White Paper

# Unleash the Power of Secure, Real-Time Collaboration

This paper includes security information for Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Support Center and Cisco WebEx Event Center.

## Introduction

Cisco WebEx® online solutions help enable global employees and virtual teams to meet and collaborate in real time as though they were working in the same room. In fact, online collaboration can improve on traditional face-to-face collaboration by making travel time and costs - and even conference room space - a non-issue. Businesses, institutions, and government agencies worldwide rely on Cisco® WebEx solutions to simplify business processes and improve results for sales, marketing, training, project management, and support.

For all of these companies and agencies, security is a fundamental concern. Online collaboration must provide multiple levels of security, from scheduling meetings to authenticating participants to document sharing.

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 business processes with confidence, even with the most rigorous security requirements.

Understanding the security features of Cisco WebEx online applications and the underlying communication infrastructure - the Cisco WebEx cloud - is an important part of your investment decision.

## The Cisco WebEx Cloud Infrastructure

Cisco WebEx Meetings is a software-as-a-service (SaaS) solution delivered through the Cisco WebEx cloud - a highly secure service delivery platform with unmatched performance, integration flexibility, scalability, and availability. The Cisco WebEx cloud offers ease of deployment and application delivery to lower your total cost of ownership, while ensuring the highest grade of enterprise security.

### Switched Architecture

Cisco deploys a 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 WebEx cloud.[1]

### Data Centers

The Cisco WebEx cloud is a communications infrastructure purpose-built for real-time web communications. WebEx meeting sessions use switching equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated, high-bandwidth fiber to route traffic around the globe. Cisco owns and operates all infrastructure used within the Cisco WebEx cloud. Data within the United States stays within the U.S. region and data within Europe remains in the European region.

[1] When the user enables Network-based Recording (NBR), the meeting is recorded and stored. In addition to NBR, WebEx also stores user profile data.

Additionally, Cisco operates network Point of Presence (PoP) locations that facilitate backbone connections, Internet peering, global site backup, and caching technologies used to enhance end-user performance and availability. Cisco personnel are available 24 hours a day, seven days a week, for logistical security, operational, and change-management support.

## Overview of the Highly Secure WebEx Meeting Experience

The WebEx meeting experience encompasses:

- Meeting-site configuration
- Scheduling security options
- Starting and joining a WebEx meeting
- Encryption technologies
- Transport-layer security
- Firewall compatibility
- Meeting data privacy
- In-meeting security
- 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, These products 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 mentioned above.

## WebEx Meeting Roles

The four roles in a WebEx meeting are Host, Alternate Host, Presenter, and Attendee. The following describe the roles of each as they pertain to security privileges.

### Host

The Host schedules and starts WebEx meetings. The Host controls the in-meeting experience. From a security standpoint, the Host can grant Presenter privileges to Attendees. The Host can also lock the meeting and expel Attendees.

### Alternate Host

The Host appoints an Alternate Host who can start a scheduled WebEx meeting in lieu of the Host. From a security standpoint, the Alternate Host has the same privileges as the Host.

### Presenter

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

### Attendee

From a security standpoint, an Attendee has no security responsibilities or privileges.

## WebEx Site Administration Module

The WebEx Site Administration module allows authorized administrators to manage and enforce security policies on a meeting-by-meeting basis for Host and Presenter privileges. For example, you can 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.

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

### Account Passwords

Enforce strong account password criteria, including:

- Mixed case
- Minimum length
- 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
- Require Hosts to change account passwords at a configurable interval
- Require all Hosts to change account password at next login
- Configure the number of days before a temporary password expires

### Personal Meeting Rooms

Personal Meeting Rooms are accessible using a personalized URL and password. These meeting rooms help enable the Host to list scheduled and in-progress meetings, start and join meetings, and share files with meeting Attendees. Administrators can set security-related features for Personal Meeting Rooms, including:

- 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 Enabled Through WebEx Site Administration

- Allow any Host or Attendee to choose to store their names and email addresses to make organizing or joining new meetings easier
- Allow Hosts to reassign recordings to other Hosts
- Restricted Site Access by requiring 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 be unlisted
- 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

The Host also has an option to allow only attendees with an account on the WebEx site.

### 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 does not 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 meetings
- End meetings automatically in a configurable time if only one Attendee remains
- 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 a customized WebEx site. Or they can schedule the meeting as unlisted, so that 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 a 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

- The host can 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 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 are 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 and installs to the Attendee’s computer. VeriSign digitally assigns Cisco WebEx the security certificates for the WebEx client software, ensuring the meeting participant knows the files are from Cisco. In subsequent meetings, the WebEx application downloads and installs only files containing changes or updates. Attendees can use the Uninstall function provided by their computer’s operating system to easily remove WebEx files.

## Encryption Technologies

WebEx meetings are designed to deliver real-time rich-media content more 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:

- For WebEx meetings on PCs and mobile devices, data is transported from the client to the Cisco WebEx cloud using 128-bit Secure Socket Layer version3 (SSLv3)
- End-to-end (E2E) encryption is an option provided with Cisco WebEx Meeting Center. 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. Unlike SSL encryption that is terminated at Cisco WebEx cloud side, in E2E-enabled meetings all meeting contents are kept as encrypted format within the Cisco WebEx cloud Infrastructure. Clear text meeting content data is only presented in meeting participants' computer memory [2]
- If a user chooses the related "Remember me" option, that user's login ID and password for WebEx meetings saved on PCs and mobile devices are encrypted using 128-bit Advanced Encryption Standard (AES)

Site administrators and Hosts can select either E2E using the "Meeting type" option. The E2E solution provides stronger security than AES alone (though E2E also uses AES for the payload encryption), because 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 WebEx 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 WebEx 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 WebEx cloud using a logical connection at the application/presentation/session layers. There is no peer-to-peer connection between Attendees' computers.

## Firewall Compatibility

The WebEx meeting application communicates with the Cisco WebEx cloud to establish a reliable and highly secure connection using HTTPS (port 443). As a result, your firewalls do not have to be specially configured to enable WebEx meetings.

[2] Note that NBR is not available when encryption is enabled. This option is only available for WebEx Meeting Center.

### Meeting Data Privacy

All WebEx meeting contents (chat, audio, video, desktop, or document sharing) are transient (only exist during the meeting). Meeting contents are not stored at either a Cisco Cloud or an attendee's computer by default. Cisco retains only two types of meeting information. They include:

- **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. EDRs contain basic meeting attendance information, including: Who (user name and email) joins what meeting (meeting ID) and when (join and quite meeting time). Such information is necessary and only for billing and reporting purposes.
- **Network-based recording (NBR) files:** If a Host chooses to record a WebEx meeting session, the recording will be stored within the Cisco WebEx cloud and can be accessed in the MyRecordings area on your customized WebEx site. The NBR recording will only be created if a Host enables it during the meeting or chooses a site-wide option to record all meetings. The NBR recording is protected by cryptographic token. The Host has full controls to NBR recording file access, including: delete it, share it with someone, or create additional passwords to protect it.

### 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 can 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 Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications.

### Third-Party Security Assessment

Cisco uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- 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

## Safe Harbor Certification

In March 2012, Cisco successfully obtained Safe Harbor Certification for customer and partner data (Safe Harbor Certification for employee data was obtained in 2011). This serves as an additional component of Cisco's comprehensive privacy compliance program, and while not required, the company recognizes the value that customers place on this certification.

The EU Data Protection Directive prohibits the transfer of European citizens' personal data to non-European Union nations that do not meet the EU's "adequacy" standard for privacy protection. The U.S. Department of Commerce, in concert with the European Commission, developed a "Safe Harbor Framework" that allows U.S. organization to comply with the Directive by abiding by a set of Safe Harbor Privacy Principles. Companies certify their compliance with these Principles on the U. S. Department of Commerce website. The Framework was approved by the EU in 2000 and gives companies that abide by the Principles assurance that the EU will consider their practices "adequate" privacy protections for EU citizens.

### SSAE16

PricewaterhouseCoopers LLP performs an annual SSAE16 audit in accordance with standards established by the AICPA. For additional information on the SSAE16 standard please see: http://www.ssae16.com.

### ISO-27001/2

Cisco designed its SSAE16 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/.

## For More Information

For more information on Cisco WebEx solutions please visit http://www.cisco.com/en/US/products/ps10362/Products_Sub_Category_Home.html or contact your sales representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Printed in USA C11-709579-00 06/12