



QUEST SOFTWARE

Quest® Defender

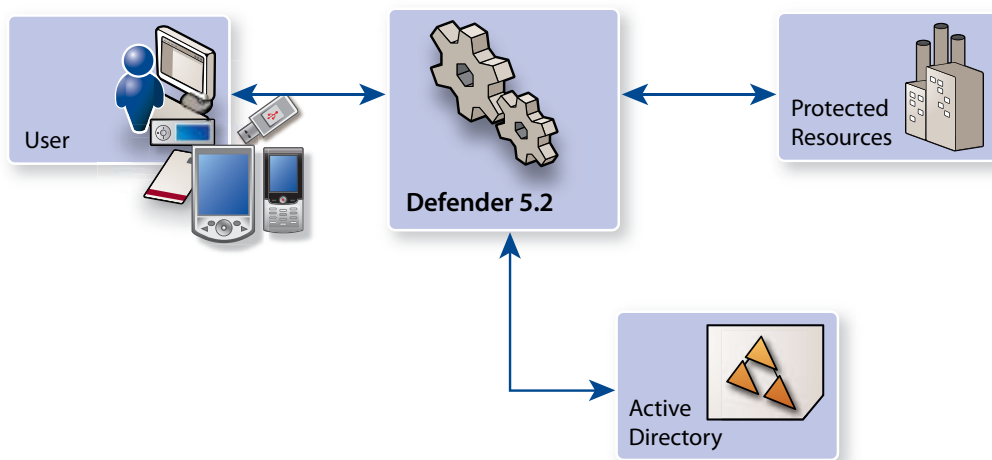
for Active Directory

Protects Your Perimeter with Strong 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 the “something you know” of usernames and passwords—has quickly moved to the forefront of most organizations’ security and compliance initiatives.

Defender, from Quest Software, provides just such a solution in an extremely flexible and affordable alternative. It is a critical component of any security infrastructure, adding strong authentication to your network, Web, and application based resources. Defender provides a unified, vendor neutral, fully scalable infrastructure that can grow and adapt with the ever-changing needs of your business.

Defender verifies authentication requests and enforces authentication policies across enterprise networks based on your existing investment in Active Directory and the identities, roles, and rules already present in that de-factor enterprise directory. Defender represents a revolution in security technology. It scales to accommodate the world’s largest networks while protecting enterprise-wide Virtual Private Networks (VPN), remote access, and e-business applications.



Defender provides a unified, vendor neutral, authentication infrastructure which can grow and adapt with the ever-changing needs of your business.

"A feature-rich product, easy-to-use and an excellent value for organizations of most sizes. We designate this product as our Best buy."

— Peter Stephenson,
Group Test – Multifactor Authentication,
SC Magazine

- Heightened security/maximum flexibility
- Active Directory-centric
- Token Agnostic
- ZeroIMPACT migration and deployment



Features

Active Directory-centric

Defender leverages the ubiquity of Active Directory and its scalability, security, and compliance to provide a two-factor authentication solution that applies to any system, application, or resource while integrating with, and taking advantage of, the corporate directory already in place.

Heightened Security/Maximum Flexibility

Defender provides strong authentication for virtually any access need on any required system or application. Its flexibility includes the ability to tier authentication, control where and how strong authentication is required, the ability for use self-registration, and full, secure encryption of data on the Defender server. The result is heightened security with low impact on operations.

Scalability and Performance

Defender offers a truly extensible architecture that is capable of scaling to fit your business needs. Defender has been deployed worldwide in organizations ranging from finance to high technology and from government to health care to name just a few. Defender is proven to deliver the highest levels of performance and availability.

User Authentication Wherever it's Required

Defender authentication can be used by your employees, business partners, and customers, whether they are local, remote, or mobile.

Whether they require access through VPN to remote access applications, wireless access points, network operating systems, intranets, extranets, Web servers, or applications, Defender's strong two-factor authentication ensures that only authorized users are permitted access.

ZeroIMPACT Migration

Defender's ZeroIMPACT migration strategy proved invaluable to security administrators. It allows organizations to undertake a gradual migration to Defender from an incumbent legacy authentication solution.

With Defender and the legacy system running side-by-side, Defender's RADIUS proxy feature enables administrators to direct user authentication requests 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 allows administrators to migrate users to Defender as and when their legacy tokens expire.

Centralized Administration

Defender has been architected to integrate fully with Active Directory. This integration leverages all the advantages of the centralized management of directory information, through a common, user-familiar interface.

User token assignment is simply an additional attribute to a user's properties within the directory, which makes the security administrator more efficient.

Two-Factor Authentication

Defender offers a truly flexible and cost-effective range of options to suit every requirement. With a vendor neutral position, Defender supports the widest range of tokens including mobile (SMS), smart cards, software, PDA, and USB hardware-based tokens.

Standards Compliance

Defender has been architected around the industry accepted standards of RADIUS, LDAP and OATH.

Security and Audit

Defender helps position your company in a forensics ready stance by maintaining a transaction log of all authentication activity, and providing a comprehensive audit trail for security administrators monitoring the enterprise.

Pluggable Authentication Module (PAM)

The Defender module for PAM allows you to specify that services and users defined on your Unix/Linux system will be authenticated by Defender.

Encryption

A Management DES (Data Encryption Standard) key is associated with the Defender Security Server and is used to ensure that communications are secure. Defender supports AES, DES, or TripleDES encryption.

Achieve compliance

Defender satisfies the requirements for access control and strong authentication while providing the ability to deliver required data to auditors. It allows you to “prove” compliance and remediate deficiencies with regard to access control and strong authentication.

Token Agnostic

Because it is entirely standards-based and through its legacy of strong relationships with all major token vendors, Defender provides a simple path to two-factor authentication regardless of the current solution in place or the preferred token vendor. It provides a more cost-effective alternative to, and simple migration path from, popular proprietary solutions

Defender Tokens

Defender supports any OATH-compliant token including the following token types:

- Authenex OATH Compliant Token
- ActivIdentity Series Token
- Defender DualTok Token (from ActivIdentity)
- Defender Go-3 Token (from Vasco)
- Digipass 260 Token (from Vasco)
- Digipass 300 Token (from Vasco)
- Defender One Token (from ActivIdentity)
- Defender Hand-Held Token (not sure of origin. These are very old)
- Defender Hand-Held Token Plus (not sure of origin. These are very old)
- Defender eToken Pro (from Aladdin)
- Defender eToken NG-OTP (from Aladdin)
- Defender eToken Pro Smart Card (from Aladdin)
- Defender USB Token (from Aladdin)
- Quest Desktop Token
- Defender Mobile
- ActivIdentity Key Chain Token

All token options provide strong two-factor authentication.

Defender WebMail

Defender WebMail is an add-on to Defender that gives secure Web-based access to your corporate e-mail system from any Web browser, anytime, anywhere—be it an Internet kiosk, café, client site, or home. All you need to carry is your Defender token and secure, appropriate authentication is ensured regardless of the access point.

About Quest Software, Inc.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 50,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at

www.quest.com.

© 2008 Quest Software Incorporated. ALL RIGHTS RESERVED. Quest Software and [product name(s)] are trademarks and registered trademarks of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.



www.quest.com
e-mail: info@quest.com
Please refer to our Web site for
international office information.