SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5
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.

© 2015 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:** 007-012595-001, Rev. B  
**Release Date:** August 2015
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS Cloud</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS-SPE and SAS-PCE</td>
<td>7</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAS</td>
<td>7</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>8</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Creating Users Stores in SAS</td>
<td>8</td>
</tr>
<tr>
<td>Assigning an Authenticator in SAS</td>
<td>9</td>
</tr>
<tr>
<td>Adding Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 as an Authentication Node in SAS</td>
<td>10</td>
</tr>
<tr>
<td>Checking the SAS RADIUS Address</td>
<td>12</td>
</tr>
<tr>
<td>Configuring Citrix NetScaler 10.1 Access Gateway</td>
<td>13</td>
</tr>
<tr>
<td>Configuring StoreFront 2.5</td>
<td>16</td>
</tr>
<tr>
<td>Synchronizing User Stores</td>
<td>18</td>
</tr>
<tr>
<td>Authenticating with Grid Tokens</td>
<td>18</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>19</td>
</tr>
<tr>
<td>Authenticating with MobilePASS Messaging Tokens</td>
<td>20</td>
</tr>
<tr>
<td>Authenticating with MobilePASS</td>
<td>21</td>
</tr>
<tr>
<td>Authenticating with a MobilePASS Token</td>
<td>22</td>
</tr>
<tr>
<td>Customizing the Citrix Access Gateway Logon Page</td>
<td>24</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>25</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5.

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

Description

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

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

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

Citrix Unified Storefront 2.5 is the industry’s first unified enterprise app and data store that aggregates, controls, and delivers all apps and data - including Windows, web, SaaS, and mobile apps - to any device, anywhere.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 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

Note: For the purpose of this guide, Citrix NetScaler 10.1 Access Gateway was tested in a Citrix NetScaler VPX configuration based on virtual appliance deployment. The server version of Citrix NetScaler 10.1 Access Gateway should work using the same process.

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 10.1 Access Gateway**
- **StoreFront 2.5**

Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5, 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 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:
  

- **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 10.1 Access Gateway and Unified StoreFront 2.5.

1. A user attempts to log on to Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 using an OTP authenticator.
2. Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 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 10.1 Access Gateway and Unified StoreFront 2.5.
4. The user is granted or denied access to the Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5, ensure the following:

- End users can authenticate from the Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 environment with a static password before configuring the Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 to use RADIUS authentication.
- Ports 1812/1813 are open to and from Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5.
- 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 10.1 Access Gateway and Unified StoreFront 2.5 using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 8
- Assigning an Authenticator in SAS, page 9
- Adding Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Address, page 12

Creating Users Stores in SAS

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

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

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


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5.

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.

Adding Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 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 10.1 Access Gateway and Unified StoreFront 2.5. You will need the IP address of Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 and the shared secret to be used by both SAS and Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5.

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**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address in a range of IP addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5, check its IP address. The IP address will then be added to Citrix NetScaler 10.1 Access Gateway and Unified StoreFront 2.5 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 10.1 Access Gateway

The next step is to configure the Citrix NetScaler Access Gateway 10.1 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.
6. On the **Policies** tab, Select **Insert Policy**.

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

![Create Authentication Server window](image)

(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:
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.

Configuring StoreFront 2.5

Citrix StoreFront 2.5 authentication must be configured to pass through from the Citrix Netscaler Gateway.

1. Open the Citrix StoreFront 2.5 management console by clicking Start > All Programs > Citrix > Citrix StoreFront.

(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)
2. In the left pane, select **Authentication**.

3. In the right pane, select **Add/Remove Methods**.

4. Select **Pass-through from NetScaler Gateway** and then click **OK**.

5. In the right pane, select **Stores**.

6. In the right pane, select **Enable Remote Access**.

7. On the **Enable Remote Access** window, do the following:
   a. Under **Remote access**, select the VPN tunnel type.
   b. Under **NetScaler Gateway appliances**, select the relevant appliance, and then click **OK**.
Synchronizing User Stores

Before SAS can authenticate any user in your organization, you need to create a SAS user store that includes the users that would need to use multi-factor authentication. User entries/records are created in the SAS user store through a number of methods. It is important to use the method that fits the configuration used with Citrix NetScaler Access Gateway. The following table presents Citrix NetScaler Access Gateway authentication methods and recommended SAS methods.

<table>
<thead>
<tr>
<th>Citrix NetScaler Access Gateway Authentication Method</th>
<th>SafeNet Authentication Service User Store Lifecycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Users – Citrix Access Gateway's internal user store is currently being used.</td>
<td>Manual - Create users manually in a SAS user store, either by creating one user at a time, or by importing one or more user records via a flat file.</td>
</tr>
<tr>
<td>LDAP – An external user directory is being used.</td>
<td>Automated – Users are updated automatically by synchronizing the Active Directory/LDAP server using the SAS LDAP Synchronization Agent.</td>
</tr>
<tr>
<td>RADIUS – A legacy multi-factor authentication solution was deployed.</td>
<td>Automated – Contact SafeNet customer support to ask about SAS migration guides.</td>
</tr>
</tbody>
</table>

For additional details on adding users to SafeNet Authentication Service, refer to the SAS Subscriber Account Operator Guide. All SAS documentation can be found on the SafeNet Knowledge Base website.

Authenticating with GriD Tokens

This method allows a user to generate a one-time password (OTP) without the requirement for hardware tokens or software applications. GrID works by presenting the user with a matrix of cells during enrollment containing random characters from which they select a personal identification pattern (PIP). Thereafter, whenever the user wishes to authenticate to a SAS-protected resource, they are presented with a challenge grid containing random characters. The user enters the characters in the cells that correspond to their PIP. Each time the challenge grid appears, the characters in the cells will be different, so the user is always entering a one-time passcode.

In order to use GriD authentication with Citrix NetScaler Access Gateway, you need to replace the existing index.html file located in /netscaler/ns_gui/vpn with the following version (DOW4091):

http://bel1web002:9876/Files/07584a2c3e334138ab88bb49fa76d9e
After downloading the file, locate the following line:

```javascript
var BlackShieldServerLocation = "(https://grid.safenet-inc.com/blackshieldss/O/1MAGXLUGLK/index.aspx)";
```

Change the url to the SAS Gridsure URL:


**Note** – it assumes using SAS cloud as the RADIUS authenticator, in case of working with On Premise environment the **BlackShieldServerLocation** to SafeNet Authentication Service’s self-service URL.

### Running the Solution

To authenticate using a Grid token:

1. Log in to the VPX virtual server using a web browser.
2. Enter the user name and Windows password, and then click **Get Grid**.

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

3. In the **Grid Pattern** field, enter the numbers that correspond to your selected PIP, and then click **Log On**.

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

The Citrix desktop window is displayed.
Authenticating with MobilePASS Messaging Tokens

To avoid the duplicate **Password** field when using SMS authentication with Citrix NetScaler Access Gateway, you can choose to hide this secondary authentication field (which is used to trigger the SMS messaging) by customizing the default **index.html** file.

**Customizing the Login Page**

1. Connect to the VPX server console using **ssh/direct**.
2. Back up the following file: `/netscaler/ns_gui/vpn/login.js`
3. Edit the file `login.js`.
   a. Locate the following section:
      ```javascript
      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>');
      }
      ```
   b. Add the highlighted values as shown:
      ```javascript
      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>');
      }
      ```
4. To ensure that the changes will be retained the next time the system is rebooted, follow this procedure:
   a. Run the following commands to create a directory to store the modification files:
      ```bash
      mkdir /var/customization
      ```
   b. Run the following commands to copy the modified files to the `/customization` directory:
      ```bash
      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
      ```
5. If the file `/nsconfig/rc.netscaler` does not exist, execute the following command to create it:

   `touch /nsconfig/rc.netscaler`

6. 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`

### Authenticating with MobilePASS

To authenticate using MobilePASS Messaging Tokens token:

1. Log in to the VPX virtual server via the web browser.
2. Enter the user name and user domain password, and then click **Log On**.

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

3. SMS is triggered and the **Additional Information Required** window is displayed.

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

4. Enter the passcode that was sent to your mobile device, and then click **Submit**.
   
   The Citrix desktop window is displayed.
Authenticating with a MobilePASS Token

To authenticate using a MobilePASS token:

1. Log in to the VPX virtual server using a web browser.
2. Enter your user name, Windows password, and SafeNet OTP passcode, and then click Log On.

The Citrix desktop window is displayed.
Customizing the Citrix Access Gateway Logon Page

When two-factor authentication is configured on Citrix Access Gateway Enterprise Edition, the user is prompted with the User name, Password 1, and Password 2 fields. The Password 1 and Password 2 field labels can be changed, without interruption, to something more descriptive, such as Windows Password or SafeNet Passcode.

To customize the login page:
1. Log in to Citrix NetScaler using SSH.
2. Go to /netscaler/ns_gui/vpn/resources.
3. In the Resources folder, you will find several language-specific xml files. In this procedure, the English language file (en.xml) will be modified; however, the procedure can be applied to other languages as needed.
5. Edit the en.xml file using a text editor, such as Notepad.
   a. Search for the Password string and change it as desired.
   b. Search for the Password2 string and change it as desired.
   c. Save the file.
6. Go to /netscaler/ns_gui/vpn.
7. Back up the file login.js.
8. Edit the login.js file using a text editor, such as Notepad.
   a. Search for the following line:
      ```javascript
      if ( pwc == 2 ) { document.write("\nnbsp;1"); }
      ```
   b. Delete the 1 character
   c. Save the file.

The modifications result in the following changes to the logon window:

(The screen image above is from Citrix® software. 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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>