Genesys Conferencing

Genesys Meeting Center

Security

Whitepaper

April 2002

Contents

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, Genesys Conferencing developed the Genesys Meeting Center to be secure by design, providing users with high-level security throughout all phases of conferencing, presentation storage, delivery and collaboration.

Genesys applies security to the Meeting Center in three ways, through:

- Access security,
- Network security, and
- Content security.

This paper describes how Genesys Conferencing ensures effective content and network security controls to protect organizations using the Genesys Meeting Center.

It includes discussions of: how the Genesys Meeting Center 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.

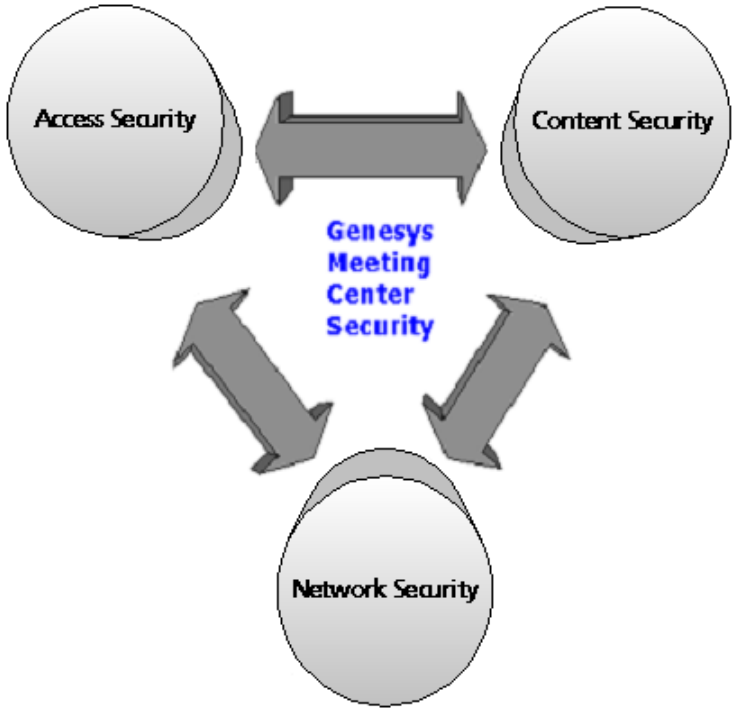

Figure 1 Genesys Meeting Center Security overview

Main Benefits

- Participants are not required to install anything on their desktops to access the Genesys Meeting Center, which is key to ensuring there is no security risk for an organization given the recent rash of virus attacks.
- All Genesys Meeting Center features are firewall transparent, meaning that it adapts to the security of any firewall for which regular web browsing is enabled.
- The new application sharing engine uses native HTTP for greater efficiency and ability to work with a greater number of firewall/proxy server configurations. It natively communicates through Port 80 using the HTTP protocol, no longer needing to access the Application Sharing Server through Port 443, alleviating any security concerns about opening another port in the firewall.

Access Security

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

Access Security Features

PINs

Every account holder is assigned a PIN number, required to modify the account, upload presentations, and schedule or give conferences. The PIN is unique and should be kept confidential.

If the PIN is forgotten, a request can be made to have it emailed by the Genesys Meeting Center. This option is available to account holders during login.

Meeting Password

When inviting viewers to a presentation or meeting, you can specify a password for the meeting so only invited people can attend. When viewers arrive at your presentation, they log in with your meeting number and prove their identify by entering the meeting password.

Locking the Door

Moderators may "Lock the Door" to the meeting – in other words, close the meeting. Participants trying to enter both the audio and web portion of a meeting go into a virtual waiting room to wait to be greeted and admitted by the moderator. The moderator always has a list of everyone in the room (both audio and/or the web meeting).

Dismissing Participants

A moderator can quickly dismiss individual or all participants from a Genesys Meeting Center meeting – both web and audio.

Notification Tones

In an audio conference, a notification tone informs the moderator of the arrival of new participants. When the door of the meeting room is open, the arrival of a new participant is announced to all by a double beep. If the door is closed, the arrival of a new participant is announced to the moderator only, by a triple beep. Newcomers wait in the waiting room on hold, with music in the background until the moderator lets them in.

Session Management

Session Management Features

Session Timeout

Sessions are set to timeout after one hour. As session management is used to monitor ongoing meetings, this was determined as the ideal time period.

Session End Message

When a moderator terminates a session, participants receive a static banner messages asking them to exit the meeting.

Randomly Generated Session Management Values

The Genesys Meeting Center uses a non-persistent, randomly generated IIS cookie to identify participation in a meeting. Only session moderators need to accept the cookie. All participants are also assigned a randomly generated token as representation in the meeting. The token is a random number between 1- 42 billion. When the session is terminated, both the cookie and the token disappear.

Browser Cache

The Genesys Meeting Center currently does not clean the browser cache of presentation screens (DHTML and GIF images) that were accessed during the meeting. As all presentations may be captured through screenshots by participants, we do not consider clearing the cache to be useful. If presentations are delivered via SSL, browsers do not cache the information by default. No other meeting information is available after the session is terminated.

Security of HTTP Posts and URL Access

HTTP posts and URL accesses do not contain any confidential information.

Transaction Rollback

Since moderators control all content, transactions such as deleting presentations are permanent. As there is content backup, deleted information may be recovered by Genesys technicians from physical tape backups upon request and for a fee.

Network Security

When discussing Web-based applications, it is important to consider the three different ways they can be accessed:

- Plug-ins,
- Signed applets, and
- Unsigned applets.

The Genesys Meeting Center ensures an organization's security is not compromised by using unsigned java applets, known as "sandboxed applets". Unsigned applets do not request access to file systems, the Microsoft Windows registry or any part of the computer's operating system.

For more information, see Table1: Java Applet and Plug-in Overview.

Table 1: Java Applet and Plug-in Overview

	Java Applet	Plug-in
Description	Part of a web page. Small, safe and considered simple to install. **Key benefit:** Java applets are controlled by the browser being used, preventing damage to computers.	A software module that adds a specific feature or service to an organization's system. For example, for Netscape Navigator plug-ins enable it to display different types of audio or video messages. Plug-ins can be quite large. **Key benefit:** Plug-ins are downloaded once and remain installed on a computer without having to be downloaded every time the web application is accessed.
Unsigned	Unsigned Applets do not request access to file systems, the Windows registry or any part of the operating system.	N/A
Signed	Plug-ins, Active X controls and signed applets seek much higher levels of permission: can write files to the computer disk, modify files, communicate to other computers on the network and, if maliciously designed, can change and corrupt a computer's Windows registry or Windows setting (i.e. turn off security settings). High risk: For large organizations with users surfing the Web all day. Users can make bad decisions about what content to download, with an impact to themselves and their organizations.	

Genesys Conferencing
Unsigned Java Applets are used by the Genesys Meeting Center. In the industry, it is referred to as "the zero footprint application".

With the recent series of virus attacks that harmed many organizations, there is a growing trend in I/T departments to aggressively police and control the material that users within their organizations can download. Many do not allow any plug-ins to be installed.

With the Genesys Meeting Center, viewers require no plug-ins. At the end of a conference, viewer computers are exactly the way they were before the web conference. No software is left behind on their computers, since nothing is installed.

Moderator Plug-ins are Optional

Some of the more advanced features of the Genesys Meeting Center, such as Application Sharing, Microsoft Outlook Control, enhanced Web tours, and the Enhanced Uploader, contain plug-ins available as a convenience to moderators and presenters. With the exception of Application Sharing, they are not required in order to use the Genesys Meeting Center. They are also designed not to require any administrator access, i.e. system libraries and Windows/sys32 libraries.

Use of Native HTTP

The new application sharing engine natively communicates through Port 80 using the HTTP protocol. There is no longer a need to access the Application Sharing Server through Port 443, alleviating any security concerns about opening another port in the firewall. This results in greater efficiency and ability to work with a greater number of firewall/proxy server configurations.

Network Security Standards

The Genesys web conferencing service is offered as an ASP solution, and does not need any onsite architecture. However, if the Genesys Meeting Center Tempest Security option is adopted, a 'content server' is installed either behind the corporate firewall or on the DMZ.

- Our onsite architecture is standard web server technology, and all monitoring and intrusion detection standards can be set on this server.
- The content server can be installed either on the DMZ, or behind the corporate firewall. Customer access service methods may be applied to the content server's access methods.

Content Security

The Genesys Meeting Center allows organizations to go beyond Access Security and offers multiple levels of Content Security depending on an organization's needs:

SSL Encryption

Genesys Conferencing offers Verisign 128-bit Secure Sockets Layer (SSL) encryption for all presentation content, login and password information. Industry-standard protocols, methods and processes are used for secure data transfer. This option provides the same level of security technology as used by financial institutions and is available for a low annual fee.

"Tempest" Security Solution

In addition to standard security protocols used at the account and presentation level, Genesys also offers an option to place the Publishing and Content Server at the customer's site, inside an organization's firewall and/or VPN. These client-managed servers store the organization's confidential presentation material, enabling the organization to make it as secure an environment as it requires.

This allows you to maintain all the benefits of Genesys' distributed architecture, while allowing you to manage your information in any manner you desire.

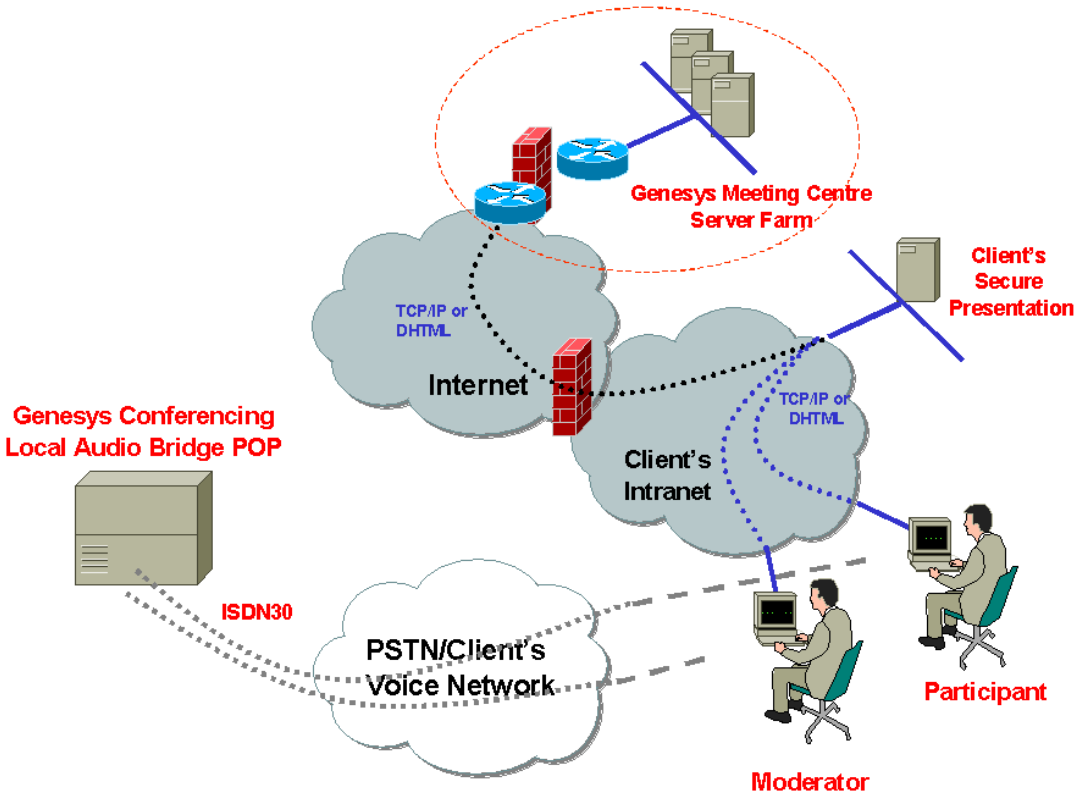

Figure 2 Tempest Security Solution: The Client Presentation remains secure behind the firewall as presentations are published to the servers, while leveraging all of the features of the Genesys Meeting Center's integrated Audio and Web conferencing.

Secure Application Design

Secure Application Design Features

Operating Systems

The Genesys Meeting Center is based on standard web server technology, Microsoft IIS and Free BSD Apache servers are used. All web servers are 'locked' using the latest standards provided by Microsoft or free BSD, as well as proprietary control procedures.

Testing Fields and Processes

All fields are checked for validation and length restrictions. All processes are extensively tested before being put into production.

Read-Only Format Used

All information transmitted is in read-only format.

Storage of Confidential Information

All confidential information is stored on a non-persistent IIS cookie that is unique to one session.

Security Event Logging and Archiving

Logs are recorded and archived for all components.

System Development Life Cycle (SDLC)

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

Web Specific Application Standards:

Executable CGI Programs

CGI scripts and executables are placed in non-standard directories to avoid ease of detection. In addition, all scripts are execute only, without read or write permissions.

Disabling Dynamic Directory Listings on Web Servers

All of the IIS web servers and Apache Free BSD are set with directory write access and directory listing turned off

Code Signing Method

Any code that is persistently downloaded to web browser clients is signed with Verisign certificates.

Encryption

By design, no confidential information is available in either URL or HTTP headers. All confidential information is encrypted via SSL.

World-class Infrastructure

The Genesys Meeting Center offers a distributed architecture where several servers can be used during a meeting. For example, separate servers are used for serving content, application sharing, and control codes. This enables the Genesys Meeting Center to scale beyond single server systems. (For a complete overview of our distributed architecture, please review the *Genesys Meeting Center Architecture Whitepaper*.)

Genesys' commitment to reliability and security practices are further enhanced by our use of World-class Data Center service providers with co-location agreements throughout the world. Our Data Center partners operate state of the art facilities offering:

- 24/7 top-security-controlled access (guards, cameras,
- motion sensors, etc.)
- 24/7 monitoring
- Raised floors
- HVAC temperature-control systems with separate cooling zones
- Seismically braced racks
- Redundant subsystems (fiber cables, power supply)
- State-of-the-art smoke detection and fire suppression systems

Third Party Operational Control Security Standards

Administrative Procedures

Exodus hosts Genesys Conferencing's Internet data centers. Exodus provides the physical environment necessary to keep our servers up and running 24 hours a day, 7 days a week. These world-class facilities are custom-designed with raised floors, HVAC temperature control systems with separate cooling zones, and seismically braced racks. They offer the widest range of physical security features, including state-of-the-art smoke detection and fire suppression systems, motion sensors, and 24x7 secured access, as well as video camera surveillance and security breach alarms.

Within these facilities, we are able to 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. We also have 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.

For more information please visit http://www.exodus.com/idc/index.html

Data Backup

We have a two-tier backup program, including real time redundant storage of all information through our 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 is automatically separated by our initial customer segregation.

Disaster Contingency and Business Resumption Plans

Genesys Conferencing has multiple levels of disaster recovery programs and testing. For content

servers on a client site (Genesys Meeting Center Tempest Security option), we provide instructions and 24x7 support for duplication, redundancy, load balancing, and eventual restoration for all infrastructure on the client side.

Disaster contingency plans

Offsite Backup Storage

The Genesys Meeting Center infrastructure is replicated through multiple locations, and we have an independent, off-line back-up infrastructure that can be made available in the unlikely case of a multi-location failure.

Communications Redundancy

All Genesys Meeting Center communications capacities are guaranteed redundancy by the Exodus Internet Data Centers

Warm/Hot Sites

The Genesys Meeting Center multiple redundant site architecture guarantees the capability of switching from a failed data center to another in case of an incident. If a Genesys Meeting Center conference server experiences failure, the meeting can be restarted and the system will automatically reallocate a different data center.

Disaster Contingency Plans

Genesys Conferencing provides 24x7 monitoring for systems, with random weekly testing of pagers and alert procedures for response times.

Every quarter, full system failures are simulated to test recovery process.

Business Resumption Plans

All critical customer transactions benefit from existing backup, redundancy, and recovery programs. On specific requests, we can dedicate specific architecture to specific transactions.

Redundancy and Fail-over Procedures

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

Internet Infrastructure Security Standards

Genesys Conferencing Internet Security Tools

Standards for hosted Internet infrastructure applications or services:

Firewall Compatibility

The Genesys Meeting Center is firewall friendly. The Genesys Meeting Center is not accessible if your firewall:

- Blocks access to our IP addresses, or
- Filters unsigned Java Applets.

When the Genesys Meeting Center filters Active X / or Netscape Navigator plugins, the moderator cannot access all Genesys Meeting Center features, including application sharing. However, basic slide presentations, webtours and surveys will continue to function. Participants are not affected by Active X/or Netscape Navigator plugin filters.

Our web conferencing service is built to work in all existing firewall environments, as the service works on the HTTP protocol, needing port 80 traffic.

Note:

The Genesys Meeting Center only requires outbound access to be provided and in no way requires any inbound connections to devices such as computers or disks.

Host/Network Intrusion Detection Systems Compatibility

The Genesys Meeting Center uses HP Openview and Netcool for host/network monitoring, as well as proprietary controls for improved intrusion detection systems. On the meeting level, all connections to the Genesys Meeting Center 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.

Redundancy and Fail-over Architecture

All architecture is redundant and real time replicated. Fail-over procedures will switch conferences from failed data centers to live data centers.

Standards for Third Party hosted Internet infrastructure applications or services

Firewall configuration and placement (DMZ, multi-layered firewalls).

The Genesys Meeting Center Tempest Security option, if adopted, offers the possibility to place 'presentation content' either inside your firewall, or on the DMS. All other Genesys Meeting Center infrastructure components are placed in our data centers which are accessed via the Internet.

Firewall type (e.g. IP filter, state-based).

The Genesys Meeting Center data centers use Cisco Pix firewalls.

TCP/IP addressing scheme and all routes for the hosted applications.

If the Tempest security option is chosen, the 'content server' can be configured to accept only internal IP addresses, or internal and external IP addresses. All other infrastructure is addresses via the Internet with external IP addresses.

Host /network intrusion detection systems

Exodus Data Centers have the industries highest standards of host/network intrusion detection systems. On top of the systems monitored and maintained by Exodus for our data centers, we also use HP Openview and Netcool, together with proprietary monitoring systems of the entire network. All firewalls and routers are monitored continuously.

Real-time alarms for high-risk event classes

HP Openview, Netcool and our own systems provide real-time alarms for all event classes.

Intrusion response team

Genesys Conferencing incident response teams are on call 24x7.

Methods for Security Event Logging and Archiving by Component.

All of our monitoring tools produce continuous logs of all transactions/events, which are permanently archived.

Standards and Implementations for Browser Encryption, Certificates and PKI.

All login, password and join conference transactions use SSL encryption (Verisign certificates). All presentation content can optionally be transmitted via SSL as well.

Ongoing Third Party Certification Programs.

Security audits and standards compliance certificates are pending.

Contact Us

Thank you for your interest in Genesys Meeting Center. We'd like to hear from you. And we're here to help.

Genesys Worldwide

Genesys Conferencing is the world's largest organization dedicated to virtual group communications. Established in 18 countries throughout North America, Europe and Asia Pacific, Genesys Conferencing offers a one-stop conferencing shop to over 17,000 customers across the globe.

For sales and technical support information, please go to the Genesys Conferencing website at: http://www.genesys.com/.