

## ***Defender 5: The Right Way to Prove, Identify and Establish Trust***

---

*Written by:  
Quest Software, Inc.*



**Technical Brief**

**© Copyright Quest® Software, Inc. 2008. All rights reserved.**

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

## **WARRANTY**

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

## **TRADEMARKS**

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
[www.quest.com](http://www.quest.com)  
e-mail: [info@quest.com](mailto:info@quest.com)  
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Updated—January, 2008



# CONTENTS

<b>INTRODUCTION</b> .....	<b>1</b>
<b>PROVING IDENTITY AND ESTABLISHING TRUST</b> .....	<b>2</b>
<b>TWO-FACTOR AUTHENTICATION</b> .....	<b>3</b>
THREE FACES OF TWO-FACTOR AUTHENTICATION .....	3
WHY IS TIME-SYNCHRONOUS BETTER? .....	4
ADDITIONAL BENEFITS TO CONSIDER .....	4
<b>CONCLUSION</b> .....	<b>7</b>
<b>ABOUT QUEST SOFTWARE, INC.</b> .....	<b>9</b>
CONTACTING QUEST SOFTWARE .....	9
CONTACTING QUEST SUPPORT .....	9

# INTRODUCTION

Before the Internet, business transactions were typically conducted face-to-face, so establishing your business partner's identity presented few problems. But in today's online transactions, recognizing a party trying to access your network resources is much more difficult.

To establish a connection and verify the identities of the parties taking part in a transaction, passwords or pass-phrases may be exchanged. Passwords do provide a degree of assurance of identity, but they can be easily compromised: they are written down, visually or electronically observed, or even coerced.

This technical brief explains how you can prove the identity of the other party in an e-transaction or exchange of information. It also describes why Quest's Defender is an excellent solution to help you accomplish this. Seamlessly integrated with Microsoft's Active Directory, Defender offers a truly extensible architecture that is capable of scaling to fit your business needs. Defender has been deployed around the globe in organizations within industries such as finance, technology, government, and healthcare. It is proven to deliver the highest levels of performance and availability.

# PROVING IDENTITY AND ESTABLISHING TRUST

We use a variety of methods to prove identity and establish trust:

- **Something you know**  
A secret password or pass-phrase associated with your name provides a degree of identification, but as we have seen, passwords alone cannot guarantee the identity of an individual.
- **Something you own**  
A physical device, such as a token, smart card, or USB keyfob, can also help identify you. One common example of this technology is the automatic teller machine (ATM) card.

Combining something you own with something you know (such as a personal identification number (PIN) or passcode) provides a much stronger level of authentication. The combination of something you know and something you own is often referred to as **two-factor authentication**.

- **Something about you**  
Something that is unique to you, such as your fingerprint or the pattern of your iris or your voice, adds a third factor to the equation. While these techniques may seem to border on science fiction, recent development in biometric technology are in fact producing working fingerprint, iris, and facial recognition security systems.

# TWO-FACTOR AUTHENTICATION

A single factor authentication, such as a remembered password, provides an inherently low proof of authenticity. But with the addition of the second physical proof, the certainty of authenticity increases exponentially.

Probably the most common example of two-factor authentication in use today is the ATM card. The combination of *something you own* (the card), and *something you know* (the PIN) provides sufficient authentication and proof of identity to permit access to bank services and funds.

The Defender solution is built on two-factor authentication. Each authorized user is issued a registered Defender token that generates a single-use passcode, typically every 60 seconds. The passcode is unique for that token and can be used only once. Defender, as the authentication server protecting the business infrastructure, validates the passcode and grants or denies access as appropriate.

It is impossible to predict the value of future codes, even if you were to record and analyze previous codes. So when a user supplies a valid code together with a password or PIN, there is a high degree of certainty that the person is a valid user.

## Three Faces of Two-factor Authentication

The IT professional community generally agrees that two-factor authentication is vital for effective network security. Two-factor authentication comes in three principal types:

### Challenge-Response (Asynchronous)

1. The user enters a username.
2. The server sends an eight-digit challenge.
3. The user enters his or her password or PIN and challenge into the token device.
4. A response is displayed on the token.
5. The user enters the response and it is validated by the server.

### Event-Synchronous

1. The user generates the token's one-time passcode by pushing a button on the token.
2. The user enters a username, one-time passcode, and password or PIN.
3. The server authenticates by matching the one-time passcode entered by the user with the server passcode (the server passcode is generally based upon the next event in the sequence).

## Time-Synchronous

1. The user generates a one-time passcode by pushing a button on the token.
2. The user enters a username and one-time passcode.
3. The server and token each compute a passcode by combining the seed record and current CST.
4. The server authenticates the user by matching the one-time passcode entered by the user with the server's one-time passcode.

## Why is Time-Synchronous Better?

Which of the three approaches is best? Defender supports all three options, but it is generally accepted that time-synchronous authentication is the most effective method.

Challenge-response authentication requires a complex five-step process, so it is prone to user error. And in event-synchronous authentication, the token's one-time passcode is based on the next number in a sequence rather than on a random number, so the system is prone to hacking.

With time-synchronous authentication, the internal clocks of the Defender Security Server and the token are synchronized, so the time can be used as a common seed that enables each device to generate the same sequence of pseudo random numbers. The token uses the seed to generate a new one-time passcode every 60 seconds, and the Defender Security Server uses the same seed to validate any one-time passcode generated by the token.

The advantages of time-synchronous authentication include the following:

- Because the technology is based on the token's secret seed, it is virtually hacker proof.
- Authentication requires only two simple steps, resulting in fewer errors.
- Fewer keystrokes, fewer mistakes, fewer instances of account lockout greatly reduce administrative overhead.

## Additional Benefits to Consider

Any technology product should function as described and be available at a reasonable price. With Defender, you also get:

- A truly extensible, manageable solution capable of growing as your business grows
- A product that can be readily integrated with existing infrastructure and procedures
- A product from a stable company with a wealth of experience
- A technology partner for now and the future.

Purchasing decisions are not made on price alone; Defender delivers the added value you need in an easy-to-use package that is efficiently deployed.

***Seamless Deployment*** - Provisioning represents a major part of any security solution rollout. Defender offers two features that make deployment easy.

First, Defender offers self registration: hardware tokens can be distributed to individuals without the need for identity association and tracking. Before authenticating for the first time, the user self-registers the token, which enables Defender to identify the user and record the relevant identity against the appropriate token records. Self registration significantly lowers deployment and administration costs.

Defender also supports a unique security proxy feature that enables you to deploy it alongside your existing security solution. In this mode of operation, when the Defender Security Server receives a request from a user not defined to Defender, it passes the request to the defined proxy server. This makes it possible to migrate users in a controlled fashion, perhaps by department or as old tokens expire, instead of all at once in a 'big bang' switch.

***Simple Administration*** - The Defender system is administered through the native Active Directory administration tools, giving you centralized management, security, and auditing.

***Hassle-Free Replication*** - Unlike alternative security solutions that rely upon proprietary replication to create database replicas, Defender's database is part of Active Directory and is therefore ubiquitous.

***A Host of Authentication Solutions*** - Choice is key for Quest: we offer a wide range of authentication solutions, both software and hardware. Whether the solution that best fits your organization is a hardware token, a PDA, or a mobile-based solution, Quest can help.

Best of all, you can be assured that Quest is watching the market and working on all of the latest technologies, so as your requirements change, Defender will be ready to meet your needs.

***Flexibility*** - Whatever your target application, be it B2B, B2C, or enterprise, a Defender-based authentication solution can protect your networks and the applications deployed across your networks.

Defender can be configured to operate with most communications solutions that are compliant with RADIUS (an internationally recognized security standard), including remote access servers, firewalls, VPN, and wireless solutions.

Whatever the issues facing your organization, Defender represents a cost effective solution with a cohesive ROI argument.

**Wide Range of Technology Support** - Defender 5 includes support for the RADIUS and LDAP industry standard protocols. This ensures the widest range of supported environments and applications possible.

The Quest commitment includes keeping its products at the head of the pack as new technologies constantly emerge.

**Unmatched Worldwide Service** : Quest is renowned for its world-class customer service. This is the foundation on which Quest has built its outstanding reputation over the last 20 years, and the bedrock of its philosophy for the future.

**No Token Programming Required:** The latest range of Quest Defender authentication tokens are shipped to our customers ready to use: no programming is required by your administration team.

**Expert Consultancy Services:** The Quest Professional Services team is always on hand to help you ensure your projects are done on time, on budget, and without technical hitches.

**Proven Track Record** - Quest has been solving security problems for many years. With over 50,000 customers worldwide, our highly experienced team of professionals has the wealth of experience to offer the best service and long-term vision. We will remain your strategic partner for many years to come.

**Deep E-security Portfolio** - Quest has a a myriad of security products, and each can interoperate with other products. This allows us to bring you the most extensive range of tailor-made security solutions available.

**Solid Return on Investment** - Our experience spans all platforms, from the largest OS/390 environment to the small office/home office (SOHO) configuration. Quest is more than simply a point product vendor; we are a security partner with a comprehensive suite of security solutions to accommodate a wide range of security needs.

ROI calculations for e-security solutions are based on four principal areas: higher revenues, reduced costs, improved compliance, and mitigated risk. Defender addresses each of these four areas, ensuring a good return on investment.

# CONCLUSION

The remainder of this document provides information to help you build a business case applicable to your own Quest Defender implementation.

The following section contains some of the questions that a business must consider when attempting to quantify the ROI of a security product, such as Defender. This list is by no means exhaustive; however, it serves as the basic structure from which to build a sound and cohesive business proposal for a Defender-based solution.

As we have seen, ROI calculations for e-security solutions are based on four principal areas: higher revenues, reduced costs, improved compliance, and mitigated risk:



## Revenues

- Will the solution extend the scope of your business as a result of improved security?
- Does the introduction of better security widen the net of customers and partners?
- Will customer satisfaction be improved, leading to increased revenues?
- Will your business be better able to compete within its market space as a result of better security?

## Costs

- What long-term savings are associated with your e-business project?
- What long-term costs will be avoided as a result of deploying the e-business applications?

- Can you quantify the improvements in the efficiency and effectiveness of your staff that will result from your plans?

### **Compliance**

- How important is security and trust between your partners and customers?
- Have your customers or business partners mandated improvements to your security infrastructure?
- Have you ever lost customers because security requirements were not met?
- Must you adhere to any regulations or legislation?

### **Mitigated Risk**

- How important is the data you are protecting?
- How valuable are your e-business transactions?
- Are you mitigating the risk of a security breach?

A significant factor when considering the ROI for Defender is the comfort of knowing that *your investment is secure*. Your *future business* development can be planned and along with it, the IT structures required to support *growth*.

Defender offers the *essential security* you need to conduct your *e-business with confidence*, safe in the knowledge that your critical digital assets, customers, and employees are *protected by reliable, future-proof software*, and that your *investment* is equally well protected by a technology partner with a sound background and a *commitment to your future* technology needs.

# 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's Windows Management solutions simplify, automate and secure Active Directory, Exchange and Windows, as well as integrate Unix and Linux into the managed environment. Quest Software can be found in offices around the globe and at [www.quest.com](http://www.quest.com).

## Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

Email: [info@quest.com](mailto:info@quest.com)

Mail: Quest Software, Inc.  
World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
USA

Web site [www.quest.com](http://www.quest.com)

Please refer to our Web site for regional and international office information.

## Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>

From SupportLink, you can do the following:

Quickly find thousands of solutions (Knowledgebase articles/documents).

- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: [http://support.quest.com/pdfs/Global\\_Support\\_Guide.pdf](http://support.quest.com/pdfs/Global_Support_Guide.pdf)