SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Citrix NetScaler Access Gateway 12

gemalto

security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Number: 007-013946-001, Rev. A

Release Date: October 2017

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 Access Gateway 12.

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.

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 12 using SafeNet tokens.

It is assumed that the Citrix NetScaler Access Gateway 12 environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Citrix NetScaler Access Gateway 12 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) Typical installation mode**— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode**— IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

For more details about different SAC installation modes, refer to the Customization section in SafeNet Authentication Client Administrator Guide.

- **Citrix NetScaler Access Gateway 12**

Environment

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

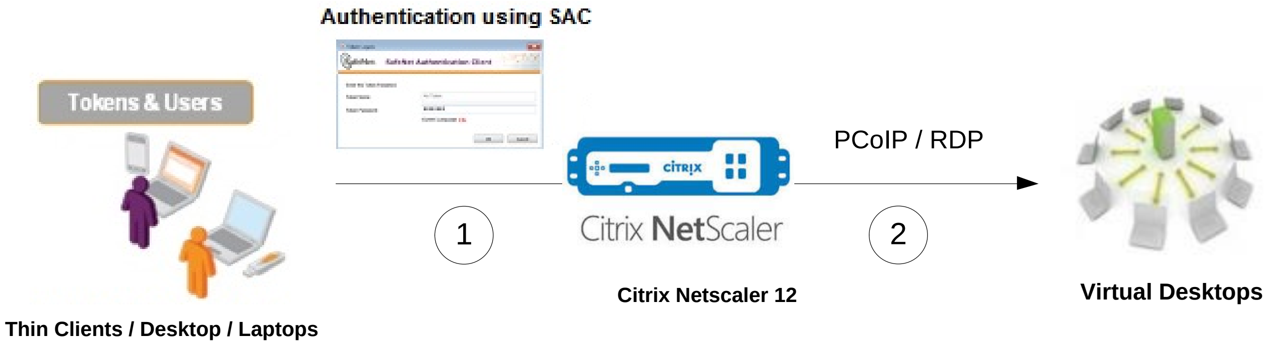
- **SafeNet Authentication Client (SAC)**— Version 10.4
- **Citrix NetScaler Access Gateway 12**— Version 12

Audience

This document is intended for system administrators who are familiar with Citrix NetScaler Access Gateway 12, and are interested in adding certificate-based authentication capabilities using Gemalto tokens and smart cards. See Supported Tokens and Smart Cards in SafeNet Authentication Client, on page 7.

CBA Flow using SafeNet Authentication Client

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



1. A user attempts to connect to the Citrix NetScaler Access Gateway 12 server using the Citrix NetScaler Access Gateway 12 client application. The user inserts the Gemalto token or smart card on which the certificate resides and when prompted, the token or smart card password is entered.
2. After successful authentication, a user is granted access to a virtual desktop machine.

Prerequisites

The following prerequisites must be installed and configured before implementing certificate-based authentication for Citrix NetScaler Access Gateway 12 using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. 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) must 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 Gemalto token or smart card with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (Version 10.4) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (version 10.4) supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

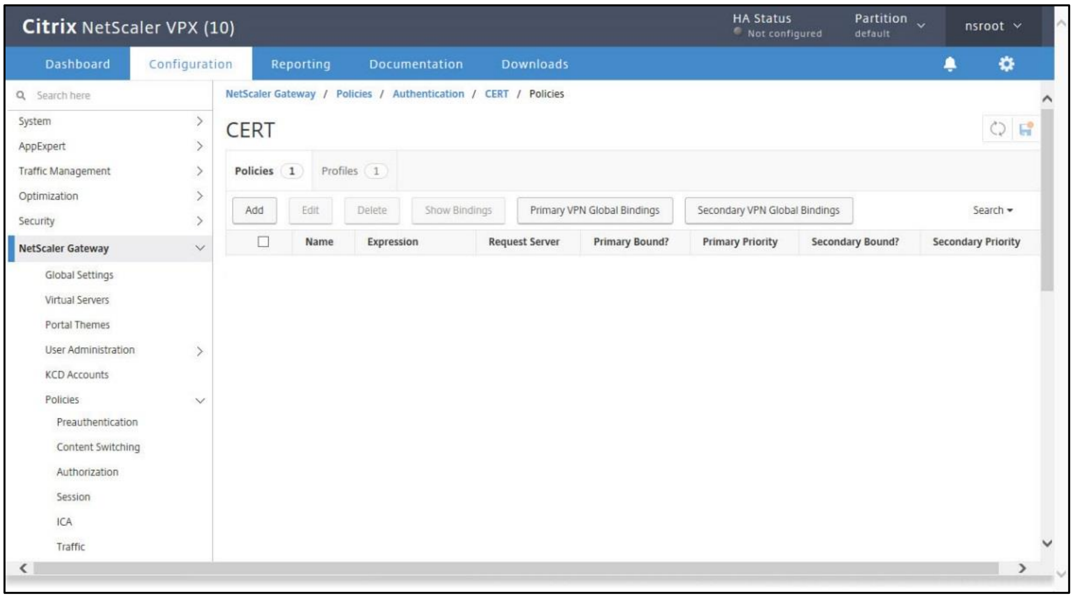
- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For all supported devices please refer to SafeNet Authentication Client Customer Release Notes.

Configuring Citrix NetScaler Access Gateway 12

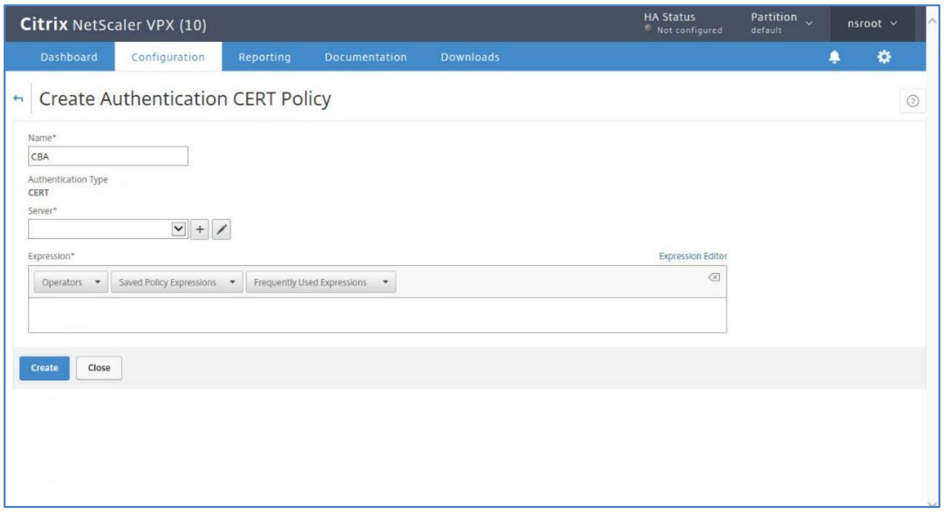
In the following section we will describe how to configure Citrix Netscaler Access Gateway version 12 to support PKI authentication using Safenet Authentication Client and Gemalto's tokens and smart cards.

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



3. In the top pane, click **Add**
4. In 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).



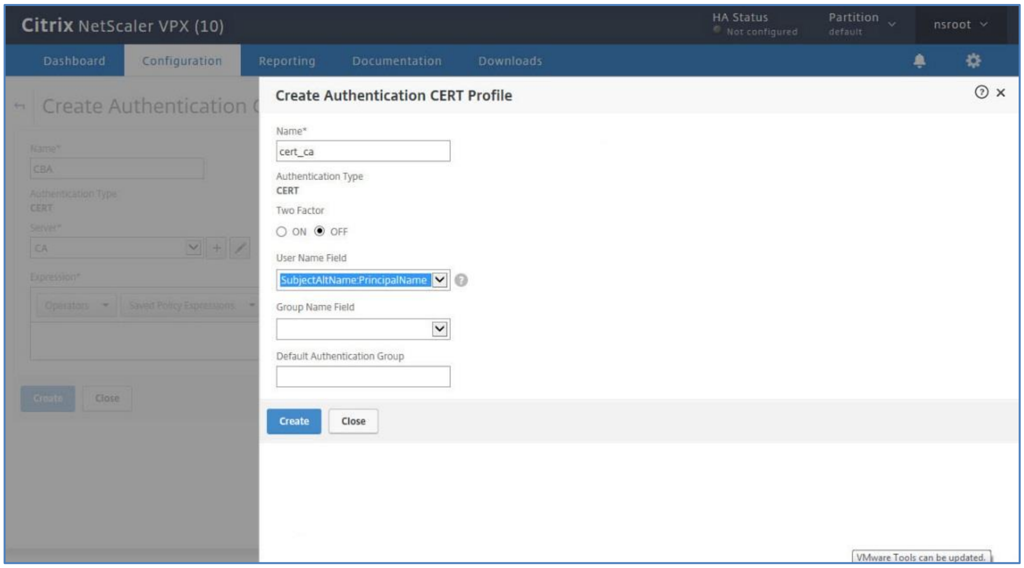
Name*
CBA

Authentication Type
CERT

   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**.



Create Authentication CERT Profile

Name*: cert_ca

Authentication Type: CERT

Two Factor: ○ ON ● OFF

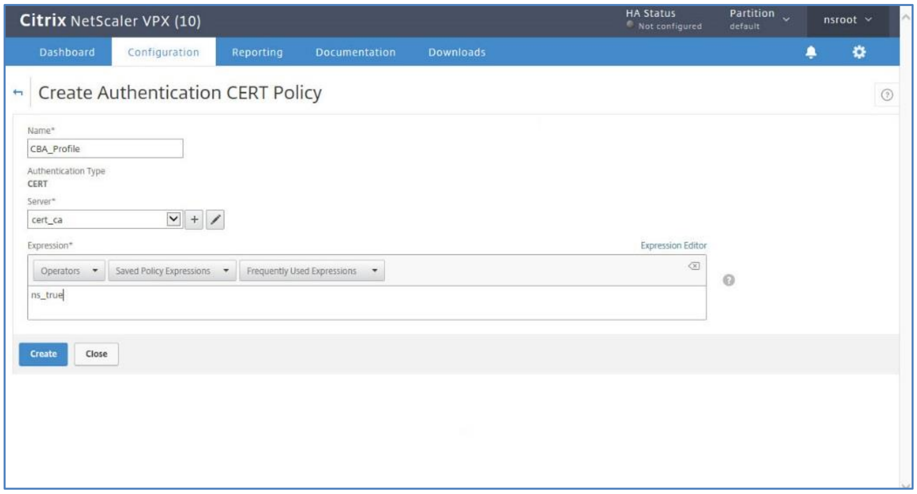
User Name Field: SubjectAltName:PrincipalName

Group Name Field:

Default Authentication Group:

d. In the **Create Authentication CERT Policy** window, under **Expression**, click **Saved Policy Expressions**, and then select **ns_true**.

e. Click **Create**.



Create Authentication CERT Policy

Name*: CBA_Profile

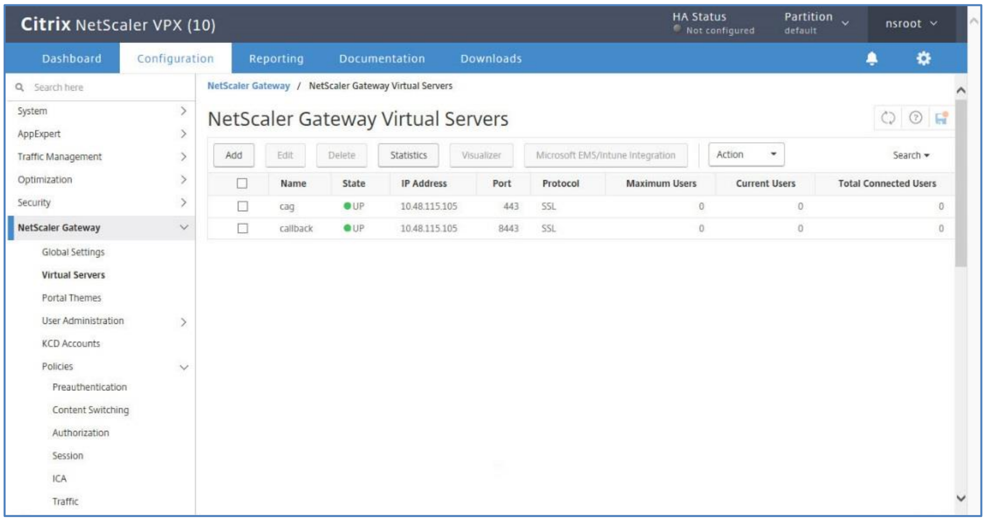
Authentication Type: CERT

Server*: cert_ca

Expression*: ns_true

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

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

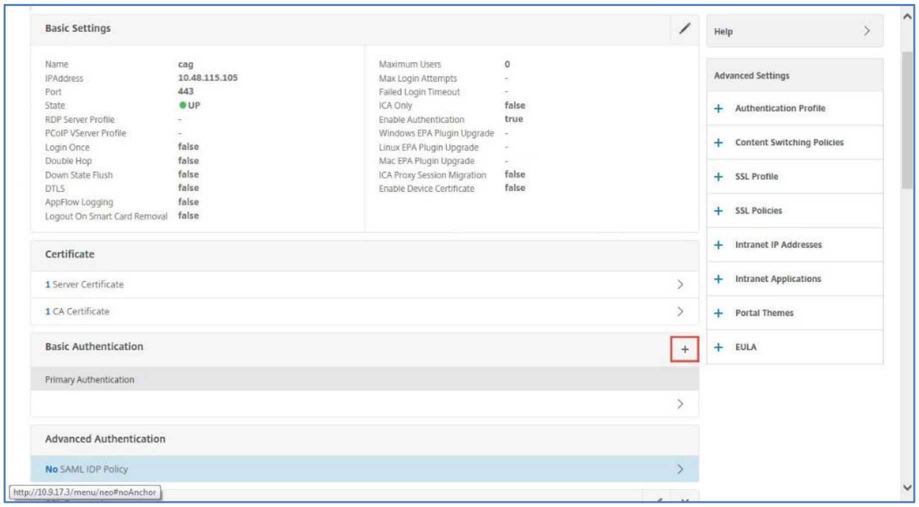


NetScaler Gateway Virtual Servers

☐	Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
☐	cag	● UP	10.48.115.105	443	SSL	0	0	0
☐	callback	● UP	10.48.115.105	8443	SSL	0	0	0

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

7. On the **VPN Virtual Server** window, under **Basic Authentication**, click the + icon.



Basic Settings

Name	cag
IPAddress	10.48.115.105
Port	443
State	● UP
RDP Server Profile	-
PCoIP VServer Profile	-
Login Once	false
Double Hop	false
Down State Flush	false
DTLS	false
AppFlow Logging	false
Logout On Smart Card Removal	false
Maximum Users	0
Max Login Attempts	-
Failed Login Timeout	-
ICA Only	false
Enable Authentication	true
Windows EPA Plugin Upgrade	-
Linux EPA Plugin Upgrade	-
Mac EPA Plugin Upgrade	-
ICA Proxy Session Migration	false
Enable Device Certificate	false

Certificate

1 Server Certificate

1 CA Certificate

Basic Authentication

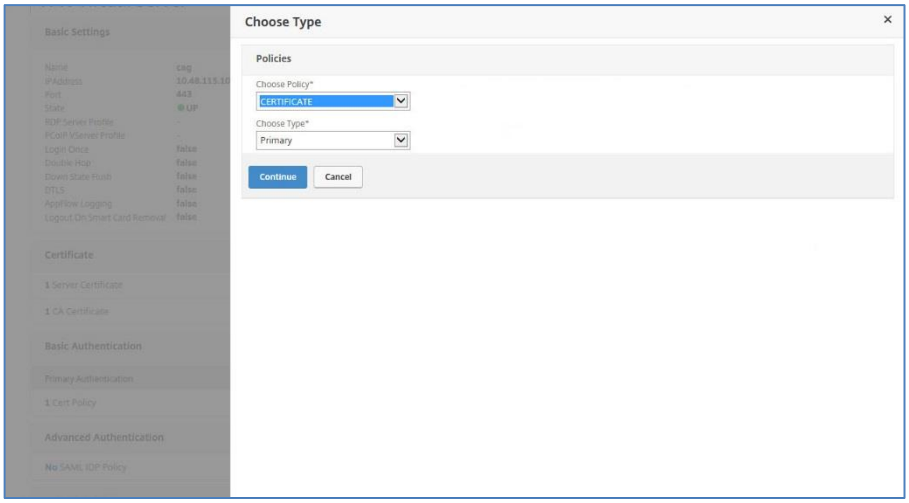
Primary Authentication

Advanced Authentication

No SAML IDP Policy

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

Choose Policy	Select **CERTIFICATE**.
Choose Type	Select **Primary**.



Basic Settings

Name	cag
IPAddress	10.48.115.10
Port	443
State	● UP
RDP Server Profile	-
PCoIP VServer Profile	-
Login Once	false
Double Hop	false
Down State Flush	false
DTLS	false
AppFlow Logging	false
Logout On Smart Card Removal	false

Certificate

1 Server Certificate

1 CA Certificate

Basic Authentication

Primary Authentication

1 Cert Policy

Advanced Authentication

No SAML IDP Policy

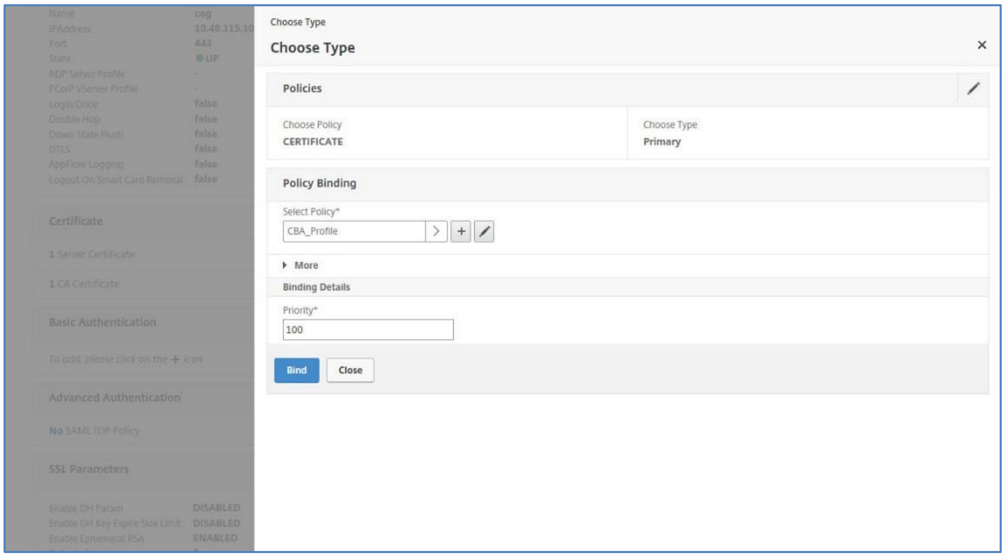
Choose Type

Policies

Choose Policy*: CERTIFICATE

Choose Type*: Primary

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**.



Name	cag
IPAddress	10.48.115.10
Port	443
State	● UP
RDP Server Profile	-
PCoIP VServer Profile	-
Login Once	false
Double Hop	false
Down State Flush	false
DTLS	false
AppFlow Logging	false
Logout On Smart Card Removal	false

Certificate

1 Server Certificate

1 CA Certificate

Basic Authentication

To add, please click on the + icon

Advanced Authentication

No SAML IDP Policy

SSL Parameters

Enable DH Param	DISABLED
Enable DH Key Expire Size Limit	DISABLED
Enable Ephemeral RSA	ENABLED

Choose Type

Choose Type

Policies

Choose Policy: CERTIFICATE

Choose Type: Primary

Policy Binding

Select Policy*: CBA_Profile

Binding Details

Priority*: 100

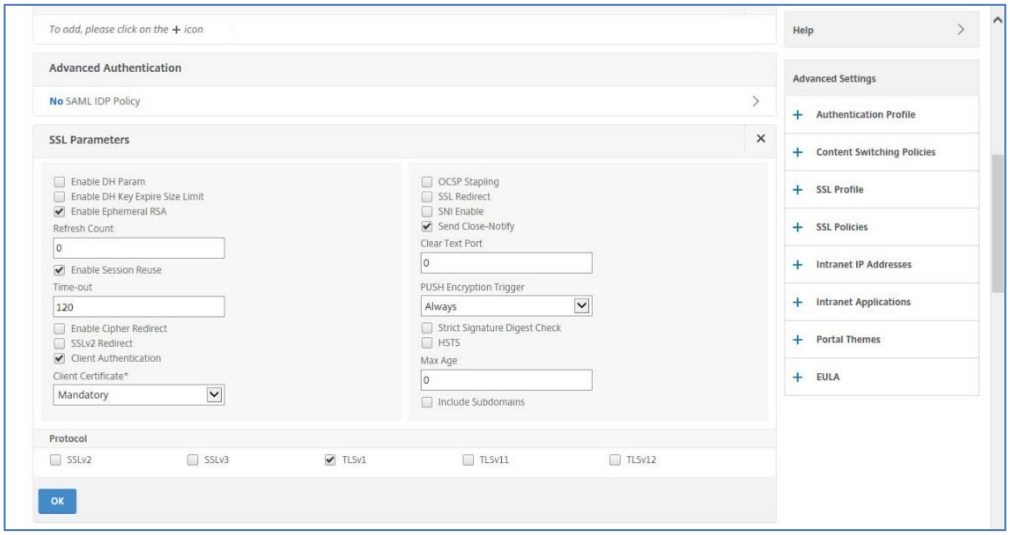
Now you need to configure the virtual server **SSL Parameters** for certificate-based authentication.

10. On the **VPN Virtual Server** window, under **SSL Parameters**, click the ✎ icon, and then perform the following steps:

    a. Clear the **Enable Ephemeral RSA** and **Enable Session Reuse** options.

    b. Select the **Client Authentication** option.

    c. In the **Client Certificate** field, select **Optional**.



To add, please click on the + icon

Advanced Authentication

No SAML IDP Policy

SSL Parameters

☐ Enable DH Param
☐ Enable DH Key Expire Size Limit
☑ Enable Ephemeral RSA
Refresh Count: 0
☑ Enable Session Reuse
Time-out: 120
☐ Enable Cipher Redirect
☐ SSLv2 Redirect
☑ Client Authentication
Client Certificate*: Mandatory

☐ OCSP Stapling
☐ SSL Redirect
☐ SNI Enable
☑ Send Close-Notify
Clear Text Port: 0
PUSH Encryption Trigger: Always
☐ Strict Signature Digest Check
☐ HSTS
Max Age: 0
☐ Include Subdomains

Protocol

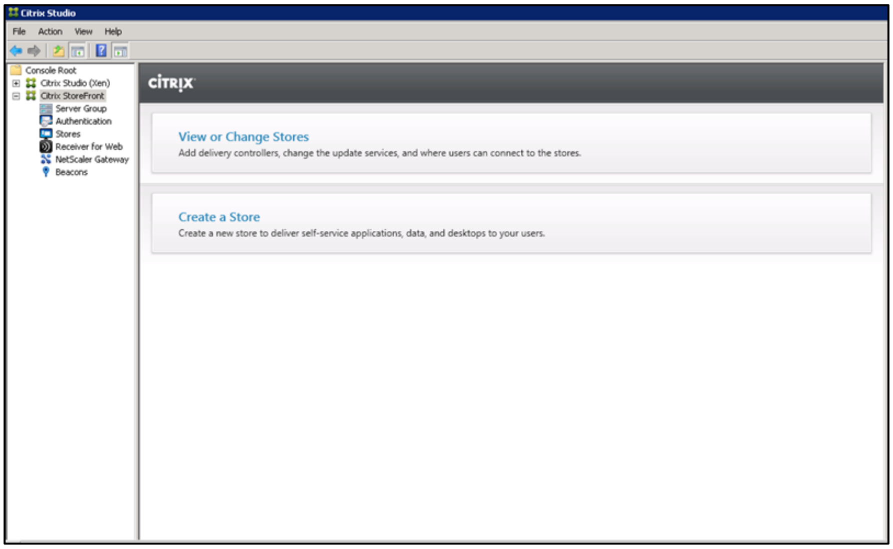
☐ SSLv2 ☐ SSLv3 ☑ TLSv1 ☐ TLSv11 ☐ TLSv12

    d. Click **OK,** then 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.

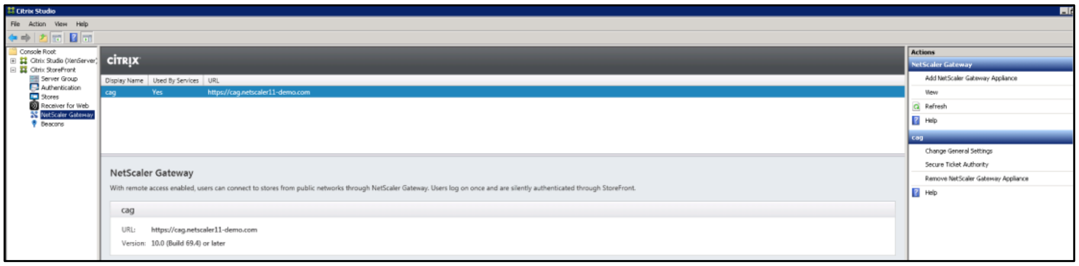
1. Open the **Citrix Studio** console.
2. In the left pane, select **Citrix StoreFront > NetScaler Gateway**.



View or Change Stores
Add delivery controllers, change the update services, and where users can connect to the stores.

Create a Store
Create a new store to deliver self-service applications, data, and desktops to your users.

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**.



Display Name	Used By Services	URL
cag	Yes	https://cag.netscaler11-demo.com

NetScaler Gateway

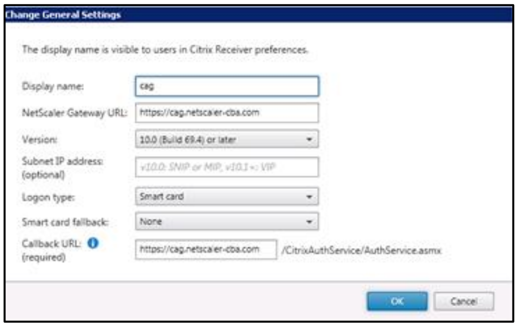
With remote access enabled, users can connect to stores from public networks through NetScaler Gateway. Users log on once and are silently authenticated through StoreFront.

cag

URL: https://cag.netscaler11-demo.com

Version: 10.0 (Build 69.4) or later

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



The display name is visible to users in Citrix Receiver preferences.

Display name: cag

NetScaler Gateway URL: https://cag.netscaler-cba.com

Version: 10.0 (Build 69.4) or later

Subnet IP address: (optional) v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Smart card

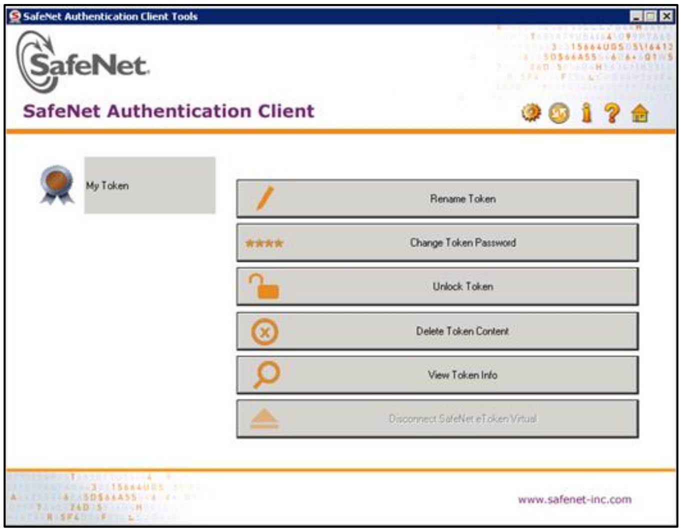
Smart card fallback: None

Callback URL: (required) https://cag.netscaler-cba.com /CitrixAuthService/AuthService.asmx

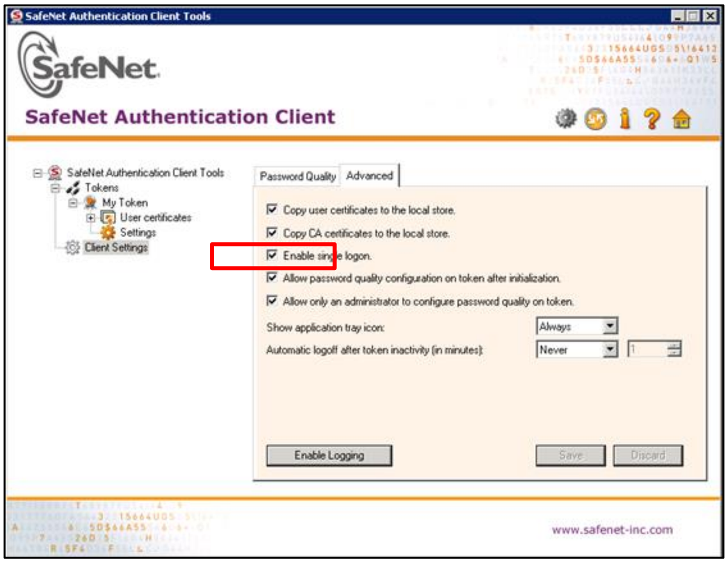
Configuring Smart Card Pass-Through

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, select **SafeNet Authentication Client Tools > Tokens > Client Settings**.
4. In the right pane, click the **Advanced** tab, and then select **Enable single logon**.



☑ Copy user certificates to the local store.

☑ Copy CA certificates to the local store.

☑ Enable single logon.

☑ Allow password quality configuration on token after initialization.

☑ Allow only an administrator to configure password quality on token.

Show application tray icon: Always

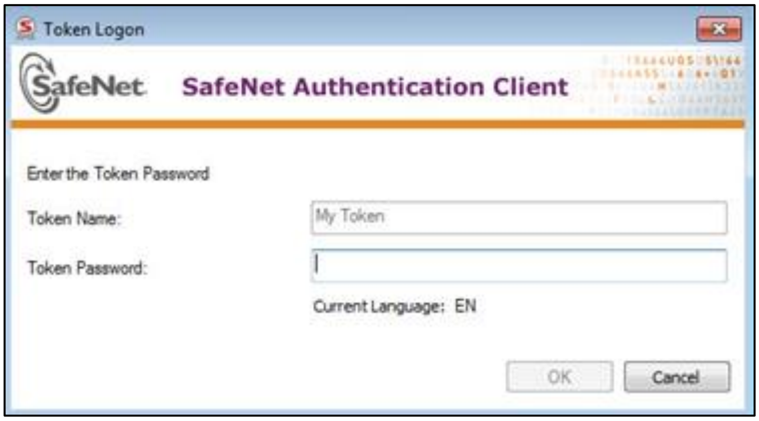
Automatic logoff after token inactivity (in minutes): Never 1

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**.



Token Logon

SafeNet Authentication Client

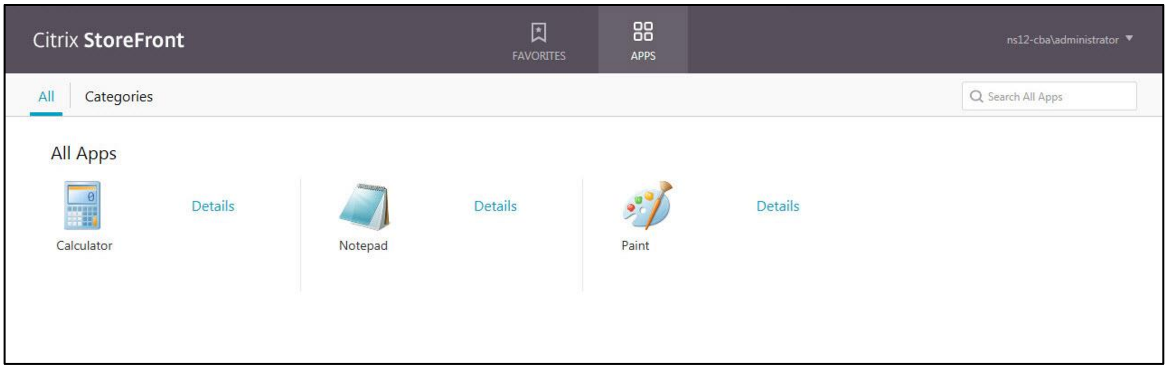
Enter the Token Password

Token Name: My Token

Token Password:

Current Language: EN

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.

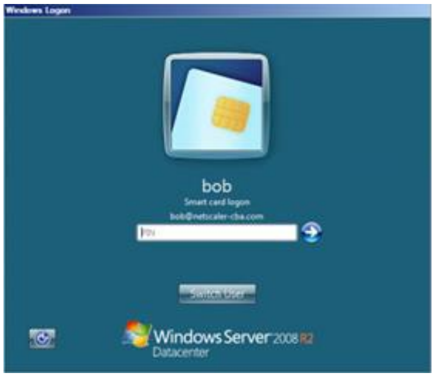


Citrix StoreFront

ns12-cba\administrator

All Apps

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



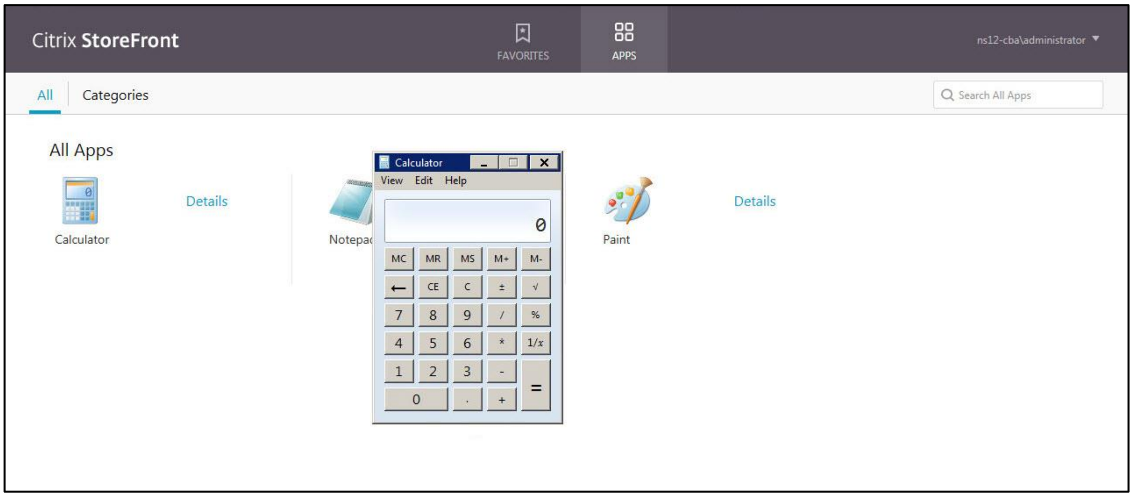
Windows Logon

bob

Smart card logon

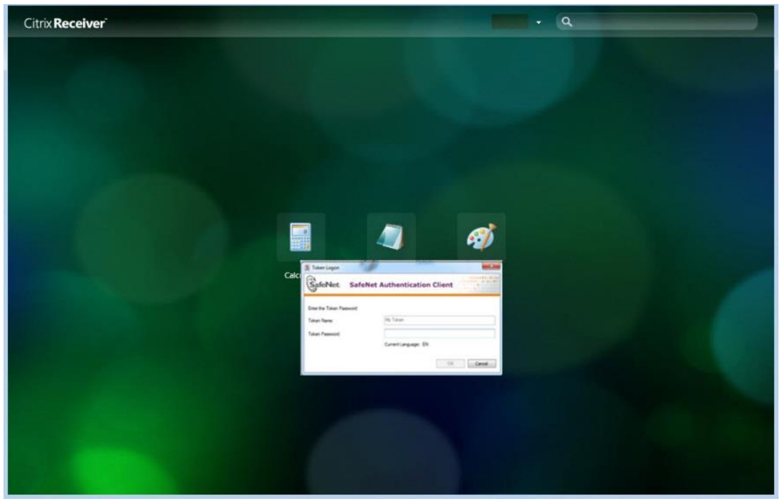
bob@netscaler-cba.com

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



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**.



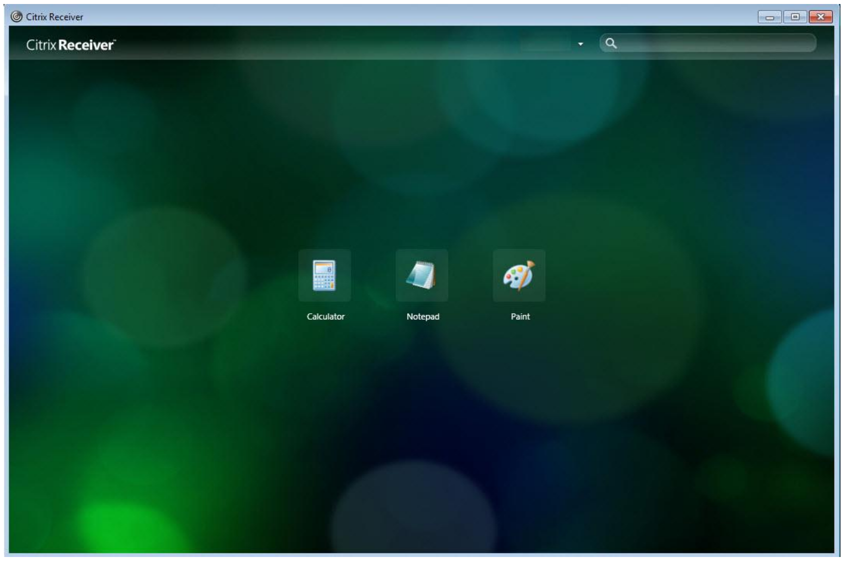
Enter the Token Password

Token Name: My Token

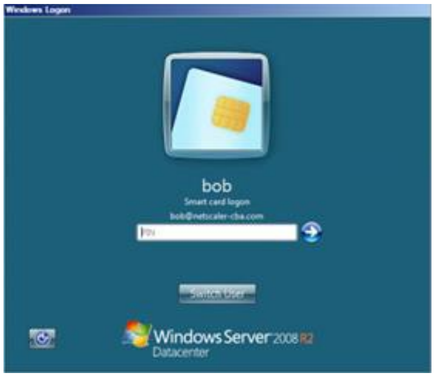
Token Password:

Current Language: EN

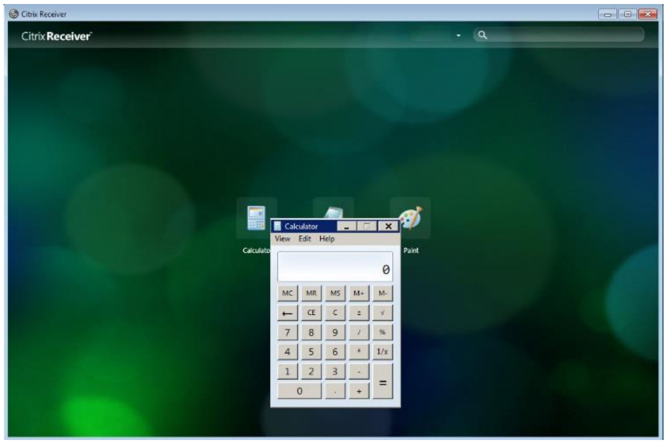
3. After successful authentication, you are redirected to the Citrix StoreFront console. Click on the icon of any of the published applications to launch it.



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



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

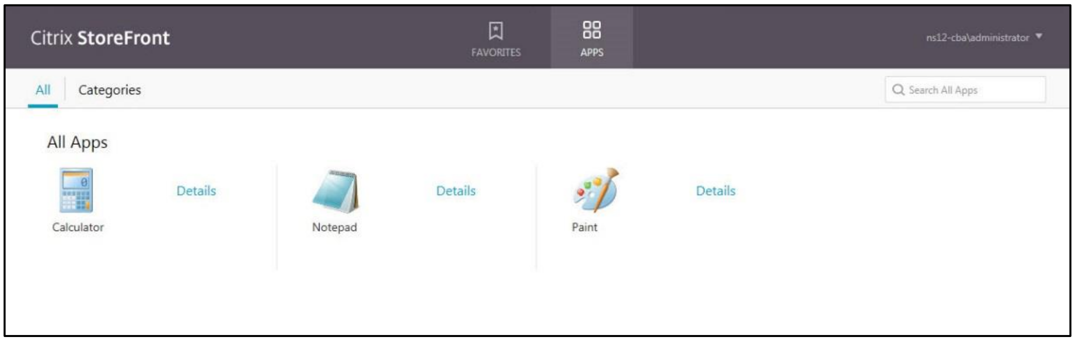


Using SAC CBA with SSO for Citrix Web Access

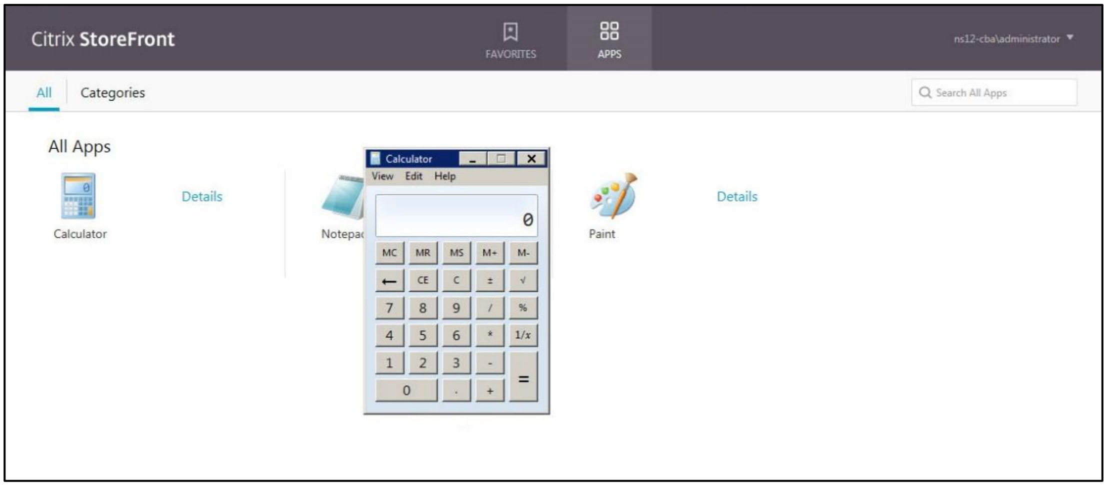
1. Log in to the client machine using the smart card for SSO.

   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.



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

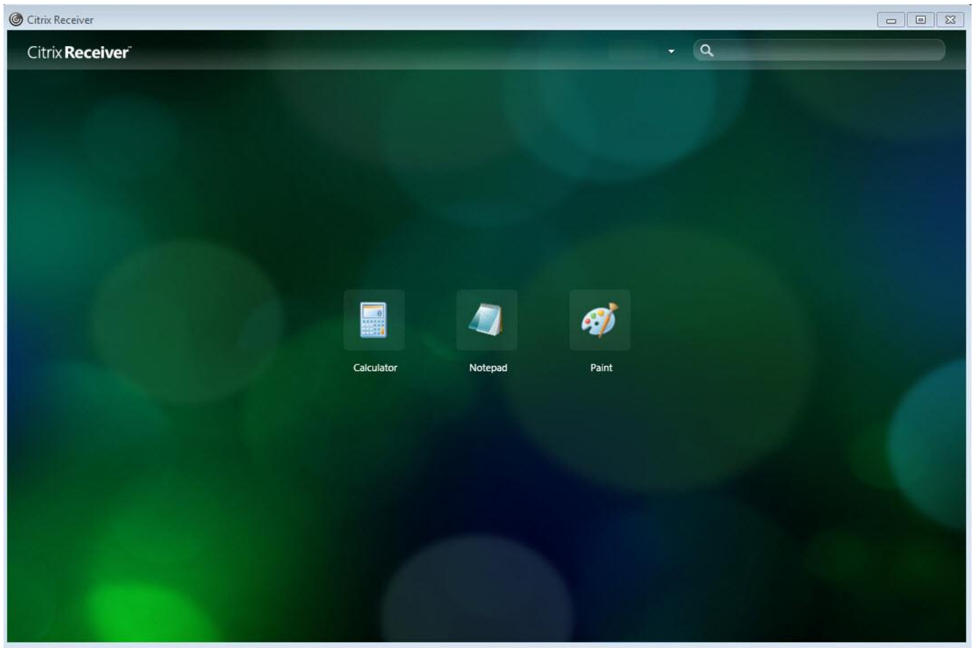


Using SAC CBA with SSO for Citrix Receiver Application Access

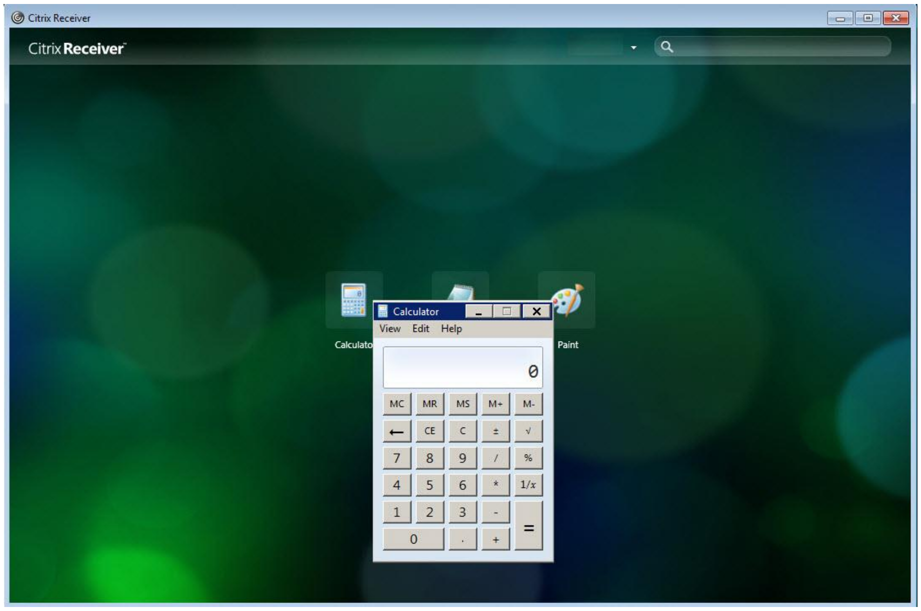
1. Log in to the client machine using the smart card for SSO.

   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.



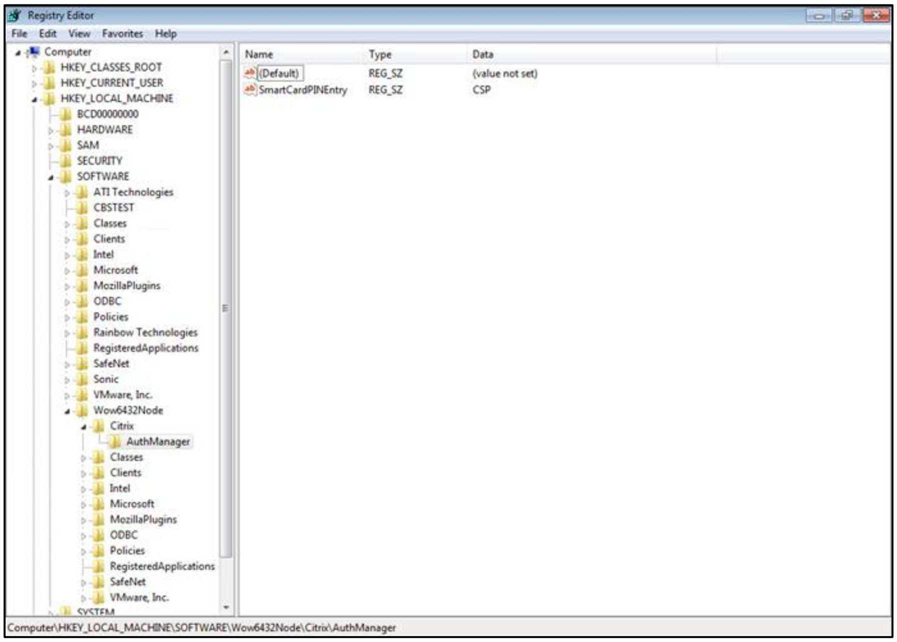
3. Click on the icon of any of the published applications to launch it. The application will open.



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

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

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
SmartCardPINEntry	REG_SZ	CSP

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManager

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
Customer Support Portal	https://supportportal.gemalto.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.
Technical Support contact email	technical.support@gemalto.com