

*DigitalMeeting™*

*DigitalMeeting™* Web  
Security Overview  
February 2006

*DigitalMeeting™*  
Powered by **technilink**



## Table of Contents

|                                    |   |
|------------------------------------|---|
| Introduction.....                  | 3 |
| Dedication to Security .....       | 3 |
| System Overview.....               | 4 |
| User Control .....                 | 4 |
| Access Levels.....                 | 4 |
| Basic Level.....                   | 5 |
| Secure Level.....                  | 5 |
| Participant Management.....        | 5 |
| Disconnect.....                    | 5 |
| Lock Conference.....               | 5 |
| Attendee Monitoring.....           | 5 |
| Content Management .....           | 5 |
| Additional Security Features ..... | 6 |
| Encryption.....                    | 6 |
| Content Encryption.....            | 6 |
| HTTPS Protocol .....               | 6 |
| Switch Routing.....                | 7 |
| Physical Security .....            | 7 |
| Firewall.....                      | 7 |
| Application Directors .....        | 7 |
| Application Servers .....          | 7 |
| Data Storage.....                  | 8 |
| Increased Performance.....         | 8 |
| Content Management .....           | 8 |
| Content Control.....               | 8 |
| Conclusion.....                    | 8 |

# DigitalMeeting™

## Introduction

*DigitalMeeting* Web is technilink's easy-to-use web conferencing service that is fully integrated with *DigitalMeeting* audio conferencing. This low-cost application includes all the key features most commonly used in web conferencing applications and enables rich, collaborative sharing of applications and documents.

*DigitalMeeting* Web allows you to:

- \_ Manage your conference online using easy point and click conference commands
- \_ Show slide presentations and graphics to meeting participants
- \_ Designate multiple co-presenters in your meeting
- \_ Show your desktop to meeting participants
- \_ Show applications from your computer to meeting participants
- \_ Record a conference (audio only or include synchronized visuals)
- \_ Collaborate on documents in real time.
- \_ Receive instant feedback on a presentation.
- \_ Visit Web locations and show your visit to all attendees.
- \_ Chat with participants who express interest in your products or services

*DigitalMeeting* Web is designed to maximize productivity by integrating the convenience of a conference call with the benefits of an in-person meeting.

## Dedication to Security

Today's fast-paced marketplace requires organizations to open their networks to customers, suppliers, and business partners. This same openness, however, brings security risks that must be properly managed.

The frequency and sophistication of network attacks is growing with the use of automated hacking tools that can inflict serious damage in just a few hours. Left undetected or improperly corrected, vulnerabilities provide an open door for 99 percent of all network attacks. The consequences for anything less than a rigorous dedication to security are great. Outages caused by hackers and viruses cost businesses millions in actual revenue, and even more in lost reputation, negative brand impact, and diminished consumer confidence each year.

At technilink, we understand that keeping up with security is a full-time job for any organization. Software patches are released as new vulnerabilities are discovered, cyber crimes are detected, and virus definitions are updated. Computer hackers are continually probing networks and servers for any vulnerability to exploit. Monitoring for patterns in network traffic to detect suspicious activity requires around-the-clock dedication, expertise, and sophistication.

We feel a secure and reliable environment should be the number one priority of any conferencing service. *DigitalMeeting* Web is designed and developed with security as its cornerstone. From the 128 bit AES encryption and application directors, to our data storage, *DigitalMeeting* Web's architecture is developed to be secure at every level. We feel you should not have to worry about the integrity of your data as you transmit it over the internet nor should you have to worry about malicious attempts to intercept that data. Our dedication to a secure environment allows our users to conduct a worry free conference with their most trusted information.

**DigitalMeeting™**

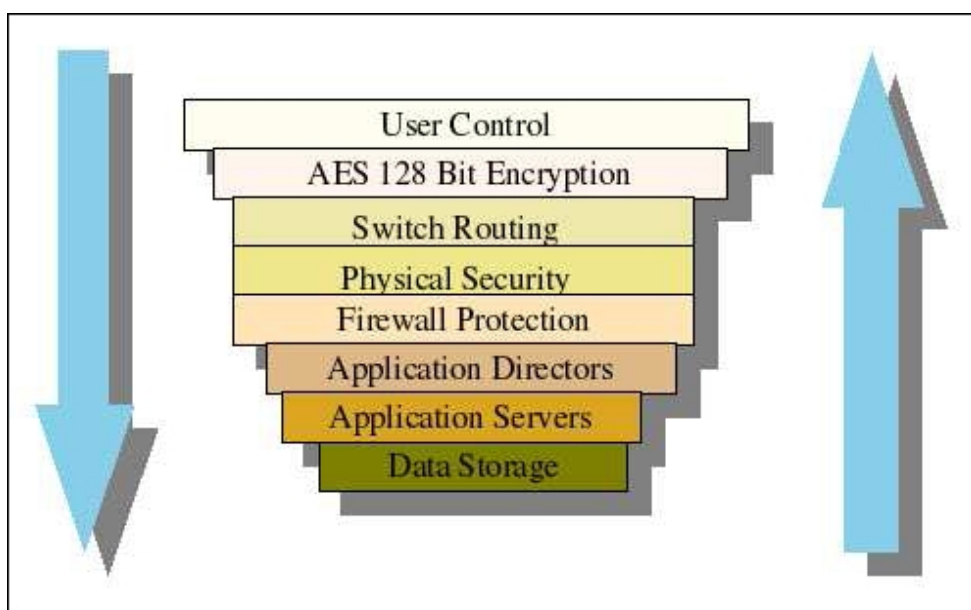
Powered by **technilink**



## System Overview

*DigitalMeeting* Web provides a hosted web and audio conferencing service designed to connect meeting hosts and participants in the easiest and most secure way possible. While the service strives to provide a simple and elegant solution for online meetings, at the same time it hides a vast amount of design and logic that constantly protects the users and their content as data passes between meeting users and servers.

*DigitalMeeting* Web has designed an eight-tiered structure to protect the security of your conference. Each tier provides an additional layer of security. Taken together all eight tiers combine to protect your conference from all levels of intrusion. Our eight tiered network is shown below and as you can see from the diagram it affects the information flow to and from the user's computer.



## User Control

The Chairperson (owner of the meeting or host) has several controls available to them to ensure the security of their conference. These controls allow the Chairperson to set access levels, disconnect participants, lock conferences, set view mode, and gather registration information. In addition to these in-conference security measures, administrators and IT departments can set global user options at an individual or company level.

## Access Levels

The *DigitalMeeting* Web service gives the Chairperson several custom levels of access depending on their security needs. Each level is completely controlled by the Chairperson and can be enabled or disabled on a per conference basis.

# DigitalMeeting™

## Basic Level

The basic level is the default level of security. At this level, all meeting participants with the proper access code and time can enter the conference. No additional authentication is required. This level of security is perfect for large meetings where there will be a multitude of attendees.

## Secure Level

When more security is needed, participants can be required to enter both an access code and an additional security code. The security code can be any alpha numeric code up to nine characters as defined by the Chairperson. For security and convenience, these security codes can be changed on a per conference basis.

## Participant Management

The *DigitalMeeting* Web service also allows meeting organizers to monitor and control their attendees. The moderator controls allow the host to see which participants are in the lobby (pre-conference) by their registration name and, if audio is connected, by their caller ID information. The controls also give the Chairperson a robust interface through which they can disconnect participants, lock the conference, and monitor attendees.

## Disconnect

This feature enables the Chairperson to selectively disconnect participants from their meeting. This allows the Chairperson to manage what participants see, such as when there is confidential material to be shown. The feature can also be used to disconnect disruptive or unauthorized attendees.

## Lock Conference

Locking the conference will prevent additional participants from entering. This is a useful feature when the Chairperson wants to share sensitive information at the beginning of the conference with a select few participants and wants to prevent early entrances. It can also be used when all attendees are present and the Chairperson wants to prevent unauthorized entry.

## Attendee Monitoring

The moderator controls list all web and audio attendees. The web attendees are listed by their registration information which is required of them to enter the conference. This information gives Name, Company, E-Mail and Phone Number information. The audio line will show originating phone number. By watching this list during conference, hosts can see who is entering and exiting their conference. They can also turn on name announcement which announces each attendee by name as they enter the conference.

## Content Management

Hosts retain complete control over their content at all times. All content is uploaded to secure servers before the meeting begins and then can be marked for deletion at the end of each conference or on an individual basis. Additionally, hosts control the view mode of participants at all times. Participants enter the conference in viewing only mode. It is at the host's discretion whether they want to promote specific attendees to higher levels of control. Hosts always retain the ability to demote participants as needed back to viewing only mode.

# DigitalMeeting™

## Additional Security Features

In addition to the security measures mentioned on the previous page, customers may request that technilink set restrictions on functions they deem too intrusive or sensitive for their employees to use. These options include:

### Disable slides

Users will not be able to upload or push slides. This option ensures that users cannot upload company information to the *DigitalMeeting* Web server.

### Delete slides on exit

Will delete any uploaded slides when a user exits the conference controls. This ensures any uploaded data is deleted as soon as a user closes *DigitalMeeting* Web at the end of a conference. Users will have to re-upload slides the next time they wish to present.

### Disable Chat

Chat feature will not be enabled; no transcript of chat messages will be recorded or sent to the meeting host.

### Disable application and desktop showing

Users will not be able to share individual applications or their desktop.

### Disable recording

Users will not be able to record the audio or visual portions of their conference.

### Disable remote control

Users will not be able to pass control of their application or desktop to another participant.

### Disable co-presenter

Users will not be able to promote participants to allow the participant to push slides or share their applications or desktop.

## Encryption

Beneath the user controlled security measures lay advanced encryption and data paths. The application uses these paths to communicate with the central service and therefore other meeting participants. Encryption is vital for many reasons. If even one of the meeting participants' networks has been compromised then unsecured data can be captured and stolen. Using very strong encryption ensures that data is not viewable even on hacked or compromised networks.

### Content Encryption

Before data is ever sent or received it is first protected using military grade AES 128 bit encryption, the highest level of the AES standard and certified by the NSA for classified and top secret level information. This level of encryption ensures that sent data is secure and only viewable by other members of the meeting who have proper authorization.

### HTTPS Protocol

All attendees initiate a Secure Sockets Layer (SSL) connection to the *DigitalMeeting* Web service using the HTTPS (HTTP Secure) protocol, which encrypts data sent over the connection. The SSL connections protect data transferred over http using encryption

## DigitalMeeting™

enabled by a server's SSL Certificate. An SSL Certificate contains a public key and a private key. A public key is used to encrypt information and a private key is used to decipher it. When a browser points to a secured domain, an SSL handshake authenticates the server and the client and establishes an encryption method and a unique session key. They can begin a secure session that guarantees message privacy and message integrity.

### Switch Routing

The meeting service has multiple data paths across many Internet providers allowing data to traverse along the shortest route and bypass downed routes and Internet connection failures. The meeting switches will only allow routable traffic for the meeting service through, rejecting 'spoofed' or forged addresses. This intelligent network allows for faster routes no matter where in the world meeting participants may be.

### Physical Security

The meeting service is hosted in a state-of-the-art ISO 9001:2000 certified data center. This data center is monitored and staffed 24/7/365 and uses multiple levels of security including video surveillance, software monitoring and alerts, network monitoring, physical access logging and reporting. The data center also operates on multiple city power grids, multiple battery systems, multiple diesel backup generators and has contracts with multiple diesel distributors in case of prolonged power outages. Physical access to the conferencing systems is restricted to only high level system individuals whose access is logged and reported by the data center staff.

### Firewall

All traffic coming or going through the meeting switch is filtered through the firewall layer. The firewall ensures that only authorized IP addresses and ports are allowed through. It also ensures that the application directors are the only publicly available servers that meeting participants can access. This protects the application servers and data network from direct outside access. The firewall layer also allows for dynamic protection against intrusion and service attacks while providing visible alerts and countermeasures for unauthorized access.

### Application Directors

Meeting participants never access any of the application servers, database or file servers directly. All traffic is received by the application directors that provide the proper links and maintain connections on behalf of the meeting users. This extra layer of protection will drop malformed requests from non-meeting participants and ensure only valid traffic is passed.

Application directors also provide intelligent traffic routing at the application layer with the ability to reroute requests from dead servers and distribute network and application load among the conferencing clusters. This ensures uninterrupted service when the meeting system loses an application server due to software, hardware, or network failure.

### Application Servers

Application servers verify the authentication validity of every request that they receive. The authorization keys required for access are time-based and expire after a short amount of

# DigitalMeeting™

inactivity or direct logout. Once a key has been invalidated it can no longer be used to access any part of the service. By using a combination of network layer encryption and application layer key-based authorization, the service is able to maintain both data protection and user identity. Keys are used to correlate a user's identity with a security level. These security levels dictate which commands users are allowed to invoke and what data they are allowed to retrieve or change.

## Data Storage

The data layer sits behind the application server layer and is not directly accessible by any meeting user. By using a separate layer, we are able to securely house your data and prevent unwanted intrusion or malicious attempts to access it. We are also able to increase performance and help you manage your content more efficiently and securely.

## Increased Performance

By uploading your data into the *DigitalMeeting* Web service, you are relying upon our servers to transmit that information to your participants. The results are increased performance and better stability. *DigitalMeeting* Web has dedicated content servers with very high bandwidth which deliver content rapidly to all meeting participants. Using our servers also prevents latency occurring on slower networks.

## Content Management

*DigitalMeeting* Web, at your discretion, allows your uploaded content to persist on our network after you log out. This enables different presenters to use the same presentation without having to upload it each time they start a conference. Not only does this save time, it also allows the content to reside in a secure area while not in use.

## Content Control

*DigitalMeeting* Web does not store any financial or personal data that an intruder could use. Critical data does not leave the central storage facilities by any means other than through the authorized system for playing and deleting recorded information and via secured backups to tape which are vaulted offsite. Additionally, recordings are not stored with any meta information that would allow a user to associate any of the millions of files the system contains with any usable information.

## Conclusion

Technilink has made your privacy and security our number one priority. We have instituted safe guards at every level of our product architecture. Whether it is your PowerPoint file, your proprietary application, or your desktop, the *DigitalMeeting* Web service will keep your information private. Our ongoing commitment also ensures that we are constantly assessing our security procedures and evaluating new technology in an effort to serve our customers better.

**DigitalMeeting™**

Powered by **technilink**

