

SafeNet Authentication Client Integration Guide

Using SAC CBA for Citrix XenDesktop 7.6

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: 007-013237-001, Rev. B

Release Date: January 2016

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	5
Environment.....	5
Audience	5
CBA Flow using SAC	6
Prerequisites	6
Supported Tokens in SAC	7
Certificate-based USB Tokens	7
Smart Cards	7
Certificate-based Hybrid USB Tokens	7
Software Tokens	7
Configuring Citrix XenDesktop 7.6.....	8
Configuring a Smart Card for the Citrix Receiver.....	8
Configuring a Smart Card for the StoreFront Receiver for Web	9
Configuring Citrix StoreFront 2.6 to Use Smart Card Pass-through Authentication.....	10
Configuring SafeNet Authentication Client.....	10
Configuring the StoreFront 2.6 Server	11
Changing the CSP PIN Prompt from the Citrix Default to SafeNet Authentication Client	11
Running the Solution	12
CBA using Citrix Receiver for Web Access.....	12
CBA Pass-through using Citrix Receiver for Web Access	15
CBA using Citrix Receiver	16
CBA Pass-through using Citrix Receiver	18
Support Contacts	20

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Citrix XenDesktop 7.6.

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 XenDesktop delivers Windows applications and desktops as secure mobile services. With XenDesktop, IT can mobilize the business, while reducing costs by centralizing control and security for intellectual property.

The XenDesktop installation installs the following components:

- **Citrix StoreFront**—Citrix StoreFront replaces the Citrix Web Interface and supplies web access to the XenDesktop machines. Additional information on using StoreFront can be found at the following link: <http://blogs.citrix.com/2013/09/09/web-interface-or-storefront/>
- **Citrix Studio**—Citrix Studio provides a management interface to Citrix XenDesktop and Citrix StoreFront.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Citrix XenDesktop 7.6 using SafeNet tokens.

It is assumed that the Citrix XenDesktop 7.6 environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Citrix XenDesktop 7.6 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 7.6**

Environment

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

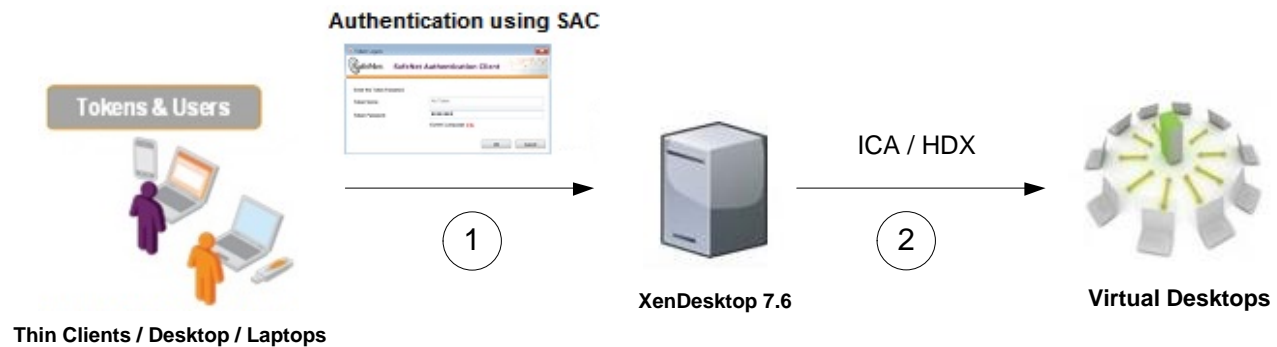
- **SafeNet Authentication Client (SAC)**—Version 9.0
- **Citrix XenDesktop 7.6**
- **Citrix StoreFront 2.6**

Audience

This document is targeted to system administrators who are familiar with Citrix XenDesktop 7.6, 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 7.6 server using the Citrix Receiver or via the StoreFront Receiver for Web. 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 XenDesktop 7.6 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 enrolled with an appropriate certificate.
- SafeNet Authentication Client (SAC 9.0) 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 7.6.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

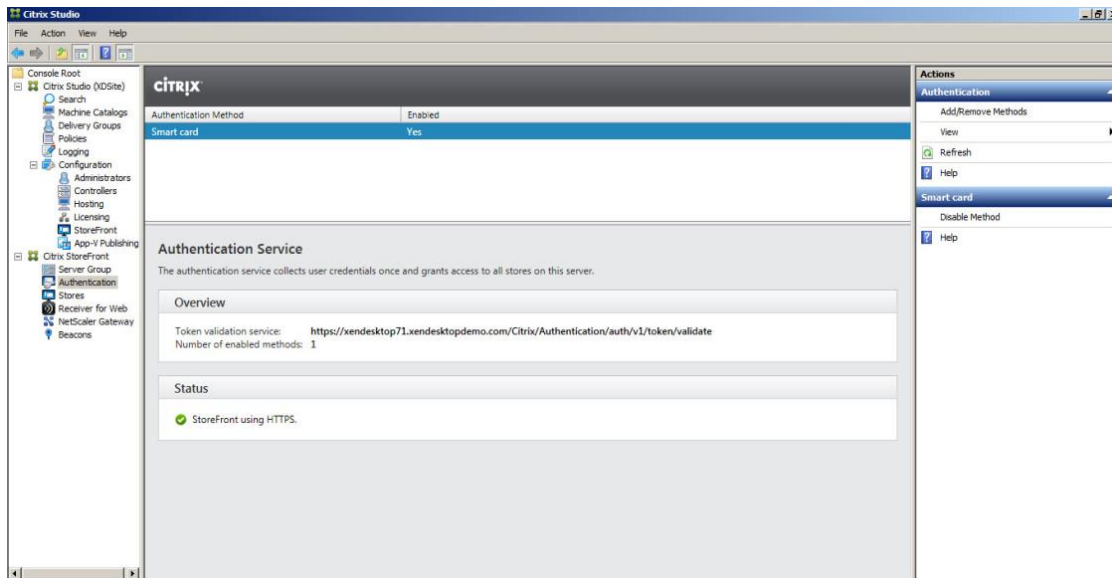
- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring Citrix XenDesktop 7.6

In this section, you will configure the various Citrix components to work with certificate-based authentication. Configure the authentication method to **Smart Card**. With this configuration method, the user will be required to enter a smart card PIN/password when logging in to the XenDesktop published machine.

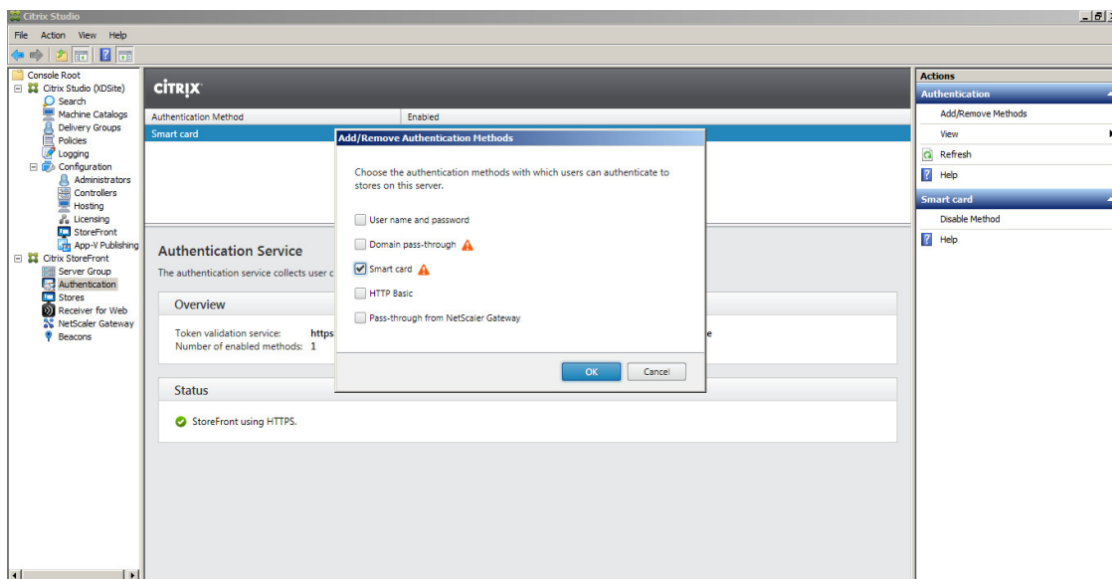
Configuring a Smart Card for the Citrix Receiver

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



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

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

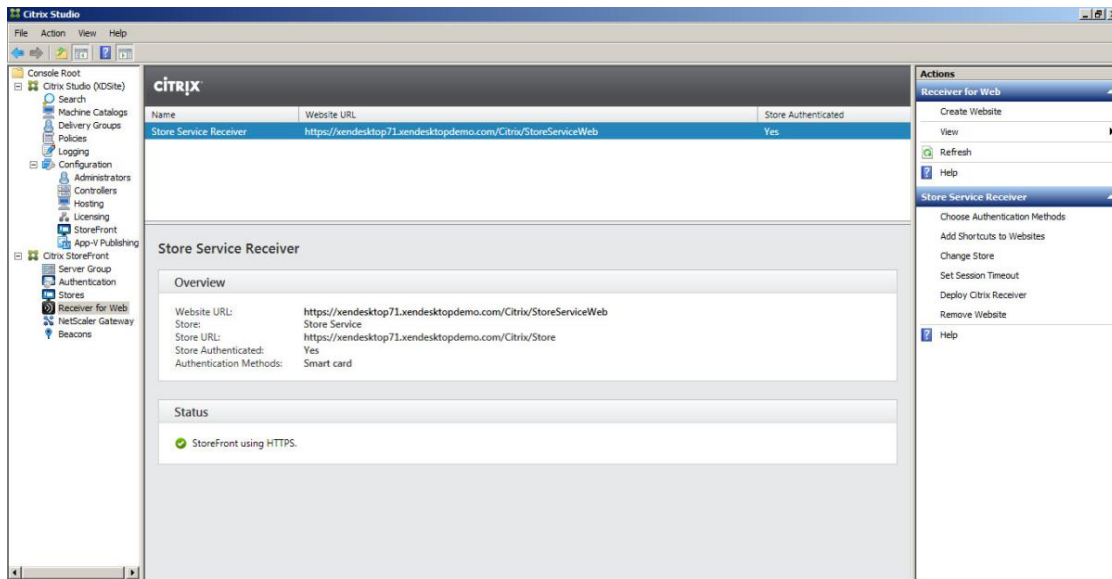


(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

4. On the **Add/Remove Authentication Methods** window, select **Smart card**, and then click **OK**.

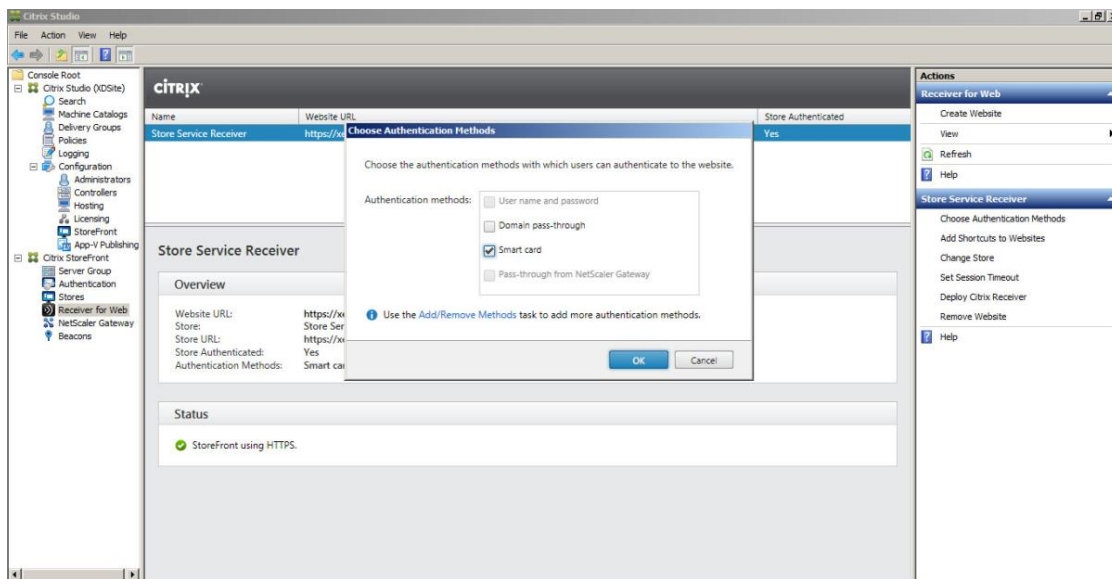
Configuring a Smart Card for the StoreFront Receiver for Web

1. In the left pane, select **Citrix StoreFront > Receiver for Web**.



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

2. In the right pane, click **Choose Authentication Methods**.



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

3. On the **Choose Authentication Methods** window, select **Smart card**, and then click **OK**.

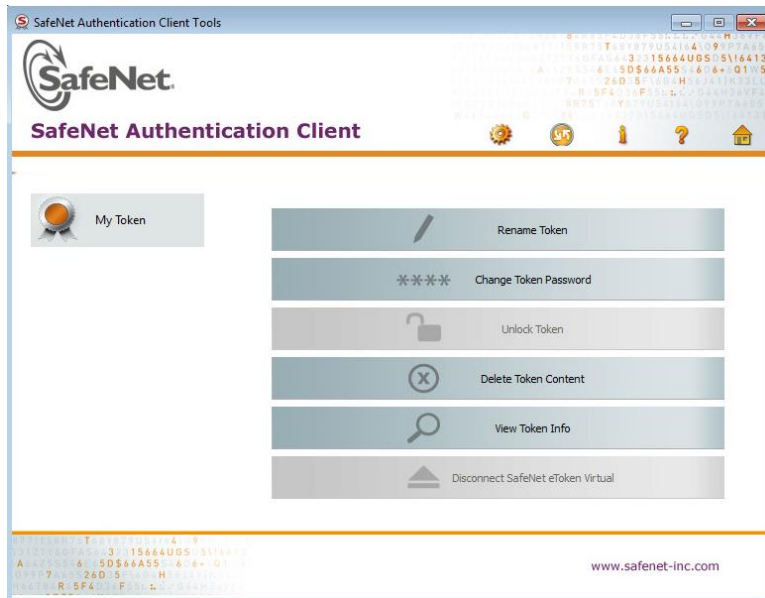
Configuring Citrix StoreFront 2.6 to Use Smart Card Pass-through Authentication


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

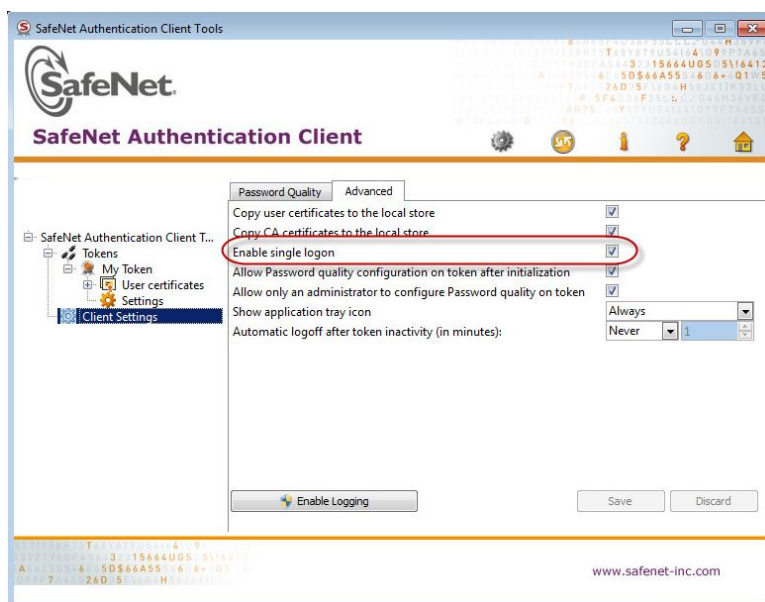
Configuring SafeNet Authentication Client

Enable single logon 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 then click **Save**.



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 2.6 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\\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

Change the Citrix default CSP dialog PIN prompt to use SAC.

1. On the client machine where the Citrix Receiver is installed, from the Windows **Start** menu, select **Run**, and then type **regedit.exe** to open the Windows Registry Editor.
2. Complete the following steps:
 - a. Go to **HKLM\Software\[Wow6432Node]\Citrix\AuthManager**, and add the following key value:
SmartCardPINEntry=CSP
 - b. Exit the Windows Registry.

For more information, go to:

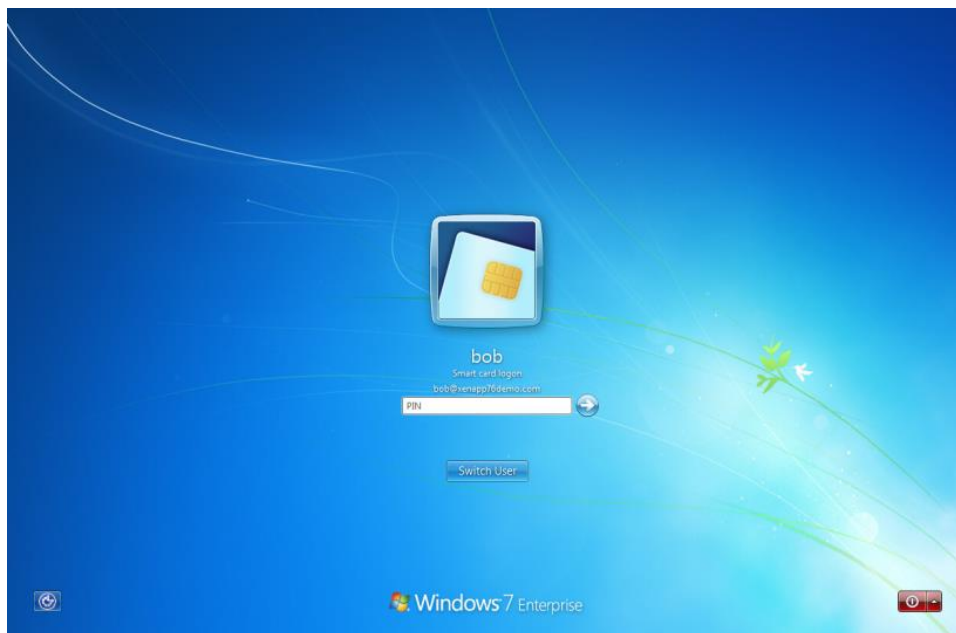
<http://support.citrix.com/proddocs/topic/receiver-windows-40/receiver-windows-smart-card-cfg.html>

Running the Solution

Check the final running solution of Citrix XenApp 7.6 and StoreFront 2.6 with SafeNet Authentication Client. In this solution, SafeNet eToken 5100 is used.

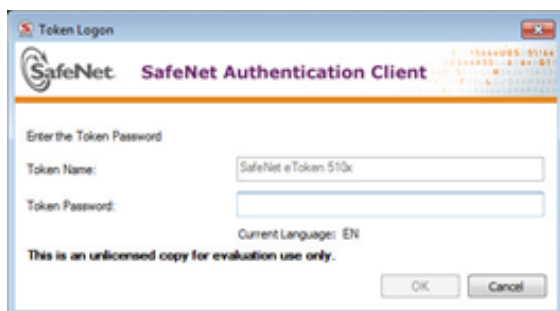
CBA using Citrix Receiver for Web Access

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

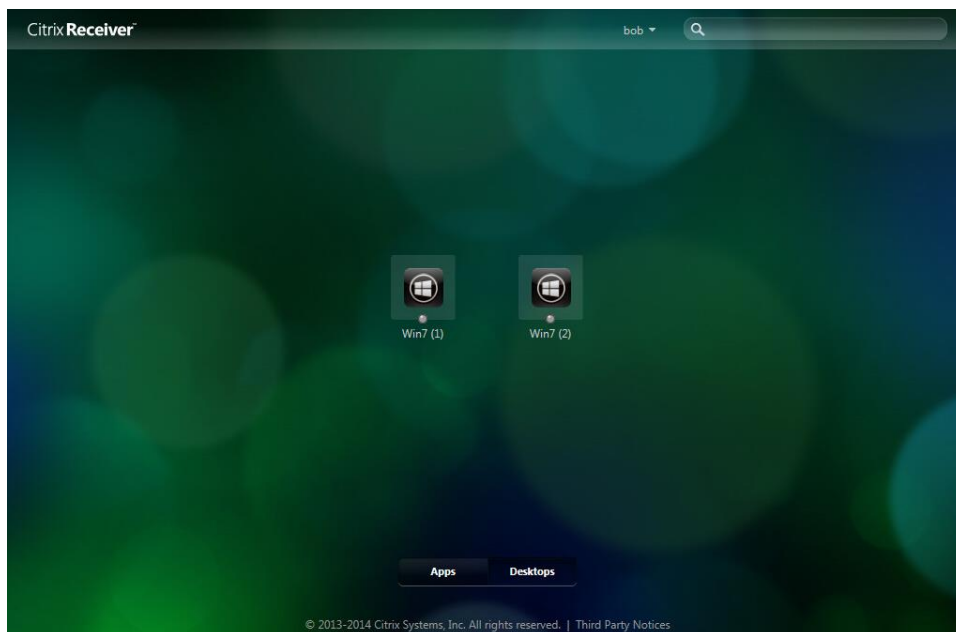


(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

2. Open a web browser and type the **StoreFront Web Receiver** URL.
3. The **SafeNet Authentication Client** login window is displayed. Enter the **Token Password**, and then click **OK**.



After a successful authentication, you are granted access to the StoreFront Web Receiver application.



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

4. Select a machine to use. The **Windows Login** window is displayed.



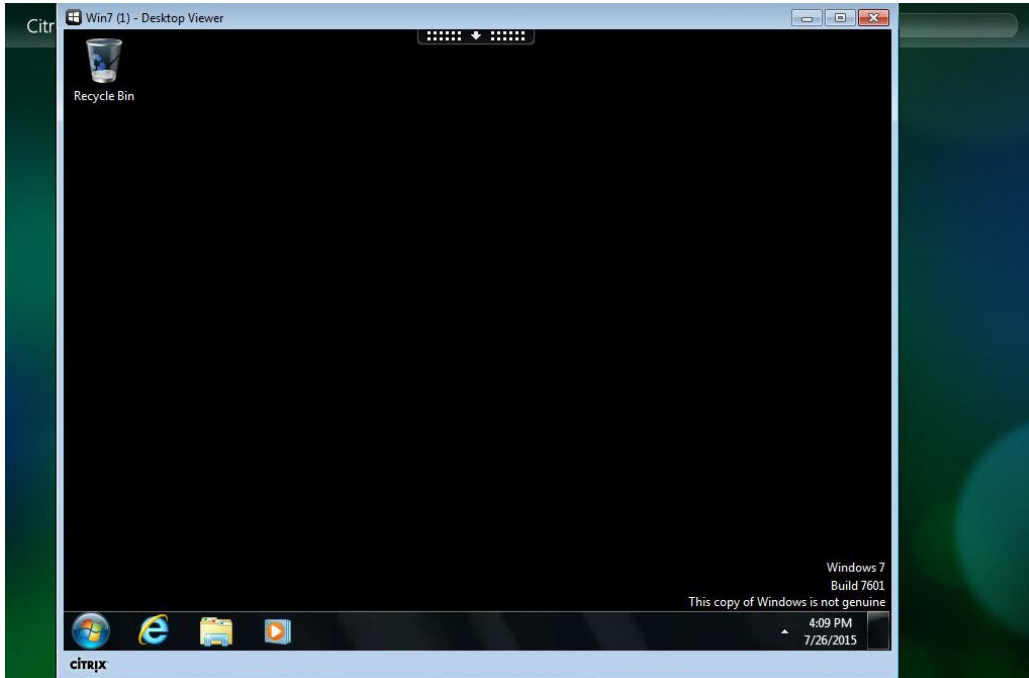
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

5. Select the smart card authentication method, and then enter your **Smart card logon** PIN.



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

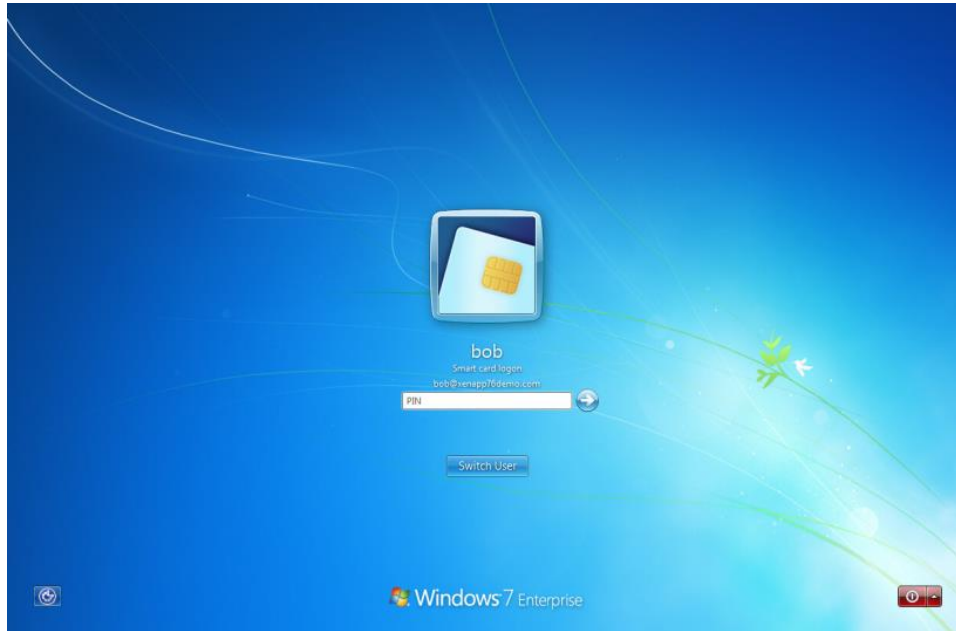
After successful authentication, you will be logged on to the machine.



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

CBA Pass-through using Citrix Receiver for Web Access

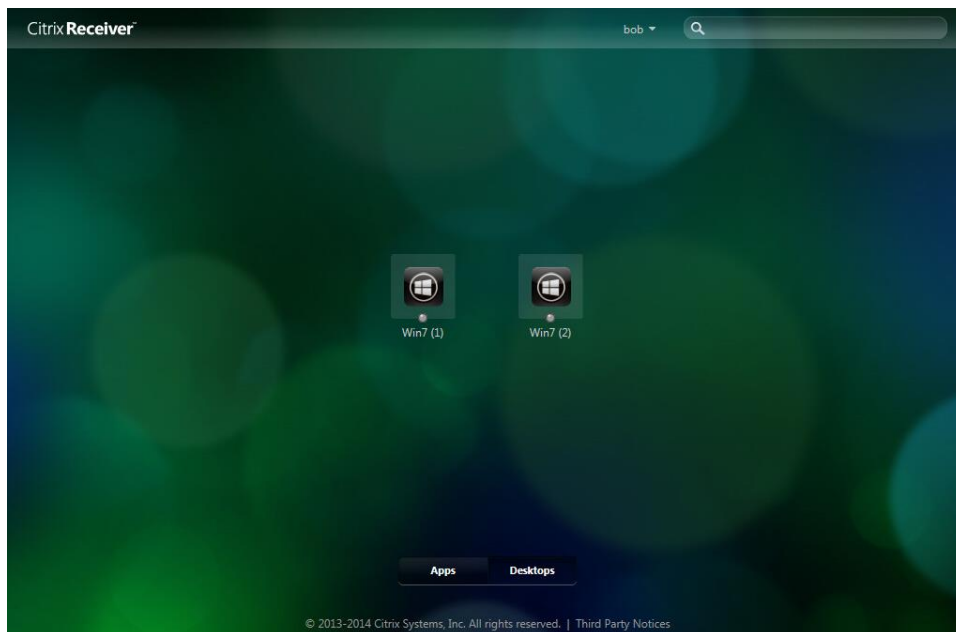
1. Login to the client machine using **Smart card logon**.



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

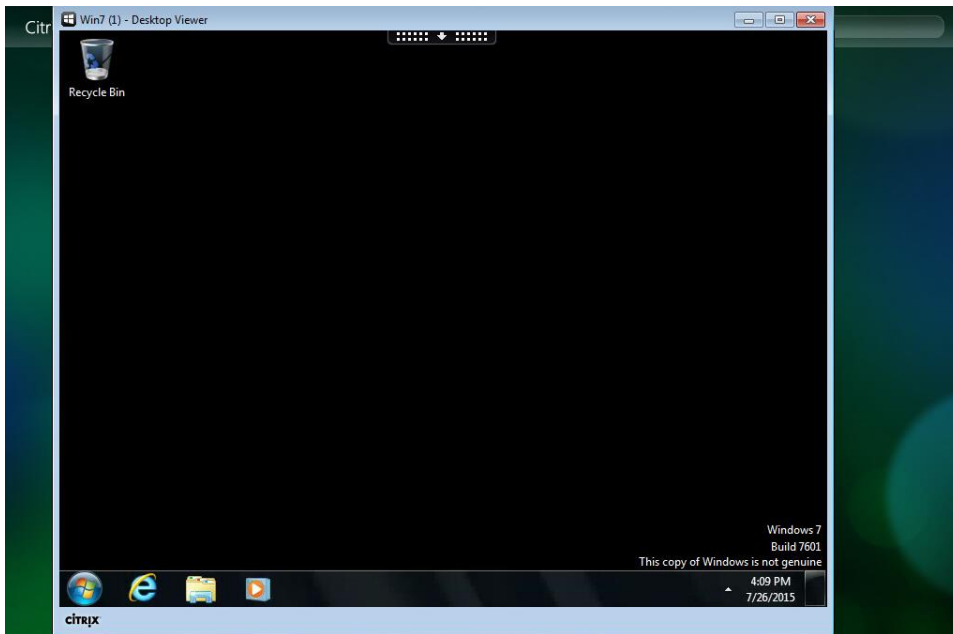
2. Open a web browser and type the **Citrix Receiver for Web** URL.

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.)

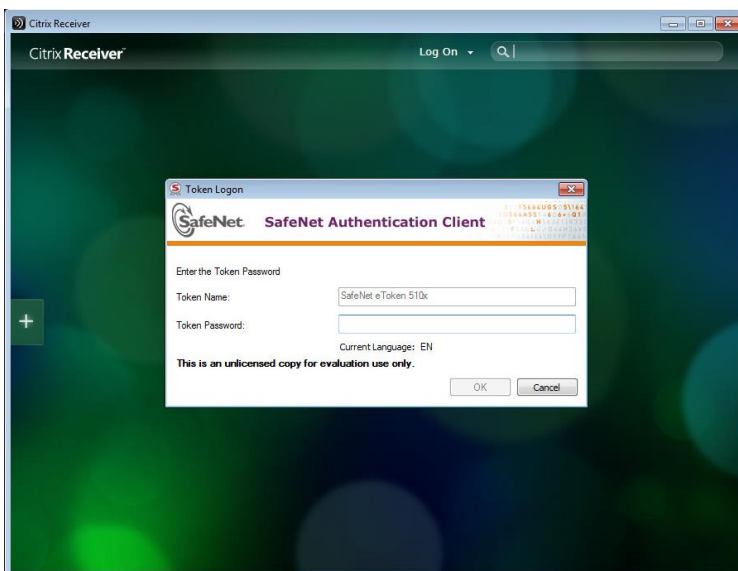
3. Select a machine to use. Since Citrix is configured for pass-through authentication, the machine will open without requiring the user to authenticate again.



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

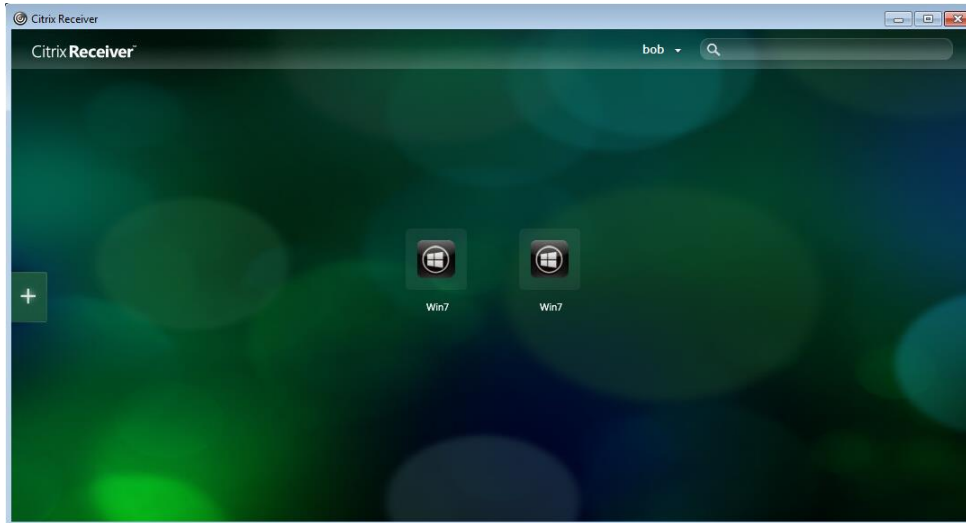
CBA using Citrix Receiver

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



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

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



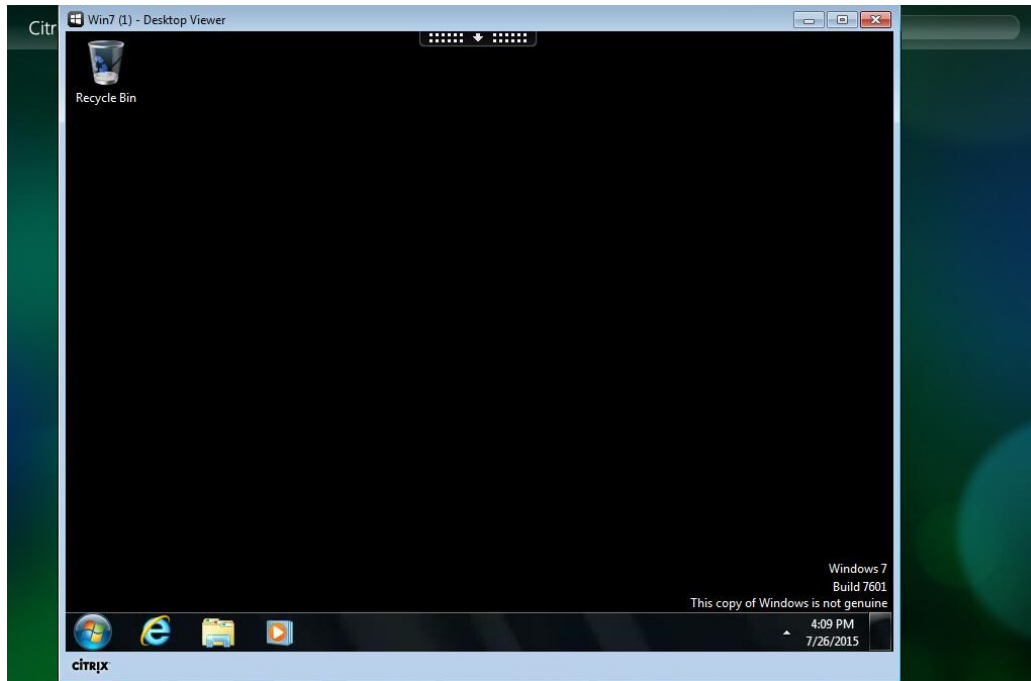
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

3. Select a virtual desktop. The **Windows Login** window is displayed.



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

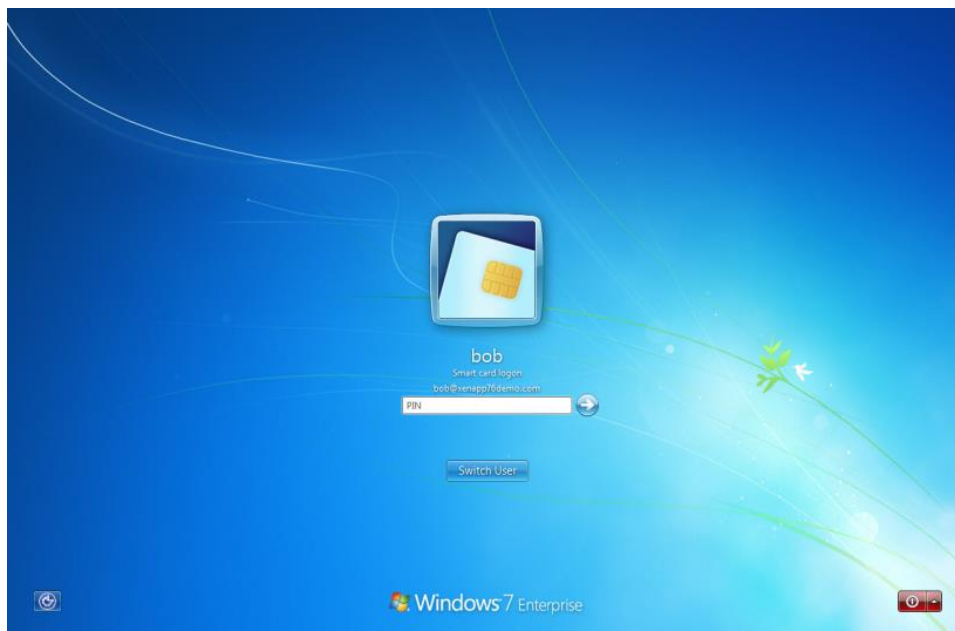
4. Select the smart card authentication method, and then enter your **Smart card PIN**.
After a successful authentication, you will be logged on to the virtual desktop.



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

CBA Pass-through using Citrix Receiver

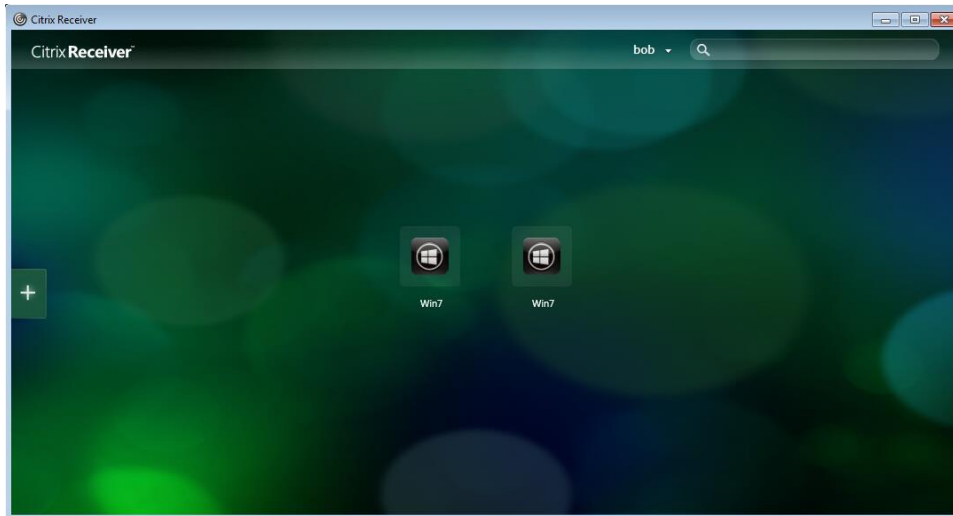
1. Log in to the Windows client workstation using **Smart card logon**.



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

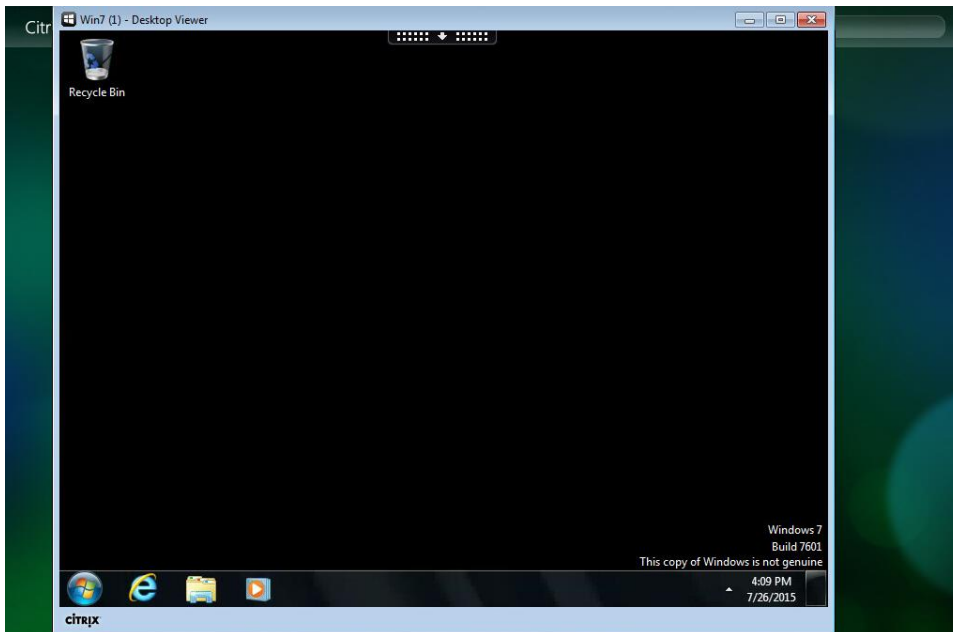
2. After successful authentication, launch Citrix Receiver.

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



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

3. Select a virtual desktop. Since Citrix is configured for pass-through authentication, the virtual desktop can be accessed 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, 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, Inc. 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.	