

Outlook Web Access Authentication and The Log Off Myth
By Mark Rotman, Messageware Incorporated



Recently there has been a lot of discussion on newsgroups and forums regarding what level of protection the Log Off button in OWA for Exchange provides. This briefs will dispel the myths and highlight the issues regarding the Log Off button and its use.

Part I of this brief reviews how Internet Browser authentications work and how credentials for Exchange OWA are validated. Part II focuses on the Log Off Buttons in OWA for Exchange 5.5 and 2000.

Part I. The Log Off Myth

First and very importantly, users view the Log Off button in OWA as a security method for “disconnecting” from and securing their email. Users expect that accessing OWA after a Log Off will require entry of their password. Unfortunately, the Log Off button has provided users a false sense of security. The following authentication review is intended to provide insight into the security methods used by Exchange.

Authentication Review

Exchange supports two authentication modes, BASIC and INTEGRATED. Basic Authentication transmits the userid and password on every request. The userid and password are encoded, but not encrypted. Implementing HTTPS (SSL) will encrypt the encoded userid and password making the password exchange secure. Integrated authentication (NTLM) initially negotiates and generates a token using a hash algorithm and does not transmit the password over the connection. All subsequent requests do not require authentication.

The first time that the browser requests OWA ([\\server\exchange](http://server/exchange)) it attempts an Anonymous access. The Server responds with an Access Denied and possible authentication methods (Integrated, Basic, or both). This causes the browser to prompt the user for a userid and password. The userid and password are stored in the Browser cache for subsequent use against the server.

Web Browsers and Servers are designed to optimize the number of times that a user is prompted for credentials. The client-server design of Basic and Integrated Authentication schemes do not provide for the server to invalidate or clear the credentials that have been cached on the browser. Hence it is very difficult for the server to know whether the credentials (userid & password) are originating from the cache or from an

actual user prompt. **There are no server commands that universally clear the cached password from a browser.**

Log Off in Exchange 5.5 and 2000

Unfortunately, the way that these authentication schemes are architected and implemented, hitting the Log Off button in Outlook Web Access may not protect, secure, or reduce your exposure to intentional or accidental access, leaving your users exposed.

Part II: Is Your Log Off Button Exposing You?

Outlook Web Access in Exchange 5.5 and Exchange 2000 are very different from each other. Exposures due to the Log Off button have different manifestations in each of these systems. There are additional differences based on the browser and client Operating System that are used. However, the underlying issue is that the cached credential from the last HTTP session with each server remains for the life of the browser application, which can leave a users email exposed to unauthorized access.

Log Off in Exchange 5.5 OWA

In OWA 5.5, there are two sessions established: an ASP session that maintains state and mailbox information and a HTTP session associated with userid and password credential. Clicking the Log Off button abandons the ASP session, but does not affect the HTTP session or the cached credential. Access to an OWA mailbox without entering a password is possible.

Access from Netscape

When connecting to OWA 5.5 after a Log Off, entering the Mailbox name will establish an ASP session and the Server's response places Netscape into an authentication mode for HTTP. Netscape automatically attempts the cached credential. The server is unaware that the credential is from the cache and full authenticated access to the mailbox is restored.

Access from Internet Explorer

When connecting to OWA 5.5 after a Log Off, entering the Mailbox name will establish an ASP session and the Server's response places Internet Explorer into an authentication mode for HTTP. Internet Explorer will prompt the user for a new credential. If the user cancels the authentication prompt and performs a Reload, Internet Explorer automatically attempts the cached credential. The server is unaware that the credential is from the cache and full authenticated access to the mailbox is restored.

Log Off in Exchange 2000 OWA

In OWA 2000, there is only a HTTP session. Clicking the Log Off button returns a warning page to the user indicating the need to close all browser windows and exit the browser application. Completely exiting the browser application normally clears the HTTP session and the cached credential. Unfortunately there are circumstances where the user cannot or does not exit the browser application. It is in these cases that cached credentials can remain and full authenticated access to the mailbox can be restored.

Cached Credential Exposure

The cached credential from the HTTP session in OWA 5.5 or OWA 2000 can remain and expose your mail system when any of the following situations occur:

- When the browser application is not completely terminated. Many users use Windows Explorer / My Computer (explorer.exe versus iexplorer.exe) to navigate locally and to the Internet. This can result in the cached credential remaining after all applications are closed.
- When all browser windows cannot be closed due to desktop security policies. This security setting is more common on machines where the intended use is browser-only access, such as kiosks.
- When the browser application does not exit after all browser windows are closed. On the Macintosh, users must manually perform additional procedures to completely halt the execution of a browser.
- When the browser is navigated or redirected to a new web site. When users click a link on the desktop or in an application, the browser may be directed to another web site. This new site replaces the OWA interface and access to the Log Off button. Users may not realize that their mail session is still active.
- When users do not close all browser windows. A minimized child window, such as Compose Message, can be easily missed on a busy desktop where another window is maximized.

Testing the OWA Exposure

There are Security Audits for OWA 5.5 and OWA 2000 that contain the specific tests for cached credential exposures. The audit documents are available at www.messageware.com/products/audit.html.

Dealing with the OWA Exposure

To handle Exchange authentication, additional work must be performed to ensure that authentication occurs following a Log Off. Today there are Microsoft Partners that have delivered solutions to the market that handle this problem. One solution, SecureLogoff from Messageware, is a software based solution that integrates into Exchange and IIS to ensure that authentication occurs following a Log Off or Timeout.

#####

About Messageware

Messageware Incorporated is a leading Microsoft Exchange OWA add-on products and consulting organization that is focused on e-mail and messaging based products. For more information about Messageware, please visit www.messageware.com.