

Actualización de Confianzas para la Interfaz CTI en Webex para Broadworks

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración y renovación de anclajes de confianza](#)

[Descripción general del proceso](#)

[Descargar certificado de CA de Webex](#)

[Dividir cadena de certificados](#)

[Para el primer certificado \(certificado raíz\):](#)

[Para el segundo certificado \(certificado de emisión\):](#)

[Copiar archivos](#)

[Actualizar delimitadores de confianza](#)

[Confirmar actualización](#)

[Comprobar intercambio de señales TLS](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso para actualizar los anclajes de confianza para la interfaz CTI en Webex para Broadworks.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Familiaridad con la configuración de los parámetros del concentrador de control
- Introducción a la configuración y navegación por la interfaz de línea de comandos (CLI) de Broadworks.
- Comprensión básica de los protocolos SSL/TLS y autenticación de certificados

Componentes Utilizados

La información de este documento se basa en Broadworks R22 y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento asume que los hosts Broadworks XSP/ADP están orientados a Internet.

Configurar

Este procedimiento implica descargar archivos de certificados específicos, dividirlos, copiarlos en determinadas ubicaciones del XSP y, a continuación, cargar estos certificados como nuevos anclajes de confianza. Es una tarea importante que ayuda a garantizar una comunicación segura y de confianza entre su XSP y Webex.

Este documento muestra los pasos para instalar Trust Anchors para la interfaz CTI por primera vez. Este es el mismo proceso cuando necesita actualizarlos. Esta guía describe los pasos para adquirir los archivos de certificado necesarios, dividirlos en certificados individuales y luego cargarlos en nuevos anclajes de confianza en el XSP|ADP.

Configuración y renovación de anclajes de confianza

La configuración inicial y cualquier actualización posterior son el mismo proceso. Cuando agregue confianzas por primera vez, complete los pasos y confirme que se agregan.

Al actualizar, puede agregar las nuevas confianzas y eliminar las antiguas después de instalar las nuevas o dejar ambas confianzas. Los fideicomisos antiguos y nuevos pueden funcionar en paralelo, ya que los servicios W4B admiten la presentación del certificado correspondiente para que coincida con cualquiera de los dos fideicomisos.

Para resumir:

- El nuevo certificado de confianza de Cisco se puede agregar en cualquier momento antes de que caduque la confianza anterior.
- La confianza anterior se puede quitar al mismo tiempo que se agrega la nueva o en cualquier fecha posterior si el equipo de operaciones prefiere ese enfoque.

Descripción general del proceso

A continuación se muestra una descripción general del proceso, que se aplica tanto a la instalación inicial como a las actualizaciones de Trust Anchors:

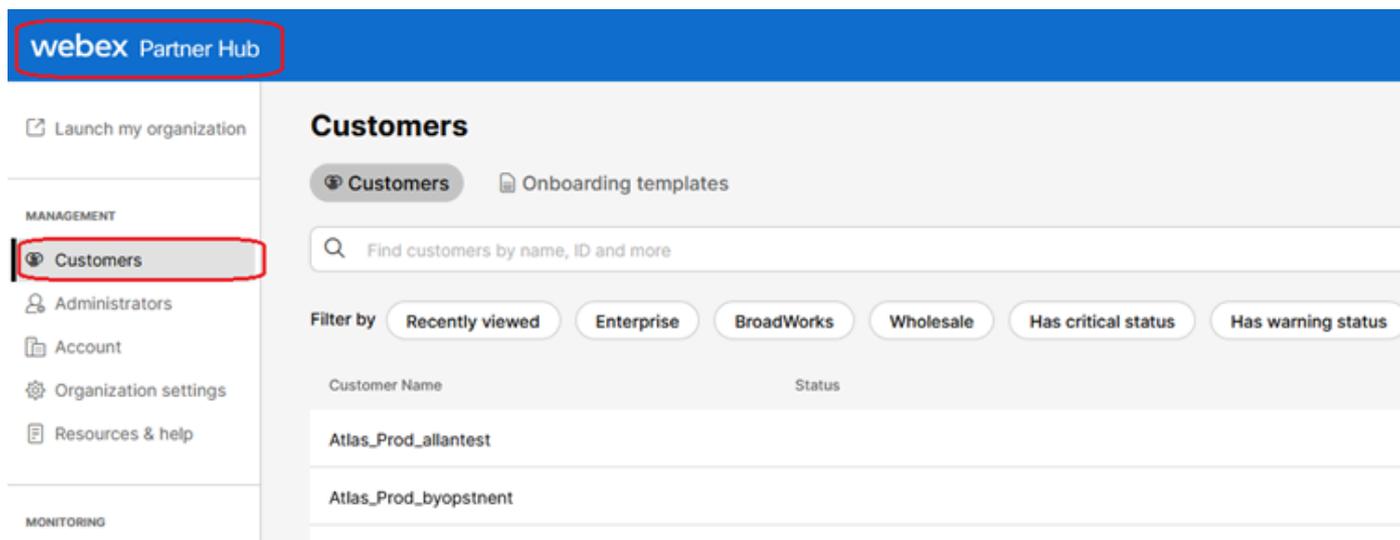
- Descargue el certificado de CA de Webex: Obtenga el archivo CombinedCertChain2023.txt del Partner Hub en Configuración > Llamadas de BroadWorks.
- Dividir cadena de certificados: divida el archivo de cadena de certificados combinado en dos

archivos de certificados independientes, root2023.txt y issue2023.txt, mediante un editor de texto.

- Copiar archivos: transfiera ambos archivos de certificado a una ubicación temporal en el XSP|ADP.
- Actualizar delimitadores de confianza: utilice el comando updateTrust en la interfaz de línea de comandos XSP|ADP para cargar los archivos de certificado en los nuevos delimitadores de confianza.
- Confirmar actualización: compruebe que los delimitadores de confianza se han actualizado correctamente.

Descargar certificado de CA de Webex

1. Inicie sesión en Partner Hub.



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 with a 'MANAGEMENT' section containing 'Customers', 'Administrators', 'Account', 'Organization settings', and 'Resources & help'. The 'Customers' item is highlighted with a red box. The main content area is titled 'Customers' and includes a search bar, filter buttons (Recently viewed, Enterprise, BroadWorks, Wholesale, Has critical status, Has warning status), and a table with columns 'Customer Name' and 'Status'. The table lists two customers: 'Atlas_Prod_allantest' and 'Atlas_Prod_byopstnent'.

Hub de partners de Webex



Nota: Partner Hub es diferente de Control Hub. En Partner Hub, verá Clientes en el panel izquierdo y Partner Hub en el panel de título.

2. Vaya a Configuración de la organización > Llamadas de BroadWorks y haga clic en Descargar CA de Webex.

Launch my organization

MANAGEMENT

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

MONITORING

- Analytics
- Troubleshooting

SERVICES

- Services

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 configuración de la organización que muestra el enlace de descarga de certificados



Nota: Seleccione la última opción. En esta captura de pantalla, puede ver que la última es Descargar certificado de CA Webex (2023)

3. El certificado que se muestra aquí. La imagen está ofuscada por razones de seguridad.

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



1

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

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



2

: Es una buena práctica verificar que cada nuevo archivo contenga solo un certificado y que los marcadores BEGIN y END estén correctamente incluidos.

Copiar archivos

Copie root2023.txt y issue2023.txt en un directorio temporal en el XSP/ADP como /var/broadworks/tmp/. Esto se puede hacer usando WinSCP o cualquier otra aplicación similar.

```
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
```

Actualizar delimitadores de confianza

Cargue archivos de certificado para establecer nuevos anclajes de confianza. Desde CTI XSP/ADP BWCLI, ejecute estos comandos:

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



Nota: Cada alias debe ser único. Por ejemplo, `webexclientroot2023` y `webexclientissuing2023` sirven como alias de ejemplo para los delimitadores de confianza. No dude en crear alias personalizados, asegurándose de que cada uno sea distinto.

Confirmar actualización

Confirme que los anclajes se actualizan ejecutando 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]
```

Su interfaz CTI se ha actualizado con el certificado más reciente.

Comprobar intercambio de señales TLS

Tenga en cuenta que el registro TLS de Tomcat debe estar habilitado en gravedad de FieldDebug para ver el intercambio de señales SSL.

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

La depuración de TLS solo se realiza en ADP 2022.10 y versiones posteriores. Consulte [Configuración y desconexión de la conexión criptográfica de Cisco BroadWorks Log](#).

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).