

WEB VISUALS

Security Overview Introduction

Online meetings—sharing ideas and information over the Internet—have become a vital part of today's business environment. Yet behind the growing use of web conferencing solutions is a justifiable concern about data security.

We understand your need to communicate remotely while maintaining your strict security standards. Web Visuals, our collaborative audio, web and desktop video conferencing service, addresses that need through the next-generation SwitchTower® multimedia network. The SwitchTower network provides an unparalleled remote meeting experience within a completely secure environment. By offering tight conferencing security in a fully integrated platform and uptime of 99.9%, we believe that your enterprise should have it all.

This document describes how Web Visuals operates over the SwitchTower network to deliver optimal security, while giving you the control to make the choices that best fit your company's data protection needs.

Flexible Options for Total Security

With multiple layers of encryption and in-depth access control, Web Visuals provides an advanced level of security unavailable in other web conferencing solutions. In addition, Web Visuals provides the flexibility and control to determine the level of security required on a meeting-by-meeting basis.

Web Visuals' Encryption Architecture

When we designed our data encryption architecture for the SwitchTower network, we had the future in mind. As more companies come to rely upon online meeting technology in order to conduct their day-to-day affairs, we anticipate that system administrators will require a web conferencing solution that offers flexible security settings tailored to their specific corporate security policies.

In addition, trends indicate that security concerns will prompt some companies to bring components of their conferencing solution in-house. The SwitchTower network was designed to be flexible on both fronts. This next-generation environment calls for a data encryption scheme that supports multiple hops, robust server configurations and the ability to encrypt different data types.

The SwitchTower network security architecture is modeled after the PGP scheme, which was a ground-breaking security method that is now a standard for corporate email encryption. Like email, web conferencing presents a scenario where data can be passed across many connections with an unknown transmission route. Like PGP, we developed a scalable, automatic and self-managing method of protecting your data as it moves across company networks, the SwitchTower network and the Internet. The SwitchTower network employs high-performance encryption algorithms that encrypt the data from its origination to its final endpoint, without being decrypted and re-encrypted at multiple exchange points. The result is a highly sophisticated end-to-end 128-bit encryption scheme that guarantees your data is protected from the time it is sent out from the meeting moderator to the time it reaches the meeting participants.

An additional feature that sets Web Visuals security apart is the level of choice it offers you to encrypt differing data types over a single socket. The benefit is the ability to maximize throughput performance by encrypting only the data that your company feels is sensitive. For example, if the documents you are sharing within your meeting are highly sensitive but the video is not, then you can choose to encrypt the Document Viewing feature but not the video transmission. Traditional methods of encryption would involve securing multiple sockets, which could affect speed and performance.

In developing this security architecture, we also leveraged industry-standard encryption components.

Secure Socket Layer (SSL)

We use industry standard Secure Socket Layer (SSL) to protect all web pages displayed within Web Visuals. These pages are primarily responsible for the pre-meeting and post-meeting functions specific to moderators, such as account provisioning, login and reports. Data collected or displayed on these web pages is protected through SSL server authentication, used to allow the end user to verify the server's identity. SSL also provides for encryption over the entire socket connection in order to detect any attempt at tampering with or observing data in transit. Finally, SSL helps ensure data security between the client application and Web Visuals servers.

Public Key Encryption (PKE)

In order for a secure connection to be established, Web Visuals utilizes Public Key Encryption (PKE) in a sophisticated form of data key exchange. PKE is used in the negotiation that ultimately determines the unique key that will be used between the sender and the server that will receive and decrypt the data.

In summary, Web Visuals' encryption architecture, powered by the SwitchTower network, offers customers the highest standards of data security, scalability and choice, all while leveraging industry-standard protocols. You are assured that the integrity of your company's data is protected both in standard ASP and on-premise deployments.

Access control choices

Web Visuals also gives you numerous methods to restrict and secure access to online meetings. This flexibility gives you complete control over all aspects of the conference while easily determining the appropriate level of security needed.

Each moderator is assigned a unique conference ID and PIN, which is required when initiating either a web or audio conference. As an added layer of security, you can create a security passcode unique to each conference.

Because encryption can affect conference performance, Web Visuals puts the decision about what to encrypt in your hands to determine what security level is appropriate for a particular conference. You can individually specify whether to encrypt features such as Document Viewing, Application and Browser Sharing, Participant Information, Chat and Video. To alter security settings, you simply click on the Security tab within your profile and select which features to encrypt. These selections can be changed at any time.

The following access control settings give the conference moderator additional security options:

- Conference lock – Ensure that no other participants enter the conference, including the conference operator, unless requested.
- Entry/exit announcements – Hear a tone or participants' names as they enter or leave the call.
- Participant list – See both participants' names and Automatic Number Identifications (ANI), commonly known as Caller ID, to verify identities and provide a participant count.
- Dial-out to participants – Dial-out to participants via the telephone or the web interface to verify the identity of the people in your meeting.
- Security passcodes – Designate security passcodes for any web or audio conference, which are then required in order for participants to access both portions of the conference.
- Conference operators – Request a public or private conference operator to answer additional questions about the conference participants over the telephone or on the web.
- Post-conference reports – Receive detailed reports that list the participants in your event.

As a result of this comprehensive access control, only authorized users can access Web Visuals conferences and shared data, and moderators can choose which control features to activate on a case-by-case basis.

Conclusion

The security of your data is the top priority. With comprehensive measures implemented at multiple levels within each conference, you can be confident your proprietary information is secure from unauthorized access at all times. Together, Web Visuals and the SwitchTower network ensure that you can have it all: secure, reliable web, audio and video conferencing, high performance and the control to tailor your entire meeting experience to meet your remote communication needs.