

在Webex for Broadworks中更新CTI介面的信任關係

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[設定與更新信任錨點](#)

[流程概要](#)

[下載Webex CA憑證](#)

[分割憑證鏈結](#)

[對於第一個憑證 \(根憑證\) :](#)

[對於第二個證書 \(頒發證書\) :](#)

[複製檔案](#)

[更新信任錨點](#)

[確認更新](#)

[檢查TLS握手](#)

[相關資訊](#)

簡介

本檔案介紹在Webex for Broadworks中更新CTI介面信任錨點的程式。

必要條件

需求

思科建議您瞭解以下主題：

- 熟悉控制中心中的設定配置
- 瞭解如何配置和導航Broadworks命令列介面(CLI)。
- 對SSL/TLS協定和證書身份驗證有基本的瞭解

採用元件

本文檔中的資訊基於Broadworks R22及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設

) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本檔案假設Broadworks XSP/ADP主機面向網際網路。

設定

此程式包括下載特定憑證檔案、將其分割、複製到XSP上的特定位置，然後將這些憑證作為新的信任錨點上傳。這是一項重要任務，有助於確保XSP和Webex之間的安全和可信通訊。

本文檔介紹首次為CTI介面安裝Trust Anchors的步驟。當您需要更新它們時，這是相同的過程。本指南概述了獲取所需證書檔案、將其拆分為各個證書，然後將其上傳到XSP|ADP上的新信任錨點的步驟。

設定與更新信任錨點

初始設定和任何後續更新都是相同的過程。首次增加信任時，請完成這些步驟並確認已增加信任。

更新時，您可以新增信任，並在安裝新信任後刪除舊信任，或保留兩個信任。舊信任和新信任可以並行工作，因為W4B服務支援提供相關證書以匹配兩個信任中的任何一個。

總結一下：

- 新的思科信任證書可以在舊信任到期之前隨時增加。
- 舊信任可在新增新信任的同時移除，若作業團隊偏好該方式，則可在稍後移除舊信任。

流程概要

以下是該過程的概述，適用於初始安裝和對Trust Anchors的更新：

- 下載Webex CA證書：在Settings > BroadWorks Calling下，從合作夥伴中心獲取CombinedCertChain2023.txt檔案。
- 拆分證書鏈：使用文本編輯器將組合的證書鏈檔案拆分為兩個單獨的證書檔案：root2023.txt和issuing2023.txt。
- 複製檔案：將兩個憑證檔案傳輸到XSP|ADP上的暫存位置。
- 更新信任錨點：使用XSP|ADP命令列介面中的updateTrust命令將證書檔案上傳到新的信任錨點。
- 確認更新：驗證信任錨點是否已成功更新。

下載Webex CA憑證

1. 登入合作夥伴中心。

webex Partner Hub

Launch my organization

MANAGEMENT

- Customers**
- Administrators
- Account
- Organization settings
- Resources & help

MONITORING

Customers

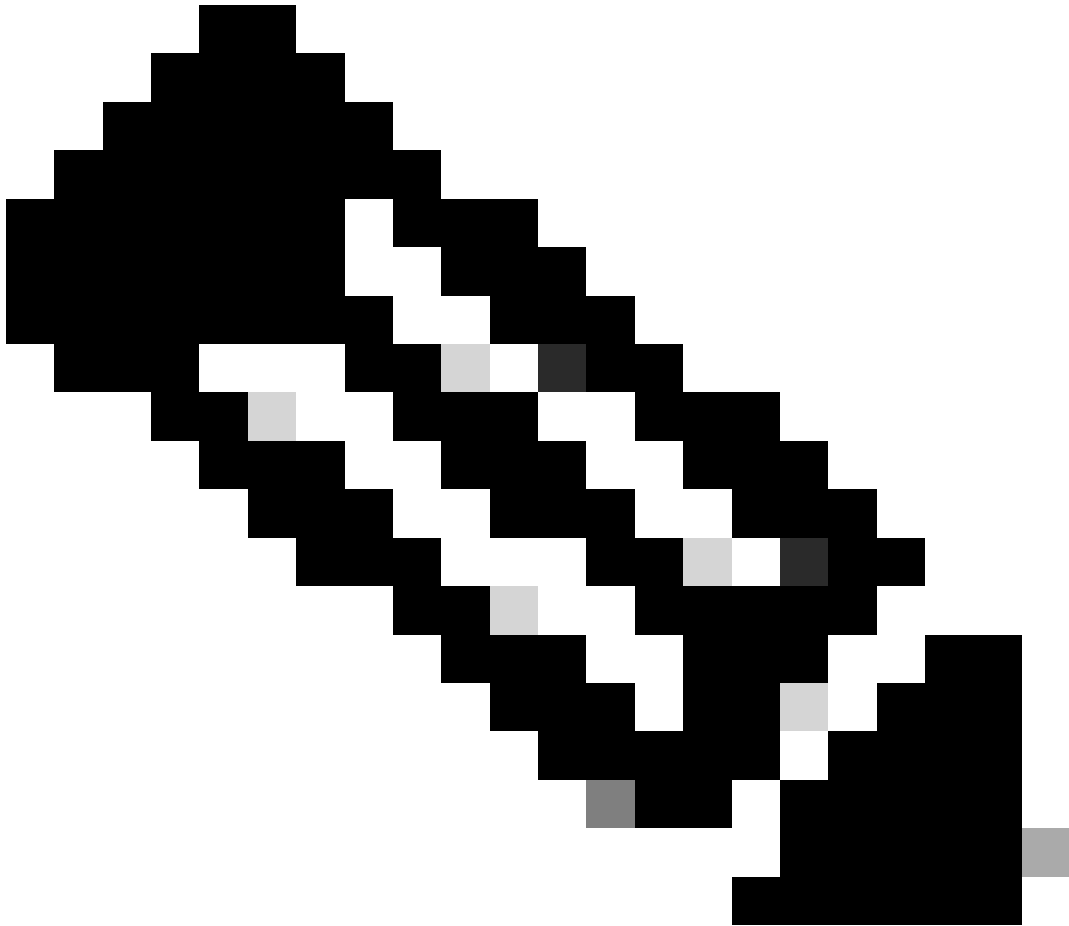
Customers Onboarding templates

Find customers by name, ID and more

Filter by: Recently viewed Enterprise BroadWorks Wholesale Has critical status Has warning status

Customer Name	Status
Atlas_Prod_allantest	
Atlas_Prod_byopstnent	

Webex合作夥伴中心



注意：合作夥伴中心與控制中心不同。在Partner Hub中，您可以在左側窗格中看到Customers，在標題窗格中看到Partner Hub。

2. 轉到組織設定> BroadWorks Calling , 然後按一下下載Webex CA。

The screenshot displays the 'Organization Settings' page in the Webex Partner Hub. The left sidebar contains navigation options: 'Launch my organization', 'MANAGEMENT' (Customers, Administrators, Account, **Organization settings**, Resources & help), 'MONITORING' (Analytics, Troubleshooting), and 'SERVICES' (Services). The main content area is titled 'Organization Settings' and features a red box around the 'BroadWorks Calling' link. Below this, there are sections for 'Clusters' (1 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), and 'Callback DNS SRV groups' (4 active groups, View groups, Create group). A 'Configuration Validation (BYoPSTN)' section explains that 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](#). Below this, the 'Organization name' is 'Atlas_Prod_byopstnt' and the 'Organization ID' is 'cde790d5-ca2a-49eb-b1c8-c2be70ec8c6b'. At the bottom, under 'Partner Configuration Resources', there are two links: 'Download Webex CA certificate' and 'Download Webex CA certificate (2023)', with the latter being highlighted by a red box.

顯示憑證下載連結的組織設定頁面



附註：選擇最新的選項。在此螢幕截圖中，您可以看到最新版本為Download Webex CA certificate (2023)

3. 此處顯示的憑證。出於安全原因，對映像進行模糊處理。

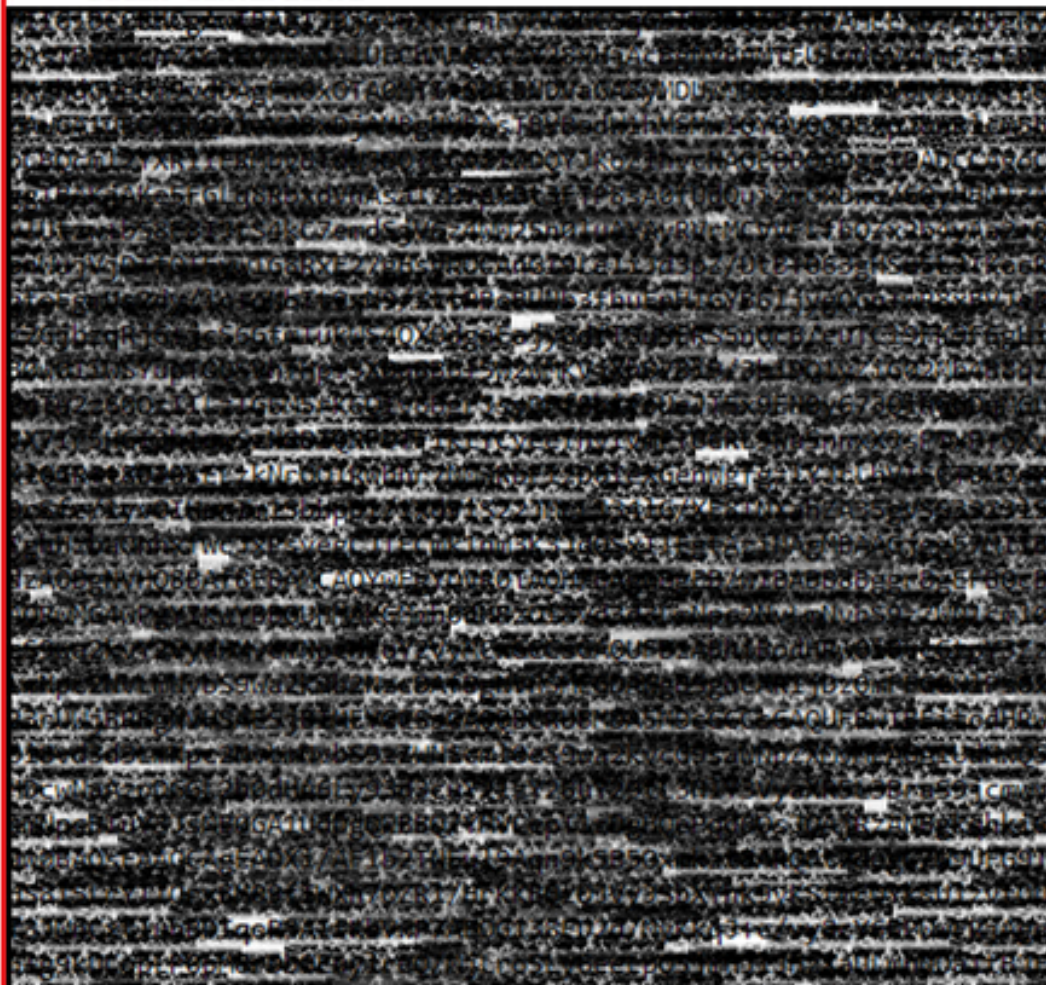
-----BEGIN CERTIFICATE-----



1

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

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



2

之前，需要拆分這些檔案。若要將憑證鏈結分割為個別憑證，請完成以下步驟。此程式顯示將合併的憑證檔案分成根目錄和發行憑證的步驟。

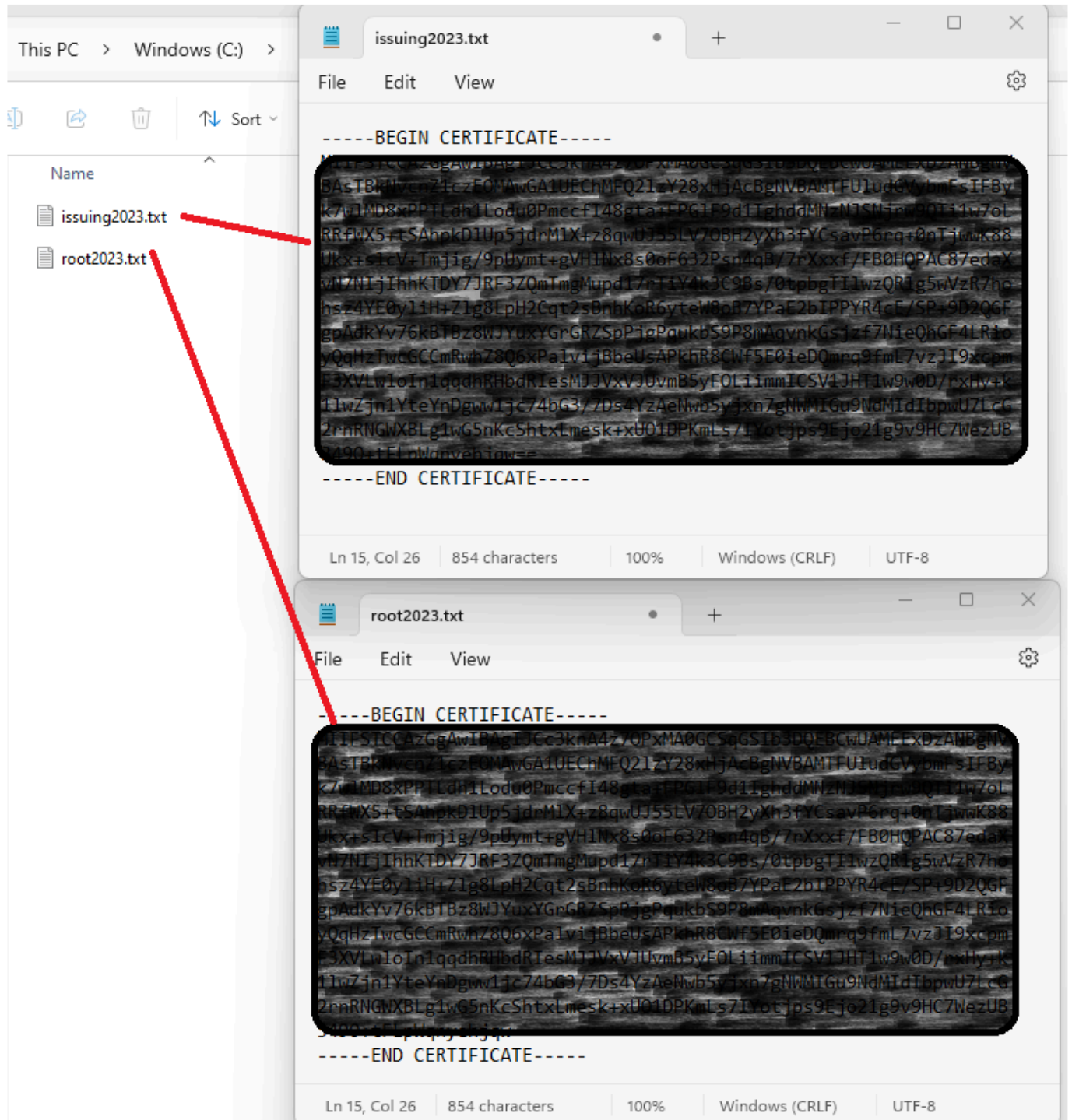
1. 合併的證書檔案被分割為2個單獨的證書。
 - root2023.txt
 - issuing2023.txt
2. 辨識各個證書。
 - 該檔案包含由標籤-----BEGIN CERTIFICATE-和-----END CERTIFICATE-描述的多個證書。每個區塊代表一個憑證。
3. 拆分證書
 - 若要分割憑證鏈，您必須為您辨識的每個憑證區塊建立新的文字檔。

對於第一個憑證（根憑證）：

- 選擇文本的第一塊，包括-----BEGIN CERTIFICATE—和-----END CERTIFICATE—行。
- 複製選取的文字。
- 開啟新的文字檔案，並將複製的文字貼到此檔案中。
- 將新檔案另存為root2023.txt

對於第二個證書（頒發證書）：

- 返回原始的組合憑證鏈結檔案。
- 選取第二個文字區塊（鏈結中的下一個憑證），包括-----BEGIN CERTIFICATE—和-----END CERTIFICATE—行。
- 重複複製所選文字、將其貼入新文字檔案，以及將檔案另存為issuing2023.txt的程式



密文分割憑證



注意：最好是驗證每個新檔案只包含一個證書，並且正確包括BEGIN和END標籤。

複製檔案

將root2023.txt和issuing2023.txt複製到XSP/ADP上的臨時目錄(例如/var/broadworks/tmp/)。您可以使用WinSCP或任何其他類似應用程式來完成此操作。

```
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
```

更新信任錨點

上傳憑證檔案以建立新的信任錨點。在CTI XSP/ADP BWCLI中，發出以下命令：

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

注意：每個別名都必須是唯一的。例如，webexclientroot2023和webexclientssuing2023用作信任錨點的示例別名。您可以隨意建立自訂別名，確保每個別名都是不同的。

確認更新

透過發出以下命令確認錨點已更新

```
XSP|ADP_CLI/Interface/CTI/SSLCommonSettings/ClientAuthentication/Trusts> get  
Alias Owner Issuer
```

```
=====  
webexclientssuing2023 Internal Private TLS SubCA Internal Private Root  
webexclientroot2023 Internal Private Root Internal Private Root[self-signed]
```

您的CTI介面現已更新為最新的證書。

檢查TLS握手

請注意，需要以FieldDebug嚴重性啟用Tomcat TLS日誌，才能檢視SSL握手。

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

TLS調試僅在ADP 2022.10及更高版本中。請參閱[Cisco BroadWorks Log Cryptographic Connection Setup and Teardown](#)。

相關資訊

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。