Making Everything Easier!™

Quest Software Edition

Multifactor Authentication

FOR DUMMIES®

Compliments of

QUEST SOFTWARE®

Kevin Beaver
Jackson Shaw

Multifactor Authentication

FOR

DUMMIES®

QUEST SOFTWARE EDITION

by Kevin Beaver and Jackson Shaw

Wiley Publishing, Inc.

Multifactor Authentication For Dummies®, Quest Software Edition

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

ISBN: 978-1-118-12846-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Table of Contents

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact `info@dummies.biz`. For details on licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Linda Morris

Editorial Manager: Rev Mengle

Business Development Representative: Melody Layne

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Sean Decker

Proofreader: Jessica Kramer

Special Help: Brian Underdahl

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Diane Graves Steele, Vice President and Publisher, Consumer Dummies

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Introduction

Are you ready to tackle identity and access management for your enterprise? Would you like to improve efficiency, enhance security, and also tackle thorny compliance issues? If so, you've come to the right place.

Multifactor Authentication For Dummies, Quest Software Edition, shows you how to use Quest One Identity Solution to manage administrative access. You'll see how the right identity and access management solution can save you money, improve your security, and result in happier users.

How This Book Is Organized

This book is divided into two chapters:

- **Chapter 1, "Using Multifactor Authentication."** In Chapter 1, you see how using usernames and passwords to authenticate users may be the most common method of authentication, but it is also one of the least secure methods. We discuss strong authentication methods, such as two-factor authentication, which can greatly enhance enterprise security.
- **Chapter 2, "Ten Benefits of Quest One for Identity and Access Management,"** presents 10 different ways that Quest can benefit your enterprise.

Icons Used in This Book

This book uses the following icons to call your attention to information you might find helpful in particular ways.

The information in paragraphs marked by the Remember icon is important and therefore repeated for emphasis. This way, you can easily spot the information when you refer to the book later.

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Need more?

This book was excerpted from *Identity & Access Management For Dummies,* Quest Software Edition, done on behalf of Quest. If you'd like a copy of the full book, which describes the Quest One Identity Solution in greater detail, please contact your Quest representative or contact Quest directly at `www.quest.com/IAMbookregistration` or 1-800-306-9329.

Chapter 1

Using Multifactor Authentication

In This Chapter

- Looking at traditional solutions to authentication
- Understanding strong and multifactor authentication
- Implementing multifactor authentication

Most organizations rely on usernames and passwords to authenticate their users. In other words, a user just needs a username and a password to prove he is who he says he is. Unfortunately, usernames and passwords don't always provide adequate security. Usernames are often easy to obtain (or guess), and users have a tendency to make passwords easy to find by writing them on sticky notes, reusing versions of the same password, or basing them on easy-to-remember (and therefore easy-to-guess) personal information. To address this relative lack of security, some enterprises are turning to multifactor authentication.

In this chapter, we examine the concept of multifactor authentication and look at how the Quest One Identity Solution can help overcome the shortcomings of traditional username and password authentication.

Looking at Traditional Solutions

Before networked computing, business transactions were typically conducted face-to-face, so establishing the identity of those involved in the transaction presented few problems. But

with today's connected workforce, recognizing a user trying to access your network resources is much more difficult.

Relying on usernames and passwords is not unreasonable; after all, that's the procedure that a lot of organizations know and follow. But usernames and passwords have several problems that can make them less than ideal from a security standpoint:

- Usernames are usually standardized within an organization, so they're often quite easy to guess.
- Given a choice, most users select very simple, short passwords that are easily discovered.
- When users are required to create more complex passwords, they usually write them down. The classic place for this written password is on a sticky note on the side of the computer monitor, but just inside the top desk drawer is the next most popular.
- If users don't write down their passwords, they're likely to forget them and need to call the help desk for a password reset. Some estimates say that the average user does this one and a half times every year.
- If users need to use different systems in the course of doing their jobs, they're often required to have different usernames and passwords for each system, which only compounds the lost and forgotten password problem.

Organizations often respond to the problem of insecure passwords by taking steps that make passwords even harder to remember. These steps include

- Requiring longer passwords
- Adding complexity requirements such as the inclusion of uppercase and lowercase letters, at least one numeric character, and at least one special character, such as those that appear on the number keys
- Forcing users to change passwords frequently
- Keeping a record of passwords used in the past and not allowing passwords to be reused
- Prohibiting the use of "real" words like names or terms that appear in the dictionary

Just because passwords are "secure" doesn't mean they cannot be cracked. Numerous tools — both free and commercial — are available that can easily and relatively quickly crack passwords. One lost or stolen laptop computer is all it takes to expose your entire network to unauthorized use.

Unfortunately, these steps to strengthen passwords often result in the exact opposite — decreased security — because users tend to write down their passwords when they're asked to remember multiple complex passwords.

Understanding Strong and Multifactor Authentication

Organizations that realize the limitations of passwords have looked at other ways to increase security, including implementing strong authentication. *Strong authentication* is often also referred to as *two-factor authentication* or, more generically, *multifactor* authentication. However, soliciting multiple answers to challenge questions or identifying a personal security image and even implementing complex passwords is considered strong authentication, but not multifactor authentication. Multifactor authentication combines one item from "something you know" with one or more items from either "something you have" or "something you are." One common example of multifactor authentication is the automated teller machine (ATM) card, which combines something you have (the ATM card) with something you know, such as a personal identification number (PIN) or passcode.

- **Something you know:** Your username or a secret password or passphrase associated with your name provides a degree of identification.
- **Something you have:** A physical device, such as a hardware token, smart card, a USB key, or cell phone running a software token.
- **Something you are:** Something that is unique to you, such as your fingerprint, the pattern of your iris, or your voice.

Case study: Multifactor authentication

Here's a before-and-after scenario showcasing the benefits of a unified approach to multifactor authentication. A recent audit revealed that for certain employees, data-sets, applications, and use-cases, authentication with a username and password isn't enough. So the company decided to implement a multifactor authentication option for the following situations:

- Users logging in remotely over the VPN
- Users required to access applications with "administrator" credentials
- Anyone who accesses the company's financial system
- Any transaction involving high dollar amounts or movement of sensitive data

Multifactor authentication has been implemented in pockets throughout the company, but because of the costs and administrative burden, it was not a company-wide implementation.

Frank would like to settle on a single solution, but he doesn't want to rely on proprietary technology and the practices of some vendors that lock customers into expensive on-going maintenance. (For example, he wants to avoid a solution where he has to buy the tokens from the vendor. They "die" at pre-determined dates depending on what you pay for, and you have to manage them through separate and proprietary management consoles.)

How do things change after a unified multifactor authentication solution is put in place? The company implements a single multifactor solution that uses Active Directory (AD) as the identity store and the AD Users and Computers (ADUC) console as the management interface. Because the solution and its tokens are entirely standards-based, the company can buy them from any vendor they like. In addition, tokens don't have preset "death" dates and instead last as long as the battery holds out (usually five to seven years instead of three years for pre-programmed tokens). The company can also use software tokens (that is, on a Blackberry, iPhone, Android and so on) that never die. The solution also works on the company's Unix, Linux, and Mac systems because they have been joined to AD and can initiate single sign-on (SSO) through any of the multifactor authentication options they have chosen. Now a single token, managed very easily and inexpensively, provides all of the security and compliance they need.

One-time passwords

Token-based multifactor authentication creates a one-time password. A one-time password is a password that can only be used for a single login and is equivalent to forcing a user to change their password after each use without the associated impracticality or inconvenience. One-time passwords are generated automatically by a small physical device called a *hardware token* that users carry with them. However, a one-time password can be generated using a *software token* that is installed on a user's cell phone or other device. Regardless of the type of token, the one-time password is generated as needed using a special algorithm (mathematical procedure). Several different types of tokens can be used, depending on user requirements and compatibility with the systems you are using.

Three methods of multifactor authentication

Token-based multifactor authentication is a great way to secure your network resources. Token-based authentication has three ways to authenticate a user.

Challenge-response (asynchronous)

Challenge-response authentication uses the following steps:

1. The user enters a username.
2. The server sends a challenge code.
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

Event-synchronous works like this:

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

Time-synchronous uses these steps:

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 a seed record (a random number) and the current value of the universal time clock (also known as coordinated universal time, which is a system that keeps computers across time zones around the world in sync).
4. The server authenticates the user by matching the one-time passcode entered by the user with the server's one-time passcode.

Implementing Multifactor Authentication

Implementing multifactor authentication in your organization can be a key to improving security, but not all solutions are the same.

The problems with traditional multifactor solutions

Unfortunately, even though traditional multifactor systems provide better security than username and password alone, they have a number of shortcomings that made these solutions far less than ideal. Essentially, these proprietary solutions are often too expensive, too hard to manage, and create an added layer of complexity that burdens both end users and the IT staff who must manage them.

In addition, many multifactor authentication vendors generate significant revenue through manufacturing the hardware tokens themselves. To preserve these revenue streams, these vendors charge a premium for the tokens designed to work only on their proprietary platforms. In addition, token "life" is typically predetermined and the token works for only the length of time that the customer paid for, requiring repeated and periodic purchase of new tokens even though the battery within the token is still working.

Because most solutions do not integrate with Active Directory, companies needed to maintain a separate, often proprietary directory just for the multifactor authentication solution. Having two different directories creates headaches for both the IT staff and end users.

Information systems complexity is the enemy of security. The more systems you have to maintain, the greater the room for error and oversight, which, often ironically, creates more business risk.

For the IT staff, maintaining both the AD and the separate strong authentication databases can mean double the workload. In addition, because IT has to provision, de-provision, or re-provision users in two separate places whenever a change occurs, the possibility of errors greatly increases, whereas the responsiveness of IT decreases due to their heavier workload.

The lack of integration with AD also makes managing multifactor authentication more difficult. Because you are not able to manage the multifactor authentication system with familiar and commonly used AD administration tools, extra tools, time, and training are required.

In the final analysis, any multifactor authentication solution that does not integrate with AD increases your costs and requires more management.

Understanding the Quest One Defender solution

The Quest One Defender solution is built on AD. Each authorized user is issued a registered Defender token that generates a single-use passcode, typically every 60 seconds. The

passcode (or one-time password) is unique for that token and can be used only once. The Defender Security Server validates the pass code 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.

Earlier in this chapter, we mentioned that token-based multifactor authentication uses three different methods:

- Challenge-response
- Event-synchronous
- Time-synchronous

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 more vulnerable 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 onetime 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.
- This method results in fewer keystrokes, fewer mistakes, fewer instances of account lockout greatly reduce administrative overhead.

Implementing multifactor authentication with existing investments

You already have an investment in AD, so why would you want to add another proprietary directory that requires you to duplicate your efforts? Quest strongly believes that reducing the number of identities you need to manage for each user is the path to efficiency and savings.

Because Defender works with AD, you don't need to create additional user identities in order to implement multifactor authentication for access to your enterprise's resources. Rather, you can pursue the get to one goal, whereby users have a single identity that they use throughout the enterprise.

In addition, because the Quest One approach to identity and access management actually empowers many non-Windows systems to join AD (thus eliminating even more redundant directories and identities), a single multifactor authentication solution based on AD secures logons for Unix, Linux, Java, and Mac systems as well. In addition, if you are using a Windows-based smart card solution, joining Linux or Java systems to Active Directory enables you to extend smart card authentication to those systems as well — without additional infrastructure and without multiple smart cards.

Benefits of this approach

Take a closer look at some of the benefits you'll receive by using Quest One Defender as your multifactor authentication solution. Any technology product should function as described and be available at a reasonable price. After all, no one has unlimited time and budget in IT! With Defender, you also get

- A truly extensible, manageable solution capable of growing as your business grows
- A solution that can be readily integrated with existing infrastructure and procedures

- A solution 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 and software 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.

Any time you can move tedious, repetitive tasks away from IT staff and towards a technology-based automated process, it directly benefits the business. IT staff can focus on more analytical and strategic issues, and users can get the satisfaction of *not* having to rely on IT for everything — everyone wins!

Defender's ZeroIMPACT migration strategy is invaluable to security administrators. It allows organizations to undertake a gradual migration to Defender from an incumbent legacy authentication solution. Defender supports a unique security proxy feature that enables you to deploy it alongside your existing security solution.

For example, 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.

User authentication wherever it's required

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

Whether they need to go through a VPN to remotely access applications, wireless access points, network operating systems, intranets, extranets, Web servers, or other applications, Defender's multifactor authentication ensures that only authorized users are permitted access.

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.

Simple administration

The Defender system is administered through the native AD administration tools, giving you centralized management, security, and auditing. This also means that your IT staff will use familiar tools rather than having to learn a whole new system.

Hassle-free replication

Unlike alternative security solutions that rely upon proprietary replication to create database replicas, Defender's database is part of AD and is therefore ubiquitous. Here, too, you can leverage existing IT skills instead of spending valuable time adapting to a different way of doing things.

Active Directory-centric

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

Defender has been architected to integrate fully with AD. 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.

A host of tokens available

Choice is key for Quest One: It offers a wide range of options for tokens, both software and hardware. Whether the solution that best fits your organization is a hardware token, cell phone–based, or a smartphone-based solution, Quest One can help.

Defender also supports any OATH-compliant (Open Authentication standard) token no matter where you purchased it from. In addition, unlike other solutions, Defender's software tokens never expire and the hardware tokens can used for the life of the battery (typically 5–7 years).

In addition, Quest is watching the market and working with all of the latest technologies, so as your requirements change, Defender will be ready to meet your needs.

Flexibility

Defender can be configured to operate with most communications solutions that are compliant with RADIUS (an internationally recognized security standard that stands for Remote Authentication Dial-In User Service), and LDAP (Lightweight Directory Access Protocol) including remote access servers, firewalls, VPNs, and wireless solutions.

Solid return on investment

Quest One's 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; they are a partner with a comprehensive suite of identity and access management solutions to accommodate a wide range of needs.

Return on investment (ROI) calculations for security solutions are based on four principal areas:

- Higher 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?

  Information security and compliance — when done right — can both be used as a competitive advantage for your business.

- Reduced costs
  - What long-term savings are associated with your project?
  - What long-term costs will be avoided as a result of deploying the solution?
  - Can you quantify the improvements in the efficiency and effectiveness of your staff that will result from your plans?
- Improved 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 network resources and data?
  - Are you minimizing the risk of a security breach?

Defender addresses each of these four areas, ensuring a good return on investment.

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.

Deep identity and access management portfolio

Quest One is a myriad of identity and access management solutions, and each can interoperate with other components of Quest One. This allows Quest to bring you the most extensive range of tailor-made solutions available — including solutions for authentication.

Chapter 2

Ten Benefits of Quest One for Identity and Access Management

In This Chapter

- Getting to one password and one identity
- Managing privileged accounts securely
- Streamlining provisioning
- Unifying roles with identity intelligence
- Using multifactor authentication
- Handling identity administration more efficiently
- Knowing what users are doing

In this chapter, we look at ten benefits your organization will discover by following the Quest One Identity Solution approach to identity and access management — all of which can lead to more efficient IT management and reduce business risks.

Getting to One Password

Quest One starts to address the *managing strong passwords doesn't have to be complicated* issue with Quest Password Manager. Quest Password Manager enables end users to reset their own password and synchronizes that password across multiple platforms and applications.

Quest Password Manager supports a broad range of platforms and applications in addition to Microsoft Active Directory (AD) to create a unified approach to password management. Through Quest Authentication Services, organizations can actually reduce the number of passwords to manage and centralize self-service password resets on Unix, Linux, Mac, and Java systems through a single AD password.

Quest Enterprise Single Sign-on provides a single point of user login/authentication to virtually any system and application that cannot be "joined" to AD. This includes standard username/password logins as well as the entire range of strong authentication options such as smart cards, biometrics, or one-time passwords (OTP).

The result of the Quest One approach to password management is improved efficiency, increased security, and enhanced compliance.

Getting to One Identity

Quest Authentication Services enables a high number of non-Windows systems (specifically Unix, Linux, and Mac) to participate as "full citizens" in AD. As a result, those systems are no longer required to use individual user identities for authentication and can instead authenticate with the single identity that already exists in AD. For Java applications, the same benefit can be achieved through Quest Single Sign-on for Java.

This approach to unifying identities in an already deployed directory results in dramatic gains in efficiency as user accounts need only be provisioned and managed in one place for multiple systems. Security and compliance also increase as stricter policy, and more secure practices can be implemented in one innately secure directory instead of across multiple, disparate systems.

Managing Privileged Accounts Securely

Privileged accounts — that is user accounts with a high level of authority — present a unique set of management

challenges. These accounts are typically shared between several users, which can lead to mismanagement or worse, abuse of privileges. On Windows systems, administrators have much greater control over the access that is granted to individual users. Quite simply, Windows systems offer a granularity of control that is lacking in Unix and Linux systems. On Windows systems, you can use Quest ActiveRoles Server to implement strictly enforced role-based security or granular control over exactly what administrative users are able to do and which resources they can access. ActiveRoles Server helps you achieve and sustain regulatory compliance by implementing secure, automated and auditable internal controls over granting and revoking access to network resources.

Quest also empowers you to have the same level of control in Unix and Linux systems.

Quest Privilege Manager for Unix enhances security by protecting the full power of root access from potential misuse or abuse through fine-grained, policy-based control. Unix systems pose a special risk to the enterprise because of the virtually unlimited power that root access gives an administrator. You need a way to control this power while still enabling users to have the access they need.

Privilege Manager helps you to define a security policy that stipulates who has access to which root function, as well as when and where individuals can perform those functions. It controls access to existing programs as well as any purpose-built utilities used for common system administration tasks. With Privilege Manager, you don't need to worry about someone deleting critical files, modifying file permissions or databases, reformatting disks, or damaging Unix systems in more subtle ways.

By enabling administrators to define fine-grained security policies, delegating common management tasks and logging all Unix root activities down to the keystroke level, Privilege Manager for Unix reduces security risks, increases IT productivity, and enables organizations to achieve and sustain compliance in a cost-effective manner.

Achieving Single Sign-on

User logins and the associated problems with multiple logins across many diverse systems is a major source of inefficiency and insecurity for most organizations. Quest One helps address these challenges through a comprehensive suite of single sign-on (SSO) solutions that increase efficiency, enhance security, and help you to achieve compliance.

Quest Authentication Services and Single Sign-on for Java enable a high number of systems and applications to authenticate with a user's AD password, the AD credential, and controlled through AD security policy. This "true" single sign-on approach covers Unix, Linux, Mac, Java, SAP, Siebel, DB2, any application that uses pluggable authentication application programming interfaces (GSSAPI), any application that is Kerberos-enabled, and applications that are LDAP-aware (lightweight directory access protocol).

For systems that are not equipped to leverage AD authentication for true single sign-on, Quest offers an AD-based enterprise single sign-on solution. Quest Enterprise Single Sign-on empowers users to log on to any system or application with only a single password entered into AD. With Enterprise Single Sign-on, all subsequent, non-AD logons are performed automatically under the covers by the solution.

Only Quest One offers the best of both worlds: true single sign-on and enterprise single sign-on for the ideal blended approach to perhaps the most prominent challenge in identity and access management.

Streamlining Provisioning

Quest One helps you control your identity management universe and creates a single point of administration for identities across the enterprise, eliminates redundant efforts, reduces errors, and saves time. For example, a single provisioning action in AD can take care of users in Unix, Linux, and Mac systems that have become unified with AD through Quest One solutions. Similarly, turning off that single user account in AD immediately terminates access across the same wide range of non-Windows systems. Quest One also offers solutions that

are not centered around AD. Enterprise-wide provisioning capabilities are available through Quest One Identity Manager and implement a foundation for all provisioning actions without requiring heavy amounts of custom coding. The bottom line is that with fewer places to perform provisioning actions (as well as re-provisioning and de-provisioning), you can benefit from increased efficiency in your identity administration, a higher level of security as human error is reduced, and elevated compliance as de-provisioning is accelerated and more securely controlled.

Improving Role Management

Quest One helps you unify roles to arrive at a single, authoritative set that can affect the entire enterprise. This approach — infused with identity intelligence — means that roles and how they impact access can be implemented and controlled based on your business needs — not the capabilities (or lack of capabilities) built into your existing identity and access management solutions.

With roles unified, the associated critical concepts of rules, policy, workflow, and approvals can also be unified. Similarly, the intelligence offered by the Quest One approach ensures that each of these controlling factors does the right thing for user access without custom coding. This approach also provides dynamic adjustment and the ability for those on the front lines — end users and line-of-business personnel — to drive identity management.

Using Multifactor Authentication

Quest One Defender leverages the ubiquity of AD and its scalability, security, and compliance to provide a multifactor authentication solution that takes advantage of the corporate directory already in place.

Defender has been architected to integrate fully with AD. 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.

Defender authentication can be used by your employees, business partners, and customers, whether they are local, remote, or mobile. Whether they require remote access through VPN to key applications, wireless access points, network operating systems, intranets, extranets, or Web servers, Defender's strong multifactor authentication ensures that only authorized users are permitted access. With integration with Quest Authentication Services, a single Defender token secures access not only for Windows systems but for Unix, Linux, and Mac as well.

Defender offers self-registration: Hardware tokens can be distributed to individuals without the need for identity association and tracking. Self-registration significantly lowers deployment and administration costs.

Defender's ZeroIMPACT migration strategy allows organizations to undertake a gradual migration to Defender from an incumbent strong authentication solution. Defender supports a unique security proxy feature that enables you to deploy it alongside your existing one-time password (OTP) solution.

Quest Defender authentication tokens are shipped to customers ready to use and have no preprogrammed expiration — they last as long as the battery lasts (typically five to seven years). Once again, you save time and money because less work is required and replacement tokens can be purchased less frequently.

Making Users Happy

Users hate waiting on the phone to talk to the help desk. Heck, many don't even like calling the help desk at all! Quest One can help by providing a variety of self-service capabilities. From password resets to updating personal information, and from requesting system access to approving requests from staff members, the Quest One approach to identity and access management is optimized to accelerate efficiency, relieve IT from unnecessary and tedious involvement, and get the work

in the hands of those who understand the objectives of what they are trying to accomplish.

For example, self-service password reset helps improve productivity for users who are on a different schedule than your help desk or those calling during off-hours. By having access to an automated, 24x7x365 password reset and account unlock interface, users can continue to be productive, rather than being locked out until the help desk opens up in the morning.

Handling Identity Administration More Efficiently

Quest ActiveRoles Server can help you automatically execute some of the most time-consuming identity administration tasks. It empowers you to provision, re-provision, and de-provision Active Directory users quickly, cost-efficiently, and securely. ActiveRoles Server helps you keep up with requests to create, change, or remove user access to various network resources so that you no longer need to rely on manual provisioning processes to maintain compliance. This is especially important with the advent of compliance regulations like the Sarbanes-Oxley Act and the intense scrutiny they place on access to business-sensitive applications.

ActiveRoles Server provides practical user and access lifecycle management. ActiveRoles Server automates user and group provisioning lifecycle tasks to reduce your administrative workload and increases user access control whether the user is a new hire, intra-organization transfer, or termination.

The power of Quest One for identity administration doesn't stop at AD. Synchronization technology, identity intelligence, and consolidation of identities enables Quest One solutions to securely and efficiently perform administrative actions for the entire enterprise — beyond AD. The addition of powerful, identity intelligence-driven administration capabilities available through Quest One can enable you to implement the foundation for all identity administration actions (including provisioning, role definition and management, and password

management) enterprise-wide without the burden of lots of custom coding and difficult-to-manage connectors.

Knowing What Users are Doing

Understanding user and administrator activity is at the heart of a secure and well-managed infrastructure, but knowing what users do with the access they have to critical network resources has been a challenge to IT organizations. Quest's ChangeAuditor addresses all of these concerns in heterogeneous environments.

ChangeAuditor enables you to securely collect your event data, keep more data online, report intelligently, and improve system security and performance. ChangeAuditor alerts you in real-time to unusual user, administrator and system activity. ChangeAuditor also offers alerts that can be sent directly to you by e-mail or to third-party monitoring applications.

Quest Reporter provides automated discovery and comparison of configuration-related items to support planning, securing, and auditing. Reporter enables you to collect, compare, report on and resolve Active Directory and Windows-based configurations. Armed with this information, you can quickly make strategic and tactical security decisions that involve your Active Directory and Windows environment.

Reporter supports effective knowledge management and informed decision making, ensures proactive security, improved standards and policy compliance, and improves migration planning.

The capabilities of ChangeAuditor and Reporter extend beyond AD to Unix, Linux, and Mac systems that have become "full citizens" in Active Directory through Quest Authentication Services.