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:** 007-013608-001, Rev. A  
**Release Date:** September 2016
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Dell Wyse vWorkspace.

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 Wyse vWorkspace provides a single, graphical console that helps you manage your virtual infrastructure and perform administrative tasks. Key features of Dell Wyse vWorkspace are

- Connection brokering
- Enterprise level management
- Optimized user experience

Dell Wyse vWorkspace allows management of your environment to be simplified. It supports multiple desktop virtualization technologies and combines them into a single console, a single point of access, and a single client. Dell Wyse vWorkspace also provides the richest and most intuitive user experience available on a variety of access devices.

This document describes how to:

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

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

Dell Wyse vWorkspace 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)**—Cloud Version 3.5.2912.32855
- **Dell Wyse vWorkspace**—Version 8.6

Audience

This document is targeted to system administrators who are familiar with Dell Wyse vWorkspace, 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.

  ![SAS cloud hosted RADIUS service diagram](image)

- **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.

  ![Local RADIUS hosted on-premises diagram](image)

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:

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 Wyse vWorkspace.

1. A user attempts to log on to Dell Wyse vWorkspace using an OTP authenticator.
2. Dell Wyse vWorkspace 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 Wyse vWorkspace.
4. The user is granted or denied access to the Dell Wyse vWorkspace based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Dell Wyse vWorkspace, ensure the following:

- End users can authenticate from the Dell Wyse vWorkspace environment with a static password before configuring the Dell Wyse vWorkspace to use RADIUS authentication.
- Ports 1812/1813 are open to and from Dell Wyse vWorkspace.
- 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.

Third-Party Prerequisites

- Dell Wyse vWorkspace is up and running.
- Active Directory Roles must be installed in the same machine on which Dell Wyse vWorkspace is to be configured.
- Create AD user, assign, and provide the permissions to the user to access the Manage Applications on Dell Wyse vWorkspace.
- Ensure that all services and roles configured on Wyse vWorkspace.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Dell Wyse vWorkspace 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 Wyse vWorkspace as an Authentication Node in SafeNet Authentication Service, page 8
- 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
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 Wyse vWorkspace.

The following authenticators are supported:

- eToken PASS
- 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 Wyse vWorkspace 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 Wyse vWorkspace. You will need the IP address of Dell Wyse vWorkspace and the shared secret to be used by both SAS and Dell Wyse vWorkspace.

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]

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 (for example, <strong>vWorkspace</strong>).</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will be authenticated with SAS (for example, <strong>vWorkspace</strong>).</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will be authenticated with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Synchronization</td>
<td></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>
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 Wyse vWorkspace, check its IP address. The IP address will then be added to Dell Wyse vWorkspace 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**.

![COMMS tab and Auth Nodes module](image1)

3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes module](image2)

**Configuring Dell Wyse vWorkspace**

Configure two-factor Authentication in Dell Wyse vWorkspace.

1. On the server machine, open the Dell Wyse vWorkspace console.

2. On the Dell Wyse vWorkspace console, in the left pane, under **vWorkspace**, click **Web Access**.

![vWorkspace console](image3)

*(The screen image above is from Dell. Trademarks are the property of their respective owners.)*
3. In the right pane, under vWorkspace Farm Web Access, select the default website that you created (for example vWorkspace), and then click Properties. The Web Access Site Properties window is displayed.

4. On the Web Access Site Properties window, in left pane, under Domain/Login Settings, click User Domains.

(The screen image above is from Dell. Trademarks are the property of their respective owners.)
5. In the right pane, under **User Domains**, perform the following steps:
   a. In the **Domain** field, enter the AD domain name (for example, `safenetdemos1`), and then click **Add**.
   b. Select the **Allow user to select a domain** option.
   c. Click **OK**.

6. In the left pane, under **Domain Login Settings**, select **Two-Factor Authentication**.
7. In the right pane, under **Two-Factor Authentication**, select **Enable two-factor authentication**, and perform the following steps:

a. Select the **RADIUS (Quest Defender, RSA ACE/Server, Secure Computing Remote Access)** option.

b. In the **Servers** field, enter the SAS RADIUS IP Address, and then click **Add**.

c. In the **Port** field, enter **1812**.

d. In the **Secret key** field, enter the SAS RADIUS Shared Secret that you entered earlier in step 5 of “Creating Users Stores in SafeNet Authentication Service” on page 7.

e. Select **Use separate OTP field**.

f. Select the **Unencrypted (PAP)** option.

g. Click **OK**.

(The screen image above is from Dell. Trademarks are the property of their respective owners.)
8. The **Web Access Site Properties** window is displayed. For applying settings, select the **Contact the Web Access site directly and update its configuration** option, and then click **OK**.

![Web Access Site Properties](image)

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

9. A success message is displayed. Click **OK**.

![Configuration has been saved successfully](image)

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

### Running the Solution

For this integration, end user is configured with SafeNet MobilePASS+ token for authentication with the SafeNet Authentication Service (SAS).

1. In a web browser, enter the following URL to access Dell Wyse vWorkspace:

   https://<FQDN of Dell Wyse vWorkspace Management console or IP Address/vWorkspace>
2. On the login window, complete the following fields, and then click **Login**.

<table>
<thead>
<tr>
<th><strong>User name</strong></th>
<th>Enter your AD username.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Enter your AD password.</td>
</tr>
<tr>
<td><strong>Passcode</strong></td>
<td>Enter the OTP passcode that you generated using the SafeNet MobilePASS+ Token.</td>
</tr>
</tbody>
</table>

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

After successful authentication, in the web browser, you are logged into the Dell Wise vWorkspace.

(The screen image above is from Dell. Trademarks are the property of their respective owners.)
Appendix – Configuring Two-Factor Authentication without Using a Separate OTP Field

1. On the Web Access Site Properties window, in the left pane, under Domain/Login Settings, click Two-Factor Authentication.

2. In the right pane, perform the following steps:
   a. Clear the Use separate OTP field option.
   b. Under Password structure, select AD Password/OTP or OTP/AD Password based on your preferred configuration.
   c. In the OTP length field, enter the length of OTP based on your preferred configuration.

3. Click OK.

(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>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto&lt;br&gt;4690 Millennium Drive&lt;br&gt;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>