



DATA SHEET



Securing Microsoft® Outlook Web Access with VeriSign Unified Authentication

Email is an integral part of the enterprise DNA, used for making business decisions minute by minute on a worldwide basis. Microsoft Exchange and Microsoft Outlook is the most widely deployed email server application. As more and more enterprise employees work remotely, from home offices or from mobile locations, the need for reliable and secure email access is growing.

To enable remote access, many companies have deployed Virtual Private Networks (VPN) which add an additional layer of complexity to network security, are often unstable, and require installation and maintenance of VPN clients on remote users' computers. Some enterprises have deployed SSL VPNs which do not require installing or maintaining clients, but still require an additional network layer. An alternative to VPN or SSL VPNs, that leverages an enterprises' existing Exchange environment is Microsoft® Outlook Web Access (OWA). With OWA, enterprises have the option to deploy a Web-based version of Outlook that can be accessed from any machine with a web browser. However, while OWA addresses the complexity of remote access, it still relies on single-factor authentication - username and password - for secure logon. Adding VeriSign Unified Authentication and the VeriSign One-Time Password (OTP) token to an OWA deployment provides a secure, second-factor of authentication to your remote email application, while easing complexity at the network level and providing ease of use for remote users.

VeriSign® Unified Authentication reduces the complexity and cost of strong authentication by providing a single, highly scalable platform for managing all types of two-factor authentication credentials. The VeriSign One-Time Password Token enables strong authentication through an easy-to-use and highly cost effective token that complies with the OATH standard and comes with a full warranty.



Where it all comes together.™

+ Leverage Your Existing Technology Investments

VeriSign Unified Authentication is a single, integrated platform that can manage multiple user credential types such as OTP tokens. By leveraging key Windows backend components such as Microsoft® IAS server, Microsoft® Active Directory, and Microsoft® Management Console, Windows based enterprises do not have to invest in a different infrastructure to support two-factor authentication for their network access applications.

+ Flexible Deployment Options

VeriSign-hosted Validation. To ensure continuous availability, VeriSign Unified Authentication offers a validation service built on the proven VeriSign Domain Name System (DNS) infrastructure. All critical security components (e.g., OTP vault, Certificate Authority infrastructure, and PKI roots) reside on the DNS network, and all functions (e.g., OTP and digital certificate verification) are executed there. The globally distributed DNS network has a fully redundant infrastructure with 24/7 service support and 99.999 percent uptime, enabling services to leverage the VeriSign infrastructure to deliver superior availability. This option scales smoothly from hundreds to millions of users, ensuring high performance and allowing enterprises to deploy strong authentication on an as-needed basis.

In-premise Validation Engine. VeriSign also offers an in-premise validation solution for enterprises. This in-premise validation module is built with the same technology as VeriSign-hosted Validation. Enterprises will be able to utilize the VeriSign highly scalable validation software and the single, integrated management platform, which leverages an enterprise's existing infrastructure while providing uncompromised reliability and scalability.

+ Full Administrative Control

VeriSign Unified Authentication includes a Web-based management console that automates user enrollment and consolidates credential provisioning and lifecycle management. Administrators can issue, revoke, renew, recover, and audit OTP from a single, unified interface. Enterprises maintain full control over internal security policies and user information. All user identities, credential templates, and authorization policies remain within the enterprise directory under the strict supervision of the enterprise. VeriSign never views or stores enterprise data.

Self-Service Applications

The built-in VeriSign Unified Authentication self-services help minimize support costs by enabling users to perform most lifecycle operations on their own. Users can access self-service applications through either of the following user interfaces:

- Web interface. Enables users to access self-service applications through a Web interface to enterprise-hosted token management services.
- Programming interface. To enable the integration of the user self-services into existing user portal or existing customer support applications, VeriSign also provides an integration SDK.



DATA SHEET

Besides issuing new credentials, OTP token activation, and certificate auto-enrollment, the self-service applications enable users to:

- Synchronize a token
- Replace a lost or broken token
- Enroll for new certificates or renew existing one

Visit us at www.Verisign.com for more information.

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," TeraGuard, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

10-25-2005