Aggiornamento dei trust per l'interfaccia CTI in Webex per Broadworks

Sommario

Introduzione

Questo documento descrive il processo di aggiornamento dei trust anchor per l'interfaccia CTI di Webex per Broadworks.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Familiarità con la configurazione delle impostazioni nell'hub di controllo
- Informazioni sulla configurazione e l'esplorazione dell'interfaccia della riga di comando (CLI) di Broadworks.
- Conoscenza di base dei protocolli SSL/TLS e dell'autenticazione dei certificati

Componenti usati

Le informazioni fornite in questo documento si basano su Broadworks R22 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento si presume che gli host Broadworks XSP/ADP siano connessi a Internet.

Configurazione

Questa procedura prevede il download di file di certificati specifici, la loro suddivisione, la copia in percorsi specifici dell'XSP e quindi il caricamento di tali certificati come nuovi trust anchor. Si tratta di un'attività importante che contribuisce a garantire una comunicazione sicura e affidabile tra XSP e Webex.

In questo documento viene descritto come installare i trust anchor per l'interfaccia CTI per la prima volta. È lo stesso processo quando è necessario aggiornarli. In questa guida vengono illustrati i passaggi per acquisire i file di certificato necessari, suddividerli in certificati singoli e quindi caricarli in nuovi trust anchor in XSP|ADP.

Impostazione e rinnovo dei trust anchor

L'impostazione iniziale e gli eventuali aggiornamenti successivi sono lo stesso processo. Quando si aggiungono trust per la prima volta, completare la procedura e confermare che i trust sono stati aggiunti.

Durante l'aggiornamento, è possibile aggiungere i nuovi trust ed eliminare i trust precedenti dopo l'installazione dei nuovi trust oppure lasciare entrambi i trust. I trust vecchi e nuovi possono funzionare in parallelo, in quanto i servizi W4B supportano la presentazione del certificato corrispondente a uno dei due trust.

Per riepilogare:

- Il nuovo certificato trust Cisco può essere aggiunto in qualsiasi momento prima della scadenza del trust precedente.
- Il trust precedente può essere rimosso contemporaneamente all'aggiunta del nuovo trust o in qualsiasi data successiva se il team operativo preferisce tale approccio.

Panoramica sul processo

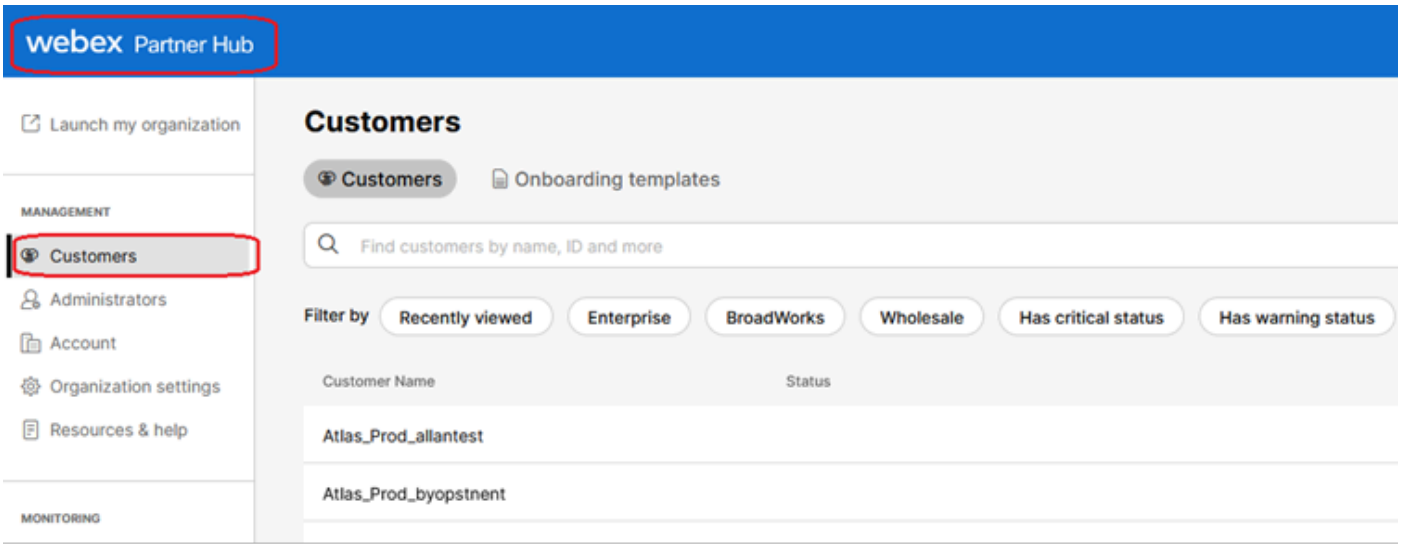
Di seguito è riportata una panoramica del processo, applicabile sia all'installazione iniziale che agli aggiornamenti dei trust anchor:

- Scarica il certificato CA Webex: ottieni il file CombinedCertChain2023.txt dall'hub partner in Impostazioni > Chiamate BroadWorks.

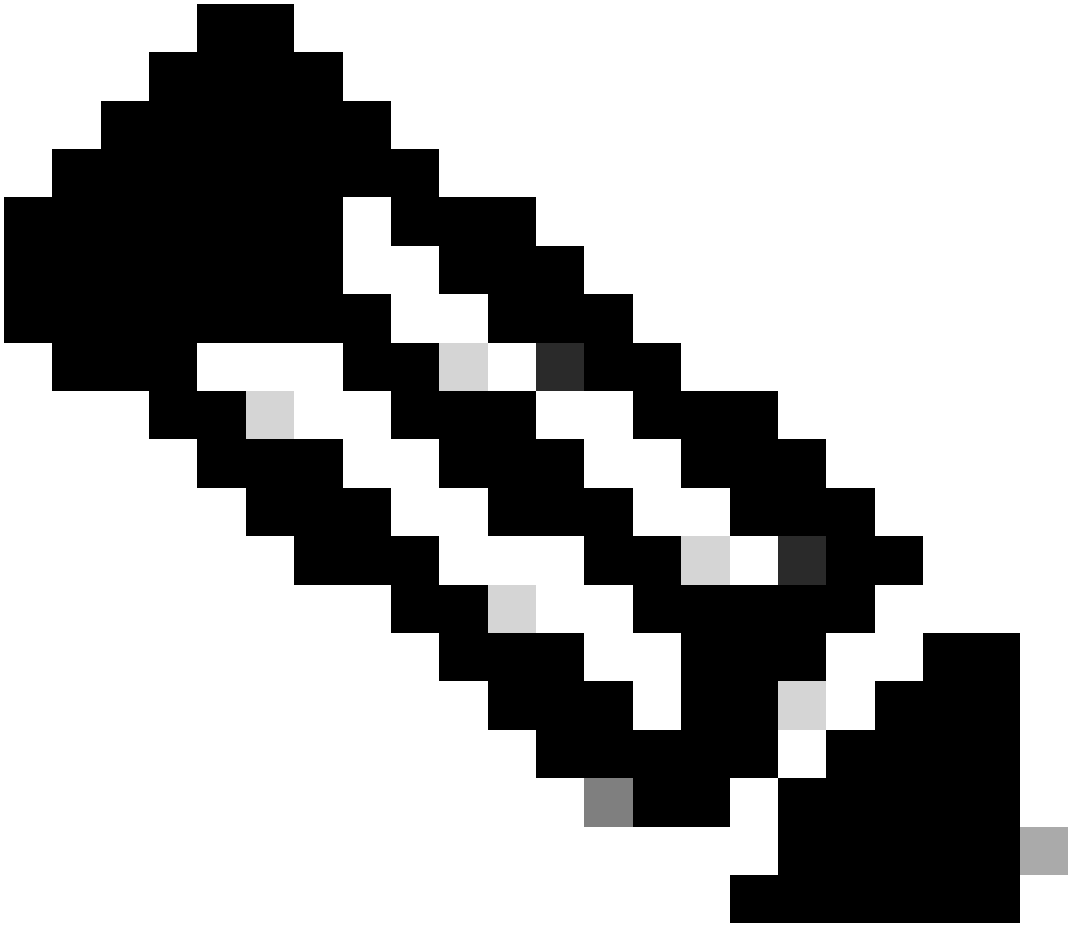
- Dividi catena di certificati: consente di dividere il file della catena di certificati combinata in due file di certificati separati, root2023.txt e issuer2023.txt, utilizzando un editor di testo.
- Copia file: trasferire entrambi i file di certificato in un percorso temporaneo in XSP|ADP.
- Aggiorna trust anchor: utilizzare il comando updateTrust nell'interfaccia della riga di comando XSP|ADP per caricare i file dei certificati in nuovi trust anchor.
- Conferma aggiornamento: verificare che i trust anchor siano stati aggiornati correttamente.

Scarica certificato CA Webex

1. Accedere a Partner Hub.

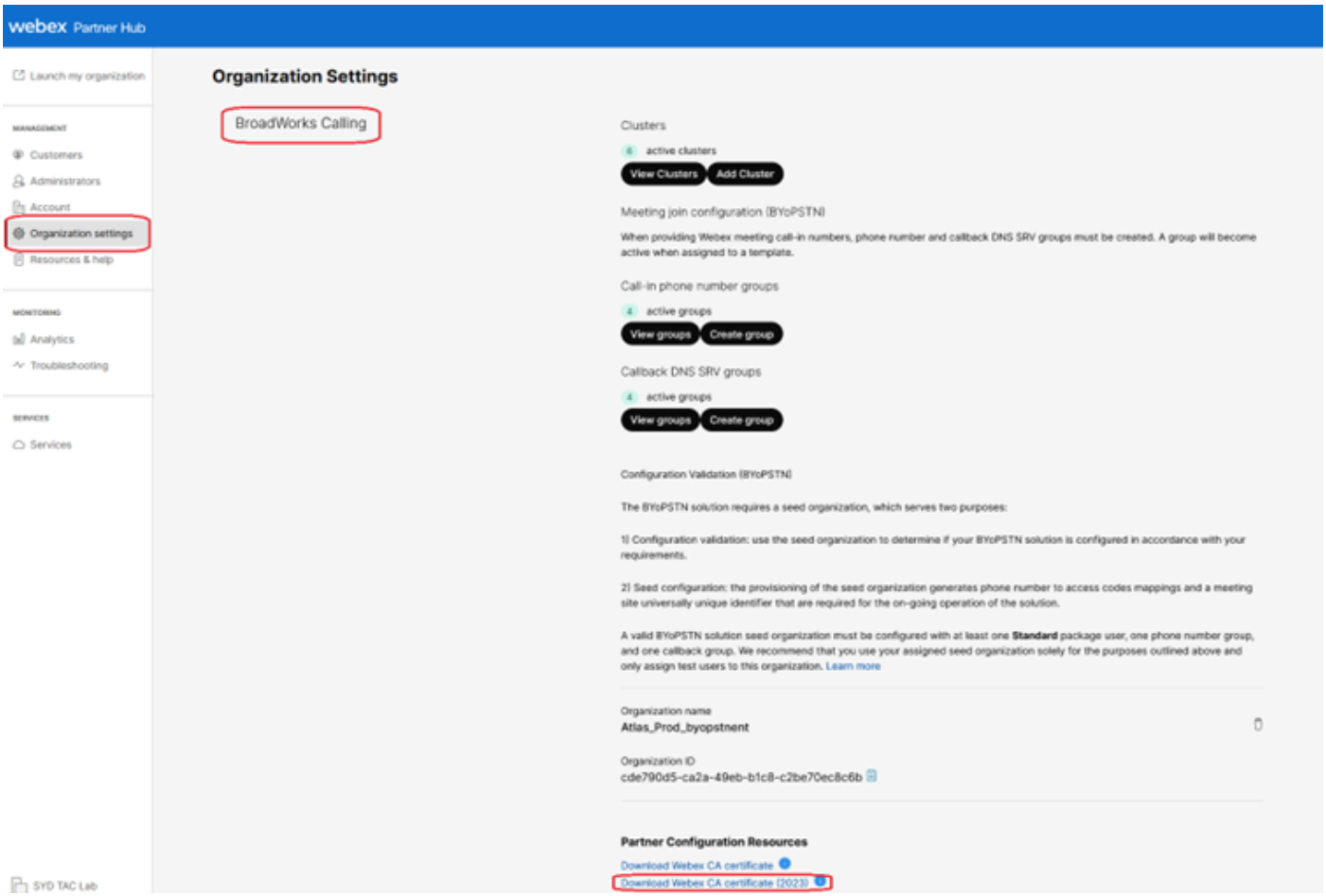


Webex Partner Hub

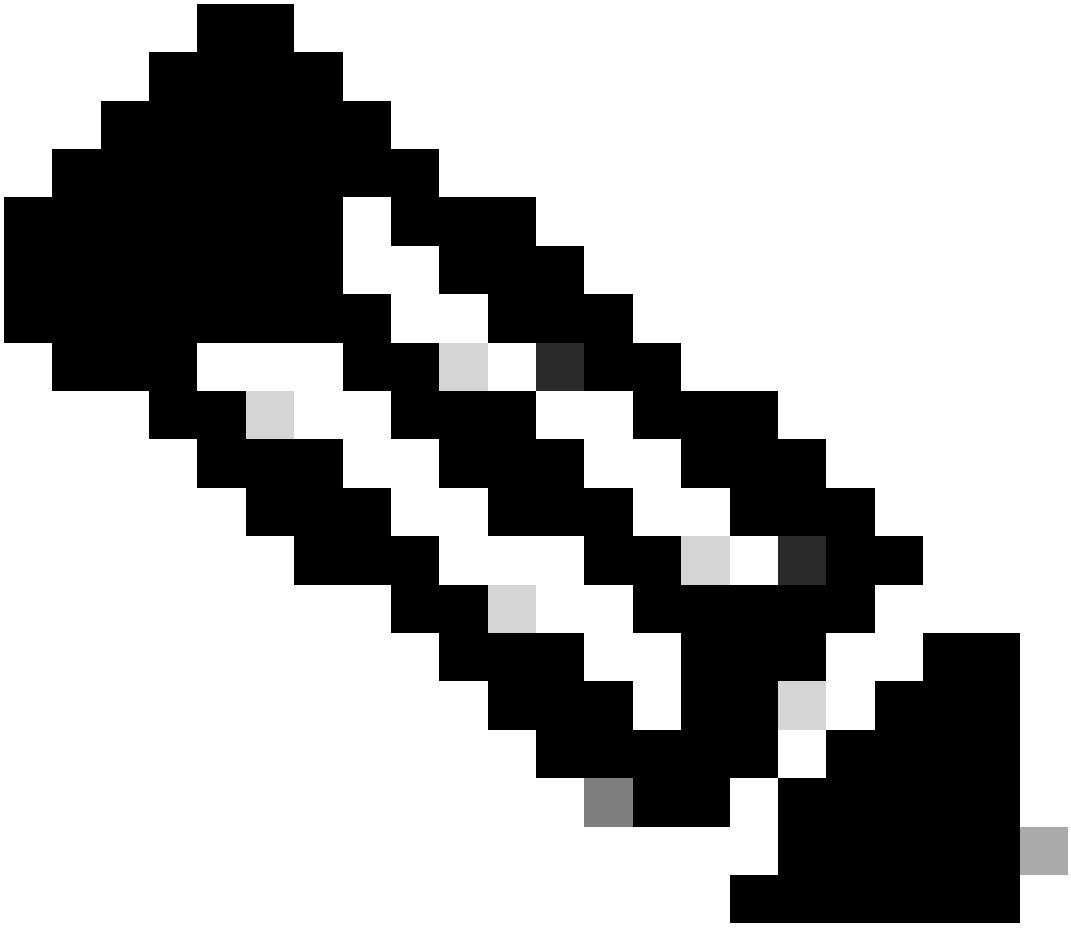


Nota: Partner Hub è diverso da Control Hub. In Partner Hub, i Clienti sono visualizzati nel riquadro di sinistra e Partner Hub nel riquadro del titolo.

2. Selezionare Organization Settings > BroadWorks Calling e fare clic su Download Webex CA.



Pagina Impostazioni organizzazione con il collegamento per il download del certificato



Nota: scegliere l'opzione più recente. In questa schermata, è possibile vedere l'ultima versione è Scarica certificato Webex CA (2023)

3. Il certificato qui indicato. L'immagine è offuscata per motivi di sicurezza.

1

2

: è buona norma verificare che ogni nuovo file contenga un solo certificato e che gli indicatori BEGIN e END siano inclusi correttamente.

Copia file

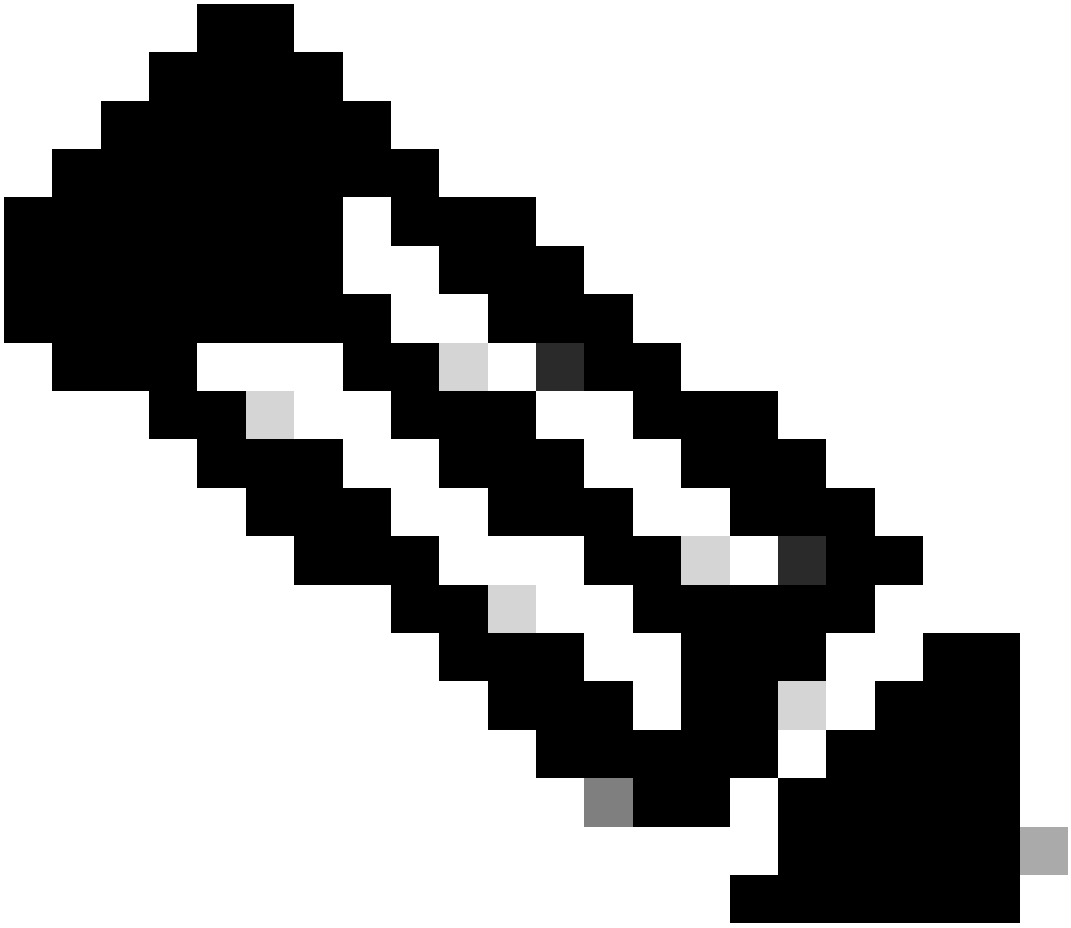
Copiare entrambi i file root2023.txt e issuer2023.txt in una directory temporanea dell'XSP/ADP, ad esempio /var/broadworks/tmp/. A tale scopo, è possibile utilizzare WinSCP o un'altra applicazione simile.

```
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
```

Aggiorna trust anchor

Caricare i file dei certificati per stabilire nuovi trust anchor. Da CTI XSP/ADP BWCLI, eseguire questi comandi:

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



Nota: ogni alias deve essere univoco. Ad esempio, webexclientroot2023 e webexclientissuing2023 fungono da alias di esempio per i trust anchor. È possibile creare alias personalizzati, assicurandosi che ognuno sia distinto.

Conferma aggiornamento

Confermare l'aggiornamento dei punti di ancoraggio eseguendo questo comando

```
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]
```

L'interfaccia CTI è stata aggiornata con il certificato più recente.

Controlla handshake TLS

Notare che il log TLS Tomcat deve essere abilitato con la gravità FieldDebug per visualizzare l'handshake SSL.

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

Il debug TLS è disponibile solo in ADP 202.10 e versioni successive. Vedere Impostazione e chiusura della connessione crittografica ai log di Cisco BroadWorks.

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).