BroadData Unified Meeting

Security Whitepaper v4.2

Introduction

As organizations unlock the true potential of meeting over the Web as an alternative to costly and time-consuming travel, they do so in the face of great political and economic change.

All organizations using web and audio conferencing need to be confident that their presentations and meetings are protected. Whether meeting internally or with trusted external parties, it is important for meeting participants to be able to collaborate and share sensitive corporate information freely yet securely, within the confines of strict firewall protection.

With these goals in mind, we developed the Unified Meeting service to be secure by design, providing users with high-level security throughout all phases of conferencing, presentation storage, delivery and collaboration. Security is applied to Unified Meeting in four ways, through:

- Access Security
- Session Management
- Content Security
- Secure Application Design

This paper describes how effective security controls to protect organizations using the Unified Meeting. It includes discussions of how the Unified Meeting provides standard security protocols at the account and presentation levels, additional security options such as Secure Sockets Layer (SSL) 128-bit encryption, and firewall transparency.

Main Benefits

- Moderators and presenters install a Unified Meeting application that can be deployed organization-wide via MSI. The MSI file can be evaluated by an organization's system administrators and used with any configuration management system. Using the MSI, the Unified Meeting can be remotely installed on users' desktops within the controlled environment of the organization.

- Participants have the option of installing the application or using a secure client that is 100% browser based.

- All Unified Meeting features are firewall transparent, meaning that the system adapts to the security policies of firewalls for which regular web browsing is enabled. The Unified Meeting does not try to circumvent firewall security policies.

- Unified Meeting uses HTTP on port 80 or, if SSL is enabled, port 443. If a preferred port is not open, it will automatically fail over to the next one specified as in the

examples below.

+ Archives that are accessed using SSL will first attempt to use UDP over port 1755, then TCP over port 1755, then HTTP over port 80 or port 443.

+ Archives that are accessed without using SSL will first attempt to use TCP over port 1755, then TCP over port 80.

Access Security

The Unified Meeting uses industry-standard security protocols at the account and presentation level.

ACCESS SECURITY FEATURES

Leader PIN and Password

Every account holder is assigned a User Login and a Password. You need it to modify the account, upload presentations, and schedule or initiate meetings. The User Login and Password should be kept confidential.

Consecutive attempts to enter an invalid User Login or Password while trying to access portions of a meeting will result in a lock on the account.

Moderator Dial-Out

The moderator can dial out to participants instead of having them dial in to the meeting. This allows moderators to validate the participant and control the dissemination of meeting numbers and passwords.

Web Room Password

When inviting participants to a presentation or meeting, you can specify a password (up to 25 alphanumeric characters) for the web portion of the meeting, so only invited people can attend. When participants attempt to join your meeting, they log in with your meeting number and prove their identity by entering the web room password.

Locking the Door

Moderators may “lock the door” to a meeting. Participants trying to enter the audio and/or web portion of a meeting go into a virtual waiting room where they wait to be greeted and admitted by the moderator. The moderator can admit participants in the waiting room via the telephone keypad (DTMF command) or the web interface.

Dismissing Participants

A moderator can quickly dismiss an individual or all participants from a Unified Meeting session. When a participant is dismissed, that person is dismissed from both the audio and web portions of the meeting.

Session Management

SESSION MANAGEMENT FEATURES

Session Timeout
Conference Manager sessions time-out after 30 minutes of inactivity. After 30 minutes, the account is logged out from the Conference Manager, but this action does not affect meetings in progress.

End of Meeting
When a moderator ends a meeting, participants are automatically dismissed from the web portion of the meeting and the moderator can optionally choose to dismiss audio participants from the voice portion of the conference.

Randomly Generated Session Management Values
The Unified Meeting uses a randomly generated token, chosen from 42 billion possible combinations and stored as a session (non-persistent) cookie, to identify a logged-in account holder. It is needed to authenticate your credentials with the backend servers. When the Conference Manager session is terminated, both the cookie and the token disappear. Participants require the same token on a session cookie to access a meeting.

Browser Cache
The Unified Meeting does not clean a participant's browser cache of presentation slides (DHTML and GIF images) that were accessed during the meeting. Since presentations can easily be captured using screenshots (Alt-PrintScreen key) and other techniques, clearing the cache is not a useful precaution. No other meeting information is available after the session is terminated.

Deleting Presentations
Account holders are in full control of presentation content uploaded to Unified Meeting. Presentations can only be viewed during a meeting hosted by the account owner, or as part of an archived meeting made available for viewing by the account owner. Presentations and archived meetings can be removed from Unified Meeting at any time. Once deleted by the account holder, presentations are impossible to "undelete." A 7-pass magnetic overwrite obliterates all traces of the presentation from Unified Meeting servers.

For privacy reasons, no backup copies of presentation content are ever made. But real-time replication ensures presentations are available in the event one of the servers suffers an outage.

Content Security

The Unified Meeting allows organizations to go beyond access security and offers multiple levels of content security that are designed to suit the needs of the organization.

CONTENT SECURITY FEATURES

SSL Encryption
We offer 128-bit Secure Sockets Layer (SSL) encryption for all presentation content and publishing, logins and password information, and application sharing. This option provides the same level of security used by online financial institutions.
You need the same session management token for reaching a meeting as you would to access any content from our servers.

Publisher
The publisher is not a web server. It is a basic server that only knows how to receive PowerPoint™ files and convert them into DHTML files. Because it lacks the functionality of a web server, it does not have the same vulnerabilities that a web server does.

Slide Access
Presentation slides are stored on a standalone filer that is not publicly addressable. Even if you have the URL of the slide, you cannot use that to view the slide on the filer. Only our content servers can access presentations through an ISAPI filter. These content servers also act as a gateway between the filer and the Internet.

Database
Unified Meeting databases are not publicly addressable. Only machines within its data center with IP addresses that are on an access list can reach them. Authentication for this data is enabled on the table level. That means someone without the proper credentials cannot query against the database, even if they have gained access to the machine.

Secure Application Design

SECURE APPLICATION DESIGN FEATURES

Operating Systems
The Unified Meeting is based on standard web server technology (Microsoft IIS and FreeBSD Apache servers) and proprietary servers developed from the ground up. They are built specifically to meet the demands of online conferencing. All servers are locked down using best practices provided by Microsoft or FreeBSD, as well as proprietary security measures.

Testing Fields and Processes
All user input fields are checked for validation and length restrictions. All processes are extensively tested before being put into production.

Security Event Logging and Archiving
Security logs are recorded and archived for all components.

System Development Life Cycle (SDLC)

Security is designed and applied from the ground up and throughout the development and product life cycle.

Change Management
Implementation and rollback plans are mapped out in detail before any changes are made. Releases follow a formalized product release cycle and are thoroughly tested on pre-production servers to ensure that upgrades do not affect functionality or meeting data.

Web Specific Application Standards

ENCRYPTION

By design, no confidential information is available in either URL or HTTP headers. Using SSL, all confidential customer information is sent fully encrypted.

World-class Infrastructure

The Unified Meeting offers a distributed architecture where several geographically dispersed and load balanced servers allow for managing content, sharing applications, and controlling codes. This enables Unified Meeting to scale beyond single server systems.

Our commitment to reliability and security practices are further enhanced by the use of Tier 1 Internet Data Center (IDC) service providers with co-location agreements throughout the world. IDC partners are certified according to ISO 17799 standards and operate state-of-the-art facilities offering these features.

- 24/7 security-controlled access (guards, cameras, motion sensors, etc.)
- 100% guarantee of uninterrupted power supply via the N + 1 standard
- Raised floors
- Line sensor water detection system
- HVAC temperature-control systems with separate cooling zones
- Seismically braced racks
- Redundant subsystems (fiber cables, power supply)
- VESDA smoke detection and FM-200 fire suppression systems

THIRD PARTY OPERATIONAL CONTROL SECURITY STANDARDS

Administrative Procedures
Various Tier 1 IDC service providers host the Internet data centers. Companies such as COLT Telecommunications, Savvis Communications, and SingTel provide the physical environment necessary to keep our servers up and running at all times
Within these facilities, we can deliver the highest levels of reliability through a number of redundant systems, such as multiple fiber trunks coming into each IDC from multiple sources, fully redundant power on the premises, and multiple backup generators. There is also around-the-clock systems management with onsite personnel trained in the areas of networking, Internet, and systems management. The result is a physical and technical environment affording customers the reliability and security that they need.

Data Backup

We have a two-tier backup program, including real time redundant storage of non-presentation related information through its international server architecture, and daily physical tape backups of all conference reports and conference component information.

Segregating Backups
The real time replication of all conference data (except presentations) is automatically segregated so that no two customers can have their data intermixed.

Disaster Contingency & Business Resumption Plans

We embody a culture of security and reliability that manifests itself in resilience procedures that account for even the most exceptional disruptions.

DISASTER CONTINGENCY PLANS

Monitoring & Maintenance
We provides constant system monitoring, with random testing of pagers and alert procedures for response times. There are also regular capacity reporting and planning plus preventative maintenance programs
Every quarter, full system failures are simulated to test recovery processes.

OFFSITE BACKUP STORAGE

The Unified Meeting infrastructure is replicated through multiple locations, and key data is continuously replicated between separate regions. There is an independent, off-line back-up infrastructure that can be made available in the unlikely case of a multi-location failure.

COMMUNICATIONS REDUNDANCY

All Unified Meeting communications capacities have guaranteed redundancy and no single point of failure. This includes bridging facilities in 20 countries. In the event of a service-affecting incident, pre-defined and well-rehearsed procedures will redirect incoming calls to alternate bridges.

WARM/HOT SITES

The Unified Meeting employs a multi-redundant site architecture that guarantees the capability of switching from a failed data center to another in case of disaster. If a Unified Meeting conference server experiences failure, the meeting can be automatically restarted and the system will automatically relocate to a different server and/or data center.

BUSINESS RESUMPTION PLANS

All critical customer transactions benefit from existing backup, redundancy, and recovery programs. On request, we can dedicate parts of the infrastructure to specific customer needs.

REDUNDANCY AND FAIL-OVER PROCEDURES

All Unified Meeting servers and communications lines are redundant and replicated throughout its multi-site international infrastructure. In case of localized failure, the Unified Meeting will re-route new meetings to another data center.

Internet Infrastructure Security Standards

FIREWALL COMPATIBILITY

The Unified Meeting is a firewall-friendly program but will not function correctly if a client-side firewall blocks access to IP addresses or filters JavaScript.
Unified Meeting is designed to be compatible with any firewall/proxy configurations that allow users to browse the web using HTTP over port 80.

Note: Unified Meeting only requires outbound connections on port 80. Inbound connections are not required and never attempted. Please see the Main Benefits section for more information on the usage of ports in the Unified Meeting.

HOST/NETWORK INTRUSION DETECTION SYSTEMS COMPATIBILITY

Unified Meeting uses industry standard tools for host/network monitoring, as well as proprietary controls for improved intrusion detection. At the meeting level, all connections to the Unified Meeting are identified and listed in the moderator interface, and the moderator always has power to disconnect any unauthorized connection, as well as the ability to lock the conference to limit further access.

STANDARDS FOR 3RD PARTY HOSTED INTERNET INFRASTRUCTURE APPLICATIONS OR SERVICES

Firewalls
All Unified Meeting servers are protected by firewalls and carefully monitored for intrusion.

Real-time Alarms
All Unified Meeting servers and devices are capable of raising real-time alarms in the case of failure or intrusion detection. Network Operations Centers are staffed at all hours to respond to alarms.

Methods for Security Event Logging and Archiving by Component
Unified Meeting monitoring tools produce continuous logs of all transactions/events, which are permanently archived.

Ongoing Third Party Certification Programs
Security assessment of the production network and infrastructure have been conducted by a qualified third party and certification has been received to confirm that the production network supporting the Unified Meeting platform is free of all known material network security vulnerabilities.