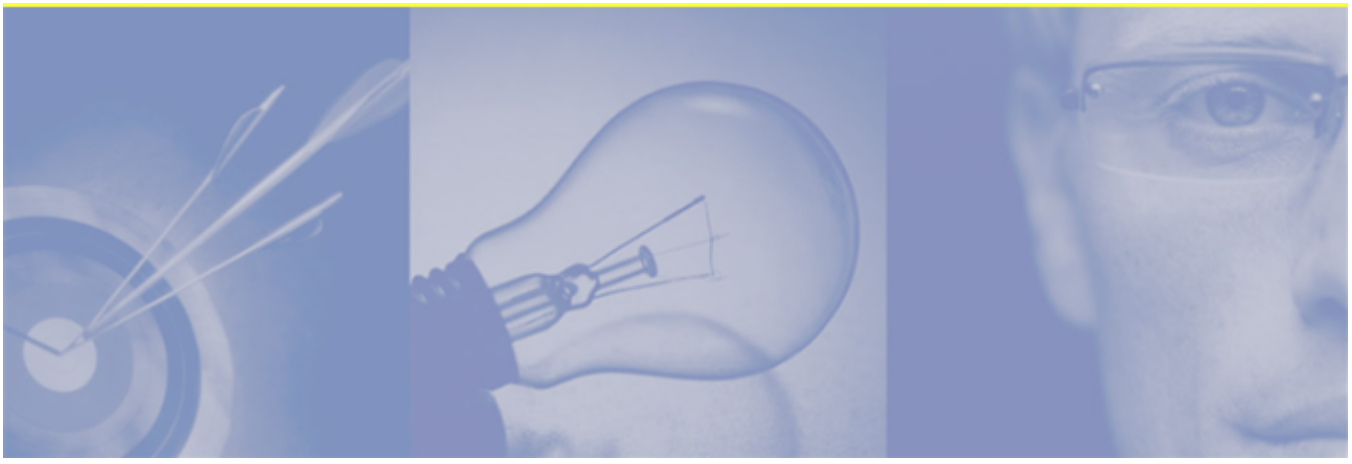
QUEST SOFTWARE
Simplicity At Work™

Authentication Services 4.1



Quest Defender Integration Guide

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Patents

Trademarks

Third-Party Contributions

This product may contain one or more of the following third-party components. For copies of the text of any license listed, please go to *http://www.quest.com/legal/third-party-licenses.aspx* .

Component	Notes
Apache Commons 1.2	Apache License Version 2.0, January 2004
Boost	Boost Software License Version 1.0, August 2003
Expat 2.0.0	© 1998, 1999, 2000 Thai Open Source Software Center Ltd
Heimdal Krb/GSSapi 1.2	© 2004 - 2007 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.
OpenSSL 0.9.8d	This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) © 1998-2008 The OpenSSL Project. All rights reserved.

Contents

Chapter 1

About This Guide

Topics:

The *Quest Defender Integration Guide* is intended for Windows and non-Windows system administrators, network administrators, consultants, analysts, and any other IT professionals who will be integrating Quest Defender with Authentication Services for token-based two factor authentication. This guide walks you through the process of installing and configuring the necessary Quest Defender access policies and Group Policy settings.

About Quest Software

Note: Quest Authentication Services, formerly Vintela Authentication Services, was re-branded for the 4.0 release.

Quest Software, Inc. simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. Contact Quest for more information:

Contacting Quest Software

Phone:	1.949.754.8000 (United States and Canada)
Email:	*info@quest.com*
Mail:	Quest Software, Inc.
	World Headquarters
	5 Polaris Way
	Aliso Viejo, CA 92656 USA
Web site:	*quest.com*

Quest One Identity Solution

This product is a component of the Quest One Identity Solution, a set of enabling technologies, products, and integration that empowers organizations to simplify identity and access management by:

- Reducing the number of identities
- Automating identity administration
- Ensuring the security of identities
- Leveraging existing investments, including Microsoft Active Directory

Quest One improves efficiency, enhances security and helps organizations achieve and maintain compliance by addressing identity and access management challenges as they relate to:

- Single sign-on
- Directory consolidation
- Provisioning
- Password management
- Strong authentication
- Privileged account management
- Audit and compliance

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal.

Information Sources	Contact Points
Quest Support	Support Portal: *https://support.quest.com* Quest Support Portal gives you access to these tools and resources: • **Search Knowledge Base** Search our extensive Knowledge Base to quickly find answers to common questions. Popular solutions, latest releases, product notifications, product documentation, patches, video tutorials, are just a few clicks away. New content is added every day. • **Communities** Join other peers to get solutions, join discussion forums, hear from experts and voice your opinion in your product community. • **Manage Service Requests** Submit a Service Request as well as update and review the status of current Service Requests. • **Additional Resources** • Obtain Support by Product • Software Downloads • Documentation You can submit a service request with Quest Support at *https://support.quest.com/CaseManagement/ManageServiceRequest.aspx* or phone: 1.800.306.9329.
Public Forum	The Community site is a place to find answers and advice, join a discussion forum, or get the latest documentation and release information: *All Things Unix Community.*
Support Services	View *Support Services Overview Datasheet* for a detailed explanation of support programs, online services, contact information, policies and procedures at: *Support Services*. Find out everything you need to know about Quest Software's Global Support at: *Support Policies*

Chapter 2

Introducing Quest Defender

Topics:

Quest Defender enhances security by enabling two-factor authentication to network, Web, and applications-based resources. Quest designed Defender to base all administration and identity management on an organization's existing investment in Active Directory and eliminates the costs and time involved in setting up and maintaining proprietary databases.

Quest supports Quest Defender integration on all platforms that support Authentication Services, except Mac OS X and AIX 5.2 or earlier.

Note: On AIX 5.3 and later you must use PAM authentication.

In addition, Defender works with any OATH-compliant hardware token enabling organizations to select the most appropriate token for their users. By leveraging an organization's existing investment in Active Directory and supporting multiple token vendors, Defender enables organizations to increase security and achieve and sustain compliance in a cost-effective manner.

Quest Defender Integration

Quest Defender provides strong authentication capabilities.

Why is strong authentication an important part of an Active Directory bridge solution?

When Authentication Services integrates Unix with Active Directory it provides centralized access control and password policy enforcement. However, there are situations where security policies dictate a stronger level of authentication. Authentication Services addresses this need with optional strong authentication capabilities. Customers now can use the same solution for integrated Active Directory authentication and strong authentication. Organizations that have tight security requirements will no longer be forced to purchase and implement a third-party solution.

How is strong authentication used with an Active Directory bridge solution?

An organization may have many Unix systems deployed in a traditional highly-secure DMZ environment. As they are integrated with Active Directory, they will require an Active Directory credential to authenticate. Now, an additional layer of authentication can be added for administrators accessing these systems, using either a hardware or software token.

If an organization has integrated hundreds or thousands of Unix systems with Active Directory, a system administrator can now use the same Active Directory credential to access all of them. An additional level of security can be easily added by requiring the system administrator to use one-time password (OTP) in additional to the Active Directory credential.

How do Authentication Services' strong authentication capabilities compare to other Active Directory bridge solutions?

Strong authentication combined with an Active Directory bridge is a unique and critical differentiator for Quest. No other Active Directory bridge vendor offers strong authentication as an integrated part of its solution, and no strong authentication vendor offers Unix coverage and Active Directory integration.

Is there an additional charge for strong authentication with Authentication Services 4.x?

There is no additional cost for strong authentication with Authentication Services 4.x; it is a new feature available to new and upgrading customers.

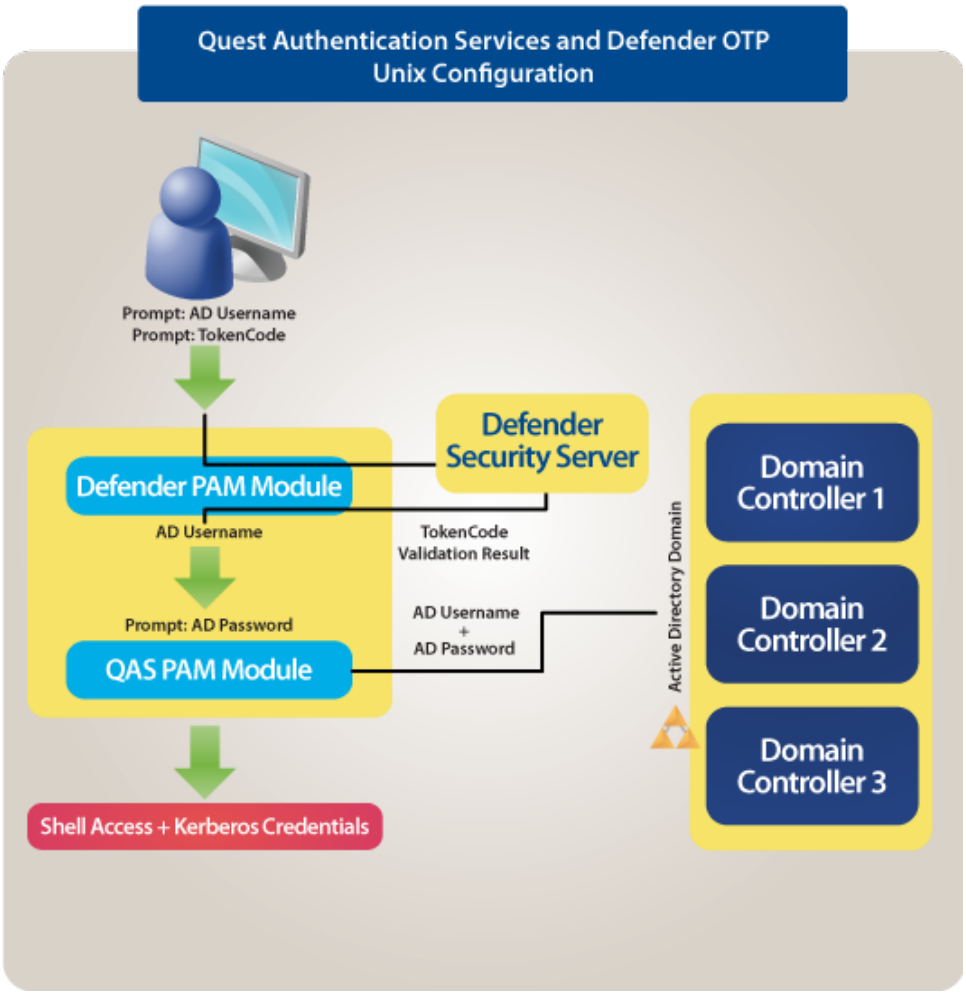
Authentication Services 4.1.0 provides strong authentication for up to 25 users at no additional cost through included licenses and tokens for Quest Defender. These licenses will cover and secure 25 of an organization's Unix system administrators. Strong authentication support for additional end-users is available at an additional per-user cost.

How does strong authentication with Authentication Services 4.x work?

Authentication Services 4.1.0:

- Includes strong authentication modules and native packages for all supported platforms (100+)
- Remotely deploys and installs the strong authentication module
- Provides hardware and software tokens for one-time passwords
- Enables policy-based configuration of strong authentication through Active Directory Group Policy

This graphic describes the flow of events that occur during a Unix or Linux login after both Quest Defender and Authentication Services are configured according to this guide:



Quest Defender Installation Prerequisites

Before you install Quest Defender on your host, ensure that you have:

1. Installed a Defender security server in your Active Directory domain
2. Installed the Defender Microsoft Management Console (MMC) snap-in
3. Installed Authentication Services on your Unix or Linux machine

Chapter 3

Configuring Quest Defender

Topics:

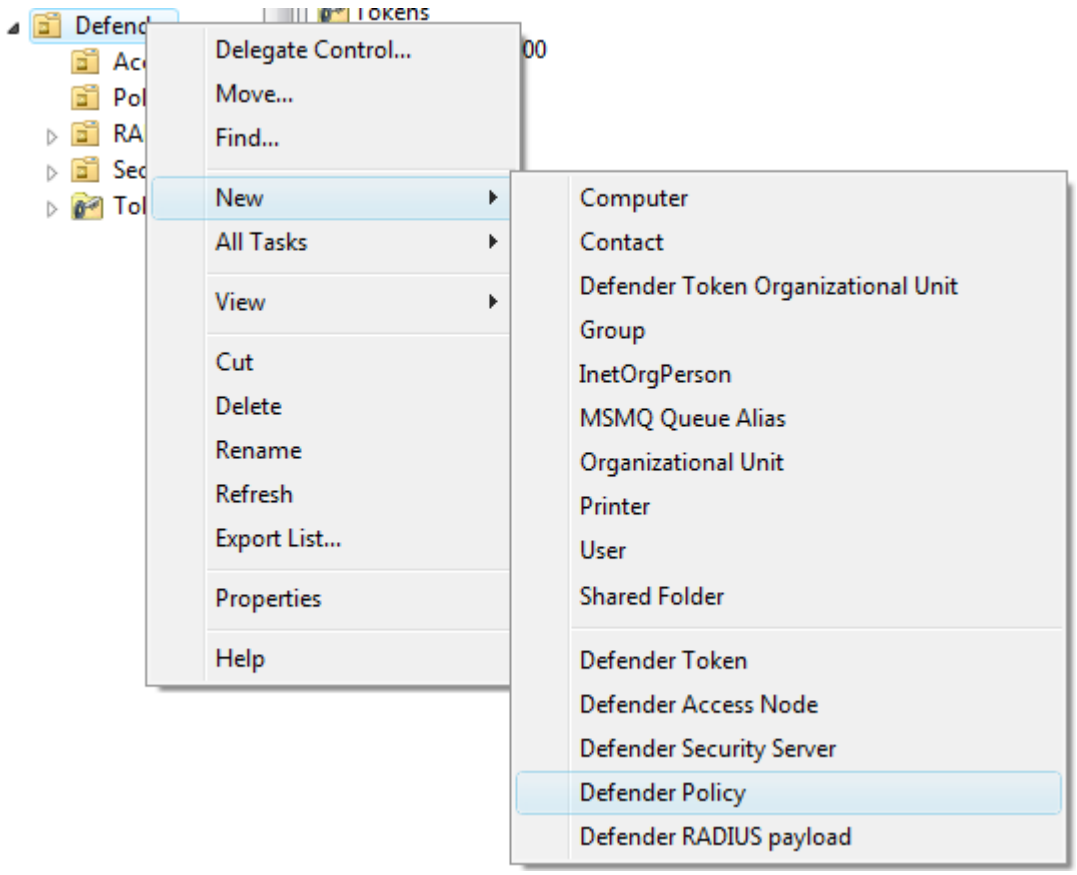
To integrate Quest Defender with Authentication Services, perform the tasks described in this section.

Create a Security Policy

You use a security policy to specify which type of credential is to be sent to the Defender security server.

To create a security policy

1. Open Active Directory Users and Computers.
2. Right-click **Defender** and navigate to **New | Defender Policy** to launch the creation wizard.



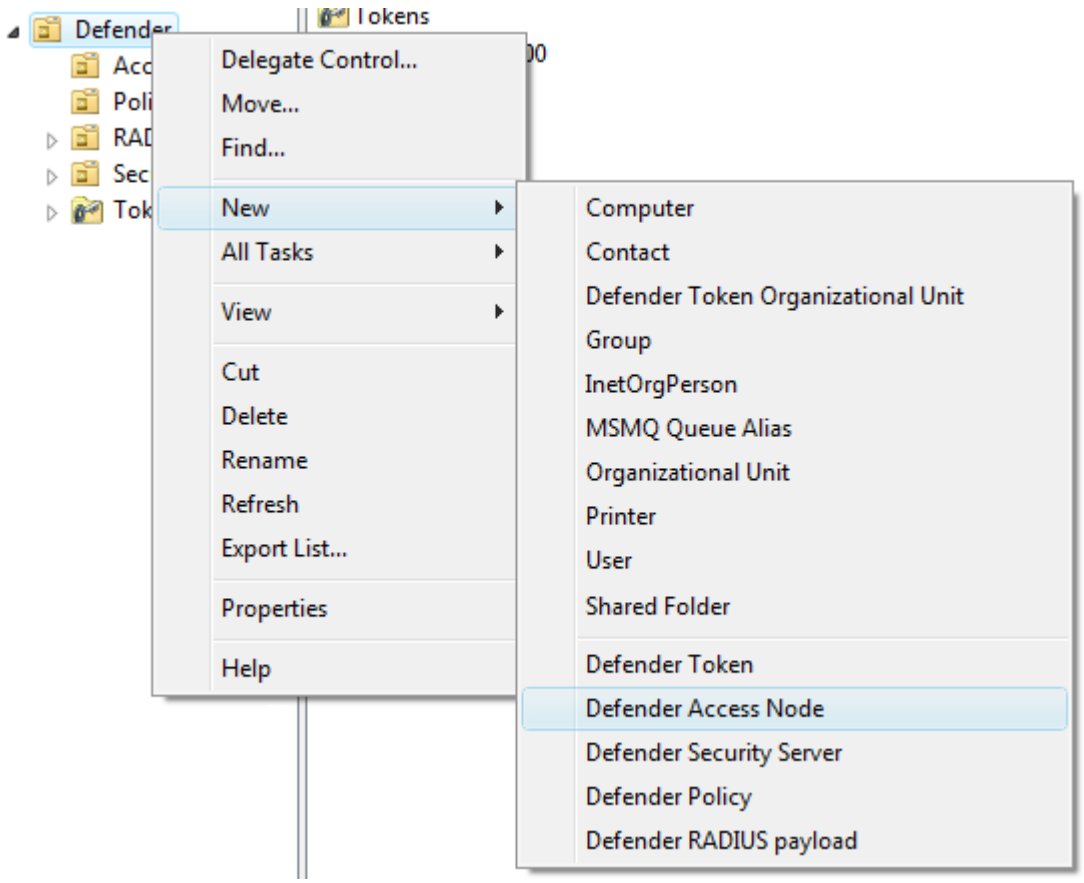
3. Give the security policy a **Name** and **Description** and click **Next**.
4. Select **Token** for *Method* and click **Next**.
5. Select **None** for the *Method* and click **Next**.
6. Continue through the rest of the wizard, accepting the defaults and click **Finish**.

Create an Access Node

An access node is used to associate a security policy and a Defender security server to a machine or subnet of machines. In order to complete this task, you need to know the IP address of the machine or IP address and subnet mask of the subnet of machines that you would like to secure with Defender and Authentication Services.

To create an Access node

1. Open Active Directory Users and Computers.
2. Right-click **Defender** and navigate to **New | Defender Access Node** to launch the creation wizard.



3. Give the access node a **Name** and **Description** and click **Next**.
4. Select a **Node Type** of *Radius Agent*.

   Note: `pam_defender` only works with *Radius Agent*.

5. Select the appropriate *User ID* for your environment based on the information below, then click **Next**.

   The User ID you select must match the attribute that you are using in Authentication Services for Unix user name. Look in the **Preferences** of the Authentication Services Control Center to determine which attribute Authentication Services is configured.

User ID	Description
SAM Account Name	This is the default Unix user name for Authentication Services 4.1.0. It refers to the `sAMAccountName` attribute of the user.
User Principal Name	Previous versions of Authentication Services used this as the default Unix user name. It refers to the `userPrincipalName` attribute of the user.
Defender ID	This refers to the `defender-id` attribute of the user, which is part of the Defender schema extension. You could configure this as the Unix user name, but Quest does not recommend that.
Proper Name	This refers to the `cn` attribute of the user.

6. Enter the **IP Address** of the machine or subnet of machines.

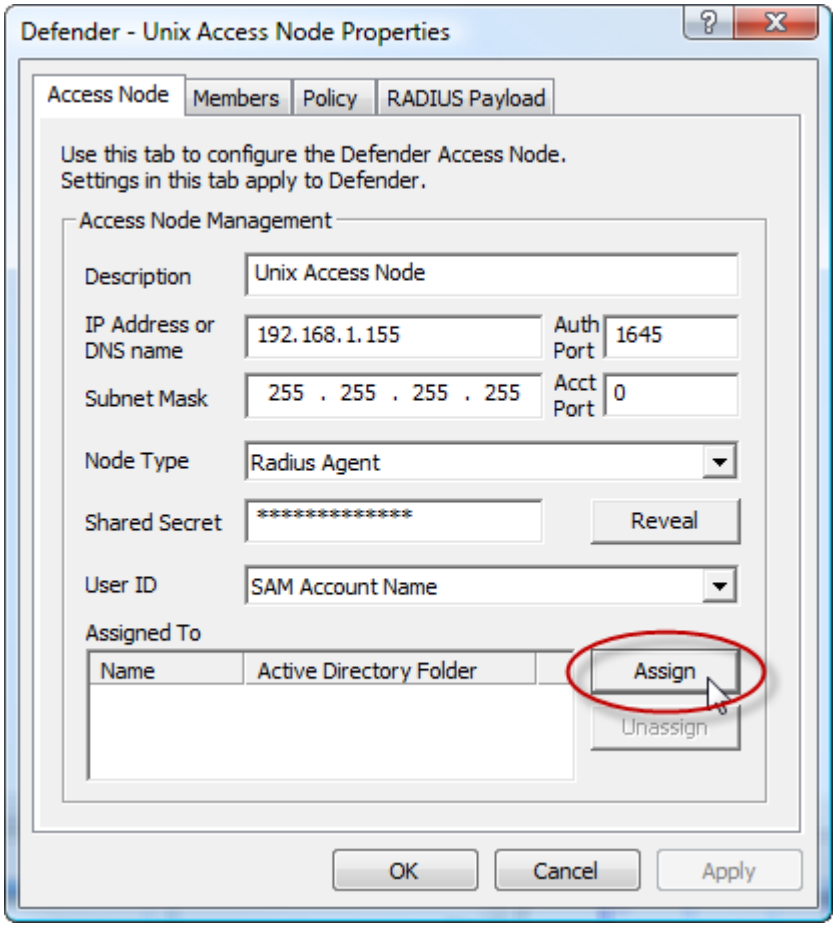
7. Enter the **Port** to use to establish a connection with the Defender security server (the default for a Radius Agent is port 1812).
8. Change the **Subnet Mask** from **255.255.255.255** to the appropriate value if you plan to use a subnet of machines.
9. Enter a *Shared Secret* to use in radius communications with the Defender security server and click **Next**.
10. Click **Finish** to complete the wizard.

Assign the Access Node to the Security Server

You must assign an access node to a Defender security server in order for machines assigned to that access node to know where to send one-time passwords for authentication.

To assign the access node to the security server

1. Open Active Directory Users and Computers.
2. Under the *Defender* node, open **Access Nodes**.
3. Double-click the access node that you created previously.
4. On the *Access Node* tab, click **Assign**.



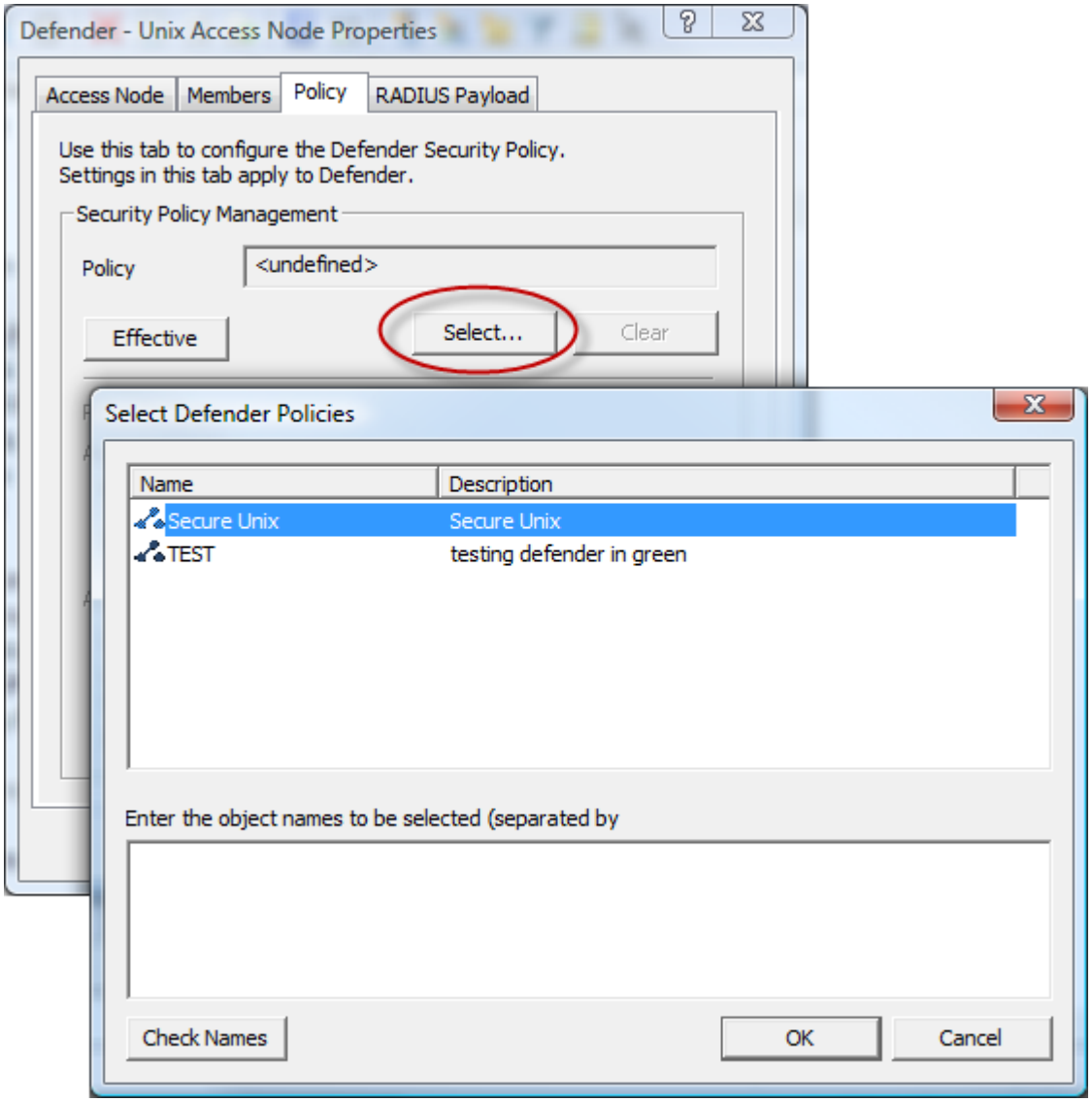
5. Select your Defender security server from the list and click **OK**.
6. Click **OK** to save your changes to the access node.

Select the Security Policy for the Access Node

An access node needs security parameters to follow as one-time password services are extended to the machines assigned to the access node. Use this step to assign a previously created security policy to your access node.

To select the security policy for the access node

1. Open Active Directory Users and Computers.
2. Under the *Defender* node, open **Access Nodes**.
3. Double-click the access node that you created previously.
4. On the *Policy* tab, click **Select**.



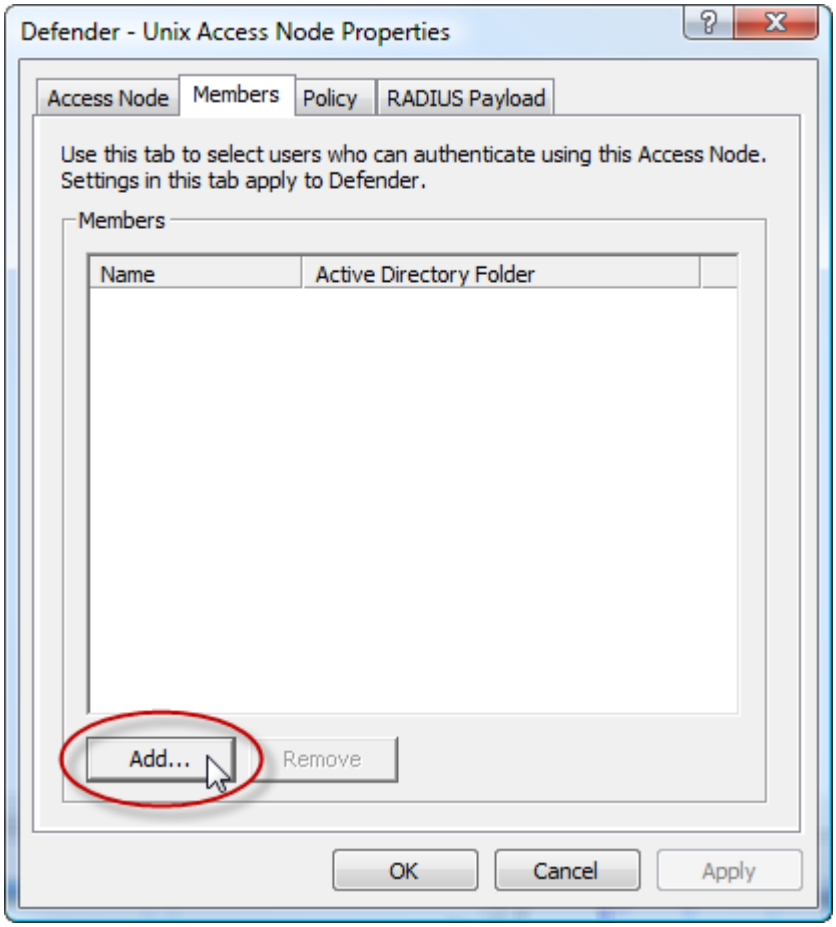
5. Select your security policy from the list and click **OK**.
6. Click **OK** to save your changes to the access node.

Add Members to the Access Node

This step is optional. If you only want to use Defender one-time passwords with specific users, then add members to the access nodes. You can add users individually or groups as members of an access node. If you add no member to the access node, all users will be required to use one-time passwords, including local Unix users such as root.

To add members to the access node

1. Open Active Directory Users and Computers.
2. Under the **Defender** node, open **Access Nodes**.
3. Double-click the access node that you created previously.
4. On the *Members* tab, click **Add**.



5. Find the users and groups that you want to add as members and click **OK**.

   Note: Defender does not support implicit group membership.

6. Click **OK** or **Apply** to save your changes to the access node.

Add One-Time Password Tokens

Quest Defender supports many different types of hardware and software tokens. Before you can use one-time passwords to access your Unix and Linux machines, you must add your tokens to Active Directory so they can be assigned to users.

To add one-time password tokens

1. Open Active Directory Users and Computers.
2. Under the **Defender** node, open **Import Tokens** for hardware tokens

   - OR -

   Open **Program Tokens** for software tokens.

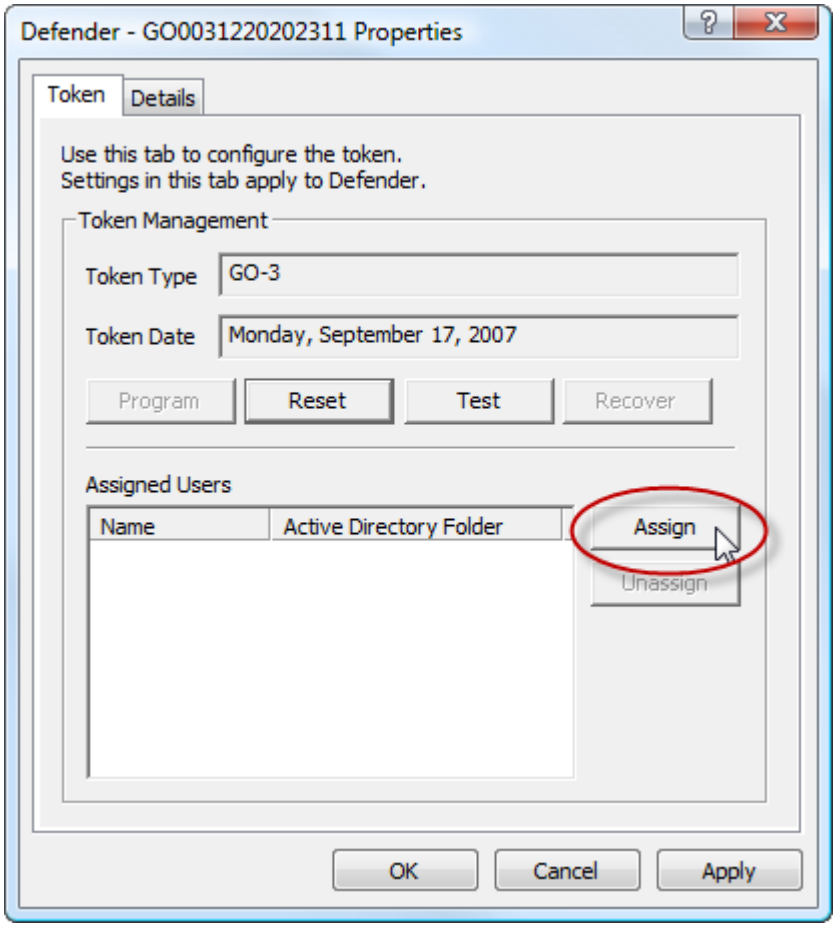
Note: Refer to the Quest Defender documentation for specific instructions on adding your tokens.

Assign Tokens to Users

Once your tokens are added to Active Directory, you can assign them to users.

To assign tokens to users

1. Open Active Directory Users and Computers.
2. Under the *Defender* node, open **Tokens**.
3. Double-click a token that you created in the previous section.
4. On the *Token* tab, click **Assign**.



5. Select the desired user and click **OK**.
6. Click **OK** to save your changes to the token.
7. Repeat for each user.

Chapter 4

Configuring Authentication Services

Topics:

You may either configure Authentication Services to integrate with Quest Defender using Group Policy or manually. Quest recommends you use Group Policy.

Group Policy Configuration

Authentication Services relies on Group Policy for managing the configuration of options and features. To enable one-time password support for Authentication Services through Defender you must modify a Group Policy setting. This setting allows you to turn `pam_defender` configuration on or off and also allows you to select which services (login applications) you want it to support. It gathers the rest of the one-time password configuration information it needs on the Unix or Linux machine from the access node and other Defender objects in Active Directory. This Group Policy can only apply to machines running Authentication Services that have `pam_defender` installed. Also, if it can not find an access node that applies to the machine, it makes no configuration changes.

To Enable One-Time Password Authentication for Unix

1. In the Group Policy Object Editor, navigate to **Unix Settings | Quest Defender**.
2. Double-click the Defender Settings policy in the right-hand pane.
3. Click **Enable Defender PAM authentication**.
4. Configure Defender to require a one-time password for specific login services, or all login services.

   A login service is any process that authenticates a user to a Unix host. You configure login services for PAM in the `pam.conf` file. By default `sshd` and `ssh` are automatically configured since this is the most typical scenario. You can specify additional services. The name of the service must correspond to the service name in `PAM.conf`. On some platforms the service names may differ, in that case, specify all service names for all platforms where you have installed Quest Defender.

   a) To prompt for a one-time password for all services, select **Require Defender PAM authentication for all services**.
5. Click **OK** to save your settings and close the *Defender Settings Properties* dialog.

Apply One-Time Password Authentication Settings

The configuration of the one-time passwords are applied periodically according to a configurable Group Policy refresh interval (by default every 90 minutes).

To force a Group Policy refresh

Note: Your machine must already be joined to the domain to force a Group Policy refresh.

1. Log in to the Linux or Unix machine.
2. At a command prompt, execute the following command as root:

   ```
   /opt/quest/bin/vgptool apply
   ```

   The output from this command, when one-time passwords are successfully enabled, look similar to the following example:

   ```
   root@testmachine:~# vgptool apply

   Group Policy Apply - CallType: REFRESH


   Updating VGP From Policy
   ------------------------
   [vgp_vgpext.so]

   Accumulating Settings from GPOs
   -------------------------------
   GPO: Defender DEMO  CSE: vgp_defender.so
   ```

```
GUID: 1EBC7D87-EFB7-4376-AA1E-3CE5850AC5E5  PTYPE:
786318DB-DE76-42F2-8A57-F1E0C3ACE113

Applying Settings Changes
-------------------------
[vgp_licext.so]
[vgp_vasext.so]
[vgp_scecli.so]
[vgp_sudoext.so]
[vgp_dfc.so]
[vgp_unixext.so]
[vgp_sshcfg.so]
[vgp_samba.so]
[vgp_defender.so]
  Quest Defender Policy
    Adding Defender authentication module
    Current defender.conf (showing server information only)
      10.5.37.22:1645
    Current pam_radius_acl.conf
      *:testuser1
      *:testuser2
      *:testuser3
[vgp_qpm4u.so]
[vgp_admext.so]
```

3. Login using the one-time password.

Manual Configuration

You can configure one-time password information manually. Manual configuration requires a machine running Authentication Services that has `pam_defender` installed. The machine must also be joined to an Active Directory domain. If an access node cannot be found that applies to the machine, no configuration changes are made.

Configuring with VASTOOL

To configure one-time passwords with `vastool`

1. Log in to the Linux or Unix machine.
2. At a command prompt, execute the following command as root:

   ```
   /opt/quest/bin/vastool otp configure radius
   ```

   The output from this command when one-time passwords are successfully enabled look similar to the following example:

   ```
   root@testmachine:~vastool otp configure radius
   Configuring defender.conf
     Server: 10.5.37.22  Port: 1645
   Configuring PAM Radius Access Control List
     testuser1
     testuser2
     testuser3
   ```

3. To configure `pam` for all services, run the following command as root:

   ```
   /opt/quest/bin/vastool otp configure pam
   ```

   - OR -

To configure pam for `gdm`, run the following command as root:

```
/opt/quest/bin/vastool otp configure pam gdm
```

Note: When successful these commands produce no output.

4. Log in using the one-time password.

Troubleshooting

You can configure the `pam_defender` module to log debug information to a file.

To configure `pam_defender` to log debug information

1. Run the following command:

   ```
   /opt/quest/bin/vastool otp configure trace <path to log file>
   ```

   This creates the `/tmp/pam_def.ini` file that the defender `pam` module uses to determine whether it should log debug information and adds the necessary information to this file to configure full debug.

2. Modify the `pam` configuration for your system, as follows:
   a) Find all lines that specify the `pam_defender` module.
   b) Add the "debug" option to the end of those lines.

Index