Copyright

Microsoft, MS, MS-DOS, MS-Mail, MS-Proxy, Exchange, Microsoft Press, Microsoft Access, Internet Information Server, IIS, Internet Explorer, IE are registered trademarks.

Windows, Windows NT, Windows95, Windows98 are copyrights by the Microsoft Corporation Redmond.

Apple, AppleTalk and Macintosh are registered trademarks. Apple Script, Active Help, PowerBook, Power Macintosh, QuikTime and System 7 are copyright by Apple Computer Inc.

Arial and Times Roman are copyright by The Monotype Corporation PCL.

Hewlett Packard, HP, Netserver, Netserver LX Pro and Laser Jet are copyright by the Hewlett Packard Company. CPQ, Deskpro, Proliant, SmartArray, EMEA and SP Connect are registered trademarks of Compaq Computer Corporation.

X86, Pentium, MMX, XENON are registered trademarks of the Intel Corporation.

Lotus Notes is a registered trademark of the Lotus Development Company.

OS/2, IBM, OpenDOC, Power PC, AIX, ThinkPad and ADSM are registered trademarks of the International Business Machine Corporation.

Postscript, PDF, Acrobat and Photoshop are trademarks of Adobe System Inc.

RedHat Linux is a registered trademark of RedHat Inc.

Solaris, SPARC, Java and JavaScript are registered trademarks of the SUN Corporation.

CISCO, PIX, Lightstream and Catalyst are registered trademarks from the CISCO Corporation. Alteon is a register Trademark of the Alteon Websystem Company.

Nortel, NT and Passport are registered trademarks of the Northern Telecom Limited.

Equant is copyright by the Equant Company.

Firewall-1, CVP and FloodGate are registered trademarks of Checkpoint Inc.

RSA SecurID is a trademark of RSA Security Inc., a wholly owned subsidiary of EMC Corporation.

While we have endeavored to supply as complete and accurate a list as possible, Quest Software Solutions makes no warranties, express or implied, as to the completeness and accuracy of this list. This list does not constitute an endorsement of any particular manufacturer.
Table of Contents:

Copyright .......................................................................................................................... 2
Table of Contents: .......................................................................................................... 3
Quest and Vintela Authentication Services—the Market Leader ................................. 4
Overview of VAS and SecurID configuration ................................................................ 5
Best Practices for configuring VAS and SecurID .......................................................... 5
  LDAP Synchronization ................................................................................................ 6
  Job Information .......................................................................................................... 7
  The LDAP Server Information ................................................................................ 7
  LDAP User Search Information ............................................................................... 8
VAS Configuration ........................................................................................................ 8
Unix Agent (PAM) configuration .................................................................................. 10
Application Configuration ............................................................................................ 11
  FTP .......................................................................................................................... 11
  SSH .......................................................................................................................... 11
  AIX 5.3 .................................................................................................................... 11
  AIX 5.1 and 5.2 ........................................................................................................ 11
Should You Require a PIN? ......................................................................................... 12
Supported Platforms ................................................................................................... 13
VAS + SecurID Limitations ......................................................................................... 13
Quest and Vintela Authentication Services—the Market Leader

At its core Vintela Authentication Services provides centralized authentication for Unix, Linux, and Mac systems to Active Directory (AD). With more than 500 current customers and 3 million 'seats', Vintela Authentication Services is the clear market leader in Active Directory integration.

**Quest is the clear market leader in AD integration and identity and directory consolidation**

With an unparalleled relationship with Microsoft and recognized by Microsoft, Vintela Authentication Services is able to offer the most robust support of Active Directory integration on the market. Out of the thousands of companies that partner with Microsoft, only Quest was named the 2007 ISV of the Year by Microsoft. Quest also won the same award in 2004 and has either won or been a finalist in each of the last four years. This means that no matter what your Active Directory environment looks like, Vintela Authentication Services can extend it to your Unix, Linux, and Mac systems. This includes support for multiple forests and domains, Windows 2000 and 2003 at any Forest functional level, and even two-way, one-way, and no-way trusts. In addition, Vintela Authentication Services provides the flexibility to offer rich, benefit laden deployment in both schema-based and schema-less options.

**Benefits of Vintela Authentication Services**

Vintela Authentication Services provides many significant benefits to companies seeking to simplify identity and access management by leveraging Active Directory for non-Windows system and application authentication and authorization. Among the benefits this approach offers to Unix, Linux, and Mac systems and a number of applications, some of the most popular include:

- Extending the benefits of Windows Group Policy to Unix, Linux, and Mac systems
- Consolidate Unix, Linux, and Mac identities in Active Directory to simplify your identity management challenges
- Easily migrate from NIS (Network Information Service) to Active Directory
- The flexibility to deploy the solution specific to the unique requirements of your Unix environment, according to your timeline and priorities, and with a simple path to identity best practices
- Increased efficiency, security, and compliance through AD-based single sign-on, reduced sign-on, and centralized authentication
- Reduced complexity and faster deployment for existing or planned identity framework implementation
Overview of VAS and SecurID configuration

This guide is provided to assist in the integration of RSA SecurID and Quest Software’s Vintela Authentication Services (VAS) product. This integration guide will provide guidance on how to configure a two-factor authentication solution that leverages the benefits of your Active Directory infrastructure.

After you have finished with this integration you will have a Unix/Linux solution that provides the enhanced security of one-time passwords (OTPs) and tight integration for Kerberos enabled applications (single sign-on for example).

The figure below demonstrates a simplified flow of events that occur during the login event when both VAS and RSA SecurID are configured as suggested in this guide. It may be useful to refer to this figure throughout the process of implementing the integration suggested in this guide.

![Diagram](image)

Figure 1 - Login Event After SecurID and VAS Integration

Best Practices for configuring VAS and SecurID

RSA’s SecurID product and Quest Software’s VAS solution both leverage the stackable nature of the Unix PAM (Pluggable Authentication Module) architecture to provide a compatible solution, but there is more to getting these two products working together than simply stacking two PAM modules. By following the best practices in this section, you will enable the most complete and easy to use integration of the two products.
LDAP Synchronization

The first integration issue to address is user synchronization. All users who are to authenticate using RSA SecurID must exist in database internal to the RSA product. All VAS users must exist in Active Directory. If both the SecurID and VAS are to be used in conjunction these databases must be synchronized so that usernames are the same in both databases. Fortunately RSA’s authentication Manager does provide a tool that allows you to synchronize the RSA user database with an external LDAP store on a regular interval.

To add a user synchronization job open the RSA Authentication Manager console and select User > LDAP Users > Edit Synchronization.

![Figure 2 - Opening the LDAP Synchronization Page](image)
You should now see the LDAP synchronization configuration page as shown in Figure 3.

Figure 3 - LDAP Synchronization Configuration Page

**Job Information**
Provide a name for your synchronization job and specify an interval that suites your environment (the default interval is every 12 hours).

**The LDAP Server Information**
The synchronization job supports three different LDAP server types. The server types are really nothing more than schema mappings. When you choose Active Directory as your server type you are simply saying to use the following schema mapping:
chDefaultLogin=samaccountname
chLastName=sn
chFirstName=givenName
chDisabledUser=UserAccountControl
chGroupMembers=Member

This schema mapping should be sufficient in almost all circumstances, but if it is
necessary to make a custom Active Directory schema mapping this can be
accomplished by modifying the “active.map” file found on your RSA server in the
utils/toolkit directory.

LDAP host can information be configured with the hostname or IP Address of an Active
Directory domain controller or you can configure a VAS LDAP proxy instance on your
RSA server providing instead the proxy’s listening address and port.

Why configure a proxy instance for LDAP Synchronization?
The proxy provides an alternative to setting up SSL and certificates to secure traffic
between your machine and the Active Directory domain controller. If you are installing
your RSA server on a UNIX machine that will be joined to the Active Directory domain
using VAS, you can take advantage of that fact to secure your LDAP communications
via Kerberos. The LDAP Synchronization job can communicate in clear text over the
loopback interface without any worries, while the VAS LDAP proxy provides an
encrypted tunnel for that information directly to a domain controller. Additionally the
LDAP proxy will make the synchronization job more robust by failing over to alternate
domain controller if the first domain controller is unavailable.

To configure the VAS LDAP proxy you must add the following to the bottom of the
/etc/opt/quest/vas/vas.conf file on the RSA server machine.

[vasproxyd]
syncProxy = {
    listen-addrs = 127.0.0.1:389
}

LDAP User Search Information
Provide an appropriate search filter search base and search scope in this section. A
reasonable search filter might be “(&(objectcategory=person)(objectclass=user))”. Your
search scope and search base are completely determined by the location of your users
within Active Directory. If all your users are in one container, you can specify a “One
Level” search and point the search base to that container.

VAS Configuration
VAS can be configured to use any attribute as the username attribute. Changing this
attribute changes which value a user is required to provide as their username at login.
Naturally this attribute should be samaccountname since this is the same attribute that
SecurID is using for usernames. The default VAS configuration uses User Principal
Name (UPN) as username attribute so you may need to change your default VAS
configuration. In many cases you could safely leave VAS configured to use UPN as the
username attribute. This is because the value of samaccountname and the username
part of the UPN are same by default and in may Active Directory deployments this never
changes. It becomes truly necessary to configure VAS to use samaccountname as the username attribute if, in your Active Directory deployment, you regularly change the value of users samaccountname so that it differs from the username portion of the UPN. Best practice dictates that samaccountname should be used to avoid potential issues with this in the future.

To change the default username attribute used by VAS modify the /etc/opt/quest/vas/vas.conf file adding the following setting:

```bash
[vasd]
username-attr-name = samaccountname
```

It is recommended that VAS Group Policy (VGP) be deployed as a means of easily managing vas.conf file changes on all Unix machines through one simple interface. All vas.conf changes can be made through the VGP MMC interface.

![Figure 4 - Configuring VAS to use samAccountName as the User Naming Attribute via VGP](image)
Unix Agent (PAM) configuration

To get a working PAM configuration simply modify the PAM configuration file(s) so that the pam_vas3.so module is directly beneath the pam_securid module. The following is an example of a working configuration from a Solaris 10 machine configured with SecurID and VAS 3.1.2:

telnet auth  requisite  /opt/pam/lib/pam_securid.so debug
telnet auth  sufficient /opt/quest/lib/security/$ISA/pam_vas3.so create_homedir debug trace
telnet auth  requisite   /opt/quest/lib/security/$ISA/pam_vas3.so echo_return
...<Other Modules Below>...

VAS comes with a command-line utility that facilitates VAS PAM configuration. During the process of joining a Unix/Linux machine to your Active Directory domain this command-line tool configures all PAM services for VAS authentication. Versions of VAS Post 3.2 (3.3 or later) always place themselves below the pam_securid.so module. This means if you have already configured the SecurID PAM module on one of your machines, simply joining the domain will result in the recommended PAM configuration. If you have a version of VAS prior to 3.3, you will need to manually modify your PAM configuration.

If you have not yet installed the SecurID PAM module do so now. There is a simple script included with the pam_securid distribution media that facilitates installation.

When configuration is complete the user will be faced with two prompts before they can access the system. The successful login experience is depicted in Figure 5.

```
root# telnet unix-rsa
Trying 10.5.37.55...
Connected to unix-rsa.rc.red.vas.
Escape character is '^]'.
Enter USERNAME:brian
Enter PASSCODE:
Password:
Last login: Wed Aug 22 14:34:06 from 10.5.38.26
Sun Microsystems Inc.  SunOS 5.10  Generic January 2005
bash-3.60$ klist
Ticket cache: FILE:/tmp/krb5cc_540934
Default principal: brian@RC.RED.VAS
Valid starting             Expires              Service principal
08/22/07 14:37:20 08/22/07 15:37:20 krbtgt/RC.RED.VAS@RC.RED.VAS
08/22/07 14:37:20 08/22/07 14:47:20 host/unknown.rc.red.vas@RC.RED.VAS
-bash-3.60$
```

Figure 5 - Successful log in experience with both VAS and SecurID configured

You can configure the pam_securid module as either requisite or required. This change only affects unsuccessful login attempts (successful login attempts will remain the same with either configuration). If you configure pam_securid as requisite, entering a bad passcode will result in immediate failure (you will never even see the password prompt). If, on the other hand, you configure pam_securid as required, entering a bad
passcode will still cause authentication to fail, but not until you have been prompted for your AD user password by the pam_vas3 module. Configuring pam_securid as requisite makes easier for end users to see whether they typed their passcode or password wrong.

Application Configuration

For a Unix service such as telnet, ssh, or ftp to work correctly with SecurID and VAS, the application must be compiled with PAM support as well as supporting interactive prompting. Many applications will need no configuration to work correctly. There are, however, some important exceptions.

FTP

Most vendor provided FTP servers do not support interactive prompting and as a consequence cannot be used with the configuration demonstrated by this guide.

SSH

Most commercial SSH servers support interactive prompting. This is usually advertised “Keyboard-Interactive” prompting.

OpenSSH

Most versions of OpenSSH, while providing support for interactive prompting, require configuration before they will properly prompt in keyboard interactive mode. To verify that your OpenSSH configuration supports keyboard interactive authentication open your sshd.conf file and make sure “ChallengeResponseAuthentication” is set to yes while “PasswordAuthentication” is set to no. Also make sure that the “UsePAM” option is set to yes. Restart the sshd process if any changes were made. If your get errors about “UsePAM” not being supported upon restarting sshd, it will be necessary to recompile SSH with PAM support or acquire a new version that comes pre-built with PAM support.

AIX 5.3

All applications on AIX 5.3 support the AIX native LAM architecture as well as PAM. The default authentication method is LAM, for SecurID and VAS to work correctly together you must configure all applications to use PAM authentication. This is accomplished by modifying /etc/security/login.cfg. Simply change the “auth_type” variable from “STD_AUTH” to “PAM_AUTH”.

AIX 5.1 and 5.2

AIX does support PAM authentication as early as AIX 5.1; however, none of the applications shipped with these versions of AIX are compiled with PAM support. This means that any application that you need to work with SecurID must be compiled with PAM support or acquired from a third party. VAS does support native LAM authentication on these platforms, but as RSA only supports the PAM architecture you will need use configure PAM authentication and acquire PAM enabled applications to get VAS and SecurID working together.
Should You Require a PIN?

For VAS to be able to provide Kerberos credentials after a user logs in, it is necessary that a user’s AD password be provided. If you require a PIN to be provided, you will still need to provide the user’s AD password.

This can complicate login for end users by requiring them to have one thing (OTP) and know two separate things (PIN and AD password) before they can login. This gives the user an opportunity to forget two different things, potentially increasing help desk calls. It is therefore suggested that when using VAS with SecurID that the user’s AD password be used for the second authentication factor instead of a PIN.

PINs are disabled on a user-by-user basis through the RSA Authentication manager console. To disable any given user’s pin, open the RSA Authentication manager and select **User > Edit User**. Once you have selected your user, you will be presented with the edit user dialog depicted in Figure 6. Uncheck “Required to Create a PIN” and “Allowed to Create a PIN” and click **OK** to complete the process.

![Figure 6 - Disabling a User PIN](image-url)
Supported Platforms

VAS supports all the platforms supported by RSA SecurID. SecurID lists the following as supported platforms on the RSA website (http://www.rsa.com/node.aspx?id=1177). Refer to the RSA website for the most up to date information.

- HP-UX 11.00, 11i (PA-RISC 2.x)
- HP-UX 11iv2 (Itanium®)
- HP-UX 11i
- HP-UX 11i on PA-RISC 2.x processors
- Sun® SolarisTM 10 x86 on 32-bit (Intel®)
- Sun® SolarisTM 10 x86 on 64-bit (Intel® Xeon and AMD Opteron)
- Sun® SolarisTM 10 on 64-bit (UltraSPARC)
- Sun® SolarisTM 8, 9 and 10
- Sun® SolarisTM 8 and 9 on UltraTM SPARCTM processors
- SUSE Linux Enterprise Server 9 (SP3) on 64-bit (Intel® Xeon, AMD Opteron)
- SUSE Linux Enterprise Server 10 on 64-bit (Intel® Xeon, AMD Opteron)
- SUSE Linux Enterprise Server 9
- Red Hat® Enterprise Linux® AS/ES/WS 4.0 on 64-bit (Intel® Xeon and AMD Opteron)
- Red Hat® Enterprise Linux® AS/ES 3.0 and 4.0
- AIX® 5L v5.3 with ML2, ML3, TL4
- AIX® 5L 5.3 with TL5 (SP6) 64-bit (RISC/6000® PowerPC®)
- IBM® AIX® 5L v5.1 and 5.2 on PowerPC® and RISC System/6000® processors

RSA currently provides three different Unix agent packages. This supported platform list includes all the platforms supported by all three of the Unix agent packages.

VAS + SecurID Limitations

One of the strengths of VAS is that it provides a number of ways to map a user’s local identity on a given machine to its global Identity in the Enterprise Directory (Active Directory). This means if a user has two different usernames on two different Unix machines, VAS can be configured to recognize each of these usernames as belonging to the same Active Directory Identity. Unfortunately SecurID has no mechanism for mapping multiple identities into one, because of this you cannot use VAS local override files to change the username of a user, nor can you use PSS to map an AD user to local account with a different username when configuring VAS to work with SecurID. You can still use local override files or PSS to override other Unix user attributes.

There is currently no mechanism provided by either VAS or SecurID for retrieving a user’s AD password from the ACE server. This means that Unix users will always be required to provide both their SecurID token code and their AD user password to gain access to a Unix Resource.