



**Deepnet Unified Authentication
for Outlook Web Access
User Guide**

**Copyright 2006,
Deepnet Security Limited.**

Trademarks

Deepnet Unified Authentication, MobileID, QuickID, PocketID, FlashID, SmartID, TypeSense, VoiceSense, MobilePass, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer

This document is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
The Maples Business Centre
144 Liverpool Road
London, N1 1LA
United Kingdom

Tel: +44(0)20 7700 4282
Fax: +44(0)20 7697 8282
www.deepnetsecurity.com
support@deepnetsecurity.com

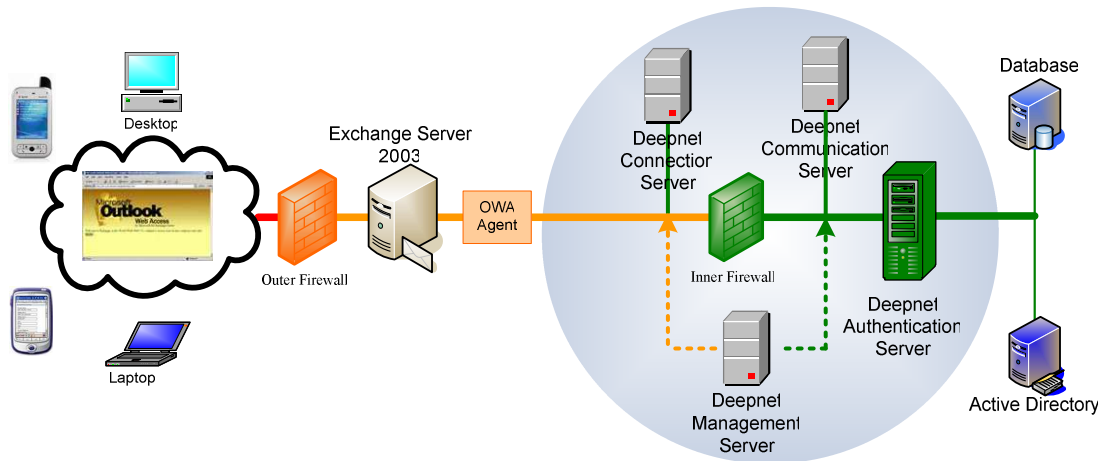
Table of Contents

Overview	3
Installation	4
Installation Prerequisites.....	4
Installation Procedure.....	4
Configuration	5
Configure Exchange Server	5
Configure Authentication Platform.....	6
Configure OWA Agent.....	6
Authentication	9
Limitation	10

Overview

Microsoft Outlook Web Access (OWA) is the component of the Microsoft Exchange server that provides email access from Web browser over the Internet. Deepnet Unified Authentication for OWA enables strong two-factor authentication for the Microsoft OWA 2003 Logon form, requiring a user to authenticate with a second factor credential such as one-time password before access to email is allowed.

Deepnet Unified Authentication for OWA is one of many enterprise solutions that the Deepnet Unified Authentication Platform supports. The following diagram illustrates the typical components involved in the Deepnet Unified Authentication for OWA solution:



The complete solution consists of the following components:

- Deepnet Unified Authentication Platform
- OWA Agent

OWA Agent acts as the bridge that connects the Microsoft Exchange Server and the Deepnet Authentication Server.

Installation

Installation Prerequisites

- Deepnet Unified Authentication Platform installed and registered. Please refer to the User Guide of the Platform for details.
- Microsoft Exchange Server 2003 installed and operational.

Installation Procedure

Deepnet Unified Authentication for OWA should only be installed after the Deepnet Unified Authentication Platform has been successfully installed and operational.

Deepnet Unified Authentication for OWA should be installed on the machine on which the Microsoft Exchange Server 2003 is installed and operating.

To install the Deepnet Unified Authentication for OWA, simply launch the installer "SetupOWA.exe" and follow the on-screen instruction.

Configuration

After the successful installation of Deepnet Unified Authentication for OWA (the Authentication Agent), you need to configure the following components:

- Exchange Server
- Authentication Platform
- OWA Agent

Configure Exchange Server

Deepnet Unified Authentication for OWA only supports the form-based logon authentication. Therefore the Exchange Server 2003 should be firstly configured to enable the form-based authentication.

Enabling forms-based authentication

You must enable Secure Sockets Layer (SSL) on the server before you enable forms-based authentication. For more information about how to install a certificate in Microsoft Windows Server 2003 before you enable SSL, click the following Microsoft Knowledge Base article:

How to install imported certificates on a Web server in Windows Server 2003
<http://support.microsoft.com/kb/816794/>

To enable forms-based authentication in Exchange 2003, follow these steps.

Note: In a front-end/back-end server environment, you must enable forms-based authentication only on the front-end server. Do not enable forms-based authentication on the back-end server. In an environment where you do not use a front-end server, enable forms-based authentication on the mailbox server.

1. Start Exchange System Manager.
2. If administrative groups are enabled, expand **Administrative Groups**.
3. Expand **Servers**, and then expand your front-end server.
4. Expand **Protocols**, expand **HTTP**, right-click **Exchange Virtual Server**, and then click **Properties**.
5. Click the **Settings** tab, and then click to select the **Enable Forms Based Authentication** check box.
6. In the **Compression** list, click the level of compression that you want.

Note: We recommend that you do not enable compression in a single-server environment because compression in a single-server environment places an additional load on the server.

7. Click **OK**.
8. If you receive a message that states that the IIS service must be restarted, click **OK**. To restart IIS, type the following command at a command prompt:
iisreset

If you enabled forms-based authentication on a front-end server, follow these steps on your back-end servers:

1. Start Exchange System Manager.
2. If administrative groups are enabled, expand **Administrative Groups**.
3. Expand **Servers**, and then expand your back-end server.
4. Expand **Protocols**, expand **HTTP**, and then expand **Exchange Virtual Server**.
5. Right-click the Exchange virtual directory that appears under the **Exchange Virtual Server** container, and then click **Properties**.
6. Click the **Access** tab, and then click **Authentication**.
7. If it is not already selected, click to select the **Basic authentication** check box.
8. Enter a backslash (\) in the **Default Domain** box.
9. Click **OK** twice to close the property windows.

Configure Authentication Platform

Deepnet Unified Authentication Platform can support multiple applications. Depending on your company's IT infrastructure and security policy, you may set up different applications for different types of access. For instance, one application for VPN remote access, one for Windows logon and one for OWA. You can, of course, set up just one application for all types of access.

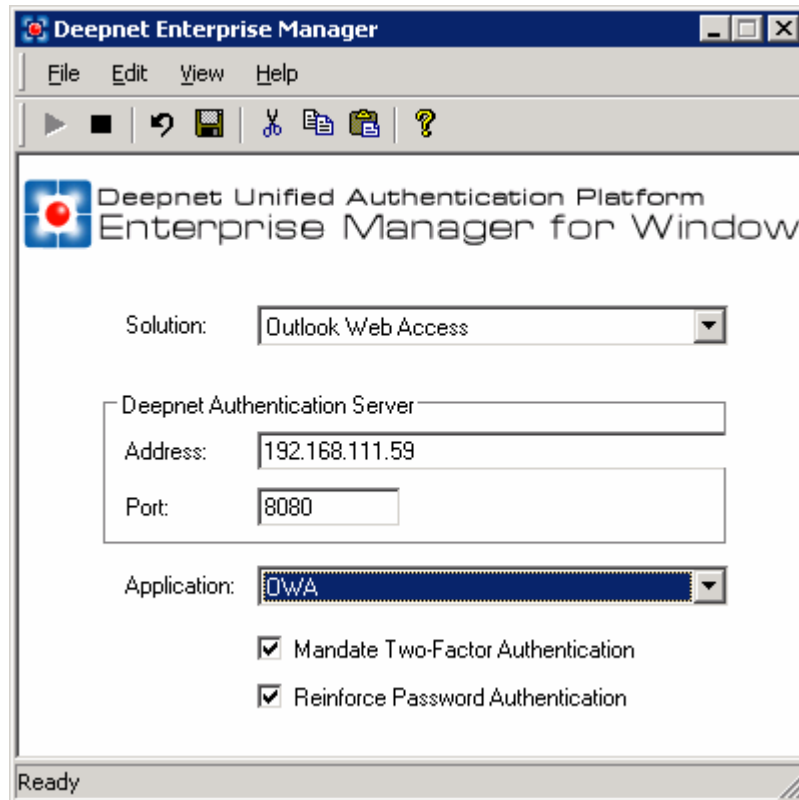
Once the application for OWA has been added to the Authentication Platform, you will then need to add to the application those users who are required to be authenticated with two-factor authentication. Each user should be allocated one or more authentication token(s) such as MobilePass and/or Mobile2x2.

Please refer to the user guide of the authentication platform for details of how to set up the application, create users and tokens.

Configure OWA Agent

The OWA Agent needs to be configured so that it is connected to the authentication server and the application for OWA. In addition, there are options that help enforce your security policy.

The configuration tool for the OWA Agent is part of the Deepnet Enterprise Manager which is a management tool for all solutions including Windows Logon, OWA and other enterprise solutions that Deepnet supports.



Basic Configuration

1. Click the "Solution" dropdown list and select "Outlook Web Access".
2. Enter the Address and Port of the authentication server.
3. Click the "Application" dropdown list and select the application that you have set up for OWA. (In the above screenshot, the sample application is named OWA).

Mandate Two-Factor Authentication

Deepnet Unified Authentication for OWA supports the concurrent use of both legacy Microsoft static password protection and Deepnet's strong two-factor authentication, for different users within the domain. This enables a staged migration of users to two-factor authentication in your organisation, as/when convenient and appropriate.

The "Mandate Two-Factor Authentication" option applies to users who have not been added to the OWA application. If this option is **not** checked then those users who have **not** been added to the OWA application will **not** be required to authenticate themselves to access OWA. If the option is checked then everyone will be mandated to authenticate themselves with two-factor authentication.

Note: Users added to the OWA application are mandated to use two-factor authentication regardless whether or not the “Mandate Two-Factor Authentication” option is checked.

Reinforce Password Authentication

If this option is checked then the authentication agent always verifies the static password first before asking for the second factor authentication.

If the company offers MobilePass tokens to its users, it is recommended that this option should be enabled.

If this option is enabled, you need to make sure that either your OWA application is connected to the Active Directory or each user has been given a static password in the authentication server. In latter case, the user’s login name and password have to be the same as their Windows login name and password.

Save Settings

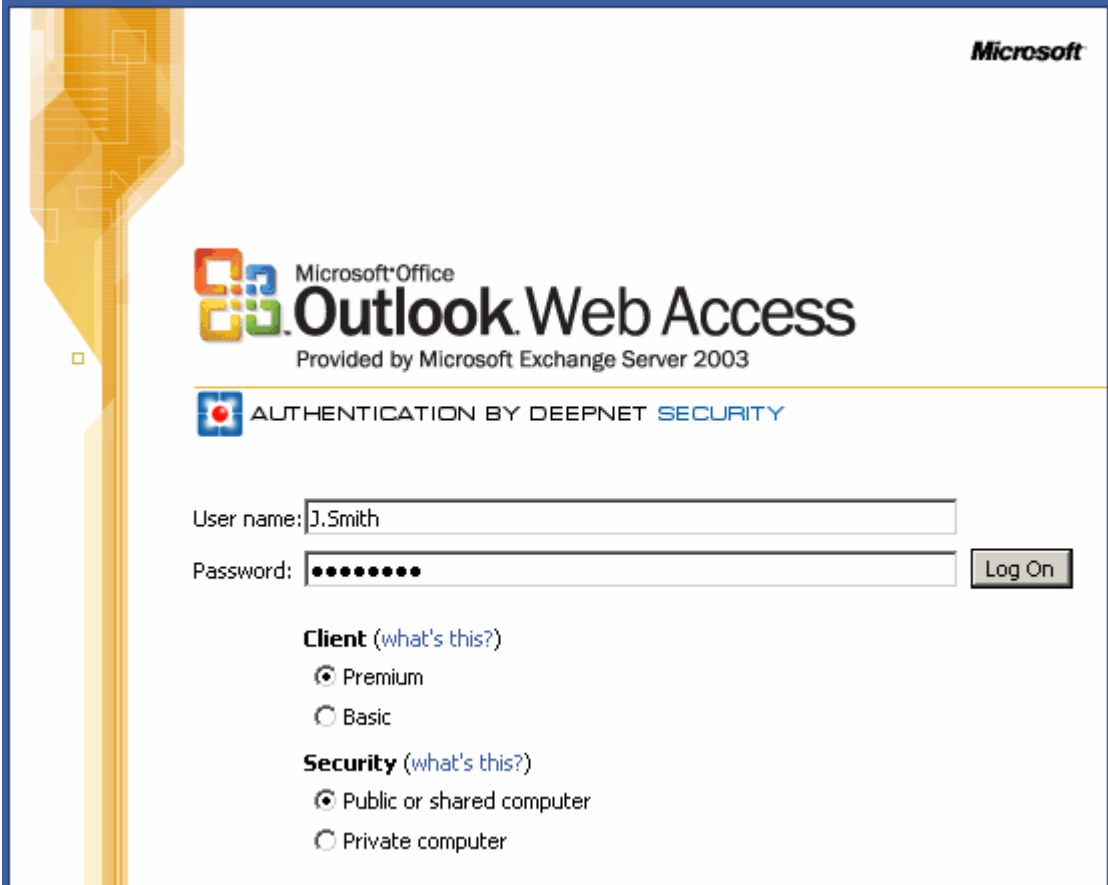
Click the “Save” button  to save your settings.

Authentication

The process of the Two-Factor authentication for OWA logon goes through two screens: the first-factor authentication and the second-factor authentication.


The First-Factor Authentication

The first-factor authentication is the same as the traditional static password authentication in which the user is asked to enter their user name and windows account password.



Microsoft

Microsoft Office
Outlook Web Access
Provided by Microsoft Exchange Server 2003

 AUTHENTICATION BY DEEPNET SECURITY

User name:

Password:

Client ([what's this?](#))

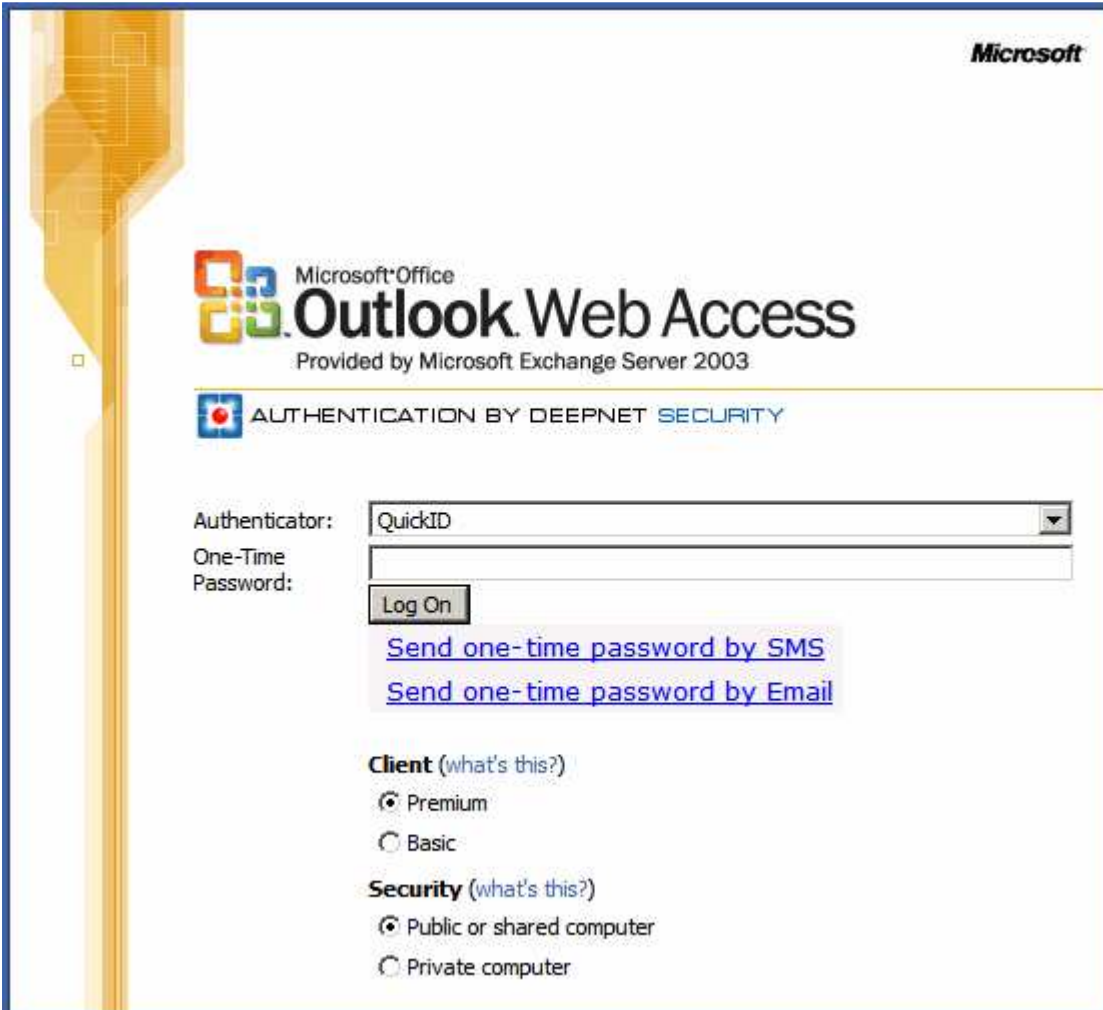
- Premium
- Basic

Security ([what's this?](#))

- Public or shared computer
- Private computer

The Second-Factor Authentication

The second-factor authentication asks the user to provide the credentials generated from their token, such as, an one-time password.



The screenshot shows the Microsoft Office Outlook Web Access login page. 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 banner for "AUTHENTICATION BY DEEPNET SECURITY". The authentication form includes a dropdown menu for "Authenticator" set to "QuickID", a text input field for "One-Time Password", and a "Log On" button. Below the form are two links: "Send one-time password by SMS" and "Send one-time password by Email". At the bottom, there are two sections: "Client (what's this?)" with radio buttons for "Premium" (selected) and "Basic", and "Security (what's this?)" with radio buttons for "Public or shared computer" (selected) and "Private computer".

Limitation

Currently, Deepnet Unified Authentication for OWA only supports one language, English.