Copyright 2022 One Identity LLC.
ALL RIGHTS RESERVED.

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

The information in this document is provided in connection with One Identity products. No license,
express or implied, by estoppel or otherwise, to any intellectual property right is granted by this
document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE
TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,
ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR
STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-
INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT,
CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT
LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF
INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF
ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes
no representations or warranties with respect to the accuracy or completeness of the contents of this
document and reserves the right to make changes to specifications and product descriptions at any
time without notice. One Identity does not make any commitment to update the information
contained in this document.

If you have any questions regarding your potential use of this material, contact:
One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office
information.

Patents
One Identity is proud of our advanced technology. Patents and pending patents may apply to this
product. For the most current information about applicable patents for this product, please visit our

Trademarks
One Identity and the One Identity logo are trademarks and registered trademarks of One Identity
LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit
our website at www.OneIdentity.com/legal. All other trademarks are the property of their
respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property
damage, for which industry-standard safety precautions are advised. This icon is
often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data
if instructions are not followed.

Safeguard Authentication Services Defender Integration Guide
Updated - 17 March 2022, 15:58
Version - 5.0.6
Privileged Access Suite for Unix

Unix security simplified

Privileged Access Suite for Unix solves the intrinsic security and administration issues of Unix-based systems (including Linux and macOS) while making satisfying compliance requirements easier. It unifies and consolidates identities, assigns individual accountability, and enables centralized reporting for user and administrator access to Unix. The Privileged Access Suite for Unix combines an Active Directory bridge and root delegation solutions under a unified console that grants organizations centralized visibility and streamlined administration of identities and access rights across their entire Unix environment.

Active Directory bridge

Achieve unified access control, authentication, authorization, and identity administration for Unix, Linux, and macOS systems by extending them into Active Directory (AD) and taking advantage of AD’s inherent benefits. Patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD’s security, compliance, and Kerberos-based authentication capabilities to Unix, Linux, and macOS. See www.oneidentity.com/products/safeguard-authentication-services/ for more information about the Active Directory Bridge product.

Root delegation

The Privileged Access Suite for Unix offers two different approaches to delegating the Unix root account. The suite either enhances or replaces sudo, depending on your needs.

- By choosing to enhance sudo, you will keep everything you know and love about sudo while enhancing it with features like a central sudo policy server, centralized keystroke logs, a sudo event log, and compliance reports for who can do what with sudo.

  See www.oneidentity.com/products/privilege-manager-for-sudo/ for more information about enhancing sudo.

- By choosing to replace sudo, you will still be able to delegate the Unix root privilege based on centralized policy reporting on access rights, but with a more granular permission and the ability to log keystrokes on all activities from the time a user logs in, not just the commands that are prefixed with “sudo.” In addition, this option
implements several additional security features like restricted shells, remote host command execution, and hardened binaries that remove the ability to escape out of commands and gain undetected elevated access.

See www.oneidentity.com/products/privilege-manager-for-unix/ for more information about replacing sudo.

Privileged Access Suite for Unix

Privileged Access Suite for Unix offers two editions: Standard edition and Advanced edition. Both editions include the Safeguard Authentication Services patented technology that allows organizations to extend the security and compliance of Active Directory to Unix, Linux, and macOS platforms and enterprise applications. In addition:

- The Advanced edition licenses you for Privilege Manager for Unix.

About this guide

The 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 Defender with Safeguard Authentication Services for token-based two factor authentication. This guide walks you through the process of installing and configuring the necessary Defender access policies and Group Policy settings.

NOTE: The term "Unix" is used informally throughout the Safeguard Authentication Services documentation to denote any operating system that closely resembles the trademarked system, UNIX.
Introducing Defender

Defender enhances security by enabling two-factor authentication to network, Web, and applications-based resources. One Identity 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.

One Identity supports Defender integration on all platforms that support Safeguard Authentication Services, except macOS 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.

Defender integration

Defender provides strong authentication capabilities.

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

When Safeguard 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. Safeguard 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 perimeter network 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 Safeguard 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 One Identity. 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 Safeguard Authentication Services 4.x?**

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

Safeguard Authentication Services provides strong authentication for up to 25 users at no additional cost through included licenses and tokens for Safeguard Authentication Services 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 Safeguard Authentication Services 4.x work?**

Safeguard Authentication Services:

- 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.

The following figure describes the flow of events that occur during a Unix or Linux login after both Safeguard Authentication Services Defender and Safeguard Authentication Services are configured according to this guide.
Defender installation prerequisites

Before you install Safeguard Authentication Services 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 Safeguard Authentication Services on your Unix or Linux machine.
Configuring Defender

To integrate Defender with Safeguard 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 then 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 Safeguard 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 then 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 Safeguard Authentication Services for Unix user name. Look in the Preferences of the Control Center to determine which attribute Safeguard Authentication Services is configured.

<table>
<thead>
<tr>
<th>Table 1: User IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User IDs</strong></td>
</tr>
<tr>
<td>SAM Account Name</td>
</tr>
<tr>
<td>User Principal Name</td>
</tr>
<tr>
<td>Defender ID</td>
</tr>
<tr>
<td>Proper Name</td>
</tr>
</tbody>
</table>

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.
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.

### Adding one-time password tokens

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 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.
Configuring Safeguard Authentication Services

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

Group Policy configuration

Safeguard Authentication Services relies on Group Policy for managing the configuration of options and features. To enable one-time password support for Safeguard 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 Safeguard 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.

Enabling one-time password authentication for Unix

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 Defender.

- 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).

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

**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-EBF7-4376-AA1E-3CE5850AC5E5  PTYPE: 786318DB-DE76-42F2-8A57-F1E0C3ACE113

Applying Settings Changes
```
---
[vgp_licext.so]
vkg_vasext.so
[vgp_scecli.so]
vkg_sudoext.so
[vgp_dfc.so]
vkg_unixext.so
[vgp_sshcfg.so]
vkg_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]
vkg_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 Safeguard 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:
3. To configure pam for a specific service, such as gdm, run the following command as root:

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

| NOTE: When successful this command produces 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.
About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product
Index

A
access node
  associating a security policy 9

D
Defender Settings properties 14

G
Group Policy
  configuring 14

M
Members
  adding 11

O
one-time password
  setting 15
  using vastool to configure 16
one-time password tokens
  adding 12

P
PAM authentication
  enable 14
  login service
    defined 14
  pam_defender debug
    setting up 17

prerequisites 8
Privilege Manager Defender
  About 6

S
security policy
  selecting 11
  specifying type of credential 9
security server
  assigning access nodes 11
  strong authentication 6

tokens
  assigning to users 12

U
Unix or Linux login
  flow 6