

ISA Security Report: OWA Issues Undetected by ISA Server

Table of Contents

The Importance of Securing Outlook Web Access.....	Page 3
Security Events in Outlook Web Access.....	Page 3
OWA Security Issues Undetected by ISA Server.....	Page 4
Securing Outlook Web Access from Navigation Security Events.....	Page 5
Securing Outlook Web Access from Session Inactivity Security Events.....	Page 6
Appendix 1: Testing for OWA Security events with ISA Server installed.....	Page 7

The Importance of Securing Outlook Web Access

With over 70% of organizations using Microsoft Exchange, Outlook Web Access (OWA) offers a cost effective alternative to VPN as a remote messaging system of choice. Most companies use either ISA or FBA or both, in conjunction with third-party authentication solutions to secure their Exchange environment. **However, even with this infrastructure, OWA accounts can be vulnerable to unauthorized users.** Security events occur unknowingly every time a user is logging in to Outlook Web Access on a shared computer, for example at a conference kiosk, client site PC, or university computer lab. If even one user account is compromised, this can result in consequences ranging from loss of competitive information to violation of compliance laws.



Question:

What are the consequences to your organization if an unauthorized user gains access to an employee's email account?

Security Events in Outlook Web Access

Navigation Security Events

There are several ways in which users can navigate away from an active OWA session without first logging off. Below are the most common scenarios:

- 1) User enters a new address in the address bar of the browser
- 2) User clicks on a favorite in the browser toolbar
- 3) User presses the Back button
- 4) User presses the Home button

When users navigate away from an OWA session without first logging off, a security vulnerability is created. Any person can return to the active session without entering new login credentials.

Session Inactivity Security Events

Users can also leave an OWA session active by forgetting to logoff AND close the browser window. IT departments have secured addressed this issue by implementing security solutions from different vendors, such as single sign-on, two-factor authentication, and multiple layers of authentication. However, these authentication solutions rely on the user selecting computer role (public or private) and they do not offer much control over how timeouts are configured.

OWA Security Issues Undetected By ISA Server

While ISA Server is an excellent firewall solution for Microsoft Exchange, there are still many security events that ISA Server does not detect that can leave organizations vulnerable to data leaking to unauthorized users. *See Appendix 1 for a list of test scenarios.* This is of particular concern to companies who need to keep their confidential information secure for competitive or regulatory reasons.

ISA 2006

Previous versions of ISA Server had an optional administrative setting to automatically log off a user when the user navigated away from an active OWA session to another web page.



ISA 2006 does not have the auto logoff feature, so if users do not remember to logoff before leaving the active OWA session, unauthorized users can easily gain access to the user's OWA Inbox.

<http://www.microsoft.com/technet/isa/2006/deployment/exchange.msp>

ISA 2004 & ISA 2000 below:

ISA Server 2000 and 2004 have an optional administrative setting that automatically logs off users when they leave an active OWA session for another web page, as shown in Figure 1

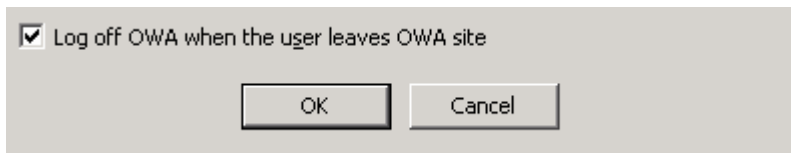


Figure 1: Auto logoff feature in ISA Server 2000 & 2004

However, this setting does not detect all navigation security events.



ISA 2000 & ISA 2004 fail to detect when a user leaves the ISA site when the user is on a machine with a pop-up blocker turned on.

While ISA Server 2000 & 2004 provide the auto-logoff feature for OWA, it also forces the logoff when the user accidentally navigates away from an active session – for example, by pressing the home button or the refresh button. In scenarios like this, the user does not wish to end the OWA session but the ISA settings force the auto logoff and the user must enter his login credentials again to return to the OWA session.

Securing Outlook Web Access from Navigation Security Events

Messageware NavGuard is an application for Outlook Web Access that extends the security of ISA Server by monitoring when a user has navigated away from an active OWA session. NavGuard prompts the user when a security event has occurred, with the option to logoff before navigating away to another page or continue using OWA. This can occur in many situations, including the following:

- 1) User enters a new address in the address bar of the browser
- 2) User clicks on a favorite in the browser toolbar
- 3) User presses the Back button
- 4) User presses the Home button

NavGuard also provides a user-friendly prompt when the user has accidentally navigated away from an active OWA session, by pressing the Refresh button on the browser bar or Ctrl-R.



When a user navigates away from an active OWA session, NavGuard prompts the user to either return to the active OWA session, or log off the session securely. See Figure 2 for a screenshot of the NavGuard prompt.

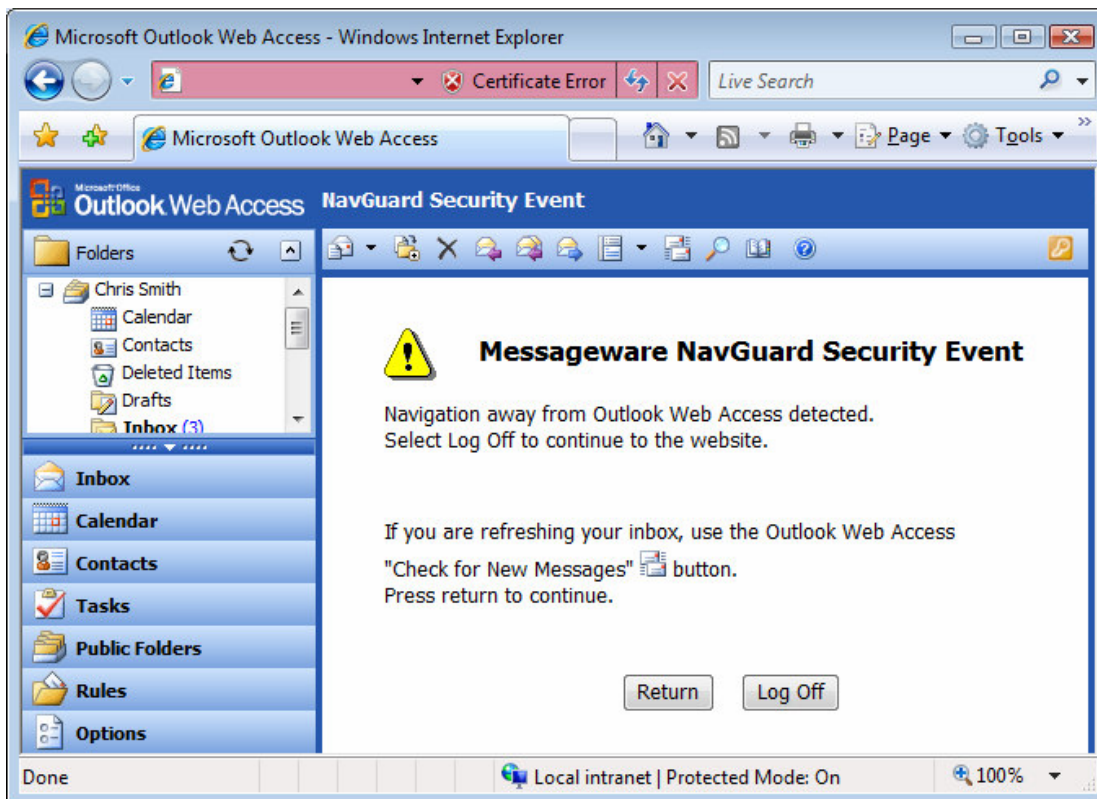


Figure 2: Messageware NavGuard prompts the user when a navigation security event has occurred.

Securing Outlook Web Access from Session Inactivity Security Events

Messageware TimeGuard provides important Outlook Web Access security features to protect users' OWA sessions from unauthorized access. TimeGuard extends the security provided by ISA and forms based authentication (FBA) to offer total protection for OWA users.

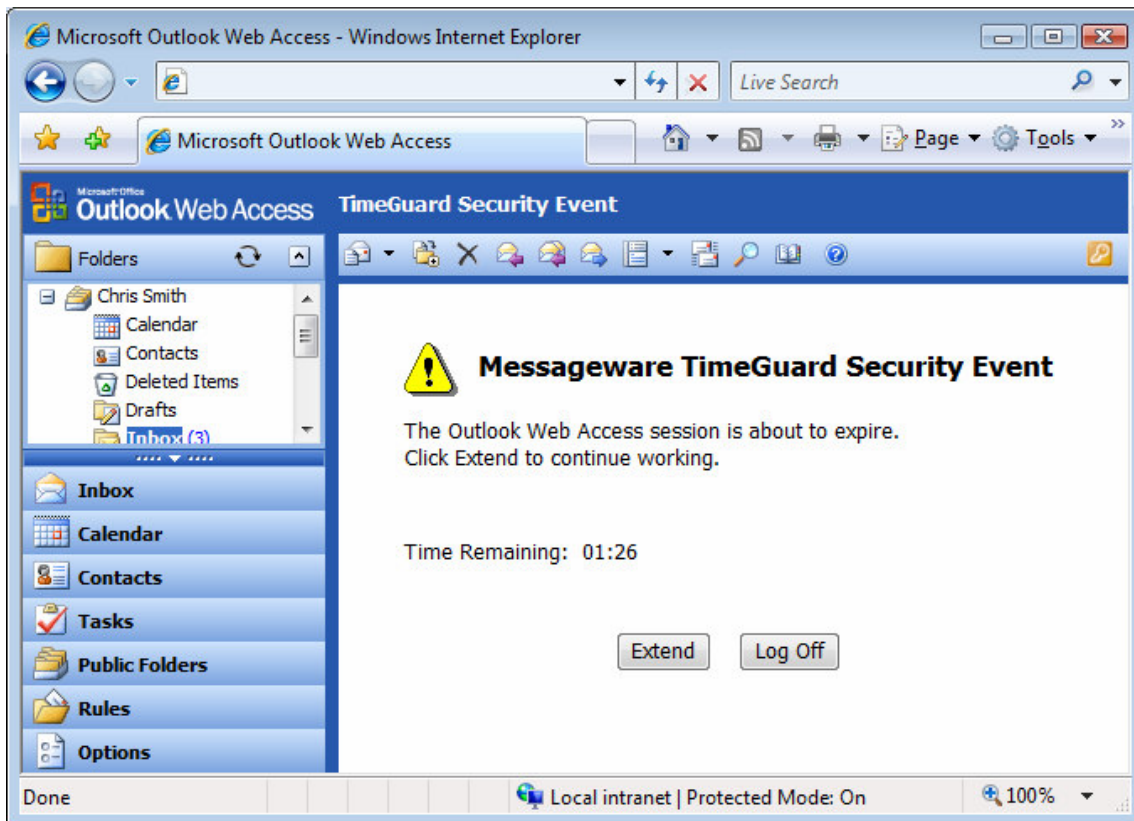
Customizable settings - Exchange System Administrators can customize session inactivity prompts at a very granular level, according to user role, user hardware or IP address.

User-friendly prompts - TimeGuard provides a user-friendly prompt shortly before the user reaches the session inactivity limit, giving him the option to either extend the session or logoff.

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



When an active OWA session is reaching its predefined session inactivity period, the user is prompted with the option to extend the session or logoff. After a maximum session limit has been reached, the user is prompted that the session will automatically logoff and they will need to login again to continue using OWA.



Appendix 1: Testing for Security Events in OWA with ISA Server Installed

The following tests that demonstrate scenarios where additional security protection is required even when ISA Server is running. The following tests demonstrated the security vulnerabilities for companies running the following environments:

- Exchange Server with ISA Server 2006
- Exchange Server with ISA Server 2000 with popup blocker enabled
- Exchange Server with ISA Server 2004 with popup blocker enabled

Test 1:

Step 1:	Log on to OWA
Step 2:	Navigate to another web page by entering the URL of the page in the address bar of the browser
Step 3:	Press the back button
Result:	The user returns to the active OWA session without being required to re-authenticate

Test 2:

Step 1:	Log on to OWA
Step 2:	Navigate to another web page by entering the URL of the page in the address bar of the browser
Step 3:	Click on the drop down menu of the address bar to view the history of visited sites. Select the OWA session
Result:	The user returns to the active OWA session without being required to re-authenticate

Test 3:

Step 1:	Open up a new web browser window (browser shows home page)
Step 2:	Log on to OWA
Step 3:	Press the back button of the browser
Step 4:	Press the forward button
Result:	The user returns to the active OWA session without being required to re-authenticate

Copyright

The information contained in this document represents the current view of Messageware Incorporated on the issues discussed as of the date of publication. © Messageware Incorporated 2007

Messageware is the world's leading provider of solutions that enhance and secure Microsoft Office Outlook Web Access. Our award-winning products are used by thousands of the world's most successful organizations and over 4 million users. Founded in 1993, Messageware is a long standing Microsoft Gold Certified Partner and a Global Exchange ISV. For more information visit www.messageware.com



OWA Suite

Comprehensive Outlook Web Access Productivity and Security

Request your free trial of the Messageware OWA Suite including NavGuard and TimeGuard by visiting

http://www.messageware.com/free_trial.htm

or call 905.812.0638 x2