SafeNet Authentication Client

Integration Guide

Using SAC CBA for Citrix XenDesktop/XenApp 7.17

gemalto
security to be free

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.

Document Part Number: 007-000152-001, Rev. A

Release Date: July 2018

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Citrix XenDesktop/XenApp 7.17.

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*.

XenApp is the industry-leading solution for virtual application delivery, providing Windows applications to workers on any device, anywhere. By centralizing control with XenApp, you can provide your team the freedom of mobility, while increasing security and reducing IT costs.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Citrix XenDesktop/XenApp 7.17 using SafeNet tokens.

It is assumed that the Citrix XenDesktop/XenApp 7.17 environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Citrix XenDesktop/XenApp 7.17 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 XenDesktop**
- **Citrix StoreFront**

Environment

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

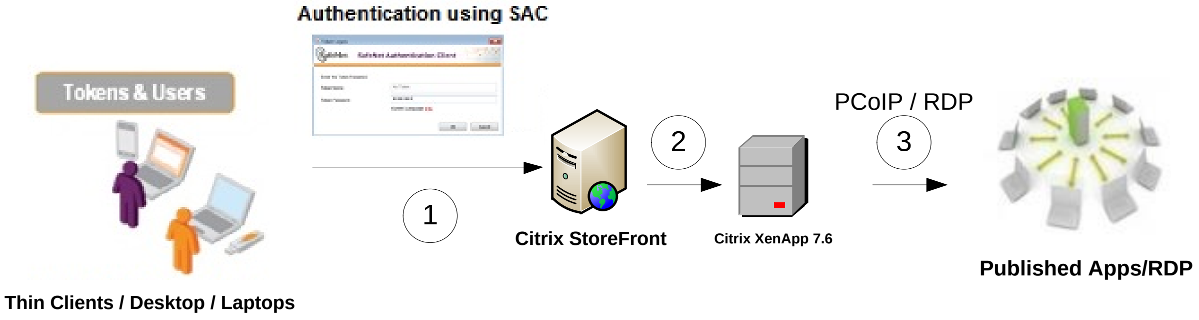
- **SafeNet Authentication Client (SAC)**—Version 10.6
- **Citrix XenDesktop/XenApp**—Version 7.17
- **Citrix StoreFront**—Version 3.14

Audience

This document is targeted to system administrators who are familiar with Citrix XenDesktop/XenApp 7.17, and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

CBA Flow using SAC

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



1. A user attempts to connect to the Citrix XenDesktop/XenApp 7.17 server using the Citrix Receiver or using the StoreFront web portal. 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 the published apps/desktops.
3. The user selects the app/desktop to use.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Citrix XenDesktop/XenApp 7.17 using SafeNet tokens.

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Note that any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, TPO (token policy object) should be configured with a Microsoft CA connector. For additional details, refer to the “Connector for Microsoft CA” section in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token with an appropriate certificate enrolled.
- SafeNet Authentication Client (10.6) should be installed on all client machines.

Supported Tokens in SAC

SAC supports a number of tokens that can be used as second authentication factor for users who authenticate to Citrix XenDesktop/XenApp 7.17.

SafeNet Authentication Client (10.6) 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 B
- Gemalto IDPrime MD 840 B
- Gemalto IDCore 30B

For a full list of supported devices, refer to *SafeNet Authentication Client Customer Release Notes*.

Configuring Citrix XenDesktop/XenApp 7.17

NOTE: XenApp 7.17 and StoreFront 3.14 were installed on the same server in the lab that was prepared to create this guide.

It is assumed that before using the guide, you have Citrix XenApp 7.17 and Citrix StoreFront 3.14 installed and configured with username and password authentication.

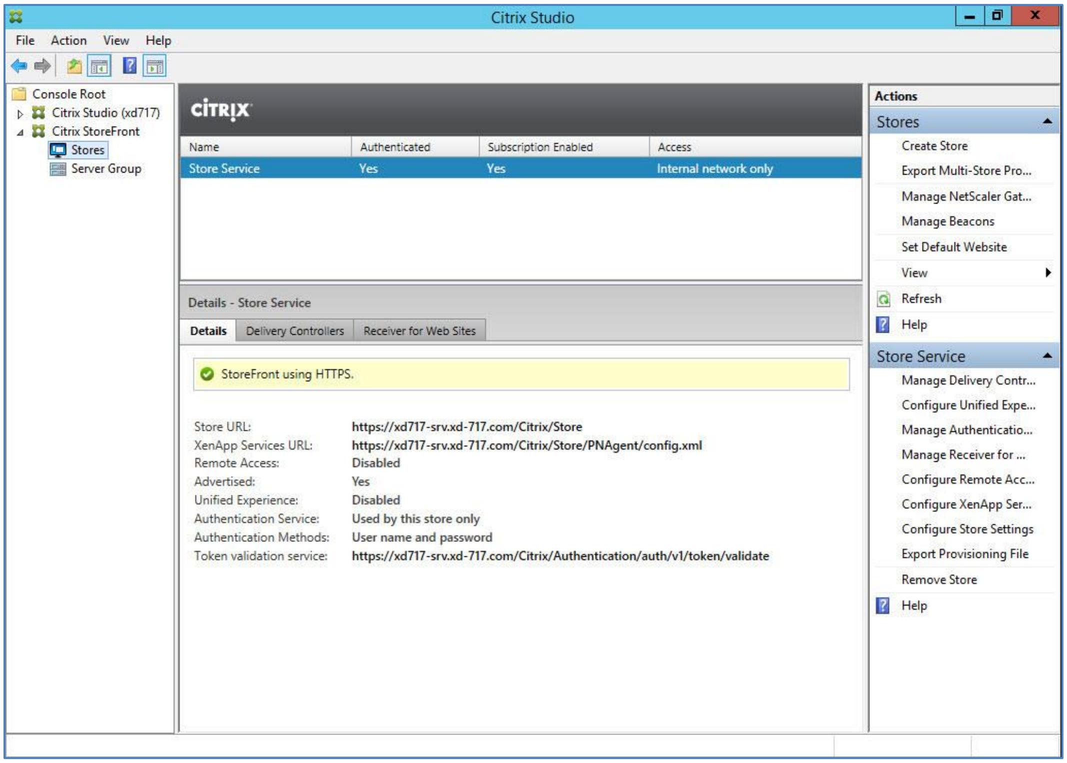
To configure CBA with Citrix XenDesktop/XenApp 7.17, perform the following:

- Configuring Citrix StoreFront Authentication for Citrix Receiver, page 7
- Configuring Citrix StoreFront Authentication for Web Access, page 9

Configuring Citrix StoreFront Authentication for Citrix Receiver

Citrix StoreFront authentication will be used when connecting to XenApp using Citrix Receiver.

1. Open **Citrix Studio.**
2. In the left pane, select **Citrix StoreFront > Stores**.



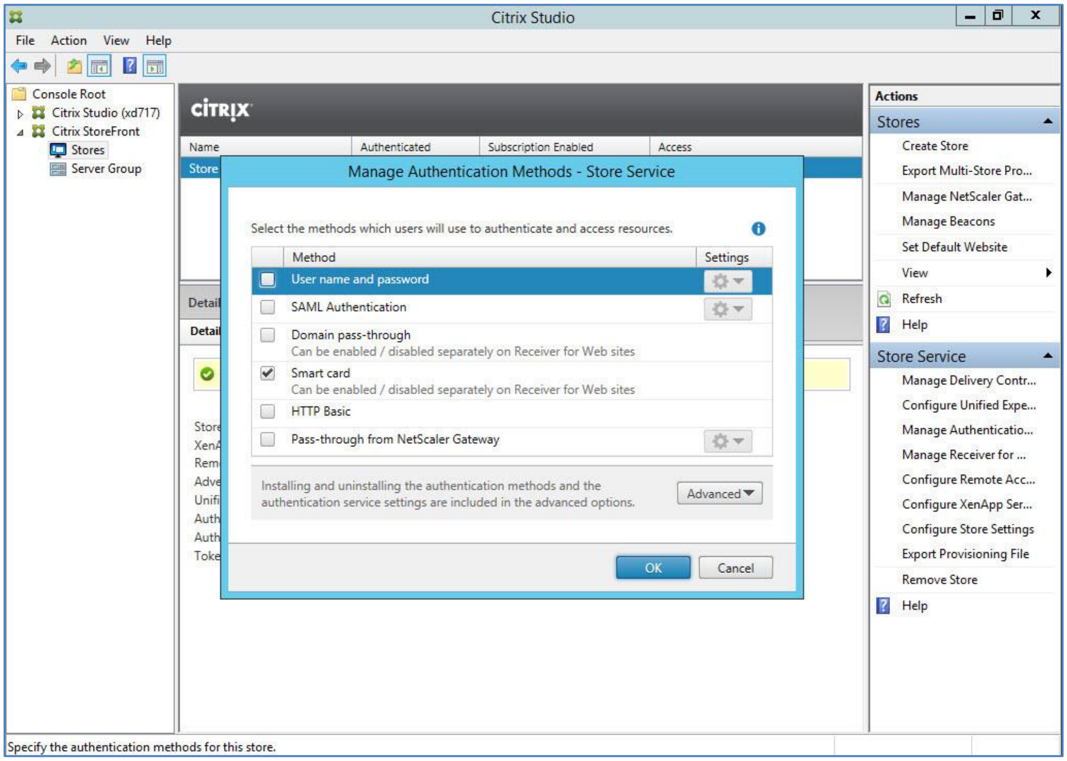
Name	Authenticated	Subscription Enabled	Access
Store Service	Yes	Yes	Internal network only

StoreFront using HTTPS.

Store URL:	https://xd717-srv.xd-717.com/Citrix/Store
XenApp Services URL:	https://xd717-srv.xd-717.com/Citrix/Store/PNAgent/config.xml
Remote Access:	Disabled
Advertised:	Yes
Unified Experience:	Disabled
Authentication Service:	Used by this store only
Authentication Methods:	User name and password
Token validation service:	https://xd717-srv.xd-717.com/Citrix/Authentication/auth/v1/token/validate

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

3. In the **Store Service** pane, select **Manage Authentication**.
4. In the **Manage Authentication Methods** window, select **Smart card**, and then click **OK**.



Manage Authentication Methods - Store Service

Select the methods which users will use to authenticate and access resources.

	Method	Settings
□	User name and password	
□	SAML Authentication	
□	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
☑	Smart card Can be enabled / disabled separately on Receiver for Web sites	
□	HTTP Basic	
□	Pass-through from NetScaler Gateway	

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

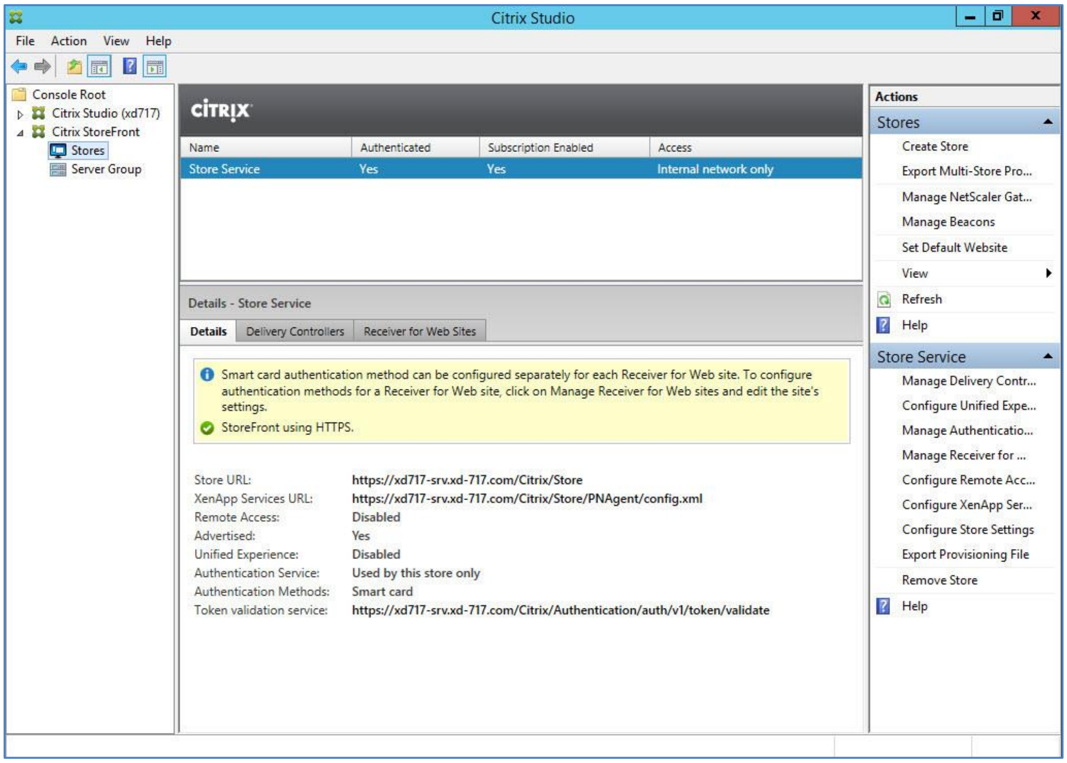
Specify the authentication methods for this store.

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

Configuring Citrix StoreFront Authentication for Web Access

Configure the Receiver to use CBA for web access.

1. Open **Citrix Studio**.
2. Select **Citrix StoreFront > Stores.**



Name	Authenticated	Subscription Enabled	Access
Store Service	Yes	Yes	Internal network only

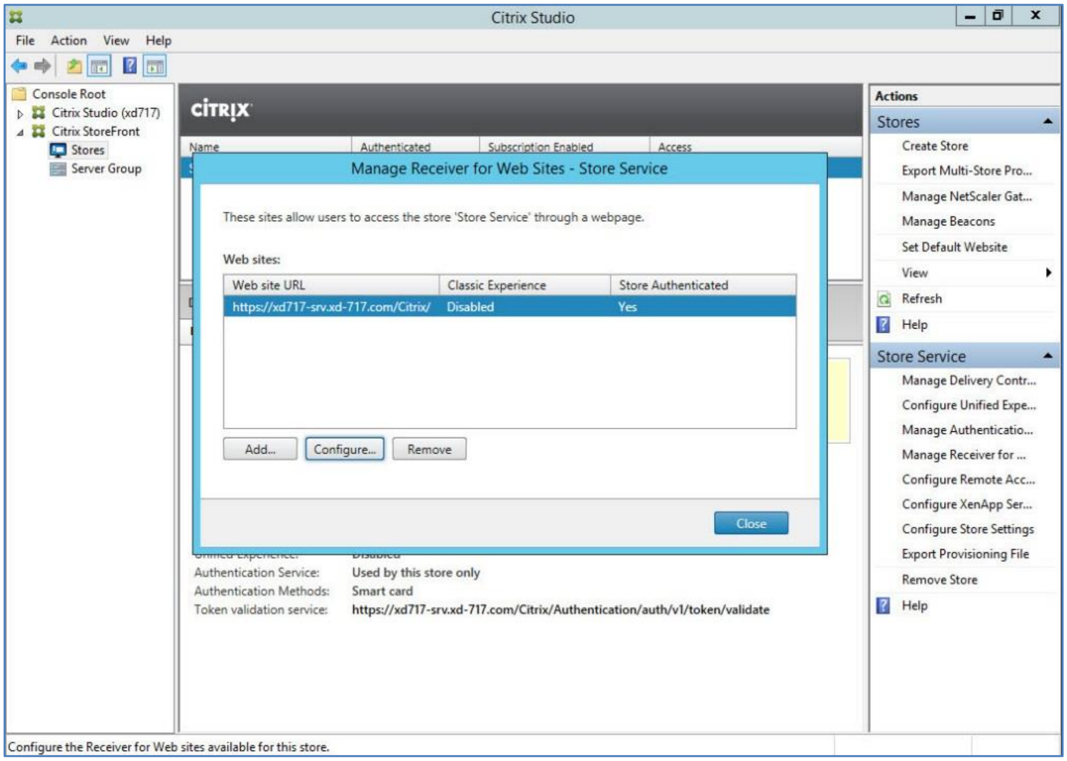
Smart card authentication method can be configured separately for each Receiver for Web site. To configure authentication methods for a Receiver for Web site, click on Manage Receiver for Web sites and edit the site's settings.

StoreFront using HTTPS.

Store URL:	https://xd717-srv.xd-717.com/Citrix/Store
XenApp Services URL:	https://xd717-srv.xd-717.com/Citrix/Store/PNAgent/config.xml
Remote Access:	Disabled
Advertised:	Yes
Unified Experience:	Disabled
Authentication Service:	Used by this store only
Authentication Methods:	Smart card
Token validation service:	https://xd717-srv.xd-717.com/Citrix/Authentication/auth/v1/token/validate

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

3. In the **Store Service** pane, select **Manage Receiver for Web Sites**. The **Manage Receiver for Web Sites** window opens



Manage Receiver for Web Sites - Store Service

These sites allow users to access the store 'Store Service' through a webpage.

Web sites:

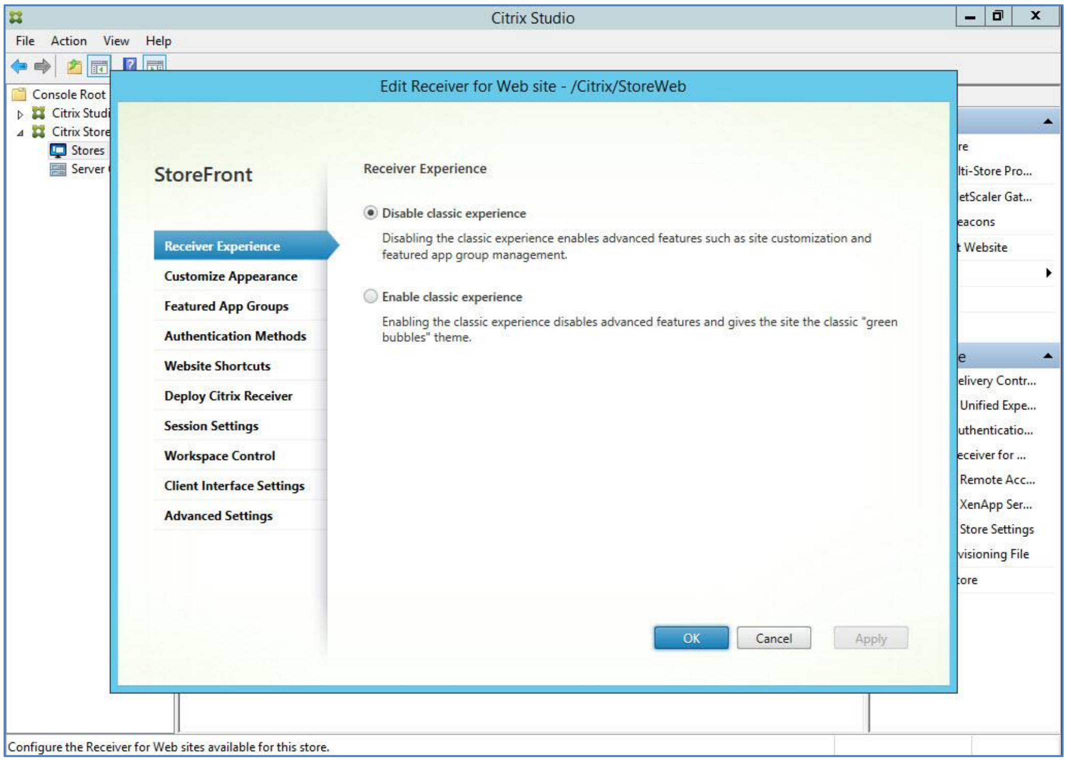
Web site URL	Classic Experience	Store Authenticated
https://xd717-srv.xd-717.com/Citrix/	Disabled	Yes

Unified Experience: Disabled
Authentication Service: Used by this store only
Authentication Methods: Smart card
Token validation service: https://xd717-srv.xd-717.com/Citrix/Authentication/auth/v1/token/validate

Configure the Receiver for Web sites available for this store.

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

4. Select the web site and press **Configure**. The **Edit Receiver for Web site** window opens.



Edit Receiver for Web site - /Citrix/StoreWeb

Receiver Experience

● Disable classic experience

Disabling the classic experience enables advanced features such as site customization and featured app group management.

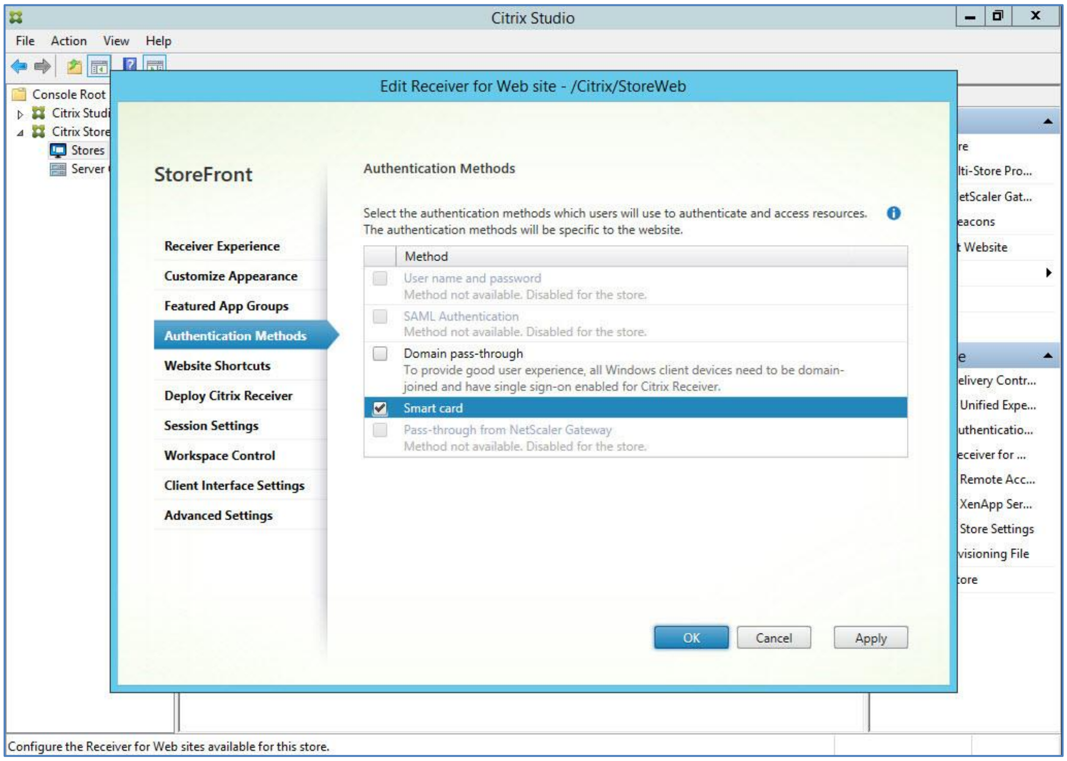
○ Enable classic experience

Enabling the classic experience disables advanced features and gives the site the classic "green bubbles" theme.

Configure the Receiver for Web sites available for this store.

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

5. Select **Authentication Modes**. Select **Smart card** and press **OK**.



Authentication Methods

Select the authentication methods which users will use to authenticate and access resources.
The authentication methods will be specific to the website.

	Method
□	User name and password Method not available. Disabled for the store.
□	SAML Authentication Method not available. Disabled for the store.
□	Domain pass-through To provide good user experience, all Windows client devices need to be domain-joined and have single sign-on enabled for Citrix Receiver.
☑	Smart card
□	Pass-through from NetScaler Gateway Method not available. Disabled for the store.

Configure the Receiver for Web sites available for this store.

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

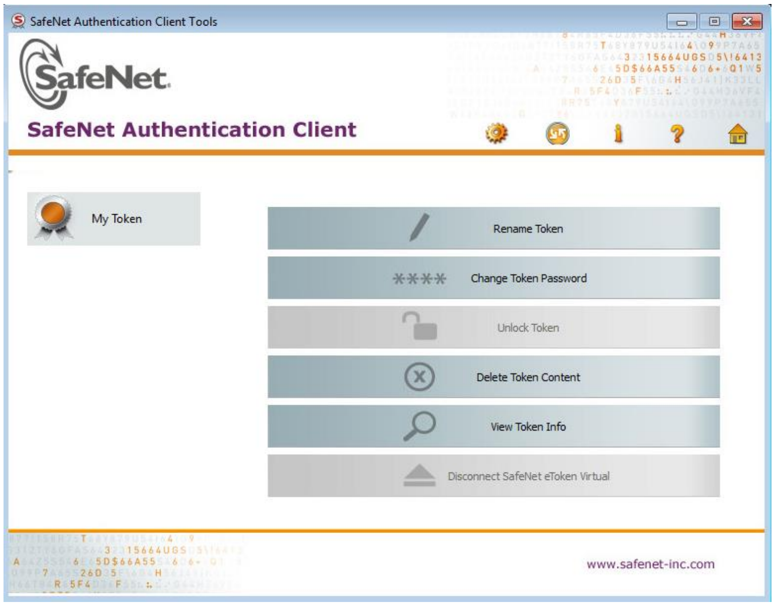
Configuring Citrix StoreFront 3.14 to Use Smart Card Pass-through Authentication

Complete the procedures in this section to configure Citrix StoreFront to use smart card pass-through authentication.

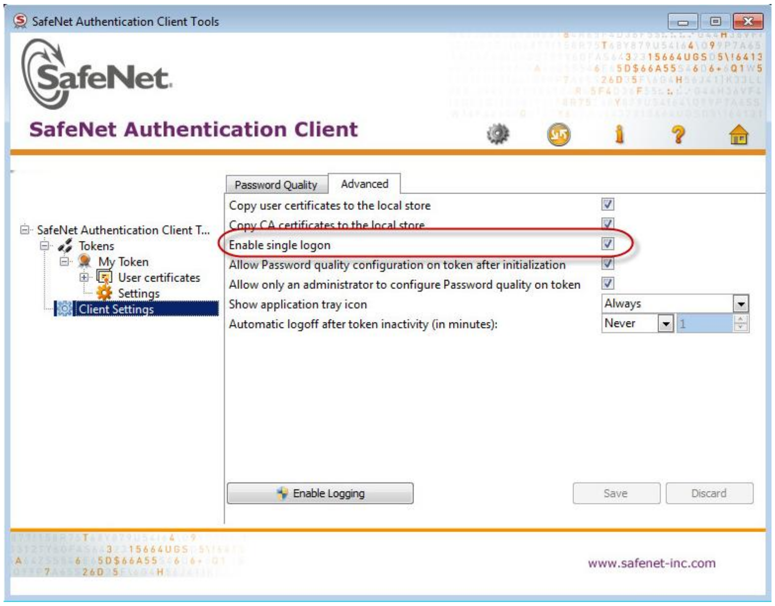
Configuring SafeNet Authentication Client

Enable single log on in SafeNet Authentication Client.

1. Open the **SafeNet Authentication Client** console.



2. Click the **Advanced View** icon ⚙ , click **Client Settings**, and then click the **Advanced** tab.
3. Select **Enable single logon**, and the click **Save**.



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

4. From the Windows **Start** menu, select **Run**, and then type **regedit.exe**, to open the Windows Registry Editor.

5. Complete the following steps:

   a. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC**, create a new key, and name it **General**.

   b. In the new key, create a new DWORD (32-bit), name it **SingleLogon**, and specify a value of **1**.

   c. Exit the Windows Registry.

Configuring the StoreFront 3.14 Server

Configure the **default.ica** file on the IIS.

1. Open the **default.ica** file with a text editor. (This file is typically located in C:\inetpub\wwwroot\Citrix\<Store_Name>\App_Data\.)

2. In the **[Application]** section, add the following setting: **DisableCtrlAltDel=Off**

3. Save the file.

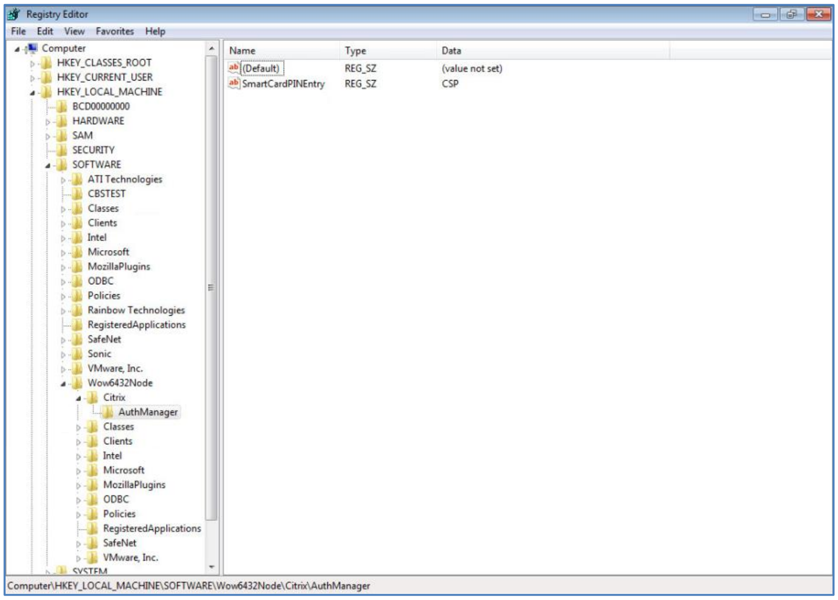
For more information, go to:

http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-configure-conf-smartcard.html

Changing the CSP PIN Prompt from the Citrix Default to SafeNet Authentication Client

To change the Citrix default CBA PIN prompt to SAC, do the following on the client machine:

1. On the client machine, from the Windows **Start** menu, select **Run**, and then type **regedit.exe**, to open the Windows Registry Editor.
2. Add the following key value to the registry key: **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

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

Configuring Citrix Receiver for Single Sign-On

We recommend reading the following document for Citrix Receiver Single Sign-On (SSO) configuration:

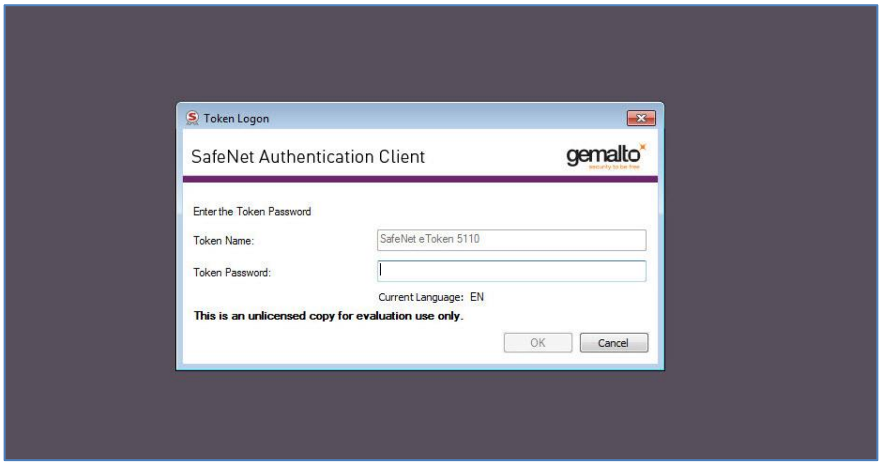
http://support.citrix.com/article/CTX133982

Running the Solution

Check the final running solution of Citrix XenDesktop/XenApp 7.17 with SafeNet Authentication Client. In this solution, SafeNet eToken 5100 is used.

CBA using Citrix Receiver for Web Access

1. Open a web browser and type the **Citrix Receiver for Web** URL.
2. The **SafeNet Authentication Client** opens. Enter the **Token Password**, and then click **OK**.



Enter the Token Password

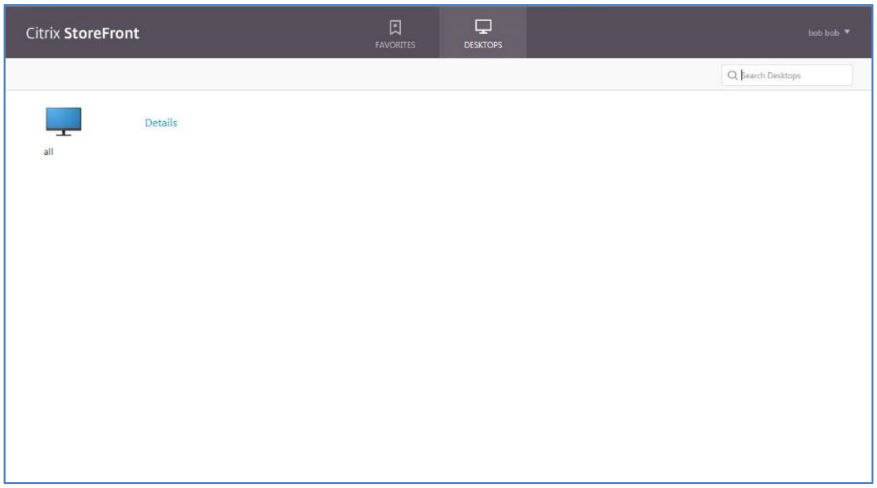
Token Name: SafeNet eToken 5110

Token Password:

Current Language: EN

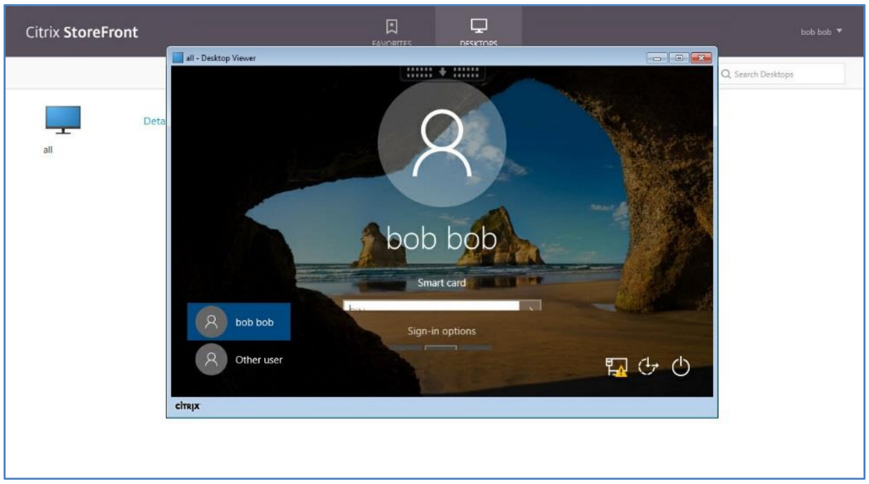
This is an unlicensed copy for evaluation use only.

After a successful authentication, you are granted access to the Citrix StoreFront web portal, and can now access the applications.



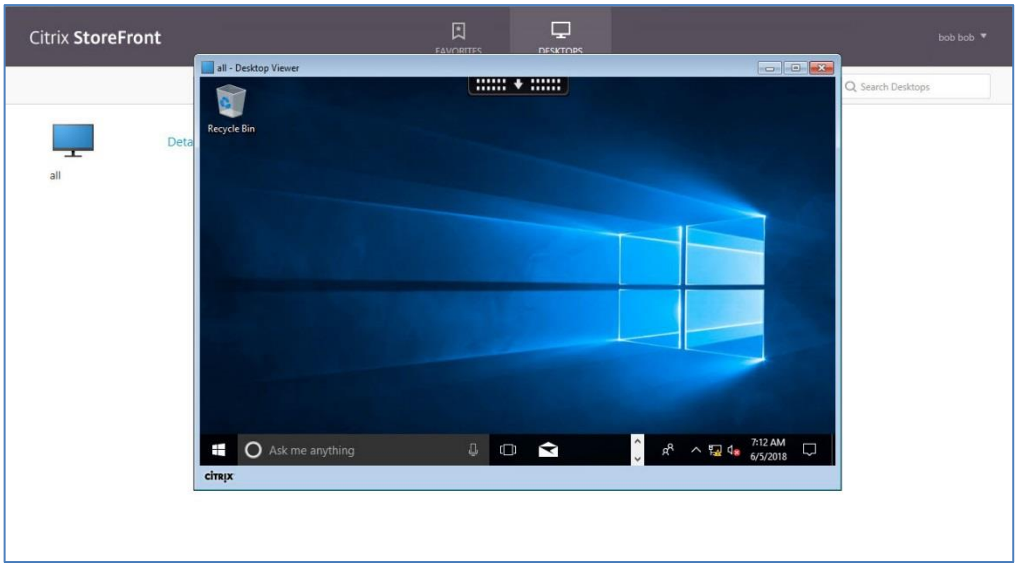
(The screen image above is from Citrix®. Trademarks are the property of their respective owners).

3. Click on a published desktop. The **Windows Login** window is displayed.



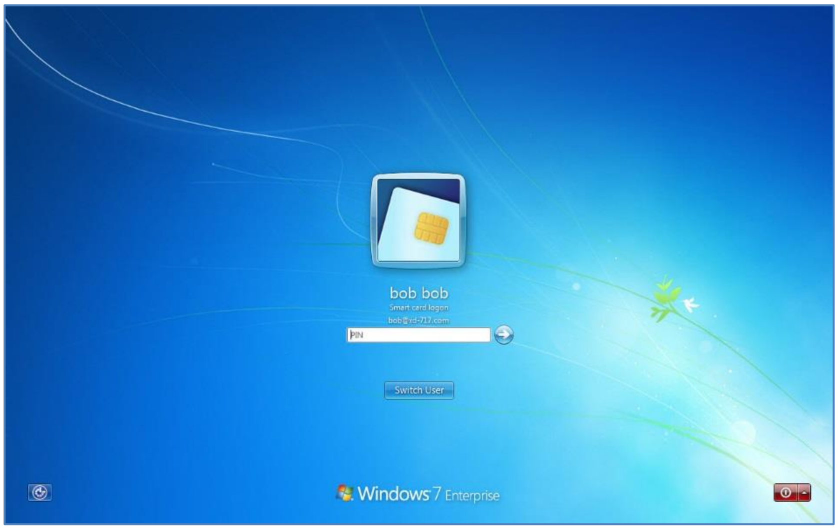
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

4. Enter your smart card PIN to login. After successful authentication, the user is logged in.



CBA Pass-through using Citrix Receiver for Web Access

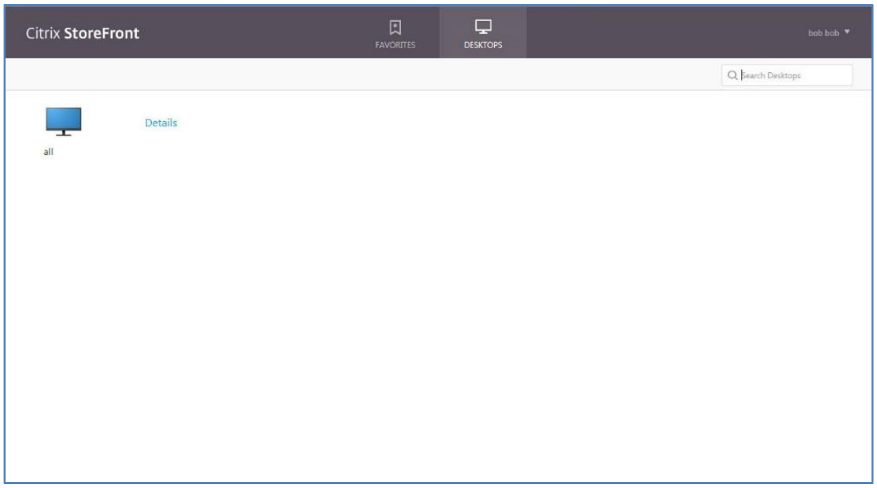
1. Login to the client machine using **Smart card logon**.



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

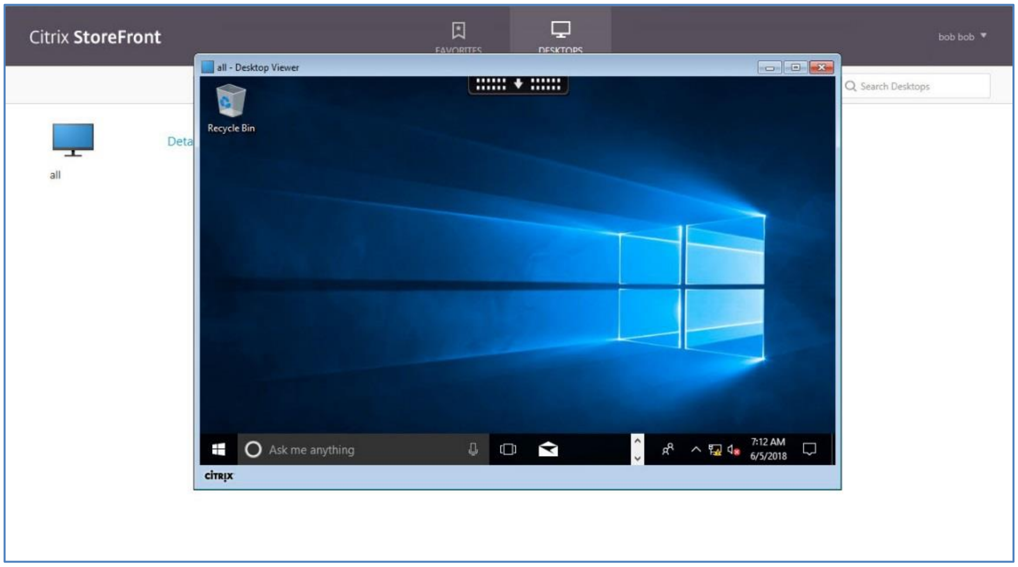
2. Open a web browser and type the **Citrix Receiver for Web** URL.

   Since Citrix is configured for pass-through authentication, the user is not required to enter the smart card PIN code, and is automatically logged in to the Citrix StoreFront web portal.



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

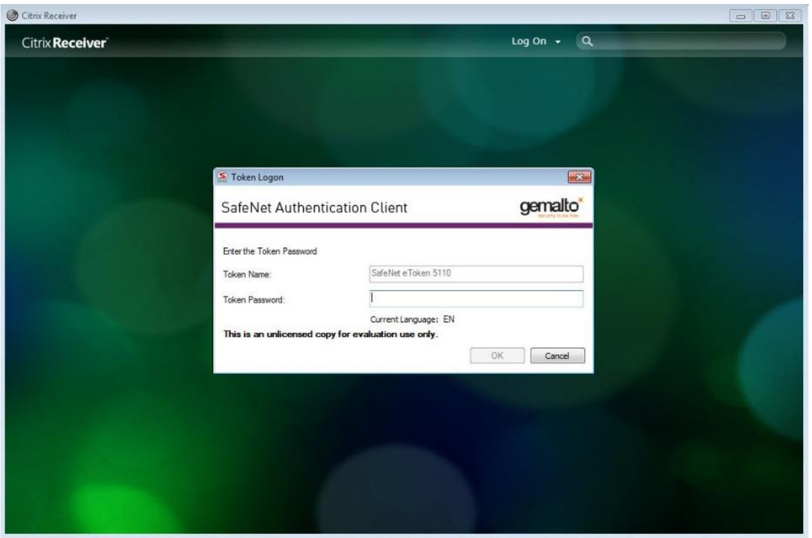
3. Click the VDI icon. Since Citrix is configured for pass-through authentication, the connection will be open without requiring the user to authenticate again.



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

CBA Using Citrix Receiver

1. Insert the selected SafeNet eToken or smartcard.
2. Open Citrix Receiver. The **SafeNet Authentication Client** opens. Enter the **Token Password**, and then click **OK.**



Enter the Token Password

Token Name: SafeNet eToken 5110

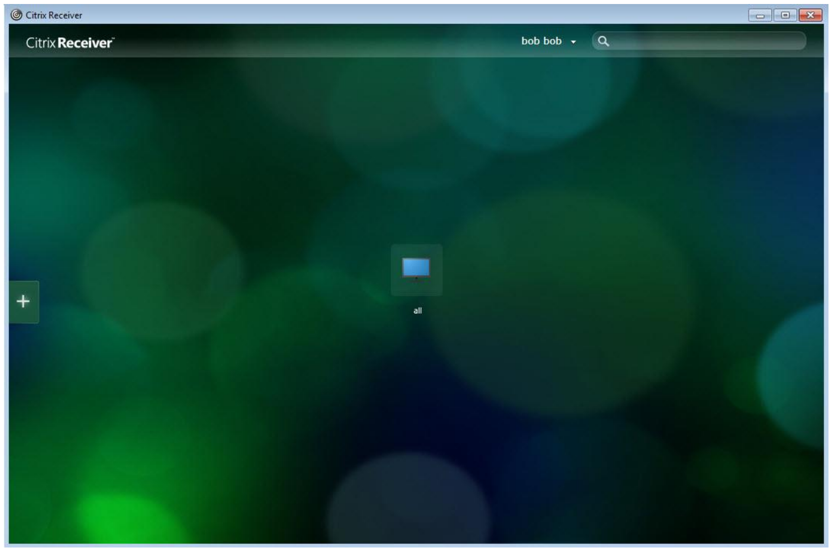
Token Password:

Current Language: EN

This is an unlicensed copy for evaluation use only.

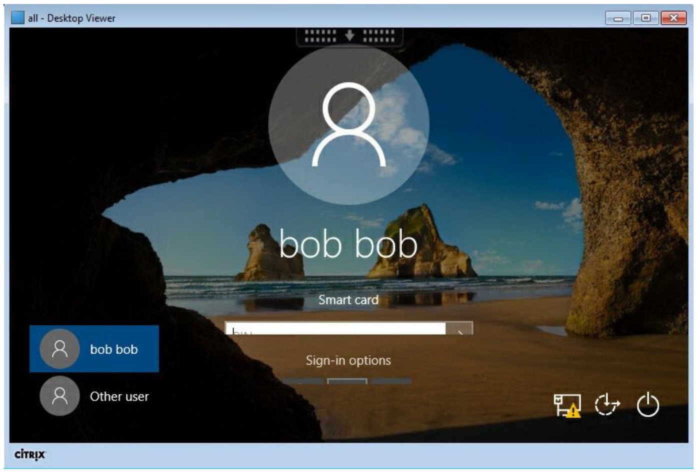
(The screen image above is from Citrix®. Trademarks are the property of their respective owners).

After a successful authentication, the Citrix Receiver application window is displayed.



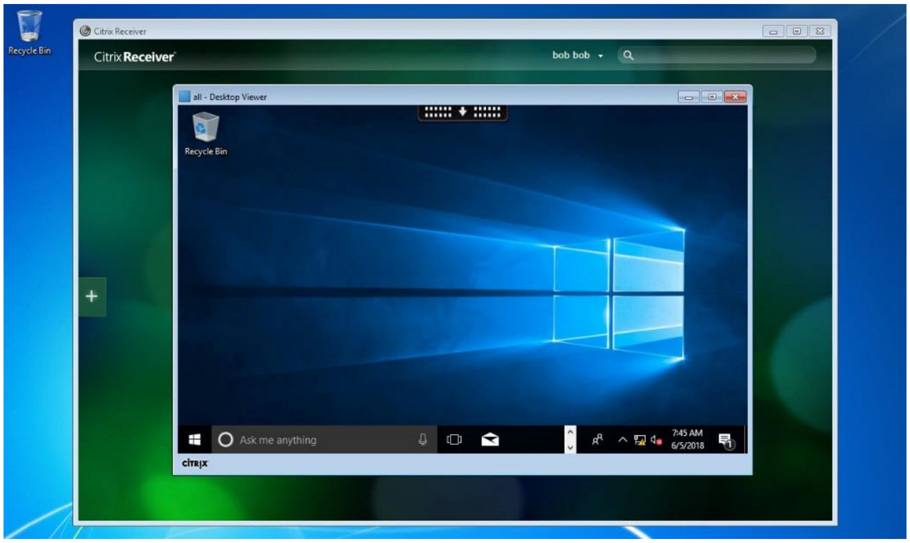
(The screen image above is from Citrix®. Trademarks are the property of their respective owners).

3. Select the VDI to open. The Windows Login window is displayed.



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

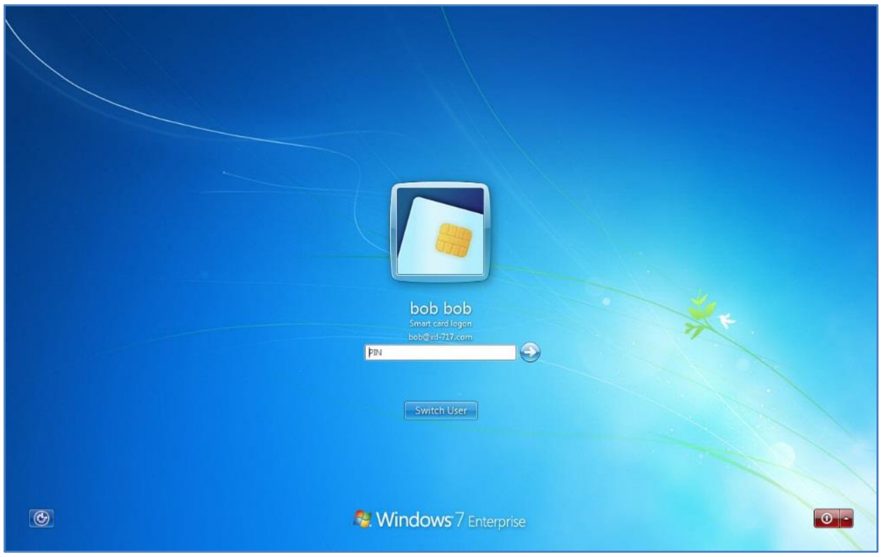
4. Click Smart card logon, and then enter your smart card PIN. After a successful authentication the user is logged in to the VDI.



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

CBA Pass-through using Citrix Receiver

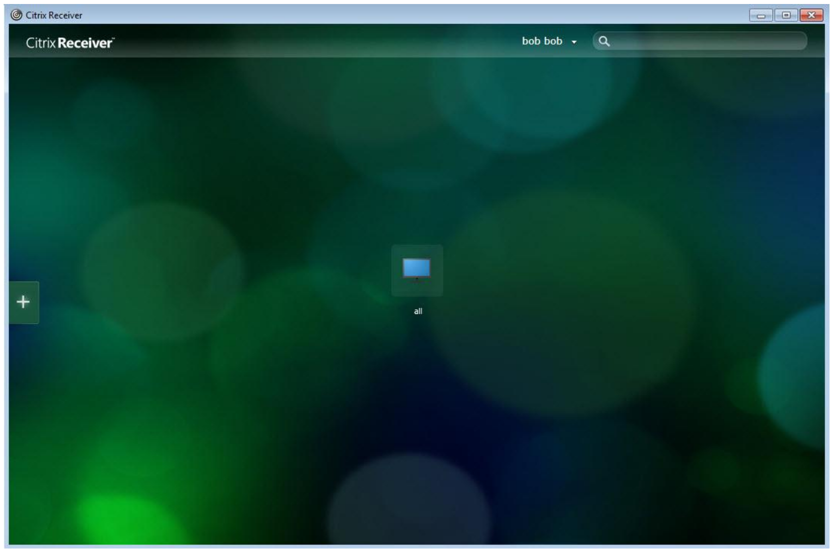
1. Log in to the Windows client workstation using **Smart card logon**.



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

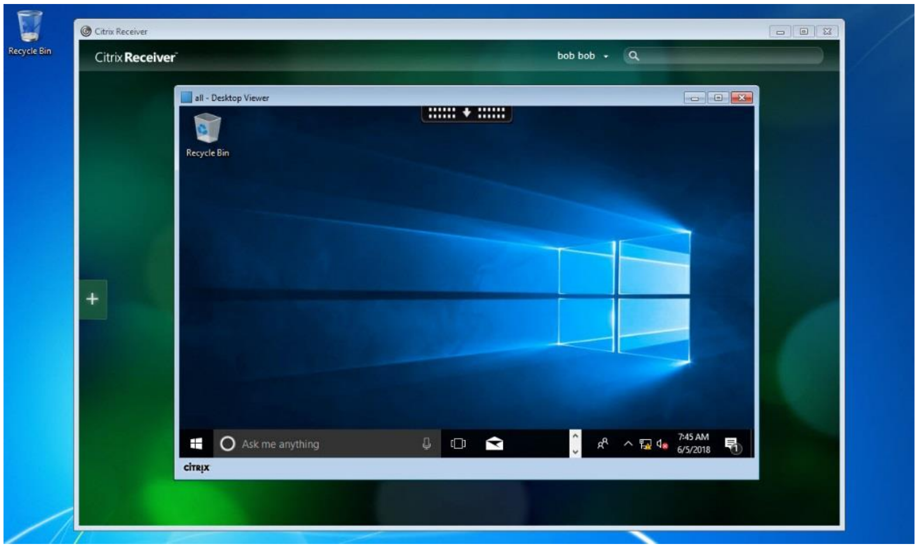
2. After successful authentication using the smart card logon certificate open the Citrix Receiver application.

   Since the Citrix is configured for pass-through authentication, the user is not required to enter the smart card PIN code, and is automatically logged in to the Citrix Receiver.



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

3. Select the VDI to use. Since Citrix is configured for pass-through authentication, the connection will open without requiring you to authenticate again.



(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, refer to 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support via email at technical.support@gemalto.com.