



Security Overview

This description is for information purpose only.

Web4, a division of netGuru, Inc., reserves the right to alter this description or to adapt it to technical conditions at any time. Web4 shall not be liable for any damage caused by the contents of this document or the use of the described product.

Web4 provides this publication "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose.

Web4 has the sole copyright for this document. Any reproduction, adaptation, or compilation work for own use and / or distribution purposes is allowed with the written consent of Web4 only.

All brand and product names in this publication are registered trademarks and trademarks of their respective holders.

Copyright © 2003 Web4, a division of netGuru, Inc.

Web4, a division of netGuru, Inc.
22700 Savi Ranch Parkway
Yorba Linda, CA 92887
USA

Tel: 1-888-376-8900(Toll Free).
1-714-974-2670(Intl)

Fax: 714-974-4771

<http://www.ereviewonline.com>

Contents

- SECURITY FEATURES AVAILABLE IN EREVIEW..... 4**
- SECURE ONLINE COLLABORATION ENVIRONMENT 4
- APPLICATION LEVEL SECURITY 5
 - Single Point of Logon - User Authentication..... 5*
 - Content Level Security..... 5*
 - SSL Security 5*
- SESSION SECURITY..... 6
- FIREWALL COMPATIBILITY 6
- SIGNED APPLET 6

Security Features available in eReview

Secure Online Collaboration Environment

eReview is an enterprise decision support tool that allows users to share any electronic document in real-time on a browser-based terminal anywhere, anytime! eReview is mission critical to the design process as it allows design teams to shorten the time to market and reduce costs in product lifecycles.

eReview ensures that the product meets the most stringent security requirements of today's markets. EReview has a powerful set of security features in-built that allows secure transmission of data across intranets, extranets and the Internet.

The purpose of this document is to provide information on security features and functions that are available in eReview. It is assumed that the reader of this document has some preliminary knowledge of various aspects of eReview and is aware of different levels of users that can use eReview.

eReview provides many means of user authentication and authorization to resources across the entire system. Authentication ensures that people are who they claim to be. Authorization uses this information to grant the appropriate level of access control to resources, including various sections and content within each of these sections.

eReview does not send the original documents over the Web. The eReview server processes the drawings and images files behind the firewall and delivers compressed versions of these documents through the HTTP server or direct TCP/IP configured port.

Application Level Security

Single Point of Logon - User Authentication

eReview implements the security at the application layer primarily via the eReview applet that gets loaded through a java-enabled browser. This ensures that the application can only be started through a browser. The coordination of the applet at the client machine with the server components is internal and eReview takes care of it. No such communication mechanism can be invoked separately outside of eReview. Only a valid eReview applet can communicate with valid eReview server components.

In short, each session is dynamic and involves a handshake between the client and the eReview server, and the communication between these can be by default encoded and optionally SSL encrypted. EReview can also handle any other encryption mechanism that the user may deem fit. HTTPS (128-bit SSL) is used in most of the web-based transmission and is considered to be a standard in secured data transmission.

eReview is accessible through a single, common logon screen providing a secure 'Front Door' to the entire system. Chairpersons can make these online collaborative sessions secure by providing a password for these sessions. This ensures that only the authorized users can join these meetings.

Granular, roles-based security allows the Chairpersons to quickly control the exact level of access of users will have to the content that is being shared in an online meeting.

Content Level Security

eReview provide an additional layer of user authorization control by restricting access to content within the application. For example, the authorized users can open some documents in "Roaming Mode" so that no one even would know that a document has been opened. These users can hide or re-dact some parts of these documents, mark them up and then switch the mode to "Collaborative" to show only the information that is relevant to other users. This ensures the content level access to the users on these documents. This means some content within a document can be hidden from the users that are there in online collaborative meetings.

SSL Security

eReview provides the option of securing all transmission with 128-bit encryption using Secure Sockets Layer (SSL).

Secure Sockets Layer, SSL, is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remains private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an SSL Certificate.

eReview can be deployed under SSL (Secure Sockets Layer). The secure, fast and easily adapted SSL protocol is the most widely used socket-level security protocol on the Internet and is supported by all major Web servers and most Internet-accessible servers.

Session Security

Users are automatically disconnected after a configurable period of inactivity. Session variables are not cached therefore security information is not available to a subsequent user at the same client computer on log off.

Firewall Compatibility

While making connection between the client and server, eReview connects through the HTTP or HTTPS from the port provided in the eReview server configuration. In the case that eReview communicates through an SSL connection, all traffic is carried over the HTTPS ports of the server.

Regardless of the connection that is established at the time of client loading, Firewalls do not have to be especially configured to start eReview sessions. In case of Firewalls blocking certain ports that carry this communication, eReview can be configured to communicate through port 80. In case of Intranets, there is no need to open any port, since all the communication being carried out is internal.

eReview is the only Java viewer and collaboration tool that honors existing firewalls and encryptions.

Signed Applet

eReview is a signed applet that ensures that the applet is coming from a trusted source. This means, the users get a security warning while the applet loads in the browser. This methodology is prevalent in the current market and is used by all signed applet technologies around the world.

