Important Items for Hybrid Services Deployments

Important Items For Hybrid Services Deployments

This section provides added context about key configuration items that relate to Cisco Webex Hybrid Services.

These points are crucial if you want to successfully deploy Expressway-hosted Cisco Webex Hybrid Services, such as Hybrid Call Service and Hybrid Calendar Service. We've highlighted these items in particular for the following reasons:

- We want to explain them, so that you understand their role in a hybrid deployment and feel reassured.
- They are mandatory prerequisites that ensure a secure deployment between our cloud and your on-premises environment.
- They should be treated as pre-day zero activities: they can take a bit longer to complete than typical configuration in a user interface, so allow a timeframe to get these items sorted.
- After these items are addressed in your environment, the rest of your Cisco Webex Hybrid Services configuration will go smoothly.

Supported Certificate Authorities

The Expressway-C connector host must be registered to Cisco Webex in order for hybrid servicesCisco Webex Calling for Branch Offices to work.

Expressway-C is deployed in the internal network, and the way it registers to the cloud is through an outbound HTTPS connection—the same type that is used for any browser that connects to a web server.

Registration and communication to the Cisco Webex cloud uses TLS. Expressway-C is the TLS client, and the Cisco Webex cloud is the TLS server. As such, Expressway-C checks the server certificate.

The certificate authority signs a server certificate using its own private key. Anyone with the public key can decode that signature and prove that the same certificate authority signed that certificate.

If Expressway-C has to validate the certificate provided by the cloud, it must use the public key of the certificate authority that signed that certificate to decode the signature. A public key is contained in the certificate of the certificate authority. To establish trust with the certificate authorities used by the cloud, the list of certificates of these trusted certificate authorities must be in the Expressway's trust store. Doing so, the Expressway can verify that the call is truly coming from the Cisco Webex cloud.

With manual upload, you can upload all relevant certificate authority certificates to the trust store of Expressway-C.

With automatic upload, the cloud itself uploads those certificates in the trust store of Expressway-C. We recommend that you use automatic upload. The certificate list might change, and automatic upload guarantees that you get the most updated list.

If you allow automatic installation of certificate authority certificates, you are redirected to https://admin.webex.com (the management portal). The redirection is done by the Expressway-C itself without any user intervention. You, as the Cisco Webex administrator, must authenticate through an HTTPS connection. Soon after, the cloud pushes the CA certificates to the Expressway-C.

Until the certificates are uploaded to the Expressway-C trust store, the HTTPS connection cannot be established.

To avoid this problem, the Expressway-C is preinstalled with Cisco Webex-trusted CA certificates. Those certificates are only used to set up and validate the initial HTTPS connection, and they don't appear in Expressway-C trust list. Once the certificates of the trusted certificate authorities are pulled from the cloud through this initial HTTPS connection, those certificates are available for platform-wide usage; then, they appear in the Expressway-C trust list.

This process is secure for these reasons:

- Requires admin access to Expressway-C and to https://admin.webex.com. Those connections use HTTPS and are encrypted.
- Certificates are pushed from the cloud to Expressway using the same encrypted connection.

This list shows the certificate authority certificates that the Cisco Webex cloud currently uses. This list might change in the future:

- C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
- C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certificate Authority
- C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2
- C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certificate Authority

A list of certificate authority certificates is also required for the Expressway-E in the traversal pair. Expressway-E communicates with the Cisco Webex cloud using SIP with TLS, enforced by mutual authentication. Expressway-E trusts calls coming from and going to the cloud, only if the CN or SAN of the certificate presented by the cloud during TLS connection setup matches the subject name configured for the DNS zone on Expressway ("callservice.webex.com"). The certificate authority releases a certificate only after an identity check. The ownership of the callservice.webex.com domain must be proved to get a certificate

signed. Because we (Cisco) own that domain, the DNS name "callservice.webex.com" is direct proof that the remote peer is truly Cisco Webex.

Related Topics

Supported Certificate Authorities for Cisco Webex

Exchange Impersonation Account

Calendar Connector integrates Cisco Webex with Microsoft Exchange 2010, 2013, 2016, or Office 365 through an impersonation account. The application impersonation management role in Exchange enables applications to impersonate users in an organization to perform tasks on behalf of the user. The application impersonation role must be configured in Exchange and is used in the Calendar Connector as part of the Exchange configuration on the Expressway-C interface.

The Exchange impersonation account is Microsoft's recommended method for this task. Expressway-C administrators don't need to know the password, because the value can be entered in the Expressway-C interface by an Exchange administrator. The password isn't clearly shown, even if the Expressway-C administrator has root access to the Expressway-C box. The password is stored encrypted using the same credential encryption mechanism as other passwords on the Expressway-C.

For additional security, follow the steps in Deploy Expressway Calendar Connector for Microsoft Exchange to enable TLS in order to secure EWS connections on the wire.