

# **InterwiseConnect™**

## **Security**

Version 7.2

**Table of Contents**

**INTRODUCTION ..... 3**

**INTERWISE CONNECT ‘OUT OF THE BOX’ SECURITY FEATURES..... 3**

**Firewalls and Ports ..... 3**

**ICC Access and Management ..... 3**

**Content Protection..... 4**

**Real Time Communications ..... 4**

**Interwise Server Manager (ISM)..... 4**

## Introduction

Interwise has invested substantial resources to provide a strict security environment compliant with market standards and procedures for communications security.

This document provides an overview of the key security features available with Interwise Connect.

## Interwise Connect ‘Out of the Box’ Security Features

### ***Firewalls and Ports***

- ◆ Interwise Connect uses one port for all Interwise communications. This port is configurable.
- ◆ Interwise Connect supports the following standards:
  - Interwise applications are fully functional behind all types of firewalls and web-proxies (with most common authentication methods, including NTLM)
  - Network Address Translation (NAT)
  - Virtual Private Networks (VPN)

### ***ICC Access and Management***

- ◆ User rights management: the Interwise Communications Center (ICC) incorporates different user roles that are manageable (e.g., Event Administrator – per Event type, User Administrator, Portal Administrator, Moderator, Participant and so on).
- ◆ HTTPS (128 bit SSL encryption) is used for user login.
- ◆ Passwords have a minimum length of 6 characters (configurable).
- ◆ Passwords are kept encrypted in the ICC database.
- ◆ The password is re-encrypted for every instance it is used in a mail notification (i.e., Event invitation) sent from the ICC.
- ◆ iMeeting Events can be setup with an access key that prevents non-invited people from entering.
- ◆ All Event types can be setup with limited access for listed invitees only.
- ◆ An ICC session times out after a predefined period of inactivity.
- ◆ Administration data sent from the ICC to Servers participating in live Events is encrypted.
- ◆ Monitoring information is limited using a combination of:
  - User Name and Password
  - Allowed and forbidden machines
  - Queries syntax
- ◆ API:
  - API calls are authenticated.
  - API calls are encrypted (optional).

- API access to the ICC can be limited to specific machines.

### ***Content Protection***

- ◆ The Event Administrator, per Event, can disable the recording of live Events by the Participant application or on the ICC.
- ◆ Recording of a live Event by Interwise Connect can be hidden or published by the Event Administrator per Event before and/or after the Event has taken place.
- ◆ Assigning them as 'Private' can restrict access to materials uploaded to the ICC. This attribute allows owner access only.
- ◆ The Push mechanism that delivers the Event's content to users can be set to use SSL and thus ensure secured and encrypted communications.

### ***Real Time Communications***

- ◆ All real-time communications can be set to use either the Interwise proprietary non-published protocol or SSL for maximum data encryption.
- ◆ A Moderator's Over The Shoulder (OTS) access to Participants' desktops is restricted. An automatic request is sent to Participants, who will grant OTS access only when they feel secure in granting such access.

### ***Interwise Server Manager (ISM)***

- ◆ Registration of Communications Servers to the ISM requires a unique registration key.
- ◆ The ISM Administrator can disable unauthorized Communications Servers.