

SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Citrix NetScaler Access Gateway

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.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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: 007-013480-001, Rev. A

Release Date: August 2016

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	5
Environment.....	5
Audience	5
CBA Flow using SafeNet Authentication Client	5
Prerequisites	6
Supported Tokens in SafeNet Authentication Client	6
Configuring Citrix NetScaler Access Gateway	7
Configuring Citrix StoreFront	11
Configuring SmartCard Pass-through.....	12
Running the Solution	13
Using SAC CBA for Citrix Web Access	13
Using SAC CBA for Citrix Receiver Application Access	14
Using SAC CBA with SSO for Citrix Web Access.....	16
Using SAC CBA with SSO for Citrix Receiver Application Access	16
Appendix: Modifying the CSP PIN Prompt from Citrix Default to SafeNet Authentication Client	17
Support Contacts	18

Third-Party Software Acknowledgement

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

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the datacenter, and accessed across a wide range of devices and locations. Deploying desktop virtualization without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

SafeNet Authentication Client (SAC) is a Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

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 to the need for a strong authentication approach based on multi-factor authentication.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Citrix NetScaler Access Gateway using SafeNet tokens.

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

Citrix NetScaler Access Gateway can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)**—SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **Citrix NetScaler Access Gateway**

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC)**—Version 10.0
- **Citrix NetScaler Access Gateway**—Version 11.0
- **Citrix XenApp**—Version 7.7

Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler Access Gateway, and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

The diagram below illustrates the flow of certificate-based authentication:



1. A user attempts to connect to the Citrix NetScaler Access Gateway server using the Citrix NetScaler Access Gateway client application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
2. After successful authentication, the user is allowed access to select a virtual desktop machine.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Citrix NetScaler Access Gateway using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (version 10.0) should be installed on all client machines.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of tokens that can be used as a second authentication factor for users who authenticate to Citrix NetScaler Access Gateway.

SafeNet Authentication Client 10.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3840

Certificate-based Hybrid USB Tokens

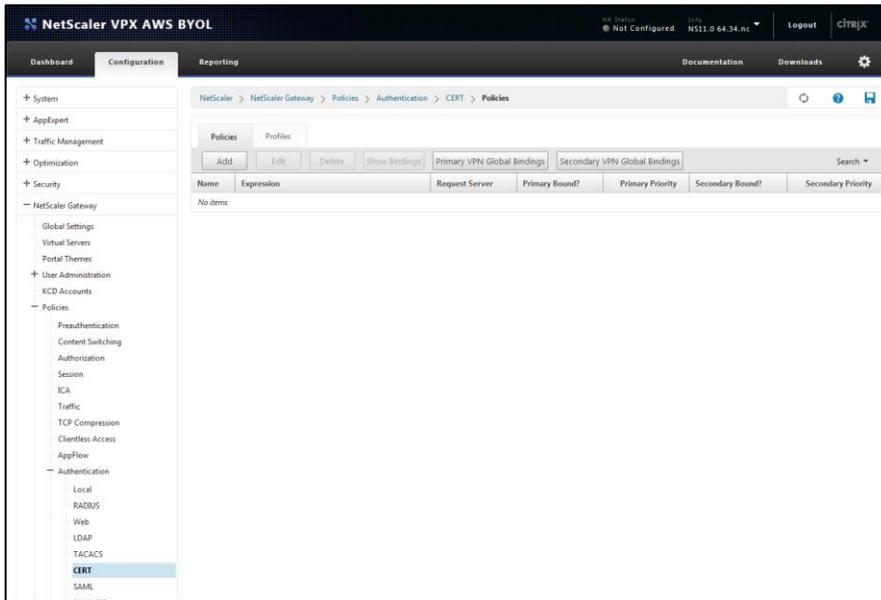
- SafeNet eToken 7300
- SafeNet eToken 7300-HID

Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

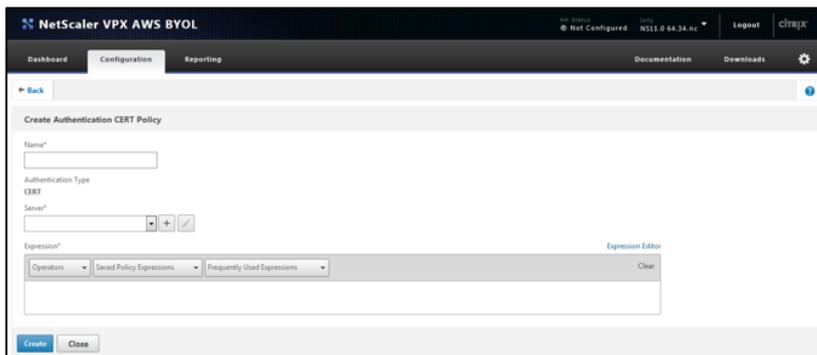
Configuring Citrix NetScaler Access Gateway

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



(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 CERT Policy** window, perform the following steps:
 - a. In the **Name** field, enter a name for the policy (for example, **CBA_Profile**).



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

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

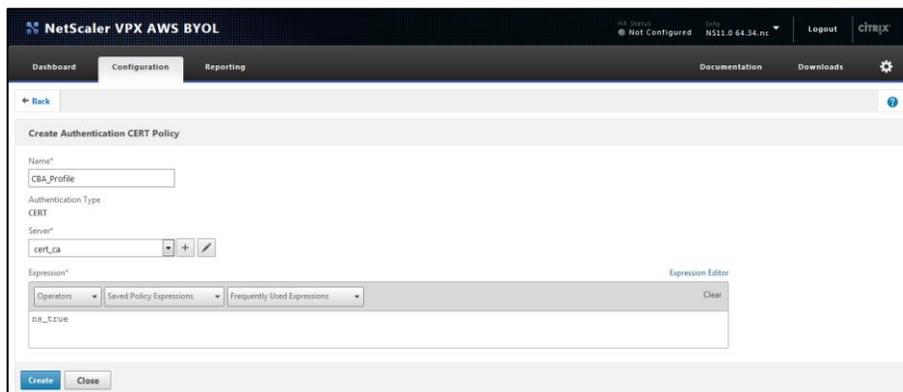
- c. On the **Create Authentication CERT Profile** window, complete the following fields, and then click **Create**.

Name	Enter a name for the profile (for example, cert_ca).
True Factor	Select OFF .
User Name Field	Select SubjectAltName:PrincipalName .



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

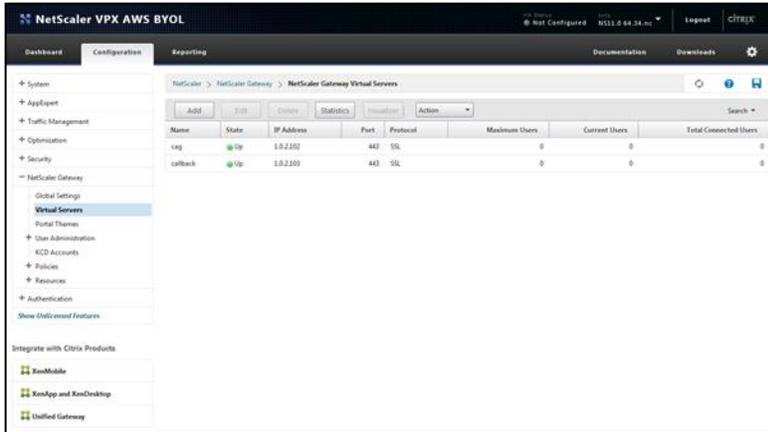
- d. On the **Create Authentication CERT Policy** window, under **Expression**, click **Saved Policy Expressions**, and then select **ns_true**.
- e. Click **Create**.



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

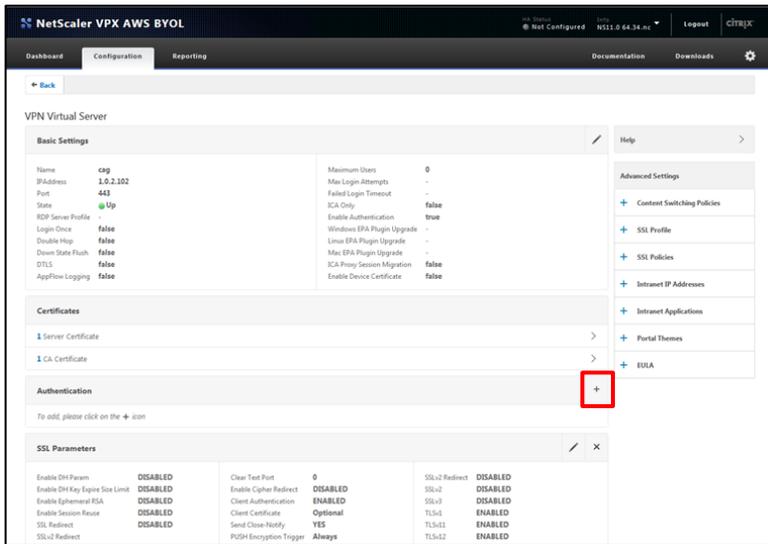
Now you need to bind the CBA authentication to the virtual server.

- 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.)

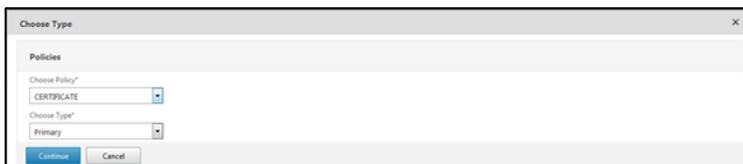
- In the right pane, select the gateway you created (for example, **cag**), and then click **Edit**.
- On the **VPN Virtual Server** window, under **Authentication**, click the  icon.



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

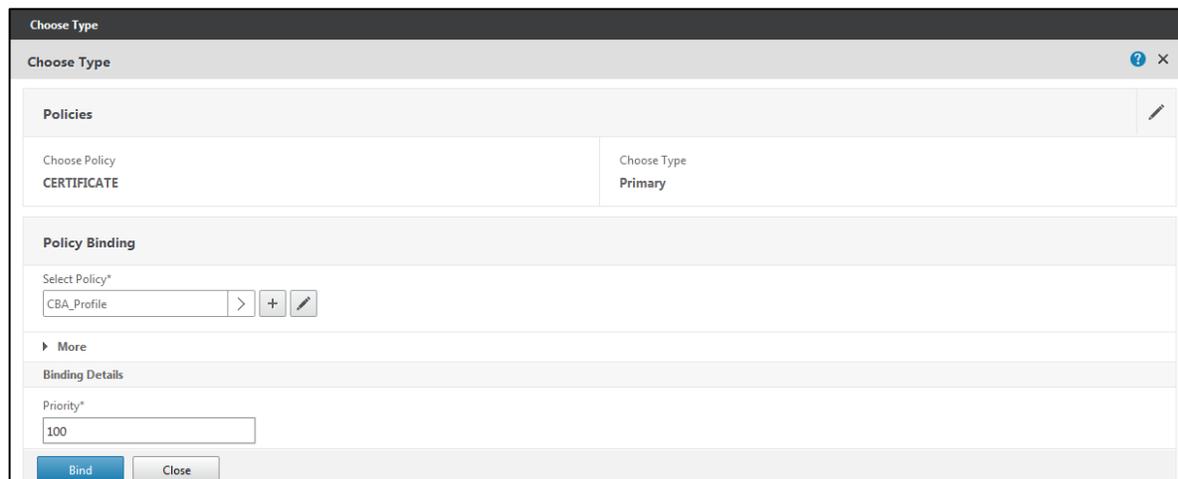
- On the **Choose Type** window, under **Policies**, complete the following fields, and then click **Continue**.

Choose Policy	Select CERTIFICATE .
Choose Type	Select Primary .



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

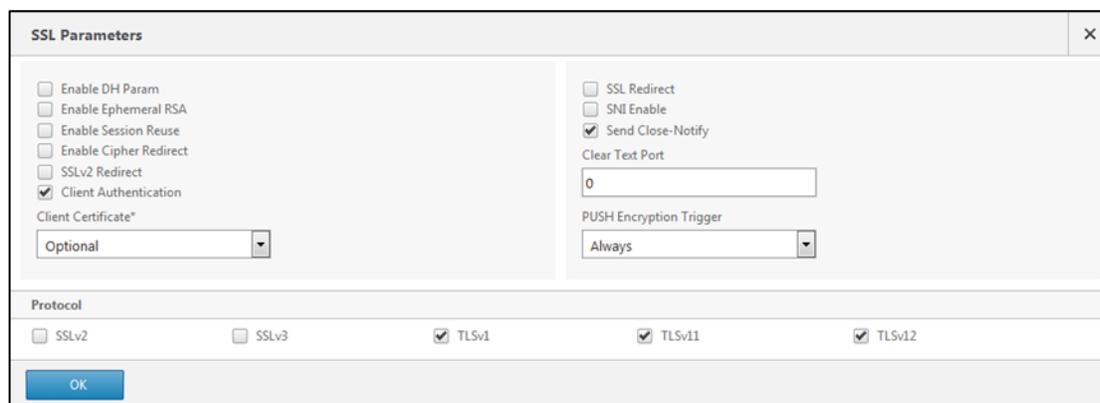
9. Under **Policy Binding**, in the **Select Policy** field, select the CERT policy (for example, **CBA_Profile**) that you created earlier in step 4, and then click **Bind**.



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

Now you need to configure the virtual server **SSL Parameters** for certificate-based authentication.

10. On the **VPN Virtual Server** window, under **SSL Parameters**, click the  icon, and then perform the following steps:
- Clear the **Enable Ephemeral RSA** and **Enable Session Reuse** options.
 - Select the **Client Authentication** option.
 - In the **Client Certificate** field, select **Optional**.



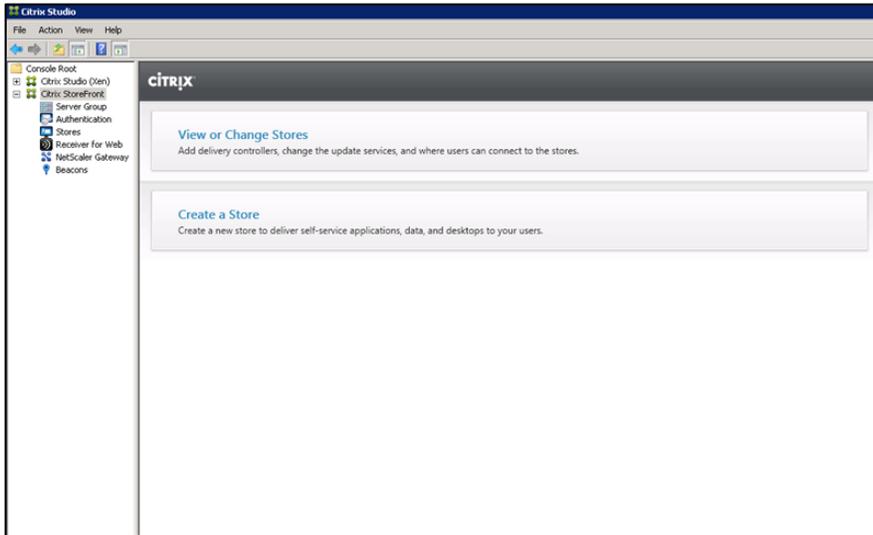
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

- Click **OK**.
- Click **Done**.

Configuring Citrix StoreFront

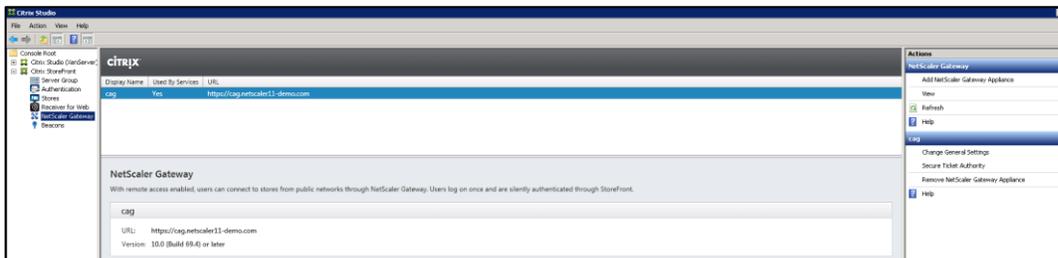
Configure Citrix StoreFront to allow NetScaler pass-through authentication in order to use Citrix NetScaler Gateway as the certificate-based authentication.

1. Open the Citrix Studio console.
2. In the left pane, click **Citrix StoreFront > NetScaler Gateway**.



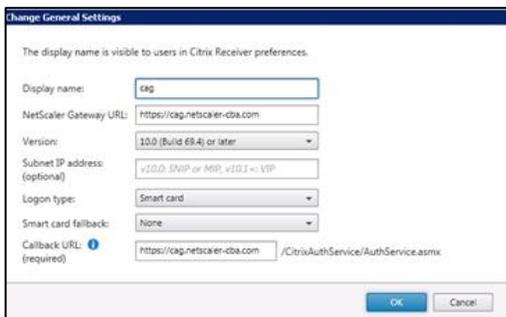
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

3. In the middle pane, select the gateway you created (for example, **cag**), and then in the right pane, under **cag**, click **Change General Settings**.



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

4. On the **Change General Settings** window, in the **Logon type** field, select **Smart card**, and then click **OK**.



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

Configuring SmartCard Pass-through



NOTE: It is assumed that all the appropriate configurations for smartcard single sign-on (SSO) are done. For more information, refer to <http://docs.citrix.com/en-us/storefront/3/configure-authentication-and-delegation/sf-configure-smartcard.html>.

1. Open the SafeNet Authentication Client Tools console.



2. In the top right-corner, click the  icon to open the Advanced view.
3. In the left pane, click **SafeNet Authentication Client Tools > Tokens > Client Settings**.
4. In the right pane, click the **Advanced** tab, and then select **Enable single logon**.

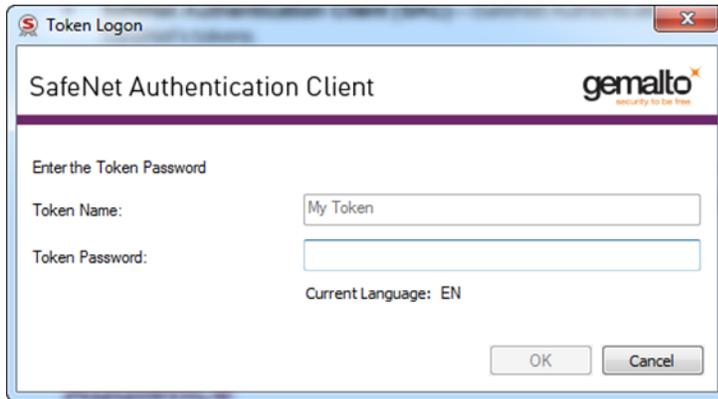


5. Click **Save**.

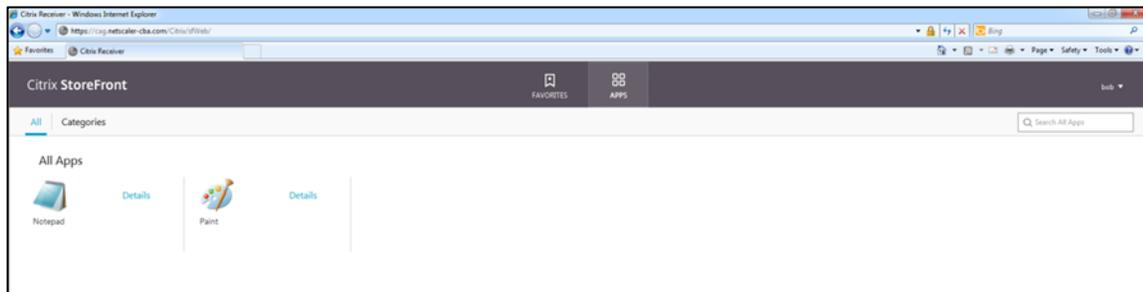
Running the Solution

Using SAC CBA for Citrix Web Access

1. In a web browser, open the Citrix NetScaler Access Gateway URL.
2. On the **SafeNet Authentication Client** login window, enter the token password, and then click **OK**.



3. After successful authentication, you are redirected to the Citrix StoreFront console. Click on the icon of any of the published applications to launch it.



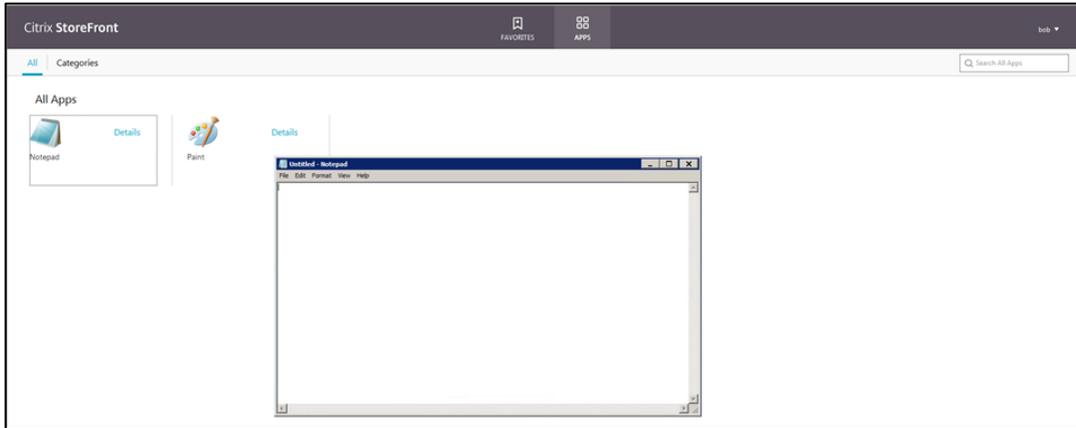
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

4. On the **Windows Logon** window, enter your smart card PIN, and then click the  icon.



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

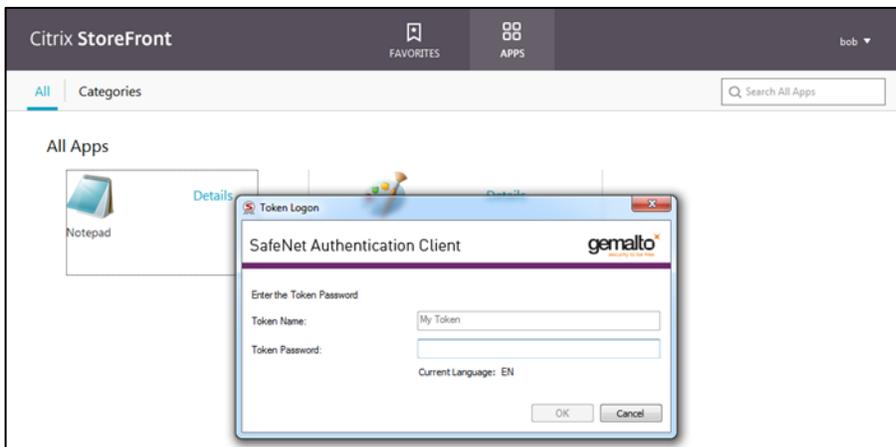
After successful authentication, you will be able to access the application.



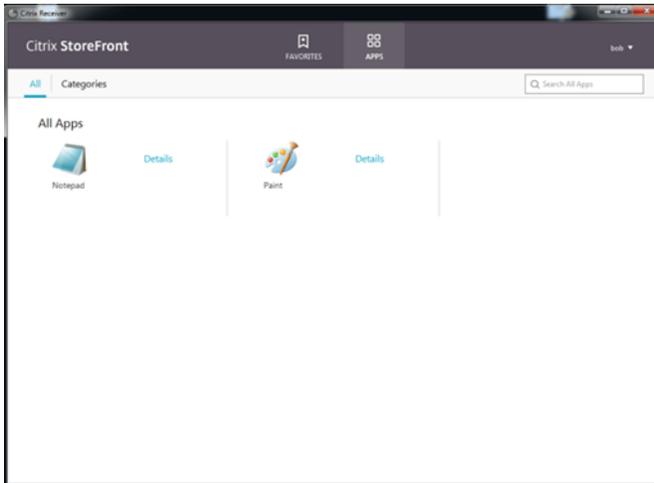
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

Using SAC CBA for Citrix Receiver Application Access

1. Open the Citrix Receiver application.
2. On the **SafeNet Authentication Client** login window, enter the token password, and then click **OK**.



3. After successful authentication, you are redirected to the Citrix StoreFront console. Click on the icon of any of the published applications to launch it.



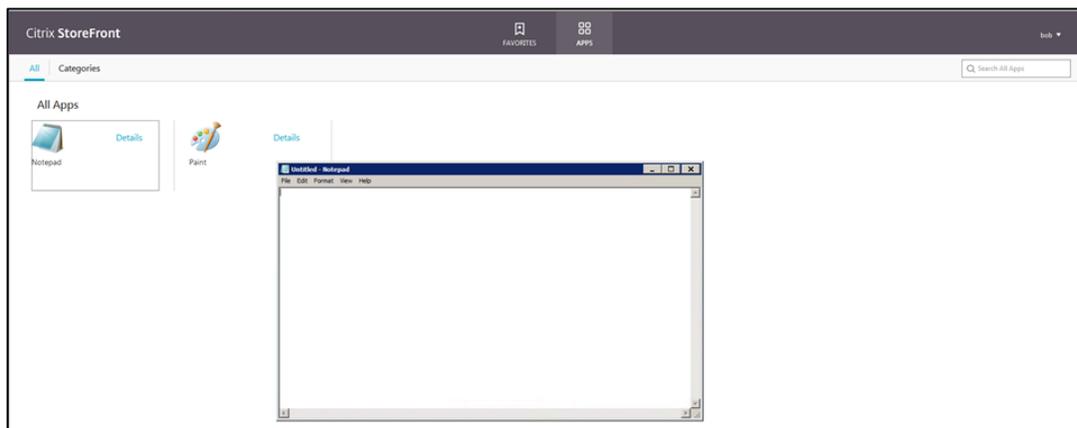
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

4. On the **Windows Logon** window, enter your smart card PIN, and then click the  icon.



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

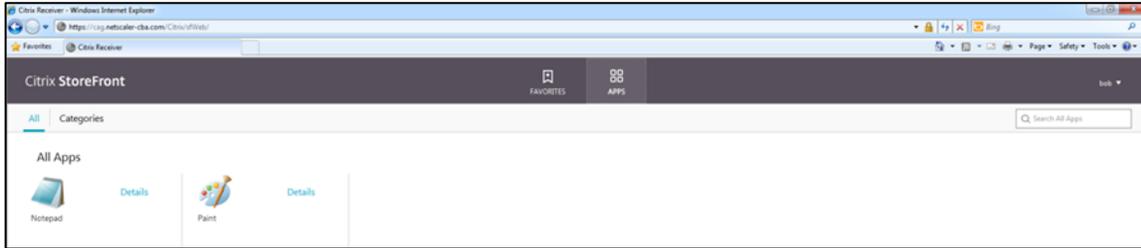
After successful authentication, you will be able to access the application.



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

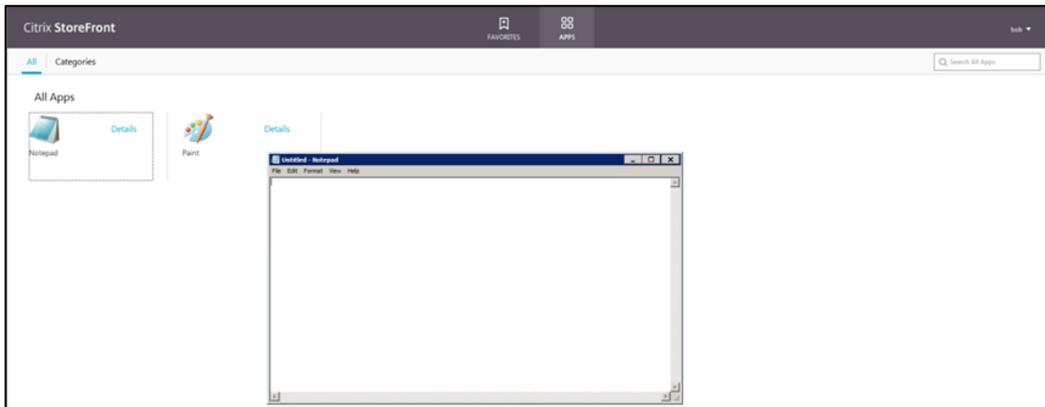
Using SAC CBA with SSO for Citrix Web Access

1. Log in to the client machine using the smart card for SSO.
After successful authentication, you will be logged in to the client machine.
2. Open the Citrix NetScaler Access Gateway URL in a web browser. You are redirected to access Citrix StoreFront as the SSO authentication is configured.



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

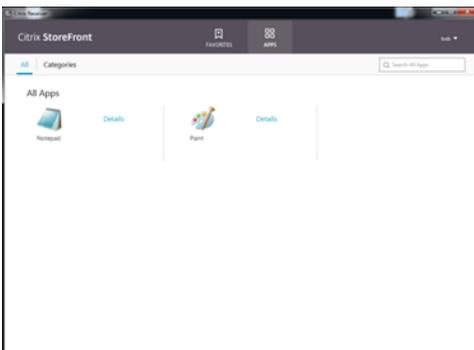
3. Click on the icon of any of the published applications to launch it. The application will open.



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

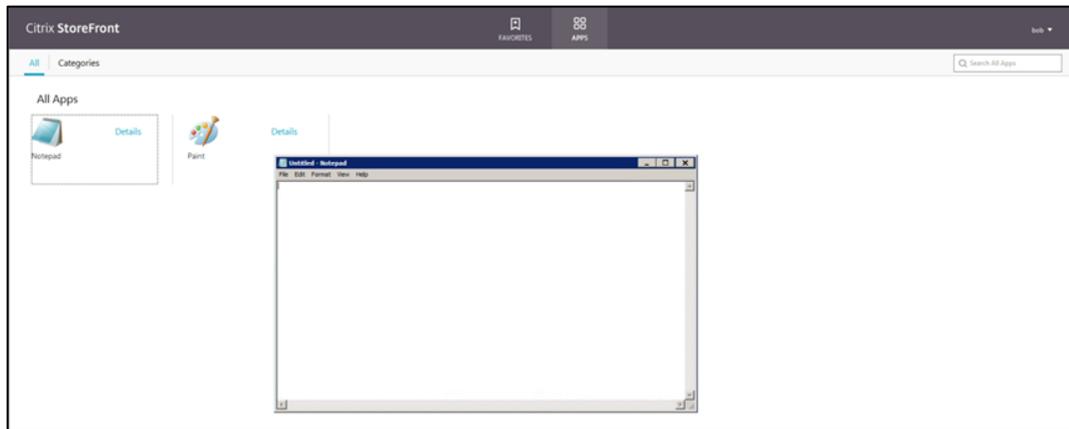
Using SAC CBA with SSO for Citrix Receiver Application Access

1. Log in to the client machine using the smart card for SSO.
After successful authentication, you will be logged in to the client machine.
2. Open the Citrix Receiver application. You are redirected to access the Citrix StoreFront console as the SSO authentication is configured.



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

- Click on the icon of any of the published applications to launch it. The application will open.

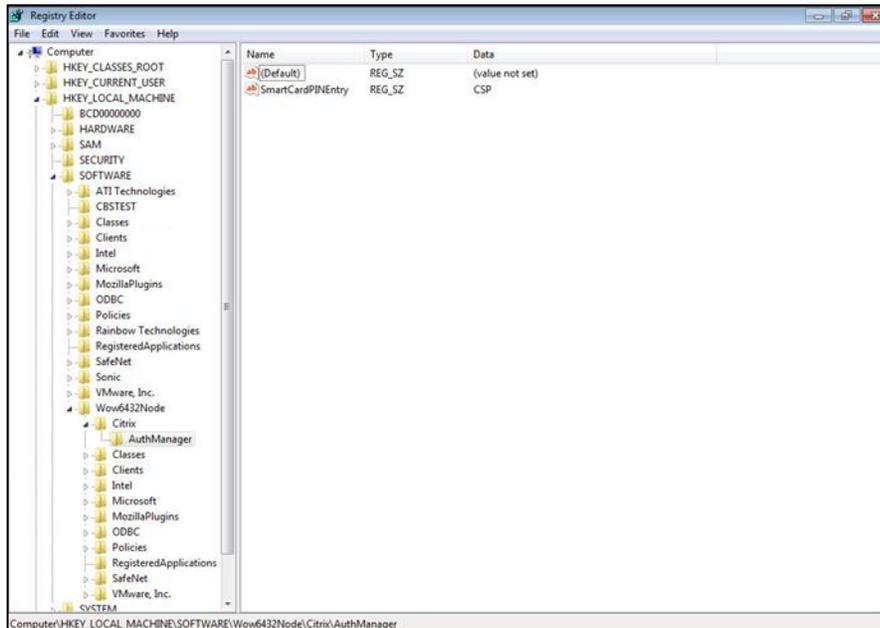


(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

Appendix: Modifying the CSP PIN Prompt from Citrix Default to SafeNet Authentication Client

- Log in to the client machine as an administrator.
- Open Registry Editor and then in the registry key, add the following key value:

HKLM\Software\[Wow6432Node]Citrix\AuthManager: SmartCardPINEntry=CSP



(The screen image above is from Microsoft® 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.

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.	