



# **inteliCall Meeting Center**

Version 3.5

## **Security White Paper**

**January 2006**

© 2004 - 2006 InteliCall Conferencing Inc. This is an InteliCall white paper. All rights reserved.

Trademarks: "InteliCall Meeting Center" is a trademark of InteliCall Incorporated. Other brands or products are the trademarks or registered trademarks of their respective holders and should be treated as such.

# Contents

---

<b>Introduction</b> .....	<b>1</b>
Main Benefits .....	1
<b>Access Security</b> .....	<b>3</b>
Access Security Features .....	3
PIN .....	3
Participant Identification.....	3
Web Room Password .....	3
Presenter Password.....	3
Locking the Door.....	3
Moderator Dial-Out .....	3
Dismissing Participants.....	4
Notification Tones .....	4
<b>Session Management</b> .....	<b>5</b>
Session Management Features .....	5
Session Timeout .....	5
End of Meeting.....	5
Randomly Generated Session Management Values.....	5
Browser Cache .....	5
Deleting Presentations.....	5
<b>Network Security</b> .....	<b>6</b>
Optional Moderator Plug-ins .....	7
Protocols .....	7
<b>Content Security</b> .....	<b>8</b>
Content Security Features .....	8
SSL Encryption .....	8
Publisher .....	8
Slide Access .....	8
Database.....	8
<b>Secure Application Design</b> .....	<b>9</b>
Secure Application Design Features.....	9
Operating Systems .....	9
Testing Fields and Processes.....	9
Security Event Logging and Archiving .....	9
System Development Life Cycle (SDLC).....	9
Change Management .....	9
Web Specific Application Standards .....	9
Code Signing Method .....	9
Encryption .....	9
<b>World-class Infrastructure</b> .....	<b>10</b>
Third Party Operational Control Security Standards.....	10
Administrative Procedures .....	10
Data Backup .....	10

Segregating Backups.....	10
Disaster Contingency & Business Resumption Plans .....	11
Disaster Contingency Plans .....	11
Communications Redundancy.....	11
Warm/Hot Sites.....	11
Business Resumption Plans .....	11
Redundancy and Fail-over Procedures.....	11
Internet Infrastructure Security Standards.....	12
Firewall Compatibility .....	12
Host/Network Intrusion Detection Systems Compatibility.....	12
Standards for 3 <sup>rd</sup> Party Hosted Internet Infrastructure Applications or Services ..	12
<b>Contact Us .....</b>	<b>13</b>
InteliCall Worldwide.....	13

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

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

- Access security
- Network security
- Content security

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

It includes discussions of how the IntelliCall 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.

## Main Benefits

Participants are not required to install anything on their desktops to access the IntelliCall Meeting Center, which dramatically reduces security risk and ensures universal accessibility.

Moderators and presenters may have to install ActiveX controls in order to use advanced features, such as application sharing or video broadcasting. All IntelliCall Meeting Center plugins are code signed by Entrust. This guarantees that the code was published by IntelliCall Conferencing and not tampered with. See <http://www.entrust.com> for more information on code signing.



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

IntelliCall Meeting Center uses HTTP on port 80 or, if SSL is enabled, port 443. Some of the Meeting Center's features will try to use TCP on port 443 instead, because it provides greater network efficiency while HTTP provides maximum firewall/proxy compatibility. If port 443 is unavailable, the IntelliCall Meeting Center will only use HTTP over port 80.

# Access Security

---

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

## Access Security Features

### **PIN**

Every account holder is assigned a Personal Identification Number (PIN). You need it to modify the account, upload presentations, and schedule or initiate meetings. The PIN should be kept confidential.

Five consecutive attempts to log in to a web meeting with an incorrect PIN (15 for audio) will lock the account. Only a IntelliCall Conferencing Customer Service Representative can reset a locked account.

### **Participant Identification**

Moderators may require their attendees to identify themselves upon entering a meeting. When attendees enter the participant ID, they announce their web presence to the moderator. Similarly, the moderator may request voice identification (roll call) before permitting entrance to the meeting.

### **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 arrive at your presentation, they log in with your meeting number and prove their identity by entering the web room password. This feature is also available for the audio portion, using a numeric PIN.

### **Presenter Password**

Presenters or participants to whom the moderator wishes to grant control of the meeting also need a password in order to assume control.

### **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.

### **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.

## **Dismissing Participants**

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

## **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 music hold, until the moderator lets them in. Even a help desk staff member who is assisting customers cannot enter a conference silently.

# Session Management

---

## Session Management Features

### Session Timeout

Conference Manager sessions time-out after one hour of inactivity. After an hour, the account is logged out. This measure does not affect meetings in progress.

### End of Meeting

When a moderator ends a meeting, participants are automatically dismissed from the web meeting and optionally dismissed from the audio conference.

### Randomly Generated Session Management Values

The IntelliCall Meeting Center 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. You need it 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 IntelliCall Meeting Center 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 IntelliCall Meeting Center. 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 IntelliCall Meeting Center 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 IntelliCall Meeting Center 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.

## Network Security

---

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

- Plug-ins

- Signed applets

- Unsigned applets

The IntelliCall Meeting Center uses unsigned Java applets, also known as “sandboxed applets.” They ensure that no access to a participant’s file system or Windows registry is possible.

With virus attacks as common as they are, there is a growing trend in IT 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 IntelliCall Meeting Center, participants require no plug-ins. At the end of a meeting, participant computers are left exactly the way they were before the web conference, with the exception of files in the browser cache.

## **Optional Moderator Plug-ins**

Some of the more advanced features of the IntelliCall Meeting Center, such as application sharing, Enterprise Contacts integration (With Outlook and Notes), Web Tours, and Enhanced Presentation Uploader, require plug-ins. These plug-ins are optional and all other IntelliCall Meeting Center features function fully with or without them. Locked down environments can install these components from a CD or an MSI package.

## **Protocols**

IntelliCall Meeting Center uses HTTP on port 80 or, if SSL is enabled, port 443. Some of the Meeting Center's features will try to use TCP on port 443 instead, because it provides greater network efficiency while HTTP provides maximum firewall/proxy compatibility. If port 443 is unavailable, the IntelliCall Meeting Center will only use HTTP over port 80.

# Content Security

---

The IntelliCall Meeting Center allows organizations to go beyond access security and offers multiple levels of content security depending on an organization's needs.

## Content Security Features

### SSL Encryption

IntelliCall Conferencing offers 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 IntelliCall servers.

### Publisher

The IntelliCall 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 IntelliCall content servers can access presentations through an ISAPI filter. These content servers also act as a gateway between the filer and the Internet.

### Database

IntelliCall Meeting Center 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 IntelliCall Meeting Center is based on standard web server technology (Microsoft IIS and FreeBSD Apache servers) and proprietary servers developed from the ground up by IntelliCall Conferencing. 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.

## Web Specific Application Standards

### Code Signing Method

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

### Encryption

By design, no confidential information is available in either URL or HTTP headers. All confidential information such as PINs or telephone numbers are encrypted via SSL

## World-class Infrastructure

---

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

IntelliCall' 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 of IntelliCall 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 IntelliCall Conferencing Internet data centers. Companies such as Cable & Wireless, Savvis Communications, and SingTel provide the physical environment necessary to keep IntelliCall servers up and running at all times

Within these facilities, IntelliCall 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

IntelliCall has 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**

InteliCall Conferencing embodies 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**

InteliCall Conferencing provides constant system monitoring, with random testing of pagers and alert procedures for response times. There are also regular capacity reporting and planning and preventative maintenance programs

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

#### **Offsite Backup Storage**

The InteliCall Meeting Center 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 InteliCall Meeting Center communications capacities have guaranteed redundancy and no single point of failure. This includes InteliCall-owned 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 InteliCall Meeting Center 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 InteliCall Meeting Center conference server experiences failure, the meeting can be 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, InteliCall can dedicate parts of the infrastructure to specific customer needs.

### **Redundancy and Fail-over Procedures**

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

another data center.

## **Internet Infrastructure Security Standards**

### **Firewall Compatibility**

The IntelliCall Meeting Center is a firewall-friendly program. However, it will not function correctly if a client-side firewall blocks access to IntelliCall IP addresses or filters unsigned Java Applets.

If the moderator's firewall filters ActiveX controls, the moderator cannot access all IntelliCall Meeting Center features, including application sharing. However, basic slide presentations, Web Tours, and surveys will continue to function. Participants are not affected by ActiveX filters.

IntelliCall Meeting Center is designed to be compatible with any firewall/proxy configurations that allow users to browse the web using HTTP over port 80.

**Note:** Like any web browser, IntelliCall Meeting Center only requires outbound connections on port 80. Inbound connections are not required and never attempted.

### **Host/Network Intrusion Detection Systems Compatibility**

IntelliCall Meeting Center 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 IntelliCall 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.

## **Standards for 3<sup>rd</sup> Party Hosted Internet Infrastructure Applications or Services**

### **Firewalls**

All IntelliCall Meeting Center servers are protected by firewalls and carefully monitored for intrusion.

### **Real-time Alarms**

All IntelliCall Meeting Center 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**

IntelliCall Meeting Center monitoring tools produce continuous logs of all transactions/events, which are permanently archived.

### **Ongoing Third Party Certification Programs**

Security audits and standards compliance certificates are pending.

## Contact Us

---

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

### **IntelliCall Worldwide**

IntelliCall Conferencing is one of the world's largest organization dedicated to virtual group communications. IntelliCall can serve the world's largest international customer base providing service in 20 countries throughout North America, Europe and Asia Pacific

To contact us, go to the IntelliCall Conferencing website at [www.intelliCall.net](http://www.intelliCall.net).