SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Dell™ One Identity Defender
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013670-001, Rev. A
Release Date: December 2016
## Contents

Third-Party Software Acknowledgement ........................................................................................................ 4
Description ....................................................................................................................................................... 4
Applicability .................................................................................................................................................... 4
Environment .................................................................................................................................................... 4
Audience ......................................................................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud ................................................. 5
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE ........................................................................................................................................... 6
RADIUS Authentication Flow using SafeNet Authentication Service ............................................................. 6
RADIUS Prerequisites .................................................................................................................................... 7
Configuring SafeNet Authentication Service .................................................................................................. 7
  Creating Users Stores in SafeNet Authentication Service ....................................................................... 7
  Assigning an Authenticator in SafeNet Authentication Service ................................................................. 7
  Adding Dell™ One Identity Defender as an Authentication Node in SafeNet Authentication Service ....... 8
  Checking the SafeNet Authentication Service RADIUS Address ............................................................ 10
Configuring Dell™ One Identity Defender .................................................................................................... 11
  Creating RADIUS Agent Access Nodes .................................................................................................... 11
  Creating RADIUS Proxy Access Nodes ................................................................................................... 15
  Adding Access Nodes to the Security Server ............................................................................................ 18
  Configuring Client Machine for the Remote Desktop Login ................................................................... 20
Running the Solution ....................................................................................................................................... 22
Support Contacts ............................................................................................................................................ 23
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Dell™ One Identity Defender.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Dell™ One Identity Defender is a cost effective solution that enhances security in organization by authenticating users who access valuable network resources. Users who get successfully authenticated via Dell™ One Identity Defender are granted access to protected resources.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Dell™ One Identity Defender using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Dell™ One Identity Defender to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Dell™ One Identity Defender environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Dell™ One Identity Defender can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**
- **Dell™ One Identity Defender**—Version 5.8.2.5732
Audience

This document is targeted to system administrators who are familiar with Dell™ One Identity Defender, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.gemalto.com/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.pdf

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (SAS) can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:
  

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for Dell™ One Identity Defender.

1. A user attempts to log in to the Windows client machine using the Active Directory (AD) credentials and an OTP. Active directory credentials are validated directly with AD. The OTP is sent to Dell™ One Identity Defender for validation.

2. Dell™ One Identity Defender sends a RADIUS request with the user’s credentials to SafeNet Authentication Service (SAS) for validation.

3. The SAS authentication reply is sent back to the Dell™ One Identity Defender.

4. The user is granted or denied access to the Dell™ One Identity Defender based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from Dell™ One Identity Defender, ensure the following:

- End users can authenticate from the Dell™ One Identity Defender environment with a static password before configuring the Dell™ One Identity Defender to use RADIUS authentication.
- Ports 1812/1813 are open to and from Dell™ One Identity Defender.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Dell™ One Identity Defender using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
- Adding Dell™ One Identity Defender as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10

Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Dell™ One Identity Defender.
The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


### Adding Dell™ One Identity Defender as an Authentication Node in SafeNet Authentication Service

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Dell™ One Identity Defender. You will need the IP address of Dell™ One Identity Defender and the shared secret to be used by both SAS and Dell™ One Identity Defender.

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab and then select **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link.

4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

   - **Agent Description**: Enter a host description.
   - **Host Name**: Enter the name of the host that will authenticate with SAS.
   - **Low IP Address In Range**: Enter the IP address of the host that will authenticate with SAS.
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Confirm Shared Secret**: Re-enter the shared secret key.
The authentication node is added to the system.

Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Dell™ One Identity Defender, check its IP address. The IP address will then be added to Dell™ One Identity Defender as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes](image)

### Configuring Dell™ One Identity Defender

For this Integration, Dell Defender is used for Remote desktop login.

Configure defender to authenticate users when they sign in to the Windows client machines in an organization. Configuring Dell Defender for multi-factor authentication requires:

- Creating RADIUS Agent Access Nodes, page 11
- Creating RADIUS Proxy Access Nodes, page 15
- Adding Access Nodes to the Security Server, page 18
- Configuring Client Machine for the Remote Desktop Login, page 20

### Creating RADIUS Agent Access Nodes

Access Node is an IP address or range of IP addresses from which the Defender security server accepts authentication requests.

1. On the Windows server where Dell™ One Identity Defender is installed, press `[Win]+[R]` to open the **Run** window, type `dsa.msc`, and then click **OK**.

![Run](image)

*(The screen image above is from Microsoft™. Trademarks are the property of their respective owners.)*
2. The **Active Directory User and Computers** window is displayed. In the left pane, expand the domain (for example, safenetdemos.com), and then expand **Defender**.

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)

3. Right-click **Access Nodes**, and then click **New > Defender Access Node**.

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
4. On the **New Object – Defender Access Node** window, complete the following fields, and click **Next**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the access node.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description for the access node.</td>
</tr>
</tbody>
</table>

5. Complete the following fields and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Node Type</strong></th>
<th>Select <strong>Radius Agent</strong>. The <strong>Radius Agent</strong> node type allows a NAS device to connect to the Dell Defender using the RADIUS protocol. RADIUS is transmitted over UDP and uses the port 1812 by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User ID</strong></td>
<td>Select <strong>SAM Account Name</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
6. Complete the following fields and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address or DNS name</td>
<td>Enter the IP address or DNS name of the Windows client machine from where you want to allow a connection request.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter <strong>1812</strong>.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet Mask of Windows client machine.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret that the access node uses to establish a connection with the Defender security server.</td>
</tr>
</tbody>
</table>

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)

7. Click **Finish**.

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
Creating RADIUS Proxy Access Nodes

Create a RADIUS proxy access node type to allow RADIUS requests received from a RADIUS agent access node to be forwarded to another RADIUS server (for example, SAS Free RADIUS server).

1. On the **Active Directory User and Computers** window, in the left pane, expand the domain (for example, safenetdemos.com), and then expand **Defender**.

   ![Active Directory Users and Computers window](image1)

   *(The screen image above is from Microsoft™. Trademarks are the property of their respective owners.)*

2. Right-click **Access Nodes**, and then click **New > Defender Access Node**.

   ![Active Directory Users and Computers window](image2)

   *(The screen image above is from Microsoft™. Trademarks are the property of their respective owners.)*
3. On the **New Object – Defender Access Node** window, complete the following fields, and click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the access node (for example, <strong>FreeRADIUS</strong>).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the access node (for example <strong>FreeRADIUS</strong>).</td>
</tr>
</tbody>
</table>

(′The screen image above is from Dell™. Trademarks are the property of their respective owners.′)

4. Complete the following fields and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node Type</strong></td>
<td>Select <strong>Radius Proxy</strong>. The <strong>Radius Proxy</strong> node type allows RADIUS requests received from a RADIUS agent access node to be forwarded to another RADIUS server.</td>
</tr>
<tr>
<td><strong>User ID</strong></td>
<td>Select <strong>SAM Account Name</strong>.</td>
</tr>
</tbody>
</table>

(′The screen image above is from Dell™. Trademarks are the property of their respective owners.′)
5. Complete the following fields and then click **Next**.

<table>
<thead>
<tr>
<th><strong>IP Address or DNS name</strong></th>
<th>Enter the IP address or DNS name of SAS RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>Enter <strong>1812</strong></td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Enter an appropriate subnet mask.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret used by both the SAS RADIUS server and Dell Defender access node.</td>
</tr>
</tbody>
</table>

6. Click **Finish**.

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
Adding Access Nodes to the Security Server

1. On the **Active Directory User and Computers** window, in the left pane, expand the domain (for example, *safenetdemos.com*), and then click **Defender > Security Servers**.

   ![Active Directory User and Computers](image1)

   *(The screen image above is from Microsoft™. Trademarks are the property of their respective owners.)*

2. In the right pane double-click the security server (for example, **DSS**).

3. On the **Defender – DSS Properties** window, on the **Access Nodes** tab, click **Assign**.

   ![Defender – DSS Properties](image2)

   *(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*
4. On the Select Defender Access Nodes window, select the first access node (for example, Desktop Client), and then double-click on it.

![Select Defender Access Nodes](image)

*(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*

5. Select the second access node (for example, FreeRADIUS), and then double-click on it.

![Select Defender Access Nodes](image)

*(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*

Ensure that both the access nodes (DesktopClient and FreeRADIUS) are added under Enter the object names to be selected.
6. Click OK.

7. On the Defender – DSS Properties window, click Apply, and then click OK.

![Defender - DSS Properties](image)

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)

Configuring Client Machine for the Remote Desktop Login

1. On the Windows client machine, from C:\Program Files\Dell\Defender\Desktop Login, run GinaConfig.exe to configure the Defender desktop login.

2. On the Defender Desktop Login Configuration window, click Add.

![Defender Desktop Login Configuration](image)

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
3. On the **Defender Security Server** window, in the **IP Address or DNS Name** field, enter the IP address or DNS name of the Defender security server.

4. Click **OK**.

5. On the **Defender Desktop Login Configuration** window, in the **Shared Secret** field, enter the shared secret that you entered earlier in step 6 of “Creating RADIUS Agent Access Nodes” on page 11, and then click **Apply**.

6. Click **OK**.
Running the Solution

Before running this solution, ensure that Dell™ One Identity Defender is configured for two step authentication. For this integration, the user is enrolled with a Mobile PASS token on the SafeNet Authentication Service (SAS) cloud.

On the Windows client machine login window, complete the following fields, and then click .

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter your domain user name or SAS user ID.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with your domain user name.</td>
</tr>
<tr>
<td>Passcode</td>
<td>Enter the OTP that you generated using the MobilePASS token.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft™. Trademarks are the property of their respective owners.)

After successful authentication, you are logged in to the Windows machine.

(The screen image above is from Microsoft™. Trademarks are the property of their respective owners.)
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>