SafeNet Authentication Service

Integration Guide

Using RADIUS Protocol for Citrix NetScaler Gateway 10

gemalto
security to be free

Document Part Number: 007-012651-001, Rev. B

Release Date: November 2015

Contents

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 10.

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 for managing access control and limiting 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 10 using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Citrix NetScaler Gateway 10 to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Citrix NetScaler Gateway 10 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Citrix NetScaler Gateway 10 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)**—only when using this version. For Cloud not necessary to fill in version number.
- **Citrix NetScaler Gateway 10**

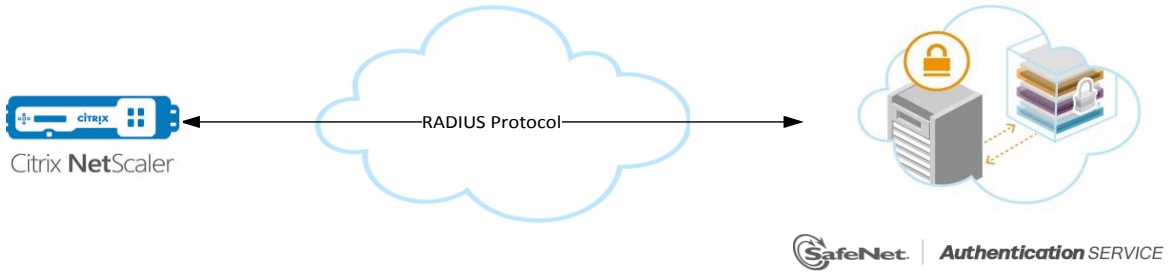
Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler Gateway 10, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

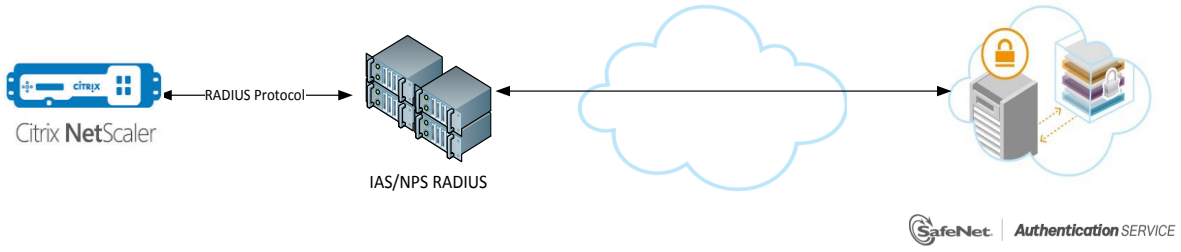
RADIUS-based Authentication using SAS Cloud

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.



- **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/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation Guide for Microsoft IAS, NPS.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 SAS-SPE and SAS-PCE

For both on-premises 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:

  http://www2.gemalto.com/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation Guide for Microsoft IAS, NPS.pdf

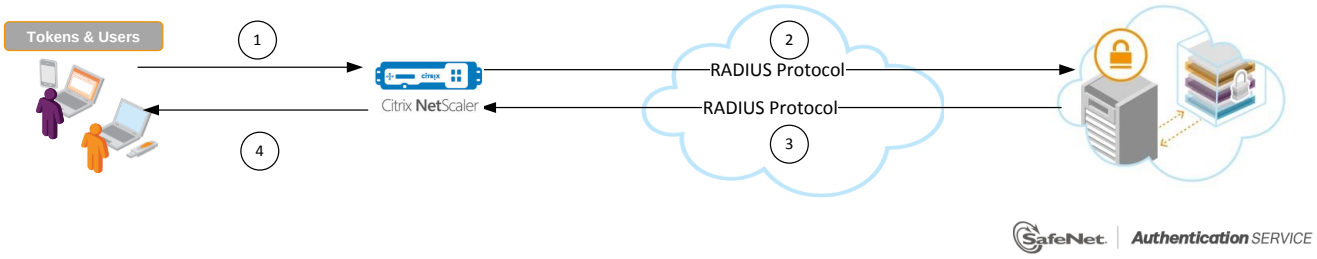
- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the 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 data flow of a multi-factor authentication transaction for Citrix NetScaler Gateway 10.



1. A user attempts to log on to Citrix NetScaler Gateway 10 using an OTP authenticator.
2. Citrix NetScaler Gateway 10 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 10.
4. The user is granted or denied access to the Citrix NetScaler Gateway 10 based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Citrix NetScaler Gateway 10, ensure the following:

- End users can authenticate from the Citrix NetScaler Gateway 10 environment with a static password before configuring the Citrix NetScaler Gateway 10 to use RADIUS authentication.
- Ports 1812/1813 are open to and from Citrix NetScaler Gateway 10.
- 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 SAS with Citrix NetScaler Gateway 10 using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Citrix NetScaler Gateway 10 as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Address, page 11

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*:

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 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 Gateway 10.

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.

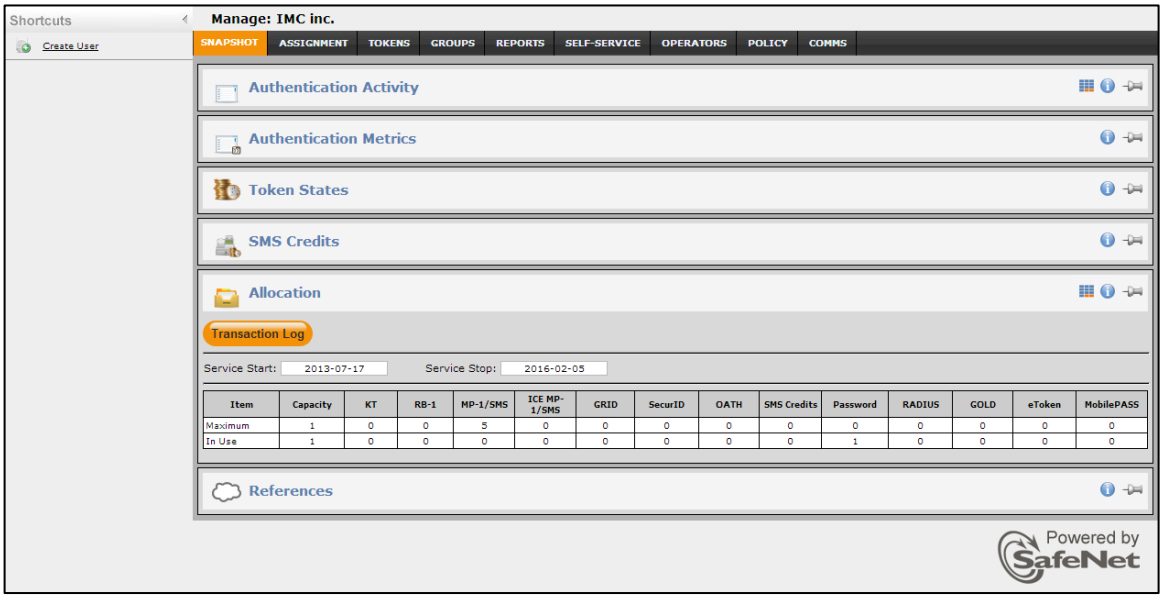
Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

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

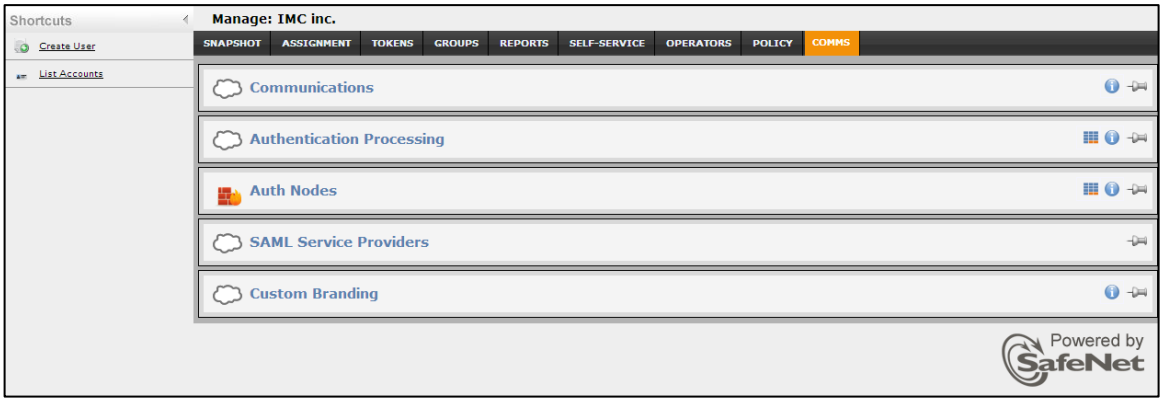
Adding Citrix NetScaler Gateway 10 as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Citrix NetScaler Gateway 10. You will need the IP address of Citrix NetScaler Gateway 10 and the shared secret to be used by both SAS and Citrix NetScaler Gateway 10.

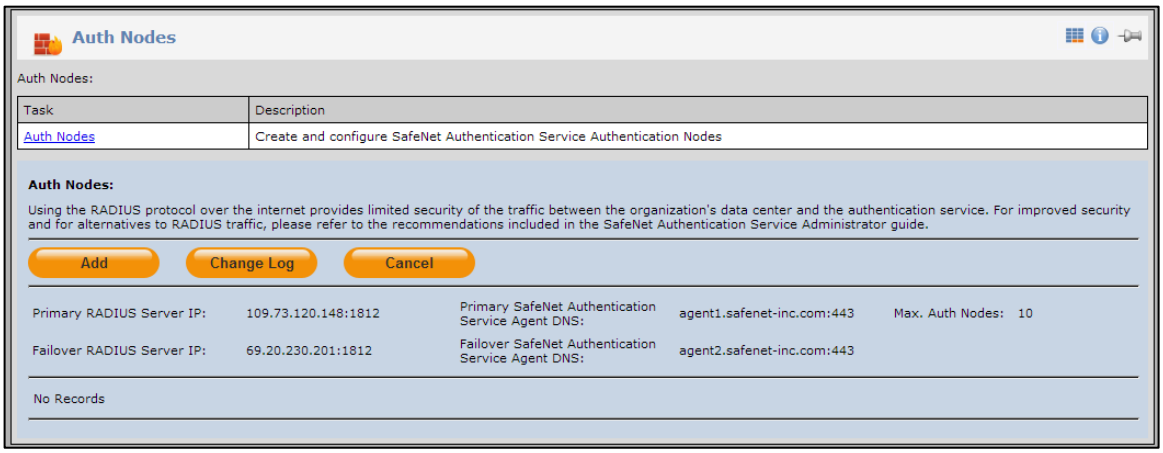
1. Log in to the SAS console with an Operator account.



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

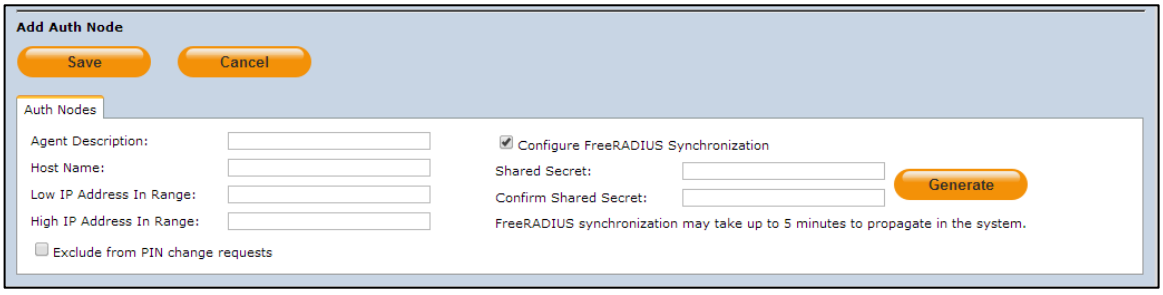


3. In the **Auth Nodes** module, click the **Auth Nodes** link.



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 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 entered above to confirm it.

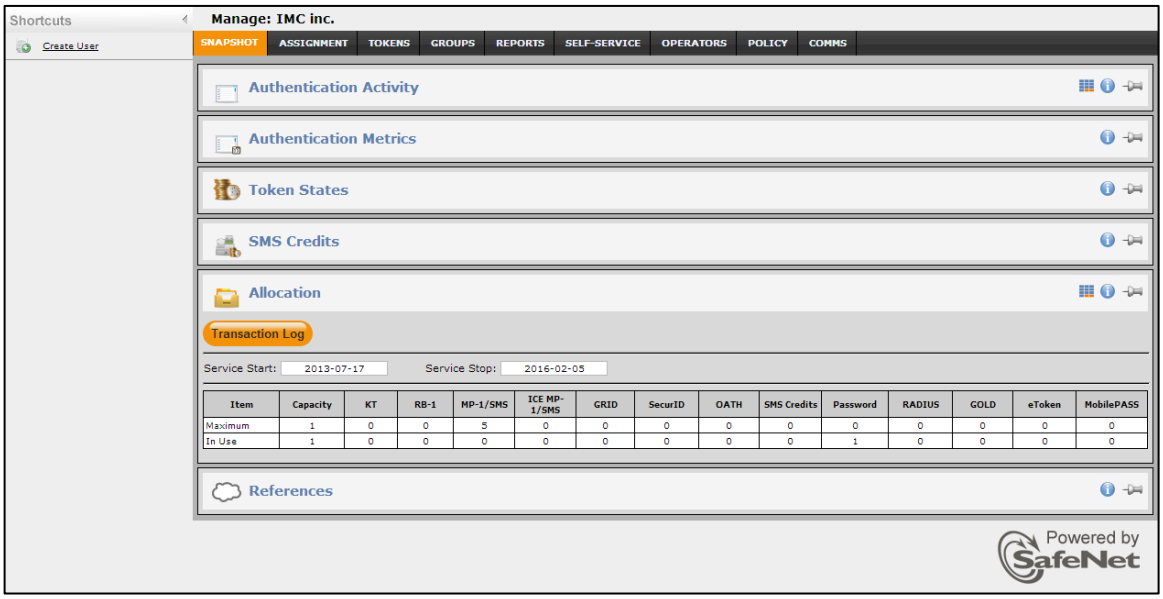


The authentication node is added to the system.

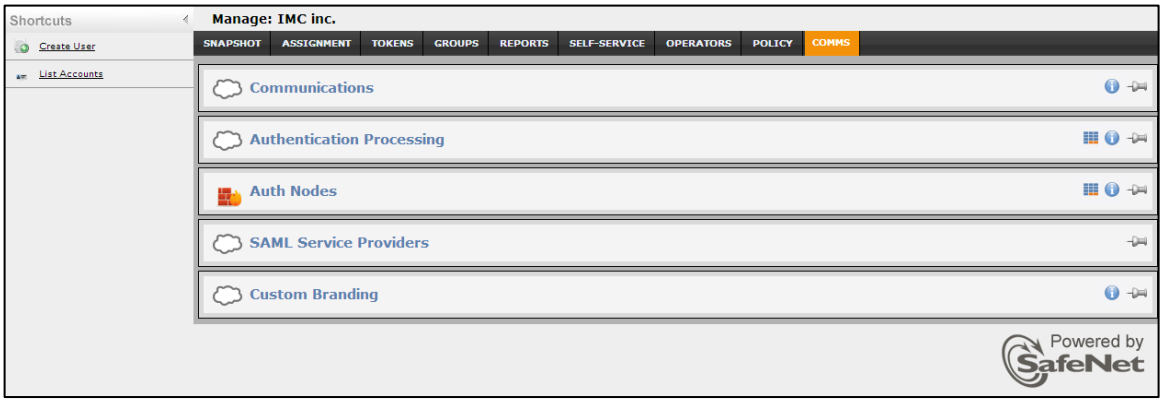
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Citrix NetScaler Gateway 10, check its IP address. The IP address will then be added to Citrix NetScaler Gateway 10 as a RADIUS server at a later stage.

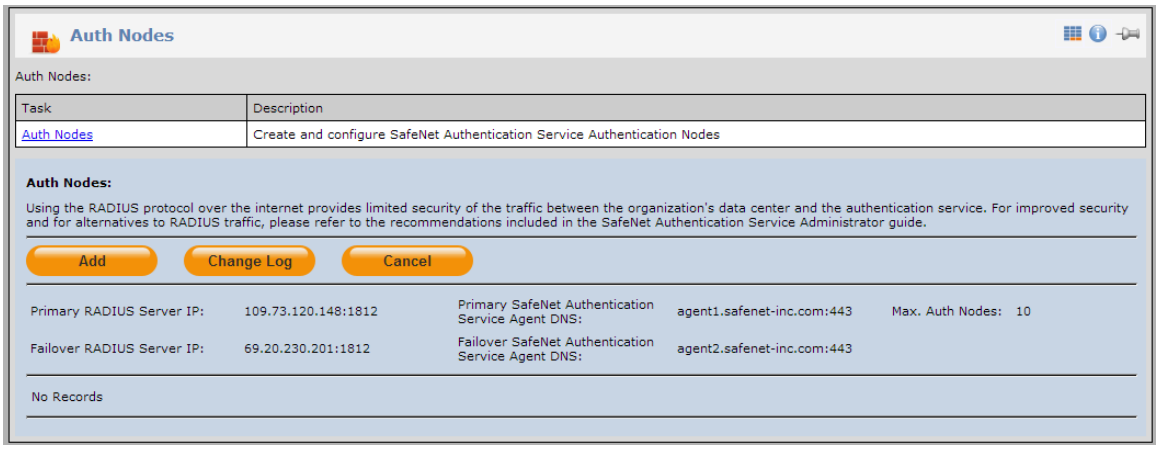
1. Log in to the SAS console with an Operator account.



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.

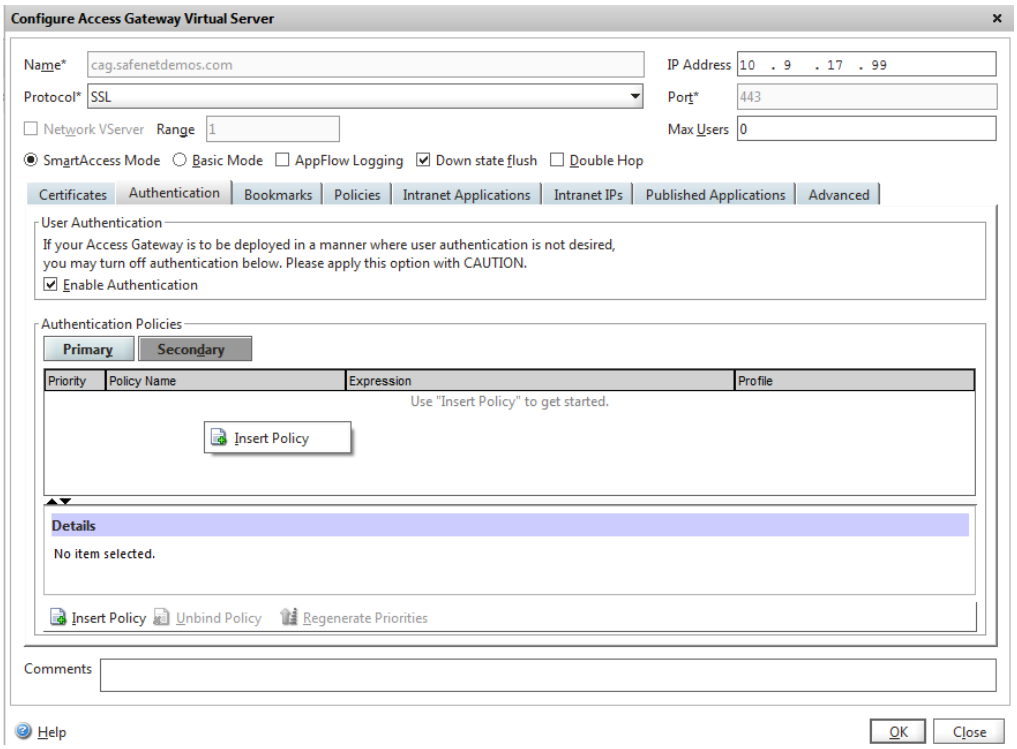


Configuring Citrix NetScaler Gateway 10

The next step is to configure the Citrix NetScaler Access Gateway 10 to use RADIUS protocol as a secondary authentication method.

Perform the following steps:

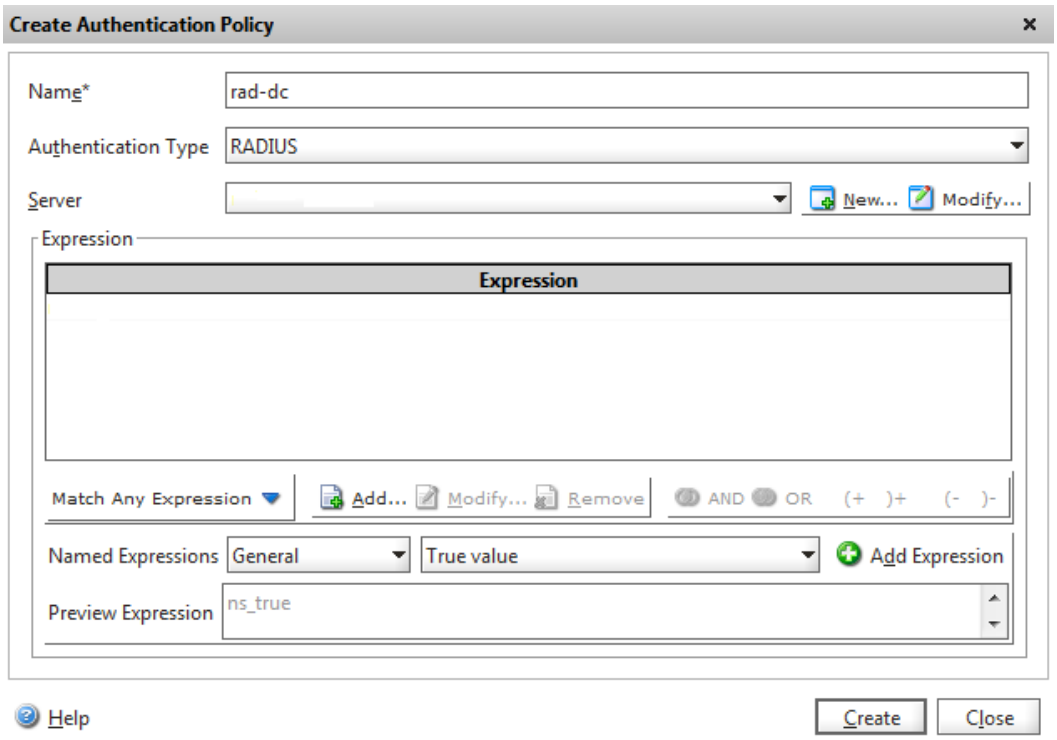
1. Log in to the Citrix **NetScaler** administrator console.
2. Navigate to **Access Gateway** → **Virtual Servers** in the left panel of the administrator console.
3. Select your existing Access Gateway Virtual Server, and then click **Open**.
4. In the **Configure Access Gateway Virtual Server** dialog, select the **Authentication** tab from your existing LDAP policy for Microsoft Domain authentication.
5. Select the **Secondary** tab under authentication policies. Create the RADIUS server authentication policy and update the RADIUS server details.



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

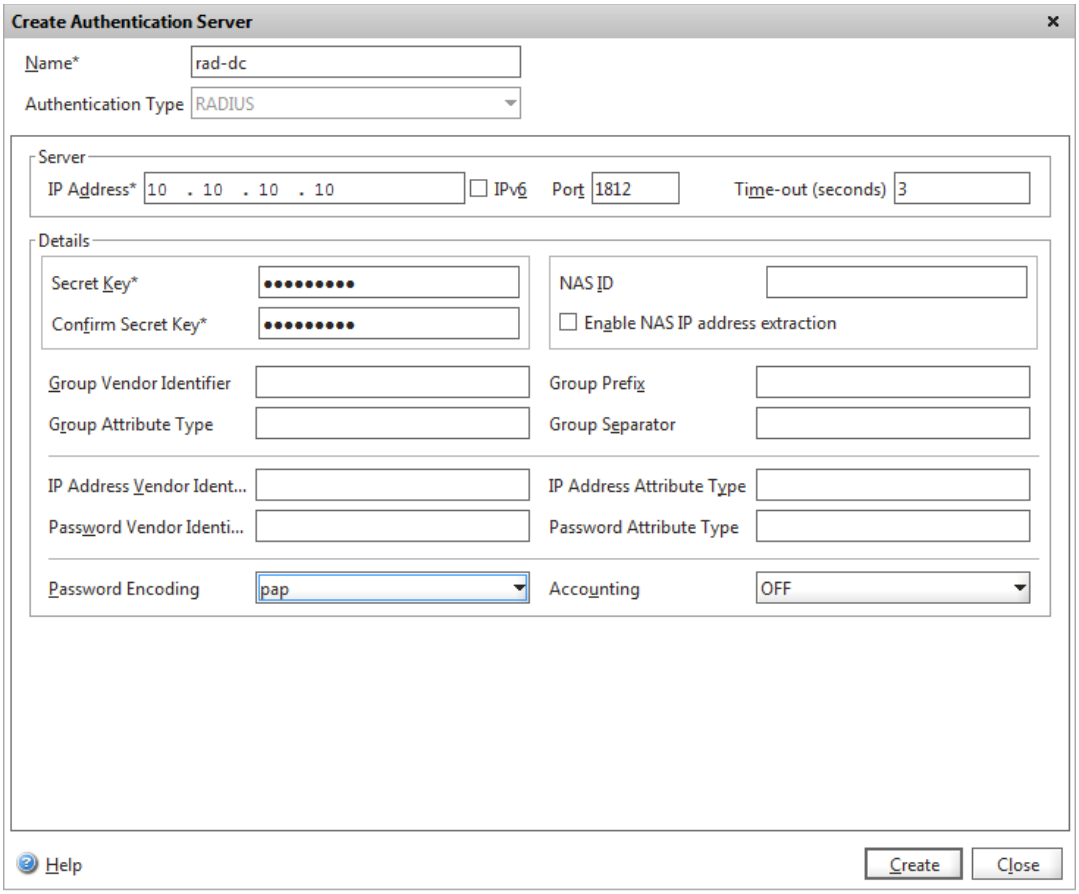
6. On the **Policies** tab, Select **Insert Policy**.

   The **Create Authentication Policy** window opens



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

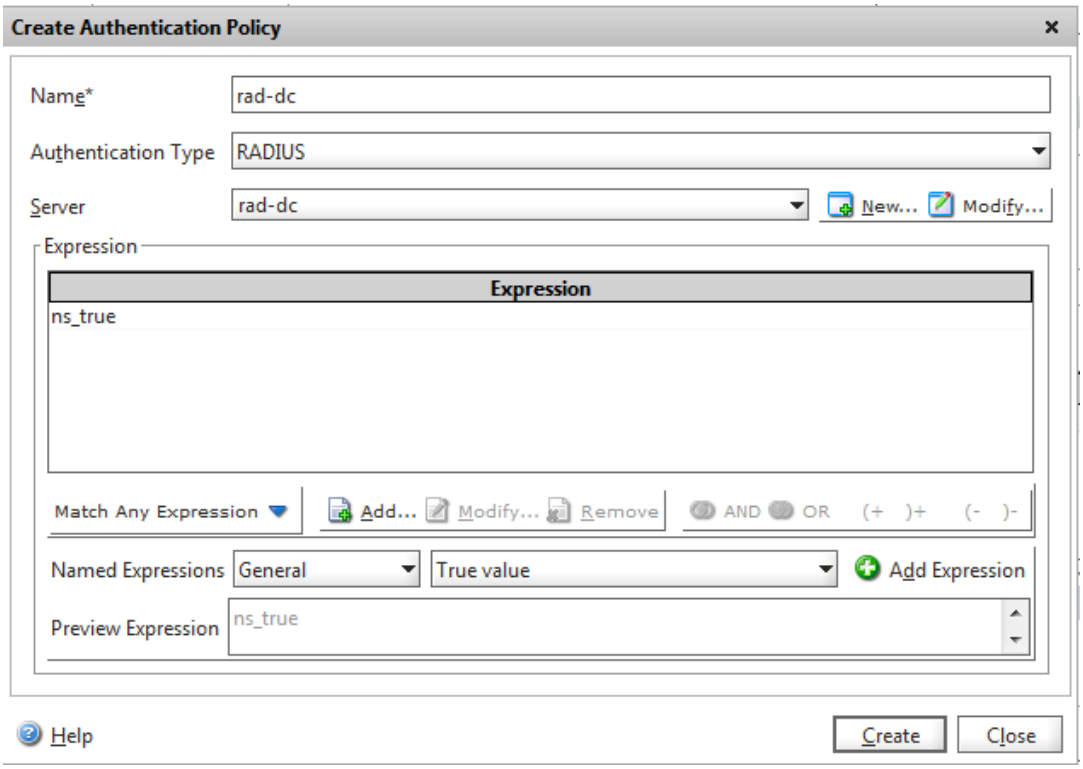
7. In **Name**, type a name for the policy.
8. In **Authentication Type**, select **RADIUS**.
9. Next to **Server**, click **New**.
10. The Create Authentication Server window opens:



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

11. In **Name**, type a name for the server.
12. Under **Server**, in **IP Address**, type the IP address of the RADIUS server.
13. In **Port**, type the port. The default is 1812.
14. Under **Details**, in **Secret Key** and **Confirm Secret Key**, type the RADIUS server secret.
15. In the **Password Encoding**, select **PAP**.
16. Click **Create**.

    The **Create Authentication Policy** window opens:



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

17. In the **Create Authentication Policy** window, next to **Named Expressions**, select the **True Value** expression, click **Add Expression**, and click **Create**.
18. Click **Close**.

Authenticating using GrID Tokens

The following sections include a short description of the GrID authentication method that can be used with Citrix Netscaler and its special configuration parameters.

This flexible method allows an end-user to generate a one-time password without the requirement for hardware tokens or software applications. GrID works by presenting the end-user with a matrix of cells during enrollment containing random characters, from which they select a personal identification pattern (PIP). Thereafter, whenever the end-user wishes to authenticate to a SafeNet Authentication Service protected resource, the user is presented with a challenge grid containing random characters.

The user then enters the characters in the cells that correspond to their PIP; no hardware to lose and far superior to static passwords. Every time the challenge grid appears, the characters in the cells are different, so the user is always entering a one-time passcode.

To use GrID authentication with Citrix NetScaler Access Gateway, you will need to replace the existing index.html file (located in /netscaler/ns_gui/vpn) on the Citrix Netscaler Access Gateway.
Click here to download the package with the updated index.html file.

After copying the file, edit it and look for the line:
var BlackShieldServerLocation = ("http://10.9.17.15/blackshieldss/O/FFW0NAWS75/index.aspx");

Change the url to the SAS GrIDsure URL.

(i.e. **https://grid.safenet-inc.com/blackshieldss/O/1MAGXLUGLK/index.aspx?getChallengeImage=true&userName=**)

Running the Solution

To authenticate using a GrID token:

1. Log in to the VPX virtual server via the web browser
2. Enter the username and user domain password in the **Windows Password** field and click **Get Grid**.

The GrID window appears.

3. Enter the Grid combination in the **Grid Token** text box and then click **Log On**.

You have logged on to the Citrix application.

Authenticating Using SMS 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 the Netscaler.

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

1. Connect to the VPX server console by ssh/direct

2. Backup the following file: /netscaler/ns_gui/vpn/login.js

3. Edit the file login.js.

4. Locate the following section:

if (pwc == 2) {

document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;"><SPAN class=CTXMSAM_LogonFont>' + _("Password2") + '</SPAN></TD> <TD colspan=2 style="padding-right:8px;"><input class=CTXMSAM_ContentFont type="Password" title="' + _("Enter password") + '" name="passwd1" size="30" maxlength="127" style="width:100%;"></TD></TR>');

5. Add the highlighted values in bold:

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> <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 commands 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 file /nsconfig/rc.netscaler does not exist, execute the following command to create it:

touch /nsconfig/rc.netscaler

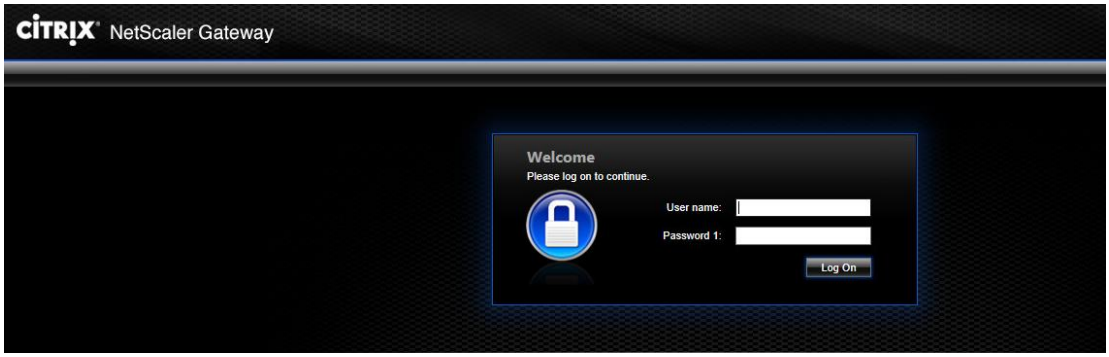
d. Run the following commands to add an entry for each command to the rc.netscaler file:

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*

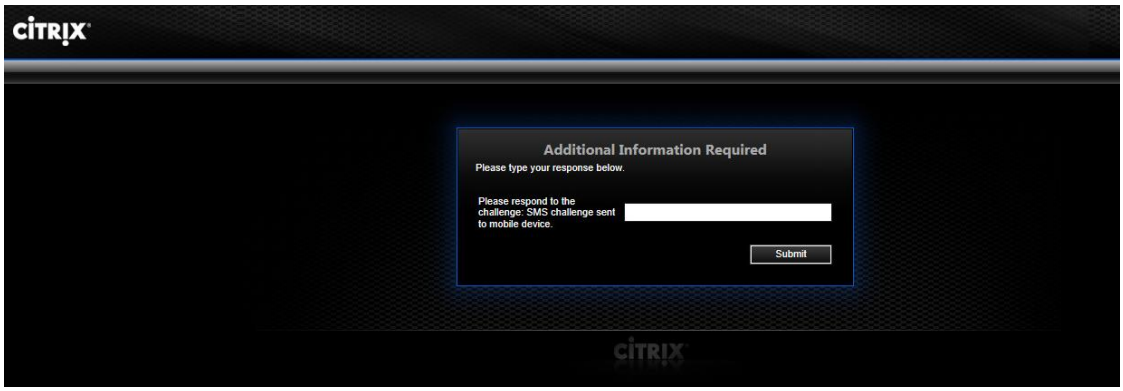
Running the Solution using SMS OOB

To authenticate using SMS OOB:

1. Login to the VPX virtual server via the web browser.



2. Enter the username and user domain password in the Password 1 text box and click Log On. An SMS is triggered and the Additional Information Required screen is displayed.



3. Enter the passcode retrieved by SMS and click Log On.

You have logged on to the Citrix Application.

Running the Solution using MobilePass token

To authenticate using MobilePASS token:

1. Log in the VPX virtual server via the web browser.

2. Enter the username and user Windows Password. In the **SafeNet Passcode** field, enter the OTP passcode.
3. Click **Log On**.

You have logged on to the Citrix application.

Customizing Citrix NetScaler Logon Page

When Multi-Factor Authentication is configured on 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. Backup 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).

```
<Property id="Enter user name" property="title">Enter user name</Property>
<String id="Password">Password</String>
<String id="Password2">Password 2:</String>
<String id="Enter password">Enter password</String>
```

7. Save the xml file.
8. Go to **/netscaler/ns_gui/vpn**.
9. Backup the file **login.js**.
10. Open the **login.js** file using a text editor.
11. Search for the following line:
    if (pwc == 2) { document.write(' 1'); }
12. Delete the **1** character and save the **js** file.
13. The modifications result in the labels **Password 1** and **Password 2** being changed to **Windows Password** and **SafeNet Password** respectively.

    Before:

After:

Citrix Netscaler with SMS and MobilePass Solution

In this section we will describe how to configure Citrix Netscaler login page to support both SMS token and MobilePass token.

For example:

"*User John logs onto the NetScaler with his MobilePASS token and fills in Username, Password token code and login successfully. Now user Sara wants to login using a SMS token (because she has no smartphone) and she complaints see needs fill in her Username, Password and token field empty to receive an SMS the first time and then she has to fill in her Username and Password again with the SMS OTP.*"

In order to configure the Netscaler for SMS token and MobilePass please use this document.

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, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.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.	