



# Interwise ECP Security Whitepaper



# ECP System Security

## *Interwise White Paper*

### Copyright

Copyright © Interwise 2003. All Rights Reserved.

February 2003

### Proprietary Notice

This document may not, in whole or in part, be photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Interwise, Inc.

This document is provided “AS IS” and the Authors assume no responsibility for any errors that may appear in the document, nor do they make any commitment to update the information contained herein. Nothing in this document constitutes, or shall otherwise be deemed to constitute, a guaranty, warranty, or license, express or implied, of any kind and the Authors make no representation whatsoever with respect to your use thereof. The Authors expressly disclaim all liability for any and all implied guaranties, warranties, and licenses. Additionally, the Authors retain the right to make changes to this document at any time, without notice.

### Trademarks

Interwise Enterprise Communications Platform, Interwise Expressway, and the Interwise logo are trademarks of Interwise. Interwise is a registered trademark of Interwise. All other trademarks are the property of their respective holders.



Interwise

25 First Street, Suite 412

Cambridge, MA 02141

USA

+1.617.475.2200 (Phone)

+1.617.621.3922 (Fax)

[www.interwise.com](http://www.interwise.com)

## Contents

<b>OVERVIEW</b>	<b>1</b>
<b>INTRODUCTION</b>	<b>1</b>
<b>ECP COMPATIBILITY WITH EXISTING IT INFRASTRUCTURE</b>	<b>2</b>
General	2
Firewall Port Usage	2
<b>PROTECTION OF INTERWISE-HOSTED ECP SERVERS AND SOFTWARE</b>	<b>3</b>
Attempts to Compromise Software Integrity	3
Attempts to Compromise User Data Integrity Stored by the ECP Application	5
Attempts to Execute ICC Functions Without Authorization	5
Attempts to Intercept and/or Compromise Integrity of ECP Data in Transit	6
Attempts to Prevent Users From Using ECP Functionality	6
Ensuring Event and Information Privacy	7
Application Sharing and “Over-the-Shoulder” Security Issues	8
Controlling User Authorization Through ECP Role-Based Security	9
Protecting Event Recordings Through Digital Rights Management	9
<b>CONCLUSION</b>	<b>9</b>
<b>ABOUT INTERWISE</b>	<b>10</b>

## Overview

At a time when news headlines are routinely dominated by stories of fast-spreading computer viruses, embarrassing hacks into government computer systems, unintended exposure of consumers' credit card information at e-commerce Websites, and recurring threats of "cyber-terrorism" against large businesses, corporate IT executives are more concerned than ever about the security of their computing resources. A major factor in the decision to purchase any new enterprise application software or service is the extent to which the supplier has equipped their solution with the necessary ingredients to protect the customer's information assets against a broad range of possible security threats.

Interwise takes this challenge very seriously, and has devoted significant engineering resources to design, implement, and deploy its Enterprise Communications Platform (ECP) application software and servers in accordance with industry best practices for system security. This document will explore, in depth, the specific architectural and operational aspects of the ECP that ensure safe and private real-time enterprise communications.

## Introduction

This paper is intended to answer the questions IT professionals might have about ECP system security when considering the use of the ECP within their own organization. We have grouped these questions into four primary areas:

- 1. Compatibility with existing IT security infrastructure.** Does installation and use of the ECP software require the customer to modify their existing IT network/security infrastructure in ways that could reduce the enterprise's existing security level, i.e., by introducing security vulnerabilities that weren't there before the ECP software was deployed?
- 2. Vulnerability of Interwise-hosted servers.** Are the Interwise-hosted servers and software vulnerable to potential compromise from a hostile attack? Can these servers be compromised so as to interfere with the proper operation of scheduled ECP events or improperly expose customer-sensitive data residing on those servers?
- 3. Security of data transmitted over public network segments.** How safe is the information that will be transferred between geographically distributed ECP servers that connect with each other over the public Internet? How safe is the information between Moderator and Participant client applications connecting over the Internet to Communication Servers on the Interwise Global Expressway or between users who login to the Interwise-hosted ECP using their Web browser?
- 4. Privacy of event access and materials.** Even when operating entirely within an organization's perimeter security (i.e., behind the corporate firewall), how well does the ECP regulate and restrict employee access to events, event content, and administrative information? Can employees who were not invited to a particular event be kept out? Can information/documents that were intended for viewing only by invited event participants be kept away from uninvited employees? Can only designated employees perform user and event administration functions?

This document addresses each of these important questions in detail, and illustrates how Interwise's ECP system provides safe and secure real-time online communication and collaboration services.

# ECP Compatibility with Existing IT Infrastructure

## General

Interwise's ECP is the most firewall- and proxy-friendly communications platform on the market today. All of the ECP applications that can be installed behind an organization's firewall(s) – the Moderator client, Participant client, Java Participant client, and locally-installed Communication Servers – offer a wide set of firewall support options, and all applications work transparently from behind firewalls and Web proxy servers without any loss of functionality.

All ECP real-time communication – whether between clients and servers, or among the servers themselves – can be encrypted with SSL. The underlying protocol is an unpublished, Interwise-proprietary, real-time messaging protocol that is encapsulated in standard TCP/IP data packets. This means that any firewall or proxy server that can pass TCP-based protocols can support ECP communication streams.

## Firewall Port Usage

The ECP client applications and Communication Servers that are installed locally behind the enterprise's corporate firewall initiate *only outgoing connection requests* to the ICC server or to external ICS servers. These applications do not listen for, or respond to, incoming connection requests from external hosts. This means the corporate firewall need not open any inbound ports to receive incoming ECP data streams.

The ECP applications require use of only a single TCP port and the choice of the port number is completely customer-configurable. There is no need for organizations to punch additional holes through their existing corporate firewalls to support ECP traffic. If necessary, however, IT organizations have great flexibility over ECP-related firewall port usage, since different ECP clients throughout the organization can connect to ECP servers via different port numbers, even when participating concurrently in the same ECP event. The ECP system can accommodate this kind of configuration by making adjustments solely on the ICC server; no changes to client-side software or settings are required.

For extra security, enterprises can also set IP-level filters on their firewalls to affirmatively allow replies only from external Interwise Global Expressway Servers with pre set IP addresses.

The ECP communication streams are also fully compatible with Web proxy servers. The Moderator and Participant clients, and the locally installed ICSs, are able to utilize "SSL Tunneling" to pass through the proxy server on port 443.

Proxy servers using basic authentication, as well as the more sophisticated Microsoft-proprietary NTLM challenge/response authentication mechanism, are both supported. The ECP client applications also transparently support packet authentication performed at the IP layer using industry-standard IPSec protocol.

In addition, ECP communication is transparent to firewalls and routers that perform NAT (network address translation). Also, any ECP applications, which gain access to the corporate LAN and/or corporate Internet gateway through a VPN connection, operate transparently without reconfiguration and without any loss of ECP functionality.

## Protection of Interwise-Hosted ECP Servers and Software

Customers who elect to use a Fully Hosted or Blended ECP deployment are wholly or partially dependent on servers that are co-located, monitored, and administered by Interwise's Global Hosting Services team. This section reviews the steps Interwise has taken to protect these servers. We first consider the types of hostile attacks that the ECP servers might realistically face and then we examine point by point how the system and its supporting infrastructure defends against each threat.

Potential security threats fall into the following main categories:

- Attempts to compromise software integrity
- Attempts to compromise user data integrity stored by the ECP application
- Attempts to execute ICC functions without authorization
- Attempts to intercept and/or compromise integrity of ECP data in transit

### Attempts to Compromise Software Integrity

This threat includes attempts to compromise the integrity of the software itself, whether it is the ECP application software or the system software running on the underlying server hardware. These attacks could be attempts to inject viruses or worms into the target software, or to gain access to the underlying OS (through "hacking,") and then explicitly destroying or tampering with system or application software components or configuration settings. Software on servers at Interwise's primary and satellite data centers are aggressively protected against these kinds of attacks in a variety of ways:

- **Controlled physical access:** Robust control is maintained over physical access to all of the ECP servers by housing them at state-of-the-art co-location facilities equipped with top-caliber access control mechanisms, including:
  - Exterior fencing or other perimeter barriers with controlled entry points with auditable access control and visitor logging, camera surveillance, and monitoring/patrolling by premises security personnel;
  - Isolated individual, locked cage for Interwise within the hosting facilities with their own controlled access points and is under camera surveillance;
  - Limited access to restricted areas within the facility (such as the facility's Network Operations Center, power/utility rooms, etc.);
  - Only Interwise personnel who are members of the Global Hosting Services team are authorized to enter the data center facilities;
  - Hosting facilities are run by industry-leading vendors that maintain high standards for their own personnel, including requiring background checks.
- **Controlled network access:** Network access to the servers is controlled and restricted through proper use of redundant firewalls, network address translation, LAN segmentation, and origin-IP filtering to restrict inappropriate network traffic from reaching the ECP servers.

Only standard ports (80 and 443) are opened on the Interwise firewalls. IP-filtering ensures that administrative functions on the co-located firewalls or servers cannot be performed from an Interwise employee's home or from any unknown host; only hosts on the corporate LAN at Interwise's Network Operations Center (or from a third-party service provider retained by Interwise to perform 24x7 intrusion detection monitoring, discussed below) can access the co-located equipment.

- **Hardened OS software:** All ECP servers have had their system software components "hardened" through application of vendor-recommended security patches and configuration settings. Vendor security alerts are monitored religiously and new updates and security patches are applied promptly. Unnecessary system services are de-installed from the servers to reduce the chances that hackers will be able to exploit any well-publicized vulnerabilities in these widely known system services. For example, the Interwise Communication Servers have no Web server, telnet, SMTP, or directory services installed. This makes it extremely unlikely that a hacker would find any well-known exploitation opportunities on these ICS machines.
- **Controlled admin passwords:** Passwords on accounts used for system administration tasks are carefully controlled and changed frequently. When a maintenance task must be performed with administrator rights, the task is performed under a Hosting Services team member's individual account, so that an audit log of changes made by specific individuals is always maintained.
- **Continuous virus scanning:** All ECP servers are scanned on a continuous basis with the Enterprise Edition of Norton's anti-virus software. Virus signature updates are obtained twice daily. Scanning reports receive both continuous automated inspection, as well as manual inspection each morning.
- **Third-party intrusion detection monitoring:** Guardent has been engaged by Interwise to perform various security monitoring and maintenance functions on the firewalls, routers, and servers at the Interwise data center. This includes 24/7 monitoring for server uptime, intrusion detection signatures and other unusual traffic patterns, raising alerts to Interwise operations personnel as necessary.

Guardent:

- Is a leading Managed Security Services Provider (MSSP) staffed with experienced Internet security professionals who developed the security infrastructures of leading telecommunications firms, financial institutions, and manufacturers.
- Advises and assists Interwise regarding proper maintenance and configuration of all firewalls, routers, and switches within the primary data center.
- Performs a formal security audit on the Interwise primary data center.
- **No dial-up access:** There are no modems or other dial-up access into any of the data centers housing Interwise servers; access is only possible via firewalls, VPN, or on-site.
- **Remote deactivation of "suspicious" servers:** ICSs at satellite data centers on the Global Expressway can be remotely deactivated from Interwise's main NOC if monitoring indicates unusual activity suggesting a hostile attack, or if virus scanning detects an infection.

- **Java packages are digitally signed:** The Java classes are signed with a digital certificate. This ensures that hostile attackers cannot substitute a “Trojan Horse” client application in place of the bona-fide Interwise-authored client.

## Attempts to Compromise User Data Integrity Stored by the ECP Application

Interwise protects against data-centric attacks in the following ways:

- **Controlled physical and network access:** Physical and network access to the ECP servers on which the sensitive data resides is controlled and restricted using the mechanisms outlined in the previous section.
- **Event materials downloaded in compressed file format:** Uploaded event materials are stored on the ICC server's file system in a packed/compressed file format. Event materials remain in this format when pushed/downloaded onto Participants' clients, and are only unpacked on a “just-in-time” basis when needed during the live event. The unpacked documents are automatically deleted from the local PC's cache at the conclusion of the event.
- **Materials encryption:** All materials that are inserted during an encrypted event are encrypted as well. In an upcoming ECP version, all uploaded event materials and recordings will be stored in encrypted format while residing on ECP Servers or on Participants' PCs until needed during an event.
- **Digital rights management for recorded events:** Facilities are provided to allow users to optionally protect event recordings with an Interwise-proprietary Digital Rights Management (DRM) mechanism that "locks" recordings with a special key and limits the number of different computers that can be used to perform the playback.
- **Database servers are hidden:** The ICC relational databases at the Interwise primary data center reside on a separate local subnet. Thanks to the network address translation, the database machine is not obviously accessible from the ICC Web server machine even if an intruder somehow compromised the latter.

## Attempts to Execute ICC Functions Without Authorization

Interwise protects against these kinds of attacks in a number of ways:

- **User login required:** With the exception of guest users who join events that are specifically designated as “open” to the general public, all other ICC-based operations require the user to first login to the ICC. A user account, must first be created by a user with appropriate administrative privileges. The length of a user's password can be customer-configured to require a certain minimum number of characters.
- **SSL-encrypted log in to the ICC:** SSL encryption is employed on the page used for user login to the ICC.
- **ECP Integration with LDAP Directory Servers:** ECP supports LDAP. The ICC can be linked to a customer's existing LDAP directory service, enabling centralized user administration. The ICC does not store the passwords locally when configured to authenticate with a directory server. This feature increases the security of the system.
- **Automatic session expiration:** Browsing sessions with the ICC automatically expire after a customer-configurable period of inactivity.

- **Role-based security model:** The activities that logged-in users can perform in the ICC are limited based on their rights/privileges according to their membership in a particular "role" with associated rights/privileges.
- **Top-level "URL gateway":** ICC Web-based functionality is channeled through a parameterized top-level gateway .asp page. The incoming request for the top-level page is automatically redirected by the Web server to a function-specific lower-level Web page for further processing. If an attacker discovered the URL of a lower level Web page and attempted to visit that page directly, the request would be rejected, a "tampering" alert would be logged on the Web server, and the would-be attacker would be redirected to an error page or other customer-configurable destination.
- **Filtered catalogs of existing events:** Listings of event Materials and recordings residing on the ICC are filtered by the ICC Web server when displayed to ECP users so that users can only see events and recordings to which they have rights/permissions.
- **Protected API function calls:** By default, all API function calls are protected in the following ways:
  - a) **Proprietary encryption:** The ICC Web server can be configured to require the API URL parameters – the "payload" of the function call – to be encrypted.
  - b) **Origin-IP Filtering:** The ICC Web server can optionally be configured to accept incoming HTTP-based API function calls originating only from servers with known IP addresses. This origin-IP filtering would block hostile API function calls from would-be attackers' unknown hosts.

## Attempts to Intercept and/or Compromise Integrity of ECP Data in Transit

Interwise protects against them in the following ways:

- **Encrypted data streams:** All data streams can be encrypted with SSL 3.0 during transmission. The encrypted data streams include the real-time data streams as well as the materials that are inserted during an event as well as those that are pre pushed to the participants.
- **Opaque data streams:** Underneath the encryption or when encryption is not used, ECP real-time data streams and push contents are sent in a compressed, unpublished proprietary messaging protocol. These streams contain audio, video, text chat, whiteboard control commands and annotations, and shared application screen image updates. Hostile decoding is complicated by the fact that for most types of Interwise data, such as shared application screen images and materials documents, the protocol is "incremental". Only changes from the previous version of the data are actually sent in the stream.

## Attempts to Prevent Users From Using ECP Functionality

This broadly describes any kind of attack in which the attacker attempts to disable the target system so it can't perform its intended function for its intended users, but without actually modifying the system's software or data.

**Denial of Service Attacks** Typically, Denial of Service (DoS) attacks are accomplished by bombarding the target system with an overwhelming cascade of incoming system requests. Interwise protects against this kind of attack by configuring its routers to watch for DoS attack

signatures and log denied connections. The routers at each Interwise data center are configured to detect, and in some cases reject, incoming traffic with the known hostile signatures, and to automatically log the IP address of the originating packets. The routers and firewalls can then be configured to filter/block subsequent incoming packets originating from these hostile IP addresses.

In addition, the ECP server architecture enables the use of redundant ICSs with automatic fail over during an event. Should a particular Communications Server be taken offline by a DoS attack, its connected clients will automatically and transparently reconnect to another ICS at the same, or at another, site. All sites on the Interwise Global Expressway are equipped with multiple ICSs to provide this redundancy.

## **Ensuring Event and Information Privacy**

It is necessary to ensure that users – whether internal or external to the organization – cannot join ECP events to which they were not invited, or view event materials or recordings which are not appropriate for them to see.

For companies whose business depends on the commercial sale of event recordings (e.g., pay-per-view courseware or lessons delivered via the ECP), ECP provides a secure mechanism for protecting the copyrighted material.

This section explores how the ECP handles user identification and authentication, role-based authorization, and special protection options for regulating playback of event recordings.

## **Defining, Registering for, and Joining events**

The ECP offers event Initiators and Administrators considerable flexibility in regulating how individuals are registered and invited to ECP events. To enter a private event, an individual must be registered in the ICC *and* registered to the specific event. Regardless of the method of entry to the private event, the participant's identity is authenticated through ICC login. Event privacy is achieved primarily by customizing event listings to expose only events to which the given user is registered. Furthermore, should users obtain listings of events to which they are not permitted access, the URL Gateway mechanism will protect the ICC data. Confidentiality in sensitive events can be assured by requiring participants to enter the events only through their customized listings page, and by confirming the physical identity of participants arriving at the live event through voice checks and, where possible, video images using the ECP's integrated audio and video conferencing capabilities.

## **Managing Uploaded and Pushed event Materials**

The presenter can specify access permissions on the uploaded materials as follows:

- **Public:** Allows all Moderators registered in the ICC to use and view the materials and make changes.
- **Read-only:** Allows all Moderators to use and view the materials, but only the Moderator who uploaded and owns the materials can make changes to them.
- **Private:** Allows only the Moderator who owns the materials to view and make changes to them. Materials marked “private” are confidential in the sense that only the Moderator who uploaded and owns them can view and modify them.

The Moderator assigns materials on the ICC to materials to a specific event. This triggers the ECP's Push Server to begin automatic distribution of the event materials to all the participants registered to that particular event. The Moderator who created the materials has the option to delete them via the ICC after the event.

For customers who opt for a Hosted or Blended ECP deployment, uploaded materials will necessarily reside, on an ICC server. Although ICC servers are secure, some customers may still have reservations about leaving ultra-sensitive company documents on a remote server that is not directly under the control of their own IT organization. In such a case, the moderator could choose *not* to upload and push the materials in advance, but rather present the materials during the live event by opening the documents and sharing them in real-time.

## Application Sharing and “Over-the-Shoulder” Security Issues

In addition to presenting pre-pushed event materials to event participants, the moderator has the ability to share display applications running on his/her local PC with the participants during a live event. This allows the participants to be given permission to control an application on the Moderator's PC, while all participants simultaneously view that activity. The question naturally arises, “Does passing control of the Moderator's local PC to a participant present a possible security threat if the participant attempts to use the shared application maliciously?” This concern can be assuaged by the following observations:

- **The Moderator can instantly regain control of his/her PC at any time**, and immediately terminate the participant's application sharing session, by simply moving the mouse on his/her local PC, or by pressing a designated “hot key” on the keyboard.
- **While the participant has control of the Moderator's local application**, the Moderator can watch all participant actions on his/her local PC's display. The participant cannot perform any operation on the Moderator's local PC without it being observed by the Moderator.
- **The participant cannot launch any new applications on the Moderator's local PC** provided that the Moderator chooses to share a *single* specific, running application rather than sharing his/her entire desktop.

A reverse variation of the application sharing capability, called “Over-the-Shoulder” (OTS). Instead of the Moderator passing control of a local application to one of the event participants, in OTS one of the participants actively allows the Moderator view the display of their PC to “look over their shoulder”. This allows the Moderator to observe the participant's use of an application in real-time and/or demonstrate proper use of the application to the participant on the participant's own PC.

A participant might be concerned about turning over control of his/her local PC to a remote Moderator. The participant's security concerns can be assuaged by the following observations:

- **The Moderator cannot gain control of the participant's local application without first requesting permission to activate the Over-the-Shoulder feature on that participant's PC.** A message box is displayed in the participant's client application and the participant can approve or reject the request.
- **The participant can instantly regain control of his/her PC at any time**, and immediately terminate the Moderator's OTS session by simply moving her mouse.
- **While the Moderator has control of the participant's local application**, the participant can watch all Moderator actions on the local PC's display.

In short, application sharing and Over-the-Shoulder, are powerful ECP capabilities but do not represent a security risk.

## **Controlling User Authorization Through ECP Role-Based Security**

The ECP employs a sophisticated and highly granular role-based security mechanism. In this mechanism, users are registered in the ICC and assigned membership in one or more *roles*; each role is associated with a specified set of *permissions* or *privileges*; each permission entitles the holder to perform certain functions and access certain kinds of data in the ICC database or server file system. The ICC adds/hides menus, links, and buttons based on the currently logged-in user's assigned permissions.

By default, a newly registered user is assigned the Basic role, which has very limited privileges (e.g., the user can view and participate in events, but cannot create any new events or perform any other administrative operations). Typically, the ICC's Super User assigns various administrative roles to certain other users in the organization so that these other users can share the administrative responsibilities. These administrators can in turn register additional users to the ICC and/or create and schedule new events as necessary according to the capabilities of their assigned role(s).

Users can be assigned combinations of roles and new roles can be assembled with custom combinations of permissions. The ECP's role-based security mechanism offers the customer significant flexibility in regulating the precise combination of permissions available to designated users within their organization.

## **Protecting Event Recordings Through Digital Rights Management**

One of the most powerful aspects of the ECP is its ability to record *any* type of event for later re-use. Individuals who were unable to attend the live event at its scheduled time can playback the recorded event "on demand" at their own convenience.

When an event is first defined, the initiator can specify whether or not the event will be recorded and stored on the ICC. The initiator can also determine whether or not participants will be allowed to make individual recordings of the live event. Thus, any event can be recorded on the server-side, on the client-side, on both sides, or on neither side – at the discretion of the user who establishes the event parameters.

Sensitive recordings, or recordings which the producer wishes to protect from prying eyes or sell commercially, can optionally be packaged using a special digital rights management capability. This capability enables customers to prevent unauthorized distribution or playback of their intellectual or proprietary recording content. Protected recordings can be restricted to one, or a limited number, of specific client computers. The essence of the protection mechanism involves the encryption of the recording file, plus the generation of a unique key that "locks" the recording and prevents it from being played back inside the Participant Application unless the key is verified against an authorization record stored in the ICC.

## **Conclusion**

This document has explored the architectural and operational aspects of the ECP that ensure secure and private real-time enterprise communications. The detailed description of the measures taken and features implemented by Interwise demonstrate that the ECP effectively addresses the

major security concerns that IT organizations might typically have when considering the purchase of any new enterprise software solution. In particular,

- The ECP is compatible with an enterprise's existing IT network/security infrastructure because the ECP client and server applications can be easily deployed without requiring any changes to existing corporate firewalls, Web proxy servers, or VPN configurations.
- The Interwise-hosted ECP servers on the Interwise Global Expressway are effectively protected against attacks from hostile agents through a broad range of security defense mechanisms.
- Customers can be confident that ECP data streams transmitted over public network segments are safe from interception and tampering.
- The ECP incorporates a variety of mechanisms to regulate access to, and to ensure the privacy of, event participation, event materials, user profile information, and event recordings.

Interwise has invested substantial resources to provide a strict security environment compliant with market standards and industry best practices for communications security. Ensuring ECP system security and protecting customer information assets remains a top priority in all future ECP product development.

## **About Interwise**

Interwise helps organizations address the communications challenges presented by dynamic business environments, global marketplaces and geographically dispersed stakeholders. The Interwise Enterprise Communications Platform (ECP) is a single platform for live collaboration, communications and eLearning. The leading choice of Global 2000 companies, Interwise maintains a presence in more than 20 countries through a direct sales force, distributors, value-added resellers and systems integrators. Visit us at (URL) <http://www.interwise.com/>.