SafeNet Authentication Service
Push OTP Integration Guide

Using RADIUS Protocol for Citrix NetScaler Access Gateway
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Citrix NetScaler Access Gateway.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Citrix NetScaler Access Gateway is a secure application and data access solution that gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities as well as evolving business requirements underscore the need for a strong authentication approach based on multi-factor authentication.

This document describes how to:

- Configure Citrix NetScaler Access Gateway to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Citrix NetScaler Access Gateway environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Citrix NetScaler Access Gateway can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with the 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 is 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 (SAS)**
- **Citrix NetScaler Access Gateway**—Version 10.5

Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler Access Gateway, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SAS Cloud

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](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](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 SAS-SPE and SAS-PCE

For both on-premise versions, 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 SAS

SafeNet Authentication Service 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 Citrix NetScaler Access Gateway.

---

1. A user attempts to log on to Citrix NetScaler Access Gateway using a Push OTP authenticator.

2. Citrix NetScaler Access Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Service 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 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 Citrix NetScaler Access Gateway.
5. The user is granted or denied access to Citrix NetScaler Access Gateway based on the OTP value calculation results from SAS.

**RADIUS Prerequisites**

To enable SafeNet Authentication Service to receive RADIUS requests from Citrix NetScaler Access Gateway, ensure the following:

- End users can authenticate from the Citrix NetScaler Access Gateway environment with a static password before configuring Citrix NetScaler Access Gateway to use RADIUS authentication.
- Ports 1812/1813 are open to and from Citrix NetScaler Access Gateway.
- 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.

**Push OTP Prerequisites**

In order to use SAS OTP, you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

**Configuring SafeNet Authentication Service**

The deployment of multi-factor authentication using SAS with Citrix NetScaler Access Gateway using the RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 8
- Assigning an Authenticator in SAS, page 8
- Adding Citrix NetScaler Access Gateway as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 11
- Enabling the Software Token Push OTP Setting, page 12
- Enabling the Allowed Targets Policy, page 13
Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the *SafeNet Authentication Service Subscriber Account Operator Guide*:


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

Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Citrix NetScaler Access Gateway.

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 Citrix NetScaler Access Gateway as an Authentication Node in SAS

Add a RADIUS entry in the SAS Auth Nodes module to prepare it to receive RADIUS authentication requests from Citrix NetScaler Access Gateway. You will need the IP address of Citrix NetScaler Access Gateway and the shared secret to be used by both SAS and Citrix NetScaler Access Gateway.

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](image1)

   **Auth Nodes:**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Nodes:</td>
<td>Create and configure SafeNet Authentication Service Authentication Nodes</td>
</tr>
</tbody>
</table>

   **Auth Nodes:**

   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.

   ![Auth Nodes](image2)

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

5. In the **Add Auth Nodes** section, 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 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).

   **High IP Address In Range** | 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).

   **Configure FreeRADIUS Synchronization** | Select this option.

   **Shared Secret** | Enter the shared secret key.

   **Confirm Shared Secret** | Re-enter the shared secret key.
The Auth Node is added to the system.

Checking the SAS RADIUS Server's IP Address

Before adding SAS as a RADIUS server in Citrix NetScaler Access Gateway, check its IP address. The IP address will then be added to Citrix NetScaler Access Gateway as a RADIUS server at a later stage.

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

2. Click the COMMS tab, and then select Auth Nodes.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes Module](image)

**Enabling the Software Token Push OTP Setting**

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Citrix NetScaler Access Gateway. You will need the IP address of Citrix NetScaler Access Gateway and the shared secret to be used by both SAS and Citrix NetScaler Access Gateway.

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

![SAS Console](image)

2. Click the **POLICY** tab, and then select **Token Policies**.

![Token Policies](image)
3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

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 SAS console with an Operator account.
2. Click the **POLICY** tab, and then select **Token Policies**.

3. In the **Token Policies** module, click the **Allow Targets Settings** link.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application, and then click **Apply**.
Configuring Citrix NetScaler Access Gateway

Configure Citrix NetScaler Access Gateway to use the RADIUS protocol as a secondary authentication method.

1. Log in to the Citrix NetScaler administrator console.
2. On the **Configuration** tab, in the left pane, click **NetScaler Gateway > Policies > Authentication > RADIUS**.

![NetScaler Gateway Configuration](image)

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

3. In the right pane, click **Add**.
4. On the **Create Authentication RADIUS Policy** window, perform the following steps:
   a. In the **Name** field, enter a name for the policy.

![Create Authentication RADIUS Policy](image)

* (The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)
b. In the **Server** field, click on the plus sign on the right.

c. On the **Create Authentication RADIUS Server** window, complete the following fields, and then click **Create**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name/Server IP</td>
<td>Select any option.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the name or IP address of the server, depending on the option selected in the previous field.</td>
</tr>
<tr>
<td>Time-out (seconds)</td>
<td>Enter 60.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the shared RADIUS secret.</td>
</tr>
<tr>
<td>Confirm Secret Key</td>
<td>Enter the shared RADIUS secret again.</td>
</tr>
</tbody>
</table>

(d. On the **Create Authentication RADIUS Policy** window, under Expression, click **Saved Policy Expressions** and select **ns_true**.

e. Click **Create**.

Now you need to bind RADIUS authentication to the virtual server.)
5. On the **Configuration** tab, in the left pane, click **NetScaler Gateway > Virtual Servers**.

   ![NetScaler Gateway Virtual Servers](image1)

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

6. In the right pane, select the gateway you created, and then click **Edit**.

7. Under **Authentication**, click the plus sign (+).

   ![NetScaler Gateway Virtual Server](image2)

   *(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)*
8. Under **Policies**, complete the following fields, and then click **Continue**.

<table>
<thead>
<tr>
<th>Choose Policy</th>
<th>Select RADIUS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Type</td>
<td>Select <strong>Secondary</strong>.</td>
</tr>
</tbody>
</table>

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

9. Under **Policy Binding**, in the **Select Policy** field, select the RADIUS policy you created in step 3, and then click **Bind**.

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

10. Click **Done**.
Authenticating Using Push OTP OOB

To avoid the duplicate password field when using SMS authentication with Citrix NetScaler Access Gateway, hide the secondary authentication password field that is used to trigger the SMS messaging, by adjusting the default login.js file found on NetScaler.

To customize the logon page and hide the second password field:

1. Connect to the VPX server console:
   ```
   ssh/direct
   ```
2. Backup the following file:
   ```
   /netscaler/ns_gui/vpn/login.js
   ```
3. Edit the `login.js` file.
4. Locate the following section:
   ```plaintext
default login.js

   if ( pwc == 2 ) {
       document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;"<SPAN class="CTXMSAM_LogonFont"> + _("Password2") + '</SPAN><TD colspan=2 style="padding-right:8px;"> <input class="CTXMSAM_ContentFont" type="hidden" value="1" title=" + _("Enter password") + " name="passwd1" size="30" maxlength="127" style="width:100%;"></TD></TR>');
   }
```
5. Add the content highlighted in yellow below:
   ```plaintext
default login.js

   if ( pwc == 2 ) {
       document.write('<TR style="display:none"><TD align=right style="padding-right:10px;white-space:nowrap;"<SPAN class="CTXMSAM_LogonFont"> + _("Password2") + '</SPAN><TD colspan=2 style="padding-right:8px;"> <input class="CTXMSAM_ContentFont" type="hidden" value="1" title=" + _("Enter password") + " name="passwd1" size="30" maxlength="127" style="width:100%;"></TD></TR>');
   }
```
6. To ensure that the changes will be kept the next time the system is rebooted, do the following:
   a. Run the following command to create a directory to store the modification files:
      ```
      mkdir /var/customization
      ```
   b. Run the following commands to copy the modified files to the customization directory:
      ```
      cp /netscaler/ns_gui/vpn/login.js /var/customizations/login.js.mod
      cp /netscaler/ns_gui/vpn/resources/en.xml /var/customizations/en.xml.mod
      cp /netscaler/ns_gui/vpn/images/caxtonstyle.css /var/customizations/images/caxtonstyle.css.mod
      ```
   c. If the `/nsconfig/rc.netscaler` file does not exist, execute the following command to create it:
      ```
      touch /nsconfig/rc.netscaler
      ```
   d. Run the following commands to add an entry for each command to the `rc.netscaler` file:
      ```
      echo cp /var/customizations/login.js.mod /netscaler/ns_gui/vpn/login.js >>/nsconfig/rc.netscaler
      echo cp /var/customizations/en.xml.mod /netscaler/ns_gui/vpn/resources/en.xml >>/nsconfig/rc.netscaler
      echo cp /var/customizations/images/* /netscaler/ns_gui/vpn/images/ >>/nsconfig/rc.netscaler
      ```
Running the Solution

After NetScaler is configured to use RADIUS with SafeNet Authentication Service, you can log in to the NetScaler Access Gateway.

Connecting to Citrix NetScaler Access Gateway using Simple Mode

1. In a web browser, open the NetScaler Access Gateway login page.
2. Enter the user name and user domain password, and then click Log On.

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

3. A push notification message is triggered. Tap Approve.
4. Enter the **PIN** and tap **Continue**.

Once you tap **Submit**, you are authenticated to Citrix NetScaler Access Gateway.

*(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)*
Customizing the Citrix NetScaler Logon Page

When multi-factor authentication is configured on the Access Gateway Enterprise Edition, the user is prompted for User name, Password 1, and Password 2. The Password 1 and Password 2 fields can be changed to something more descriptive, such as Windows Password or SafeNet passcode.

To change text on the logon page:

1. Log in to the Citrix NetScaler computer using SSH.
2. Go to /netscaler/ns_gui/vpn/resources.
   In the Resources folder, you will find several XML files, one for each language (for example, en.xml for English). This example uses the English version. For other languages, follow the same procedure.
3. Take the backup of the en.xml file.
4. Open the en.xml file using a text editor.
5. Search for the Password string and replace it with your text (for example, Windows Password).
6. Search for the Password2 string and replace it with your text (for example, SafeNet Passcode).
7. Save the en.xml file.
8. Go to /netscaler/ns_gui/vpn.
9. Take the backup of the login.js file.
10. Open the login.js file using a text editor.
11. Search for the following line:
    ```javascript
    if ( pwc == 2 ) { document.write('&nbsp;1'); }
    ```
12. Delete the character 1 and save the login.js file.

   The modifications result in the labels Password 1 and Password 2 being changed to Windows Password and SafeNet Password respectively.

Before:
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, Inc.</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</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>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>