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.
PREFACE

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Wallix AdminBastion Suite.

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.

This document contains the following chapters:

- "Authentication Flow" on page 9
- "SafeNet Authentication Service Setup" on page 10
- "Wallix AdminBastion Suite Setup" on page 14
- “Running the Solution” on page 18

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.

Wallix AdminBastion Suite appliances allow enterprises to consolidate remote access for employees, partners, guests, and other communities of interest on a single platform to minimize potential attack vectors, improve operational efficiency, and provide a superior end-user experience. Drive productivity enterprise-wide, while keeping cost and complexity at a minimum.

Wallix AdminBastion Suite provides control over access to applications, desktops, and Web sites from a broad range of remote—providing secure connectivity, end-point and server-side security, and application-level policies on a per-user basis.

This document describes how to:

- Configure Wallix AdminBastion Suite to work with SafeNet Authentication Service in RADIUS mode.

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

Wallix AdminBastion Suite 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 is used in this document is based on the following software versions:

- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—only when using this version. For Cloud not necessary to fill in version number.
- **Wallix AdminBastion Suite**—Version 5.0.4

RADIUS Prerequisites

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from Wallix AdminBastion Suite, ensure the following:

- End users can authenticate from the Wallix AdminBastion Suite with a static password before configuring the Wallix AdminBastion Suite to use RADIUS authentication.
- Ports 1812/1813 are open to and from the Wallix AdminBastion Suite.
- 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.

Audience

This document is targeted to system administrators who are familiar with Wallix AdminBastion Suite, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.
Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.
CHAPTER 1: Authentication Flow

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 Wallix AdminBastion Suite.

1. A user attempts to log on to Wallix AdminBastion Suite to access internal resources using an OTP authenticator.
2. Wallix AdminBastion Suite 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 Wallix AdminBastion Suite.
4. The user is granted or denied access to the Wallix AdminBastion Suite based on the OTP value calculation results from SAS.

For SafeNet Authentication Service (Cloud), a RADIUS agent is already configured and can be used without any additional agent installation or configuration requirements.

For SafeNet Authentication Service (SPE and PCE), a RADIUS agent (SAS Agent for Microsoft IAS or NPS, and FreeRADIUS) needs to be configured in the customer’s environment.

For more information on how to install and configure the SAS Agent for Microsoft IAS, Microsoft NPS, and FreeRADIUS, refer to the Agent Documentation.
CHAPTER 2: SafeNet Authentication Service Setup

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Wallix AdminBastion Suite using RADIUS protocol requires the following:

- Creating Users Stores, page 10
- Assigning an Authenticator, page 11
- Adding Wallix AdminBastion Suite as an Authentication Node, page 11

Creating Users Stores

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” available here.

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

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 Wallix AdminBastion Suite.

The following authenticators are supported:

- MobilePASS+ / MobilePASS 8
- SMS token
- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- GrlDSure

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” (available here) to learn how to provision the different authentication methods to the users in the SAS user store.

Adding Wallix AdminBastion Suite as an Authentication Node

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

1. Log in to the SAS console with an Operator account, click the **COMMS** tab and then select **Auth Nodes**.
2. In the **Auth Nodes** module, click on the **Auth Nodes** link.

**NOTE:** Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Wallix AdminBastion Suite, check its IP address.
3. Under **Auth Nodes**, click **Add**.

4. Under **Add Auth Nodes**, 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>Auth Node Name</td>
<td>Enter a name for the Auth node.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</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 authenticate with SAS (in this case, a range of IP addresses is being used).</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address in a range of IP addresses that will authenticate with SAS (in this case, a range of IP addresses is being used).</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>

(Primary RADIUS Server IP). The IP address will then be added to Wallix AdminBastion Suite as a RADIUS server at a later stage.
The authentication node is added to the system.

<table>
<thead>
<tr>
<th>Auth Nodes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Change Log</td>
</tr>
</tbody>
</table>

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization’s data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.
Perform the following steps to configure Wallix AdminBastion Suite to use the RADIUS protocol as a secondary authentication method:

1. In a web browser, open the Wallix AdminBastion Suite URL. For example, https://ec2-52-19-186-69.eu-west-1.compute.amazonaws.com

2. On the Wallix AdminBastion Suite login window, enter your administrator User name and Password, and then click Log in.

3. On the Wallix AdminBastion Suite administrator dashboard, in the left pane, click Configuration > External Authentications.

4. In the right pane, click +Add an authentication to add SAS as a RADIUS server in Wallix AdminBastion Suite.
5. Under Create external authentication, in Authentication type field, select RADIUS.

![Create external authentication](image1)

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

6. Perform the following steps:
   a. In the Authentication name field, enter a name for the authentication (for example, SAS Cloud).
   b. In the Server field, enter the Primary RADIUS Server IP address that is available in the Auth Nodes module of your SAS server. Refer to step 4 of “Adding Wallix AdminBastion Suite as an Authentication Node” on page 11.
   c. In the Secret field, enter the Shared Secret that you entered earlier in step 4 of “Adding Wallix AdminBastion Suite as an Authentication Node” on page 11.
   d. Click Apply.

![Create external authentication](image2)

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

Under Add an authentication, the newly configured RADIUS server will be listed.

![Add an authentication](image3)

(The screen image above is from Wallix AdminBastion Suite. Trademarks are the property of their respective owners.)
7. In the left pane, click **Users > Accounts**, and then in the right pane, select the user (for example, **Mark**), which you want to authenticate using RADIUS.

![Users page](Image)

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

8. Click **Edit this user**.

![Edit this user](Image)

(The screen image above is from Wallix AdminBastion Suite. Trademarks are the property of their respective owners.)
9. On the **Edit user** window, perform the following steps:
   a. Under **Authentication and backup servers**, in the **Available Authentications** list, select the authentication (for example, **SAS Cloud**) that you created earlier in step 6, and then click to move the authentication to the **Selected Authentications** list.
   b. Click **Apply**.

(The screen image above is from Wallix AdminBastion Suite. Trademarks are the property of their respective owners.)
CHAPTER 4: Running the Solution

Using MobilePASS+ with Push OTP

MobilePASS+ token is configured for authentication with the SAS solution. Perform the following steps to access the assigned applications:

1. In a web browser, open the Wallix AdminBastion Suite URL.
   For example, https://ec2-52-19-186-69.eu-west-1.compute.amazonaws.com

2. On the login window, perform the following steps:
   a. In the Username field, enter the username (for example, Mark).
   b. Click Log in.

3. On the registered mobile device, tap Approve to accept the OTP request.

(The screen image above is from Wallix AdminBastion Suite. Trademarks are the property of their respective owners.)
4. On the **Token Authentication** screen, enter the token PIN, and then tap **Continue** to send the approval with OTP to SAS.

![Token Authentication screen](image)

A success message is displayed on the mobile device.

**Passcode has been sent successfully**

After successful authentication, you will be able to access the internal resources.

![My Authorizations Sessions](image)

**Using MobilePASS+ in Hybrid Mode**

To use PushOTP token in the Hybrid mode, you need to customize the login page. Refer to “APPENDIX A: Customizing the Login Page for PushOTP Token”. Perform the following steps to access the assigned applications:

1. In a web browser, open the Wallix AdminBastion Suite URL.


2. On the login window, perform the following steps:

   a. Enter your user name (for example, **Mark**), and then select any of the following options:

   - Enter passcode manually
   - Use my mobile to autosend passcode
NOTE: In this scenario, the Use my mobile to autosend passcode option is selected.

b. Click Log in.

3. On the registered mobile device, tap Approve to accept the OTP request.

4. On the Token Authentication screen, enter the token PIN, and then tap Continue to send the approval with OTP to SAS.
CHAPTER 4: Running the Solution

5. A success message is displayed on the mobile device.

**Passcode has been sent successfully.**

After successful authentication, you will able to access the internal resources.

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

**Using GrIDsure**

GrIDsure token is configured for authentication with the SAS solution. Refer to "APPENDIX B: Customizing the Login Page for GrIDsure Token". Perform the following steps to access the assigned applications:

1. In a web browser, open the Wallix AdminBastion Suite URL.
   

2. On the login window, perform the following steps:
   
   a. In the **User name** field, enter your username.
   
   b. Click **Get GrID**.
   
   c. In the **Password** field, enter the grid combination.
d. Click **Log in**.

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

After successful authentication, you will be able to access the internal resources.

(The screen image above is from Wallix AdminBastion Suite. Trademarks are the property of their respective owners.)
APPENDIX A: Customizing the Login Page for PushOTP Token

Perform the following steps to customize the login page:

1. Connect to the Wallix AdminBastion suite appliance as `wabadmin` using putty or SSH.

   ```
   $ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no -p 2242 wabadmin@10.10.yy.zz
   wabadmin@10.10.yy.zz's password:
   ...
   Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
   Last login: Mon Nov 13 10:55:53 2017 from 10.10.xx.yy
   wabadmin@wab504:~$
   ```

2. Switch from `wabadmin` to the `wabsuper` user.

   ```
wabadmin@wab504:~$ super
   [sudo] password for wabsuper:
   wabsuper@wab504:/home/wabadmin$
   ```

3. Switch from `wabsuper` user to the root user.

   ```
wabsuper@wab504:/home/wabadmin$ sudo -i
   [sudo] password for wabsuper:
   root@wab504:~$
   ```

4. Open the `login.html` file that is available in the `/opt/wab/share/sitedjango/templates` directory and then perform the following steps:
   
   c. Search the following content:
      
      ```html
      <td style="width: 220px;">
      <input type="password" id="passwd" name="passwd" autocomplete="off" />
      </td>
      ```
   
   d. Enter the following content below the content searched in the previous step:
      
      ```html
      <tr>
      <th colspan=2 style="width: auto; text-align: left">
      </th>
      ```
<input type="radio" id="ManualPassword" name="RadioPassword" 
onClick='pushOTP(true);' checked >
<label for="ManualPassword">Enter passcode manually</label>
<br>
<input type="radio" id="AutosendPassword" 
name="RadioPassword"
onClick='pushOTP(false);' >
<label for="AutosendPassword">Use my mobile to autosend passcode</label>
</div>
</th>
</tr>

5. Save the Changes.

6. Run the following command to check the permission and ownership set for this file:

```bash
ls –al /opt/wab/share/sitedjango/templates/login.html
```

7. Run the following command to enforce the permission and ownership in case rights are different:

```bash
chmod 444 /opt/wab/share/sitedjango/templates/login.html
```
8. Run the following commands to restart the services:

   systemctl restart wabengine
   systemctl restart wabgui
APPENDIX B: Customizing the Login Page for GrIDsure Token

Perform the following steps to display the GrIDsure served by Gemalto:

1. Connect to the Wallix AdminBastion suite appliance as wabadmin using putty or SSH.

   ```
   $ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no -p 2242 wabadmin@10.10.yy.zz
   wabadmin@10.10.yy.zz's password:
   The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 13 10:55:53 2017 from 10.10.xx.yy
wabadmin@wab504:~$
   ```

2. Switch from wabadmin to the wabsuper user.

   ```
   wabadmin@wab504:~$ sudo [sudo] password for wabsuper:
   wabsuper@wab504:/home/wabadmin$
   ```

3. Switch from wabsuper user to the root user.

   ```
   wabsuper@wab504:/home/wabadmin$ sudo -i
   [sudo] password for wabsuper:
   root@wab504:~$
   ```

4. Open the login.html file that is available in the /opt/wab/share/sitedjango/templates directory and then perform the following the steps:
   a. Search for the following code:

      ```
      <div class="copyright">
      Copyright © 2017 WALLIX
      </div>
      ```
b. Add the following code above the code searched in the previous step:

```html
<tr>
<th colspan=2 style="width: auto;">
<input type="button" name="grIDButton" value="Get GrID"
onclick=GetGrID() />
<input type="submit" id="SubmitLogin" name="login" value="{% trans 'Log in' %}"/>
</th>
</tr>
<tr>
<th colspan=2 style="width: auto;">
<img id="grIDImage" name="grIDImage" style="visibility:hidden;"/>
</th>
</tr>
</table>
</form>
</div>
```

c. Search for the following code:

```html
{% block bottom_scripts %}
{% endblock %}
```

d. Add the following code in between the code (`{% block bottom_scripts %}` and `{% endblock %}`) searched in the previous step:

```javascript
$('#user_name').focus();
var gridURL="<Change to Org's Unique Self-Service URL from SAS>?getChallengeImage=true&userName=";
function GetGrID() {
  sUser=document.getElementsByName("user_name")[0].value;
  if (sUser != "") {
    grIDImage = document.getElementById("grIDImage");
    grIDImage.src = gridURL + sUser;
    grIDImage.style.visibility = "visible";
    document.getElementsByName("passwd")[0].focus()
  }
}
```

// BlackShieldServerLocation Org's Unique Self-Service URL might look like the following:
5. Save the Changes.

6. Run the following command to check the permission and ownership set for this file:
   
   ```bash
   ls -al /opt/wab/share/sitedjango/templates/login.html
   ```

   ![Image of ls output]

7. Run the following command to enforce the permission and ownership in case rights are different:
   
   ```bash
   chmod 444 /opt/wab/share/sitedjango/templates/login.html
   ```

   ![Image of chmod output]

8. Open the Apache2 configuration file, `wab-httpd.conf` file available in the `/etc/apache2/sites-available/wab-httpd.conf` directory.

9. In the file, add the source code (displayed in the below image) below the line containing “Content-Security-Policy” to update Content Security Policy (CSP) to allow loading of images from an external source.

   ```
   # Set up Cross-site scripting (XSS) filter
   Header always set X-XSS-Protection "1; mode=block"
   ```

10. Run the following commands to restart `wabengine` and `wabgui` services.

    ```bash
    systemctl restart wabengine
    systemctl restart wabgui
    ```