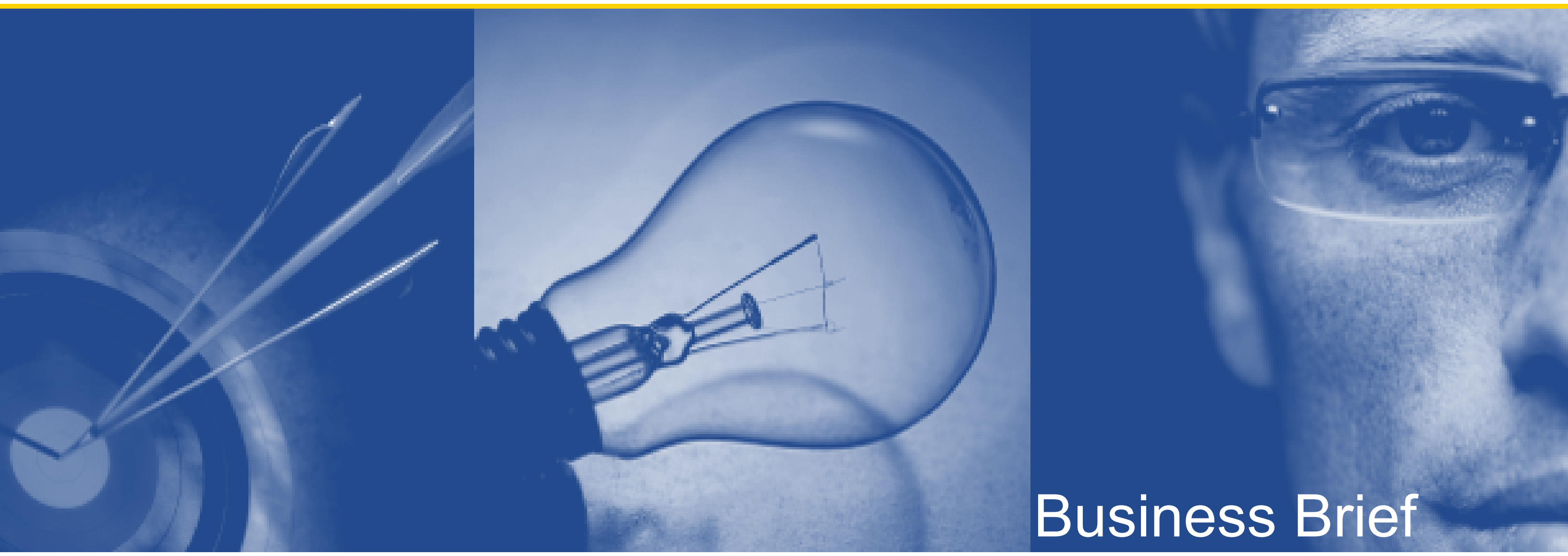
Better Together

How the Quest One Identity Solution Products Enhance Each Other

Written by
Quest Software, Inc.



World Headquarters:
5 Polaris Way
Aliso Viejo, CA 92656
e-mail: info@quest.com

Please refer to our Web site (www.quest.com) for regional and international office information.

Updated—March, 2009

CONTENTS

INTRODUCTION 1

THE QUEST ONE IDENTITY SOLUTION 2

THE PRODUCTS OF THE QUEST ONE IDENTITY SOLUTION 4

QUEST AUTHENTICATION SERVICES (FORMERLY VINTELA AUTHENTICATION SERVICES) 4
ACTIVEROLES SERVER 4
QUEST SINGLE SIGN-ON FOR JAVA (FORMERLY VINTELA SINGLE SIGN-ON FOR JAVA) 5
QUEST ENTERPRISE SINGLE SIGN-ON 5
PRIVILEGE MANAGER FOR UNIX 5
DEFENDER 5
PASSWORD MANAGER 5
WEBTHORITY 6
INSYNC 6
INTRUST 6
REPORTER 6

QUEST ONE—BETTER TOGETHER 7

IMPROVE EFFICIENCY 7
IMPLEMENT SINGLE SIGN-ON 10
ENHANCE SECURITY 12
ACHIEVE COMPLIANCE 14

APPENDIX: INTEGRATION SUMMARY 17

AUTHENTICATION SERVICES 17
ACTIVE ROLE SERVER 17
SINGLE SIGN-ON FOR JAVA 17
ENTERPRISE SINGLE SIGN-ON 18
PRIVILEGE MANAGER FOR UNIX 18
DEFENDER 18
PASSWORD MANAGER 19
WEBTHORITY 19
INSYNC 19
INTRUST 19
REPORTER 20

ABOUT QUEST SOFTWARE, INC. 21

CONTACTING QUEST SOFTWARE 21
CONTACTING QUEST SUPPORT 21

INTRODUCTION

The Quest One Identity Solution includes products that address the challenges of identity and access management by enabling organizations to improve efficiency, enhance security, and achieve compliance.

The purpose of this white paper is to provide the reader with a clear understanding of the current and planned integration between Quest products and important third-party products, including Microsoft's Identity Lifecycle Manager (ILM) and others. The paper is not intended to be a comprehensive discussion of all of the benefits that can be achieved through the use of Quest One; rather, it is a targeted discussion of integration between and among the various Quest One products.

THE QUEST ONE IDENTITY SOLUTION

The management challenges of today's complex, heterogeneous enterprise typically fall into three main areas: efficiency, security and compliance.

These challenges are most apparent in identity and access management. As organizations grow and become more complex, the number of identities that the IT department must manage also grows, and they demand an increased level of control and visibility.

It doesn't have to be that way. Quest Software offers a set of enabling technologies called the **Quest One Identity Solution**. Quest One empowers organizations to capitalize on their existing investments in identity infrastructure, in most cases, Microsoft Active Directory, for truly unified identity and access management that crosses platform boundaries.

Quest One enables organizations to simplify identity and access management by:

- Reducing the number of identities that must be managed
- Automating time-consuming identity administration tasks, particularly those that need to be repeated for multiple platforms, systems, and applications
- Enabling organizations to base their identity management strategy on existing investments and skill sets

Quest One helps improve efficiency by automating administration and consolidating identity infrastructure. In addition, Quest One is based on your existing investment in Active Directory. Consequently, organizations manage fewer identities. This makes identity management more cost-efficient with less demand on limited resources.

Quest One delivers a full-spectrum of single sign-on offerings ranging from full, Kerberos-based integration (one identity, one credential, one login), to password replay enterprise single sign-on, to password synchronization and web single sign-on.

Quest helps organizations enhance security by implementing stronger authentication for multiple systems as well as enabling control of privileged accounts—organizations control who accesses what, when, for what purpose, and even how access is granted.

Quest helps organizations achieve compliance with powerful, integrated auditing, reporting, and enforcement products, along with directory and identity consolidation. Users of the Quest One approach get compliant fast and have automated, repeatable practices and technologies to keep them there. Quest helps you achieve compliance by:

- Enforcing access control consistently across the entire enterprise
- Implementing segregation of duties across the wide range of systems and applications
- Auditing the entire identity environment as well as specialized identity tasks to "prove" compliance now and into the future.

THE PRODUCTS OF THE QUEST ONE IDENTITY SOLUTION

The Quest products included in the Quest One Identity Solution are:

Quest Authentication Services (formerly Vintela Authentication Services)

Authentication Services extends Active Directory's reach, enabling Unix, Linux, and Mac system administrators to centralize access, authentication and authorization around Active Directory. Authentication Services gives users the same username and password for Windows, Unix, Linux, Mac, and some application logins while still providing a consolidated and secure environment. It allows existing Active Directory security practices to apply to non-Windows systems as well, without the need to maintain password synchronization or perform identity administration tasks on multiple systems.

ActiveRoles Server

ActiveRoles Server helps organizations manage and automatically provision, re-provision, and de-provision users quickly, efficiently, and securely in Active Directory, Active Directory Lightweight Directory Service (AD LDS formerly ADAM), and beyond. ActiveRoles Server provides strictly enforced role-based security, automated group management, change approval and easy-to-use self-service web interfaces to achieve practical user and group lifecycle management for the Windows enterprise.

ActiveRoles Server automates user provisioning tasks to reduce administrative workloads and get new users up and running faster. Re-provisioning and de-provisioning is automated as well; when a user's access needs to be changed or removed, updates in Active Directory, Exchange, and Windows are made automatically. This streamlines operations and makes users more productive faster, creating significant cost savings for an organization.

Quest Single Sign-on for Java (formerly Vintela Single Sign-on for Java)

Single Sign-on for Java extends the native Kerberos single sign-on capabilities of Active Directory to the Java platform. It improves efficiency, enhances security, and delivers compliance by extending Active Directory's standards-based authentication to Java applications. It also provides federated single sign-on for Java applications through Active Directory Federation Services (ADFS).

Quest Enterprise Single Sign-on

Enterprise Single Sign-on is a "login automation" solution that extends Active Directory-based single sign-on to any system or application that cannot become fully integrated with Active Directory through Authentication Services or Single Sign-on for Java. It is a client-based solution that addresses many of the efficiency, security, and compliance concerns of login to heterogeneous systems.

Privilege Manager for Unix

Privilege Manager for Unix provides the ability to granularly delegate Unix root access (or any other administrative credential). This capability is generally not available natively from the platform itself. Privilege Manager provides policy-based access to specific systems for specific functions. It also includes powerful auditing capabilities (even down to the keystroke level) of all activities performed.

Defender

Defender is a classic one-time password (OTP) solution that overcomes many of the limitations of traditional OTP solutions through its reliance on Active Directory, adherence to standards, and low-impact implementation and migration capabilities.

Password Manager

Password Manager allows end users to securely reset their passwords after an account lockout or when they forget their passwords. The product reduces the help desk workload and enables administrators to implement stronger password policies. Password Manager accommodates the widest possible range of internal requirements and data security standards. It comes with global language support.

Webthority

Webthority's highly flexible architecture provides sophisticated and secure control of valuable data. It handles user identification, authentication, and access control through the combination of a proxy service and authentication services, managed by a centralized administrative console. Webthority uses an intelligent and highly secure proxy service to control the web content seen by users based on their defined role within an existing identity store (such as Active Directory). Webthority provides flexible configuration of a variety of roles, such as employee, supplier, and partner. The proxy service is a platform-independent solution that does not require web server agents.

InSync

InSync provides automated password synchronization across the enterprise so users have only a single password to remember for all supported systems and applications. This makes it easier for users to choose stronger passwords. It also means each user has only one password to reset, which reduces calls to the help desk.

InTrust

InTrust enables organizations to audit, report on, and alert on all Active Directory domain controller activity, as well as track detailed changes to Active Directory and Group Policy (including non-Windows systems that have become full citizens in Active Directory through Quest One).

Reporter

Reporter provides automated discovery and comparison of configuration-related items to support planning, securing, and auditing of your Windows infrastructure. It provides specialized reports detailing Unix-related information for non-Windows systems that have joined Active Directory through Quest One.

QUEST ONE—BETTER TOGETHER

Improve Efficiency

Quest One helps improve efficiency by automating administration and consolidating identity infrastructure. In addition, Quest One is based on existing investments in Active Directory. This enables, organizations to manage fewer identities and be more resource- and cost-efficient with them. Quest One helps improve efficiency through:

ActiveRoles Server Integration with Authentication Services

When combined with the Support Pack for Authentication Services, ActiveRoles Server extends management control to Unix, Linux, and Mac identities, including users, groups and computers, through Authentication Services. This unique solution decreases administrative costs and makes better use of third-party management solutions. Query-based management views show all identities, business rules ensure and enforce appropriate administrative practices and permission templates make it easy to delegate identity management.

ActiveRoles Server Integration with Password Manager

The ActiveRoles Server web interface supports the display of Password Manager's self-service password reset capability. This enables end users or help desk personnel to use the ActiveRoles Server web interface for both ActiveRoles Server and Password Manager self-service functions rather than having to switch to the Password Manager native web interface.

ActiveRoles Server Integration with Defender

A Support Pack for Defender enables the provisioning of Defender-related attributes by ActiveRoles Server and self-service registration of Defender tokens within the ActiveRoles Server web interface.

ActiveRoles Server Integration with Third-Party Products

Quest offers, free of charge, a SPML 2.0 (Service Provisioning Markup Language) provider that allows any system that generates an SPML-formatted request to connect through a web service and provision Active Directory. This provider can be used in tandem with ActiveRoles Server to better integrate Quest ActiveRoles Server into heterogeneous environments. The SPML provider can be used to interoperate with identity management products and suites from companies such as IBM/Tivoli, Novell, and Sun, and with any product that supports SPML.

Password Manager Integration with Authentication Services and Single Sign-on for Java

Users of Authentication Services and/or Single Sign-on for Java and Password Manager can extend the benefit of self-service password reset to non-Windows users. Non-Windows browsers are supported, so Unix and Linux users can use their favorite browser to access Password Manager to perform self-service password resets. Since Authentication Services relies on the Active Directory password for authentication of Unix, Linux, Mac and Java users, these users benefit from the same Active Directory-based self-service password reset experience. In addition, the enhanced security capabilities of Password Manager are automatically extended to Unix, Linux, Mac, and Java users.

Password Manager Integration with InSync

Quest's InSync product supports password synchronization across a wide variety of platforms and applications. Password Manager integrates with InSync to enable any passwords that are reset via Password Manager to automatically be synchronized via InSync throughout the enterprise. In 2009, the full InSync product and its complete functionality will be absorbed into Password Manager and the two will be sold as a combined offering.

Password Manager Integration with Defender

Password Manager enables Defender users to securely authenticate (through the Defender one-time password) to the Password Manager portal. This means that a Password Manager administrator has the option to allow Defender users to reset their Active Directory password simply by using two-factor authentication in place of, or in addition to, answering security questions.

Password Manager Integration with Enterprise Single Sign-on

Password Manager integrates with Enterprise Single Sign-on to allow the Password Manager self-service password reset to notify the Enterprise Single Sign-on client. This ensures seamless operations and continued single sign-on regardless of whether an Active Directory password change is initiated by IT, by Enterprise Single Sign-on or through the Password Manager self-service functionality.

Password Manager Integration with Third-Party Products

HP ProtectTools (HPPT) Authentication Services is a security solution that mitigates security risks and features a customer-unique password hashing and generation system. Organizations with HP ProtectTools Authentication Services deployed in their environment can configure Quest Password Manager to generate user passwords by using HP ProtectTools. The solution modifies the password-setting mechanism available in Password Manager so that it employs the Password Generation Utility, which is a component of HP ProtectTools Authentication Services, to generate user passwords. Once generated, the password is assigned to the user account via the password hashing system that is part of HP ProtectTools Authentication Services.

Authentication Services Integration with Privilege Manager for Unix

An organization that uses Authentication Services along with Privilege Manager for Unix benefits from the ability to centralize authentication to Active Directory. In addition, the policy that determines the delegation of administrative access can be entirely tied to existing roles and structure within Active Directory. This ability streamlines policy definition and enforcement and eliminates the need to duplicate policy in the authoritative directory and the Privilege Manager tool.

Additionally, the combination of Privilege Manager and Authentication Services enables powerful reporting on those who control and administer Unix and Linux systems. Reports highlight behavior that varies from an accepted baseline, allowing Unix and Linux administrators to pinpoint areas of activity that require further scrutiny and to examine detailed maps of who is and who is not permitted to execute specific commands across Unix and Linux hosts.

Authentication Services Integration with Quest Defender, RSA SecurID Tokens and Windows-based Smartcards

Authentication Services integrates with various two-factor authentication products to provide stronger authentication and enhanced security for Unix-based users. Organizations using Quest Defender, RSA SecurID, Versign OTP, or Microsoft-based tokens or smartcards benefit from this integration through seamless integration with their Windows and Active Directory environment. Two-factor authentication to Active Directory automatically provides appropriate access to those Unix, Linux, and Mac systems that have joined the Active Directory domain through Authentication Services. In fact, Authentication Services and Defender use a common PAM module, which further increases interoperability.

Authentication Services Integration with Third-Party Products

Authentication Services supports integration with a wide variety of products and technologies, including OpenSSH, PuTTY, Apache web server, sudo, and many others. For the latest information, please consult Quest Resource Central at http://rc.vintela.com

Authentication Services Integration with SAP

The Authentication Services Single Sign-On for SAP add-on module extends Quest’s proven Active Directory integration technology to SAP R/3 and ABAP applications accessed using SAP Client (SAPgui). Not only does Authentication Services Single Sign-On for SAP provide transparent Active Directory single sign-on from the SAP client, it also provides full mutual authentication and the ability to secure subsequent data communications. Authentication Services Single Sign-On for SAP received SAP certification on April 19, 2007.

Implement Single Sign-on

Quest One delivers a full-spectrum of single sign-on offerings including full Kerberos-based integration (one identity, one credential, one login), password replay enterprise single sign-on, password synchronization and web single sign-on. Integration points among the Quest One products include:

Single Sign-on for Java Integration with Webthority

Webthority integrates with Single Sign-on for Java to become an authentication resource for users accessing Java applications via Webthority. This combination also brings single sign-on for Java's Active Directory Federation Service (ADFS) capabilities to Webthority. In the future, Single Sign-on for Java and Webthority will be merged into a single offering for web single sign-on and access management.

Single Sign-on for Java Integration with NetWeaver Portal

A specialized version of Single Sign-on for Java, called Single Sign-on for NetWeaver, provides seamless Active Directory-based single sign-on to SAP applications running on the NetWeaver Portal. This solution enables those SAP applications to benefit from the Kerberos authentication of Active Directory as extended through Single Sign-on for Java. Single Sign-on for NetWeaver received SAP certification in October 2008.

Enterprise Single Sign-on integration with Password Manager

Quest Password Manager integrates with Quest Enterprise Single Sign-on to allow the Password Manager self-service password reset to notify the Enterprise Single Sign-on client. This ensures seamless operations and continued single sign-on, whether an Active Directory password change is initiated by IT, by Enterprise Single Sign-on or through the Password Manager self-service functionality.

Webthority Planned Integration with Enterprise Single Sign-on

In early 2009, Webthority will include integration with Enterprise Single Sign-on. This will compliment Webthority's web single sign-on capabilities by providing remote users with all of the benefits of the Enterprise Single Sign-on solution. This integration extends Enterprise Single Sign-on's login automation and password replay to protected resources accessed over the internet through Webthority.

Webthority Integration with Defender

Webthority works seamlessly with Defender to enable two-factor authentication for any web application without requiring changes, edits or reconfiguration of the web application or the underlying web server.

Webthority Planned Integration with Microsoft SharePoint Server

In early 2009, Webthority will provide secure access to the Microsoft SharePoint Server for both internal and external users within an organization. This will allow information stored on the SharePoint Server to be shared and updated by remote users.

Enterprise Single Sign-on Integration with Third-Party Solutions

Enterprise Single Sign-on integrates with the full range of multi-factor authentication options, including OTP, smart cards, and biometrics. This ensures that the single sign-on experience is maintained and secured, no matter which method is used for login. In addition, Enterprise Single Sign-on integrates with a variety of LDAP-based identity stores from a number of vendors for true enterprise single sign-on functionality.

Authentication Services Integration with Defender, RSA SecurID tokens, and Microsoft-based Smartcards

Quest Authentication Services integrates with various two-factor authentication products to provide stronger authentication and enhanced security in conjunction with single sign-on for Unix and Linux-based users. Organizations using Quest Defender, RSA SecurID, Verisign OTP, or Microsoft-based tokens or smartcards benefit through seamless integration with their Windows and Active Directory environment. A two-factor authentication to Active Directory automatically provides appropriate access to those Unix, Linux, and Mac systems that have joined the Active Directory domain through Authentication Services. In fact, Authentication Services and Defender use a common PAM module, which increases interoperability.

Authentication Services Integration with Password Manager

Users of Authentication Services and Password Manager can extend the benefit of self-service password reset to Unix, Linux, and Mac users. Support is provided for non-Windows browsers, so Unix and Linux users can use their favorite browser to access Password Manager to perform self-service password resets. Since Authentication Services relies on the Active Directory password for authentication of Unix, Linux, and Mac users, these users benefit from the same self-service password reset experience. In addition, any of the enhanced security capabilities of Password Manager automatically apply to the Unix, Linux, and Mac users.

Authentication Services Integration with Third-Party Products

Quest Authentication Services supports integration for single sign-on with a wide variety of products and technologies, including OpenSSH, PuTTY, Apache web server, sudo, and many others. For the latest information, please consult Quest Resource Central at http://rc.vintela.com

Authentication Services Integration with Siebel

Authentication version 3.5 includes a custom security adapter that provides Active Directory-based reduced sign-on to Siebel running on Unix and Linux platforms. This powerful leveraging of the Authentication Services LDAP Proxy functionality extends the value of both single sign-on and Kerberos authentication to Siebel.

Enhance Security

Quest helps organizations enhance security by implementing stronger authentication for multiple systems as well as enabling control of privileged accounts. Organizations are able to control who accesses what, when, for what purpose, and how access is granted. Quest helps enhance security through:

Defender Integration with Password Manager

Password Manager enables Defender users to use the one-time password from their Defender token to authenticate securely to the Password Manager portal. This means that a Password Manager administrator has the option to allow Defender users to reset their Active Directory password simply by using two-factor authentication in place of or in addition to answering the security questions.

Defender Integration with Authentication Services

Quest Authentication Services is integrated with Defender to provide stronger authentication and enhanced security for Unix, Linux, and Mac users. Organizations using Defender with Authentication Services benefit from seamless integration with their Windows and Active Directory environment. Functionally, a Defender authentication to Active Directory automatically provides appropriate access to those Unix, Linux, and Mac systems that have joined the AD domain through Authentication Services.

Defender Integration with ActiveRoles Server

An ActiveRoles Server Support Pack for Defender enables the provisioning of Defender-related attributes by ActiveRoles Server and self-service registration of Defender tokens within the ActiveRoles Server web interface.

Webthority Integration with Defender

Webthority works seamlessly with Defender to enable two-factor authentication for any web application without requiring changes, edits, or reconfiguration of either the web application or the underlying web server.

Defender Integration with Third-party Solutions

Defender is compatible with any RADIUS-complaint device, ensuring maximum scope and interoperability. In addition Defender is “token agnostic,” enabling the Defender software to leverage any OATH-based token from Quest or any other vendor. In addition, Defender can provide OTP login to the vast majority of LDAP-based systems and applications as well as Oracle.

Authentication Services Integration with Privilege Manager for Unix

An organization that is using Authentication Services along with Privilege Manager for Unix benefits from being able to centralize authentication to Active Directory. In addition, the policy that determines the delegation of administrative access can be entirely tied to existing roles and structure within Active Directory. This ability streamlines policy definition and enforcement and eliminates the need to duplicate policy in the authoritative directory and the Privilege Manager tool.

Additionally, the combination of Privilege Manager and Authentication Services enables powerful reporting on who can control and administer Unix and Linux systems. Reports highlight behavior that varies from an accepted baseline, allowing Unix and Linux administrators to pinpoint areas of activity that require further scrutiny and to examine detailed maps of who is and who is not permitted to execute which commands across Unix and Linux hosts.

Authentication Services Integration with Password Manager

Users of Authentication Services and Password Manager can extend the benefit of the enhanced security capabilities of Password Manager automatically to Unix, Linux, and Mac users. In addition, the self-service password reset functionality can also extend to non-Windows users. Since Authentication Services relies on the Active Directory password for authentication of Unix, Linux, and Mac users, these users benefit from the same self-service password reset experience.

Authentication Services Integration with SAP

The Quest Authentication Services Single Sign-On for SAP add-on module extends Quest’s proven Active Directory integration technology to SAP R/3 and ABAP applications accessed using SAP Client (SAPgui). Not only does Authentication Services Single Sign-On for SAP provide transparent Active Directory single sign-on from the SAP client, it also provides full mutual authentication and the ability to secure subsequent data communications. Quest Authentication Services Single Sign-On for SAP received SAP certification on April 19, 2007.

Authentication Services Integration with Siebel

Quest Authentication version 3.5 includes a custom security adapter that provides Active Directory-based reduced sign-on to Siebel running on Unix and Linux platforms. This powerful leveraging of Authentication Services LDAP Proxy functionality extends the value of both single sign-on and Kerberos authentication to Siebel.

Privilege Manager for Unix Integration with Defender

For users of Privilege Manager, Defender provides an additional level of security for execution of sensitive tasks. This OTP authentication capability can be task-based, time-based, or universally applied.

Webthority Integration with Single Sign-on for Java

Webthority is integrated with Single Sign-on for Java so that it can be used as an authentication resource for anyone accessing Java applications via Webthority. This combination also brings Single Sign-on for Java's Active Directory Federation Service (ADFS) capabilities to Webthority. In the future, Single Sign-on for Java and Webthority will be merged into a single offering for web single sign-on and web access management.

Enterprise Single Sign-on Planned Integration with Webthority

Cross-integration between Webthority and Quest Enterprise Single Sign-on enables Active Directory credentials initiated at a remote logon through Webthority to automatically apply to any application that has been single sign-on enabled through Quest Enterprise Single Sign-on. This integration ensures the most seamless single sign-on experience regardless of the location of the user relative to accessed resources.

Achieve Compliance

Quest helps organizations achieve compliance with powerful integrated auditing, reporting, and enforcement products, as well as directory and identity consolidation. Quest One users rapidly achieve regulatory compliance and have automated, repeatable practices and technologies to maintain it Quest helps you achieve compliance through:

- Enforcing access control consistently across the entire enterprise
- Implementing segregation of duties across the wide range of systems and applications
- Auditing the entire identity environment as well as specialized identity tasks to "prove" compliance now and into the future.

Authentication Services Integration with Privilege Manager for Unix

An organization that is using Authentication Services along with Privilege Manager for Unix benefits from being able to centralize authentication to Active Directory. In addition, the policy that determines the delegation of administrative access can be entirely tied to existing roles and structure within Active Directory. This ability streamlines policy definition and enforcement and eliminates the need to duplicate policy in the authoritative directory and the Privilege Manager tool.

Additionally, the combination of Privilege Manager and Authentication Services enables powerful reporting on who can control and administer Unix and Linux systems. Reports highlight behavior that varies from an accepted baseline, allowing Unix and Linux administrators to pinpoint areas of activity that require further scrutiny and to examine detailed maps of who is and who is not permitted to execute which commands across Unix and Linux hosts.

Authentication Services Integration with Password Manager

Since Authentication Services relies on the Active Directory password for authentication of Unix, Linux, and Mac users, these users benefit from the enhanced password policy capabilities available through Password Manager, which are automatically applied to Active Directory as well as to Unix, Linux, and Mac users.

Authentication Services Integration with ActiveRoles Server

Through the Authentication Services Support Pack for ActiveRoles Server, the management and control of ActiveRoles Server extends to Unix, Linux, and Mac identities such as Unix-enabled users and groups. The combined solution decreases administrative costs and better leverages third-party management solutions. Query-based management views show all of the identities; business rules ensure and enforce appropriate administrative practices; and permission templates make it easy to delegate identity management and automate non-Windows account de-provisioning around a single Active Directory-based action.

Authentication Services Integration with Third-Party products

Quest Authentication Services extends the innate security of Active Directory through support for, and integration with, a wide variety of products and technologies, including OpenSSH, PuTTY, Apache web server, sudo, and many others. For the latest information, please consult Quest Resource Central at http://rc.vintela.com

Authentication Services Integration with SAP

The Quest Authentication Services Single Sign-On for SAP add-on module extends Quest's proven Active Directory integration technology to SAP R/3 and ABAP applications accessed using SAP Client (SAPgui). Not only does Authentication Services Single Sign-On for SAP provide transparent Active Directory single sign-on from the SAP client, it also provides full mutual authentication and the ability to secure subsequent data communications. Quest Authentication Services Single Sign-On for SAP received SAP certification on April 19, 2007.

Authentication Services Integration with Reporter

Authentication Services ships with a full license of Quest Reporter for every non-Windows user that has joined the Active Directory domain through the product. This provides a powerful set of general access, identity, and rights reports on the Active Directory environment (including the non-AD-enabled non-Windows systems), as well as specialized reports on aspects specific to the Unix environment (such as UID, GID, etc.).

Webthority Integration with Single Sign-on for Java

Webthority is integrated with Single Sign-on for Java so that it can be used as an authentication resource for anyone accessing Java applications via Webthority. In addition, Webthority supports Single Sign-on for Java's Active Directory Federation Service (ADFS) capabilities. In the future, Single Sign-on for Java and Webthority will be merged into a single offering for web single sign-on and web access management.

Password Manager Integration with Defender

Password Manager enables Defender users to securely authenticate (through the Defender one-time password) to the Password Manager portal. This means that a Password Manager administrator has the option to allow Defender users to reset their Active Directory password simply by using two-factor authentication in place of or in addition to answering the security questions.

Defender Integration with Third-Party Solutions

Quest Defender is compatible with any RADIUS-complaint device, ensuring maximum scope and interoperability. In addition Defender is "token agnostic," enabling the Defender software to leverage any OATH-based token from Quest or any other vendor.

Privilege Manager for Unix Integration with InTrust

Version 5.5 of Privilege Manager includes an InTrust Knowledge Pack that allows full interoperability between InTrust and the logs gathered and created by Privilege Manager.

Webthority Integration with Defender

Webthority works seamlessly with Defender to enable two-factor authentication for any web application without requiring changes, edits, or reconfiguration of either the web application or the underlying web server.

APPENDIX: INTEGRATION SUMMARY

The following tables summarize the current and planned integration between Quest One solutions as well as between third-party systems and solutions:

Authentication Services

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
ActiveRoles Server	Additional applications	RSA SecurID
Privilege Manager for Unix	Password Manager	Verisign OTP
Defender		Microsoft-based smartcards
Reporter		OpenSSH
		PuTTY
		Apache
		SAP (ABAP)
		Siebel

Active Role Server

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Authentication Services		SPML
Password Manager		
Defender		

Single Sign-On for Java

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Password Manager	Webthority	SAP NetWeaver Portal

Enterprise Single Sign-on

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Defender	Webthority	Multi-factor authentication
Password Manager		LDAP-based identity stores

Privilege Manager for Unix

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Authentication Services		
Defender		
InTrust		

Defender

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Authentication Services		RADIUS-compliant devices
Webthority		OATH-based tokens
Privilege Manager for Unix		LDAP-based systems
Enterprise Single Sign-on		
ActiveRoles Server		
Password Manager		

Password Manager

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
InSync		HP ProtectTools
Authentication Services		
Single Sign-on for Java		
ActiveRoles Server		
Enterprise Single Sign-on		
Defender		

Webthority

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Defender	Enterprise Single Sign-on	MS SharePoint Server
	Single Sign-on for Java	Outlook Web Access

InSync

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Password Manager		

InTrust

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Privilege Manager for Unix		

Reporter

CURRENT INTEGRATION	PLANNED INTEGRATION	THIRD-PARTY INTEGRATION
Authentication Services		

	Authentication Service	Single Sign-on for Java	ActiveRoles Server	Enterprise Single Sign-on	Password Manager	Privilege Manager for Unix	SafeKeeping	Defender	Webthority	InTrust	Reporter	InSync
Authentication Services			X		X	X		X			X	
Single Sign-on for Java					X				X			
ActiveRoles Server	X				X			X				
Enterprise Single Sign-on					X			X	X			
Privilege Manager for Unix	X							X		X		
SafeKeeping								X				
Defender	X		X	X	X	X	X		X			
Webthority		X		X				X				
InTrust												
Reporter	X											
Password Manager	X	X	X	X				X				X
InSync					X							

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Visit www.quest.com for more information.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site:	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