

sonexis

Selecting a Secure Conferencing Solution

Sonexis Technology, Inc. | 2016



TABLE OF CONTENTS

2	Introduction
3	Conference Access Security
5	Document Security
5	Network Security
6	Enhancing Conferencing Security with Sonexis ConferenceManager
6	About Sonexis

INTRODUCTION

Organizations are increasingly using conferencing to enhance communications among employees, customers and partners. These conferences can be used as a cost-effective complement to travel and face-to-face meetings.

As you evaluate conferencing solutions for your organization, an important selection consideration should be the security the solution provides for your conferences. Specifically, the solution should provide conference access security and document security, and it should allow you to maintain control of your network security. By ensuring that these protections are in place, you can be more confident that your vital corporate information and property are shielded from unauthorized access.

CONFERENCE ACCESS SECURITY

The conferencing system you select should provide comprehensive security measures to ensure that conference access can be strictly controlled. These measures should include:

- **Account Creation Password:** Administrators should be able to password-protect the ability to set up an account for conferencing.
- **A unique Conference ID and PIN:** As part of the registration process, hosts should have the ability to select a unique Conference ID and PIN. These unique identifiers should be required whenever hosts log in to their account to modify account information, schedule or host conferences, or view saved conferences. The Conference ID and PIN should be unique and confidential and they should be used to identify a person as a trusted, registered user.
- **Unique Participant PINs:** The host should be able to select to generate a unique PIN for each participant. Participants will need to know the Conference ID and their PIN in order to join the conference. Using unique PINs adds an additional level of security to the conference.
- **Password Security:** As an extra layer of security and to further protect conferences, a host should have the ability to set a password for a conference. All participants would need to know this password in order to join the conference.

The screenshot shows the 'Participant Log In' interface for Conference Manager. The page has a light gray background with a subtle dot pattern. At the top left is the 'ConferenceManager' logo, at the top center is the title 'Participant Log In', and at the top right is the 'sonexis' logo. The main content area contains three input fields, each with a red asterisk icon to its left. The first field is labeled 'Conference ID:' and contains the value '8069'. The second field is labeled 'PIN:' and contains the value '6810'. The third field is labeled 'Password:' and contains the value '5439902'. Below these fields is a blue 'Log In' button with a right-pointing arrow.

- **Invitation-only Access:** Only participants invited should have the information needed to join a conference – dial-in number, URL, Conference ID, PIN, date and time of the conference, as well as the conference password, if required.
- **Participant List:** A list of all conference participants should be provided, allowing the host to see who has joined the conference at all times. Participants' phone numbers should be displayed in the audio console if your telephony configuration supports automated number identification (ANI).
- **Participant Announcements:** Participants should be announced as they enter and exit the audio conference and the host should be able to hear a roll call at any time. If unwanted visitors dial in to the audio conference, they should be immediately detected and hosts should have the option to instantly disconnect them.



- **Conference Lock:** Conferences should have the option to be "locked", thereby preventing unwanted guests from entering.
- **Dial-out Permission:** Administrators should have the ability to enable dial-out permission on a per account basis, for all hosts, or for none.

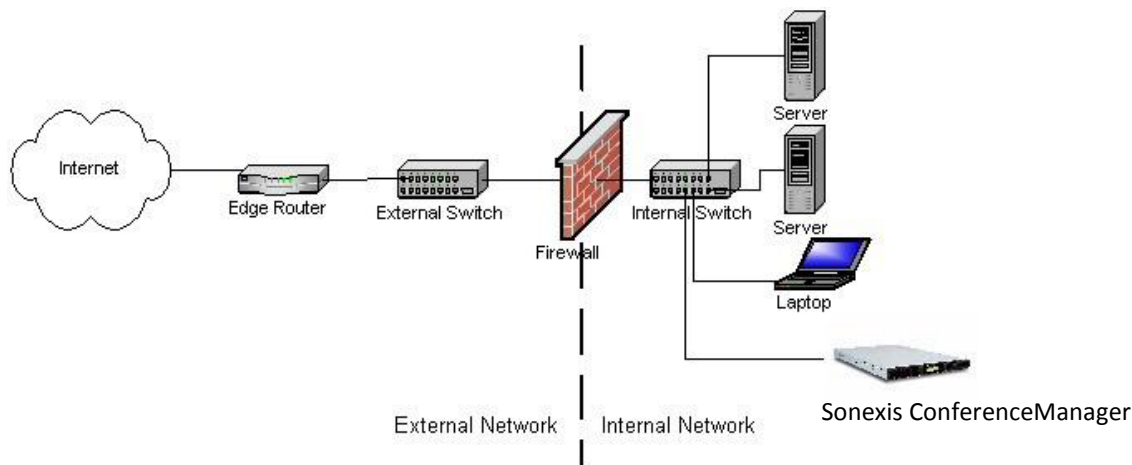
DOCUMENT SECURITY

In evaluating conferencing solutions, you should look for systems that protect the information and documents presented during conferences. You do not want this material – spreadsheets, presentations, contracts, etc. – exposed to unauthorized viewing or capture.

The two primary varieties of conferencing solutions – in-house systems and outside service provider solutions – offer two different security methods.

With an in-house conferencing system, documents are maintained behind the corporate firewall, where they are protected by your own corporate security procedures.

With an outside service provider solution, documents are typically transferred to the outside provider for use during the conference. As a result, this material is exposed outside your corporate network and becomes vulnerable.



NETWORK SECURITY

The means of providing network security will also differ significantly between in-house conferencing systems and outside service provider solutions.

An in-house conferencing system can be installed behind the corporate firewall. There, it can be protected from viruses and other intrusions by the same security protocols in place for the rest of your organization's network. In addition, an in-house system is under your organization's physical protection against power outages, temperature extremes, and other threats. By contrast, with an outside service provider solution, you rely on an outside provider to deliver network security.

ENHANCING CONFERENCING SECURITY WITH SONEXIS CONFERENCEMANAGER

The Sonexis ConferenceManager is designed to provide superior security for your conferences.

In addition to enjoying the benefits of the system's ease of use and its cost advantages, organizations also gain from the ConferenceManager's ability to better protect the information shared during audio and web conferences. By providing enhanced conference access security and document security, and allowing better control of network security, organizations can be confident that their vital corporate information and property are protected from unauthorized access.

ABOUT SONEXIS

Sonexis is a subsidiary of Compunetix, Inc. and a leading provider of an in-house audio and web conferencing platforms for the enterprise. Sonexis ConferenceManager has set new standards for ease of use and security. Designed to work within any existing voice or data network, hundreds of leading organizations have deployed Sonexis ConferenceManager with minimal cost, effort or administration. Headquartered in Pittsburgh, Pennsylvania with a Technology Center near Boston, Massachusetts, Sonexis can be reached at 888-4SONEXIS (888-476-6394) or www.sonexis.com.

For more information on Sonexis ConferenceManager and to schedule a custom ROI analysis, contact Sonexis at 978-640-2000, toll-free at 888-476-6394 or at www.sonexis.com.



sonexis

Sonexis Technology, Inc. | 2420 Mosside Boulevard | Pittsburgh, PA 15146 | 1.888.4SONEXIS (1.888.476.6394)
sales@sonexis.com | www.sonexis.com

© 2016 Sonexis Technology, Inc. Reproduction in whole or in part without written permission is prohibited. All rights reserved. Features and specifications are subject to change without notice.