Atualizar Confiança para Interface CTI no Webex para Broadworks

Contents

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

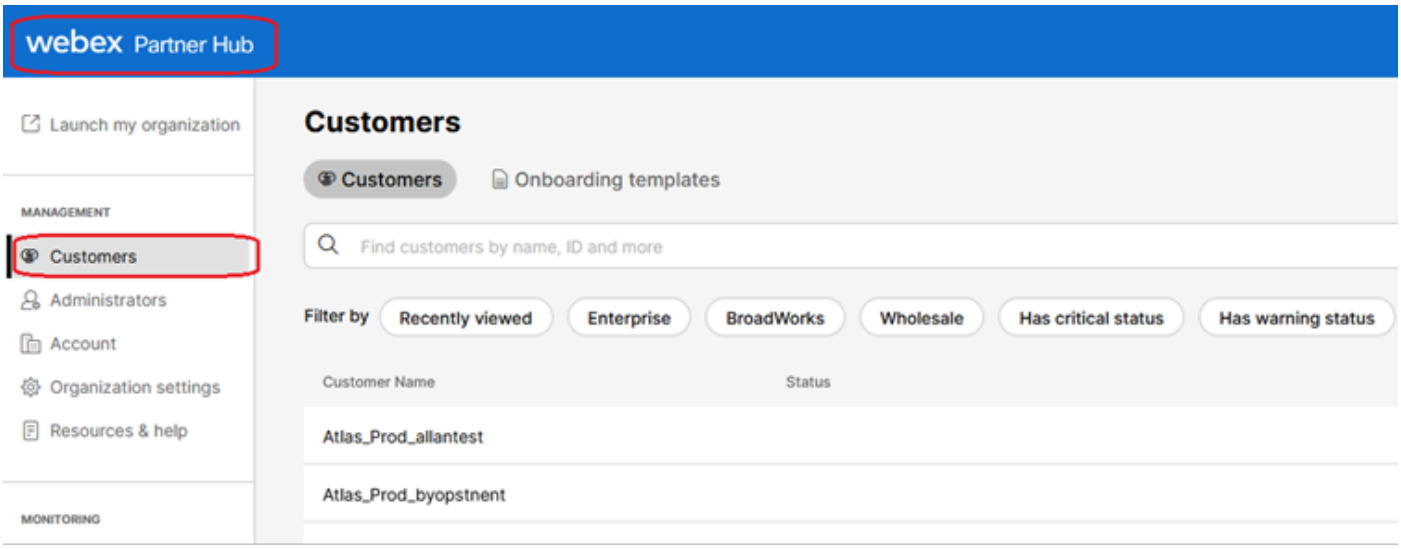
Esta é uma visão geral do processo, que se aplica à instalação inicial e às atualizações das Âncoras de Confiança:

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

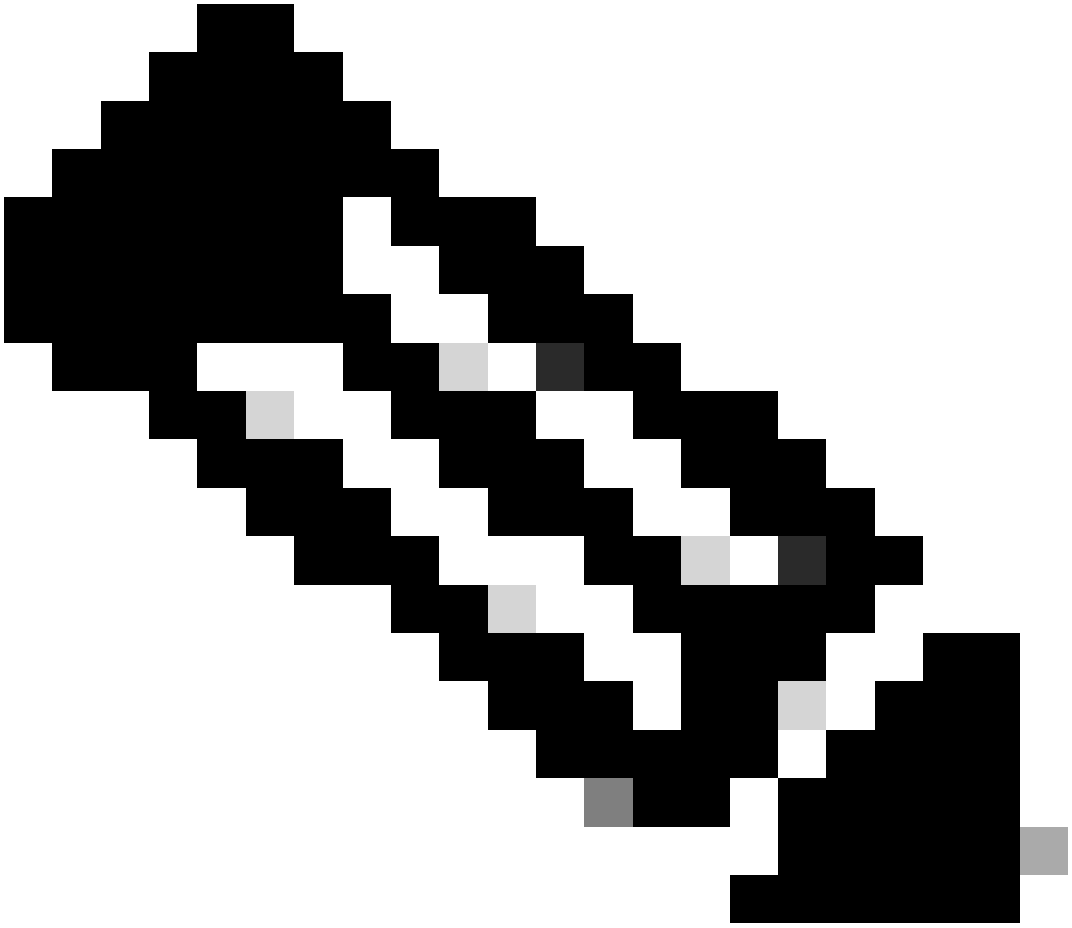
- Dividir Cadeia de Certificados: divida o arquivo da cadeia de certificados combinados em dois arquivos de certificados separados, root2023.txt e issuing2023.txt, usando um editor de texto.
- Copiar arquivos: transfere os dois arquivos de certificado para um local temporário no XSP|ADP.
- Atualizar 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.

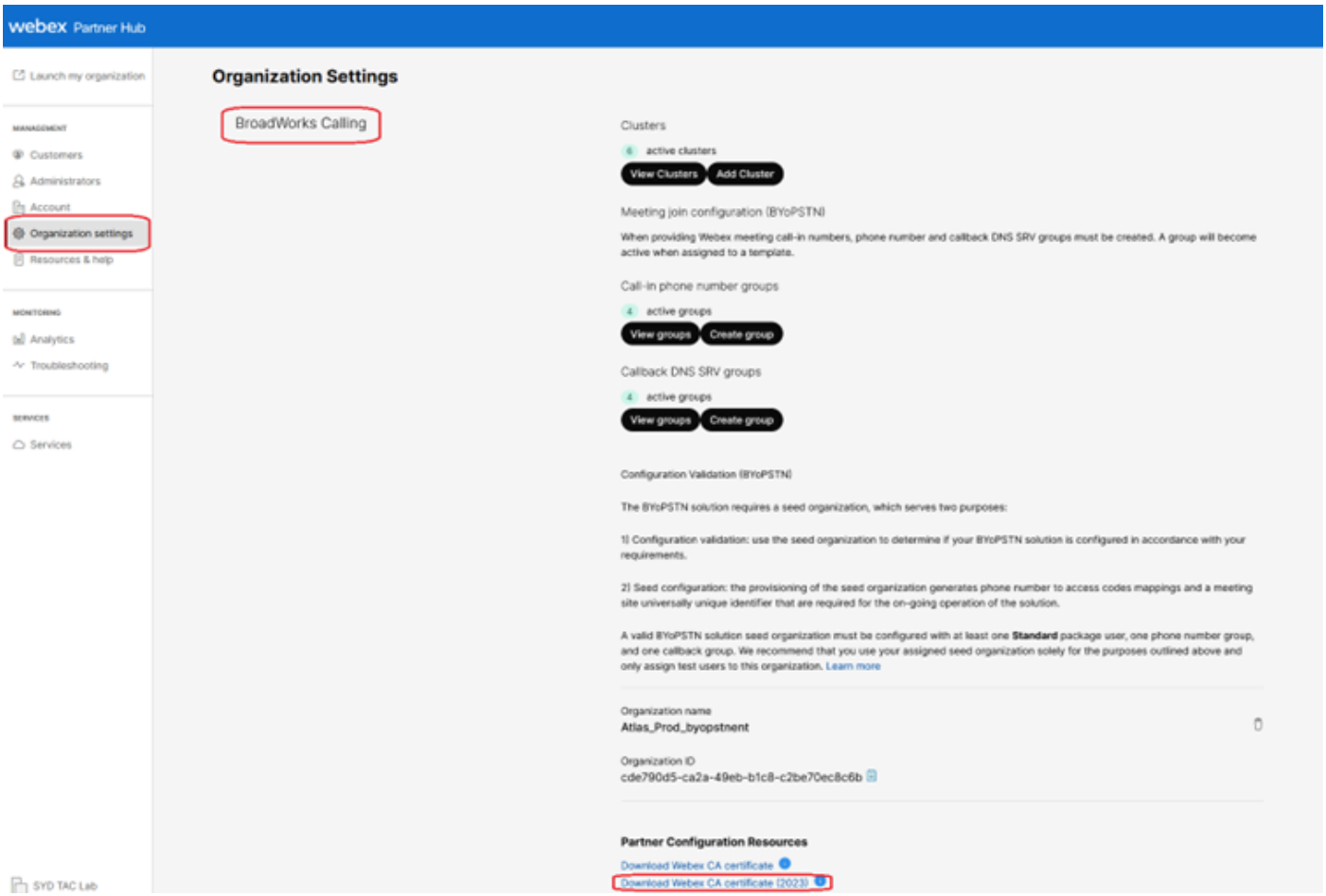


Webex Partner Hub

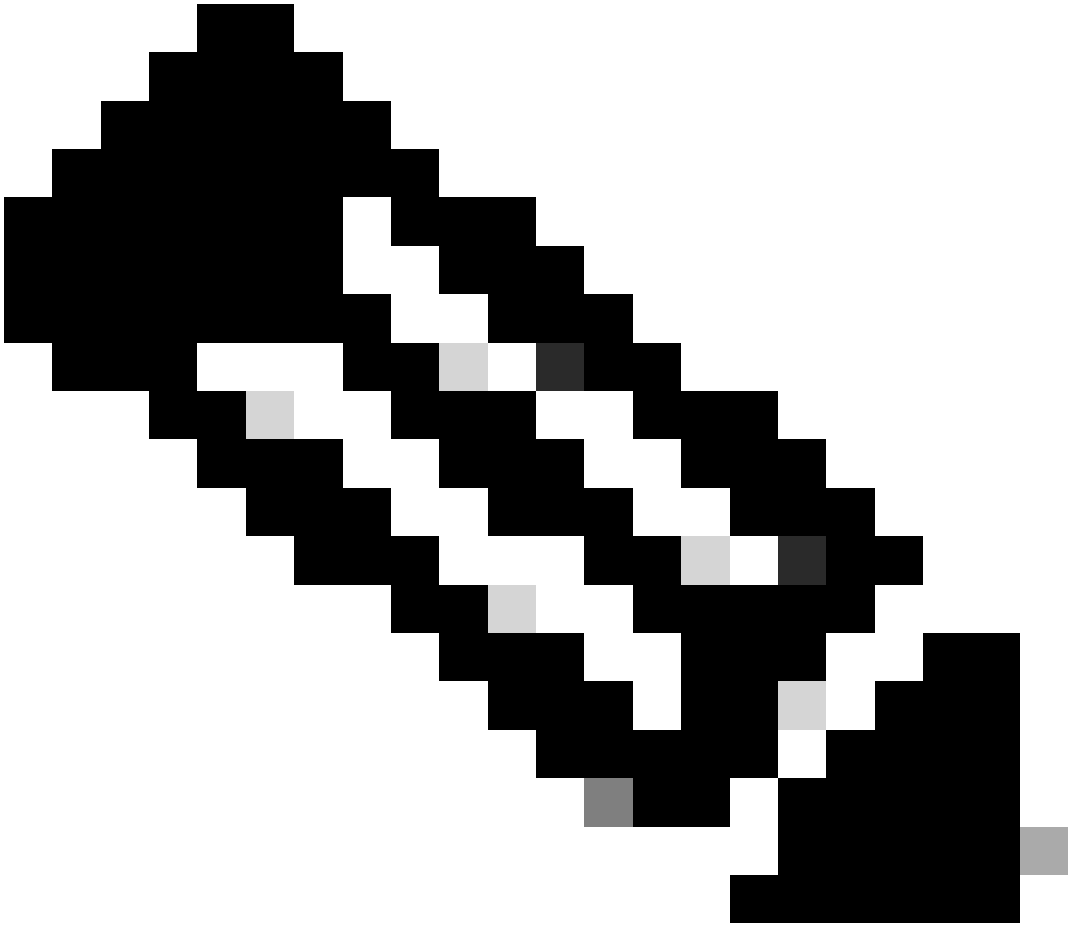


Observação: o Partner Hub é diferente do Control Hub. No Partner Hub, você verá Clientes no painel esquerdo e Partner Hub no painel de título.

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



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.

1

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

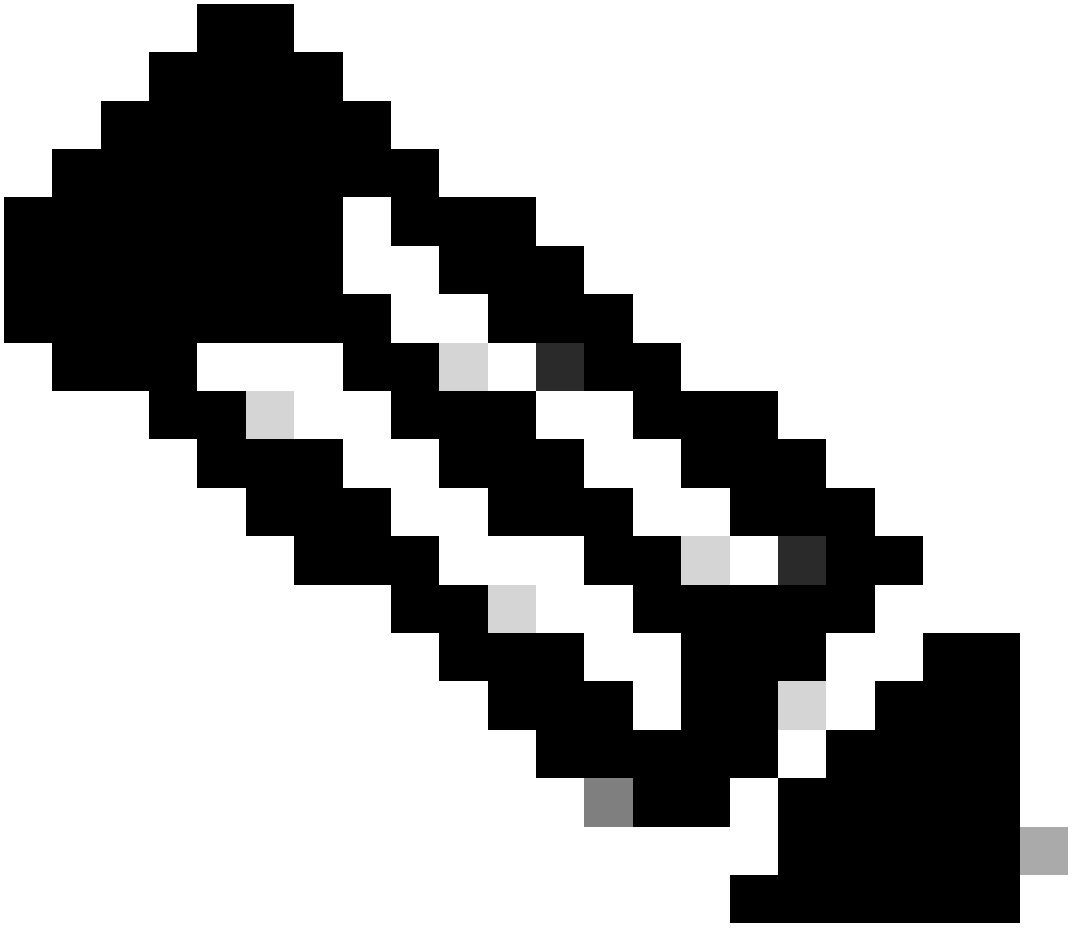
Copie root2023.txt e issuing2023.txt para um diretório temporário no XSP/ADP como /var/broadworks/tmp/. Isso pode ser feito usando WinSCP ou qualquer outro aplicativo semelhante.

```
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
================================================================================
webexclientissuing2023 Internal Private TLS SubCA Internal Private Root
webexclientroot2023 Internal Private Root Internal Private Root[self-signed]
```

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.