Mettre à jour les approbations pour l'interface CTI dans Webex pour Broadworks

Table des matières

Introduction

Ce document décrit le processus de mise à jour des ancres d'approbation pour l'interface CTI dans Webex pour Broadworks.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Familiarité avec la configuration des paramètres dans le Control Hub
- Présentation de la configuration et de la navigation dans l'interface de ligne de commande (CLI) de Broadworks.
- Compréhension de base des protocoles SSL/TLS et de l'authentification des certificats

Composants utilisés

Les informations contenues dans ce document sont basées sur Broadworks R22 et versions

ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document suppose que les hôtes Broadworks XSP/ADP sont connectés à Internet.

Configurer

Cette procédure implique de télécharger des fichiers de certificats spécifiques, de les fractionner, de les copier à certains emplacements sur votre XSP, puis de télécharger ces certificats en tant que nouvelles ancres d'approbation. Il s'agit d'une tâche importante qui permet d'assurer une communication sécurisée et fiable entre votre XSP et Webex.

Ce document montre les étapes à suivre pour installer des ancrages d'approbation pour l'interface CTI pour la première fois. Il s'agit du même processus lorsque vous devez les mettre à jour. Ce guide décrit les étapes à suivre pour acquérir les fichiers de certificat nécessaires, les fractionner en certificats individuels, puis les télécharger vers de nouvelles ancres de confiance sur le XSP|ADP.

Configuration et renouvellement des ancrages d'approbation

La configuration initiale et toutes les mises à jour suivantes sont effectuées de la même manière. Lors de l'ajout initial d'approbations, suivez les étapes et confirmez que les approbations sont ajoutées.

Lors de la mise à jour, vous pouvez ajouter les nouvelles approbations et supprimer les anciennes une fois les nouvelles installées ou laisser les deux approbations. Les anciennes et les nouvelles approbations peuvent fonctionner en parallèle, car les services W4B prennent en charge la présentation du certificat correspondant à l'une des deux approbations.

Pour récapituler :

- Le nouveau certificat de confiance Cisco peut être ajouté à tout moment avant l'expiration de l'ancienne confiance.
- L'ancienne approbation peut être supprimée en même temps que la nouvelle ou à une date ultérieure si l'équipe d'exploitation préfère cette approche.

Présentation du processus

Voici un aperçu du processus, qui s'applique à la fois à l'installation initiale et aux mises à jour des ancrages d'approbation :

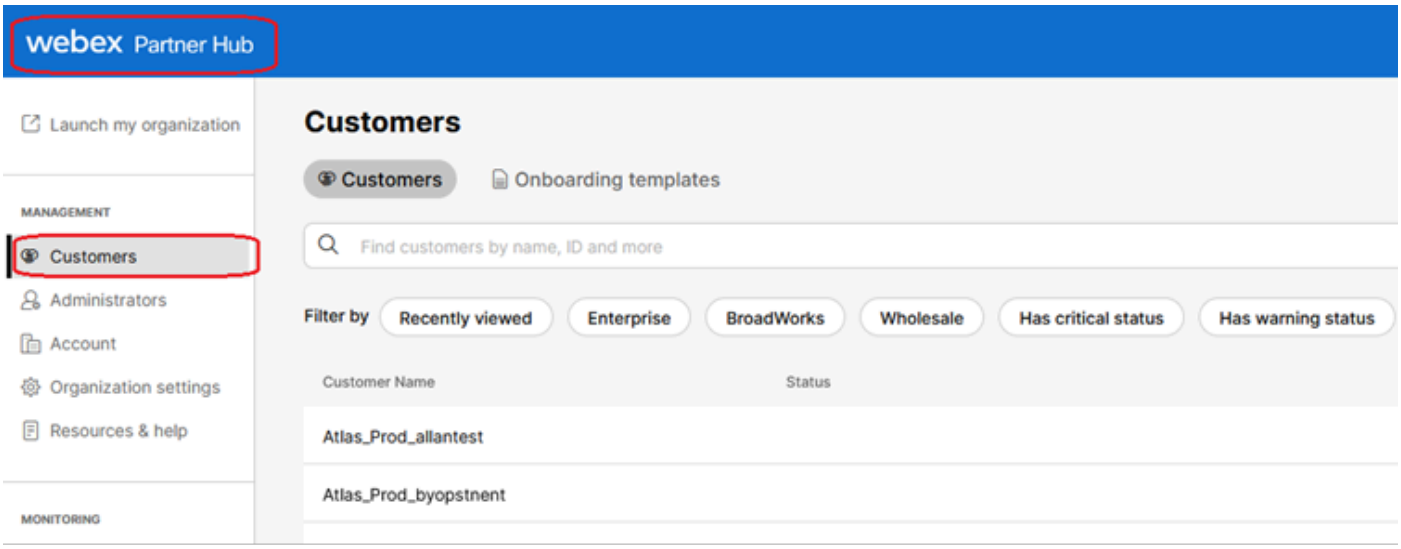
- Téléchargez le certificat CA Webex : obtenez le fichier CombinedCertChain2023.txt à partir

du Partner Hub sous Settings > BroadWorks Calling.

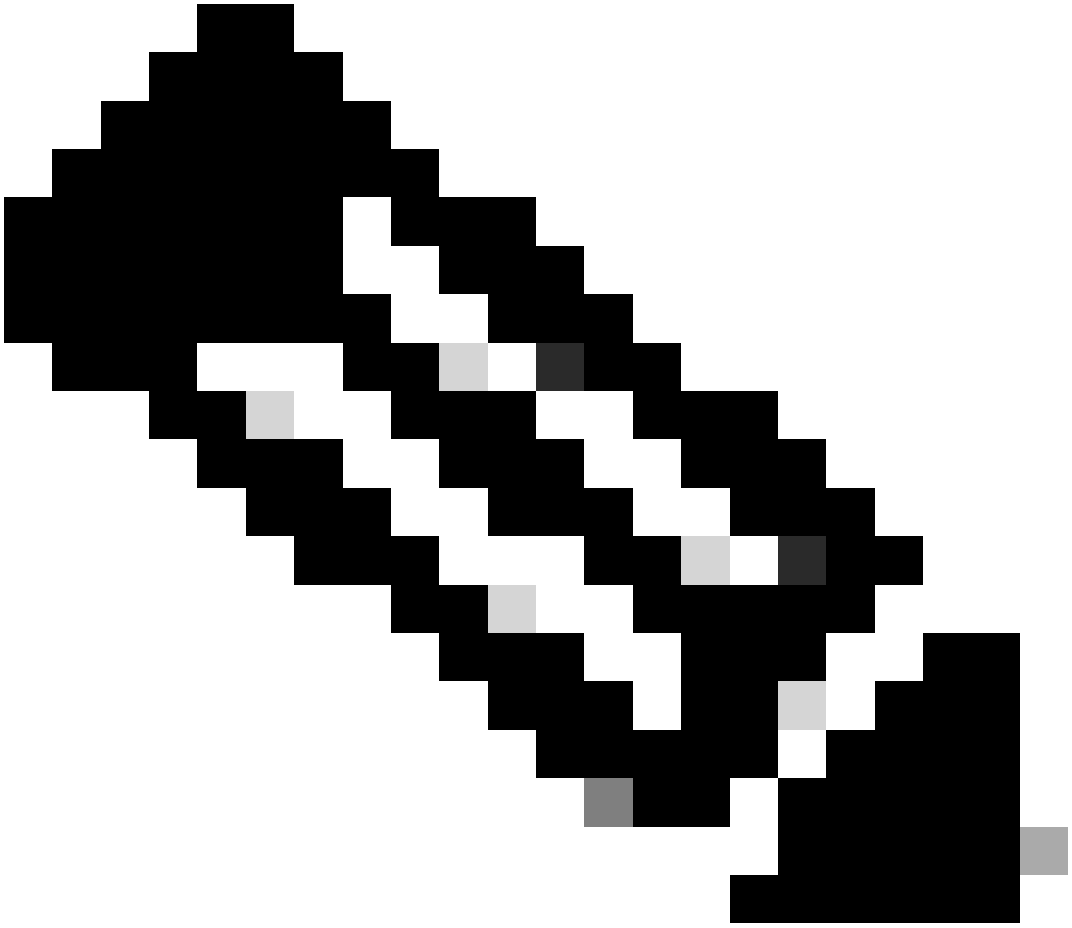
- Split Certificate Chain : scindez le fichier de la chaîne de certificats combinée en deux fichiers de certificats distincts, root2023.txt et emission2023.txt, à l'aide d'un éditeur de texte.
- Copier les fichiers : transférez les deux fichiers de certificat vers un emplacement temporaire sur le XSP|ADP.
- Update Trust Anchors : utilisez la commande updateTrust dans l'interface de ligne de commande XSP|ADP pour télécharger les fichiers de certificat vers de nouvelles ancres d'approbation.
- Confirm Update : vérifiez que les ancres d'approbation sont mises à jour.

Télécharger le certificat CA Webex

1. Connectez-vous au Partner Hub.

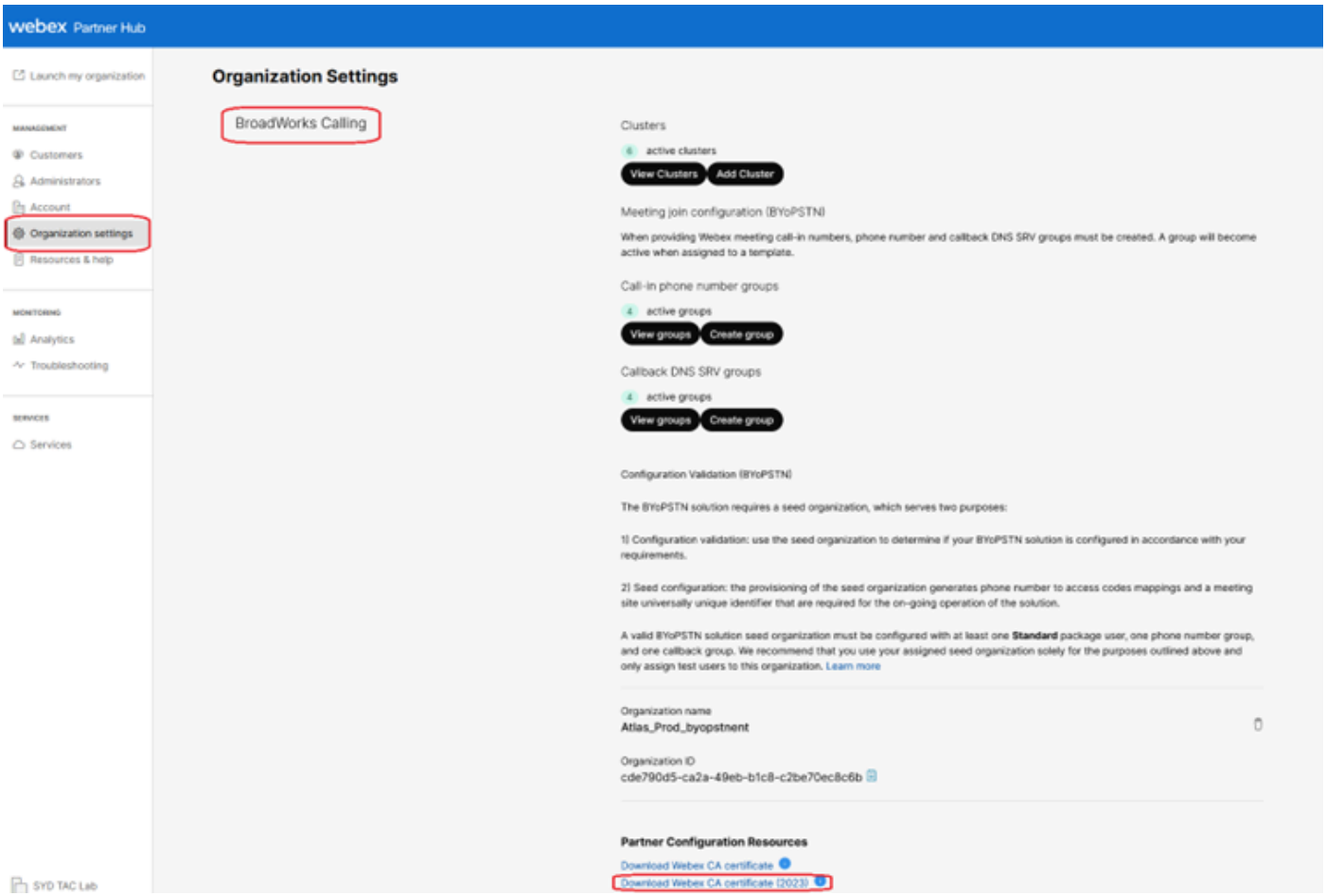


Webex Partner Hub

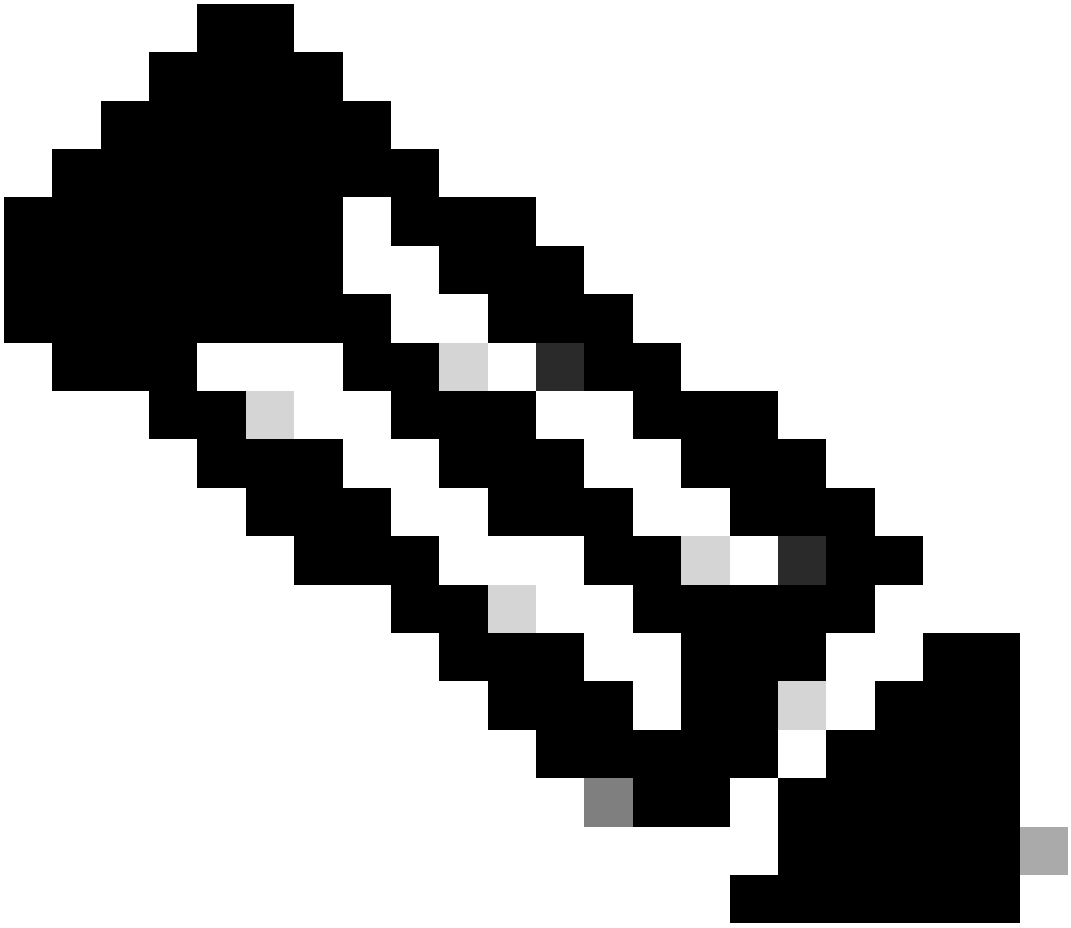


Remarque : le concentrateur partenaire est différent du concentrateur de contrôle. Dans le Partner Hub, vous voyez Customers dans le volet de gauche et Partner Hub dans le volet de titre.

2. Accédez à Organization Settings > BroadWorks Calling et cliquez sur Download Webex CA.



Page Paramètres de l'organisation affichant le lien de téléchargement du certificat



Remarque : choisissez la dernière option. Dans cette capture d'écran, vous pouvez voir la dernière est Télécharger le certificat CA Webex (2023)

---

3. Le certificat présenté ici. L'image est masquée pour des raisons de sécurité.

1

2

: il est recommandé de vérifier que chaque nouveau fichier ne contient qu'un seul certificat et que les marqueurs BEGIN et END sont correctement inclus.

Copier les fichiers

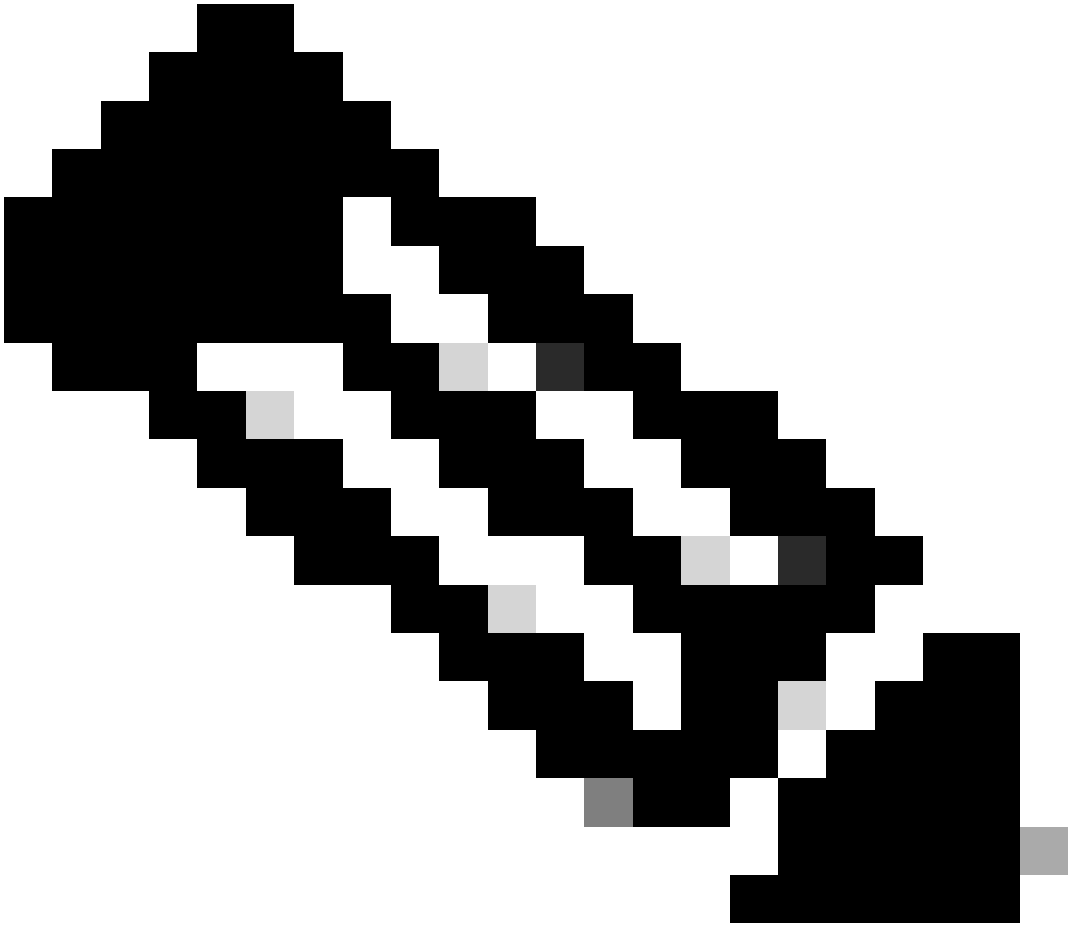
Copiez root2023.txt et emission2023.txt dans un répertoire temporaire sur XSP/ADP tel que /var/broadworks/tmp/. Cela peut être fait en utilisant WinSCP ou toute autre application similaire.

```
bwadmin@tac-ucaas.cisco.com$ ls -l /var/broadworks/tmp/
-rwxrwxrwx 1 bwadmin bwadmin 2324 Jul 21 2023 issuing2023.txt
-rwxrwxrwx 1 bwadmin bwadmin 1894 Jul 21 2023 root2023.txt
```

Mettre à jour les ancres de confiance

Téléchargez les fichiers de certificat pour établir de nouvelles ancres de confiance. À partir de CTI XSP/ADP BWCLI, émettez ces commandes :

```
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> updateTrust webexclientroot202
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> updateTrust webexclientissuing
```



Remarque : chaque alias doit être unique. Par exemple, webexclientroot2023 et webexclientissuing2023 servent d'exemples d'alias pour les ancres d'approbation. N'hésitez pas à créer des alias personnalisés, en vous assurant que chacun est distinct.

Confirmer la mise à jour

Vérifiez que les ancres sont mises à jour en exécutant cette commande

```
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> get
Alias Owner Issuer
================================================================================
webexclientissuing2023 Internal Private TLS SubCA Internal Private Root
webexclientroot2023 Internal Private Root Internal Private Root[self-signed]
```

Votre interface CTI a été mise à jour avec le certificat le plus récent.

Vérifier la connexion TLS

Notez que le journal TLS Tomcat doit être activé au niveau de la gravité FieldDebug pour afficher la connexion SSL.

```
ADP_CLI/Applications/WebContainer/Tomcat/Logging/InputChannels> get
Name Enabled Severity
=========================================
TLS true FieldDebug
```

Le débogage TLS est uniquement disponible dans ADP 202.10 et versions ultérieures. Voir Configuration et démontage de la connexion cryptographique du journal Cisco BroadWorks.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.