

Atualizar Confiança para Interface CTI no Webex para Broadworks

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurando e Renovando Âncoras de Confiança](#)

[Visão Geral do Processo](#)

[Fazer download do certificado CA do Webex](#)

[Dividir Cadeia de Certificados](#)

[Para o primeiro certificado \(certificado raiz\):](#)

[Para o segundo certificado \(que emite o certificado\):](#)

[Copiar Arquivos](#)

[Atualizar Âncoras de Confiança](#)

[Confirmar atualização](#)

[Verificar handshake TLS](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo para atualizar âncoras de confiança para a Interface CTI no Webex para Broadworks.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Familiaridade com a definição de configurações no Hub de Controle
- Entendendo como configurar e navegar na Interface de linha de comando (CLI) do Broadworks.
- Conhecimento básico dos protocolos SSL/TLS e da autenticação de certificados

Componentes Utilizados

As informações neste documento são baseadas no Broadworks R22 e superior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento pressupõe que os hosts Broadworks XSP/ADP estejam voltados para a Internet.

Configurar

Esse procedimento envolve fazer download de arquivos de certificado específicos, dividi-los, copiá-los para determinados locais no XSP e depois carregar esses certificados como novas âncoras de confiança. É uma tarefa importante que ajuda a garantir uma comunicação segura e confiável entre o XSP e o Webex.

Este documento mostra as etapas para instalar âncoras de confiança para a interface CTI pela primeira vez. Este é o mesmo processo quando você precisa atualizá-los. Este guia descreve as etapas para adquirir os arquivos de certificado necessários, dividi-los em certificados individuais e depois carregá-los em novas âncoras de confiança no XSP|ADP.

Configurando e Renovando Âncoras de Confiança

A configuração inicial e as atualizações subsequentes são o mesmo processo. Ao adicionar relações de confiança pela primeira vez, conclua as etapas e confirme se as relações de confiança foram adicionadas.

Ao atualizar, você pode adicionar as novas relações de confiança e excluir as antigas após a instalação das novas ou deixar ambas. Os trusts antigos e novos podem funcionar em paralelo, pois os serviços W4B suportam a apresentação do certificado relevante para corresponder a qualquer um dos trusts.

Para resumir:

- O novo certificado de confiança Cisco pode ser adicionado a qualquer momento antes da expiração da confiança antiga.
- A confiança mais antiga pode ser removida ao mesmo tempo em que a nova é adicionada ou em qualquer data posterior se a equipe de operação preferir essa abordagem.

Visão Geral do Processo

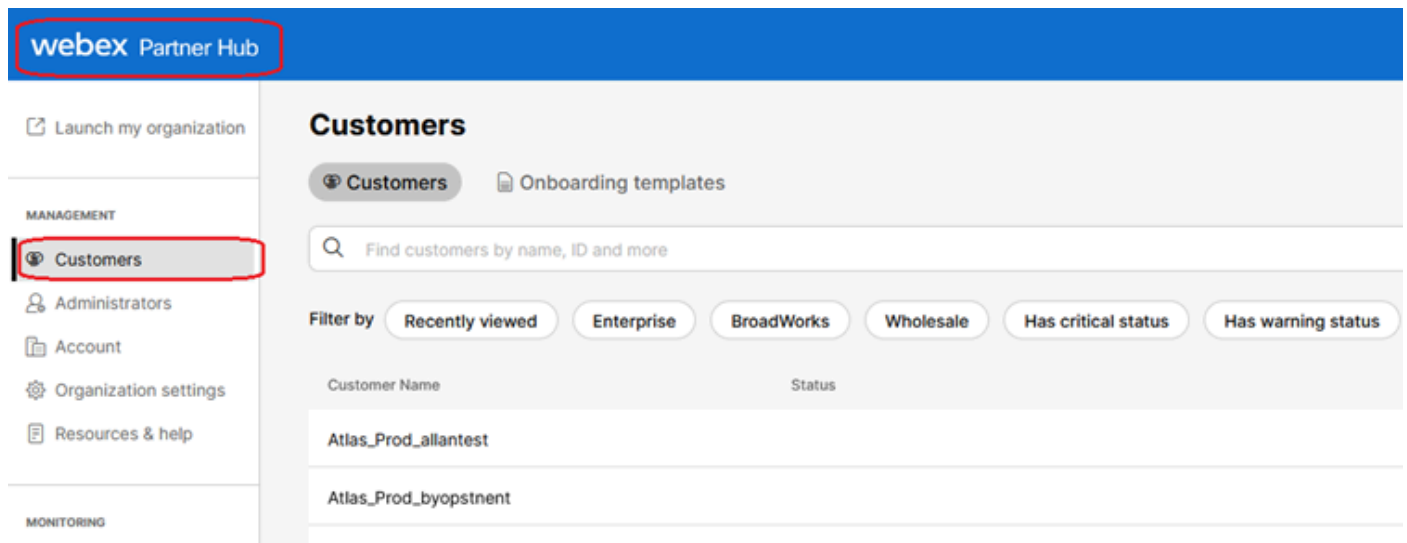
Esta é uma visão geral do processo, que se aplica à instalação inicial e às atualizações das Âncoras de Confiança:

- Baixe o certificado CA do Webex: obtenha o arquivo CombinedCertChain2023.txt do Partner Hub em Settings > BroadWorks Calling.

- Dividir Cadeia de Certificados: divida o arquivo da cadeia de certificados combinados em dois arquivos de certificados separados, root2023.txt e issuing2023.txt, usando um editor de texto.
- Copiar arquivos: transfere os dois arquivos de certificado para um local temporário no XSP|ADP.
- Atualizar Âncoras de Confiança: Use o comando updateTrust na interface de linha de comando XSP|ADP para carregar os arquivos de certificado para novas âncoras de confiança.
- Confirmar atualização: verifique se as âncoras de confiança foram atualizadas com êxito.

Fazer download do certificado CA do Webex

1. Entre no Partner Hub.



The screenshot displays the Webex Partner Hub interface. At the top, there is a blue header with the "webex Partner Hub" logo. Below the header, a left sidebar contains navigation options under "MANAGEMENT" and "MONITORING". The "Customers" option is highlighted with a red box. The main content area is titled "Customers" and includes a search bar, filter buttons, and a table of customer records.

Customer Name	Status
Atlas_Prod_allantest	
Atlas_Prod_byopstnent	

Webex Partner Hub



Observação: o Partner Hub é diferente do Control Hub. No Partner Hub, você verá Clientes no painel esquerdo e Partner Hub no painel de título.

2. Vá para Organization Settings > BroadWorks Calling e clique em Download Webex CA.

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 \(2023\)](#)

Página de Configuração da Organização Mostrando o Link de Download do Certificado



Observação: escolha a opção mais recente. Nesta captura de tela, você pode ver que o certificado mais recente é Download Webex CA (2023)

3. O certificado mostrado aqui. A imagem é ofuscada por motivos de segurança.

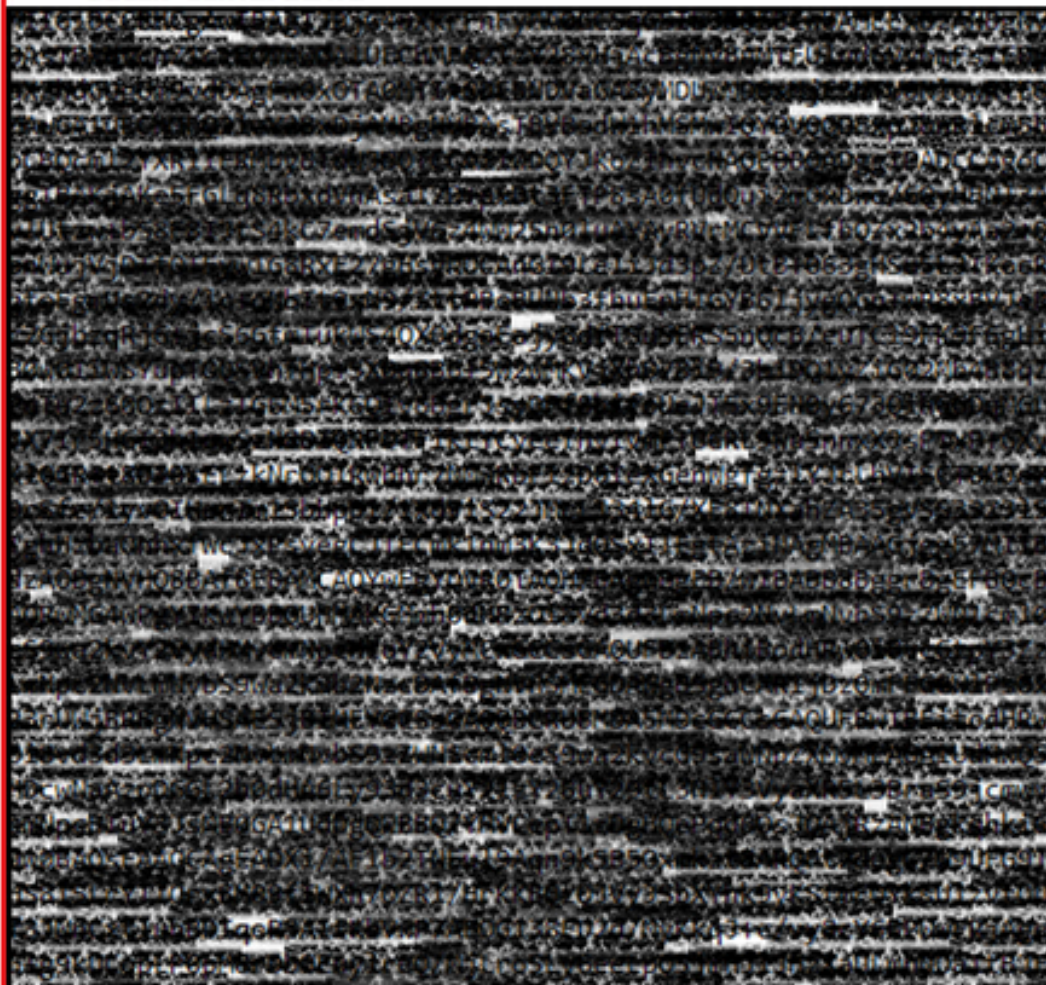
-----BEGIN CERTIFICATE-----



1

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

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



2

: é uma boa prática verificar se cada novo arquivo contém apenas um certificado e se os marcadores BEGIN e END estão incluídos corretamente.

Copiar Arquivos

Copie root2023.txt e issuing2023.txt para um diretório temporário no XSP/ADP como /var/broadworks/tmp/. Isso pode ser feito usando WinSCP ou qualquer outro aplicativo semelhante.

```
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
```

Atualizar Âncoras de Confiança

Carregue arquivos de certificado para estabelecer novas âncoras de confiança. No CTI XSP/ADP BWCLI, emita estes comandos:

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




Observação: cada alias deve ser exclusivo. Por exemplo, `webexclientroot2023` e `webexclientissuing2023` servem como alias de exemplo para as âncoras de confiança. Sinta-se à vontade para criar aliases personalizados, garantindo que cada um seja diferente.

Confirmar atualização

Confirme se as âncoras estão atualizadas emitindo este comando

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

```
=====
```

<code>webexclientissuing2023</code>	<code>Internal</code>	<code>Private</code>	<code>TLS SubCA</code>	<code>Internal</code>	<code>Private</code>	<code>Root</code>
<code>webexclientroot2023</code>	<code>Internal</code>	<code>Private</code>	<code>Root</code>	<code>Internal</code>	<code>Private</code>	<code>Root[self-signed]</code>

Sua interface CTI foi atualizada com o certificado mais recente.

Verificar handshake TLS

Observe que o registro TLS do Tomcat precisa ser habilitado na severidade FieldDebug para exibir o handshake SSL.

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

A depuração TLS está somente no ADP 2022.10 e posterior. Consulte [Configuração e Desmontagem de Conexões Criptográficas de Log do Cisco BroadWorks](#).

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.