Webex for BroadworksでのCTIインターフェイスの信頼の更新

内容

はじめに

このドキュメントでは、Webex for BroadworksのCTIインターフェイスのトラストアンカーを更新するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Control Hubの設定に関する知識
- Broadworksのコマンドラインインターフェイス(CLI)の設定およびナビゲーション方法を理解していること。
- SSL/TLSプロトコルと証明書認証に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、Broadworks R22以降に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、Broadworks XSP/ADPホストがインターネットに接続していることを前提としています。

設定

この手順には、特定の証明書ファイルのダウンロード、ファイルの分割、XSP上の特定の場所へのコピー、およびこれらの証明書の新しいトラストアンカーとしてのアップロードが含まれます。これは、XSPとWebexの間で安全で信頼できる通信を確保するのに役立つ重要なタスクです。

このドキュメントでは、CTIインターフェイスに初めてトラストアンカーをインストールする手順を示します。これは、更新が必要な場合と同じプロセスです。このガイドでは、必要な証明書ファイルを取得し、それらを個々の証明書に分割し、XSP|ADPの新しいトラストアンカーにアップロードする手順の概要について説明します。

トラストアンカーの設定と更新

初期設定とその後のアップデートは同じプロセスです。信頼を初めて追加する場合は、手順を実行して信頼が追加されたことを確認します。

更新時に、新しい信頼を追加し、新しい信頼のインストール後に古い信頼を削除するか、両方の信頼を残すことができます。古い信頼と新しい信頼は、両方の信頼のいずれかに一致する関連証明書を提示するW4Bサービスサポートとして並行して機能できます。

まとめ

- 新しいシスコの信頼証明書は、古い信頼の有効期限が切れる前であればいつでも追加できます。
- 古い信頼は、新しい信頼が追加されたときに同時に削除することも、運用チームがその方法を希望する場合は、後の任意の日付に削除することもできます。

プロセスの概要

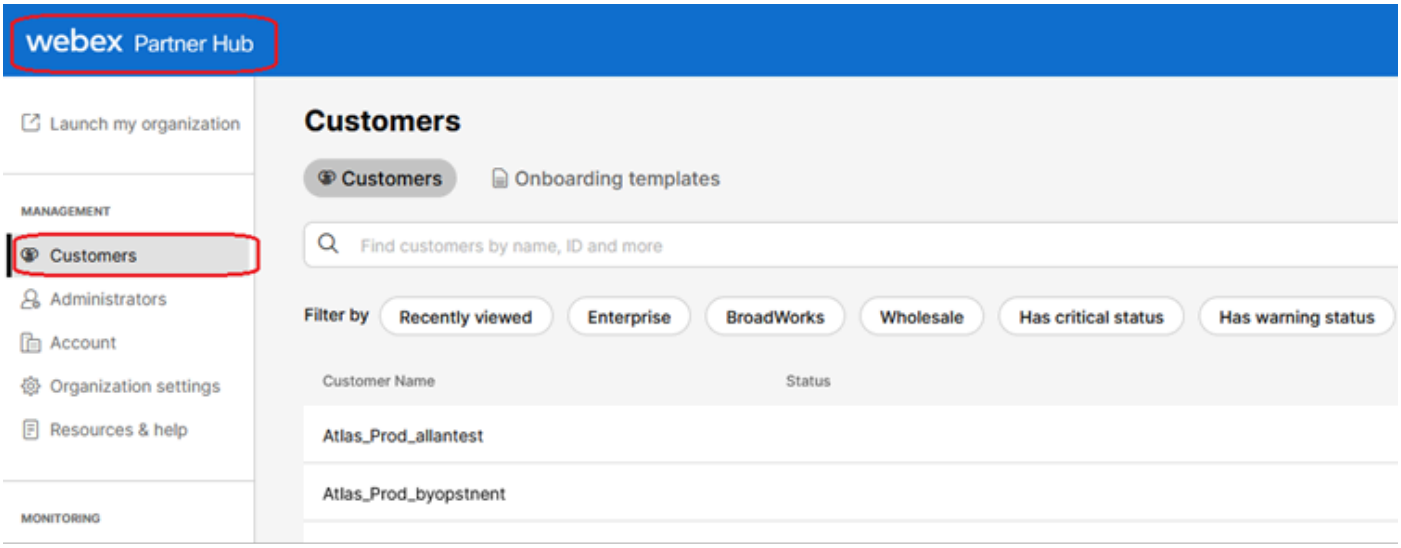
このプロセスの概要を次に示します。このプロセスは、初期インストールとトラストアンカーの更新の両方に適用されます。

- Webex CA証明書のダウンロード：パートナーハブのSettings > BroadWorks Callingから CombinedCertChain2023.txtファイルを取得します。
- 証明書チェーンの分割：結合された証明書チェーンファイルを、テキスト工ディタを使用して、root2023.txtとissuing2023.txtの2つの別々の証明書ファイルに分割します。

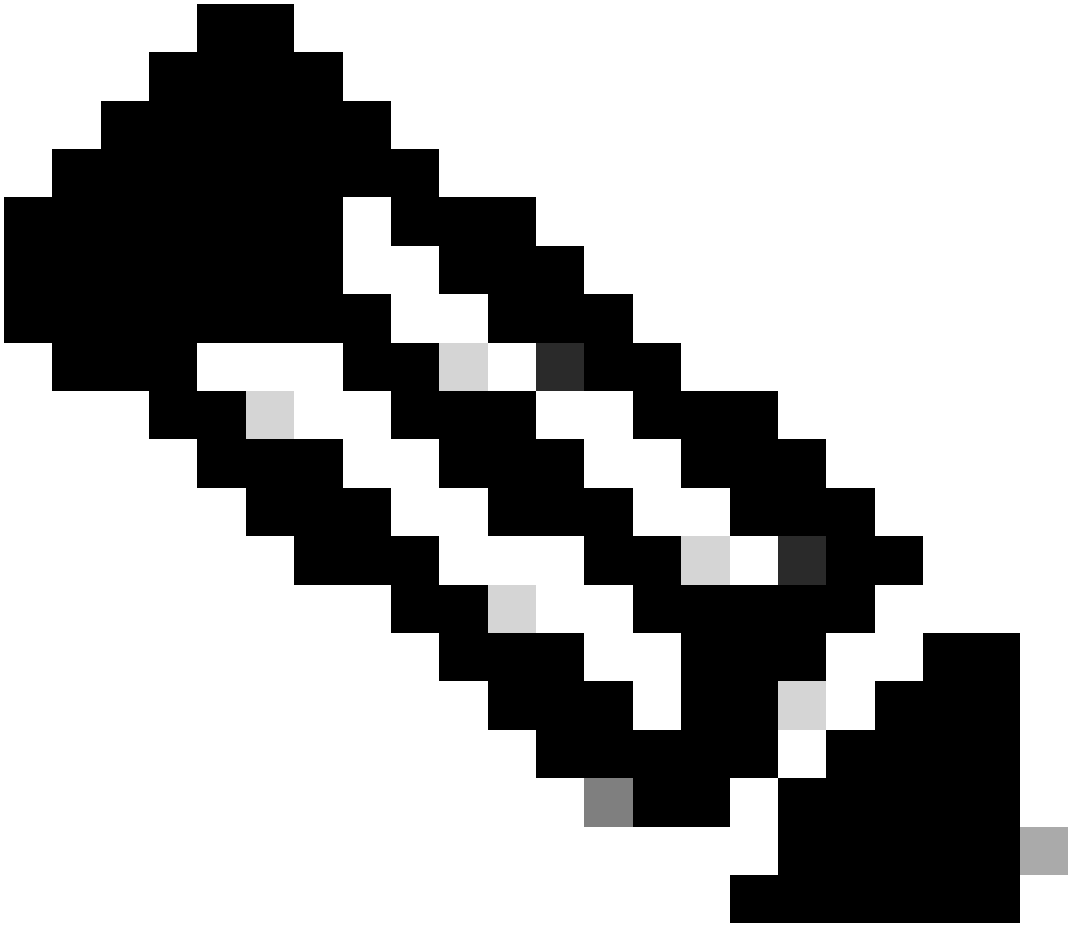
- ファイルのコピー：両方の証明書ファイルをXSP|ADPの一時的な場所に転送します。
- トラストアンカーの更新:XSP|ADPコマンドラインインターフェイス(CLI)内でupdateTrustコマンドを使用して、証明書ファイルを新しいトラストアンカーにアップロードします。
- 更新の確認：トラストアンカーが正常に更新されていることを確認します。

Webex CA証明書のダウンロード

1. Partner Hubにサインインします。

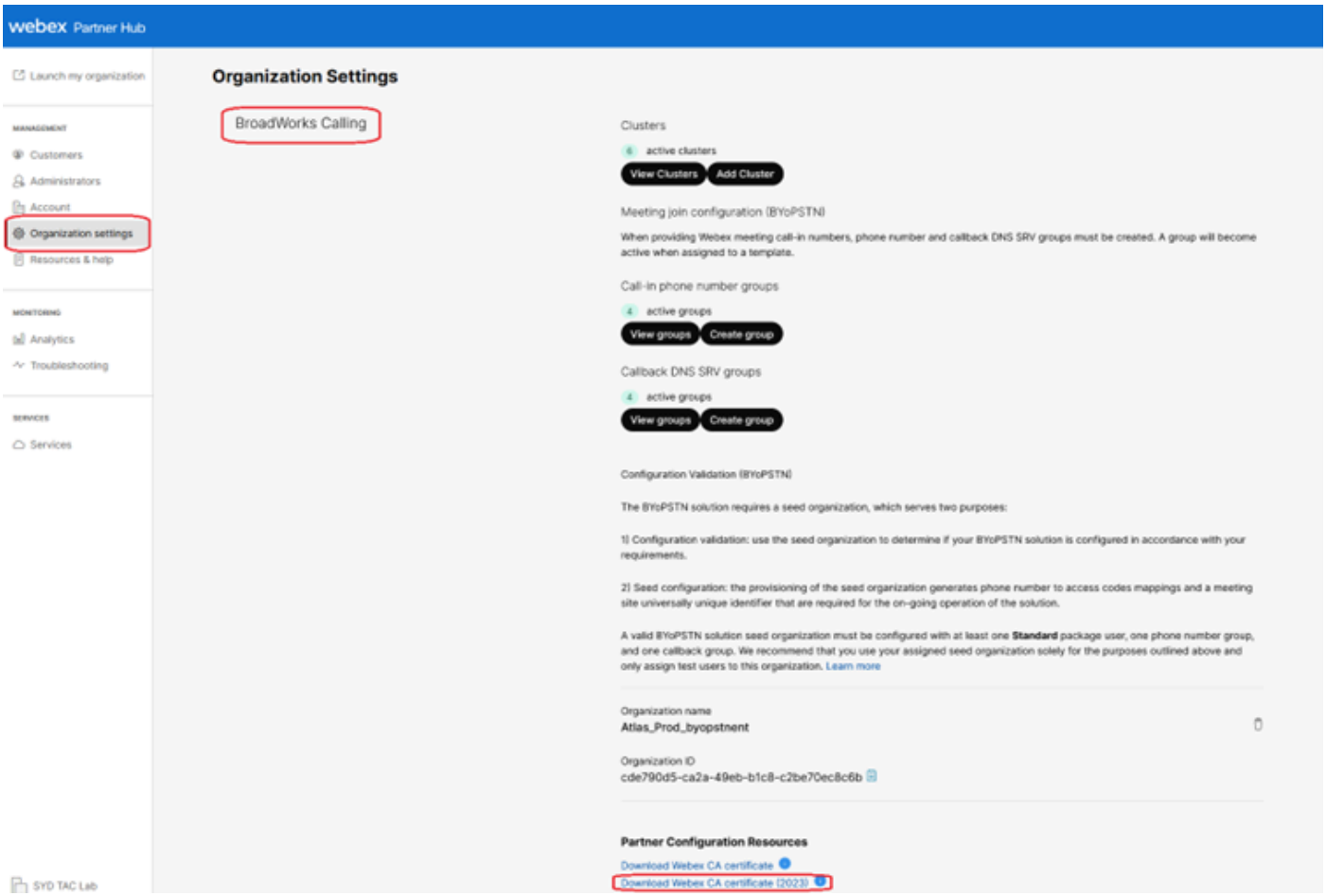


Webexパートナーハブ

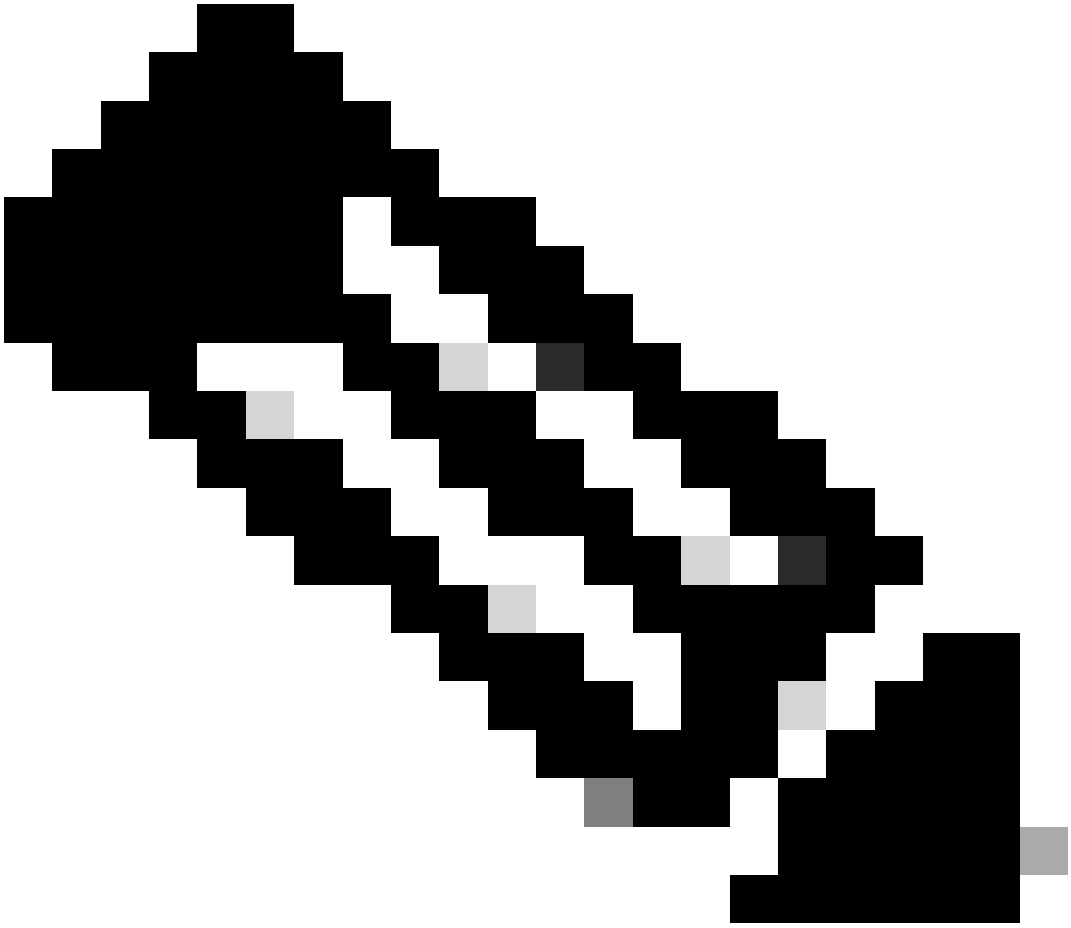


注:Partner HubはControl Hubとは異なります。Partner Hubの左側のペインには Customersが表示され、タイトルペインにはPartner Hubが表示されます。

2. Organization Settings > BroadWorks Callingの順に移動し、Download Webex CAをクリックします。



証明書ダウンロードリンクが表示された組織設定ページ



注：最新のオプションを選択します。このスクリーンショットでは、最新の「Download Webex CA certificate (2023)

3. ここに示す証明書。セキュリティ上の理由から、イメージは難読化されています。

1

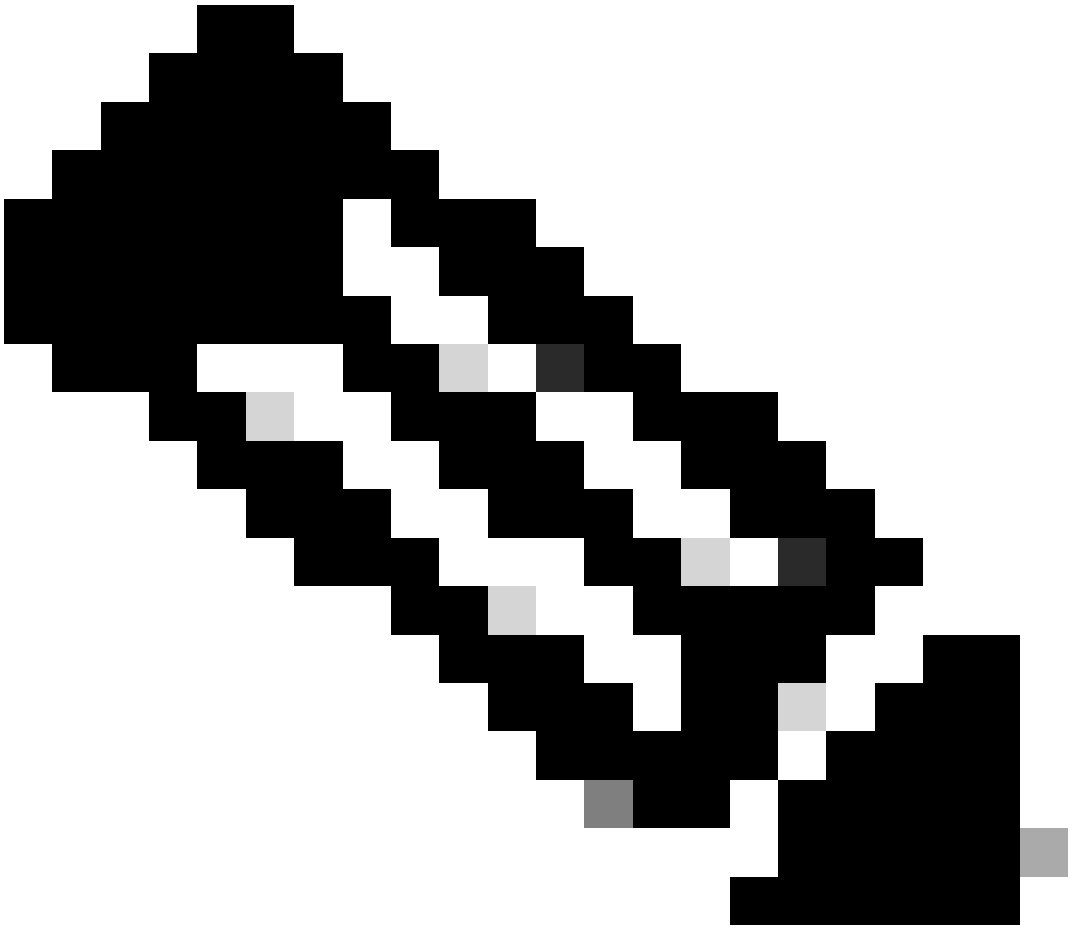
2

```
-rwxrwxrwx 1 bwadmin bwadmin 2324 Jul 21 2023 issuing2023.txt
-rwxrwxrwx 1 bwadmin bwadmin 1894 Jul 21 2023 root2023.txt
```

トラストアンカーの更新

証明書ファイルをアップロードして、新しいトラストアンカーを確立します。CTI XSP/ADP BWCLI内から、次のコマンドを発行します。

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



注：各エイリアスは一意である必要があります。たとえば、webexclientroot2023とwebexclientssuing2023は、トラストアンカーのサンプルエイリアスとして機能します。独自のエイリアスを作成して、それぞれを個別に指定できます。

更新の確認

次のコマンドを発行して、アンカーが更新されていることを確認します

```
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]
```

CTIインターフェイスが最新の証明書で更新されました。

TLSハンドシェイクのチェック

SSLハンドシェイクを表示するには、FieldDebugの重大度でTomcat TLSログを有効にする必要があることに注意してください。

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

TLSのデバッグはADP 2022.10以降でのみ行われます。「Cisco BroadWorksログ暗号化接続のセットアップとティアダウン」を参照してください。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。