# SafeNet Authentication Service

## Integration Guide

Using RADIUS Protocol for Citrix NetScaler Gateway with SMS Out-of-Band

gemalto
security to be free

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.

**Document Part Number:** 007-013446-001, Rev. C

**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 ........ 8
- Adding Citrix NetScaler Gateway as an Authentication Node in SafeNet Authentication Service ........ 9

Configuring Citrix NetScaler Gateway ........ 11

Modifying the Citrix NetScaler Gateway Login Window ........ 15

Running the Solution ........ 16

- MobilePASS Authentication Mode ........ 16
- SMS Authentication Mode ........ 17

Support Contacts ........ 20

# 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 to 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

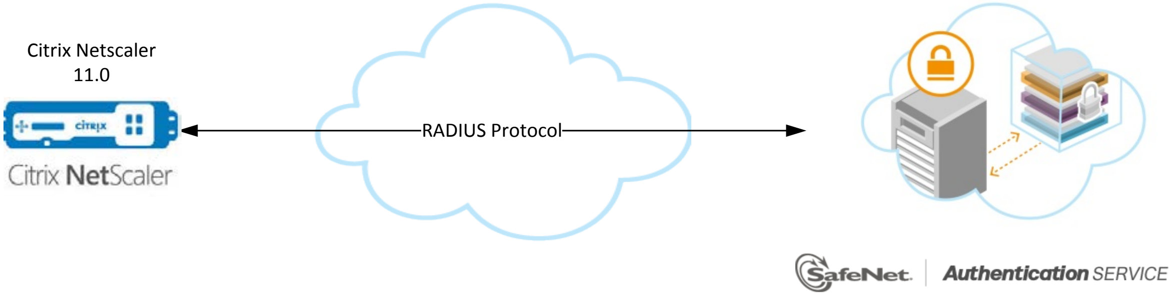
## Audience

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.

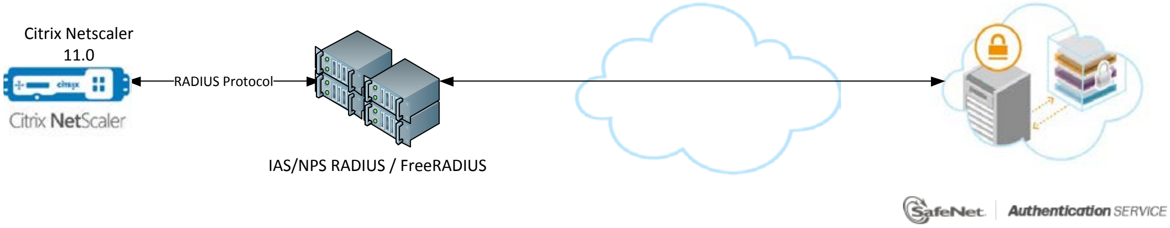
## RADIUS-based Authentication using SafeNet Authentication Service Cloud

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

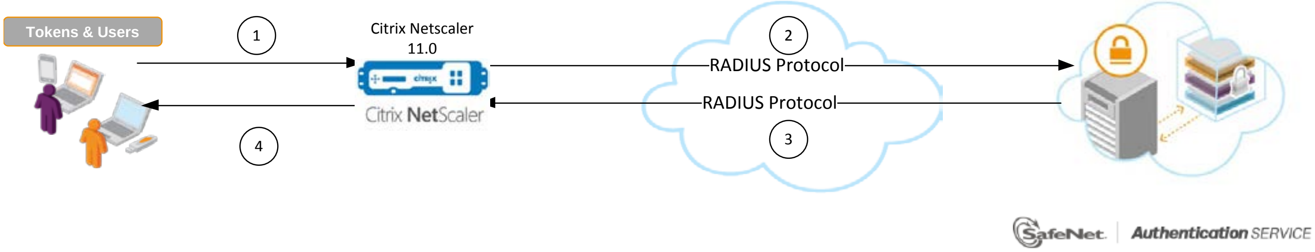
- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  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 SMS authenticator.
2. Citrix NetScaler Gateway sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
3. The SafeNet Authentication Service 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 SMS OTP value calculation results from SAS.

# RADIUS Prerequisites

To enable SafeNet Authentication Service 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 the RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- 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.

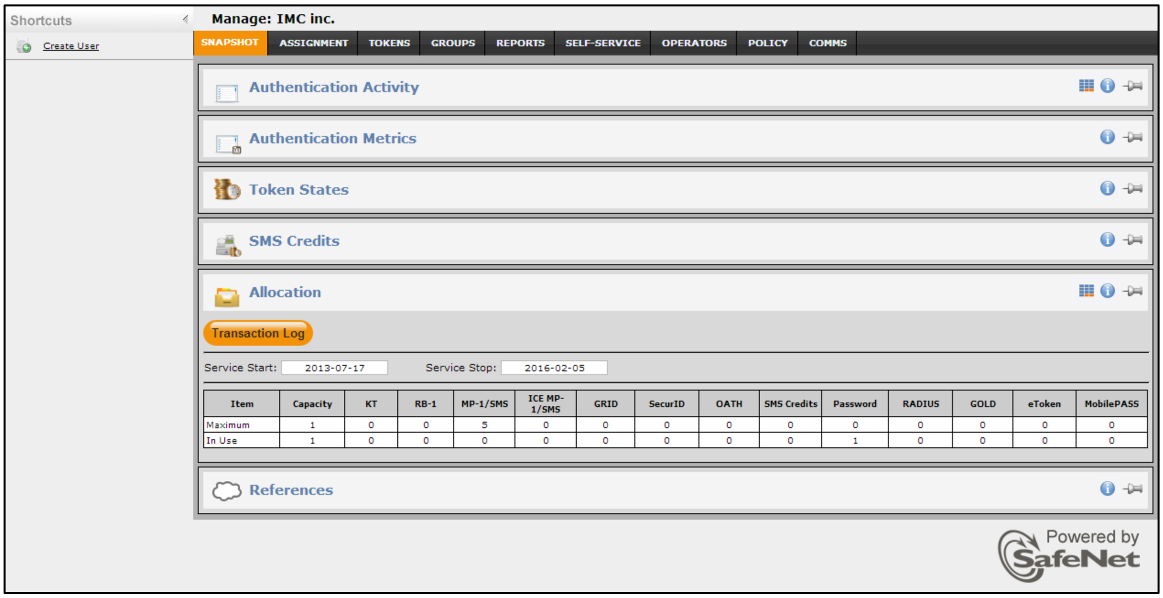
Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

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.

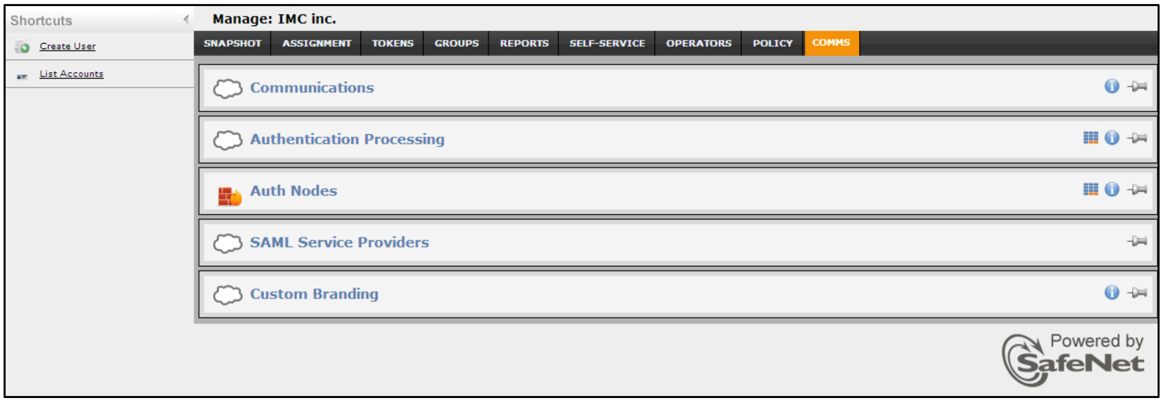
1. Log in to the SAS console with an Operator account.



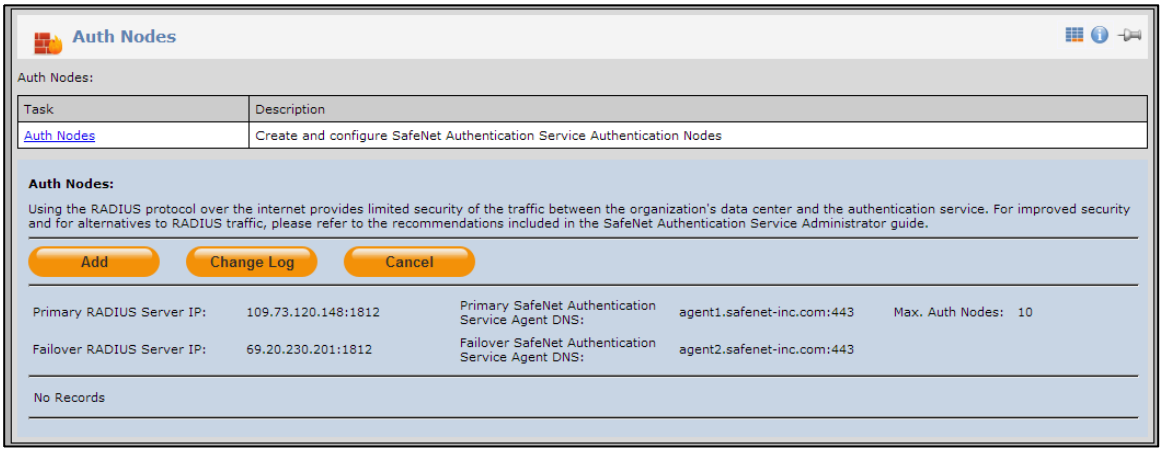
Service Start: 2013-07-17  Service Stop: 2016-02-05

| Item | Capacity | KT | RB-1 | MP-1/SMS | ICE MP-1/SMS | GRID | SecurID | OATH | SMS Credits | Password | RADIUS | GOLD | eToken | MobilePASS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Maximum | 1 | 0 | 0 | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| In Use | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

2. Click the **COMMS** tab, and then select **Auth Nodes**.



3. In the **Auth Nodes** module, click the **Auth Nodes** task.



Auth Nodes:

| Task | Description |
|---|---|
| Auth Nodes | Create and configure SafeNet Authentication Service Authentication Nodes |

**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, please refer to the recommendations included in the SafeNet Authentication Service Administrator guide.

| | | | | | |
|---|---|---|---|---|---|
| Primary RADIUS Server IP: | 109.73.120.148:1812 | Primary SafeNet Authentication Service Agent DNS: | agent1.safenet-inc.com:443 | Max. Auth Nodes: | 10 |
| Failover RADIUS Server IP: | 69.20.230.201:1812 | Failover SafeNet Authentication Service Agent DNS: | agent2.safenet-inc.com:443 | | |

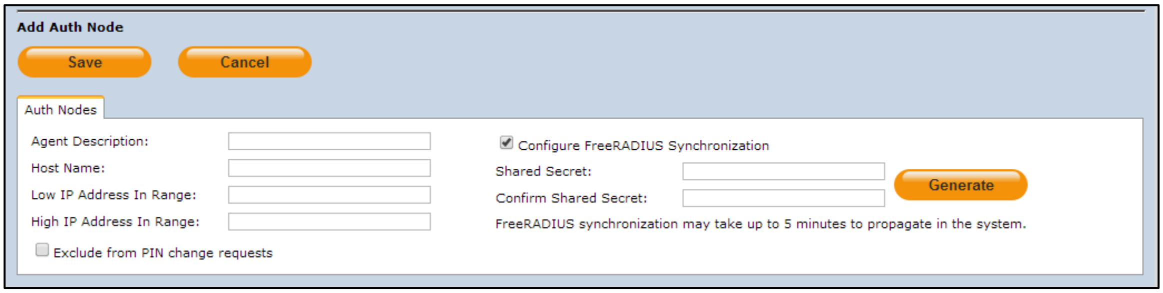
No Records

**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.

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

5. 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. |



Agent Description:

Host Name:

Low IP Address In Range:

High IP Address In Range:

□ Exclude from PIN change requests

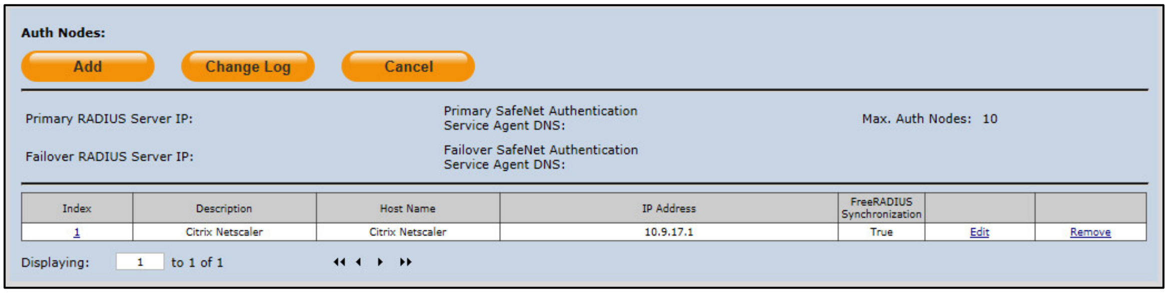
☑ Configure FreeRADIUS Synchronization

Shared Secret:

Confirm Shared Secret:

FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

The authentication node is added to the system.



**Auth Nodes:**

Add | Change Log | Cancel

Primary RADIUS Server IP:

Primary SafeNet Authentication Service Agent DNS:

Max. Auth Nodes: 10

Failover RADIUS Server IP:

Failover SafeNet Authentication Service Agent DNS:

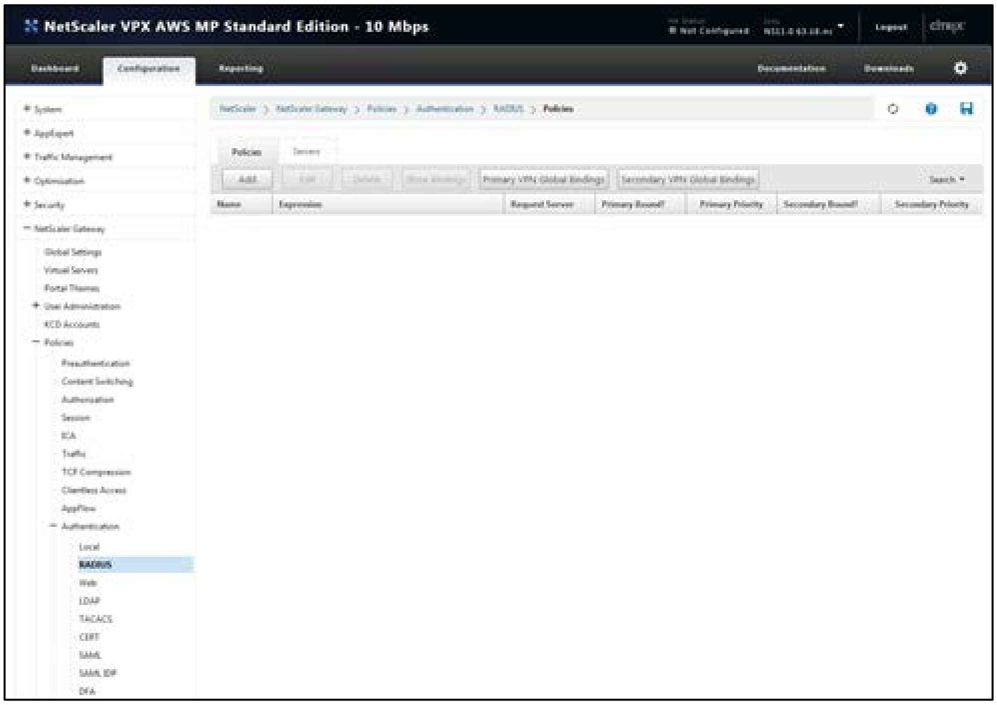
| Index | Description | Host Name | IP Address | FreeRADIUS Synchronization | | |
|---|---|---|---|---|---|---|
| 1 | Citrix Netscaler | Citrix Netscaler | 10.9.17.1 | True | Edit | Remove |

Displaying: 1 to 1 of 1

# Configuring Citrix NetScaler Gateway

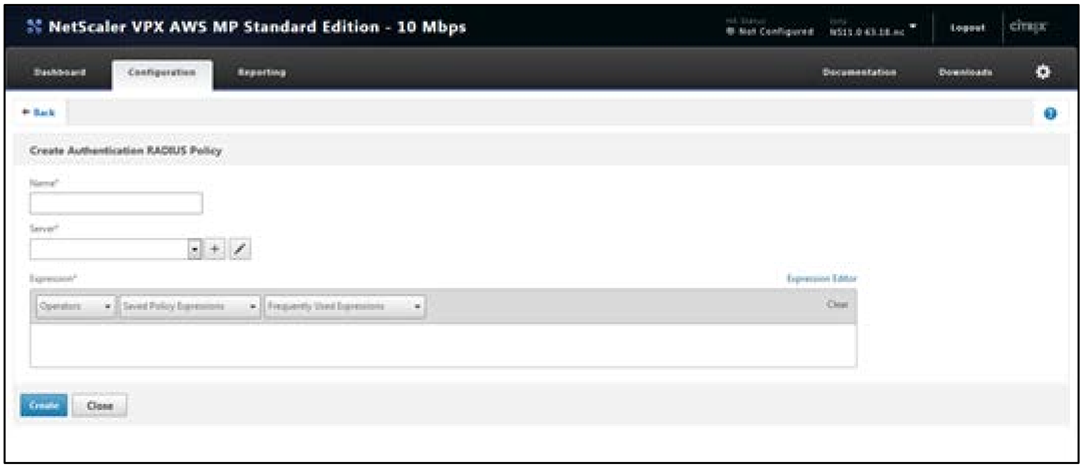
Configure Citrix NetScaler Gateway to use the RADIUS protocol as a secondary authentication method.

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.)*

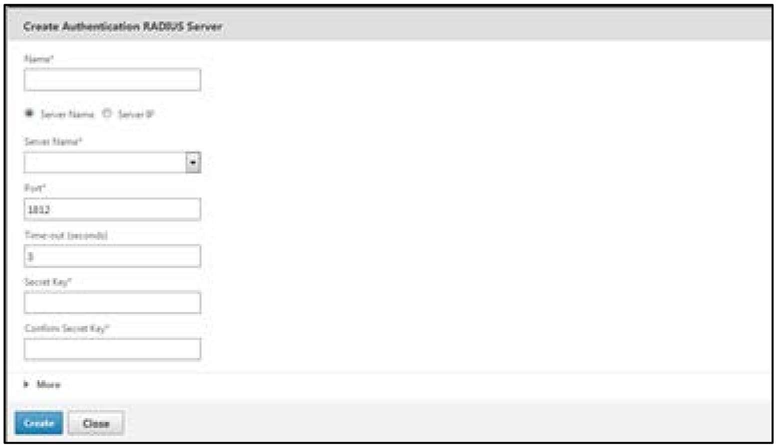
3. In the right pane, click **Add**.
4. On the **Create Authentication RADIUS Policy** window, perform the following steps:
   a. In the **Name** field, enter a name for the policy (for example, **SAS_Cloud**).



*(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. |
| **Confirm Secret Key** | Re-enter the shared secret. |



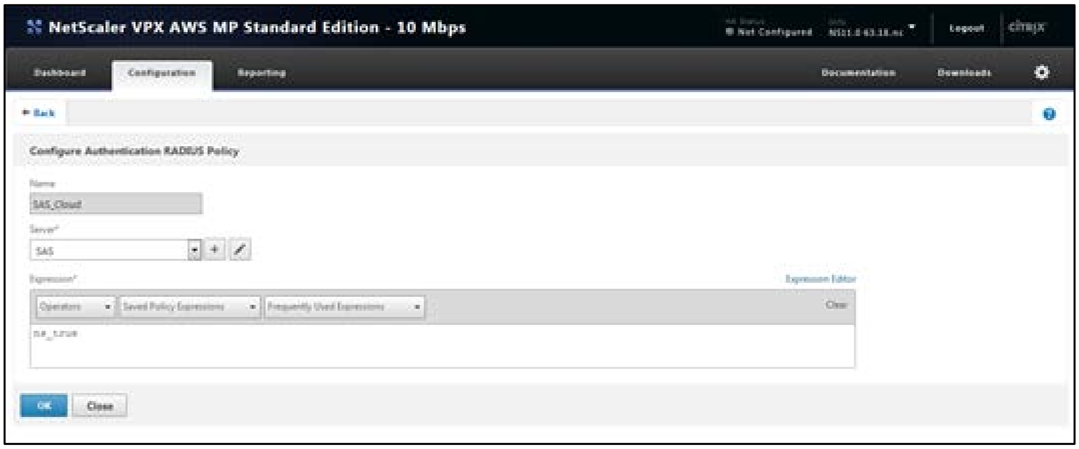
Port*: 1812

Time-out (seconds): 3

*(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**.



Configure Authentication RADIUS Policy

Name: SAS_Cloud

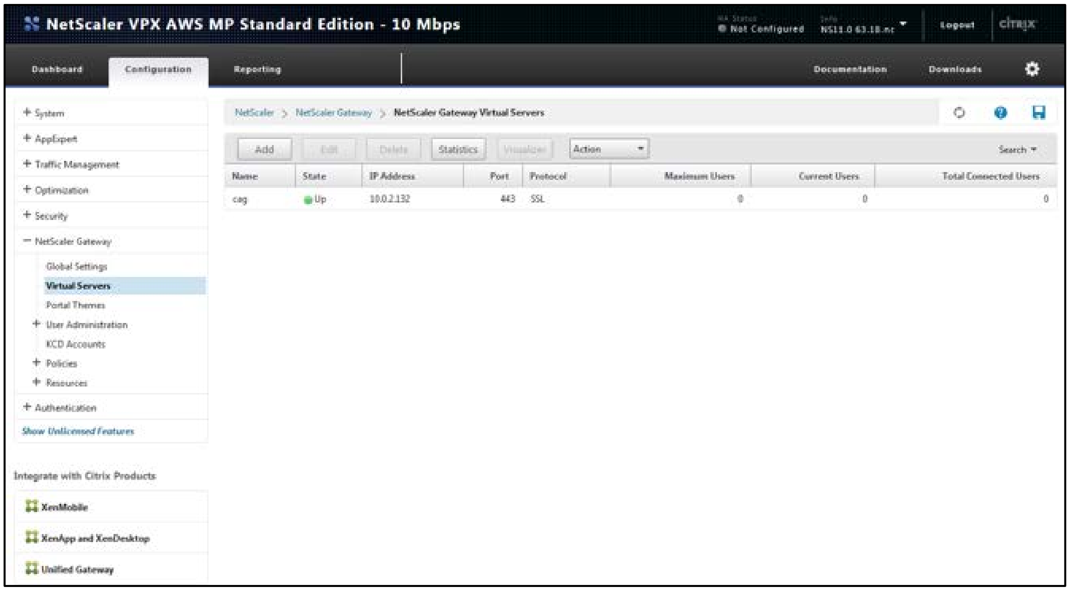
Server*: SAS

Expression*: ns_true

*(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**.

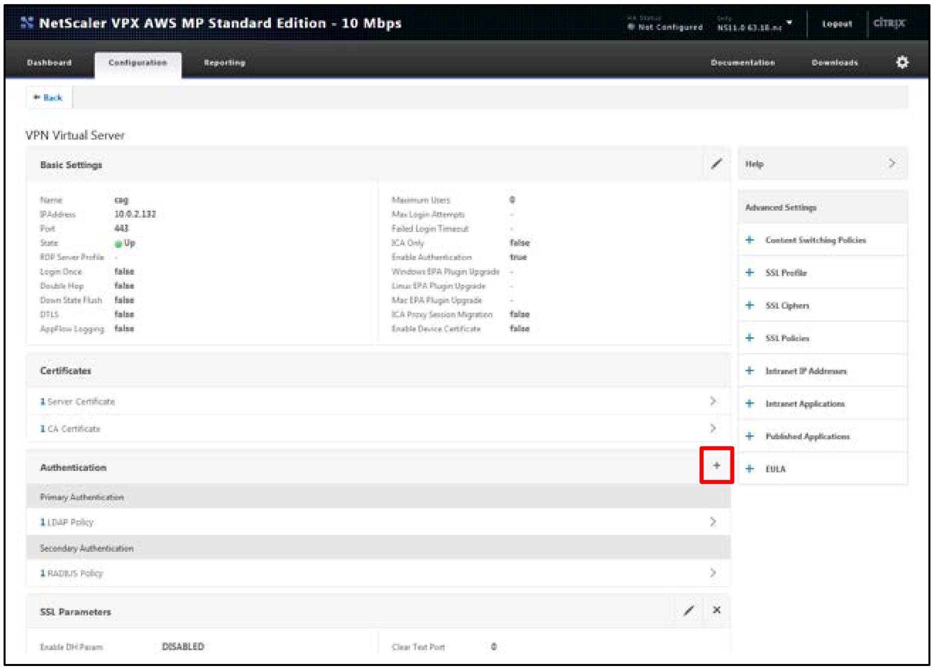


| Name | State | IP Address | Port | Protocol | Maximum Users | Current Users | Total Connected Users |
|---|---|---|---|---|---|---|---|
| cag | ● Up | 10.0.2.132 | 443 | SSL | 0 | 0 | 0 |

*(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.



VPN Virtual Server

Basic Settings

| | | | |
|---|---|---|---|
| Name | cag | Maximum Users | 0 |
| IPAddress | 10.0.2.132 | Max Login Attempts | - |
| Port | 443 | Failed Login Timeout | - |
| State | ● Up | ICA Only | false |
| RDP Server Profile | - | Enable Authentication | true |
| Login Once | false | Windows EPA Plugin Upgrade | - |
| Double Hop | false | Linux EPA Plugin Upgrade | - |
| Down State Flush | false | Mac EPA Plugin Upgrade | - |
| DTLS | false | ICA Proxy Session Migration | false |
| AppFlow Logging | false | Enable Device Certificate | false |

Certificates

1 Server Certificate

1 CA Certificate

Authentication

Primary Authentication

1 LDAP Policy

Secondary Authentication

1 RADIUS Policy

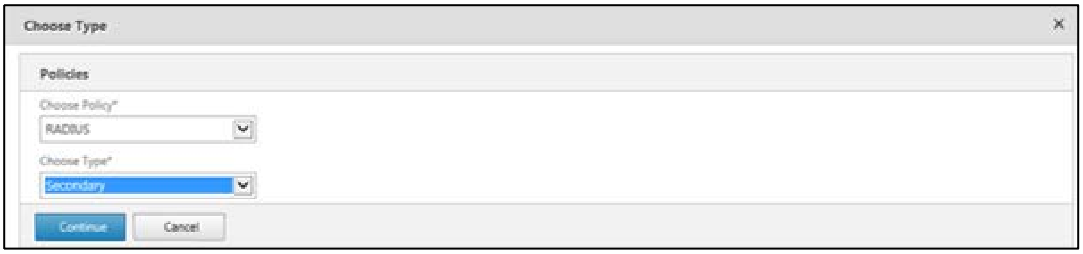
SSL Parameters

| | | | |
|---|---|---|---|
| Enable DH Param | DISABLED | Clear Text Port | 0 |

*(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**. |



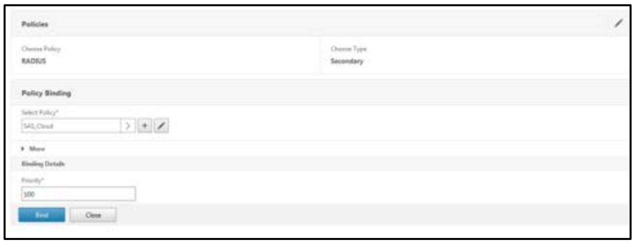
Policies

Choose Policy*: RADIUS

Choose Type*: 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**.



Policies

Choose Policy: RADIUS

Choose Type: Secondary

Policy Binding

Select Policy*: SAS_Cloud

Binding Details

Priority*: 100

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

10. Click **Done**.

# Modifying the Citrix NetScaler Gateway Login Window

Modify the **gateway_login_form_view.js** file to include the **SMS Token** and **Token Code** buttons to provide the following two authentication modes:

- MobilePASS authentication
- SMS Authentication

The **SMS Token** buttons is used to switch from MobilePASS authentication mode to SMS authentication mode, and the **Token Code** button is used to switch from the SMS authentication mode to MobilePASS authentication mode.

1. Connect to the NetScaler machine using an SSH client.
2. Back up the following file:
   **/netscaler/ns_gui/vpn/js/gateway_login_form_view.js**
3. Edit the **gateway_login_form_view.js** file.
4. Locate the line starting with:

   **var right_loginbutton**
5. Add the following after this line:
6. **var Sms = $("<input type='button'></input>").attr({'id':'SMS','value':'SMS token','class':'custombutton login_page'}).appendTo(right_loginbutton);**
7. Locate the line starting with:
   **var Login =**
8. Add the following after this line:

   ```
   Sms.click(function()
   {
       if (document.getElementById("Password2").style.display=="none") {
           document.getElementById("Password2").style.display="block";
           document.getElementById("passwd1").style.display="block";
           document.getElementById("passwd1").value="";
           document.getElementById("SMS").value="SMS token";
       } else {
           document.getElementById("Password2").style.display="none";
           document.getElementById("passwd1").style.display="none";
           document.getElementById("passwd1").value = 1;
           document.getElementById("SMS").value="Token code";
       }
   });
   ```
9. Save the file.
10. 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:

       **mkdir /var/customizations**

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

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

**NOTE**: You need to perform step 10, otherwise, a NetScaler reboot would replace the above changes to its default.

**NOTE:** You can download the modified **gateway_login_form_view.js** file from the following URL:

**https://gemalto.service-now.com/csm?id=kb_article&sys_id=024e7a174f42b288873b69d18110c7d7**

Refer to **KB ID: KB0015434**.

You need to rename the downloaded file (**gateway_login_form_view_sms.js**) to **gateway_login_form_view.js**

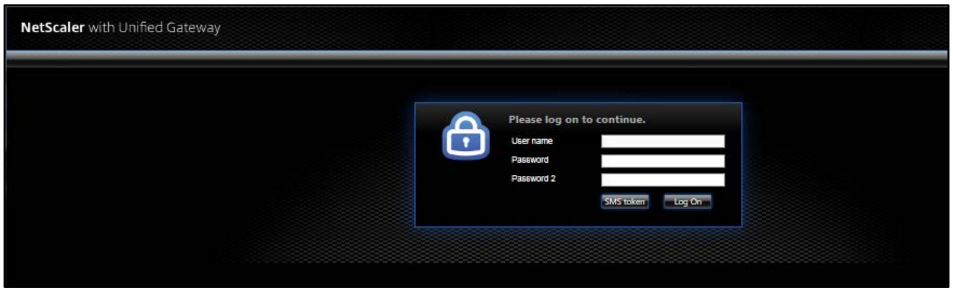
# Running the Solution

## MobilePASS Authentication Mode

1. In a web browser, open the NetScaler Gateway login window.

2. On the NetScaler Gateway login window, complete the following fields, and then click **Log On**.

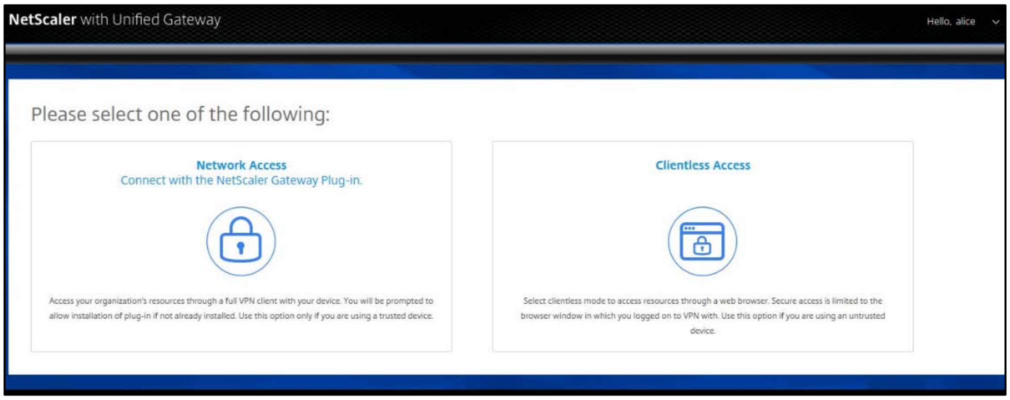
| | |
|---|---|
| **User name** | Enter your user name. |
| **Password** | Enter your AD password. |
| **Password2** | Enter the MobilePASS passcode. |



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

**NOTE:** The **SMS token** button is used to switch to the login window that is used for authentication using SMS.

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


NetScaler with Unified Gateway
Hello, alice
Please select one of the following:
Network Access
Connect with the NetScaler Gateway Plug-in.
Clientless Access

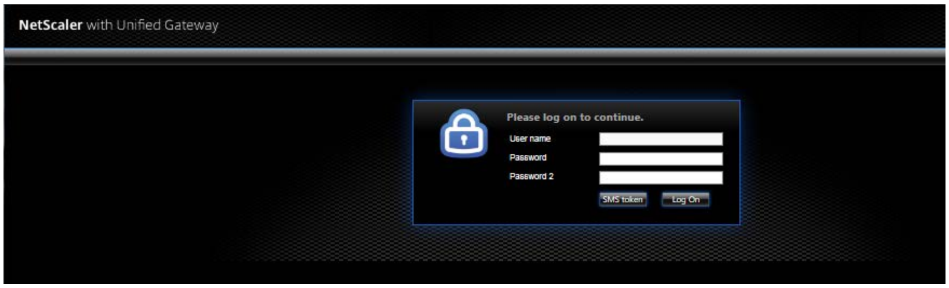
Access your organization's resources through a full VPN client with your device. You will be prompted to allow installation of plug-in if not already installed. Use this option only if you are using a trusted device.

Select clientless mode to access resources through a web browser. Secure access is limited to the browser window in which you logged on to VPN with. Use this option if you are using an untrusted device.

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

## SMS Authentication Mode

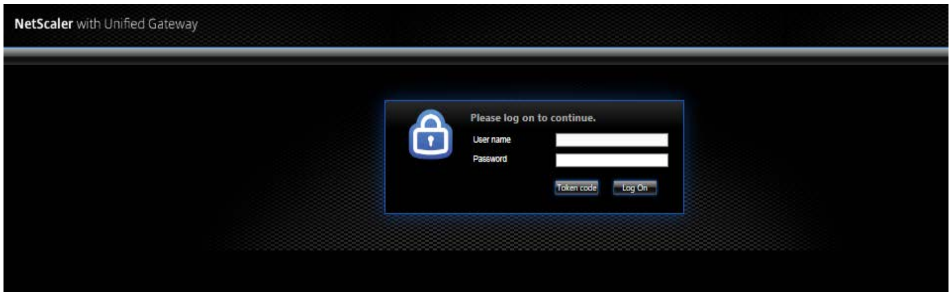
1. In a web browser, open the NetScaler Gateway login window.
2. On the NetScaler Gateway login window, click **SMS token**.



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

3. Complete the following fields, and then click **Log On**.

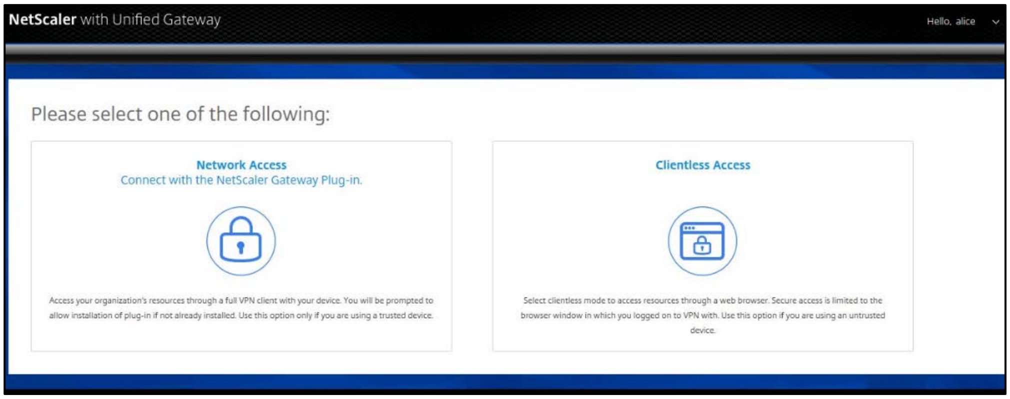
| | |
|---|---|
| **User name** | Enter your user name. |
| **Password** | Enter your AD password. |



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

**NOTE:** The **Token code** button is used to switch to the login window that is used for authentication using MobilePASS.

4. An SMS challenge notification is triggered on the mobile. Enter the passcode you received in the SMS challenge notification, and then click **Submit**.

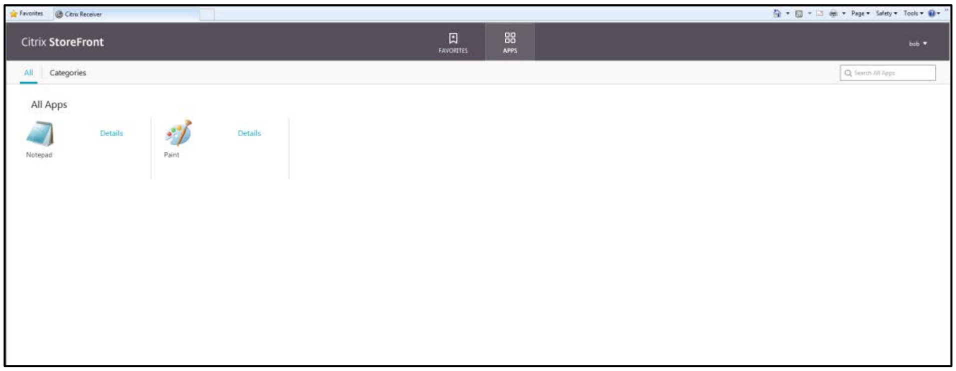

NetScaler with Unified Gateway
Hello, alice
Please select one of the following:
Network Access
Connect with the NetScaler Gateway Plug-in.
Clientless Access

Access your organization's resources through a full VPN client with your device. You will be prompted to allow installation of plug-in if not already installed. Use this option only if you are using a trusted device.

Select clientless mode to access resources through a web browser. Secure access is limited to the browser window in which you logged on to VPN with. Use this option if you are using an untrusted device.

*(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<br>4690 Millennium Drive<br>Belcamp, Maryland  21017 USA | |
| **Phone** | United States | 1-800-545-6608 |
| | International | 1-410-931-7520 |
| **Technical Support Customer Portal** | https://supportportal.gemalto.com<br>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. | |