

BENEFITS:

- Increased productivity for a mobile workforce
- Strong authentication for everyone using Outlook Web Access
- Simple, secure and easy to use for mobile employees
- Strong two-factor authentication
- Combined authentication methods for a convenient and flexible user experience
- Ease of deployment with no user software installation
- Eliminates “password only” vulnerabilities
- Simplified management of user accounts
- The most affordable solution available
- Same A-Key token will work in conjunction with an entire suite of security applications

Strong Authentication for Microsoft® Outlook® Web Access

Problem:

A common challenge for enterprises in today’s business world is allowing employees access to their company email accounts while maintaining strong security. Employees want to check their business email from any location that business sends them and a successful business offers them that capability. The availability of the Internet and the integrated nature of the Microsoft Outlook Web Access (OWA) application to an exchange server make providing access to employees’ email accounts a simple procedure. Providing strong security against everyone on the internet who can visit your OWA login page is the problem.

Solution:

The Authenex Strong Authentication System (ASAS®) provides simple and secure Outlook Web Access to a company’s exchange server for a convenient user experience. ASAS is a two-factor authentication solution that utilizes the Authenex A-Key token for security far beyond password only solutions that are inherently vulnerable to attacks. The ASAS two-factor authentication

process is based on identifying a user by something they have (the A-Key) and something they know (a PIN) – just like a bank ATM card system. Anyone who visits the company OWA page will need to use both factors to gain access.

From any web browser in any location in the world, a user can securely view their incoming email and send messages from their company account. Users will generate a One-Time Password (OTP) from the A-Key and enter it along with their PIN. Each time an OTP is generated, it is a unique value that cannot be used again. Every session will require a unique OTP value so that even if someone were monitoring the login process, they would not be able to use that login information again. The A-Key is a hybrid token that also contains a USB interface. A user is given added flexibility with the ability to insert the A-Key into the computer’s USB port and authenticate to the OWA application with their PIN. This USB functionality is “driverless” without any need to install software on the computer that’s being used and leaves zero footprint upon removal.