SafeNet Authentication Service
Push OTP Integration Guide

Using RADIUS Protocol for Dell Wyse vWorkspace
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: 007-013574-001, Rev. A
Release Date: August 2016
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SafeNet Authentication Service</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Dell Wyse vWorkspace Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Push OTP Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Creating Users Stores in SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Adding Dell Wyse vWorkspace as an Authentication Node in SafeNet Service</td>
<td>8</td>
</tr>
<tr>
<td>Checking the SafeNet Authentication Service RADIUS Address</td>
<td>10</td>
</tr>
<tr>
<td>Enabling the Software Token Push OTP Setting</td>
<td>11</td>
</tr>
<tr>
<td>Enabling the Allowed Targets Policy</td>
<td>12</td>
</tr>
<tr>
<td>Configuring Dell Wyse vWorkspace</td>
<td>14</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>17</td>
</tr>
<tr>
<td>Appendix: Configuring Radius Time-Out</td>
<td>20</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>22</td>
</tr>
</tbody>
</table>
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 Push one-time password (OTP) solution managed by SafeNet Authentication Service.
- Configure Dell Wyse vWorkspace to work with SafeNet Authentication Service in the 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 Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It's likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.
Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **MobilePASS+ application**

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)**—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 (SAS).

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides the following RADIUS topology that supports Push OTP tokens:

**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.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
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 dataflow of a multi-factor authentication transaction for Dell Wyse vWorkspace.

1. A user attempts to log on to Dell Wyse vWorkspace using a Push OTP authenticator.
2. Dell Wyse vWorkspace sends a RADIUS request with the user’s credentials to SafeNet Authentication Service (SAS) for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate that there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to Dell Wyse vWorkspace
5. The user is granted or denied access to Dell Wyse vWorkspace based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service (SAS) 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.
- On the client machine, set the RADIUS timeout value at least 60 seconds.
Dell Wyse vWorkspace Prerequisites

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

Push OTP Prerequisites

In order to use SafeNet Authentication Service (SAS) Push OTP, you will need:

- SafeNet Authentication Service configured to enable Push OTP
- MobilePASS+ application

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 10
- Enabling the Software Token Push OTP Setting, page 11
- Enabling the Allowed Targets Policy, page 12

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:
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:

- 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 click Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link, and then click Add.

4. Under Add Auth Nodes, complete the following fields, and then click Save:

   - **Auth Node Name**: Enter a host description.
   - **Resource Name**: Enter a resource name which will identify in a push notification which authentication node it relates to.
   - **Low IP Address In Range**: Enter the IP address of the host.
   - **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 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 click **Auth Nodes**.

![SafeNet Authentication Service](image1)

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

![Auth Nodes](image2)

### Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the Software Token Push OTP setting must be enabled in the SafeNet Authentication Service (SAS) token policy.

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

![SafeNet Authentication Service](image3)
2. Click the **POLICY** tab, and then click **Token Policies**.

![Image of Token Policies module](image)

3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

![Image of Software Token Push OTP Setting](image)

4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.

### Enabling the Allowed Targets Policy

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.
1. Log in to the SafeNet Authentication Service (SAS) console with an Operator account.

2. Click the POLICY tab, and then click Token Policies.

3. In the Token Policies module, click the Allowed Targets Settings link.
4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.

**Configuring Dell Wyse vWorkspace**

Configure Dell Wyse vWorkspace for Active Directory and RADIUS authentication.

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**.

   (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 screen image above is from Dell. Trademarks are the property of their respective owners.)
4. The Web Access Site Properties window is displayed. In left pane, under Domain\Login Settings, click User Domains.

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 then perform the following steps:
   a. Select the **RADIUS (Quest Defender, RSA ACE/Server, Secure Computing RemoteAccess)** 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 4 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**

In this solution, the SafeNet MobilePASS+ token is used as the enrolled OTP token for authentication with the SAS solution.

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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td>Enter your AD username.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter your AD password.</td>
</tr>
<tr>
<td><strong>Passcode</strong></td>
<td>Enter a character.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Select the user domain (for example, safenetdemos1).</td>
</tr>
</tbody>
</table>

![Login Window](image)

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

SAS will trigger an on-the-go authentication request.

3. You will receive an authentication notification on the registered mobile device. On the mobile device screen, tap **APPROVE**.

![Mobile Device Authentication](image)
4. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **CONTINUE**.

5. A success message is displayed on the mobile screen.
After successful authentication, in the web browser, you are redirected to access the Dell Wise vWorkspace. You can now access the available applications.

![Dell Wise vWorkspace](image)

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

### Appendix: Configuring Radius Time-Out

1. Open the Dell Wyse vWorkspace console.
2. In the left pane, right click on the farm name (for example, vWorkspace), and then click Farm properties.

![Dell Wyse vWorkspace Farm Properties](image)

(The screen image above is from Dell. Trademarks are the property of their respective owners.)
3. On the Farm Properties window, in the left pane, under Authentication, click Two-Factor Authentication.

4. In right pane, under Two-Factor Authentication, select Enable RADIUS (Quest-Defender, RSA ACE/Server, Secure Computing RemoteAccess), and then complete the following fields:

<table>
<thead>
<tr>
<th>Server name or IP addr</th>
<th>Enter the SAS RADIUS IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret key</td>
<td>Enter the shared secret that you entered earlier in step 4 of “Creating Users Stores in SafeNet Authentication Service” on page 7.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter 1812.</td>
</tr>
<tr>
<td>Timeout (seconds)</td>
<td>Enter the RADIUS timeout (recommended 60 seconds and maximum 300 seconds)</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select Unencrypted (PAP).</td>
</tr>
<tr>
<td>Password Layout</td>
<td>Select an option as per your preferred configuration.</td>
</tr>
<tr>
<td>One-time password length</td>
<td>Enter the length of the one-time password.</td>
</tr>
<tr>
<td>Require all users to be two-factor authenticated</td>
<td>Do not select this option.</td>
</tr>
</tbody>
</table>

![Screen Image](image)

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

5. Click OK.
6. A configuration 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.)*

### 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</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software upgrades, and access the Gemalto Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>