SafeNet Authentication Service

Push OTP Integration Guide

Using RADIUS Protocol for Citrix NetScaler Gateway 10.5

gemalto
security to be free

Document Part Number: 007-013348-001, Rev. C

Release Date: October 2016

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.

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 (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

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

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 Push one-time password (OTP) solution 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 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's 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) Cloud**—Version 3.5
- **Citrix NetScaler Gateway**—Version 10.5

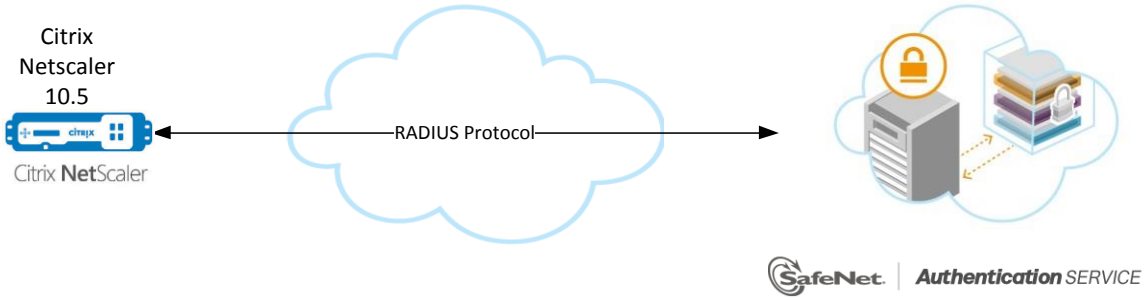
Audience

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 (SAS).

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides the following RADIUS topology that supports Push OTP tokens:

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.

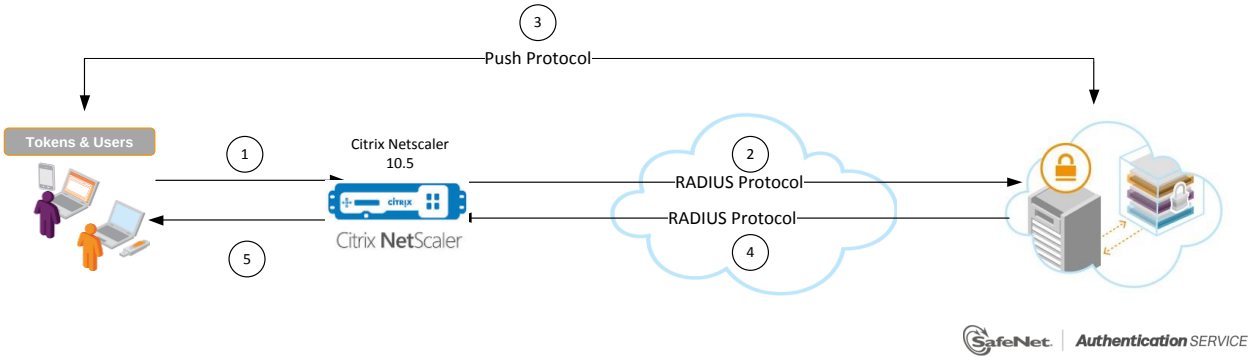


This document demonstrates the solution using the SAS cloud hosted RADIUS service.

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



1. A user attempts to log on to Citrix NetScaler Gateway using a Push OTP authenticator.
2. Citrix NetScaler Gateway sends a RADIUS request with the user's credentials to SafeNet Authentication Service (SAS) 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 that 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 Gateway.
5. The user is granted or denied access to Citrix NetScaler Gateway based on the OTP 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.
- On the client machine, set the RADIUS timeout value at least 60 seconds.

Push OTP Prerequisites

In order to use SafeNet Authentication Service (SAS) Push OTP you will need:

- **SafeNet Authentication Service configured to enable Push OTP**
- **MobilePASS+ application**

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

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*:

https://safenet.gemalto.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 MobilePASS+ authenticator is supported.

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.

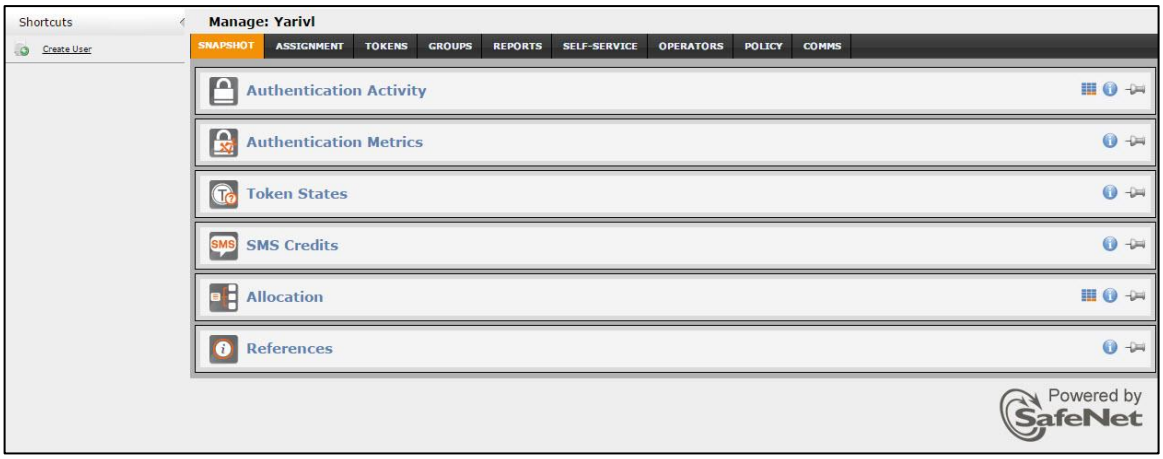
Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/

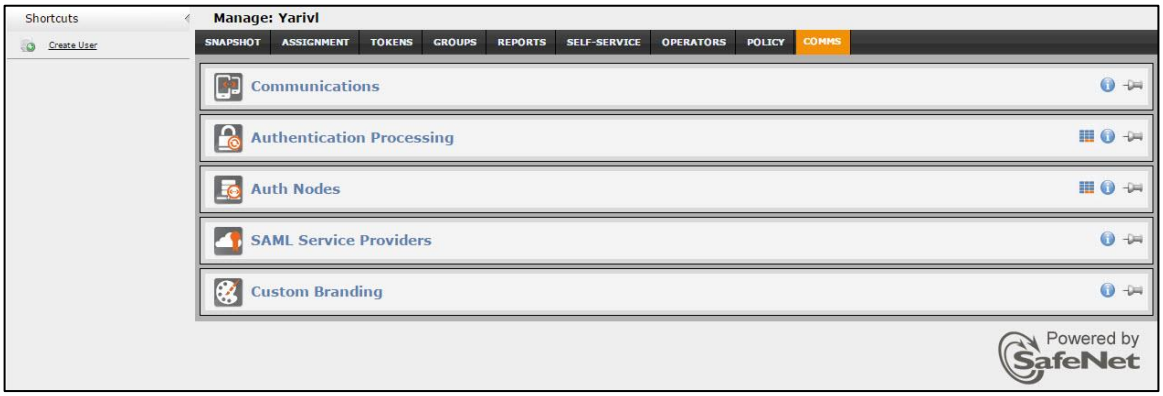
Adding Citrix NetScaler Gateway as an Authentication Node in SafeNet Authentication Service

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.



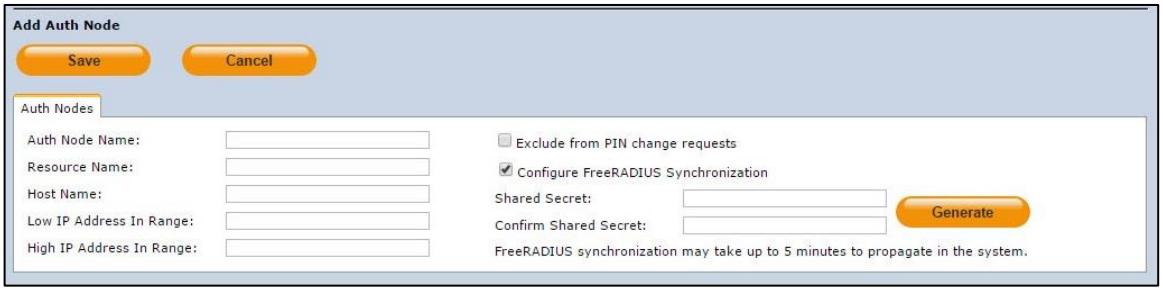
2. Click the **COMMS** tab, and then click **Auth Nodes**.



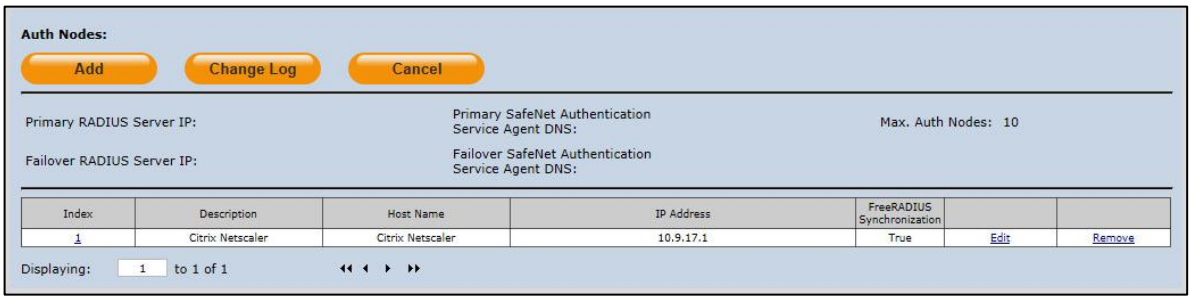
3. In the **Auth Nodes** module, click the **Auth Nodes** link, and then click **Add**.

4. Under **Add Auth Nodes**, 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.
High IP Address In Range	Enter the highest IP address in a range of IP addresses 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.



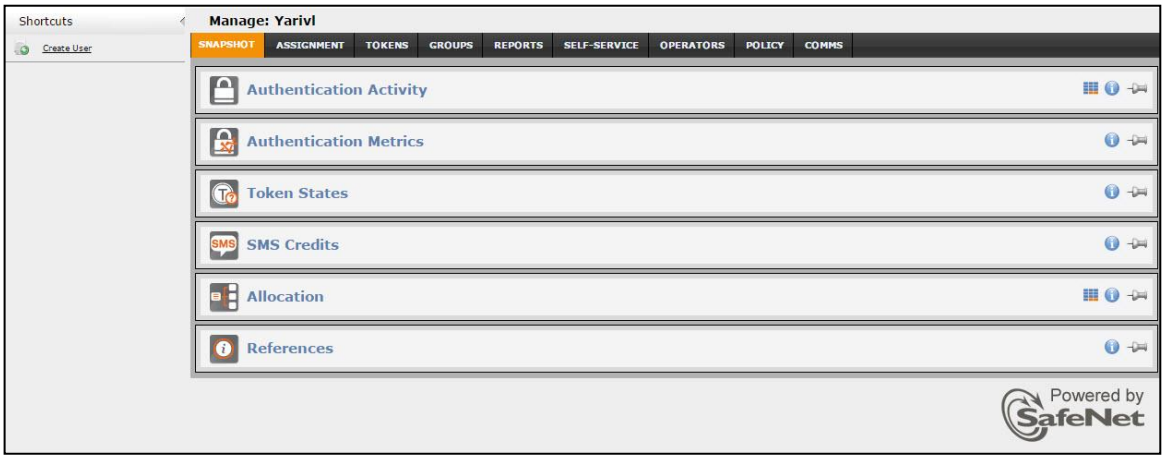
The authentication node is added to the system.



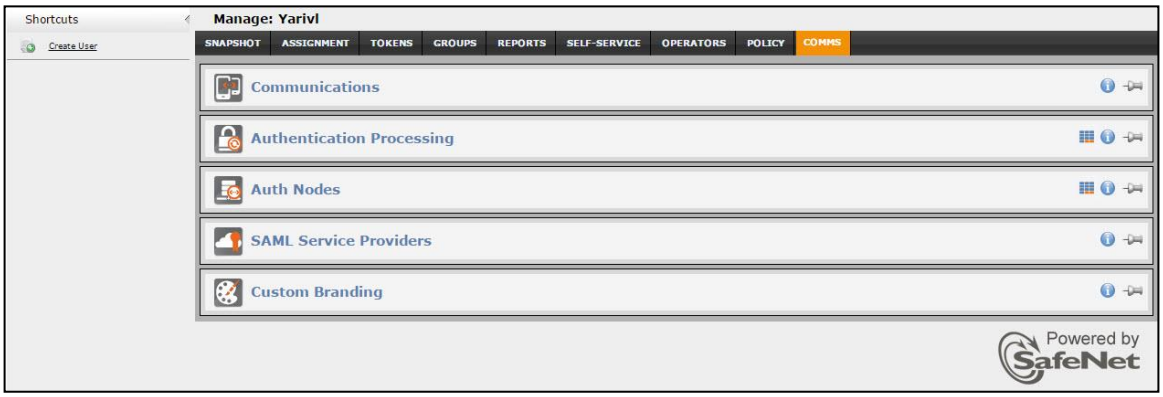
Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Citrix NetScaler Gateway, check its IP address. The IP address will be added to Citrix NetScaler 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 click **Auth Nodes**.

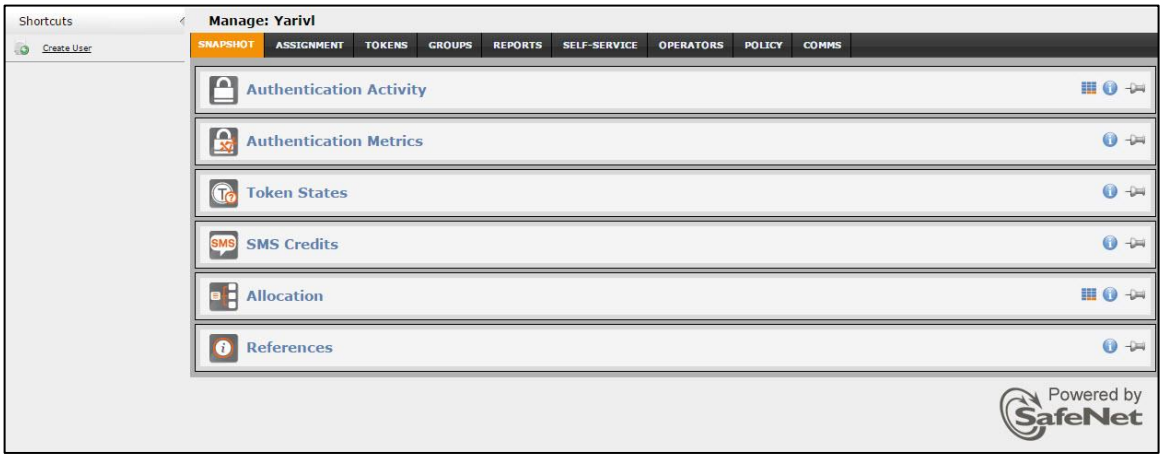


3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

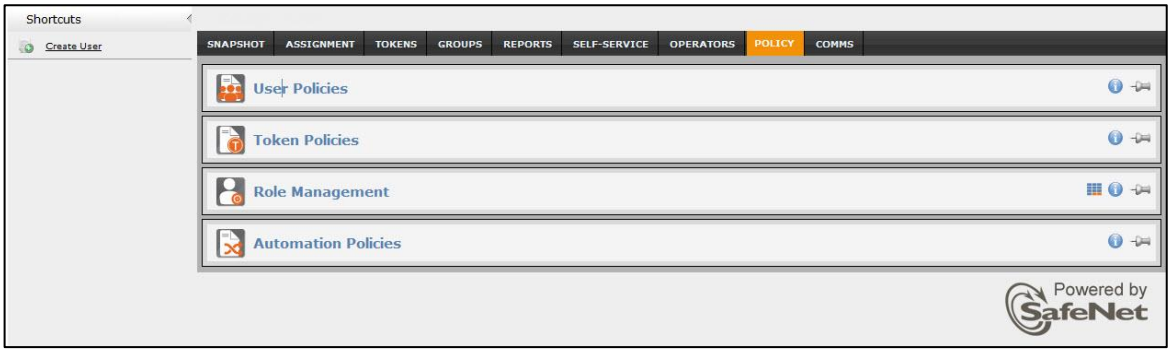
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the Software Token Push OTP setting must be enabled in the SafeNet Authentication Service (SAS) token policy.

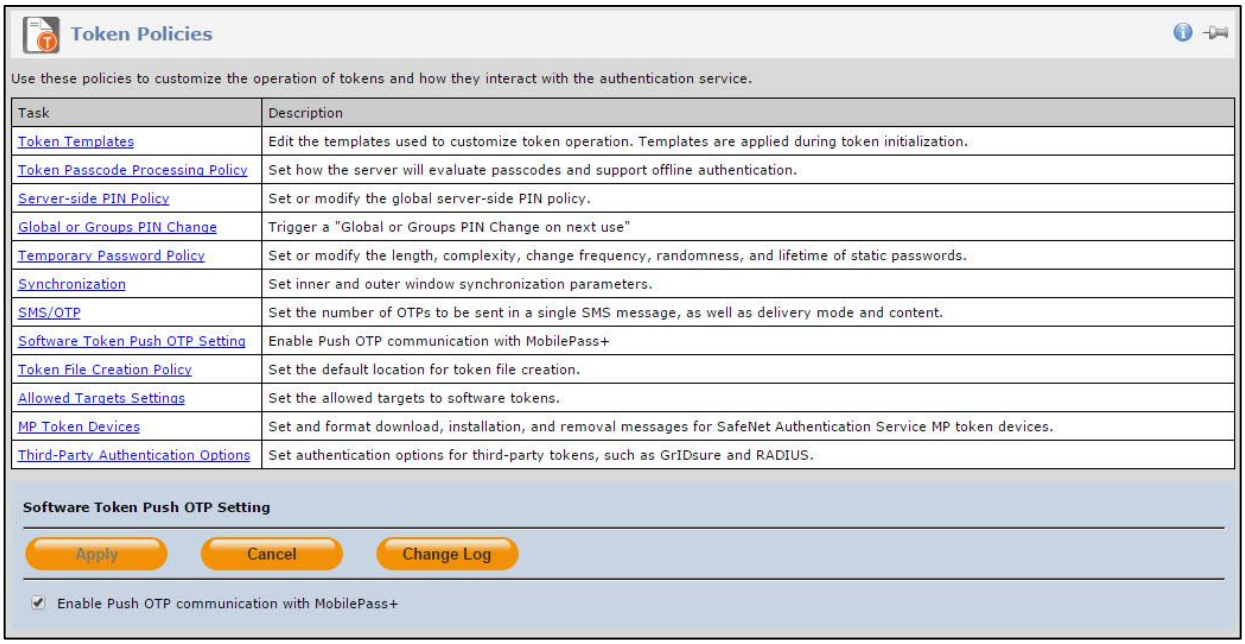
1. Log in to the SAS console with an Operator account.



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



3. In the Token Policies module, click the Software Token Push OTP Setting link.



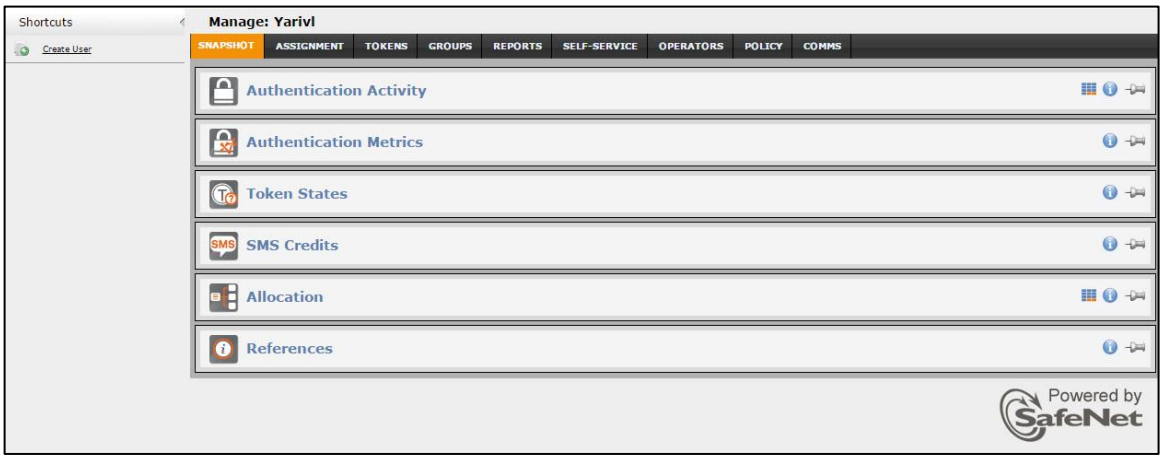
4. Select Enable Push OTP communication with MobilePass+ , and then click Apply.

Enabling the Allowed Targets Policy

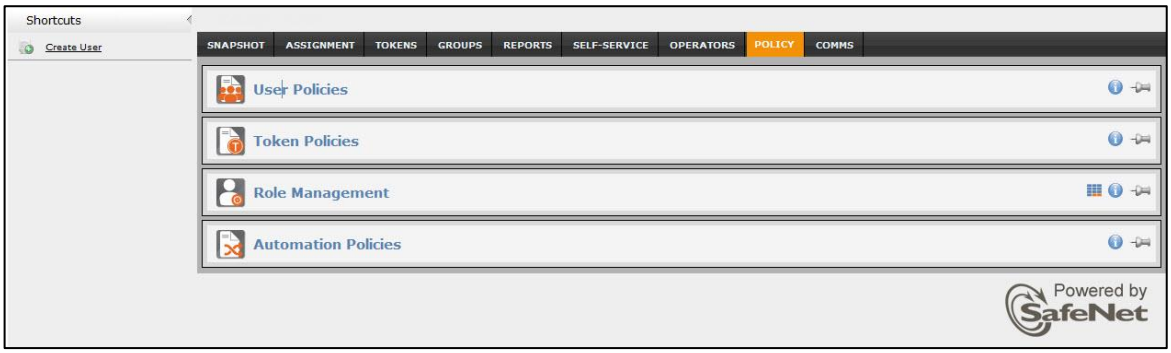
For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

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.

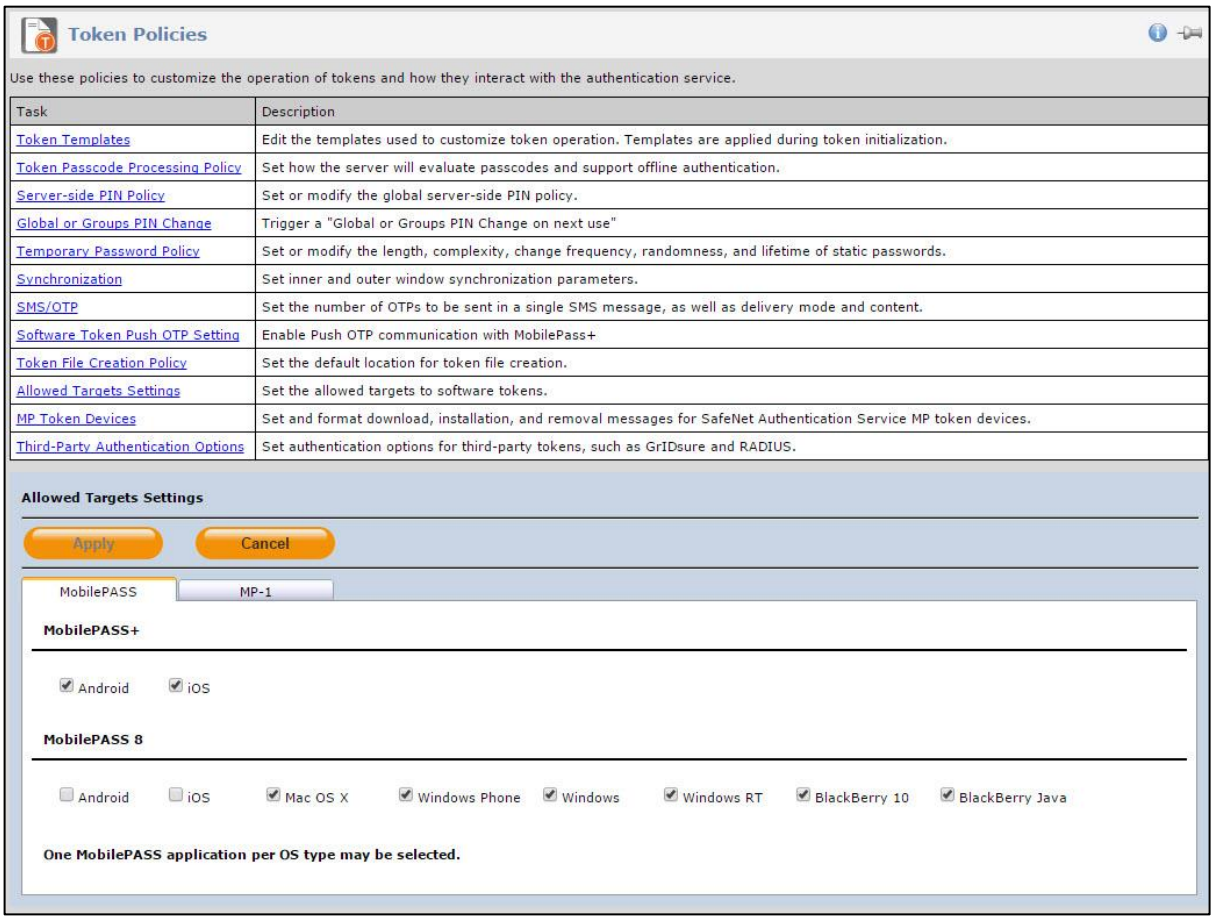
1. Log in to the SafeNet Authentication Service (SAS) console with an Operator account.



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



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



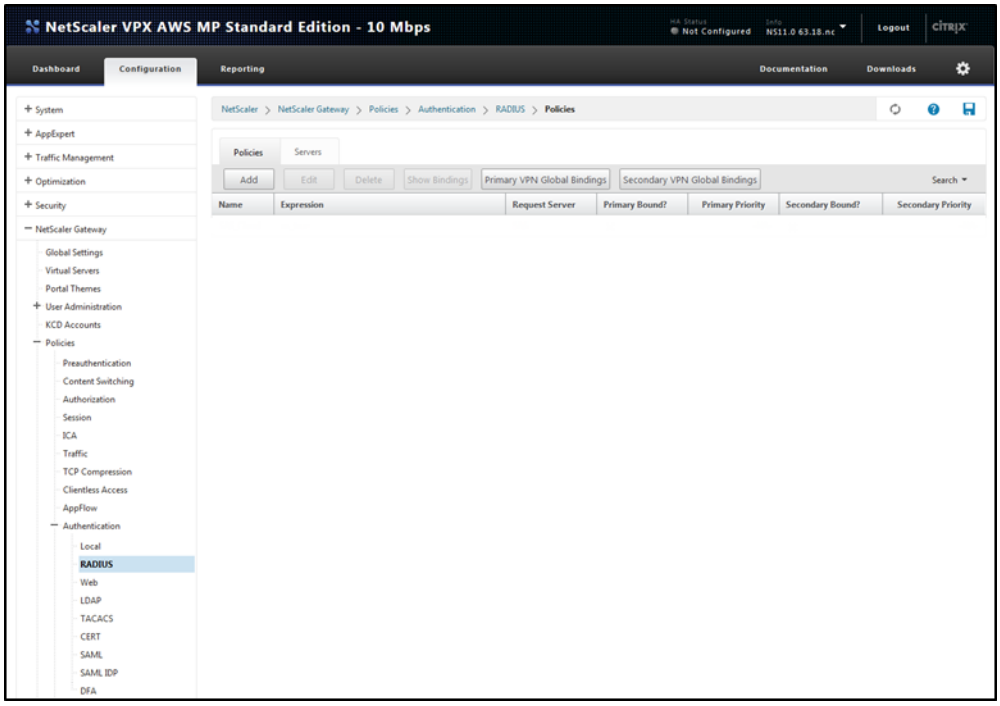
4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.

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, on the **Policies** tab, click **Add**.
4. On the **Create Authentication RADIUS Policy** window, 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.)

5. In the **Server** field, click the + icon.

6. 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.

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

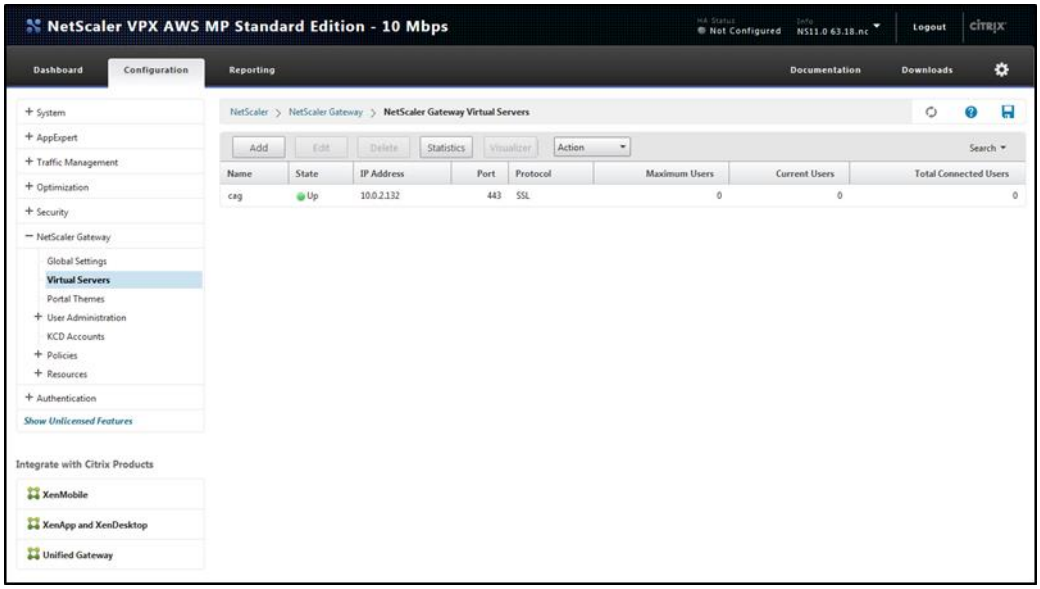
7. On the **Configure Authentication RADIUS Policy** window, under **Expression**, click **Saved Policy Expressions**, and then select **ns_true**.

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

8. Click **OK**.

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

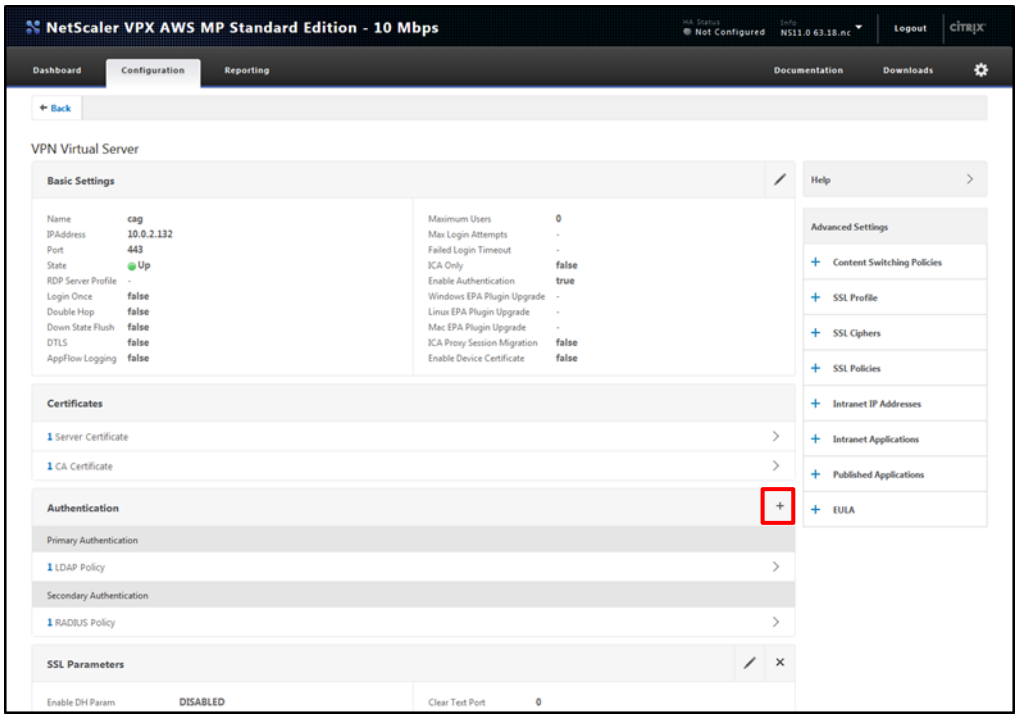
9. On the **Configuration** tab, in the left pane, click **NetScaler Gateway** > **Virtual Servers**.



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

10. In the right pane, select the gateway you created (for example, **cag**), and then click **Edit**.

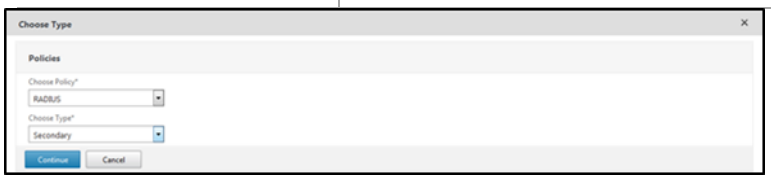
11. Under **Authentication**, click the + icon.



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

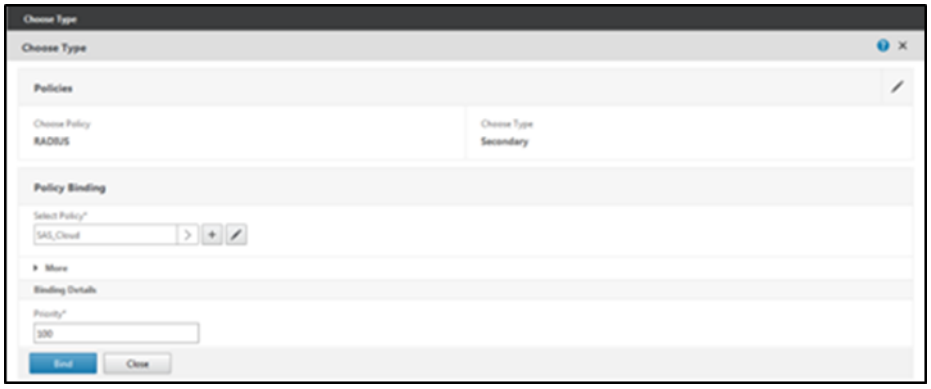
12. On the **Choose Type** window, under **Policies**, complete the following fields, and then click **Continue**.

Choose Policy	Select **RADIUS**.
Choose Type	Select **Secondary**.



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

13. 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.)

14. Click **Done**.

Modifying the Citrix NetScaler Access Gateway Login Window (Hybrid Mode)

Modify the Citrix NetScaler Access Gateway login window to support the hybrid mode.

1. Connect to the NetScaler machine using an SSH client.
2. Back up the **/netscaler/ns_gui/vpn/login.js** file.
3. Edit the **login.js** file.
4. In the file, locate the **function ns_check()** function, and then add the following code before return true;

```
// alert on password 2 wrong length
var obj = document.getElementById('passwd1');
var showPW2 = document.getElementsByName("rdoDoPass2")[1].checked;
 if ( (obj.value.length < 4) && (showPW2) )
 {
  alert("Please enter a valid OTP");
  return false;
 }

// eveything is good, show loading image

document.getElementById("divloading").style.left = ( screenLeft / 2 )*(-1);

document.getElementById("divloading").style.display = "block";
```

5. After the **function clean_name_cookie()** function, add the following function:

```
function showPassword2(show)
{
 if (show)
 {
  document.getElementById("passwd1").value="";
  document.getElementById("trDoPass2").style.display = "table-row";
 }
 else
 {
  document.getElementById("trDoPass2").style.display = "none";
  document.getElementById("passwd1").value="P";
 }
}
```

6. Delete the **function ns_showpwd_default()** function, and then add the following function:

```
function ns_showpwd_default()
{
    var pwc = ns_getcookie("pwcount");
    document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;"><SPAN class=CTXMSAM_LogonFont>' + _("Password"));
    if ( pwc == 2 ) { document.write(' '); }
    document.write(':</SPAN></TD>');
    document.write('<TD colspan=2 style="padding-right:8px;"><input class=CTXMSAM_ContentFont type="Password" title="' + _("Enter password") + '" name="passwd" size="30" maxlength="127" style="width:206;"></TD></TR>');
    if ( pwc == 2 ) {
  // checkboxs for password 2
    document.write('<TR><TD></TD><TD colspan=2><NOBR><input type="radio" name="rdoDoPass2" id="rdoDoPass2"  onClick="showPassword2(false);" checked> Use my mobile to autosend a passcode</input></NOBR></TD></TR><TR><TD></TD><TD><NOBR><input type="radio" name="rdoDoPass2" id="rdoDoPass2" onClick="showPassword2(true);">Enter a passcode manually</input></NOBR></TD></TR>');
    document.write('<TR id="trDoPass2" 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="Password" title="' + _("Enter password") + '" id="passwd1" name="passwd1" size="30" maxlength="127" style="width:206;" value="P"></TD></TR>');
    }

  // round spinning circle for loading
  document.write('<div align="center" id="divloading" style="position: absolute; left: 600px; top: 200px; z-index: 1; display: none; border: solid black 3px; width: 280px; border-radius: 15px;
```

**background-color: white;"> A login request from GEMALTO has been sent.

Please check your mobile device.

<img style="width: 50px;" src="images/loading.gif">

<input type="button" value="Cancel" onclick="document.location.reload(true);">

 ');**

UnsetCookie("pwcount");

}

7. Save the file.
8. Open the **/netscaler/ns_gui/vpn/resources/en.xml** file.
9. In the file, locate the **<String id="Password2">Password 2:</String>** line, and then change it to the following:

   <String id="Password2">Additional password</String>
10. **Save** the file.
11. Copy the **loading.gif** file (the file can be downloaded from the http://bel1web002.sfnt.local:9876/Files/2815c4db548d47c1a37a65ad086c078c link) to the **/netscaler/ns_gui/vpn/images/** folder.
12. 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 files:

       mkdir /var/customization

    b. Copy the modified files (**login.js** and **en.xml**) to the **customizations** directory.

    c. Edit the following file:
       /flash/nsconfig/rc.netscaler

    d. Add the following:
       cp /var/login.js /netscaler/ns_gui/vpn/
       cp /var/en.xml /netscaler/ns_gui/vpn/resources

    e. Save the file.

Running the Solution

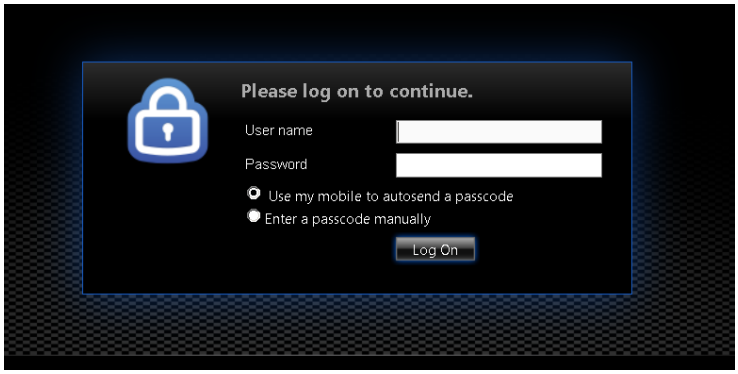
In this scenario, the hybrid mode login window is used, and you can choose any of the following options for authentication:

- Use my mobile to autosend a passcode
- Enter a passcode manually

Using the Registered Mobile to Auto Send a Passcode

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

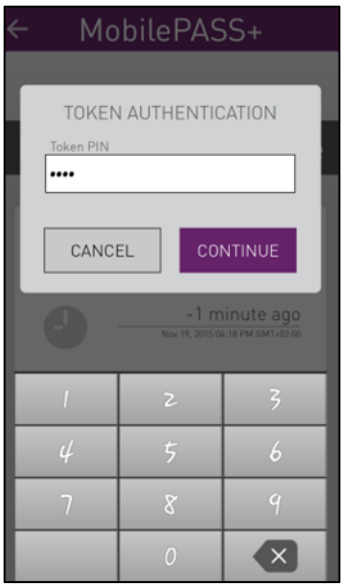
2. Enter your LDAP user name and password, and then select the **Use my mobile to autosend a passcode** option.



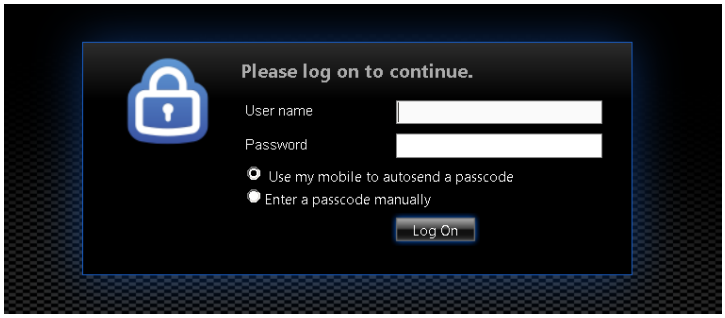
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

3. You will receive a push notification on the registered mobile device. On the mobile device screen, tap **APPROVE**.

4. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **CONTINUE**.

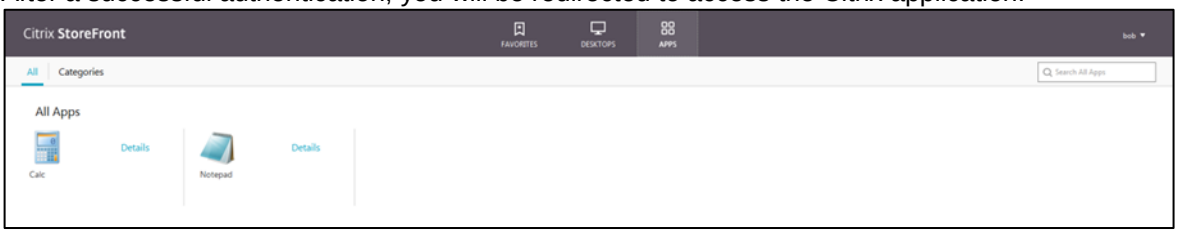


5. In the web browser, on the Citrix NetScaler Access Gateway login window, click **Log On**.



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

After a successful authentication, you will be redirected to access the Citrix application.



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

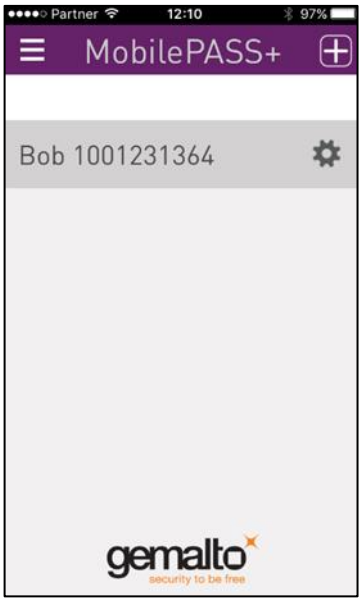
Entering a Passcode Manually

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

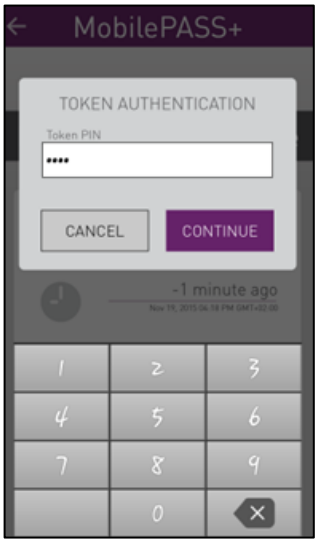
2. Enter your LDAP user name and password, and then select the **Enter a passcode manually** option.

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

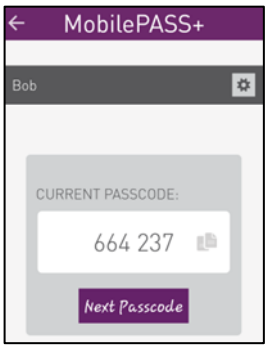
3. On the registered mobile device, open the mobile application.
4. On the mobile device screen, tap on the token.



5. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **CONTINUE**.



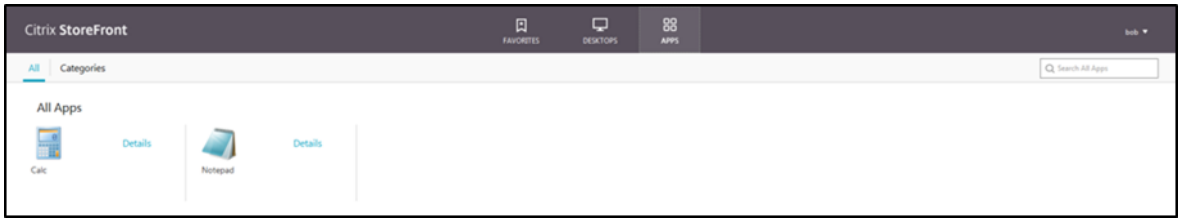
You will receive a passcode.



6. In the web browser, on the Citrix NetScaler Access Gateway login window, in the **Additional password** field, enter the passcode, and then click **Log On**.

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

After a successful authentication, you will be 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://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.	