SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Dell One Identity Cloud Access Manager
## Contents

Third-Party Software Acknowledgement ................................................................. 4
Description .............................................................................................................. 4
Applicability ........................................................................................................... 4
Environment .......................................................................................................... 5
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 .......................... 8
   Adding Dell One Identity Cloud Access Manager as an Authentication Node in SafeNet Authentication Service ................................................................. 9
   Checking the SafeNet Authentication Service RADIUS Address .................... 11
Configuring Dell One Identity Cloud Access Manager ........................................... 12
Running the Solution .............................................................................................. 18
Support Contacts ..................................................................................................... 20
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 Cloud Access Manager.

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 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 Cloud Access Manager is a web-access management solution that offers secure and unified access to all your internal and cloud-based web applications while simultaneously enhancing security and IT efficiency. Cloud Access Manager enables:

- Secure identity federation
- Single sign-on
- Adaptive security
- Multifactor authentication
- Simplified access control and auditing
- Scalable just-in-time cloud provisioning

This document describes how to:

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

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

Dell One Identity Cloud Access Manager 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 Cloud Access Manager—Version 8.1.1.8129
- Microsoft Windows Server 2008 R2

Audience

This document is targeted to system administrators who are familiar with Dell One Identity Cloud Access Manager, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service (SAS).

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.
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 (SAS) 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 the Dell One Identity Cloud Access Manager.

1. A user attempts to log on to Dell One Identity Cloud Access Manager using an OTP authenticator.
2. Dell One Identity Cloud Access Manager sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to Dell One Identity Cloud Access Manager.
4. The user is granted or denied access to Dell One Identity Cloud Access Manager 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 Cloud Access Manager, ensure the following:

- End users can authenticate from the Dell One Identity Cloud Access Manager environment with a static password before configuring the Dell One Identity Cloud Access Manager to use RADIUS authentication.
- Ports 1812/1813 are open to and from Dell One Identity Cloud Access Manager.
- 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 Cloud Access Manager using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding Dell One Identity Cloud Access Manager as an Authentication Node in SafeNet Authentication Service, page 9
- Checking the SafeNet Authentication Service RADIUS Address, page 11

**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 Cloud Access Manager.

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 Cloud Access Manager 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 Cloud Access Manager. You will need the IP address of Dell One Identity Cloud Access Manager and the shared secret to be used by both SAS and Dell One Identity Cloud Access Manager.

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.

![Auth Nodes Module](image)

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host (for example, Dell One Cloud Access Manager) that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

![Add Auth Node Form](image)

The authentication node is added to the system.

![Authentication Node Added](image)
Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Dell One Identity Cloud Access Manager, check its IP address. The IP address will then be added to Dell One Identity Cloud Access Manager 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 module](image)

### Configuring Dell One Identity Cloud Access Manager

Configure the Dell One Identity Cloud Access Manager application portal for Active Directory (AD) as primary authentication and RADIUS as secondary authentication.

**NOTE:** It is assumed that an application is already configured on Dell One Identity Cloud Access Manager.

1. Log in to the Dell One Identity Cloud Access Manager console.

![Dell One Identity Cloud Access Manager console](image)

*The screen image above is from Dell™. Trademarks are the property of their respective owners.*
2. In the left pane, click **Authenticators > Add New**.

![Add Authenticator](image-url)

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

3. In the right pane, under **Authenticator Type**, under **Directory Authenticators**, select **Microsoft Active Directory**, and then click **Next**.

![Directory Authenticators](image-url)

*(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*
4. Under **Connection Settings**, complete the following fields, and then click **Test Connection**.

<table>
<thead>
<tr>
<th>Username / UPN</th>
<th>Enter your AD username.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter your AD password.</td>
</tr>
</tbody>
</table>

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

5. A success message is displayed. Click **Next**.

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
6. Under **Primary Authentication**, ensure that **Store Credential from this authenticator as primary credentials** is not selected, and then click **Next**.

![Primary Authentication](image1)

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

7. Under **Two Factor Authentication**, in the **Two factor authentication mode** field, select **Use two factor Authentication for all application**.

![Two Factor Authentication](image2)

*(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*
8. In the **Type of two factor authentication** field, select **RADIUS Server**, and then under **RADIUS Connection Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Host / IP Address (including port)</th>
<th>Enter the IP address of the RADIUS server with Port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret that you entered earlier in step 5 of &quot;Adding Dell One Identity Cloud Access Manager as an Authentication Node in SafeNet Authentication Service&quot; on page 9.</td>
</tr>
</tbody>
</table>

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

9. Click **Next**.

10. Under **Authenticator Name**, in the **Authenticator Name** field, enter the name (for example, **SafeNet Authentication Service**) used to identify the authenticator, and then click **Finish**.

(The screen image above is from Dell™. Trademarks are the property of their respective owners.)
11. On the Dell One Identity Cloud Access Manager console, in the right pane, under **Front-end Authentication Method Created**, click **Edit Roles**.

12. Under **Roles**, select **Users**, and then Under **Edit Role**, perform the following steps:
   a. Under **Users in Role**, select **Include all users**.
   b. Under **Select User**, in the **User's Authenticator** field, select an appropriate user's authenticator (for example, **SafeNet Authentication Service**) that you created earlier in step 10.
   c. In the **Rule Type** field, select **Include all users**.
   d. Click **Save**.

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

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

Running the Solution

For this integration, the SafeNet eToken PASS token is configured for authentication with the SafeNet Authentication Service (SAS) solution.

NOTE: The Dell One Identity Cloud Access Manager application portal is used to securely access the configured application.

1. In a web browser, open the following URL to access the Dell One Identity Cloud Access Manager application portal:
   https://<Host FQDN>/Cloud AccessManager.
2. On the login window, enter the AD username and password, and then **Login In**.

![Login Window](image1)

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

3. After successful authentication of the AD credentials, you will be redirected to the following window. Enter the OTP generated using the SafeNet eToken PASS token, and then click **Submit**.

![OTP Window](image2)

*(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*
4. After successful authentication, you will be logged in to the Dell One Identity Cloud Access Manager application portal to access the configured application.

(The screen image above is from Dell™. 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>
</table>
| Address            | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland  21017 USA                                                      |
| Phone              | United States  
1-800-545-6608  
International  
1-410-931-7520                                                              |
| Technical Support  | https://serviceportal.safenet-inc.com  
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. |