

Aktualisieren der Vertrauenswürdigkeit für die CTI-Schnittstelle in WebEx für Broadworks

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Einrichten und Erneuern von Vertrauensankern](#)

[Prozessübersicht](#)

[WebEx Zertifizierungsstellenzertifikat herunterladen](#)

[Zertifikatskette aufteilen](#)

[Für das erste Zertifikat \(Stammzertifikat\):](#)

[Für das zweite Zertifikat \(ausstellendes Zertifikat\):](#)

[Dateien kopieren](#)

[Vertrauenswürdige Anker aktualisieren](#)

[Aktualisierung bestätigen](#)

[TLS-Handshake überprüfen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Prozess zum Aktualisieren von Vertrauensankern für die CTI-Schnittstelle in WebEx für Broadworks beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Vertrautheit mit der Konfiguration von Einstellungen im Control Hub
- Grundlegendes zum Konfigurieren und Navigieren in der Broadworks-Befehlszeilenschnittstelle (CLI).
- Grundlegendes Verständnis der SSL/TLS-Protokolle und der Zertifikatsauthentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Broadworks R22 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird davon ausgegangen, dass Broadworks XSP/ADP-Hosts auf das Internet ausgerichtet sind.

Konfigurieren

Bei diesem Verfahren werden bestimmte Zertifikatsdateien heruntergeladen, aufgeteilt, an bestimmte Speicherorte des XSP kopiert und dann als neue Vertrauensanker hochgeladen. Dies ist eine wichtige Aufgabe, die die sichere und vertrauenswürdige Kommunikation zwischen Ihrem XSP und WebEx sicherstellt.

In diesem Dokument werden die Schritte zur Erstinstallation von Trust Anchors für die CTI-Schnittstelle beschrieben. Dies ist der gleiche Prozess, wenn Sie sie aktualisieren müssen. Dieses Handbuch beschreibt die Schritte zum Abrufen der erforderlichen Zertifikatsdateien, deren Aufteilung in einzelne Zertifikate und das Hochladen dieser Dateien auf neue Vertrauensanker auf dem XSP|ADP.

Einrichten und Erneuern von Vertrauensankern

Die Ersteinrichtung und alle nachfolgenden Updates erfolgen nach demselben Verfahren. Führen Sie beim erstmaligen Hinzufügen von Vertrauensstellungen die Schritte aus, und bestätigen Sie, dass die Vertrauensstellungen hinzugefügt wurden.

Bei der Aktualisierung können Sie die neuen Vertrauensstellungen hinzufügen und entweder die alten Vertrauensstellungen löschen, nachdem die neuen installiert wurden, oder beide Vertrauensstellungen beibehalten. Alte und neue Trusts können parallel arbeiten, da die W4B-Services die Vorlage des entsprechenden Zertifikats für einen der beiden Trusts unterstützen.

Zusammenfassung:

- Das neue Cisco Vertrauenszertifikat kann jederzeit hinzugefügt werden, bevor die alte Vertrauensstellung abläuft.
- Die ältere Vertrauensstellung kann gleichzeitig mit dem Hinzufügen der neuen Vertrauensstellung oder zu einem späteren Zeitpunkt entfernt werden, wenn das Operations Team diesen Ansatz bevorzugt.

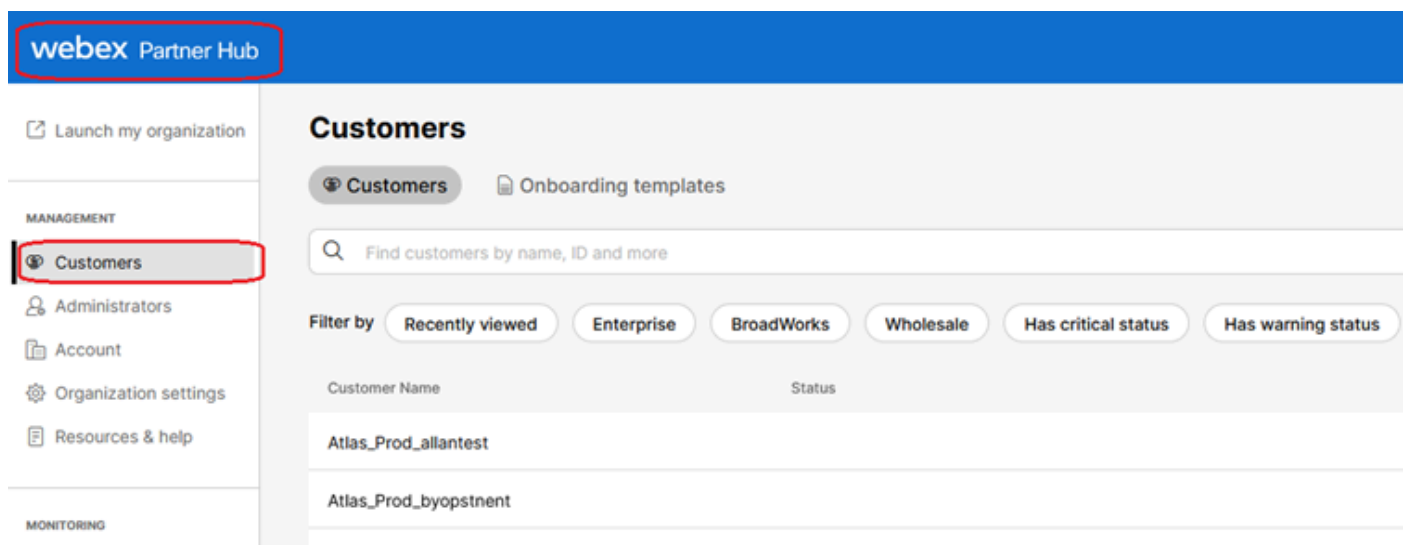
Prozessübersicht

Nachfolgend finden Sie eine Übersicht über den Prozess, der sowohl für die Erstinstallation als auch für Updates von Trust Anchors gilt:

- Laden Sie das WebEx CA-Zertifikat herunter: Rufen Sie die Datei CombinedCertChain2023.txt unter Einstellungen > BroadWorks-Aufrufe vom Partner Hub ab.
- Zertifikatskette aufteilen: Teilen Sie die kombinierte Zertifikatskettendatei mithilfe eines Texteditors in zwei separate Zertifikatdateien root2023.txt und Issuing2023.txt.
- Dateien kopieren: Übertragen Sie beide Zertifikatsdateien an einen temporären Speicherort auf dem XSP|ADP.
- Update Trust Anchors (Vertrauenswürdige Anker aktualisieren): Verwenden Sie den Befehl updateTrust in der XSP|ADP-Befehlszeilenschnittstelle, um die Zertifikatsdateien auf neue Vertrauensanker hochzuladen.
- Update bestätigen: Überprüfen Sie, ob die Vertrauensanker erfolgreich aktualisiert wurden.

WebEx Zertifizierungsstellenzertifikat herunterladen

1. Melden Sie sich bei Partner Hub an.



The screenshot shows the WebEx Partner Hub interface. The top navigation bar is blue with the 'webex Partner Hub' logo. On the left, there is a sidebar with a 'MANAGEMENT' section containing 'Customers', 'Administrators', 'Account', 'Organization settings', and 'Resources & help'. The 'Customers' item is highlighted with a red box. The main content area is titled 'Customers' and includes a search bar, filter buttons (Recently viewed, Enterprise, BroadWorks, Wholesale, Has critical status, Has warning status), and a table with columns for 'Customer Name' and 'Status'. The table lists two customers: 'Atlas_Prod_allantest' and 'Atlas_Prod_byopstnent'.

WebEx Partner-Hub



Hinweis: Partner Hub unterscheidet sich von Control Hub. Im Partner Hub werden Kunden im linken Bereich und Partner Hub im Titelbereich angezeigt.

2. Gehen Sie zu Organisationseinstellungen > BroadWorks-Anrufe, und klicken Sie auf WebEx CA herunterladen.

[Launch my organization](#)

MANAGEMENT

- [Customers](#)
- [Administrators](#)
- [Account](#)
- [Organization settings](#)**
- [Resources & help](#)

MONITORING

- [Analytics](#)
- [Troubleshooting](#)

SERVICES

- [Services](#)

SYD TAC Lab

Organization Settings

BroadWorks Calling

Clusters

4 active clusters

[View Clusters](#) [Add Cluster](#)

Meeting join configuration (BYoPSTN)

When providing Webex meeting call-in numbers, phone number and callback DNS SRV groups must be created. A group will become active when assigned to a template.

Call-in phone number groups

4 active groups

[View groups](#) [Create group](#)

Callback DNS SRV groups

4 active groups

[View groups](#) [Create group](#)

Configuration Validation (BYoPSTN)

The BYoPSTN solution requires a seed organization, which serves two purposes:

- 1) Configuration validation: use the seed organization to determine if your BYoPSTN solution is configured in accordance with your requirements.
- 2) Seed configuration: the provisioning of the seed organization generates phone number to access codes mappings and a meeting site universally unique identifier that are required for the on-going operation of the solution.

A valid BYoPSTN solution seed organization must be configured with at least one **Standard** package user, one phone number group, and one callback group. We recommend that you use your assigned seed organization solely for the purposes outlined above and only assign test users to this organization. [Learn more](#)

Organization name

Atlas_Prod_byopstnt

Organization ID

cde790d5-ca2a-49eb-b1c8-c2be70ec8c6b

Partner Configuration Resources

[Download Webex CA certificate](#)[Download Webex CA certificate \(2023\)](#)

Seite "Organisationseinstellungen" mit Link zum Herunterladen des Zertifikats



Hinweis: Wählen Sie die neueste Option aus. In diesem Screenshot können Sie sehen, dass das neueste Download WebEx CA-Zertifikat (2023)

3. Das hier gezeigte Zertifikat. Das Bild wird aus Sicherheitsgründen verschleiert.

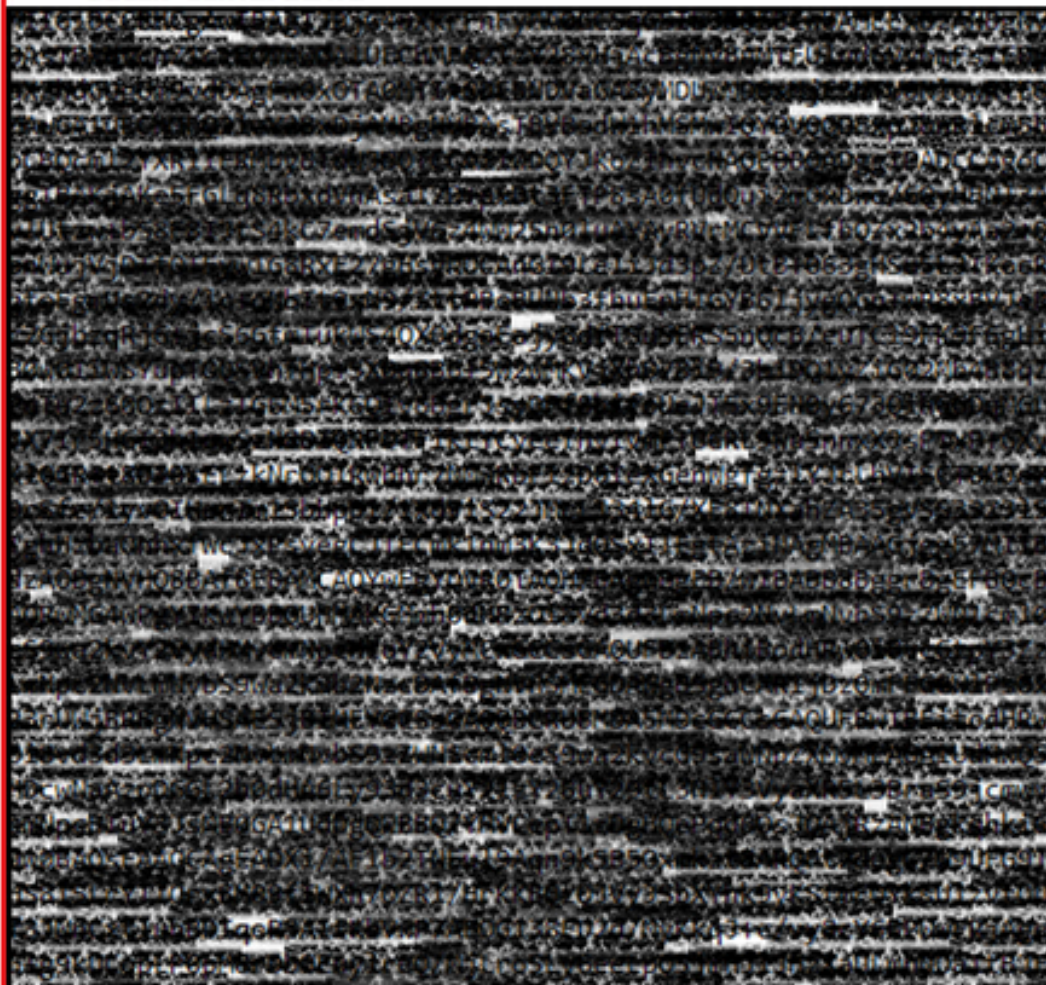
-----BEGIN CERTIFICATE-----



1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----



2

: Es empfiehlt sich, zu überprüfen, ob jede neue Datei nur ein Zertifikat enthält und ob die Kennzeichnungen BEGIN und END korrekt enthalten sind.

Dateien kopieren

Kopieren Sie sowohl root2023.txt als auch Issuing2023.txt in ein temporäres Verzeichnis auf dem XSP/ADP, z. B. /var/Broadworks/tmp/. Dies kann mithilfe von WinSCP oder einer anderen ähnlichen Anwendung erfolgen.

```
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
```

Vertrauenswürdige Anker aktualisieren

Laden Sie Zertifikatsdateien hoch, um neue Vertrauensanker einzurichten. Geben Sie im CTI XSP/ADP BWCLI die folgenden Befehle ein:

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




Hinweis: Jeder Alias muss eindeutig sein. Beispielsweise dienen webexclientroot2023 und webexclientissuing2023 als Beispielalias für die Vertrauensanker. Sie können auch eigene Aliase erstellen, um sicherzustellen, dass jeder von ihnen unterschiedlich ist.

Aktualisierung bestätigen

Bestätigen Sie mit diesem Befehl, dass die Referenzzeichen aktualisiert wurden.

```
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]
```

Ihre CTI-Schnittstelle wurde jetzt mit dem neuesten Zertifikat aktualisiert.

TLS-Handshake überprüfen

Beachten Sie, dass das Tomcat TLS-Protokoll bei dem Schweregrad FieldDebug aktiviert werden muss, um SSL-Handshake anzuzeigen.

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

TLS-Debugging ist nur in ADP 202.10 und höher verfügbar. Siehe [Einrichten und Beenden der kryptografischen Protokollverbindung von Cisco BroadWorks](#).

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.