

# 在面向Broadworks的Webex中更新CTI接口的信任关系

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[设置和续订信任锚点](#)

[流程概述](#)

[下载Webex CA证书](#)

[拆分证书链](#)

[对于第一个证书（根证书）：](#)

[对于第二个证书（颁发证书）：](#)

[复制文件](#)

[更新信任锚点](#)

[确认更新](#)

[检查TLS握手](#)

[相关信息](#)

---

## 简介

本文档介绍在Webex for Broadworks中更新CTI接口的信任锚点的过程。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 熟悉控制中心中的设置配置
- 了解如何配置和导航Broadworks命令行界面(CLI)。
- 对SSL/TLS协议和证书身份验证有基本的了解

### 使用的组件

本文档中的信息基于Broadworks R22及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

本文档假定Broadworks XSP/ADP主机面向互联网。

## 配置

此过程涉及下载特定证书文件，将其拆分，将其复制到XSP上的特定位置，然后将这些证书作为新的信任锚点上传。这是一项重要任务，有助于确保XSP和Webex之间的通信安全可靠。

本文档显示首次为CTI接口安装信任锚点的步骤。在需要更新它们时，此过程也相同。本指南概述了获取必要的证书文件、将其拆分为单个证书，然后将其上传到XSP|ADP上的新信任锚点的步骤。

## 设置和续订信任锚点

初始设置和后续更新过程相同。首次添加信任时，请完成这些步骤并确认已添加信任关系。

更新时，您可以添加新的信任关系，并在安装新信任关系后删除旧信任关系或同时保留这两个信任关系。由于提供相关证书的W4B服务支持可匹配两个信任中的任何一个，因此新旧信任可并行工作。

综述：

- 在旧信任到期之前，可以随时添加新的思科信任证书。
- 旧信任可以在添加新信任的同时删除，如果运营团队更喜欢该方法，也可以在以后某个日期删除。

## 流程概述

以下是对流程的概述，适用于初始安装和对Trust Anchors的更新：

- 下载Webex CA证书：在Partner Hub的Settings > BroadWorks Calling下获取CombinedCertChain2023.txt文件。
- 分割证书链：使用文本编辑器将组合的证书链文件分割为两个单独的证书文件：root2023.txt和issuing2023.txt。
- 复制文件：将两个证书文件传输到XSP|ADP上的临时位置。
- 更新信任锚点：在XSP|ADP命令行界面中使用updateTrust命令将证书文件上传到新的信任锚点。
- 确认更新：验证信任锚点是否已成功更新。

### 下载Webex CA证书

1. 登录到Partner Hub。

**webex Partner Hub**

Launch my organization

**MANAGEMENT**

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

**MONITORING**

### Customers

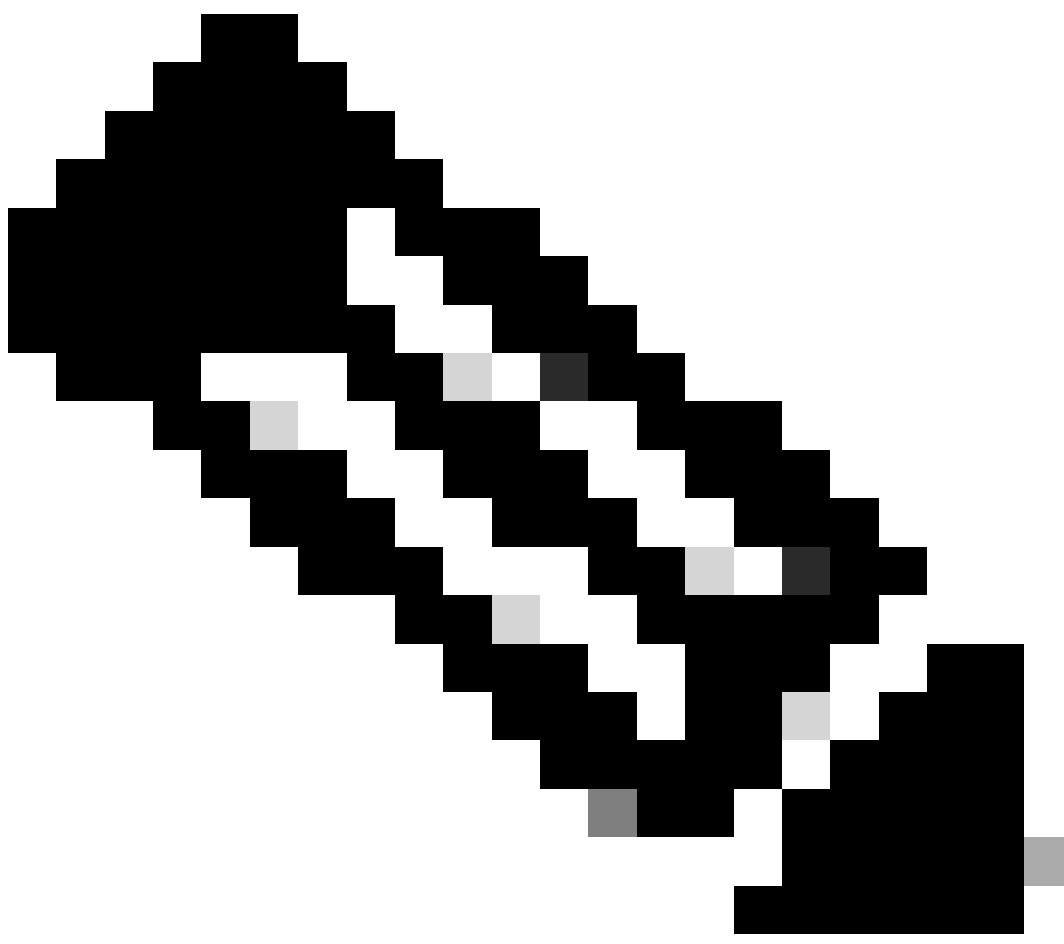
Customers Onboarding templates

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 Partner Hub



注意：Partner Hub与控制 Hub不同。在Partner Hub中，您可以在左侧窗格中看到Customers，在标题窗格中看到Partner Hub。

2. 转至组织设置> BroadWorks呼叫，然后单击下载Webex CA。

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 menu with categories: MANAGEMENT (Launch my organization, Customers, Administrators, Account, Organization settings, Resources & help), MONITORING (Analytics, Troubleshooting), and SERVICES (Services). The 'Organization settings' item is highlighted with a red box. The main content area is titled 'Organization Settings' and features a 'BroadWorks Calling' link at the top, also highlighted with a red box. Below this, there are sections for Clusters (1 active clusters), Meeting join configuration (BYoPSTN), Call-in phone number groups (4 active groups), and Callback DNS SRV groups (4 active groups). Each section has 'View' and 'Add/Create' buttons. A 'Configuration Validation (BYoPSTN)' section explains the requirements for a seed organization. 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 highlighted in red.

显示证书下载链接的组织设置页面



注意：选择最新选项。在此屏幕截图中，您可以看到最新版本为Download Webex CA certificate (2023)

---

3. 此处显示的证书。出于安全原因，对映像进行模糊处理。

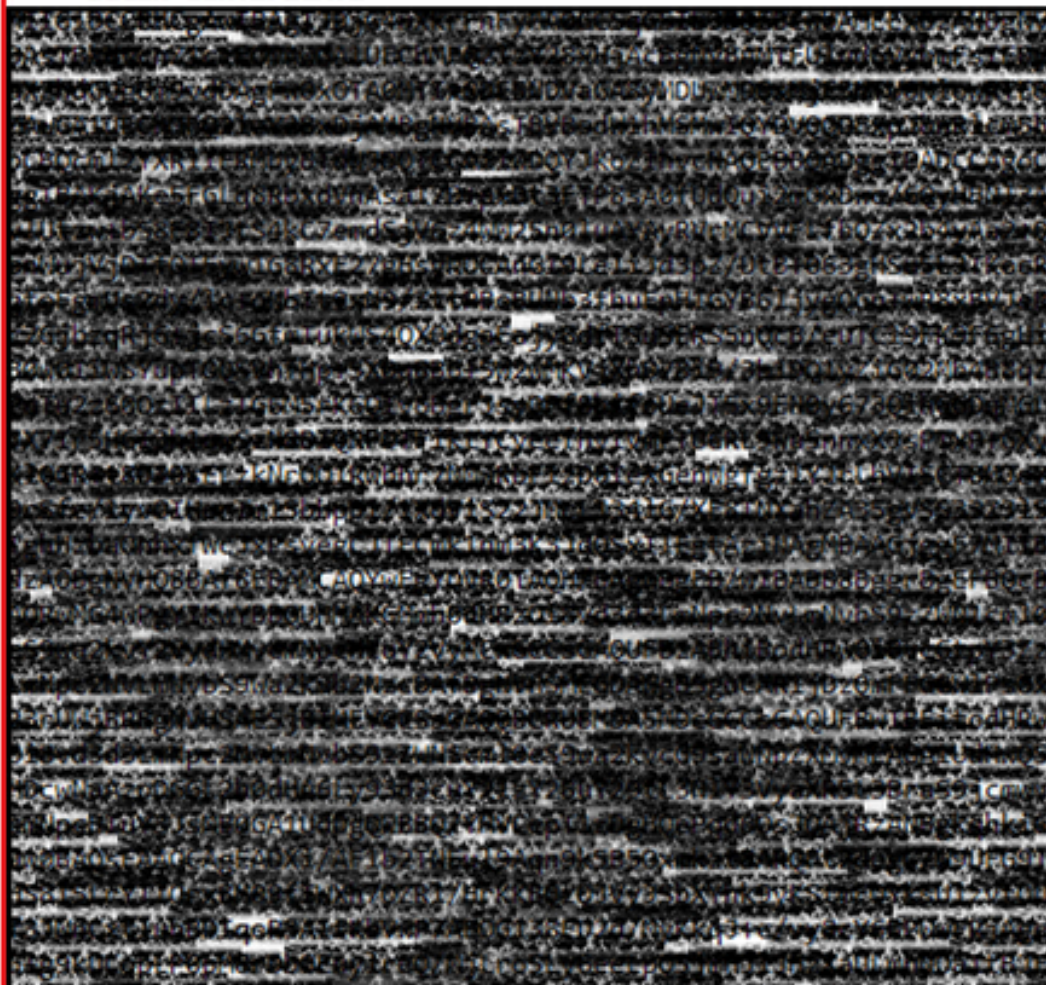
-----BEGIN CERTIFICATE-----



1

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

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



2

之前，需要拆分文件。要将证书链分割为单个证书，请完成以下步骤。此过程显示将合并的证书文件分为根和颁发证书的步骤。

1. 合并的证书文件将拆分为2个单独的证书。

- root2023.txt
- issuing2023.txt

2. 识别各个证书。

- 文件包含由标记-----BEGIN CERTIFICATE - 和-----END CERTIFICATE - 描述的多个证书。每个块代表一个证书。

3. 拆分证书

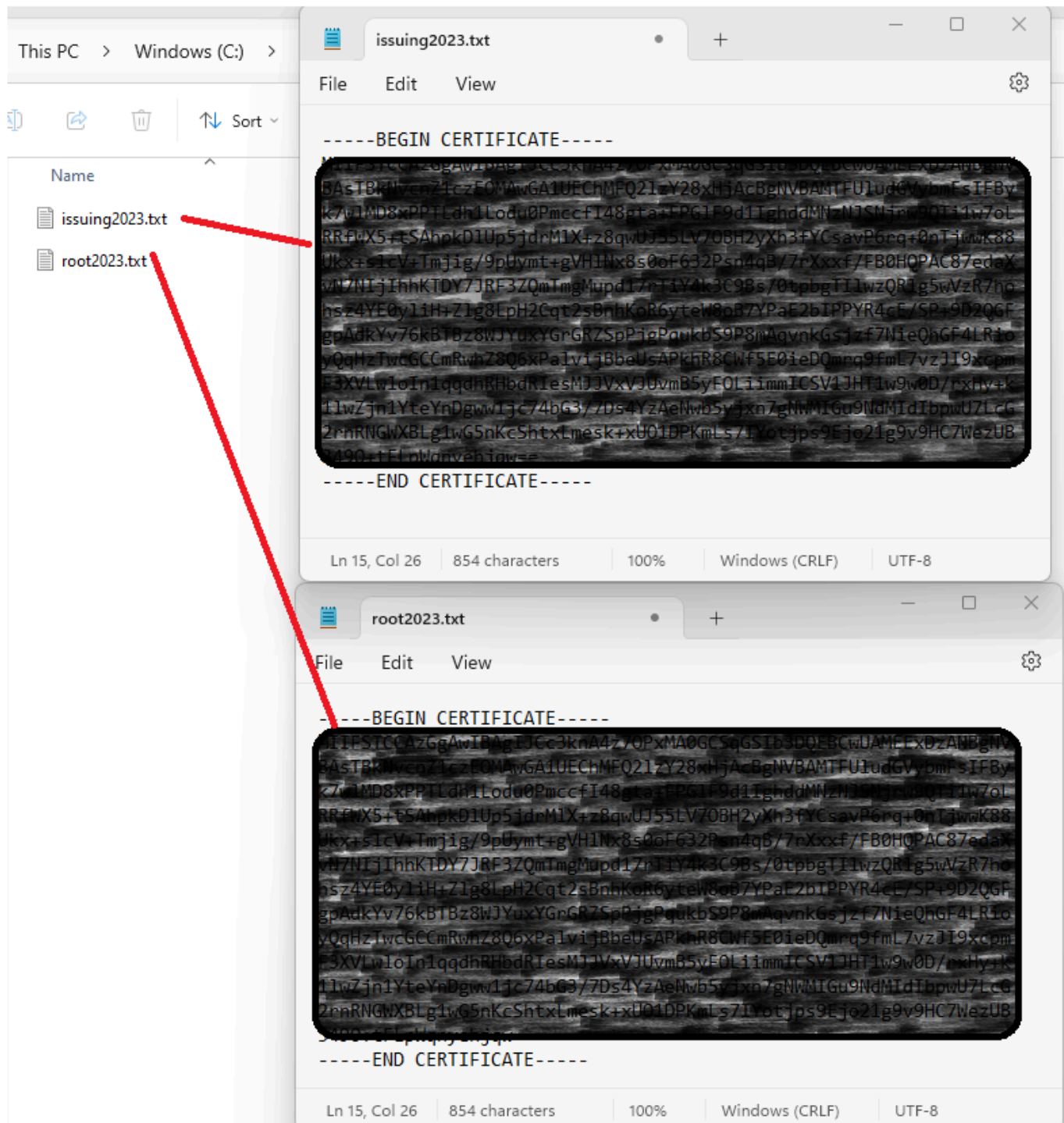
- 要拆分证书链，您必须为您标识的每个证书块创建新的文本文件。

对于第一个证书（根证书）：

- 选择第一个文本块，包括-----BEGIN CERTIFICATE—和-----END CERTIFICATE—行。
- 复制所选文本。
- 打开一个新的文本文件，并将复制的文本粘贴到此文件中。
- 将新文件另存为root2023.txt

对于第二个证书（颁发证书）：

- 返回原始的组合证书链文件。
- 选择第二个文本块（链中的下一个证书），包括-----BEGIN CERTIFICATE—和-----END CERTIFICATE—行。
- 重复复制所选文本、将其粘贴到新文本文件中以及将该文件另存为issuing2023.txt的过程



已编辑的拆分证书





注意：比较好的做法是验证每个新文件仅包含一个证书，并且正确包括BEGIN和END标记。

---

## 复制文件

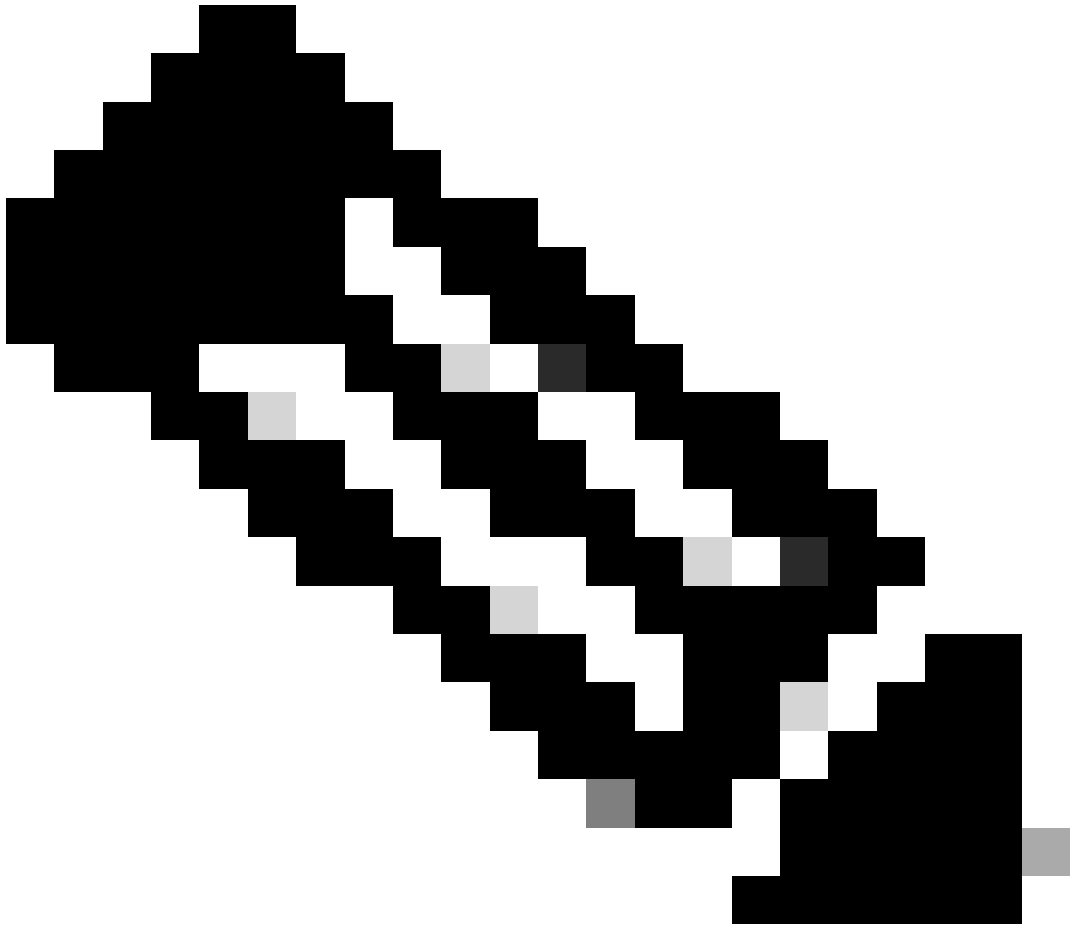
将root2023.txt和issuing2023.txt复制到XSP/ADP上的临时目录(例如/var/broadworks/tmp/)。这可以使用WinSCP或任何其他类似应用程序来实现。

```
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
```

## 更新信任锚点

上传证书文件以建立新的信任锚点。从CTI XSP/ADP BWCLI中，发出以下命令：

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



注意：每个别名必须唯一。例如，webexclientroot2023和webexclissuing2023用作信任锚点的示例别名。您可以随意创建自定义别名，确保每个别名都不同。

## 确认更新

通过发出以下命令确认锚点已更新

```
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]
```

您的CTI接口现已使用最新证书更新。

## 检查TLS握手

请注意，需要以FieldDebug严重性启用Tomcat TLS日志才能查看SSL握手。

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

TLS调试仅在ADP 2022.10及更高版本中。请参阅[Cisco BroadWorks日志加密连接设置和终止](#)。

## 相关信息

- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。