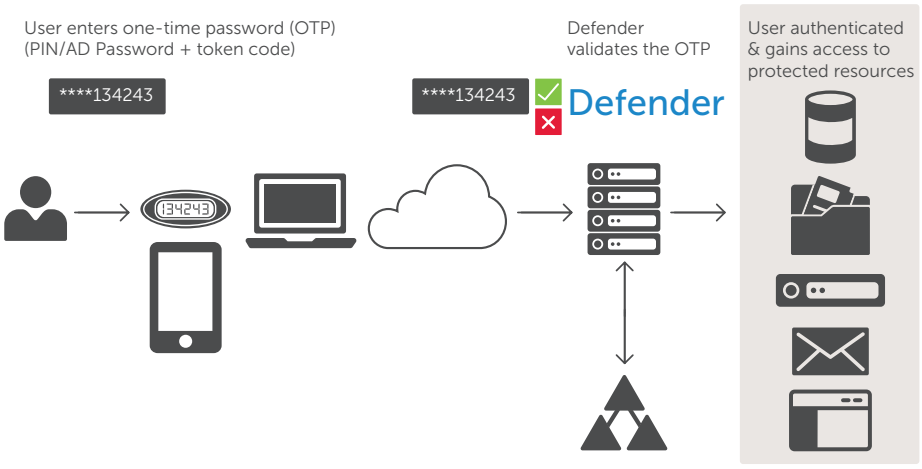
Defender®

Protect your perimeter with two-factor authentication

Today, compliance and security demands are moving organizations to levels of security beyond the traditional username and password. Two-factor authentication—combining "something you have" (for example, a token) with "something you know" (a username and password)—has quickly moved to the forefront of most organizations' security and compliance initiatives. Traditionally two-factor authentication solutions have been costly to deploy and were based on proprietary interfaces and directories. However, Defender® is entirely standards-based (OATH, RADIUS, LDAP, PAM, etc.) and utilizes Active Directory (AD) for administration and identity management. Using AD not only enhances security and scalability but also saves money by enabling current personnel to manage Defender.

In addition, Defender enables users to easily request and securely self-register hardware and software tokens, reducing the costs and time normally involved in rolling out two-factor authentication. Defender supports any OATH-compliant hardware token and offers numerous software- and web-based tokens as well. By using organizations' existing infrastructure investments, providing user self-registration and supporting multiple token types, Defender enables organizations to increase security and compliance measures in a flexible, cost-effective manner.



Defender leverages an organizations' existing infrastructure investments to increase security in a flexible and cost-effective manner.

"BAA will save money because Defender tokens last at least 67 percent longer than our previous solution, and last for the life of the battery rather than having a vendor-defined lifespan of three years. We can renew users' tokens when they expire, as a help desk business-as-usual process, instead of issuing 7,500 tokens in one go and incurring the costs associated with running such a project."

Fiona Hayward
IT Programme Manager, BAA

Benefits:

- Heightens security through strong authentication for virtually any system or application
- Leverages the scalability, security and compliance of the Active Directory already in place
- Saves time and money through user token self-registration and the convenient renewal of user tokens as battery life expires (not vendor expiration date)
- Enables rapid help-desk response to user authentication issues from any Web browser
- Delivers standards-based flexibility by supporting any OATH-compliant hardware token
- Provides a comprehensive audit trail that enables compliance and forensics

System requirements

Defender hardware tokens

Defender supports any OATH-compliant token and distributes the following token types:

- Vasco DIGIPASS GO 6
- Vasco DIGIPASS GO 7
- Yubico YubiKey
- VeriSign® VIP Credentials

Defender software tokens

- Defender Soft Token for BlackBerry
- Defender Soft Token for iPhone
- Defender Soft Token for Android
- Defender Soft Token for Windows Mobile
- Defender Soft Token for Java
- Defender Soft Token for SMS
- Defender Soft Token for Email
- Defender Soft Token for Windows Desktop
- Defender GrIDsure Web-based token
- Defender Soft Token for Palm

For complete system requirements, click here.

Features

Active Directory-centric—Use the scalability, security and compliance of Active Directory to provide a two-factor authentication to any system, application or resource taking advantage of the corporate directory already in place, instead of creating an additional proprietary one. User token assignment is simply an additional attribute to a user's properties within Active Directory.

Web-based administration—Provide Defender administrators, help desk administrators and end users options for token management, token deployment, real-time log viewing, troubleshooting and reporting using the Web-based Defender Management Portal.

Token self-registration—Enable users to request a hard or soft token based upon policy defined by administrators, and then quickly and easily assign that token to the user's account through a secure mechanism.

Help desk troubleshooter—Enable Defender and help desk administrators to troubleshoot, diagnose and resolve user-authentication-related problems with just a couple of mouse clicks from any Web browser. View a current list of authentication attempts and routes, with associated results, possible reasons for failures and one-click resolution steps. In addition, view user account details and assigned tokens, with the ability to quickly test or reset the pin; provide a temporary token response; or reset or unlock the account.

Token flexibility—Deploy any OATH-compliant hardware token from your preferred token vendor. Defender also offers a wide range of software tokens for the most popular and widely deployed mobile platforms. A universal software token license makes it easy to reissue the appropriate device license when a user decides to switch mobile platforms.

Secure webmail access—Enable secure Web-based access to your corporate email system from any Web browser, anytime, anywhere, with Webthority, a reverse proxy solution included with Defender. In addition you can require Defender token use for access to ensure appropriate authentication regardless of access point.

ZeroIMPACT migration—Undertake a gradual migration to Defender from an incumbent legacy authentication solution with ZeroIMPACT. With Defender and the legacy system running side-by-side, all user authentication requests are directed to Defender. If the user is not yet defined within Defender, the authentication request is transparently passed, via the proxy feature, to the incumbent authentication solution. This approach allows administrators to migrate users to Defender as their legacy tokens expire.

Centralized administration—Integrate Defender with Active Directory and take full advantage of centralized management of directory information, through a common, familiar user interface. User token assignment is simply an additional attribute to a user's properties within the directory, which makes security administration more efficient.

Encryption—Secure communications by associating a management DES (Data Encryption Standard) with Defender Security Server. Defender supports AES, DES or Triple DES encryption.

Pluggable authentication module (PAM) —Specify that services and users defined on your UNIX/Linux systems will be authenticated by Defender with the Defender module for PAM.

About One Identity

The One Identity family of identity and access management (IAM) solutions, truly offers IAM for the real world including business-centric, modular and integrated, and future ready solutions for identity governance, access management, and privileged management.

One Identity
4 Polaris Way Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

Datasheet-Defender-US-CW-25672