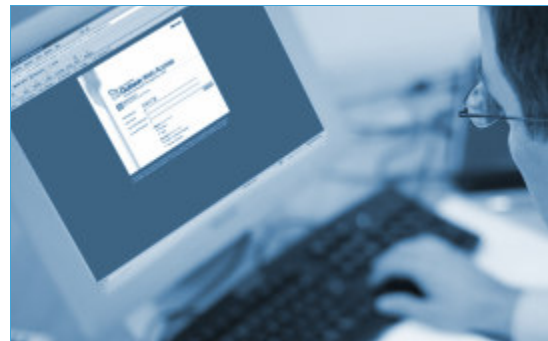


Deepnet Unified Authentication

Securing Microsoft Outlook Web Access

A common challenge for enterprises in today's business world is allowing employees access to their company email accounts from any location while maintaining strong security. Many enterprises have deployed Microsoft Outlook Web Access (OWA) providing a Web-based email system that can be accessed from any machine with just a web browser. The problem is that OWA offers minimal security as it only relies on the single-factor authentication - password - which can be easily compromised.

Adding a strong authentication to an OWA deployment provides enterprises with a secure email system. Unfortunately, most existing strong authentication solutions require additional hardware devices such as smart cards, USB keys or One-Time Password (OTP) hardware tokens, which are expensive to implement, deploy, manage and very inconvenient to the users.



Deepnet Unified Authentication Platform for OWA is a two-factor authentication solution designed specifically for securing outlook web access, without the requirements of new hardware devices. Deepnet Unified Authentication Platform utilizes the devices users already have (computers, mobile phones, PDA etc) or the user's behavioural biometrics (typing pattern, voiceprint), as the second factor. This eliminates the need to distribute new hardware, making the system cost effective, user friendly and simple to manage.

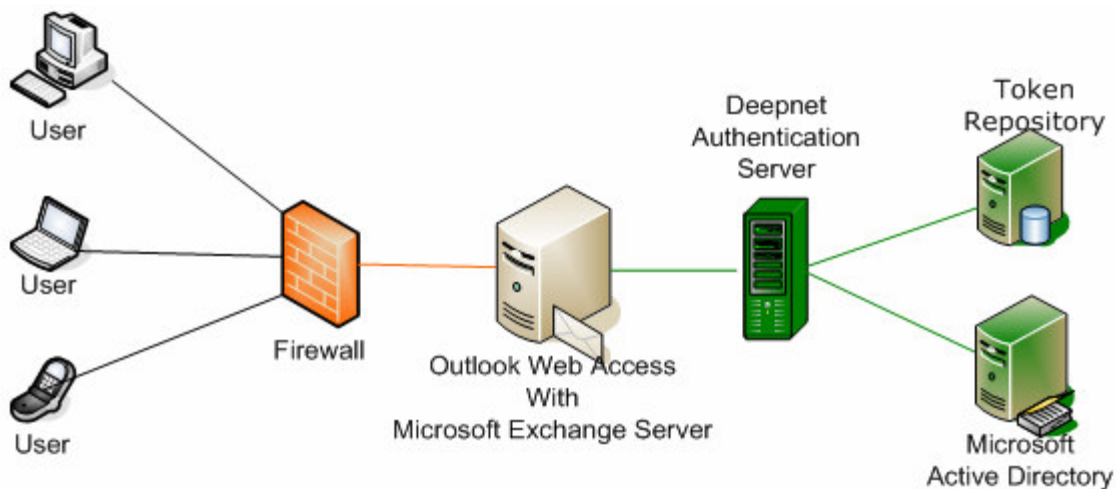
The screenshot shows the Microsoft Outlook Web Access login interface. At the top right is the Microsoft logo. The main heading is "Microsoft Office Outlook Web Access" with the subtext "Provided by Microsoft Exchange Server 2003". Below this is a section titled "Authentication by Deepnet Security" with a logo. The login form includes fields for "User Name" (j.smith), "Authenticator" (Mobile Pass), "One-Time Password" (543964), and "Account Password" (masked with asterisks). A "Log On" button is to the right of the password field. Below the form are radio buttons for "Public or shared computer" (selected) and "Private computer". A "Security (what's this?)" link is also present. At the bottom, a note states: "To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again."

Key Benefits

- Provides a secure and easy to use authentication solution for mobile workers.
- Ensures ease of deployment with a zero footprint authentication solution.
- Enforces positive user identification of mobile workers.
- Eliminates password-only related vulnerabilities.
- Manages user account centrally through the Management Console.
- Improves productivity for mobile workers without compromising security.

Technical Overview

Deepnet Unified Authentication Platform for OWA consists of the Deepnet Authentication Server, Token Repository Server and Microsoft Active Directory Server, as illustrated below.



These servers can be installed and operating on separated machines or on a single machine, depending on the scale of the customer's business applications.

Deepnet Authentication Server

Deepnet Authentication Server is a secure, scalable, cross-platform authentication server that centrally controls access to web applications. Deepnet Authentication Server is designed to be deployable across a wide range of commonly available platforms that supports Java. Therefore, it can run on Windows, Linux, Unix, Sun OS and many mainframes.

Token Repository

Deepnet Authentication Server uses a SQL database server as its token repository. It can be connected to the customer's existing SQL server (MS-SQL 2000/2003, Oracle) or MySQL server which is included in its installation package.

Active Directory

Deepnet Authentication Server supports assignment of tokens to users residing in Active Directory without modification of the directory schema. User data is not imported from the directory into Deepnet Authentication Server. Instead, Deepnet Authentication Server queries the directory during the authentication process to validate the user's status. Changes made in the directory are automatically and immediately reflected in Deepnet Authentication Server.

Authentication Methods

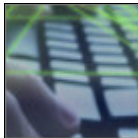
Deepnet Unified Authentication Platform supports several authentication methods including mobile phone based one-time password token, device based soft token, virtual smart card and software-only behaviour biometrics.



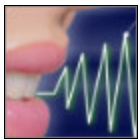
Mobile 2x2 is a one-time password token application. It is a small J2ME application downloadable to any Java enabled mobile phones, including Windows Mobile, RIM Blackberry, Symbian OS and Palm OS. Mobile 2x2 also supports Windows desktop. Its Desktop Edition runs on Windows 2000/XP and Windows Mobile.



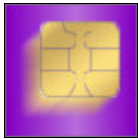
Mobile Pass is also a one-time password solution. While Mobile 2x2 generates one-time password offline, Mobile Pass delivers one-time password in real time via SMS, email or voice over the phone. Mobile Pass works with any mobile phone.



TypeSense. Based on the Keystroke Dynamics science, TypeSense accurately identifies users by their "type prints" - the unique patterns they type characters across a keyboard. TypeSense requires no hardware and no software installation.



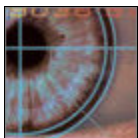
VoiceSense is a text and language independent biometric speaker verification system that also requires no hardware and no software installation. Voice can be received from the user's mobile phone, landline telephone or computer microphone.



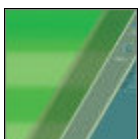
Smart ID is a virtual smart card in a software form factor, providing the same advanced security functionality as physical smart cards, but at only a fraction of the cost. Smart ID is fully compliant with PKI architecture with supports of PKCS #11 and MS-CAPI. Smart ID is available for Windows 2000/XP and Windows Mobile.



Device Pass is a software-based two-factor authentication solution based on patent-pending device fingerprinting technologies. Device Pass client is available for Windows 2000/XP and Windows Mobile.



Remote 2x2 is a remote two-factor authentication solution that requires no hardware and no software installation. All the user needs is a standard web browser such as Internet Explorer, Firefox or Safari for Mac OS.



Smart 2x2 is a smart device token that requires a browser plug-in. Smart 2x2 is natively supported by Deepnet Explorer web browser, and its plug-in software is available for Internet Explorer and Firefox for Windows.