



TimeGuard

Prevent Unauthorized Access to OWA Accounts

Users will leave an OWA session active by failing to logoff and close all browser windows. TimeGuard protects OWA accounts from users who fail to logoff and close the browser window, by prompting a user when they have exceeded a session inactivity limit with the opportunity to extend or logoff

- Protects OWA accounts from unauthorized access
- Extends the security provided by forms based authentication (FBA) and ISA to offer total protection for OWA users

"MessageWare has enabled Lloyd's to offer a controlled and secure Internet-based email system that will help increase both efficiency and productivity from employees who are travelling or working from home."

- Lloyd's of London

Product Features

● Session inactivity timeout prompts

TimeGuard prompts a user when they have reached their session inactivity limit with opportunity to extend or log off

● Maximum session timeout

TimeGuard provides a maximum timeout option which requires users to re-authenticate after a predefined maximum session time has passed

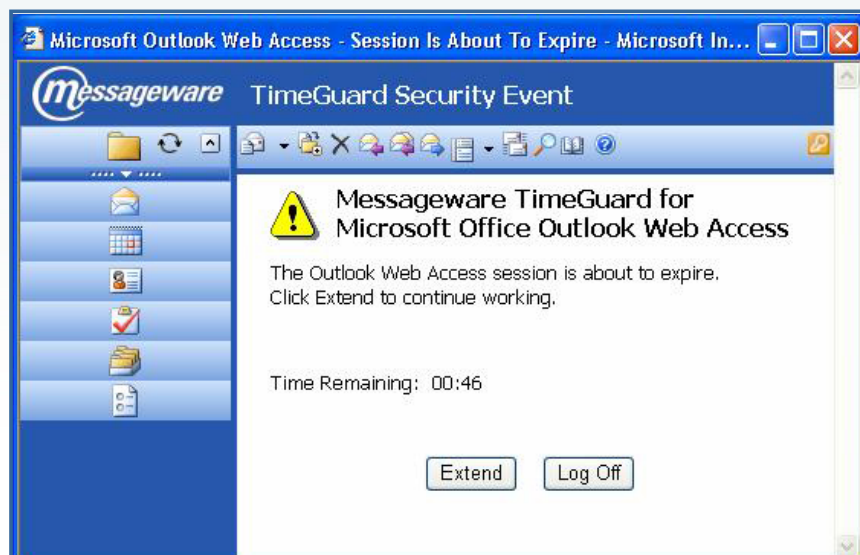
● Extends security provided by FBA and third party products

TimeGuard extends the security provided by forms based authentication (FBA) and ISA to offer total protection for OWA users

● Customization capability

Exchange System administrators can customize TimeGuard according to their corporate policies, user's hardware and current locations (zones, groups, CDR, etc.) TimeGuard settings can be customized in minutes using the user-friendly admin console

Screenshots



- ◇ The user is prompted to act after a predefined period of inactivity

Contact

MessageWare Incorporated
Tel: 905 812 0638
Email: salesteam@messageware.com
Web: www.messageware.com