers. Cette solution nécessite l'intégration du système tiers au moteur Cisco WebHooks.

```
<config>
<services><appels>
<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 si omis	Valeurs prises en charge	Description
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	NPS	NPS, Cloud, Externe	Spécifie le mode de remise des notifications push pour les appels.

6.3.3 Alerte unique

La fonction Mobile Single Alert est destinée aux déploiements de convergence fixe-mobile (FMC) / Mobile Network Operator (MNO) exploitant le service BroadWorks Mobility. Sans ce contrôle, lorsqu'il est connecté au client de Webex et reçoit un appel entrant, l'utilisateur reçoit simultanément deux appels – un natif et un appel de notification Push (VoIP). Lorsque la fonctionnalité est activée, l'application désactive les alertes de mobilité sur l'emplacement BroadWorks Mobility de l'utilisateur lors de la connexion et active les alertes lors de la déconnexion. Une condition préalable importante pour l'utilisation de cette fonctionnalité est que l'utilisateur ait le service BroadWorks Mobility affecté et exactement un emplacement configuré.

```
<config>
<services><appels>
<alerte unique activée="%ENABLE_SINGLE_ALERTING_WXT%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_SINGLE_ALERTING_WXT%	faux	Vrai, faux	Défini sur "true" pour activer l'alerte unique.

6.3.4 Cliquez pour composer (rappel)

Le Click to Dial sortant permet à l'utilisateur final de passer un appel sur son téléphone portable à commutation de circuit personnel et de transmettre son numéro de répertoire professionnel en tant qu'ID de ligne appelante.

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

Lorsque la fonctionnalité est activée, les utilisateurs peuvent sélectionner l'emplacement du SNR dans le menu de couplage de périphériques. Lorsqu'ils sont jumelés à SNR site, tous les appels sortants sont initiés à l'aide d'appels Click to Dial (rappel). Pour éviter les doubles alertes, les notifications Push pour les appels entrants sont désactivées.

Lorsqu'un utilisateur lance un appel Cliquez pour appeler, l'écran des appels sortants s'affiche avec les informations indiquant qu'il doit recevoir un appel entrant sur le site SNR sélectionné. Cet écran se ferme automatiquement en fonction de la minuterie configurable.

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

```
<config>
<services>
  <composition d'un numéro>
    <rappel activé="%ENABLE_DIALING_CALL_BACK_WXT% »
timer="%DIALING_CALL_BACK_TIMER_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_DIALING_CALL_BACK_WXT%	faux	Vrai, faux	Défini sur "true" pour activer les appels Click to Dial (Rappel).
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Contrôle le délai, en secondes, avant la fermeture automatique de l'écran de rappel.

6.3.5 Prise en charge des ORM

6.3.5.1 Appel avec numéroteur natif

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

Informations confidentielles de Cisco

La capacité de l'utilisateur à passer des appels via le numéroteur natif est contrôlée par la **balise de configuration native** . Si elle est activée, l'application lance le numéroteur natif et passe l'appel. En outre, la disponibilité des appels VoIP est contrôlée par le bandeau **voip** , en fonction des exigences de déploiement VoIP les appels peuvent être activés ou désactivés.

Si les appels VoIP et natifs sont activés, l'utilisateur peut choisir l'option à utiliser.

La balise <mode-numérotation> contrôle si les utilisateurs peuvent sélectionner le mode de démarrage/réception des appels entrants et sortants. Nécessite l'activation des appels natif et VoIP.

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

Cette fonctionnalité est utile pour les clients qui utilisent 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 principal du secteur télécom. La nouvelle balise <fac-prefix> est ajoutée sous la section <dialing><native> et le service Télécom peut l'utiliser pour résoudre ce problème.

```
<config>
<services>
  <composition d'un numéro>
    <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%"/>
    </natif >
    <mode-numérotation activé="%ENABLE_DIALING_MODE_WXT% » default="%DIALING_MODE_DEFAULT_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_DIALING_VOIP_WXT%	Vrai	vrai, faux	Réglez la valeur "true" pour activer VoIP option d'appel.
%ENABLE_DIALING_NATIVE_WXT%	false	vrai, faux	Réglez la valeur "true" pour activer l'option d'appel native.
%ENABLE_DIALING_MODE_WXT%	faux	Vrai, faux	Permet à l'utilisateur de sélectionner le mode d'appel via les paramètres d'appel dans Préférences.
%DIALING_MODE_DEFAULT_WXT%	VoIP (VoIP)	VoIP, natif	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.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%DIALING_NATIVE_FAC_PREFIX_WXT%	*vide*	chaîne	Spécifie un préfixe qui doit être précédé si l'appel sortant vers un numéro commençant par un code FAC est initié en tant qu'appel cellulaire. Par défaut, aucun préfixe FAC n'est défini et le tag est vide.

REMARQUE 1 : Au moins un appel **VoIP** et **natif** doit être activé.

REMARQUE 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.

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

6.3.5.2 Contrôles en cours d'appel

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

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

La version 43.10 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 la possibilité d'effectuer le transfert. De plus, si l'utilisateur a deux appels cellulaires indépendants sur le même appareil, le menu de transfert est amélioré pour permettre de transférer l'un à l'autre même s'il n'y a aucune association créée entre eux.

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_XSI_CALL_CONTROL_WXT%	false	vrai, faux	Active le contrôle des appels XSI pour l'environnement MNO.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Contrôle le type de déploiement MNO XSI utilisé par l'application. Les valeurs possibles sont : ▪ MNO_Access – affiche tous les appels distants (XSI) avec les types de périphériques définis dans le nœud ci-dessous. ▪ MNO_Network - affiche tous les appels distants (XSI).
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	chaîne	Les noms des types de périphériques à utiliser dans le type de déploiement MNO_Access.
%ENABLE_XSI_HOLD_CALLS_WXT%	Vrai	Vrai, faux	Contrôle si l'action Appel en attente doit être disponible pour l'utilisateur pour les appels mobiles XSI.

6.3.5.3 Identité de la ligne appelante sortante (CLID) – Dual Persona

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 lorsqu'ils passent un appel sortant.

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

Pour VoIP appels, l'utilisateur a également la possibilité de contrôler sa CLID. L'option disponible dans ce cas est uniquement de contrôler s'il faut cacher son identité ou non.

La gestion des personas et le blocage CLID sont contrôlés via des options de configuration distinctes.

```
<config>
<services>
<composition d'un numéro>
   <appelant-id-livraison-blocage activé="%ENABLE_CLID_DELIVERY_BLOCKING_WXT%"/>
   <mobility-persona-management
enabled="%ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%"/>
```


Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CLID_DELIVERY_BLOCKING_WXT%	faux	Vrai, faux	Permet d'activer le blocage de la remise 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%	faux	Vrai, faux	Active la gestion personnelle des appels natifs lorsque le type de déploiement est configuré sur MNO_Access ou MNO_Network. (La mobilité BroadWorks est utilisée 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 natifs, qui peut être contrôlée 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 si omis	Valeurs prises en charge	Description
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	Vrai	vrai, faux	Active l'abonnement pour la notification push MOBILE_CALL_INFO.

6.3.5.5 Déplacement d'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 interlocuteurs d'un appel 1:1 (même si l'interlocuteur n'est pas un utilisateur Webex). Si l'utilisateur distant est un utilisateur Webex, une fois en réunion, les interlocuteurs auront la possibilité de :

- Lancement d'Webex dans une discussion de réunion
- Ajouter une vidéo (notez que l'audio continuera dans l'appel natif)
- Partager l'écran / le contenu
- Déclencher l'enregistrement des réunions

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	vrai, faux	Active la mise sous tension (actions d'invitation et de réunion, de vidéoconférence).

6.3.5.6 Mobilité MNO - Widget d'appel

La version 43.7 de l'application Android Webex (mobile et tablette) introduit officiellement un nouveau widget de contrôle des appels (bulle), qui permet de contrôler davantage les appels natifs ancrés sur Cisco BroadWorks, à l'aide du service de mobilité. Le widget sera affiché au-dessus de l'interface utilisateur native et permettra à l'utilisateur d'effectuer les actions suivantes :

- Attente/Reprise
- Transfert aveugle/consultatif : place l'utilisateur dans la boîte de dialogue de transfert de l'application Webex.
- Transfert complet – offre la possibilité d'effectuer un transfert consultatif (version 43.10)
- Vidéoconférence – permet de réunir les participants en une réunion Webex.
- Fin d'appel

```
<config>
<services><appels>
       <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%"/>
       <remonter-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% » widget-
enabled="%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
%ENABLE_WIDGET_HOLD_CALLS_WXT%	Vrai	Vrai, faux	Contrôle la disponibilité de l'action de mise en attente dans le widget Appel.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	Vrai	Vrai, faux	Contrôle la disponibilité des actions Transférer et Terminer le transfert dans le widget Appel.
%ENABLE_WIDGET_CALLS_ESCALATE	Vrai	Vrai, faux	Contrôle la disponibilité de l'action Vidéoconférence dans le widget Appel.

Informations confidentielles de Cisco

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	Description
_TO_WEBEX_MEETING_WXT%			

6.3.6 ID 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, la notification d'appel entrant et les notifications d'appel manqué.

6.3.6.1 Écran d'appel entrant

Il existe des différences de plate-forme entre Android et iOS en ce qui concerne l'affichage des données dans l'écran d'appel entrant. L'expérience native d'affichage des informations pour les appels entrants est la suivante :

Android - il y a deux champs 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 s'assurer que l'application iOS Webex 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 nombre n'y est pas toujours affiché.

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

6.3.6.3 Notification d'appel manqué

Un paramètre de configuration supplémentaire a été ajouté pour les notifications d'appels en absence. Il peut être utilisé pour contrôler les informations de l'interlocuteur distant, comme pour les notifications d'appel entrant, en permettant 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>
```


Informations confidentielles de Cisco

```
<services><appels>
   <id_appelant>
      <Appels entrants>
         <append-number enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
      </appels entrants>
      <appels en absence>
         <append-number enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
      </appels manqués>
```

Étiquette	Valeur par défaut si omis	Valeurs prises en charge	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	Indique si le numéro doit être ajouté au nom dans la notification d'appel manqué.

REMARQUE : Si le numéro est livré sous forme de 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.

Informations confidentielles de Cisco

7 Fonctionnalités Early Field Trial (BETA)

Il n'y a pas de fonctionnalités dans BETA avec la dernière version.

Informations confidentielles de Cisco

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

Le tableau suivant présente les Webex des balises personnalisées Cisco BroadWorks, correspondant à leurs anciennes balises personnalisées pour UC-One.

Webex pour Balise Cisco BroadWorks	Balise héritée du bureau	Balise héritée 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%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%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%	S/O
%ENABLE_CALL_STATISTICS_WXT%	S/O	S/O
%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%	%DESKTOP_MWI_MODE%	%MWI_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	S/O	S/O
%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%	S/O
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	S/O	S/O
%ENABLE_BROADWORKS_ANYWHERE_WXT%	S/O	S/O

Informations confidentielles de Cisco

Webex pour Balise Cisco BroadWorks	Balise héritée du bureau	Balise héritée mobile
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	S/O	S/O
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	S/O	S/O
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	S/O	S/O
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	S/O	S/O
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	S/O	S/O
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	S/O	S/O
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	S/O	S/O
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	S/O	S/O
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	S/O	S/O
%ENABLE_EMERGENCY_DIALING_WXT%	S/O	S/O
%EMERGENCY_DIALING_NUMBERS_WXT%	S/O	S/O
%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%	S/O

Informations confidentielles de Cisco

Webex pour Balise Cisco BroadWorks	Balise héritée du bureau	Balise héritée mobile
%USE_TLS_FROM_DNS_WXT%	%USE_TLS_FROM_DNS%	S/O
%DOMAIN_OVERRIDE_WXT%	%DOMAIN_OVERRIDE%	%DOMAIN_OVERRIDE%
%SOURCE_PORT_WXT%	%SOURCE_PORT%	%SOURCE_PORT%
%USE_ALTERNATIVE_IDENTITIES_WXT%	%USE_ALTERNATIVE_IDENTITIES%	S/O
%TCP_SIZE_THRESHOLD_WXT%	%TCP_SIZE_THRESHOLD%	S/O
%SIP_REFRESH_ON_TTL_WXT%	%SIP_REFRESH_ON_TTL%	S/O
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	%ENABLE_SIP_UPDATE_SUPPORT_MOBILE%
%ENABLE_PEM_SUPPORT_WXT%	%ENABLE_PEM_SUPPORT_ DE BUREAU%	S/O
%ENABLE_SIP_SESSION_ID_WXT%	S/O	S/O
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	S/O	S/O
%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%	S/O
%CHANNEL_HEARTBEAT_WXT%	%CHANNEL_HEARTBEAT%	%CHANNEL_HEARTBEAT_MOBILE%
%XSI_ROOT_WXT%	%XSI_ROOT%	%XSI_ROOT%
%XSI_ACTIONS_PATH_WXT%	S/O	%XSI_ACTIONS_PATH_MOBILE%
%XSI_EVENTS_PATH_WXT%	S/O	%XSI_EVENTS_PATH_MOBILE%

Informations confidentielles de Cisco

Webex pour Balise Cisco BroadWorks	Balise héritée du bureau	Balise héritée mobile
%ENABLE_CALLS_AUTO_ RECOVERY_WXT%	S/O	%ENABLE_CALLS_AUTO_ RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_ SEQUENCE_WXT%	S/O	%EMERGENCY_CALL_DIAL_ SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLI ND_WXT%	S/O	S/O
%ENABLE_CALL_PICKUP_ DIRECTED_WXT%	S/O	S/O
%WEB_CALL_SETTINGS_URL _WXT%	S/O	%WEB_CALL_SETTINGS_URL %
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP %
%ENABLE_CALL_CENTER_ WXT%	%ENABLE_CALL_CENTER_ BUREAU%"	S/O
%WEB_CALL_SETTINGS_TAR GET_WXT%	S/O	S/O
%WEB_CALL_SETTINGS_CFA _ VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_CFA _VISIBLE%
%WEB_CALL_SETTINGS_DN D_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_DN D_VISIBLE%
%WEB_CALL_SETTINGS_AC R_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_AC R_VISIBLE%
%WEB_CALL_SETTINGS_CFB _VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_CFB _VISIBLE%
%WEB_CALL_SETTINGS_CFN R_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_CFN R_VISIBLE%
%WEB_CALL_SETTINGS_CFN A_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_CFN A_VISIBLE%
%WEB_CALL_SETTINGS_SIM RING_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_SIM RING_VISIBLE%
%WEB_CALL_SETTINGS_ SEQRING_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_SE QRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_ VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_RO_ VISIBLE%
%WEB_CALL_SETTINGS_ACB _VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_ACB _VISIBLE%
%WEB_CALL_SETTINGS_CW _VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_CW _VISIBLE%
%WEB_CALL_SETTINGS_CLI DB_VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_CLI DB_VISIBLE%
%WEB_CALL_SETTINGS_PA_ VISIBLE_WXT%	S/O	%WEB_CALL_SETTINGS_PA_ VISIBLE%

Informations confidentielles de Cisco

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

Informations confidentielles de Cisco

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

Informations confidentielles de Cisco

Webex pour Balise Cisco BroadWorks	Balise héritée du bureau	Balise héritée mobile
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	S/O	S/O
%ENABLE_CLID_OUTGOING_CALLS_WXT%	S/O	S/O
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	S/O	S/O
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	S/O	S/O
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	S/O	S/O
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	S/O	S/O
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	S/O	S/O
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	S/O
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	S/O
%BLF_NOTIFICATION_DELAY_TIME_WXT%	S/O	S/O
%ENABLE_GCP_NOTIFICATIONS_WXT%	S/O	S/O
%ENABLE_GCP_DISPLAY_CALLER_WXT%	S/O	S/O
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	S/O	S/O
%UDP_KEEPALIVE_ENABLED_WXT%	S/O	S/O
%TCP_KEEPALIVE_ENABLED_WXT%	S/O	S/O
%TLS_KEEPALIVE_ENABLED_WXT%	S/O	S/O
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	S/O	S/O
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	S/O	S/O

Informations confidentielles de Cisco

REMARQUE : N/A indique qu'il n'y avait pas de balise personnalisée correspondante contrôlant la fonction dans UC-One. Le fait d'avoir N/A pour les tags Desktop et Mobile Legacy indique que la Webex pour le tag Cisco BroadWorks est nouvelle et contrôle soit une nouvelle fonctionnalité, soit une fonctionnalité existante, qui n'était pas contrôlée par un tag personnalisé dans UC-One.

Informations confidentielles de Cisco

9 Annexe A : Chiffrements TLS

L'Webex du client BroadWorks utilise CiscoSSL, qui est basé sur OpenSSL avec un renforcement de sécurité supplémentaire.

Informations confidentielles de Cisco

10 Annexe B : Script de mise à disposition des balises DM

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

Notez que ce script n'est valide que pour les nouveaux déploiements dans lesquels des balises DM personnalisées sont créées. Pour modifier les balises DM personnalisées existantes, la commande dans le script suivant doit passer de "add" à "set".

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

```
%% ********************************** Connect_Tags - lire le fichier **********************************
%%
%% Instructions :
%% -------------------
%% - Ce fichier de lecture peut être utilisé pour créer, ajouter et définir Webex pour BroadWorks
%% de balises personnalisées client
%% - Utilisez %% pour commenter toutes les étapes non requises en fonction de la spécificité du
déploiement
%% besoins en service :
%% Étape 1 -- pour les nouveaux déploiements uniquement, créer le libellé initial de jeu de balises
%% Étape 2 -- ajouter une nouvelle balise personnalisée (une entrée est requise pour chaque
nouvelle balise)
%% Étape 3 -- définir la valeur pour un tag personnalisé existant (saisie requise pour chaque tag
applicable)
%% Étape 4 -- affichage et vérification visuelle des paramètres des tags
%%
%% - Éditer, modifier le fichier si nécessaire en respectant la syntaxe de commande. Enregistrer le
fichier (par exemple WxT_Tags.txt)
%% - SFTP fichier lu dans AS sous le répertoire /tmp
%% - Connectez-vous à AS, bwcli (connectez-vous en tant qu'administrateur)
%% - Exécutez la commande suivante à partir de bwcli : AS_CLI> r /tmp/ WxT_Tags.txt
%% - Vérifier les résultats
%%
%% ----------------------------------------------------------------------------------------------------
%% Étape 1 : Créer une étiquette de balise Connect - Connect_Tags
%% ----------------------------------------------------------------------------------------------------
arrêter tout ; système ; deviceTagSet
Ajouter Connect_Tags
%% ----------------------------------------------------------------------------------------------------
%% Étape 2 : Ajouter WxT pour les balises personnalisées BWKS
%% EXEMPLE – pour toutes les balises mobiles, consultez la liste ci-dessous------------------------------
----------------------
arrêter tout ; système ; deviceTagSet ; Étiquettes
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% true
%% ----------------------------------------------------------------------------------------------------
%% Étape 3 : Définir les balises personnalisées Connect (si la balise existe déjà)
%% EXEMPLE – pour toutes les balises mobiles, voir la liste ci-dessous
```


Informations confidentielles de Cisco

```
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------
%% Étape 4 : Vérifier que les tags personnalisés ont été correctement définis et définis
%% ----------
arrêter tout ; système ; deviceTagSet ; Étiquettes
obtenir tagSetName Connect_Tags
Quitter tout
```

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

10.1 Bureau

```
add tagSetName BroadTouch_tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_WXT% true
ajouter 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 (complet)
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
ajouter 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
```


Informations confidentielles de Cisco

```
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% false
ajouter tagSetName BroadTouch_tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
ajouter tagSetName BroadTouch_tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName BroadTouch_tags %SOURCE_PORT_WXT% 5060
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName BroadTouch_tags %SIP_FAILBACK_ENABLED_WXT% true
ajouter 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
ajouter 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
ajouter 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
ajouter 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% externe
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% externe
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
```


Informations confidentielles de Cisco

```
add tagSetName BroadTouch_tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
ajouter tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PARK_WXT% false
add tagSetName BroadTouch_tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
ajouter tagSetName BroadTouch_tags %RTP_ICE_PORT_WXT% 3478
add tagSetName BroadTouch_tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName BroadTouch_tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID_WXT% true
add tagSetName BroadTouch_tags %XSI_ROOT_WXT% true
add tagSetName BroadTouch_tags %SBC_ADDRESS_WXT% true
add tagSetName BroadTouch_tags %SBC_PORT_WXT% true
add tagSetName BroadTouch_tags %MWI_MODE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName BroadTouch_tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUTO_ANSWER_WXT% false
add tagSetName BroadTouch_tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName BroadTouch_tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName BroadTouch_tags %ENABLE_VIDEO_QOS_WXT% true
ajouter 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% résolu
add tagSetName BroadTouch_tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```


Informations confidentielles de Cisco

10.2 Mobile

```
add tagSetName Connect_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName Connect_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName Connect_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName Connect_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName Connect_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName Connect_Tags %ENABLE_MWI_WXT% false
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName Connect_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName Connect_Tags %USE_TLS_WXT% false
add tagSetName Connect_Tags %SBC_PORT_WXT% 5075
add tagSetName Connect_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName Connect_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
ajouter tagSetName Connect_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
ajouter 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
ajouter tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
ajouter tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
ajouter 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
ajouter 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
```


Informations confidentielles de Cisco

```
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% externe
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% externe
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% occupé
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
ajouter tagSetName Connect_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName Connect_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName Connect_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName Connect_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName Connect_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName Connect_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName Connect_Tags %XSI_ROOT_WXT% true
add tagSetName Connect_Tags %SBC_ADDRESS_WXT% true
add tagSetName Connect_Tags %SBC_PORT_WXT% true
add tagSetName Connect_Tags %MWI_MODE_WXT% true
```


Informations confidentielles de Cisco

```
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% résolu
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
```

10.3 Tablette

```
add tagSetName ConnectTablet_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName ConnectTablet_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
```


Informations confidentielles de Cisco

```
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
ajouter 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
ajouter tagSetName ConnectTablet_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName ConnectTablet_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_REKEYING_WXT% true
ajouter tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
ajouter tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
ajouter 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
```


Informations confidentielles de Cisco

```
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% externe
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% externe
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
ajouter 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% occupé
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
ajouter 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
ajouter tagSetName ConnectTablet_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName ConnectTablet_Tags %XSI_ROOT_WXT% true
add tagSetName ConnectTablet_Tags %SBC_ADDRESS_WXT% true
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% true
add tagSetName ConnectTablet_Tags %MWI_MODE_WXT% true
```


Informations confidentielles de Cisco

```
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
ajouter 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% résolu
add tagSetName ConnectTablet_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```

10.4 Balises système

La liste ci-après répertorie les balises système utilisées par Webex for BroadWorks.

```
%BWNETWORK-CONFERENCE-SIPURI-n%
%NOMBRE-PORTAIL-BWVOICE-n%
%BWLINEPORT-n%
%BWHOST-n%
%BWAUTHUSER-n%
```


Informations confidentielles de Cisco

%BWAUTHPASSWORD-n%
%BWE164-n%
%BWNAME-n%
%BWEXTENSION-n%
%BWAPPEARANCE-LABEL-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMAIRE%
%BWE911-PRIMAIRE-HELDURL%
%BWE911-IDCLIENT% ;
%BWE911-CLÉSECRÈTE%
%BWE911-LISTE-DES-NUMÉROS-D'URGENCE%
%BW-MEMBERTYPE-N%
%BWUSEREXTID-n%

Informations confidentielles de Cisco

11 Acronymes et abréviations

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

ACB	Rappel automatique
ACD	Répartition automatique d'appels
ACR (en anglais seulement)	Rejet des appels anonymes
AES	Advanced Encryption Standard
ALG	Passerelle de couche application
API	Application Programming Interface – Interface de programmation d'applications
APK	Progiciel de demande
APNS	Service de notifications push Apple
ARS	Sélection automatique du débit binaire
COMME	Serveur d'applications (Cisco BroadWorks)
AVP	Profil audiovisuel
BW	BroadWorks (en anglais seulement)
BWA	BroadWorks Anywhere
BWKS	BroadWorks (en anglais seulement)
BWM	Mobilité BroadWorks
BYOD	Apportez votre propre appareil
CC	Centre d'appel
BFC	Renvoi d'appel si occupé
L'	Renvoi d'appel en l'absence de réponse
CFNR	Renvoi d'appels non joignable
CIF	Format intermédiaire commun
CLI	Interface de ligne de commande
CLID	Identité de la ligne appelante
CLIDB	Blocage de la remise de l'ID de ligne appelante
CRLF	Saut de ligne de retour chariot
CS	Circuit commuté
CSWV (en anglais seulement)	Affichage Web Paramètres d'appel
CW	Appel en attente
DB	Base de données
DÉCIMÈTRE	Gestion des périphériques
NPD	Ne pas déranger
DNS	Système de noms de domaine

Informations confidentielles de Cisco

DPC	Contrôle de téléphone de bureau
DTAF	Fichier d'archive de type de périphérique
CEACS	Service de changement d'adresse d'appel d'urgence
FMC	Convergence fixe-mobile
FQDN	Nom de domaine complet
Le	Code d'authentification des messages de hachage
ICE	Établissement de connectivité interactive
iLBC	Codec à faible débit binaire Internet
IM	Messagerie instantanée
IM et P	Messagerie instantanée et présence
L'IOT	Tests d'interopérabilité
IP	Protocole Internet
JID	Identifiant Jabber
M/O	Obligatoire/Facultatif
ORM	Opérateur de réseau mobile
MTU	Unité de transmission maximale
Le	Chat multi-utilisateurs
MWI	Indicateur de message en attente
NAL	Couche d'abstraction réseau
NAPTR	Pointeur d'autorité de dénomination
NAT (Traduction d'adresses de réseau)	Traduction d'adresses de réseau
OTT	Excessif
PA	Assistante personnelle
PAI	P-Identité-revendiquée
PEM	P-Early Media
PLI (en anglais)	Indication de perte d'image
PLMN (en anglais)	Réseau mobile terrestre public
PN	Push Notification
QCIF	Format intermédiaire commun quart
QoS	Quality of Service
RO	Bureau distant
RTCP	Protocole de contrôle en temps réel
RTP (Real-Time Transport Protocol)	Protocole en temps réel
SaaS	Logiciel en tant que service
SAN	Autre nom du sujet
SASL	Authentification simple et couche de sécurité

Informations confidentielles de Cisco

SAVP	Profil audio vidéo sécurisé
SBC	Session Border Controller
SCA	Affichage des appels partagés
SCF	Fonction de continuité de session
Le	Protocole de transmission de contrôle de flux
SDP	Protocole de définition de session
SÉQUENÇAGE	Sonnerie séquentielle
LE TROMPEUR	Sonnerie simultanée
SIP	Protocole SIP
SNR	Rapport signal sur bruit
SNR	Single Number Reach
Le	Protocole de contrôle en temps réel sécurisé
SRTP	Protocole de transport en temps réel sécurisé
SSL (protocole SSL)	Secure Sockets Layer
STUN	Utilitaires de traversée de session pour NAT
SUBQCIF	Sous-trimestre CIF
TCP	Protocole TCP (Transmission Control Protocol)
TLS	Transport Layer Security (Protocole TLS, Sécurité des couches de transport)
TTL	Il est temps de vivre
TURN	Traversée à l'aide de NAT relais
UDP	Protocole UDP (User Datagram Protocol)
UI	Interface utilisateur
UMS	Serveur de messagerie (Cisco BroadWorks)
URI	URI (Uniform Resource Identifier)
UVS	Serveur vidéo (Cisco BroadWorks)
VGA	Tableau graphique vidéo
VoIP	Voix off IP
VVM	Visual Voicemail
WXT (en anglais)	Webex
XMPP	Protocole de messagerie et de présence extensible
XR	Rapport étendu
Xsp	Plateforme de services Xtended
Xsi	Xtended Services Interface

Informations confidentielles de Cisco