

Introduction

Enabling real-time collaboration to connect global employees and virtual teams is a growing trend among organizations seeking a competitive advantage. Worldwide, a large number of businesses and government agencies rely on Cisco WebEx™ software-as-a-service (SaaS) solutions to streamline business processes for sales, marketing, training, project management, and support. Cisco® makes security the top priority in the design, deployment, and maintenance of its network, platform, and applications. You can incorporate WebEx® solutions into your ongoing business processes—instantly, and with confidence—even in environments with the most rigorous security requirements.

Understanding the security features of Cisco WebEx online applications and the underlying communication infrastructure—the Cisco Collaboration Cloud—is an important component of your purchase decision.

Discover detailed security information for:

- The Cisco Collaboration Cloud infrastructure
- The secure WebEx meeting experience
 - Meeting-site configuration
 - Scheduling security options
 - Starting and joining a WebEx meeting
 - Encryption technologies
 - Transport-layer security
 - Firewall compatibility
 - Post-meeting data storing
 - Single Sign On
- Third-party accreditations: Independent audits validate Cisco WebEx security

The terms “WebEx meeting(s)” and “Cisco WebEx meeting sessions” refer to the integrated audio conferencing, Internet voice conferencing, and single- and multi-point video conferencing used in all Cisco WebEx online products, which include:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center (including Cisco WebEx Remote Support and Cisco WebEx Remote Access)

Unless otherwise specified, the security features described in this document pertain equally to all the WebEx applications and services mentioned above.

WebEx meeting roles

The four key roles in a WebEx meeting are Host, Alternate Host, Presenter, and Attendee.

Host

The Host schedules and starts WebEx meetings. The Host controls the in-meeting experience and—as the initial Presenter—can grant Presenter privileges to Attendees. The Host can also start a session’s audio conferencing portion, as well as lock the meeting and expel Attendees.

Alternate Host

The Host appoints an Alternate Host. The Alternate Host can start a scheduled WebEx meeting in lieu of the Host. The Alternate Host has the same privileges as the Host and can control the meeting if the Host is unavailable.

Presenter

A Presenter shares presentations, specific applications, or the entire desktop. The Presenter controls the annotation tools and can grant and revoke remote control over the shared applications and desktop to individual Attendees.

Attendee

An Attendee has minimal responsibilities and typically views session content.

The Cisco Collaboration Cloud infrastructure

The Cisco Collaboration Cloud is a communications infrastructure purpose-built for real-time web communications. Data centers strategically placed near major Internet access points use dedicated, high-bandwidth fiber to route traffic around the globe.

Switched architecture

Cisco deploys a unique, globally-distributed, dedicated network of high-speed meeting switches. Meeting session data originating from the Presenter’s computer and arriving at the Attendees’ computers is switched—never persistently stored—through the Cisco Collaboration Cloud. The Cisco Collaboration Cloud enables a uniquely secure, extremely scalable, and highly available meeting infrastructure.



Data centers

WebEx meeting sessions use switching equipment located in multiple data centers around the world. Cisco owns and operates all infrastructure used within the Cisco Collaboration Cloud. Currently this network consists of data centers in Mountain View, CA; Thornton, CO; Richardson, TX; Ashburn, VA; London, UK; Bangalore, India; Beijing, China; and Tokyo, Japan. Additionally, Cisco operates four iPoPs (network Point of Presence locations) that facilitate backbone connections, Internet peering, and caching technologies used to enhance end-user performance and availability. The iPoPs are located at San Jose, CA; New York City, NY; Mumbai, India; and Melbourne, Australia. Cisco personnel are available 24x7 to provide required logistical security, operational, and change-management support.

The secure WebEx meeting experience

WebEx meeting site configuration

The WebEx Site Administration module manages and enforces security policies for your customized WebEx site. Settings controlled at this level determine Host and Presenter privileges for scheduling meetings. For example, you may disable a Presenter's ability to share applications or to transfer files on a per-site or a per-user basis by customizing session configurations to meet your business goals and security requirements. The WebEx Site Administration module manages these security-related features:

Account management

- Lock out an account after a configurable number of failed login attempts.
- Automatically unlock a locked out account after a specified time interval.
- Deactivate accounts after a defined period of inactivity.

Specific user account management actions

- Require a user to change password at next login.
- Lock or unlock a user account.
- Activate or deactivate a user account.

Account creation

- Require email confirmation of new accounts.
- Require security text on new account requests.
- Allow self registration (sign up) for new accounts.
- Configure rules for self-registration of new accounts.

Account passwords

- Enforce strong account password criteria.
- Configure the number of days before a temporary password expires.
- Require Hosts to change account passwords at a configurable interval.
- Require all Hosts to change account password at next login.

Strong account password criteria

- Minimum length.
- Mixed case.
- Minimum numeric.
- Minimum alpha.
- Minimum special characters.
- Do not allow a character to be repeated three times or more.
- Do not allow re-use of a specified number of previous passwords.
- Do not allow dynamic text (site name, Host's name, username).
- Do not allow passwords from a configurable list (for example, "password").
- Minimum password change interval.

Strong meeting password criteria

- Require all meetings to have a password.
- Minimum length.
- Mixed case.
- Minimum numeric.
- Minimum alpha.
- Minimum special characters.
- Do not allow a character to be repeated three times or more.
- Do not allow dynamic text (site name, Host's name, username, meeting topic).
- Do not allow passwords from a configurable list (for example, "password").

Personal Meeting Rooms—accessible using a personalized URL and password—help enable the Host to list scheduled and in-progress meetings, start and join meetings, and share files with meeting Attendees. You can use Site Administration to set security-related features for Personal Meeting Rooms.

- Change the Personal Meeting Room URL.
- Configure sharing options for files in the Personal Meeting Room.
- Configure password requirements for files in the Personal Meeting Room.

Other security-related features are enabled through WebEx Site Administration.

- Allow any Host or Attendee to choose to store their name and email address to make joining successive meetings easier.
- Allow Hosts to reassign recordings to other Hosts.
- Restricted Site Access—the Site Administrator can require authentication for all Host and Attendee access. Authentication is required even to access any site information—such as listed meetings—as well as to gain access to meetings on the site.
- Require strong meeting passwords for Cisco WebEx Remote Access sessions.
- Require that all meetings are unlisted.

You can request additional configurations from your WebEx Customer Success representative.

- Require approval of “Forgot Password?” request.
- Require Site Administrator to reset account passwords, rather than re-entering on behalf of a user.
- Store passwords using one-way hashing.

Security options for scheduling WebEx meetings

Give individual Hosts the ability to specify meeting access security—within parameters configured at the Site Administration level—that cannot be overridden.

- Schedule a meeting as unlisted so that it doesn’t display on the visible calendar.
- Allow Attendees to join meetings before the Host joins.
- Allow Attendees to join audio before the Host joins.
- Display teleconference information in meeting.
- End meetings automatically in a configurable time if only one Attendee remains.
- Include Host key in meeting emails.
- Require Attendees to enter their email address when joining meetings.

Listed or unlisted meetings

Hosts can opt to list a meeting in the public meeting calendar on your customized WebEx site. Or they can schedule the meeting as unlisted, so it never appears on a meeting calendar. Unlisted meetings require the Host to inform Attendees explicitly of the existence of the meeting—either through a link sent to Attendees using the email invitation process or by requiring the Attendee to enter the provided meeting number on the Join Meeting page.

Internal or external meetings

Hosts can restrict meeting Attendees to only those with an account on your customized WebEx site, as verified by their ability to log in to the site to join the meeting.

Meeting passwords

A Host can set a meeting password and then optionally choose to include or exclude the password in the meeting invitation email.

Enrollment

- Restrict meeting access with the enrollment feature. The Host generates an “access control list” allowing only Invitees who have enrolled and been explicitly approved by the Host to join.
- Take greater control over the distribution of meeting access information by choosing not to send email invitations to a meeting.
- Secure meetings by blocking the re-use of Registration IDs in the WBS27 versions of WebEx Training Center and WebEx Event Center. Any Attendee attempting to re-use a Registration ID already in use will be prevented from joining the meeting.

In addition, a Host can maintain meeting security by restricting access and expelling participants.

Fine-tune WebEx meetings using any combination of these scheduling options to support your security policies.

Starting and joining a WebEx meeting

A WebEx meeting starts after a Host’s user ID and password is authenticated by your customized WebEx site. The Host has initial control of the meeting and is the initial Presenter. The Host can grant or revoke Host or Presenter permissions to any Attendee, expel selected Attendees, or terminate the session at any time.

The Host can appoint an Alternate Host to start and control the meeting in case the Host is unable to attend or loses their connection to the meeting. This keeps meetings more secure by eliminating the possibility the Host role will be assigned to an unexpected, or unauthorized, Attendee.

You can configure your customized WebEx site to allow Attendees to join the meeting—including the audio portion—before the Host, and to limit the features available to early-joiners to chat and audio.

When an Attendee joins a WebEx meeting for the first time, the WebEx application automatically downloads a complete file set to the Attendee’s computer. VeriSign issues digitally signed security certificates to these downloads, so the Attendee knows the files are from WebEx. In subsequent meetings, the WebEx application downloads only files containing changes or updates. Attendees can use the Uninstall function provided by their computer’s operating system to easily remove all WebEx files.

The Cisco Collaboration Cloud protects each meeting session, and the dynamic data shared within.

Encryption technologies

WebEx meetings are designed to deliver real-time rich-media content securely to each Attendee within a WebEx meeting session. When a Presenter shares a document or a presentation, Universal Communications Format (UCF), a Cisco proprietary technology, encodes and optimizes the data for sharing. The WebEx meeting application on mobile devices such as the iPad, iPhone, and BlackBerry use similar encryption mechanisms as the PC client.

WebEx meetings provide these encryption mechanisms:

1. For WebEx meetings on PCs and mobile devices, data is transported from the client to the Cisco Collaboration Cloud using 128-bit Secure Socket Layer version3 (SSLv3).
2. Documents and presentations are encrypted end-to-end using 256-bit Advanced Encryption Standard (AES) prior to transport.
3. End-to-end (E2E) encryption is an option provided with Cisco WebEx Meeting Center version WBS26 and later. This method encrypts all meeting content, end-to-end, between meeting participants, using the AES encryption standard with a 256-bit key randomly generated on the Host's computer and distributed to Attendees with a public key-based mechanism.
4. Public Key Infrastructure (PKI) based End to End encryption is an option provided with WebEx Meeting Center version WBS27 and later, using the 256-bit AES encryption standard. The mechanism requires that Attendees have a X.509 certificate to start or join a meeting.
5. A user's login password for WebEx meetings on mobile devices is encrypted using 128-bit Data Encryption Standard (DES).

Site administrators and Hosts can select either E2E or PKI using the "Meeting type" option. E2E and PKI solutions provide stronger security than AES alone (though E2E and PKI also use AES for the payload encryption) as the key is known only to the meeting Host and Attendees.

Every WebEx meeting connection must authenticate properly prior to establishing a connection with the Cisco Collaboration Cloud to join a WebEx meeting. The client authentication process uses a unique per-client, per-session cookie to confirm the identity of each Attendee attempting to join a WebEx meeting. Each meeting contains a unique set of session parameters generated by the Cisco Collaboration Cloud. Each authenticated Attendee must have access both to these session parameters and the unique session cookie to join the meeting successfully.

Transport layer security

In addition to the application layer safeguards, all meeting data is transported using 128-bit SSLv3. Rather than using firewall port 80 (standard HTTP Internet traffic) to pass through the firewall, SSL uses firewall port 443 (HTTPS traffic), restricting access over port 80 without affecting WebEx traffic.

WebEx meeting Attendees connect to the Cisco Collaboration Cloud using a logical connection at the application/presentation/session layers. There is no peer-to-peer connection between Attendee's computers.

Firewall compatibility

The WebEx meeting application communicates with the Cisco Collaboration Cloud to establish a reliable and secure connection using HTTPS (port 443) so your firewalls don't have to be specially configured to enable WebEx meetings.

Post-meeting data storing

No session information is retained on the Cisco Collaboration Cloud or on Attendee's computers once the WebEx meeting concludes. Cisco retains only two types of meeting information.

- **Event Detail Records (EDRs):** Cisco uses EDRs for billing and reporting. You may review event detail information on your customized WebEx site by logging in using your Host ID. Once authenticated, you can also download this data from your WebEx site or access it through WebEx APIs.
- **Network-based recording (NBR) files:** If a Host chooses to record a WebEx meeting session, the recording will be stored within the Cisco Collaboration Cloud and can be accessed in the MyRecordings area on your customized WebEx site.

Single Sign On

Cisco supports federated authentication for user Single Sign On (SSO) using SAML 1.1, 2.0 and WS-Fed 1.0 protocols. Using federated authentication requires you to upload a public key X.509 certificate to your customized WebEx site. You then generate SAML assertions containing user attributes and digitally sign the assertions with the matching private key. WebEx validates the SAML assertion signature against the preloaded public key certificate before authenticating the user.

Third-party reporting

Beyond its own stringent internal procedures, the WebEx Office of Security engages multiple independent third parties to conduct rigorous audits against internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications.

These auditors include Information Security Partners, LLC (iSEC Partners) for exhaustive network routing and application, and PriceWaterhouseCoopers, for SAS-70 Type II audit

iSEC Network Routing

iSEC Partners completed a variety of tests to confirm the routing to and from WebEx meeting Attendees and the Cisco Collaboration Cloud. The tests covered both traces for WebEx production servers, and route confirmation traces for various network device configurations that included routers, firewalls, and load balancers. The results of this testing indicate that communication for U.S.-based WebEx sites does not route outside of the U.S. For more information, you may request a copy of this report from the WebEx Office of Security.

iSEC Source Code Review

iSEC Partners performs ongoing, in-depth code-assisted penetration tests and service assessments. During these engagements, iSEC Partners receives access to WebEx servers, source code, and engineering staff. Unlike black box testing, this high degree of access enables iSEC Partners to:

- Identify critical application and/or service vulnerabilities and propose solutions.
- Recommend general areas for architectural improvement.
- Identify coding errors and provide guidance on coding practice improvements.
- Work directly with WebEx engineering staff to explain findings and provide guidance for remediation work.

For more information, you may request a copy of this report from the WebEx Office of Security.

SAS-70 Type II

PricewaterhouseCoopers LLP performs an annual SAS-70 Type II audit in accordance with standards established by the AICPA. For additional information on the SAS-70 standard please see: www.sas70.com/index2.htm. For more information, you may request a copy of PricewaterhouseCoopers LLP SAS-70 report from the WebEx Office of Security via your Cisco account representative.

ISO-27001/2

Cisco designed its SAS70 controls to resemble information security controls from ISO27002, noted in an appendix to ISO27001. ISO-27001 is an information-security standard published by the International Organization of Standardization (ISO) that provides best-practice recommendations on creating an information-security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk-management processes. According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information-security management system." Refer to this link for additional information on ISO-27001/2: <http://www.27000.org/>.

Conclusion

Your organization can trust Cisco WebEx online applications to enable collaboration and streamline business processes—in even the most stringent security environments. Choose easy to use, reliable, proven, and secure software-as-a-service WebEx collaboration solutions from Cisco.

