SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for Dell One Identity Cloud Access Manager
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:** 007-013659-001, Rev. A

**Release Date:** December 2016
## Contents

Third-Party Software Acknowledgement .............................................................................................. 4
Description ........................................................................................................................................... 4
Applicability ......................................................................................................................................... 5
Environment .......................................................................................................................................... 5
Audience .............................................................................................................................................. 5
RADIUS-based Authentication using SafeNet Authentication Manager .............................................. 5
RADIUS Authentication Flow using SafeNet Authentication Manager .............................................. 6
RADIUS Prerequisites ......................................................................................................................... 6
Configuring SafeNet Authentication Manager ..................................................................................... 6
  Synchronizing Users Stores to SafeNet Authentication Manager ....................................................... 7
  Configuring SafeNet Authentication Manager’s Connector for OTP Authentication .......................... 7
  Assigning a Token in SafeNet Authentication Manager ..................................................................... 7
  Adding Dell One Identity Cloud Access Manager as a RADIUS Client in IAS/NPS ....................... 8
  Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client .......... 10
Configuring Dell One Identity Cloud Access Manager ..................................................................... 11
Running the Solution .......................................................................................................................... 17
Support Contacts .................................................................................................................................. 18
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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) tokens managed by SafeNet Authentication Manager.
- Configure Dell One Identity Cloud Access Manager to work with SafeNet Authentication Manager in the 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 Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Dell One Identity Cloud Access Manager can be configured to support multi-factor authentication in several modes. RADIUS protocol will be used for the purpose of working with SafeNet Authentication Manager.
Applicability

The information in this document applies to:

- SafeNet Authentication Manager—A server version of SAM 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 Manager 8.2 HF 493
- 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 Manager.

RADIUS-based Authentication using SafeNet Authentication Manager

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
RADIUS Authentication Flow using SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Dell One Identity Cloud Access Manager.

1. A user attempts to log on to Dell One Identity Cloud Access Manager using an OTP token.
2. Dell One Identity Cloud Access Manager sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager (SAM) for validation.
3. The SAM 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 SAM and is connected to Dell One Identity Cloud Access Manager.

RADIUS Prerequisites

To enable SafeNet Authentication Manager 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 Manager

The deployment of multi-factor authentication using SafeNet Authentication Manage with Dell One Identity Cloud Access Manager using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SafeNet Authentication Manager, page 7
- Configuring SafeNet Authentication Manager’s Connector for OTP Authentication, page 7
- Assigning a Token in SafeNet Authentication Manager, page 4
- Adding Dell One Identity Cloud Access Manager as a RADIUS Client in IAS/NPS, page 8
- Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client, page 10
Synchronizing Users Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:
- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SafeNet Authentication Manager’s Connector for OTP Authentication

SafeNet Authentication Manager (SAM) is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:
- **Connectors**—SAM Connector for OTP Authentication is installed
- **SAM Back-end Service**—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:
- OTP support (required for OTP) is selected in the Token Initialization settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Assigning a Token in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Dell One Identity Cloud Access Manager.

The following tokens are supported:
- eToken PASS
Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Adding Dell One Identity Cloud Access Manager as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Dell One Identity Cloud Access Manager.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Dell One Identity Cloud Access Manager.

Dell One Identity Cloud Access Manager must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Dell One Identity Cloud Access Manager for authentication.

---

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager (SAM).

The details below refer to NPS, and are very similar to IAS.

---

1. Click **Start > Administrative Tools > Network Policy Server**.
2. On the Network Policy Server web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then click **New**.

![Network Policy Server](image1.png)

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

3. On the **New RADIUS Client** window, on the **Settings** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or FQDN)</td>
<td>Enter the Dell One Identity Cloud Access Manager IP address or FQDN.</td>
</tr>
<tr>
<td>Manual/Generate</td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in Dell One Identity Cloud Access Manager.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>
4. Click OK.

Dell One Identity Cloud Access Manager is added as a RADIUS client in NPS.

Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SafeNet Authentication Manager’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
Configuring Dell One Identity Cloud Access Manager

We will configure 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 in Dell One Identity Cloud Access Manager.

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

![Screen image](image1.png)

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

2. In the left pane, click **Authenticators > Add New**.

![Screen image](image2.png)

*(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**.

![Authenticator Type](image)

*(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>

![Connection Settings](image)

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

![Connection Settings](image1)

(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](image2)

(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](image)

(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 RADIUS server (for example, NPS server) with port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret that you entered earlier in step 3 of “Adding Dell One Identity Cloud Access Manager as a RADIUS Client in IAS/NPS” on page 4.</td>
</tr>
</tbody>
</table>

![RADIUS Connection Settings](image)

(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 the authenticator (for example, **SafeNet Authentication Manager**), and then click **Finish**.

![Authenticator Name](image)

*(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**.

![Edit Roles](image)

*(The screen image above is from Dell™. Trademarks are the property of their respective owners.)*
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 Manager**) that you created earlier in step 10.
   c. In the **Rule Type** field, select **Include all users**.
   d. Click **Save**.

   ![Image](image1.png)

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

   A success message is displayed.

   ![Image](image2.png)

   *(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 is used as the enrolled OTP token.

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 click Login in.

   (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.

   (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                            |

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.