

SafeNet Authentication Service Integration Guide

Using RADIUS Protocol for Citrix NetScaler Gateway with GridSure Token

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.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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: 007-013455-001, Rev. B

Release Date: May 2017

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	4
Environment.....	4
Audience	5
RADIUS-based Authentication using SafeNet Authentication Service Cloud	5
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE	6
RADIUS Authentication Flow using SafeNet Authentication Service	6
RADIUS Prerequisites	7
Configuring SafeNet Authentication Service	7
Creating Users Stores in SafeNet Authentication Service	7
Assigning an Authenticator in SafeNet Authentication Service.....	7
Adding Citrix NetScaler Gateway as an Authentication Node in SafeNet Authentication Service	8
Configuring Citrix NetScaler Gateway	11
Configuring to Use the GrIDSure Authentication Token.....	14
Creating a Citrix NetScaler Gateway Portal Theme.....	14
Binding a Citrix NetScaler Gateway Portal Theme to the Virtual Gateway.....	16
Modifying the Citrix NetScaler Gateway Login Page to Use the GrIDSure Token	17
Running the Solution	19
Support Contacts	21

Third-Party Software Acknowledgement

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

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

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

Citrix NetScaler Gateway 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)**
- **Citrix NetScaler Gateway**—Version 11

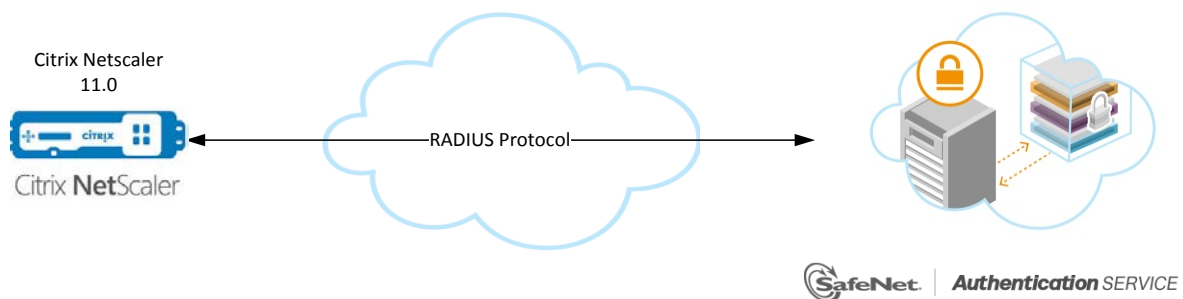
Audience

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

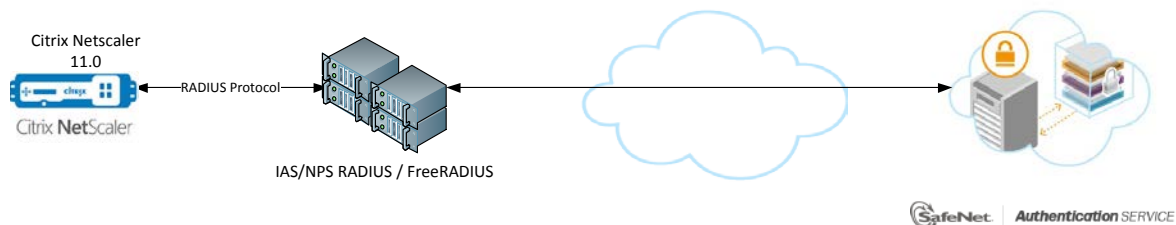
RADIUS-based Authentication using SafeNet Authentication Service Cloud

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.



- **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.



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:

http://www2.gemalto.com/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.pdf

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:

http://www2.gemalto.com/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.pdf

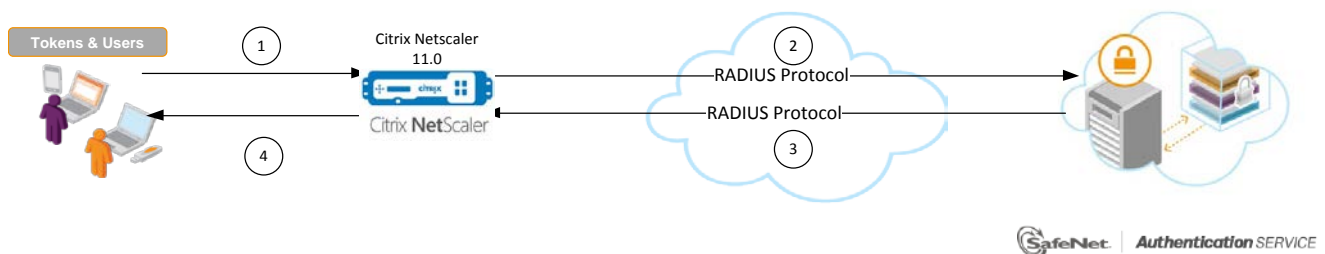
- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the [Gemalto Support Portal](#).

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 data flow of a multi-factor authentication transaction for Citrix NetScaler Gateway.



1. A user attempts to log on to Citrix NetScaler Gateway using Grid authenticator.
2. Citrix NetScaler Gateway sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the Citrix NetScaler Gateway.
4. The user is granted or denied access to the Citrix NetScaler Gateway based on the Grid value calculation results from SAS.

RADIUS Prerequisites

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

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

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Citrix NetScaler Gateway using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
- Adding Citrix NetScaler Gateway as an Authentication Node in SafeNet Authentication Service, page 8

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*:

http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/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 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 Citrix NetScaler Gateway.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS
- GrIDSure Authentication

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.

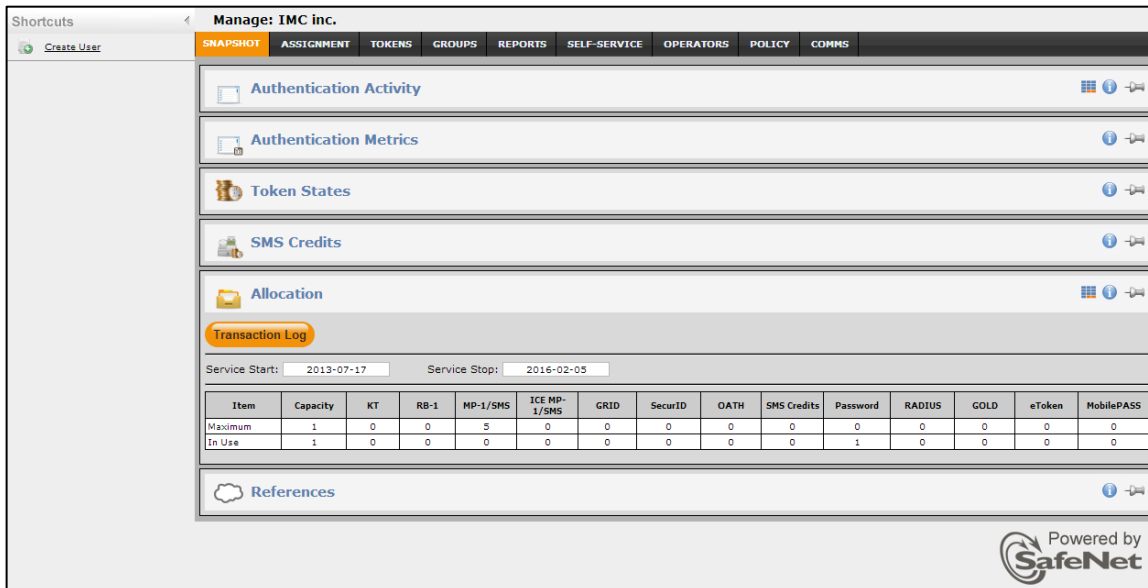
Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/

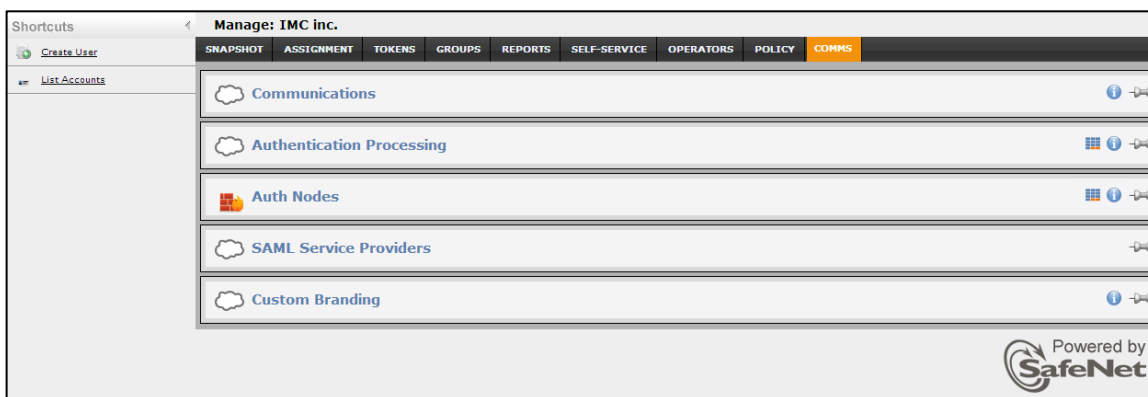
Adding Citrix NetScaler Gateway as an Authentication Node in SafeNet Authentication Service

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





NOTE: Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Citrix NetScaler Gateway, check its IP address (Primary RADIUS Server IP). The IP address will then be added to Citrix NetScaler Gateway as a RADIUS server at a later stage.

- Under **Auth Nodes**, click **Add**.
- In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

Agent Description	Enter a host description.
Host Name	Enter the name of the host that will authenticate with SAS.
Low IP Address In Range	Enter the IP address of the host that will authenticate with SAS.
Configure FreeRADIUS Synchronization	Select this option.
Shared Secret	Enter the shared secret key.
Confirm Shared Secret	Re-enter the shared secret key.

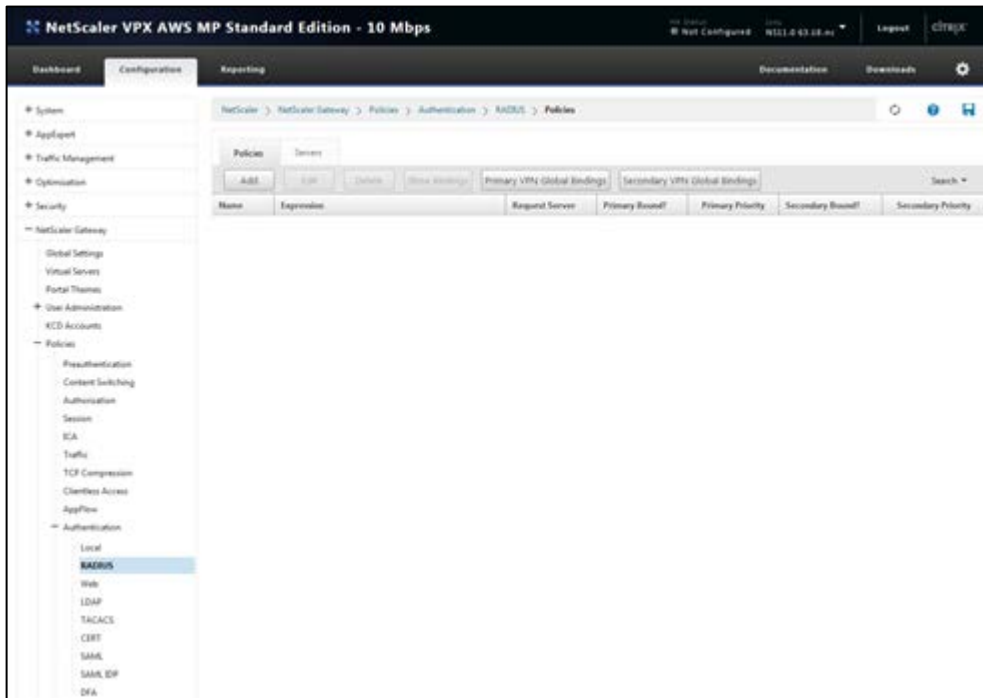
The authentication node is added to the system.

Index	Description	Host Name	IP Address	FreeRADIUS Synchronization	Edit	Remove
1	Citrix Netscaler	Citrix Netscaler	10.9.17.1	True	Edit	Remove

Configuring Citrix NetScaler Gateway

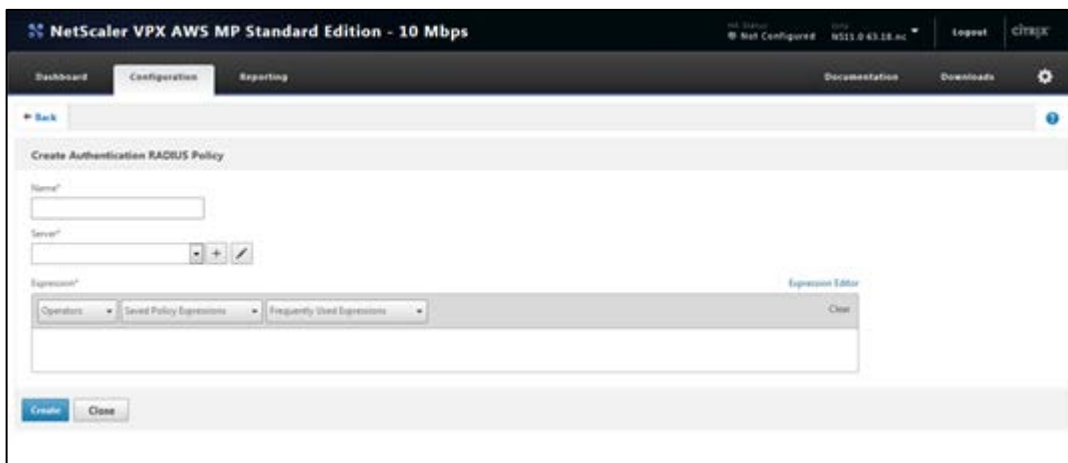
Configure Citrix NetScaler Gateway to use the RADIUS protocol as a secondary authentication method.

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



(The screen image above is from Citrix®. 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 (for example, **SAS_Cloud**).



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

- b. In the **Server** field, click the  icon.

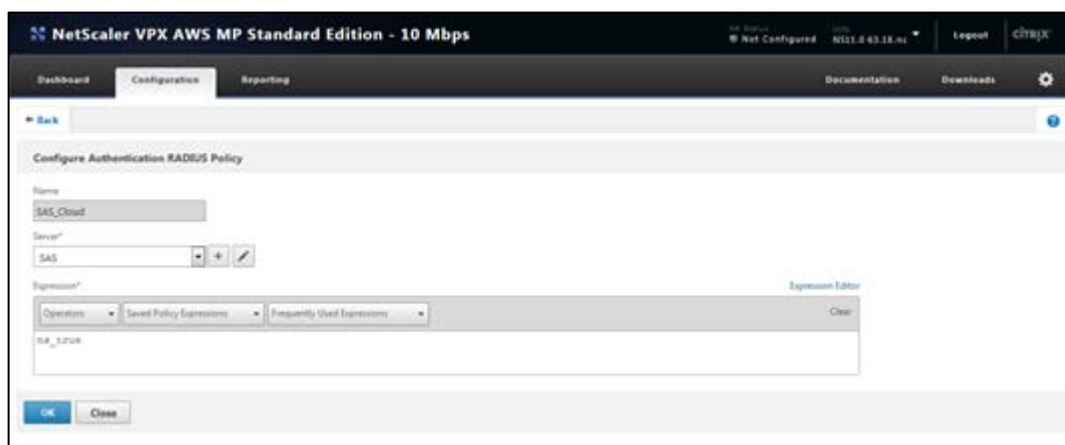
- c. On the **Create Authentication RADIUS Server** window, complete the following fields, and then click **Create**.

Name	Enter a name for the server.
Server Name/Server IP	Select an option, according to your preferred configuration.
Server Name	Enter the name or IP address of the server, depending on the option selected in the previous field.
Secret Key	Enter the shared secret that you entered in step 5 of “Adding Citrix NetScaler Gateway as an Authentication Node in SafeNet Authentication Service” on page 8.
Confirm Secret Key	Re-enter the shared secret.



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

- d. On the **Configure Authentication RADIUS Policy** window, under **Expression**, click **Saved Policy Expressions**, and then select **ns_true**.
- e. Click **OK**.




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

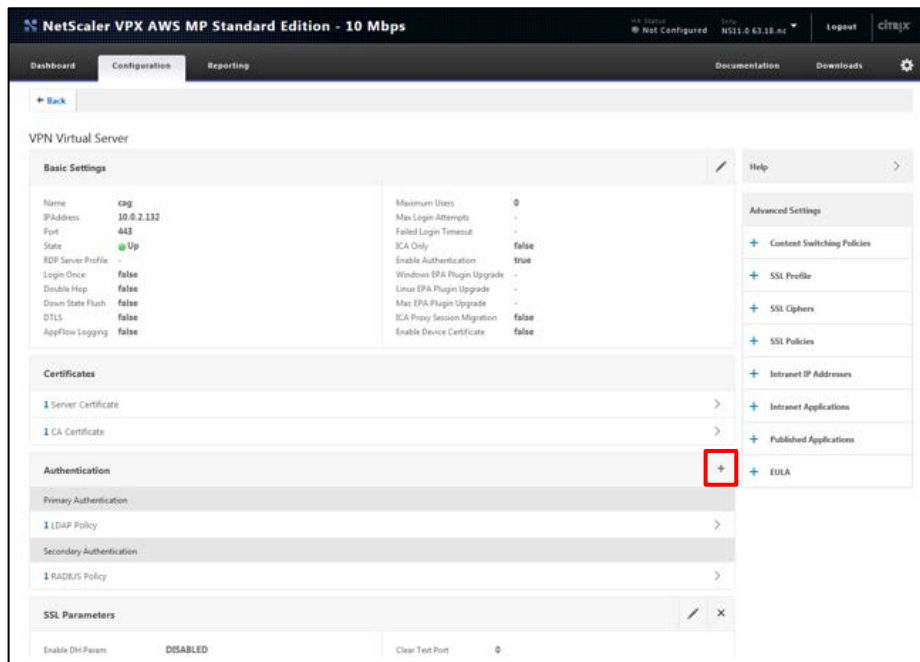
Now, you need to bind the RADIUS authentication to the virtual server.

5. On the **Configuration** tab, in the left pane, click **NetScaler Gateway > Virtual Servers**.



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

6. In the right pane, select the gateway you created (for example, **cag**), and then click **Edit**.
7. Under **Authentication**, click the  icon.



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

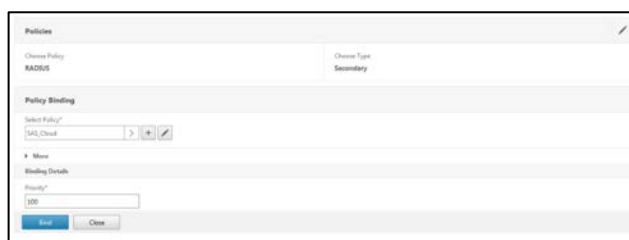
8. Under **Policies**, complete the following fields and then click **Continue**.

Choose Policy	Select RADIUS .
Choose Type	Select Secondary .



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

9. Under **Policy Binding**, in the **Select Policy** field, select the RADIUS policy (for example, **SAS_Cloud**) that you created earlier in step 4, and then click **Bind**.



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

10. Click **Done**.

Configuring to Use the GrIDSure Authentication Token

Configuring to use the GrIDSure authentication token requires:

- Creating a Citrix NetScaler Gateway Portal Theme, page 14
- Binding a Citrix NetScaler Gateway Portal Theme to the Virtual Gateway, page 16
- Modifying the Citrix NetScaler Gateway Login Page to Use the GrIDSure Token, page 17

Creating a Citrix NetScaler Gateway Portal Theme

Create a portal theme and customize the field(s) of the Citrix NetScaler Gateway login window.

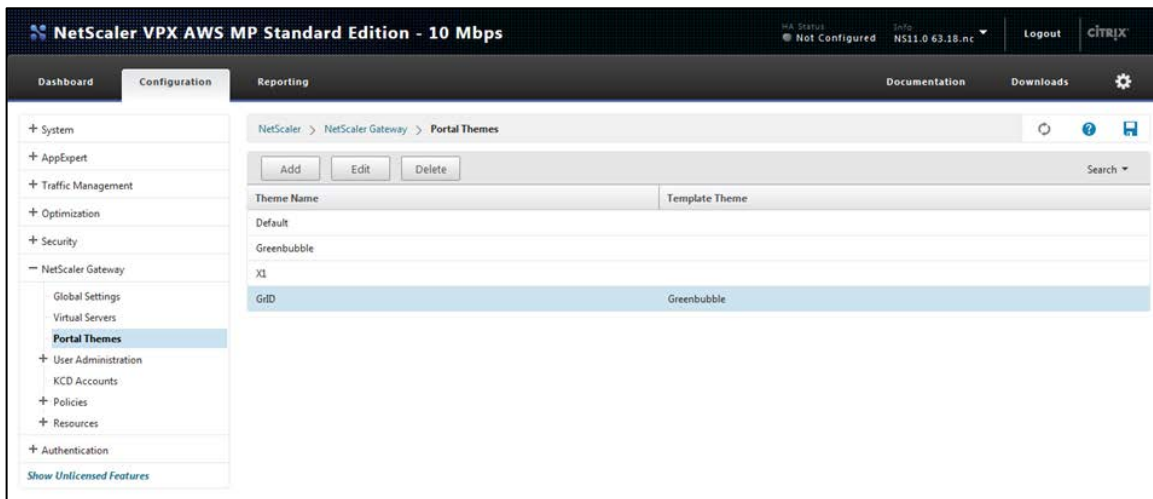
1. Log in to the Citrix NetScaler console as an administrator.

2. On the **Configuration** tab, in the left pane, click **NetScaler Gateway > Portal Themes**.



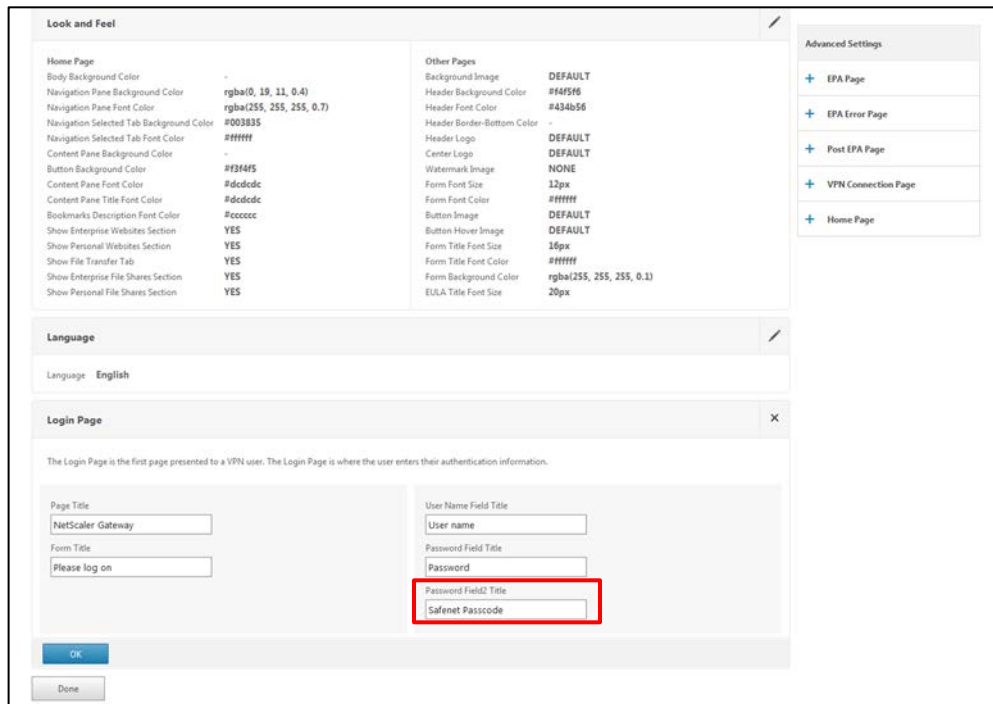
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

3. In the right pane, click **Add** and then create a portal theme (for example, **GrID**).
4. The newly created portal theme is listed. Select the portal theme and then click **Edit**.



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

- Under **Login Page**, in the **Password Field2 Title** field, enter a title for the field as per your preferred configuration, and then click **OK**.

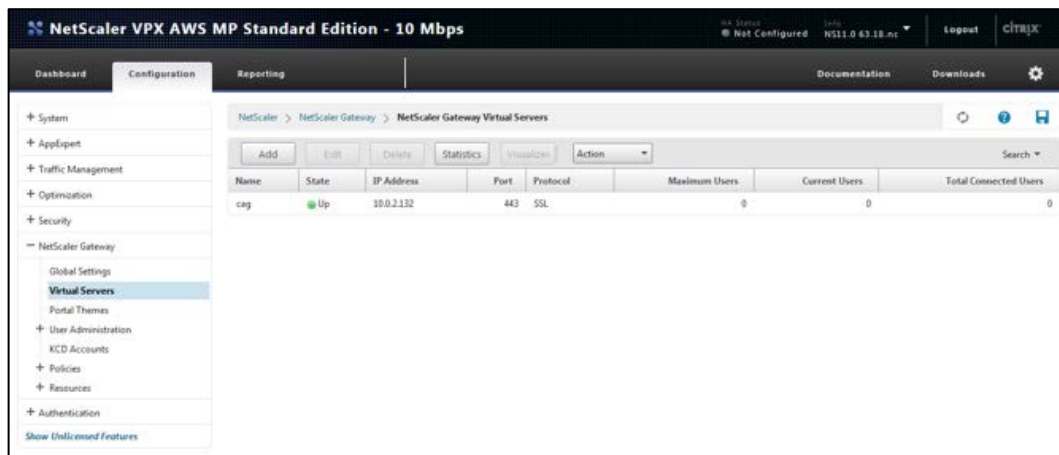


(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)


- Click **Done**.

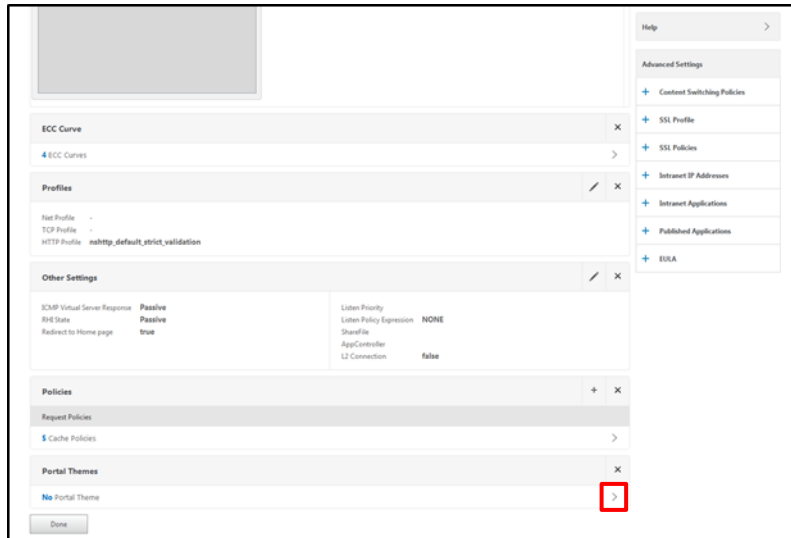
Binding a Citrix NetScaler Gateway Portal Theme to the Virtual Gateway

- Log in to the Citrix NetScaler administrator console.
- On the **Configuration** tab, go to **NetScaler Gateway > Virtual Servers**.



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

- In the right pane, select the gateway you created (for example, **cag**), and then click **Edit**.
- Under **Portal Themes**, the click  icon.



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

- On the **Portal Theme Binding** window, select the portal theme (for example, **GRID**) that you created earlier in Step 3 of “Creating a Citrix NetScaler Gateway Portal Theme” on page 14, and then click **Bind**.



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

- Click **Done**.

Modifying the Citrix NetScaler Gateway Login Page to Use the GridSure Token

Modify the **index.html** and **gateway_login_form_view.js** files to use the GridSure token.

- Connect to the NetScaler machine using an SSH client.
- Back up the following file:
/netscaler/ns_gui/vpn/index.html
- Edit the **index.html** file.
- Locate the script tag and then add the following under the tag:

```
var BlackShieldServerLocation = ("https://grid.safenet-inc.com/blackshieldss/O/XXXXXXXXXX/index.aspx");
```

```
function getChallenge(){
```

```
    var userName = document.getElementById("Enter user name").value;  
    var challengeImg = document.getElementById("challengeImage");  
    challengeImg.src = BlackShieldServerLocation + "?getChallengeImage=true&userName=" +  
        userName + "&noCache=" + new Date().toString();
```

```

    var challengeDiv = document.getElementById("challengeImageDiv");
    challengeDiv.style.display="block";
    challengeDiv.style.visibility="visible";
}

```

Where, the highlighted content is the self-service identifier.

5. Save the file.

6. Back up the following file:

```
/netscaler/ns_gui/vpn/js/gateway_login_form_view.js
```

7. Edit the **gateway_login_form_view.js** file.

8. Locate the line starting with:

```
var Login = $
```

9. After the line starting with **var Login = \$**, add the following:

```
var GrID = $("<input type='button' onclick='getChallenge()'></input>").attr({'id':'GrID','value':'Get GrID','class':'custombutton login_page'}).appendTo(right_loginbutton);
```

```
var hidChallengeImg=$(("<div id='challengeImageDiv' style='visibility:hidden; display:none;'><img id='challengeImage' src='/'></div>").appendTo(right_loginbutton);
```

10. Save the file.

11. To ensure that the changes will be kept the next time the system is rebooted, perform the following steps:

a. Run the following command to create a directory to store the modified file (for example, **/var/customizations**):

```
mkdir /var/customizations
```

b. Run the following commands to copy the modified files to the **customizations** directory:

```
cp /netscaler/ns_gui/vpn/js/gateway_login_form_view.js
/var/customizations/gateway_login_form_view.js.mod
```

```
cp /netscaler/ns_gui/vpn/index.html /var/customizations/index.html.mod
```

c. If the **/nsconfig/rc.netscaler** file does not exist, execute the following commands to create it:

```
touch /nsconfig/rc.netscaler
```

```
chmod a+x rc.netscaler
```

d. Run the following commands to add an entry for the command to the **rc.netscaler** file:

```
echo cp /var/customizations/index.html.mod /netscaler/ns_gui/vpn/index.html>>
/nsconfig/rc.netscaler
```

```
echo cp /var/customizations/gateway_login_form_view.js.mod /netscaler/ns_gui/vpn/js/
gateway_login_form_view.js>> /nsconfig/rc.netscaler
```



NOTE: You can download the modified **index.html** and **gateway_login_form_view.js** files (packaged in the **NetScaler with GridSure Token for Citrix NetScaler Access Gateway 11.zip** file) from the following URL:

https://gemalto.service-now.com/csm?id=kb_article&sys_id=44aa7e534f42b288873b69d18110c7ae

Refer to **KB ID: KB0015432**.

You need to rename the downloaded files (**index_grid.html** and **gateway_login_form_view_grid.js**) to **index.html** and **gateway_login_form_view.js**

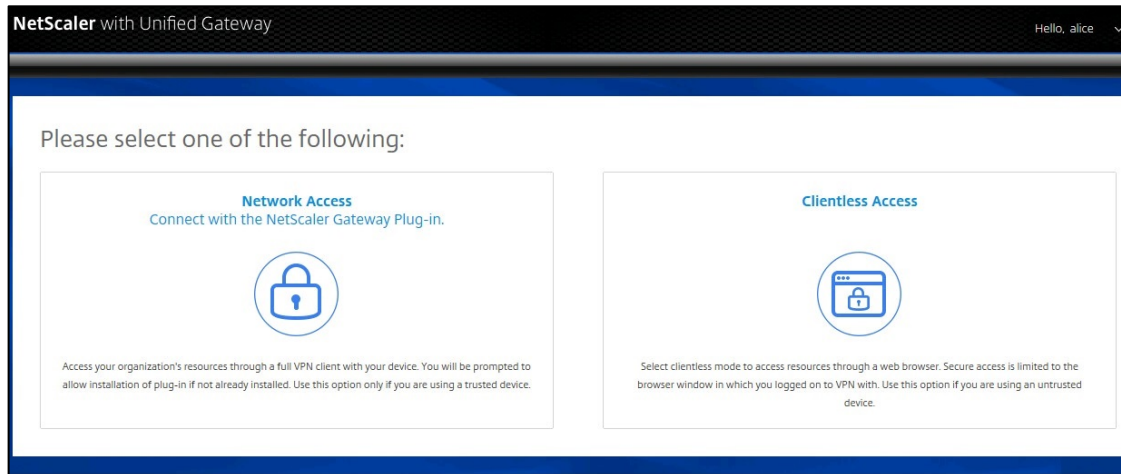
Running the Solution

1. In a web browser, open the Citrix NetScaler Gateway login window.
2. On the login window, perform the following steps:
 - a. In the **User name** field, enter the domain user name.
 - b. In the **Password** field, enter the domain password.
 - c. Click **Get Grid**.
 - d. In the **Safenet Passcode** field, enter your preferred grid pattern.
 - e. Click **Log On**.

4	1	9	6	7
6	5	8	3	5
0	5	9	1	7
2	8	4	0	4
3	2	2	6	8

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

After successful authentication, you are redirected to access the Citrix application.



(The screen image above is from Citrix®. 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.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com 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.	