

Deepnet Unified Authentication for 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 for Outlook Web Access 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.

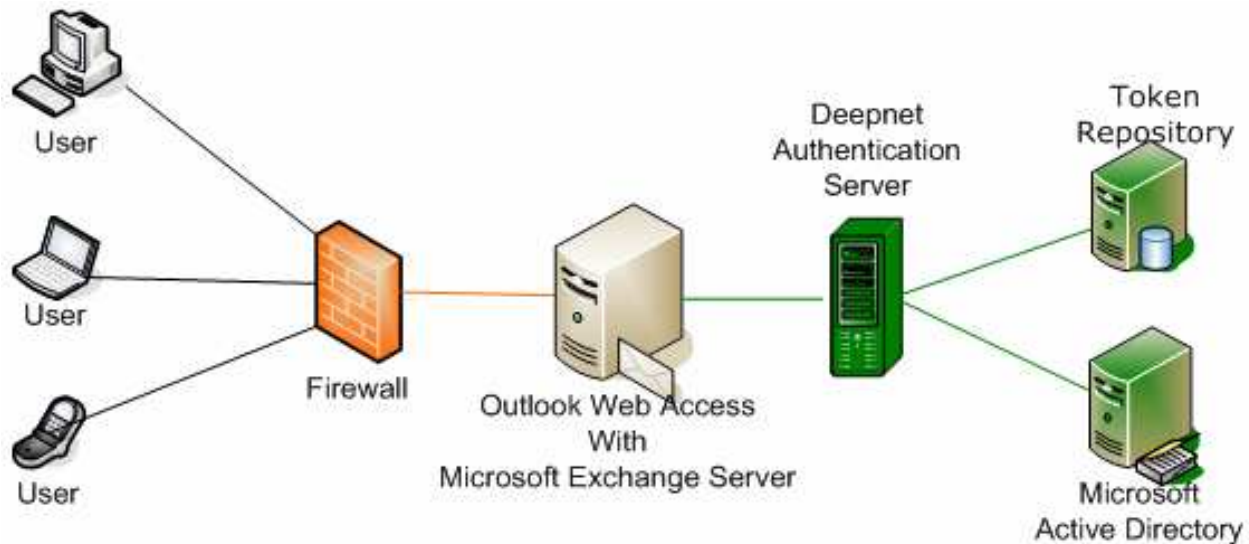
KEY BENEFITS

- 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.
- Offers flexible choices of authentication credentials and tokens.
- Unifies authentication for all enterprise applications with a single platform.

Technical Overview

Deepnet Unified Authentication for Outlook Web Access consists of the following major components:

- Deepnet Authentication Server
- Token Repository Server
- Microsoft Active Directory Server



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.