Cisco Webex Security and Privacy

The Cisco Webex Security Difference

Security is built into Cisco Webex DNA. Cisco has invested heavily to build a culture of security with the right checks and balances in place. Which is why Webex is built with security from the ground up. Webex chooses the most secure default settings out of the box thereby enabling users to starting collaborating freely without having to worry about configurations. At the same time, Webex has also built a great user experience – one that doesn't compromise security.

Cisco Webex offers you true **end-to-end encryption, compliance, visibility and control.** Webex is backed by Cisco's rich history and expertise in security — from the network, to endpoints, to the data center and our cloud services. All of Cisco's products and services are built using Cisco's Secure Development Lifecycle (CSDL) which ensures that our products are built to a security baseline. The security of our products is independently verified by Cisco's Security and Trust organization, a team with 100's of security advocates across multiple functions. Inside your own organization, or even when collaborating across company lines, Cisco Webex provides an enterprise-grade hardened collaboration platform that keeps you secure by default and protects your user data. That's **collaboration without compromise**.

Privacy, Security & Transparency - Our three security principles:

Webex is committed to respecting the PRIVACY of your data:

- Cisco does not rent or sell user data to third parties.
- Cisco implements all features with security and user data privacy in mind.
- Cisco Webex has a clear privacy policy which can be viewed here.

Webex is SECURE by default

- Webex security is built-in as a key foundational element and is secure by default – we never make it the user's responsibility to opt-out of sharing their data, or change meeting settings in order to be protected.
- Cisco ensures that dedicated room meeting IDs are not called out externally, to prevent unwanted intruders and potential toll fraud.
- All communications between Cisco Webex Applications, Webex Room devices and the Cisco Webex Cloud occur over encrypted channels. Cisco Webex uses TLS 1.2 protocol and negotiates only high strength encryption ciphers (for example, AES 256).
- Once a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.
- For businesses requiring an even higher level of security, Cisco Webex also provides true end-to-end encryption for meetings. With this option, the Cisco Webex Cloud cannot decrypt the media

streams sent by your Webex Meetings application. See What Does End-to-End Encryption Do for more detail.
- Cisco processes and stores recordings, transcriptions and closed captioning data in-house and never compromises individual customer data by outsourcing it to a third party.

Webex is TRANSPARENT about security

- Cisco's security data sheets, privacy maps and regulatory compliance certificates are available from our Trust Portal.
- Cisco has an independent Security and Trust Organization (STO) with governance over Webex products and services.
- Cisco builds all products using the Cisco Secure Development Lifecycle (CSDL) and performs regular proactive penetration testing of the Webex cloud platform and products
- Cisco's Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

Summary

Security is in Cisco's DNA; and we continue to invest heavily in security. Our Webex service was built from the ground up to provide you with a secure conferencing platform that we constantly monitor and improve.