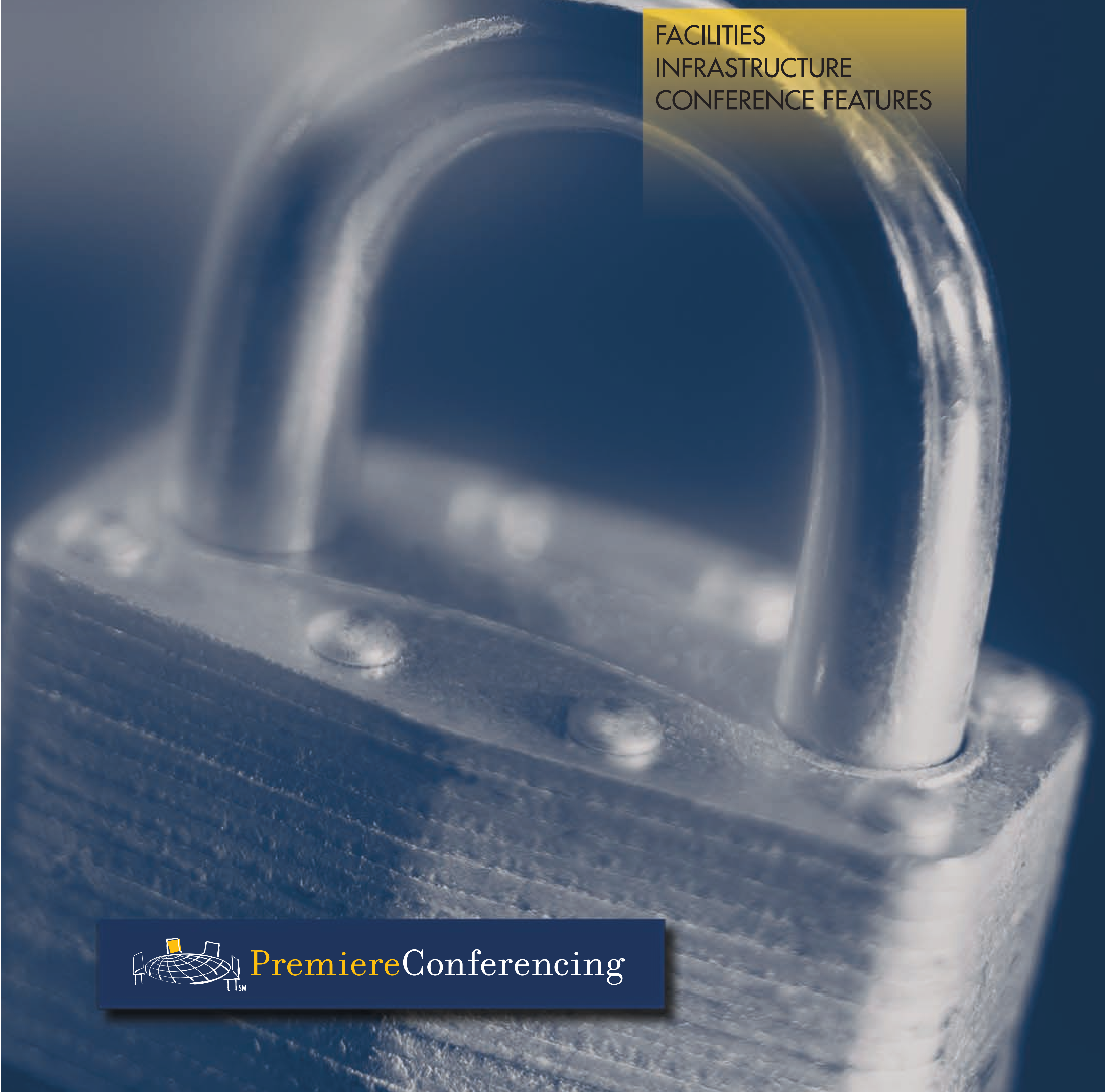
PREMIERE CONFERENCING

SECURITY

FACILITIES
INFRASTRUCTURE
CONFERENCE FEATURES



PremiereConferencing℠

PREMIERE CONFERENCING

SECURITY

- FACILITIES
- INFRASTRUCTURE
- CONFERENCE FEATURES

Premiere Conferencing: A Comprehensive Security Program

Why Choose Premiere Conferencing?
One word: Security.

At Premiere Conferencing, security is more than a word –- it is central to every aspect of the way Premiere conducts business. As host to more than 50 percent of the Fortune 500, Premiere leverages its 18 years of conferencing experience to provide solutions that help their clients conduct business communications safely and securely each day. Since 1984, Premiere has pioneered and set the standard for many of the conferencing infrastructure, architecture and security protocols used by providers in the industry today.

Premiere's services are delivered through the most technically advanced security systems available, including the use of the most current encryption technology, internally developed industry-leading conference security features, the most advanced fault tolerant and redundant architecture, and the highest level of security screening in the industry. These systems make Premiere a leader in conferencing security.

Premiere addresses three primary areas of security:

- **Facilities** – employees, physical locations, and systems
- **Infrastructure** – carrier, network, bridging, and software
- **Conference Features** – ReadyConference, PremiereCall and Web Collaboration

Facilities

Employees

Premiere offers the most aggressive information protection in the industry, beginning with new employee screening. Pre-employment screening, including mandatory confidentiality agreements and background checks, are performed by the firm of a former FBI director, to ensure that only the most dedicated employees work with clients on conferences and events.

Physical Locations

In addition, Premiere employees work in conference facilities secured by access control systems. Guests and employees without proper authorization are not permitted in the Client Services areas to protect proprietary information from being accidentally or intentionally read or overheard.

Dual Operation Centers

In the event of possible catastrophic outage, Premiere Conferencing maintains two conferencing centers: one in Colorado Springs, Colorado, and the other in Lenexa, Kansas. If either site should experience a catastrophic outage due to a natural disaster or a major loss of telecommunications service, each center is fully capable of providing the full range of Premiere Conferencing services. In addition, each site has its own administrative support staff to provide logistical capabilities and facilitate operations.

Premiere Conferencing acquired the Chidlaw Building, originally built to house the North American Air Defense (NORAD) operations, as its conferencing center in Colorado Springs. Expansion into one of the most secure facilities in North America provides Premiere with a reinforced structure, independent power resources and telecommunications connectivity unrivaled in the conferencing industry. These facilities help ensure all business communications are protected by the highest security standards possible and, more important, are available at all times.

The Lenexa, KS (suburban Kansas City) facility is equally secure, complete with redundant facilities to ensure outages never result in service interruptions.

Power Backups

Because a reliable power source is essential to business continuance and uninterrupted services, power backups are standard with every system. The switches, bridges, servers, computer network, personal computers and peripherals all have power systems to support interruptions in the power supply, and to suppress surges. Because it was originally constructed to house NORAD, the Colorado Springs center is serviced by two separate power grids, making loss of power a limited risk. In addition to battery backups, diesel generators are available for longer outages. These help ensure that conferences can be conducted without interruption, regardless of the instability of the municipal power supply.

Infrastructure

Carrier

Premiere's multiple carrier strategy limits exposure to a single provider's network problems. Carriers include AT&T, MCI WorldCom, Southwestern Bell, ICG, Qwest and Espire. All services are provided to Premiere Conferencing on fiber optic networks, over multiple routes, with dual entrances into Premiere's facilities... Premiere also has duplicate systems, such as redundant processors and control units in its switches, to avoid failure of any portion of the network.

Network

Network management tools monitor and test the network to ensure it maintains an "up" status, with notification when network outage or degradation of service is detected. Routine testing ensures disaster recovery procedures are in place, and practiced, to enable technical support personnel at both conferencing centers to respond to any outage or degradation of service.

Bridging

Premiere Conferencing currently owns and operates automated and attended bridges located in its Colorado Springs and Kansas City conferencing centers. Premiere also operates conferencing bridges internationally in Canada, the United Kingdom, France, Germany, Australia, Singapore, Hong Kong and Japan.

Premiere has developed and deployed its own internally developed automated conferencing bridges worldwide, setting the standard for many of the leading conferencing features and security protocols used by providers in the industry today. By developing and implementing its own bridges, Premiere is able to monitor security closely and respond to possible threats proactively.

Premiere installs and maintains the bridges used for attended conferencing utilizing Spectel-Multilink and Compunetix bridging equipment. The software applications running on these bridges are controlled by Premiere technicians.

Automated ReadyConference is powered by Premiere's internally developed bridging software application. Utilizing internally developed software enables Premiere to monitor and address potential security risks and respond rapidly to viruses, hackers and to address other potential security issues that might place conference security at risk.

Conference Features

General Security Protocols

Security protocols applied to all automated and attended conferencing as well as Premiere's Web collaboration services help ensure sensitive client information is kept private. The following industry-leading service options may be selected to enhance one or more of Premiere's conferencing services:

- Event login for users and administrators.
- Meeting IDs and meeting controls.
- Application of SSL (Secure Socket Layer) encryption.
- Ability for presenter to control attendee participation and access to features.
- RSVP participant verification to authorize access to the conference.
- Moderator PIN code validation to verify the moderator initiating the conference.
- Meeting Keys that provide separate access for presenters and attendees.
- Meeting Login and Passwords to allow entry control and separation of participant roles.
- Unlisted Meetings option keeps meetings from being published on any public lists on the site.
- Expel Participants features provide the ability to remove and block unwanted participants based on name, e-mail or IP address.

Automated Security Features – ReadyConference

Standard ReadyConference security features include:

- Dedicated dial-in number and unique passcode.
- Moderator passcode may be changed regularly to help ensure access security.
- Validate Moderator adds PIN code security to the conference.
- Moderator billing feature to track usage.
- Optional entry/exit voice or tones.
- Dial out to add participants.
- Complimentary moderator features including conducting a roll call, disconnecting or muting all participant lines, and locking to secure the conference.
- Playing music on hold before the conference prevents participants from interacting until the moderator joins the conference.
- All Web-based reservations are scheduled on a secure server using encryption technology.

SecureTouch

SecureTouch is a package of Premiere Conferencing's industry-leading moderator features that provides an additional layer of security to a ReadyConference call. Available as a moderator-selected option for ReadyConference calls, SecureTouch can be selected and applied to any ReadyConference from within the ReadyConference Scheduling System, ReadyClick & Conference and Reservations.

SecureTouch includes the following features:

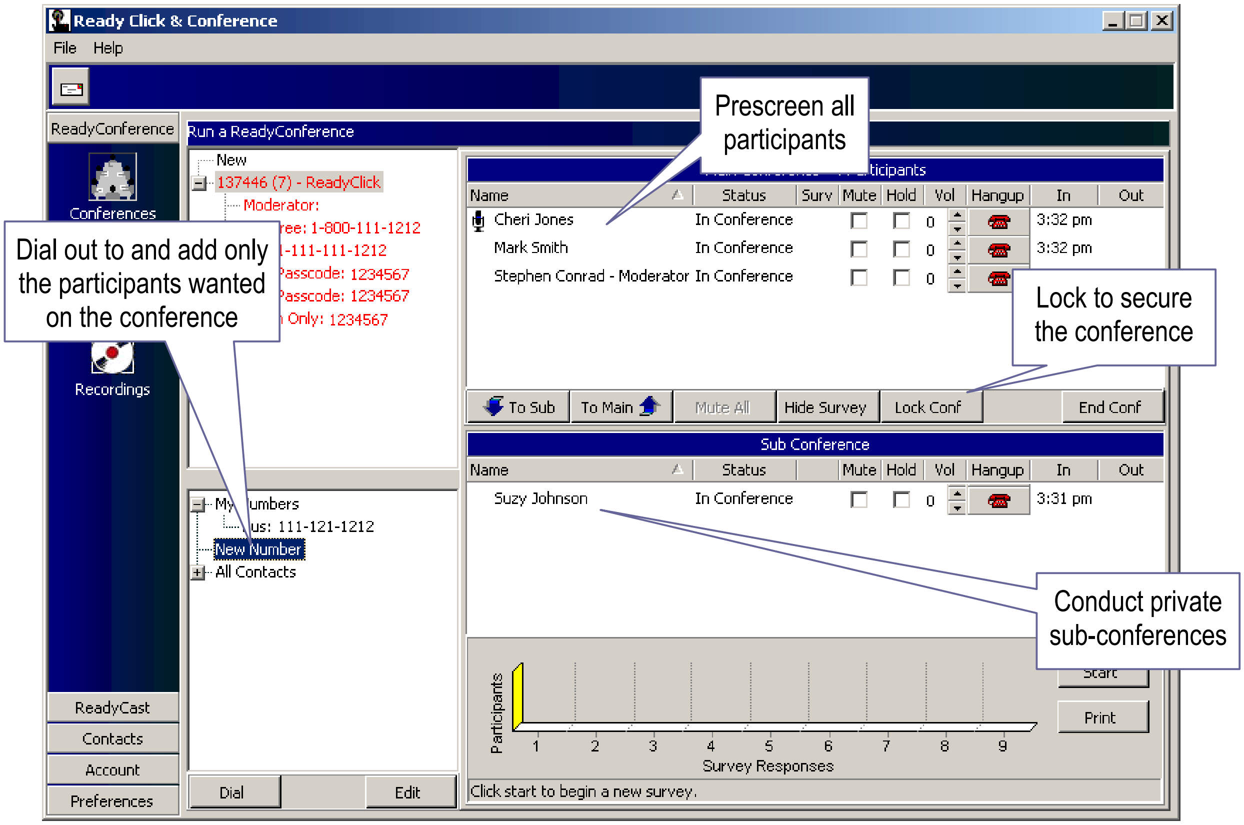
- Voice on entry/exit to let the moderator know when participants are joining/leaving the call.
- On-hold music to prevent participants from interacting until the moderator joins.
- Roll call to determine who is on the call.
- Validate Moderator provides an additional PIN code that allows only the moderator to initiate the conference.
- Lock/unlock to block participants from joining after the meeting has started.
- Mute all participant lines to prevent distractions from interrupting the call.
- Disconnect all participant lines ensures the meeting ends when the moderator leaves the call.

SecureTouch offers the flexibility of applying the highest level of security to individual conference calls, and provides organizations with the opportunity to use this feature as part of its company-wide conferencing security policy.

ReadyClick & Conference

ReadyClick & Conference gives moderators even more security and control over their conferences by allowing them to instantly initiate and manage automated conferences from their desktop. Features include the ability to mute lines, disconnect and dial out to participants, and instantly e-mail notes and documents for conference collaboration. In addition, ReadyClick & Conference lets moderators "drag and drop" any number of participants into a sub-conference for private conversations to conduct participant surveys and print results.

Additional security features provide the ability to visually identify all conference attendees, disconnect unwanted participants, add participants, and lock to secure the conference.



Main Conference - Participants

Name	Status	Surv	Mute	Hold	Vol	Hangup	In	Out
Cheri Jones	In Conference		□	□	0	☎	3:32 pm	
Mark Smith	In Conference		□	□	0	☎	3:32 pm	
Stephen Conrad - Moderator	In Conference		□	□	0	☎		

Sub Conference

Name	Status	Mute	Hold	Vol	Hangup	In	Out
Suzy Johnson	In Conference	□	□	0	☎	3:31 pm	

Click start to begin a new survey.

Prescreen all participants

Dial out to and add only the participants wanted on the conference

Lock to secure the conference

Conduct private sub-conferences

Attended Security Features – PremiereCall

Features managed by PremiereCall operators add to the security of Premiere's attended conferences. Implementing the following options can increase the security surrounding an operator-assisted PremiereCall:

- Confirmation Codes, which are six-digit codes, are required to enter the conference. For attended conferences, a new confirmation code is assigned for each conference reserved.
- Participant Lists provided before the conference gives Premiere's operators a list of "approved" participants. Callers not on the list are not permitted on the conference call.
- CommLine, a behind-the-scenes telephone line, enables moderators to approve or turn away participants not listed on their original participant list.
- Listen-only enables certain participants to be placed in "listen only," ensuring they can hear, but not participate in, the conference call.
- Sub-conferencing allows the moderator to pull key participants into sub-meetings during the conference call to discuss confidential issues.

Web Collaboration Security

The security philosophy of Premiere's audio conferences extends to its Web collaboration products. The infrastructure and feature sets of both products allow moderators to control access to their content with leading-edge technology.

ReadyCast^SM

ReadyCast is designed for smaller, intimate meetings, but with no sacrifice to security. In addition to the audio security offered by ReadyConference, ReadyCast offers the following security features:

Information Switching Platform

With ReadyCast, no files are ever stored on our server – data is transient and exchanged in real-time. Unlike most competitive offerings, ReadyCast does not require that presenters upload their presentations to ReadyCast servers in advance. With ReadyCast, conversion of the presenter's presentation or document to ReadyCast's vector-based format occurs at the presenter's system, and the data is then distributed to all participant systems, where the presentation or document is rendered. Not only does this improve the spontaneity and flexibility of a ReadyCast meeting, it greatly reduces the security risk that can come from storing confidential files on an external server.

Firewall Friendly

By using port 80 for data transmission, ReadyCast will not affect a company's overall corporate security model. Many competitors require the opening of additional ports in their corporate firewalls, therefore compromising the integrity of their firewall.

SSL Encryption

By encrypting all meeting data, ReadyCast protects meetings from packet hacks. 128-bit SSL encryption is standard on all meetings for all users.

Unlisted Meetings

By making the meeting "unlisted," it will not appear in the main Meeting Calendar on the ReadyCast site. This will assist in keeping the meetings confidential.

Meeting Passwords

Whether the meeting is impromptu or scheduled, the moderator will be prompted to create a password for the meeting. By following standard password guidelines, unwanted access to the meetings is limited.

Attendee List

In the meeting, the host will see a list of all attendees. This list allows the host to keep track of who is in the room and who is currently leading the meeting.

Attendee Expel

If an unwanted attendee appears in the Attendee list, the host has the ability to expel that attendee at any point in the meeting. This allows the host to minimize the content seen should an unwanted attendee gain access to the meeting.

Restrict Access
The Restrict Access function allows the host to lock a meeting once all invited attendees have joined. No one may enter the meeting once it has been locked. The host may toggle between locked and unlocked at any time.

Registration
The host can require registration prior to the event. This allows the host to approve or deny access to potential attendees and send vital meeting data only to those who have been approved.

VisionCast®

VisionCast is primarily used for larger events, from prospecting seminars to company-wide meetings. In addition to the security features offered by our PremiereCall audio products, the following features offer the highest level of security:

Infrastructure
With larger meetings the need for stability and reliability increases exponentially. To achieve the 99.99 percent reliability historically maintained by VisionCast, a server-centric infrastructure is required, and some meeting content must be uploaded to the hosting servers. State-of-the-art security measures are taken to protect the meeting content, including:

- Filtering routers
- Firewalls
- System level security
- Application authentication
- Application level countermeasures
- Separate data network
- Authentication to data

VisionCast offers these additional security features:

Firewall Friendly
VisionCast uses only port 80 for data transmission and will not negatively impact a company's overall corporate security model. Unlike many competitor's products which require the opening of additional ports in their corporate firewall, VisionCast does not and, therefore, does not compromise the integrity of their firewall.

No Meeting Calendar
The very presence of a meeting on a public meeting calendar poses a security risk. VisionCast meetings will never be posted on any Premiere Conferencing public meetings list. Clients may choose to publish a list of their upcoming meetings on their own Internet or intranet sites.

ID and Key Pairs
For every VisionCast meeting, a Meeting Key and a Meeting ID are created which may be customized by clients. Meeting entry is permitted only to participants with the Key and ID. Presenters and attendees have separate sets of Key and ID pairs.

Presenter and Attendee Roles

By restricting certain attendee functions, the presenter can minimize exposure to content. Presenters can move through the slides at their pace, bring applications, Web pages or their entire desktop into the meeting, and chat among the presenters. Attendees will only be able to perform functions the Presenters assign to them.

Framed Content

The VisionCast application uses a sizable frame to share applications and the desktop of a presenter. This allows the presenter to determine which portions of a document or application the audience will see by keeping sensitive data out of the share window.

Attendee List

In the meeting, the presenter will see a list of all attendees. This list will allow the presenter to keep track of who is in the room and who is viewing the content.

Attendee Expel

If an unwanted attendee appears in the Attendee list, the presenter has the ability to expel that attendee at any point in the meeting. This allows the presenter to minimize the content seen should an unwanted attendee gain access to the meeting**.**

Post-event Reports

After the event, the presenter will receive reports that include the names of attendees, company name and IP address, in addition to the responses to any polls or questions asked via the Internet during the session. These reports offer another way to review conference attendance and content.

SSL Encryption

In Q4 of 2002, VisionCast will be offered with SSL encryption. The product will utilize 128-bit RC4 SSL encryption on all facets of the meeting. This encryption will be available as an option on all meetings regardless of size or duration.

Customer Education

Premiere Conferencing educates its customers on security protocols and offers tips for ensuring they receive the maximum security possible surrounding their conferences.

Tips for Increasing Security on A ReadyConference

ReadyConference puts you in control of the conference. In addition to utilizing various security features, the following tips will help conduct an automated conference as securely as possible:

Know The Passcode.

Because a ReadyConference is not started by a conference support specialist, entering a passcode is the only way to access the conference. The reservationist will assign a passcode to the call when the reservation is made or during account setup. Callers have three opportunities to enter the passcode. If the third attempt fails, contact Reservations to verify the meeting time, passcode and dial-in telephone number.

Select Moderator Features.
Moderator Features enable participants to press *92 to hear a roll call; press *93 to terminate all participant lines; press *94 to lock and unlock the conference; press *95 to dial out to and add participants; press *96 to mute all participant lines; and press *97 to "un-mute" all participant lines. Moderator Features must be requested at the time of reservation. They are available at no charge.

Begin With a Roll Call.
Kick off the ReadyConference meeting with a roll call. Then, use the entry and exit tones that are played into the conference when participants join and leave the call to update meeting attendance. When an entry tone is heard, it helps to ask, "Who just joined us?"

Record Your ReadyConference.
If a Scheduled ReadyConference is reserved via the Web, ReadyClick & Conference, or Reservations, recording is an option. A replay will be available once the scheduled end time is reached.

Control Invitation Distribution.
When faxing or e-mailing the telephone number for a ReadyConference, take an extra step to verify the fax number or e-mail address before transmitting the document. Only share the dial-in number and passcode with the people authorized to attend the meeting.

Limit Distribution of ReadyConference Information.
Due to the 24/7 access of ReadyConference, limit the distribution of the passcode to prevent misuse of the account.

Assistance is Always Available.
Press *0 to reach a reservationist or press *1 to access the Help Menu. Pressing the star key (*) automatically re-admits moderators and participants to the meeting.

Tips for Increasing Security on your PremiereCall

The following tips will help increase the security surrounding an attended call.

Limit Distribution of Conference Information
Limit the distribution of conference information to only those participants desired on the call.

Announce Security Protocols
Premiere can make customized announcements at the beginning of an operator-assisted PremiereCall to inform participants of all security protocols. For instance, it may be announced that speakerphones are not to be used and that doors to offices are to be closed for the duration of the conference.

Shred Written Materials
Support materials used by conference participants should be shredded before disposal to prevent intentional or accidental misuse of proprietary information.

Maintain Privacy
Conduct all conferences in a location with a door that can be closed.

Avoid Speakerphones
Use a handset or a headset rather than a speakerphone to minimize the chance of being overheard.

When proprietary information might be exchanged on a conference call, please ask Premiere about additional safety measures.

Premiere Conferencing's standard and optional security features will enhance the security of your conference calls and Web collaboration events.

For more information or a customized security solution, contact a sales representative at (800) 234-2546.