Update van vertrouwen voor CTI-interface in Webex voor breedbandverbindingen

Inhoud

Inleiding

In dit document wordt beschreven hoe u vertrouwensankers voor de CTI-interface in Webex for Broadworks kunt bijwerken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Bekendheid met het configureren van instellingen in de Control Hub
- Begrijpen hoe u de Broadworks Command Line Interface (CLI) kunt configureren en navigeren.
- Basiskennis van SSL/TLS-protocollen en certificaatverificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op Broadworks R22 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document gaat ervan uit dat Broadworks XSP/ADP-hosts een internetverbinding hebben.

Configureren

Deze procedure houdt in het downloaden van specifieke certificaatbestanden, splitsen ze, kopiëren ze naar bepaalde locaties op uw XSP, en dan uploaden van deze certificaten als nieuwe vertrouwensankers. Het is een belangrijke taak die u helpt om een veilige en betrouwbare communicatie tussen uw XSP en Webex te garanderen.

Dit document toont de stappen om voor het eerst Trustankers voor de CTI-interface te installeren. Dit is hetzelfde proces wanneer u deze moet bijwerken. Deze handleiding beschrijft de stappen om de benodigde certificaatbestanden te verkrijgen, deze in afzonderlijke certificaten te splitsen en vervolgens te uploaden naar nieuwe vertrouwensankers op de XSP|ADP.

Vertrouwankers instellen en vernieuwen

De initiële setup en eventuele volgende updates zijn hetzelfde proces. Wanneer het toevoegen van vertrouwen voor het eerst, voltooi de stappen en bevestig de vertrouwen worden toegevoegd.

Bij het bijwerken, kunt u de nieuwe trusts toevoegen en of de oude trusts verwijderen nadat de nieuwe zijn geïnstalleerd of beide trusts verlaten. Oude en nieuwe trusts kunnen parallel werken als W4B diensten ondersteuning bij het presenteren van het relevante certificaat om een van beide trusts te matchen.

Kort samengevat:

- Het nieuwe Cisco-vertrouwenscertificaat kan op elk moment worden toegevoegd voordat het oude vertrouwen verloopt.
- Het oudere vertrouwen kan worden verwijderd op hetzelfde moment als het nieuwe wordt toegevoegd of op een later tijdstip als het verrichtingsteam de voorkeur geeft aan die aanpak.

Overzicht van het proces

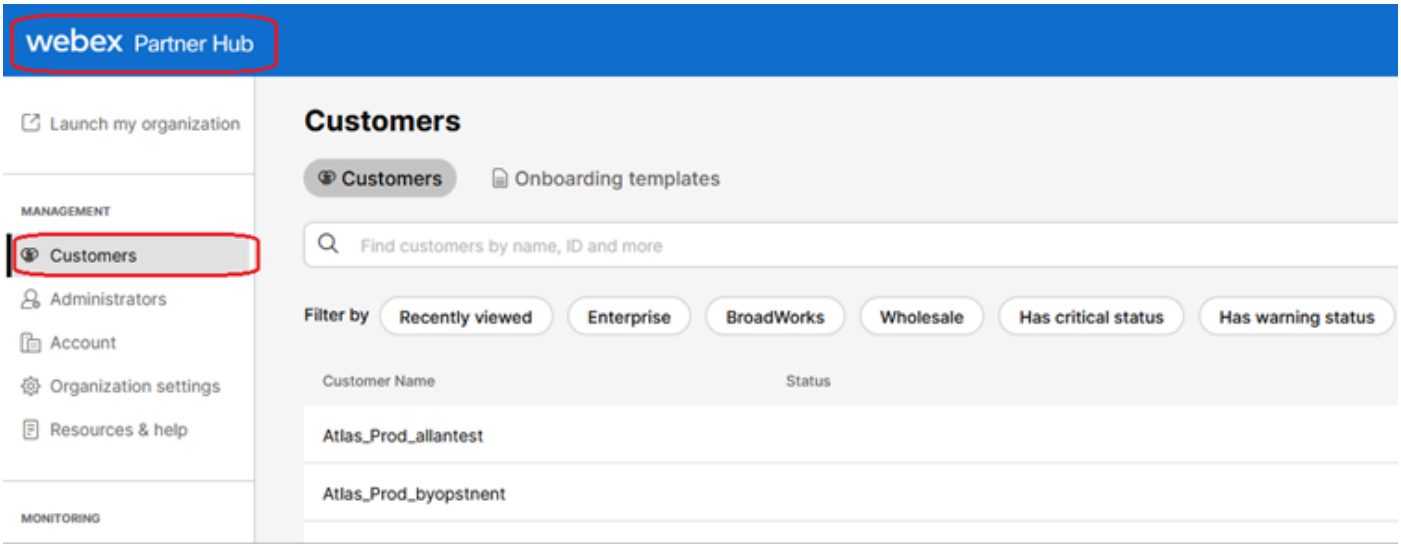
Hier is een overzicht van het proces, dat van toepassing is op zowel de eerste installatie als updates van Trust Anchors:

- Webex CA-certificaat downloaden: Verkrijg het CombinedCertChain2023.txt-bestand van de Partner Hub onder Instellingen > BroadWorks Calling.

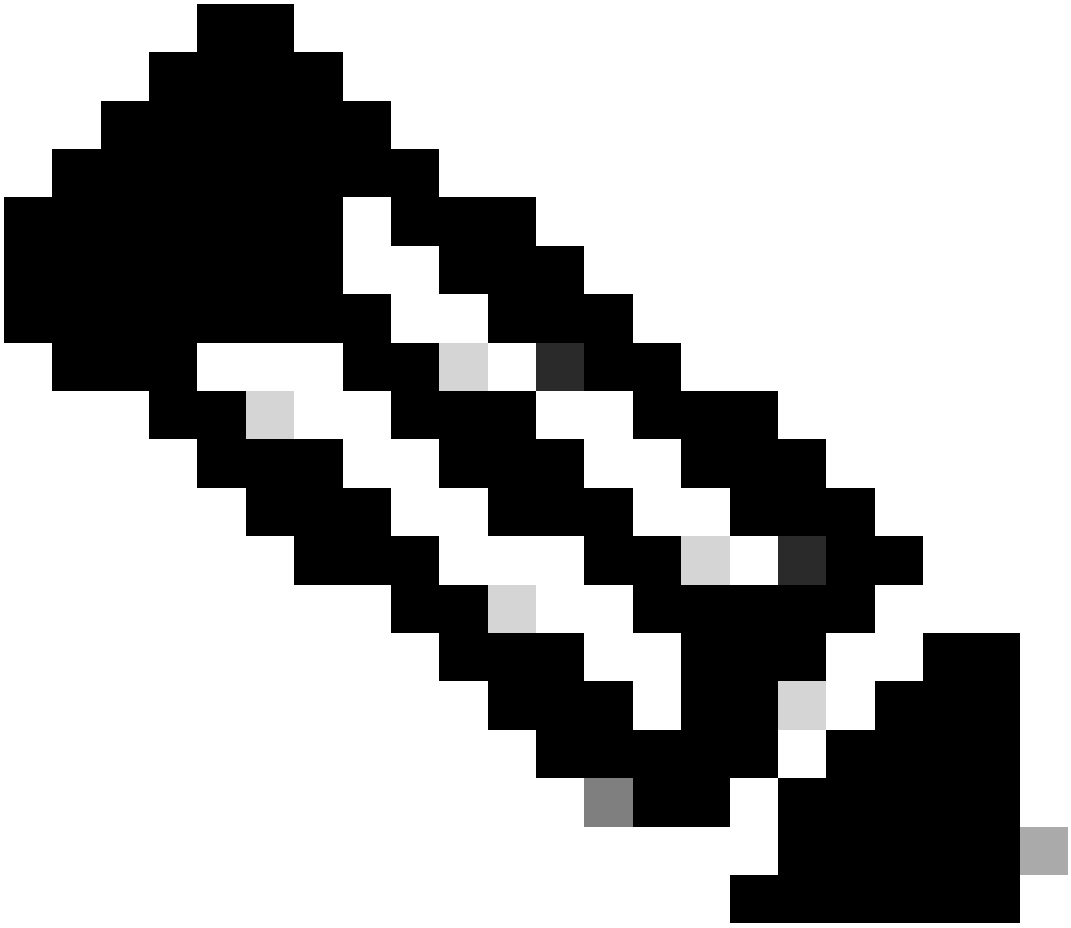
- Splitsen Certificaatketen: Splitsen van het gecombineerde certificaat kettingbestand in twee afzonderlijke certificaat bestanden, root2023.txt en issue2023.txt, met behulp van een teksteditor.
- Bestanden kopiëren: beide certificaatbestanden overbrengen naar een tijdelijke locatie op de XSP|ADP.
- Update Trust Anchors: Gebruik de updateTrust opdracht binnen de XSP|ADP opdrachtregel interface om de certificaatbestanden te uploaden naar nieuwe vertrouwensankers.
- Bevestig Update: Controleer dat de trust ankers met succes worden bijgewerkt.

Webex CA-certificaat downloaden

1. Meld u aan bij de Partner Hub.



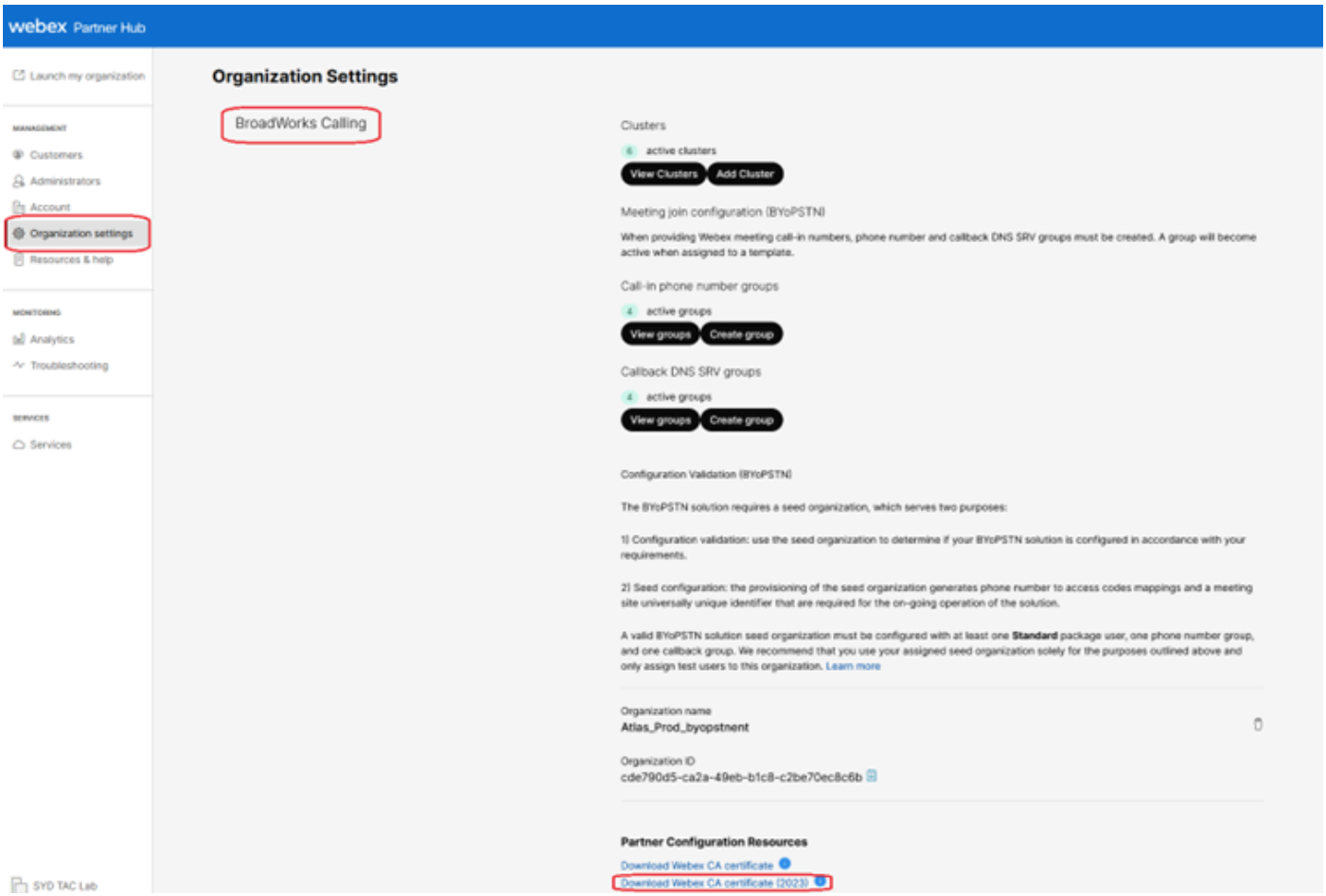
Webex Partner Hub



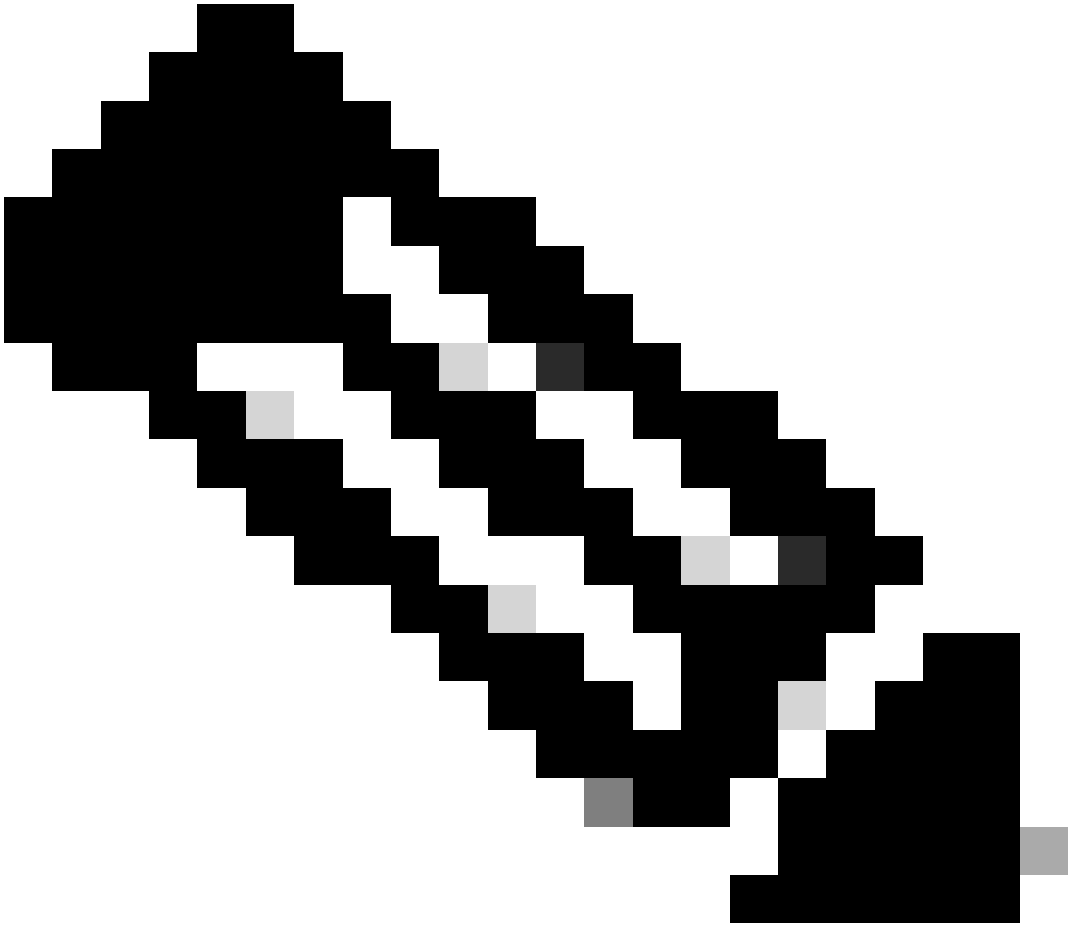
Opmerking: Partnerhub is anders dan Control Hub. In Partner Hub ziet u Klanten in het linker deelvenster en Partner Hub in het titelvenster.

---

2. Ga naar Organisaties > BroadWorks Calling en klik op Download Webex CA.



Organisatieinstelling Pagina met certificaat Download Link



Opmerking: kies de meest recente optie. In deze screenshot, kunt u het laatste is Download Webex CA certificaat (2023)

3. Het hier getoonde certificaat. De afbeelding is om veiligheidsredenen verduisterd.

1

2

: het is een goede gewoonte om te controleren dat elk nieuw bestand slechts één certificaat bevat en dat de begin- en eindmarkeringen correct zijn opgenomen.

Bestanden kopiëren

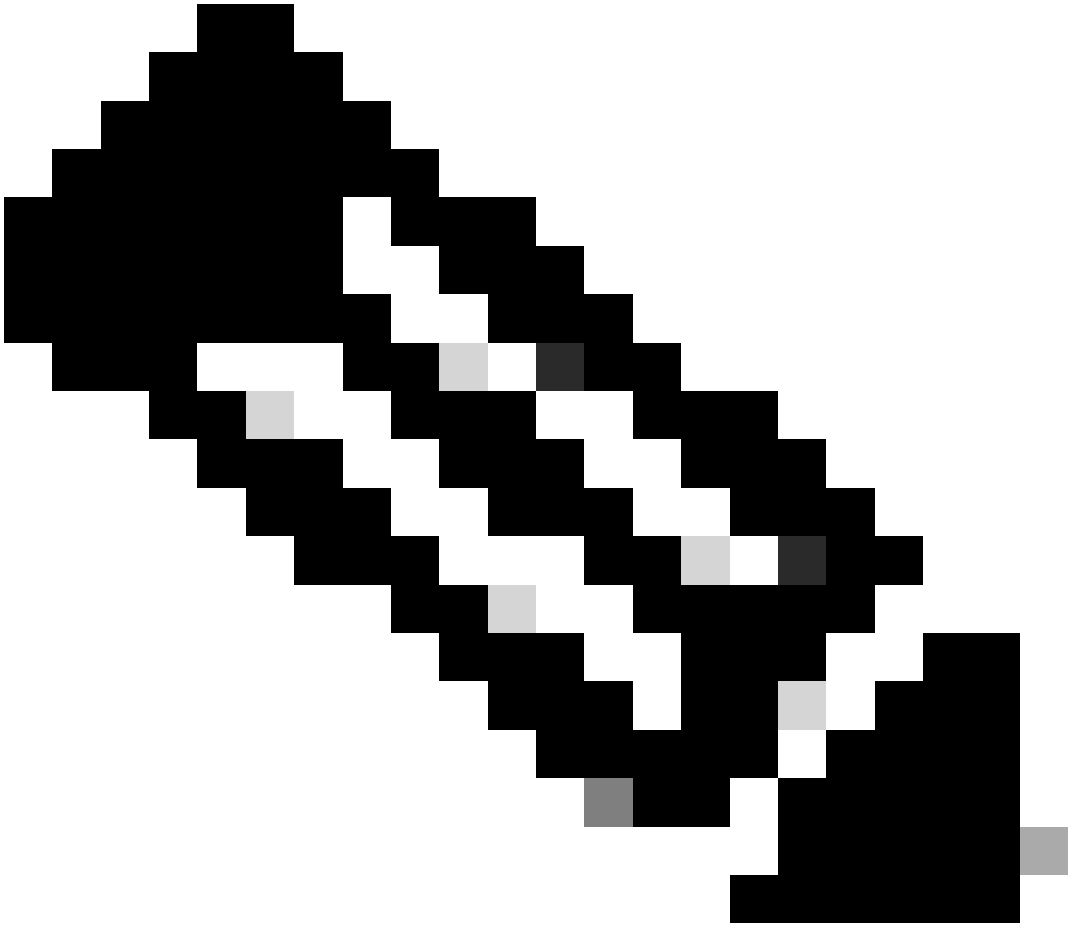
Kopieer zowel root2023.txt en issu2023.txt naar een tijdelijke directory op de XSP/ADP zoals /var/Broadworks/tmp/. Dit kan worden gedaan met WinSCP of een andere soortgelijke toepassing.

```
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
```

Trustankers bijwerken

Upload certificaatbestanden om nieuwe vertrouwensankers op te zetten. Vanuit CTI XSP/ADP BWCLI geeft u deze opdrachten uit:

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



Opmerking: elk alias moet uniek zijn. Bijvoorbeeld, webexclientroot2023 en webexclientissing2023 dienen als voorbeeldaliassen voor de vertrouwensankers. Voel je vrij om aangepaste aliassen te creëren, ervoor te zorgen dat elke één verschillend is.

Update bevestigen

Bevestig dat de ankers worden bijgewerkt door dit bevel uit te geven

```
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]
```

Uw CTI-interface is nu bijgewerkt met het nieuwste certificaat.

TLS-handdruk controleren

Merk op dat het TLS-logbestand van Tomcat moet zijn ingeschakeld bij de FieldDebug-ernst om SSL-handshake te bekijken.

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

TLS debug is alleen in ADP 2022.10 en hoger. Zie Installatie en verwijdering van cryptografische verbindingen in Cisco BroadWorks.

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.