



WebEx Support Center - Remote Support Security Overview

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	4
The Secure WebEx Support Center Remote Support Experience	6
Third Party Accreditation	10
Conclusion	12



Introduction

WebEx™ Communications, Inc. provides real-time collaboration services to a large and growing number of corporations. These corporations use WebEx applications for diverse purposes ranging from sales, marketing, 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 corporations 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 available with WebEx Support Center Remote Support and inherent to the underlying WebEx communication infrastructure known as the WebEx MediaTone™ Network. This document will explain the following:

- MediaTone security
- The Secure WebEx Meeting Experience
 - Starting and joining a Support Session
 - In Support Session
 - Transport layer security
 - Firewall compatibility
 - Post Support Session
- 3rd party certification

You should be aware of the key roles available within Remote Support application, such as CSR and Customer/Attendee:

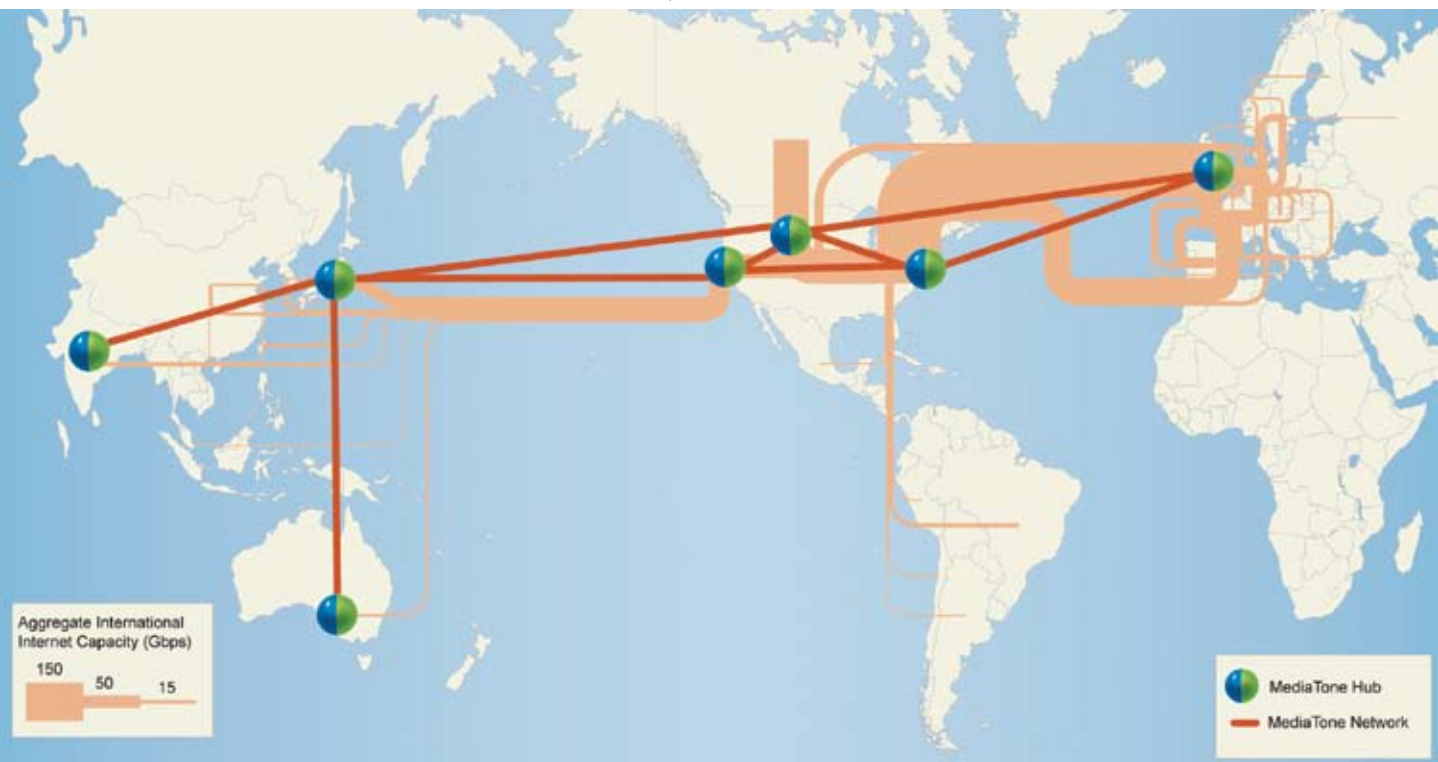
- A CSR starts WebEx Support sessions. The CSR also controls the in-session experience and can trigger different features within Remote Support, such as desktop or application sharing, file transfer, and reboot.
- A Customer/Attendee has minimal responsibilities and typically grants only permissions for CSR actions.



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 routes traffic 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 Attendees' machines is switched—never persistently stored—through the WebEx MediaTone Network. This is unlike other web meeting applications that use a store and forward server model that stores potentially sensitive content for an indeterminate period of time on their 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 datacenter 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 maintains nodes in Melbourne, Australia and Bangalore, India.

To gain access to any facility, one must first be on the approved access list managed by the WebEx Security team, described in the next section. Additionally, WebEx employs biometric security devices to control physical access.

Security Personnel

WebEx employs 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 spends significant resources on training from vendors and industry experts, and the Security personnel regularly receive training in all aspects of enterprise security 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 contributing to WebEx obtaining both WebTrust and SAS-70 Type II certifications, as discussed later in this paper.



The following security capabilities are available to the Host:

- Terminate desktop/application sharing session for all customers in the Support session.
- Terminate File Transfer session for all customers and CSRs.
- Restrict access to the Support session for invited CSRs.
- End the Support session.

The following security capabilities are available to the Customer:

- Grant permission to CSR for different features built in within Remote Support, such as Desktop or Application Sharing, File Transfer, Reboot, and log on as different user. CSR cannot take control or gather information from customer's desktop without customer's permission.
- End Desktop/Application sharing or File transfer session at any point of Support session.
- Leave Support session at any point in Support session.

The Secure WebEx Support Session Experience

WebEx Remote Support Site Configuration

The WebEx Site Administration module enables customers to enforce security policies across their WebEx site. For example, a customer may disable the CSR's ability to Share Desktop 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 the following:

- Must unlist all Support Sessions.
- Require Customer to enter required information in pre-session form.
- Create disclaimer on customer's pre-session/entry form.
- Require strong password.
- Provide customer-configurable strong password criteria.
- Restrict Site Access. The Site Administrator can determine that access to a site for all users – CSRs and Customers – requires authentication. In this manner, the Administrator is certain that authentication is required even to join Support session.
- Require approval of "Forgot Password?" request.
- Require that all Support sessions have a unique Support number.

Starting and Joining a Support Session

WebEx Support sessions must be started by a CSR. A CSR is required to authenticate to the WebEx site with their user ID and password. The CSR may start a WebEx Support session only after he or she is authenticated. CSR has the first level of control in the Support session. CSR can invite customer to join the session – either by sending an email invitation or passing a URL and unique session number to the customer. CSR can also terminate the session for all customers at any time:

In-Session Security

During the Support session, WebEx implements security primarily via the WebEx Support Manager. The WebEx Support Manager is designed to deliver, in real time, rich-media content securely to each Attendee within a WebEx Support 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.



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 Support Manager functions similarly. The WebEx Support 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 Support 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 Support Manager, the content is "stamped" with a Session ID that only it and the Attendee's Support 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.

The WebEx Support Manager:

- Initiates only from within a Web browser and cannot be started independently.
- Is digitally signed by VeriSign.
- Provides the only means possible to participate in a WebEx session.
- Depends entirely on 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 Support Session.

It is impossible to participate in a WebEx session without close coordination between the Support Manager and the MediaTone Switching Network. Since the data in a WebEx session is shared using the Support 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 Support Manager and the MediaTone Switch.

Every WebEx Support Manager connection must authenticate properly prior to establishing a connection with the MediaTone 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.



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 Support Manager and the MediaTone 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 enables customers to restrict access over port 80 without affecting their WebEx traffic.

Lastly, WebEx Support session 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 Support 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 Support 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 Support Manager communicates with the WebEx switch to establish a reliable and secure connection. At the time of instantiation, the WebEx Support Manager determines the best method for communication. In the process of establishing this connection, the WebEx Support Manager attempts to connect using TCP (port 1270) or HTTP/HTTPS (port 80/443). Quite often port 1270 is blocked by a firewall and in this case the WebEx Meeting Service Manager tunnels 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 established at the time of instantiation, by establishing this communication between the Support Manager and the WebEx switch, firewalls need not be specially configured to enable WebEx sessions.

Post Support Meeting

Once the Support Session ends, no session information is retained on the MediaTone switches or on Attendees' PCs. If a CSR opts that a session be recorded, the recording will be located either 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 User 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 globally recognized.

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 this 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. The company'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 Support session. However, the WebEx MediaTone Network is designed such that no information shared in a WebEx Support session 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 use WebEx applications and services everyday. This would not be possible without 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

