



WebEx Support Center Remote Access Security

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
Getting Familiar with WebEx Support Center Remote Access Security Features	4
Understanding Remote Access Network Security	7
Security Concerns FAQs	9
Conclusion	10



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.

Introduction

As the global leader of real-time communications, WebEx provides a unique communications infrastructure based on information switch technology. This proprietary technology enables true interactive communication sessions with levels of functionality, reliability, security, and scalability unmatched by any other organization in this industry. WebEx provides secure, real-time global communication and collaboration services with integrated voice, data and videoconferencing communications.

As data security remains the highest priority at WebEx, the purpose of this document is to provide an overview of the WebEx Remote Support Center Remote Access security functions and features of the WebEx communication infrastructure and present in all WebEx services.

About WebEx Support Center Remote Access

WebEx Support Center Remote Access, built on the WebEx information switch technology, allows unassisted remote access functionality with maximum security, scalability and extensibility.

Host machines limit access to users that come from a specified IP address range. Administrators may define up to three IP address ranges. When initiating a Remote Access session, the host machine requires an access code or phone authentication to access the machine. This code is stored on the server and can be accessed only by administrators with proper authentication. Remote Access sessions are completely transient, storing no session data on the server. The WebEx Network mediates each Remote Access session, with each party (Technical Support Representative/remote machine) initiating an OUTBOUND call from their respective networks. No inbound connections are initiated. In addition, the host computer logs each Remote Access session. Once the remote user logs onto the host machine, the IP address of the host machine is never revealed to the user.



Getting Familiar with Remote Access Security Features

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 maintains 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. WebEx employs biometric security devices to further control physical access.

Strong Encryption

WebEx never sends clear text data during a Remote Access session. WebEx uses a proprietary data format to transmit data to and from clients to WebEx servers. For maximum security, Remote Access may be configured to encrypt all data using 128-bit Secure Sockets Layer (SSL) encryption, the leading Internet standard for securing sensitive data communications, to deter third parties from accessing this data during transit.

Firewall Compatibility

While establishing a Remote Access session, the WebEx client communicates with the conferencing server to establish a reliable and secure connection. In the process of establishing the connection, the WebEx client first attempts to connect using TCP (port 1270). If this port is blocked by a firewall, the WebEx client will then tunnel WebEx communications using HTTP (port 80). Optionally, you may purchase and use SSL, which routes the traffic over port 443. Initiating communication between the thin client and the WebEx servers in this manner eliminates the need to reconfigure firewalls, and complies with corporate security policies that guard against the opening of firewall ports.

Session data between machines is switched--never persistently stored — ensuring a high level of security.



Companies have the option of setting up dual authentication, with phone authentication providing a second level of security

Application-Level Access

Remote Access provides both application-level and desktop-level access. TSRs may use Remote Access to view/share specific software applications on a remote machine. Granting access to specific applications, rather than general access to desktop and network resources, provides a higher level of security. Competing solutions provide desktop level access only.

No IP Address Revealed

The TSR does not need to know the IP address of the remote machine in order to initiate a Remote Access session.

IP Address Access Controls

Administrators may limit remote machine access to those users with an accepted IP address. Administrators may specify up to three IP address ranges.

User Profile Access Controls

To initiate a Remote Access session, each TSR must provide a valid user-name and password to log in to the WebEx network. This prevents unauthorized persons from using Remote Access. In addition, Administrators may configure TSR user profiles to limit access to specific machines. The TSR may have access to whole groups of computers or to specific machines.

TSR Support Session Authentication

The TSR must know the access code of the remote computer they are accessing. Administrators may assign access codes for groups of computers or individual machines.

TSR Phone Authentication

Phone authentication provides a unique dual authentication option for an additional layer of security. When a TSR attempts to access a remote computer, the WebEx server dials out to the TSR's telephone number. In order to obtain access to the remote computer, the TSR must use the telephone keypad and enter the correct access code.



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 Support Center, 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.

Session Logging

Remote Access can maintain an event log that tracks all activity on an installed Remote Access agent. This log may be stored locally on the remote machine or accessed via the administration page. The session log includes availability time, access time and duration, and user name.

Session Recording

Remote users may record sessions automatically or on-demand . Recorded sessions, which capture all actions taken on the remote machine, can be stored on the remote user's local machine or on a network drive, as specified by the administrator.

Inactivity Timeout

Remote Access automatically terminates a session after a specified period of inactivity.

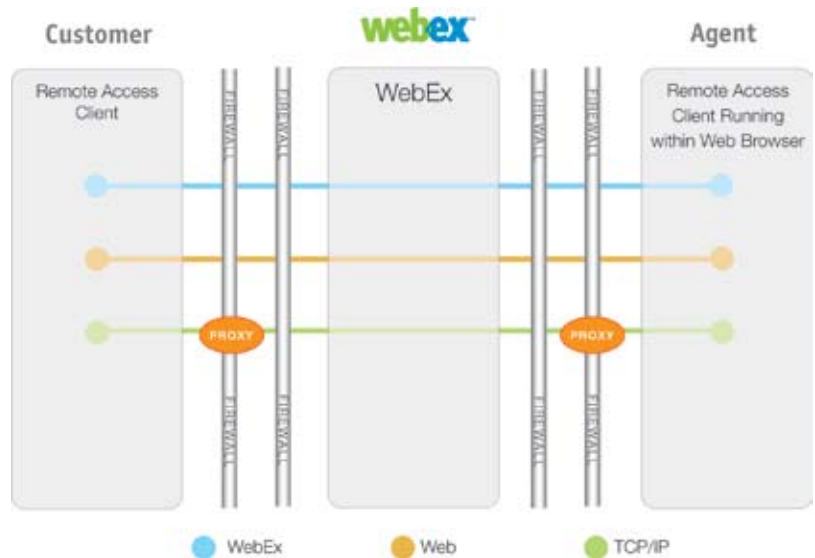


Each WebEx session has a unique set of session parameters that are generated by the MediaTone Meeting Switch. Each authenticated Attendee must have access to these session parameters in conjunction with the unique session cookie in order to successfully join the WebEx session.

Understanding Remote Access Network Security

Remote Access sessions provide only a logical connection between the two PCs via the WebEx network; there is no direct network connection between the two computers. The logical connection is fixed—there's no way to exit and connect to something else—and allows only application functions to be performed (no way to do general purpose tasks outside of what Remote Access allows).

The following diagram illustrates the layering of the physical TCP/IP connection and the higher-level, logical connections.



WebEx Remote Access Connection Layers

A Remote Access connection comprises several superimposed layers. The lowest layer, TCP/IP, enables general data communication and underlies all communications. Above this is the web layer, which provides the logical connection from a web browser to a web server. At the top is the WebEx layer, which provides a direct, end-to-end connection between the agent and host computer.



Each layer serves a different purpose and has different capabilities. While the lowest level provides arbitrary data communications, higher layers are more specific and less flexible. As each layer is established, the network connection becomes further constrained by the limitations of each layer.

The layers can be characterized by connection flexibility, protocols used, and capabilities allowed. The following table summarizes each layer.

Layer	Connection Flexibility	Protocols	Capabilities Allowed	Scope and Security
Network	Can be used to create arbitrary connections between network components subject to limits imposed by network security (e.g. firewalls).	Used TCP/IP	Arbitrary capabilities as defined by the application creating the connection.	Although TCP/IP underlies all communications, it is used directly by the web browser only to initiate a connection to a web server. In many cases, this will be a connection to an internal proxy server. No other connections are initiated outside of the web connection, allowing no opportunities for others to control the connection.
Web	Can be used only to establish a connection between a web browser and a web server. Connection must be initiated by the web browser and made OUTBOUND to the web server.	HTTP, SSL	HTTP allows a rich data stream to implement a wide variety of application-specific capabilities.	The Web layer provides a secure connection between the web browser and the web server, allowing no other use of the connection. Once established, the endpoints are fixed. Spoofing would require compromising components within the company or WebEx.
WebEx	No flexibility at all. Endpoints are fixed between the WebEx Remote Access server and the Web browser plug-in.	Proprietary protocols specific to WebEx Remote Access.	Capabilities are defined explicitly by the WebEx Remote Access server and the Remote Access agent/client running in the web browser. No other capabilities allowed.	Provides Remote Access remote support functionality. May use only application-specific functions since WebEx components are running on each end of the connection. Compromise would require taking over both the client and WebEx components within a secure connection.



Security Concerns FAQ

Can unauthorized third parties gain access to a customer's network via the Remote Access agent?

No. To join a Remote Access session an unauthorized third party would need to:

- Establish an account on the authorized site to access the specific machine.
- Come from an accepted IP address.
- Acquire authorized web or phone access codes.

Can unauthorized third parties gain access to network resources from the PC?

No. The third party would have to take over the Remote Access session. This is not feasible, requiring the third party to break into the TCP/IP connection, the SSL encryption (providing the site has SSL), the HTTP session, and the Remote Access application session—simultaneously and instantaneously.

The risk of providing access to a remote support agent is essentially the same as that for a support agent on site. The lack of physical access may actually make remote access more secure since the Remote Access logical connection eliminates risks from accidental disclosure of unrelated information, contamination, or accidental damage.

Can confidential data be intercepted on the network?

All Remote Access communications can be encrypted using 128-bit SSL, making it unfeasible to decrypt the data stream. In addition, any third party trying to intercept data would need access to the specific network segments containing the SMARTtech session data.

Can viruses be transmitted to a customer's PC?

Only if infected files were explicitly transferred to the customer PC by an agent. Because Remote Access uses a logical connection, there's no means within Remote Access session to transmit a virus.



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.

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

europe@webex.com

United Kingdom

Tel: 0800.389.9772

europe@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

