



WebEx Security Overview

A thick, horizontal green bar with a wavy, organic shape on its top edge, spanning the width of the page below the title.

WebEx Communications Inc.

3979 Freedom Circle, Santa Clara, CA 95054, U.S.A.

Corp.: +1.408.435.7000 **Sales:** 1.877.509.3239

www.webex.com

Table of Contents

Introduction	3
The Underlying Infrastructure	5
The Secure WebEx Meeting Experience	7
Third Party Accreditation	11
Conclusion	13



Introduction

WebEx™ Communications, Inc. provides real-time collaboration services to a large and growing number of businesses. These businesses use WebEx applications for diverse purposes ranging from sales and marketing to training, project management and support. WebEx customers span a variety of market sectors including technology, finance, manufacturing and healthcare. WebEx assigns data security the highest priority in the design, deployment and maintenance of its network, platform and applications, and its offerings meet the most stringent security requirements of businesses and government agencies so they can use WebEx services effectively and routinely, secure in the knowledge that their sessions are safe and private.

WebEx assigns data security the highest priority in the design, deployment and maintenance of its network, platform and applications, and its offerings meet the most stringent security requirements of businesses and government agencies.

The purpose of this document is to provide information on the data security features and functions that are available in the various WebEx applications and are inherent to the underlying WebEx communication infrastructure known as MediaTone™. In the following pages we will examine:

- MediaTone infrastructure
- The Secure WebEx Meeting Experience
 - Site configuration
 - Scheduling a meeting
 - Starting and joining a meeting
 - In-meeting
 - Transport layer security
 - Firewall compatibility
 - Post meeting
- 3rd party security accreditation

The reader of this document is assumed to be familiar with core WebEx capabilities and services, including an understanding of the WebEx MediaTone Network. WebEx web meeting applications and value-added applications include:

- Meeting Center, for highly interactive team collaboration
- Training Center, to deliver effective training via the Web
- Event Center, for large Web-based seminars
- Support Center, for remote support sessions
- Sales Center, for online sales meetings
- SMARTtech, to create a managed network of remotely accessible computers
- GlobalWatch, for meeting performance monitoring



Additionally, WebEx offers integrated audio conferencing, VoIP, and single and multi-point video conferencing.

The reader of this document should also be aware of the key roles available in the various applications, such as Host, Presenter and Attendee:

Host

A Host schedules and starts WebEx sessions. The Host also controls the in-meeting experience and as the initial Presenter can grant Presenter privileges to Attendees. The Host also starts a session's audio conferencing portion, can lock the meeting, and expel attendees.

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.

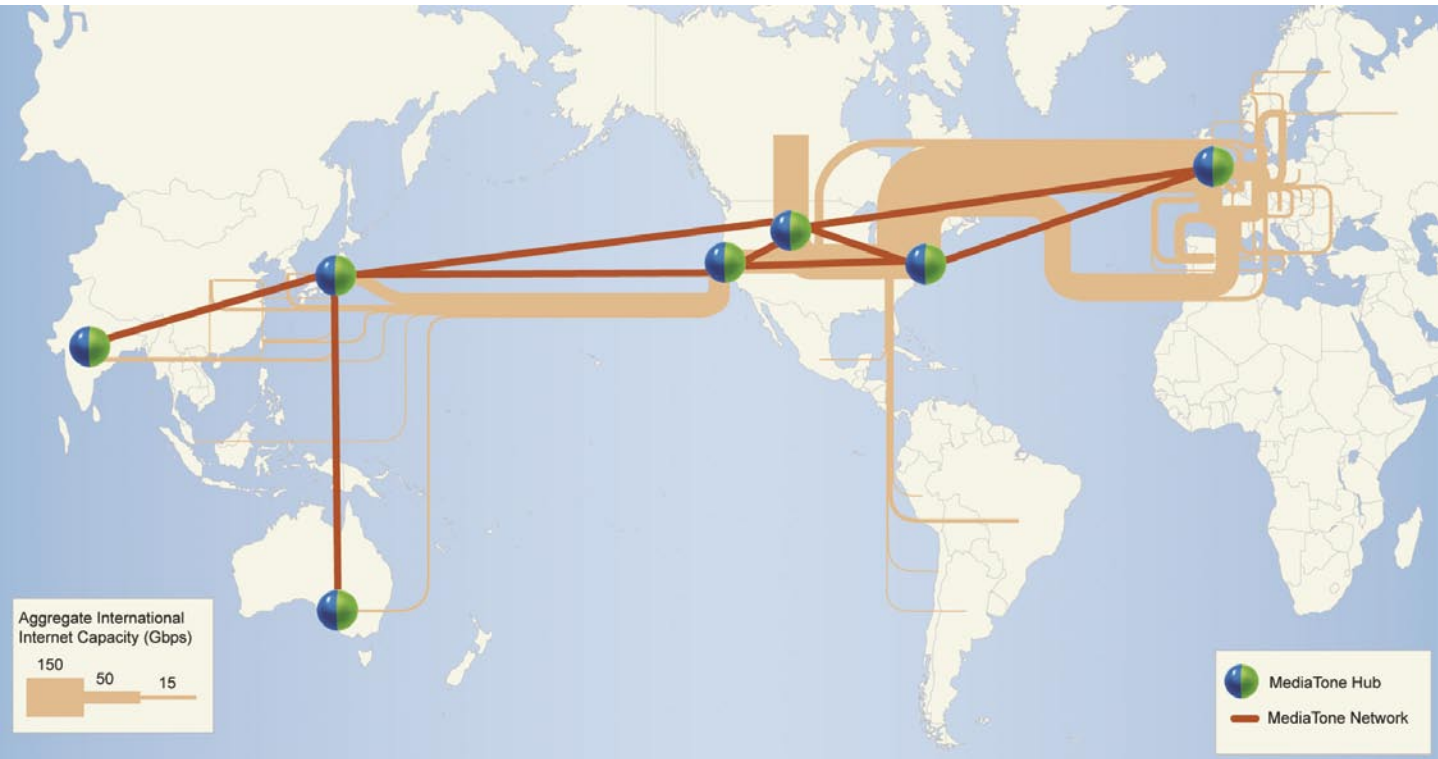
Unless otherwise specified, the topics described in this document pertain equally to all WebEx applications and services.



The Underlying Infrastructure

The WebEx MediaTone Network

The WebEx MediaTone Network is a communications infrastructure purpose-built for real-time web communications. It consists of a series of data centers located around the world, strategically placed near major internet access points. WebEx traffic is routed between the WebEx data centers using dedicated, high-bandwidth fiber.



Switched Architecture

WebEx uniquely deploys a globally-distributed network of high-speed MediaTone switches. With this architecture, session data originating from the Presenter's machine and arriving at the Attendees' machines is switched — never persistently stored — through the WebEx MediaTone Network. This is unlike other web meeting solutions that use a store and forward server model where potentially sensitive content is persistently stored on vendors' equipment. WebEx sessions are thus completely transient and operate similarly to a voice conversation over the public phone network. In addition to unique security benefits, this architecture also enables an extremely scalable and highly available meeting infrastructure unburdened by the physical limitations of premise-based server solutions



WebEx security personnel spend a significant amount of time receiving training in all aspects of enterprise security from vendors and industry experts to remain at the forefront of security trends.

Data Centers

WebEx session content is switched using WebEx equipment located at WebEx owned and operated data centers worldwide. Current WebEx data center locations include: Mountain View, CA; Denver, CO; Reston, VA; London, UK; and Tokyo, Japan. Each facility is staffed, 24 hours a day, seven days a week. WebEx also has nodes in Melbourne, Australia and Bangalore, India.

To gain access to any facility, one must be on the approved-access list managed by the WebEx security team, described next. Access is further controlled by biometric security devices.

Security Personnel

WebEx has a dedicated security department, which reports directly to the WebEx CIO. The team includes a GIAC-Certified Forensic Analyst, two CISSPs, a GIAC Certified Intrusion Analyst, and an ISSMP. WebEx security personnel spend a significant amount of time receiving training in all aspects of enterprise security from vendors and industry experts to remain at the forefront of security trends.

The separation of duties that exists between WebEx security personnel and other WebEx personnel was a major factor that enabled WebEx to qualify for both WebTrust and SAS-70 Type II certifications (discussed later in this paper).



The following security capabilities are available to the Host:

- Start/Schedule WebEx meetings.
- Grant/Revoke Presenter privileges.
- Grant/Revoke Host privileges.
- Terminate application sharing session for all Attendees in the meeting.
- Restrict access to the meeting when the meeting is in progress.
- Expel Attendees.
- End the meeting.
- Mute/Un-Mute Attendees using the integrated teleconferencing features.
- Take notes using the integrated note taking feature or assign these privileges to an Attendee and send these notes to each Attendee before closing the meeting.

The following security capabilities are available to the Presenter:

- View the list of Attendees in the session.
- Enable/Disable Attendees to save or print presentations or documents shared in the session.
- Enable/Disable Attendees to switch pages in a presentation or document share.
- Enable/Disable Attendees to annotate on session content.
- Enable/Disable Attendees to send text messages to other Attendees, the Presenter (or both).
- Enable/Disable Attendees to record the session.
- Ability to grant temporary control of a shared application to specific Attendees.
- Temporarily freeze application or desktop share, preventing the Attendees from viewing shared content during this time in order to allow the Presenter private and secure access to sensitive portions of the application.
- Patent Pending capabilities that keep Host and Presenter meeting management such as chat, note taking, and attendee management private.

The Secure WebEx Meeting Experience

WebEx Meeting Site Configuration

The WebEx Site Administration module allows customers to enforce security policies across their WebEx site. For example, the Presenter's ability to share desktop can be disabled on a per-site basis. Settings established at this level propagate to all sessions created on the specific site. Other security related features of Site Administration Configuration include:

- All meetings must be unlisted.
- Require Meeting Attendee e-mail address.
- Require strong password.
- Customer-configurable strong password criteria.
- Restricted Site Access - The Site Administrator can determine that access to a site for all users — Hosts and Attendees — requires authentication. In this manner, the Administrator is certain that authentication is required even to access to site information (e.g., listed meetings) as well as to gain access to meetings on the site.
- Require approval of "Forgot Password?" request.
- Require that all meetings must have a password.

Scheduling a Meeting

In addition to security parameters defined at the site level, a Host can specify meeting access controls around the following parameters:

(Note that Hosts cannot override parameters configured at the site level.)

- **Listed or Unlisted meeting**
 - This option allows the Host to list the meeting on their site's public meeting calendar or to make the meeting unlisted. Unlisted meetings never appear on a meeting calendar and are accessible only through a link sent via the e-mail invitation process or by an Attendee explicitly providing the meeting number on the meeting join page. In either case, the Host must explicitly inform the Meeting Attendee of the existence of the meeting.
- **Open or password protected**
 - The Host may require the Attendees to enter a password before joining and may also exclude the meeting password from the meeting invitation e-mail.



To gain a better understanding of UCF, it is useful to compare it to PDF. The PDF format is a bandwidth-friendly, encoded representation of the original object. This encoded content contains no original content but only a representation of the original content, which is interpreted by the Adobe Acrobat viewer. The WebEx Meeting Service Manager functions similarly. The WebEx Meeting Service Manager, running on the Presenter's machine, encodes a representation of the original object and delivers only that representation to the Attendees within the session, who then render the content. The encoded content never contains the source presentation content and it is viewable only by the WebEx Meeting Service Manager. This unique approach results in two important benefits: Reduced bandwidth, since the encoded size is often 2-3 times smaller than the source; and increased security, since no clear text or original content ever leaves the Presenter's machine.

After the presentation content is encoded on the Presenter's machine by the WebEx Meeting Service Manager, the content is "stamped" with a Session ID that only it and the Attendee's Meeting Service Manager know. WebEx uses this value in order to thwart hackers from reassembling session content. These techniques provide safeguards to prevent reconstruction of the data conferencing portion of the WebEx session.

- **Enrollment**

- To further restrict access the Host can use an "access control list" via the enrollment capability, specifying that only users specifically invited to the meeting can join the meeting — only after the Invitee has enrolled and has been explicitly approved by the Host.
- If not already mandated at the site level, the Host can choose to not send e-mail invitations for the meetings. This allows the Host greater control over the distribution of the meeting access information.

WebEx customers may use any combination of the above to fine-tune WebEx to meet their security policies.

Starting and Joining a Meeting

WebEx meetings must be started by a Host. A Host is required to authenticate to the WebEx site with their user ID and password. Once the Host is authenticated, he or she can start a WebEx meeting. The Host has the first level of control in the meeting and is made the initial Presenter. He or she can grant or revoke Host or Presenter permissions at any time to any Attendee in the meeting. The Host can also terminate the session for all Attendees at any time or expel selected Attendees.

The WebEx site can be configured to allow Attendees to join before the Host. When joining before Host, Attendees cannot share presentations or use any of the other features of the meeting service except for the chat feature.

In-Meeting Security

During the meeting, WebEx implements security primarily via the WebEx Meeting Service Manager. The WebEx Meeting Service Manager is designed to deliver, in real time, rich-media content securely to each Attendee within a WebEx session. All content that a Presenter shares with the Attendees in a WebEx session is only a representation of the original data. This content is encoded and optimized for sharing using UCF (Universal Communications Format) a WebEx proprietary technology.

The WebEx Meeting Service Manager:

- Is invoked only from within a Web browser and cannot be started independently.
- Is digitally signed by Verisign.
- Is the only means possible to participate in a WebEx session.
- Is entirely dependent upon connections established on a session-by-session basis with the WebEx MediaTone Network.
- Performs a proprietary encoding process that encodes all shared data.



- Encrypts all presentation sharing content using the AES encryption standard.
- Encrypts the connection to the MediaTone Network using the 128-bit SSL encryption standard.
- Provides a visual identification of every Attendee in the meeting.

It is impossible to participate in a WebEx session without the close coordination between the Meeting Service Manager and the MediaTone Switching Network. Since the data in a WebEx session is shared using the Meeting Service Manager, which must establish a connection with a MediaTone Switching Network, these security features are inherent throughout the session. In short, each session is dynamic and involves a handshake between the Meeting Service Manager and the MediaTone Meeting Switch.

Each WebEx session has a unique set of session parameters that are generated by the MediaTone Meeting Switch. Each authenticated Attendee must have access to these session parameters in conjunction with the unique session cookie in order to successfully join the WebEx session.

Every WebEx Meeting Service Manager connection must authenticate properly prior to establishing a connection with the MediaTone Meeting Switch to join a WebEx session. The client authentication process uses a unique per-client, per-session cookie to confirm the identity of each Attendee attempting to join a WebEx session. Each WebEx session has a unique set of session parameters that are generated by the MediaTone Meeting Switch. Each authenticated Attendee must have access to these session parameters in conjunction with the unique session cookie in order to successfully join the WebEx session.

Transportation Layer Security

In addition to all the safeguards discussed in the application layer, for utmost security, WebEx by default encrypts all presentation content using the Advanced Encryption Standard (AES) algorithm and further provides the option of securing all session content by encrypting the communication channel between the WebEx Meeting Service Manager and the MediaTone Meeting Switch using a 128-bit Secure Sockets Layer (SSL) encryption tunnel.

Rather than using firewall port 80 (standard HTTP Internet traffic) to pass through the firewall, SSL uses firewall port 443 (HTTPS traffic). This allows customers to restrict access over port 80 without affecting their WebEx traffic.

Lastly, WebEx meeting participants connect to the WebEx MediaTone Network via a logical connection; there is no peer-to-peer connection between the local machines. The logical connection is controlled by the WebEx Meeting Service Manager and is dedicated exclusively to WebEx session communications. As a result, there is no way to perform general-purpose tasks outside of what the WebEx Meeting Service Manager allows.



The only information that WebEx retains pertaining to a session is Event Detail Records or EDR, used for billing and reporting purposes.

Firewall Compatibility

The WebEx Meeting Service Manager communicates with the WebEx switch to establish a reliable and secure connection. At the time of instantiation, the WebEx Meeting Service Manager will determine the best method for communication. In the process of establishing this connection, the WebEx Meeting Service Manager attempts to connect using TCP (port 1270) or HTTP/HTTPS (port 80/443). Quite often port 1270 is blocked by a firewall and when this is the case the WebEx Meeting Service Manager will tunnel all WebEx communications using HTTP/HTTPS. In the case that a WebEx site incorporates an SSL connection, all the traffic is carried over HTTPS (port 443). Regardless of the connection that is established at the time of instantiation, by establishing this communication between the Meeting Service Manager and the WebEx switch, firewalls do not have to be specially configured to enable WebEx sessions.

Post Meeting

Once the meeting is over, no session information is retained on the MediaTone Meeting Switches or on Attendee's PCs. If a Host opts that a session be recorded, the recording will either be located on a client machine or under the secured MyRecordings area — separate from the shared WebEx communications framework. This is analogous to a voice mail and the phone system. The voice mail itself is persistently stored separate from the core communications network, yet the communications network gave rise to the voice mail. The network itself retains no content; only the voice mail contains content.

The only information that WebEx retains pertaining to a session is Event Detail Records or EDRs. WebEx uses the EDRs for billing and reporting purposes. The EDRs are stored at the WebEx Operational Database and are available to customers for review on their WebEx site once they have logged in using their Host ID or for download from the WebEx site or through the WebEx APIs.



Unlike any other seal that claims to protect consumer or business privacy, WebTrust is the only seal administered by a third-party. WebEx undergoes an annual recertification process to maintain our WebTrust seal.

For more information on WebTrust please visit: <http://www.webtrust.net/>



SAS-70 is the authoritative guidance that allows WebEx to disclose its control activities and processes in a uniform reporting format.

For more information on SAS 70 please visit: <http://www.sas70.com/>



Third Party Accreditation

WebTrust

Ernst & Young LLP has accredited WebEx with the WebTrust seal. WebTrust is a seal of assurance awarded to companies that consistently adhere to certain business standards established by the American Institute of Chartered Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) and recognized globally.

The WebTrust Security Principle sets out an overall objective for the security of data transmitted over the Internet and stored on an e-commerce system. In the course of a WebTrust audit, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved. Backed by the AICPA and CICA, WebTrust is the only seal that can give the business community true confidence that a company can be trusted with their most important asset and prized possession: their private information.

Independent verification is the key to WebTrust. Unlike any other seal that claims to protect consumer or business privacy, WebTrust is the only seal administered by a third-party. WebEx undergoes an annual recertification process to maintain our WebTrust seal.

SAS-70 Type II

Ernst & Young LLP also performs an annual SAS 70 Type II audit and provides WebEx with a corresponding report. The Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SAS-70 Type II audit is widely recognized, and it represents that WebEx has been through an in-depth audit of its control activities. The report allows WebEx to demonstrate that it has adequate controls and safeguards when it handles and processes data belonging to its customers.

SAS-70 is the authoritative guidance that allows WebEx to disclose its control activities and processes in a uniform reporting format. The SAS-70 Type II audit and corresponding report certify that an independent auditor (Ernst & Young) examines, on an ongoing basis, the controls and safeguards WebEx has put in place around the data confidentiality and security of its customers data. This SAS-70 Type II report is available for review by customer security and audit teams under NDA.



WebEx's Commitment

WebEx believes that privacy and security are of the highest importance to our clients and business partners. WebEx's commitment includes:

- Consult with specially trained and licensed WebTrust and SAS-70 auditors to review our security policies and procedures.
- Maintain the highest business standards found on the Internet.
- Have our production environment regularly audited to make sure the standards are maintained.

HIPAA Considerations

WebEx is not a health-related business and has no control over the selection of content shared by users in a WebEx meeting.

However, the WebEx MediaTone Network is designed such that no information shared in a WebEx meeting is stored or retained on WebEx switches. This architecture, combined with the above-mentioned security elements, allows HIPAA-regulated entities to easily comply with regulatory guidelines relating to the use, disclosure, and storage of medical information.



Conclusion

Companies and government agencies throughout the world are using WebEx applications and services every day. This would not happen if WebEx did not give careful attention to the incorporation of security principles and standards in the design and operation of the WebEx infrastructure and services. Data security remains the highest priority at WebEx, enabling WebEx to achieve its goal of providing the most efficient and secure online real-time communication service.

©2005 WebEx Communications, Inc. WebEx, WebEx MediaTone, and the WebEx logo are registered trademarks of WebEx Communications, Inc. All rights reserved. All other trademarks are the property of their respective owners.

Worldwide Sales Offices:

Americas & Canada

Tel: +1.877.509.3239

AmericasInfo@webex.com

Europe, Middle East & Africa

Tel: + 31 (0)20.4108.700

europa@webex.com

United Kingdom

Tel: 0800.389.9772

europa@webex.com

Australia & New Zealand

Tel: + 61 (0)3.9653.9581

AsiaPacInfo@webex.com

China (HK)

Tel: + 852.8201.0228

AsiaPacInfo@webex.com

India

Tel: 080.2228.6377/17030 9330

sales@cyberbazaarindia.com

Japan

Tel: + 81 3 5501 3272

JapanInfo@webex.com

Korea

Tel: +82.2.2108.5900

webex@okmodern.com

