SafeNet Authentication Client

Integration Guide

Using SAC CBA with Citrix XenDesktop 7.5

Document Information

Document Part Number	007-012539-001, Rev. B
Release Date	December 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

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

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.

Overview

This document provides guidelines for deploying certificate-based multi-factor authentication for user authentication to Citrix XenDesktop using any of SafeNet's certificate-based authenticators.

SafeNet's certificate-based authenticators provide secure remote access, as well as other advanced functions, in a single authenticator, including digital signing, password management, network logon, and combined physical/logical access.

The authenticators come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are being interfaced using a single middleware client, SafeNet Authentication Client (SAC). SafeNet Authentication Client manages SafeNet's extensive portfolio of certificate-based authenticators, ensuring full support for all currently deployed eToken and iKey devices.

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

With the XenDesktop Installation the following components will be installed:

- **Citrix StoreFront** – In this lab the Citrix StoreFront replaces the Citrix Web Interface and supply a 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.

Multi-Factor Authentication Dataflow and Environment

To enable certificate-based multi-factor authentication for Citrix XenDesktop using SafeNet certificate based authenticator, the user needs to deploy the following:

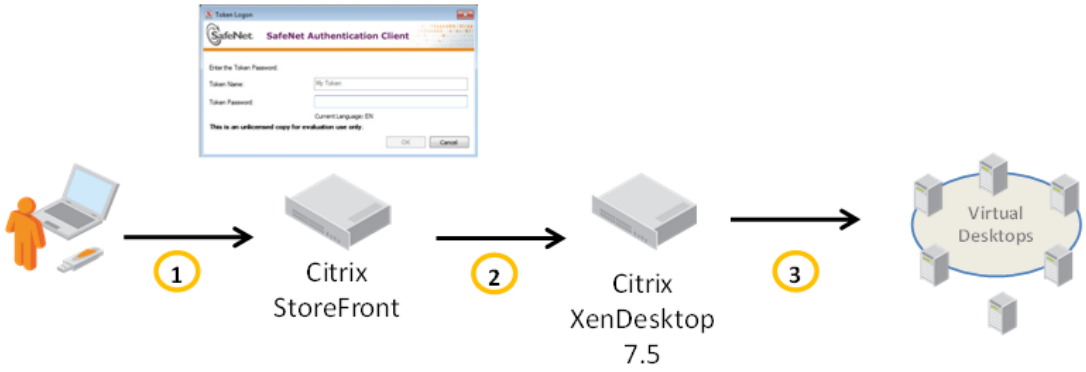
- Microsoft technology, including Active Directory (AD) and Microsoft CA
- SafeNet Authentication Client—A unified middleware client for all SafeNet certificate-based authenticators.
- Citrix XenDesktop 7.5 Server—The server side of Citrix XenDesktop. This document describes Citrix XenDesktop version 7.5.
- Citrix Receiver—A client application installed on the endpoint device (PCs, tablets, smartphones, etc.) that interfaces with Citrix-enabled IT infrastructure.

- Citrix StoreFront Server—Installed via the XenDesktop 7.5 installation and configured using the Citrix Studio application.
- Master Image—The master image that will be used by Machine Creation Services (MCS) to create VMs. This is also known as a “golden image” or a “base image.”

NOTE: This document assumes that Citrix XenDesktop Server is installed and interfaced with Citrix StoreFront, and that the solution is using static passwords or any other user-authentication method. For additional information on how to install Citrix XenDesktop, refer to: **http://www.citrix.com/wsdm/restServe/skb/attachments/RDY8316/XenDesktop%207.1%20Reviewer's%20Guide.pdf**

Figure 1 shows the environment required to implement a Citrix solution using SafeNet’s certificate based authentication, and illustrates the dataflow of the authentication request:

1. A user is required to authenticate to Citrix XenDesktop using SafeNet’s certificate-based authenticator. SafeNet’s authenticator is deployed with a user-unique client certificate for authentication. When the user is authenticated, they must provide a PIN to access the authenticator.
2. The credentials are passed to Citrix XenDesktop, which returns a response to the Citrix Receiver client or Citrix Web Receiver, which will accept or reject the authentication request.
3. After successful authentication, the user receives the XenDesktop interface where he can run published machines or apps.



Preparation and Prerequisites

This section describes the perquisites needed to be installed and configured before implementing certificate based authentication for Citrix XenDesktop.

Microsoft CA

In order to use a CBA, the Microsoft Certificate Authority must be installed and configured. In this integration guide we installed the Microsoft CA on the DC machine.

SafeNet Authentication Client

The SAC 8.3 Post GA, build 67 includes all the files and drivers needed to support SafeNet smart card integration.

SafeNet Authentication Client must be installed on each computer where the smart card is going to be used, including:

- XenDesktop 7.5 Server
- XenDesktop Master Image
- All other client machines that connects to the XenDesktop server using CBA

Citrix XenDesktop 7.5 Server

Citrix XenDesktop Server should be installed and configured to authenticate with basic authentication (user name and password). The authentication is being configured (in the StoreFront server) using Citrix Studio, which is installed with the XenDesktop 7.5 installation.

Citrix Receiver

Citrix Receiver is designed as an integral component for XenDesktop. This easy-to-install software client provides access to applications, desktops, and data easily and securely from any device, including smartphones, tablets, PCs, and Macs.

The receiver can be installed from the StoreFront web interface or directly from the Citrix website. In this integration, Citrix Receiver 4.1 is used.

Citrix StoreFront

In Citrix StoreFront, you must configure a server group and a store service. All services needs to be configured to use an HTTPS connection. As a prerequisite, this document assumes that a basic authentication (username and password) is configured, which can be done through the Citrix StoreFront.

Master Image

In this integration, virtual machines are published via the XenDesktop. All machines are installed in the VMware ESX platform. It is assumed that at least one resource (in this case, a machine) has been published through the Citrix XenDesktop.

The master image is a base image, from which the XenDesktop will publish the virtual machines to the users.

The basic configuration for the master image should be as follows:

- The master image should be associated to the domain.
- SAC 8.3 should be installed.
- Citrix VDA (Virtual Desktop Agent) should be installed on the master image.

Citrix Configuration for Certificate-Based Authentication

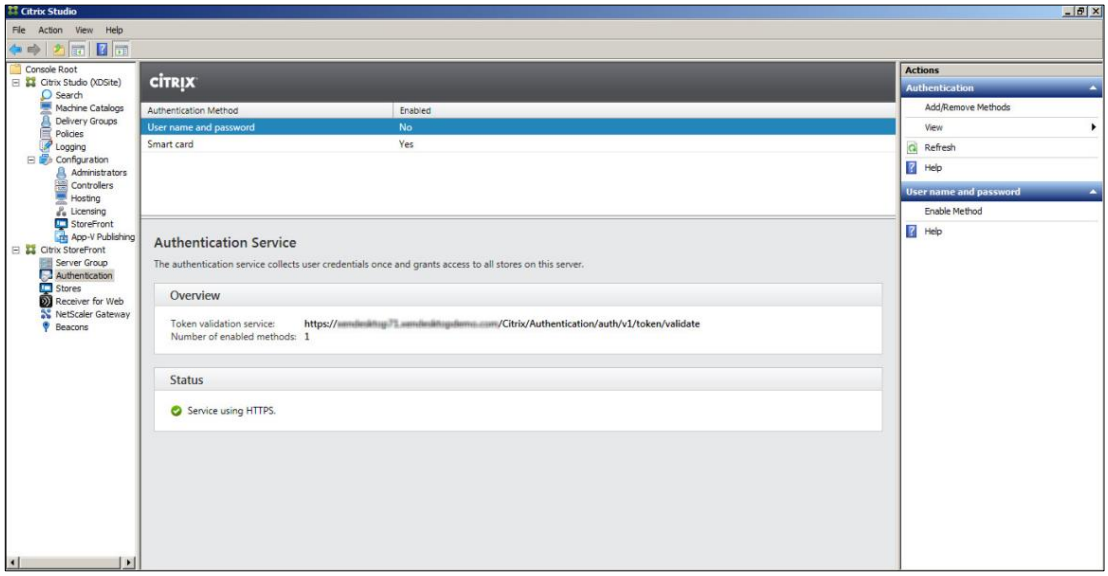
In this section, you will configure the various Citrix components to work with certificate-based authentication.

Citrix StoreFront

Configure the authentication method to **Smart Card**, based on your preference and in conjunction with the description above. With this configuration method, the user will be asked to enter the smart card PIN/password when logging in to the XenDesktop published machine.

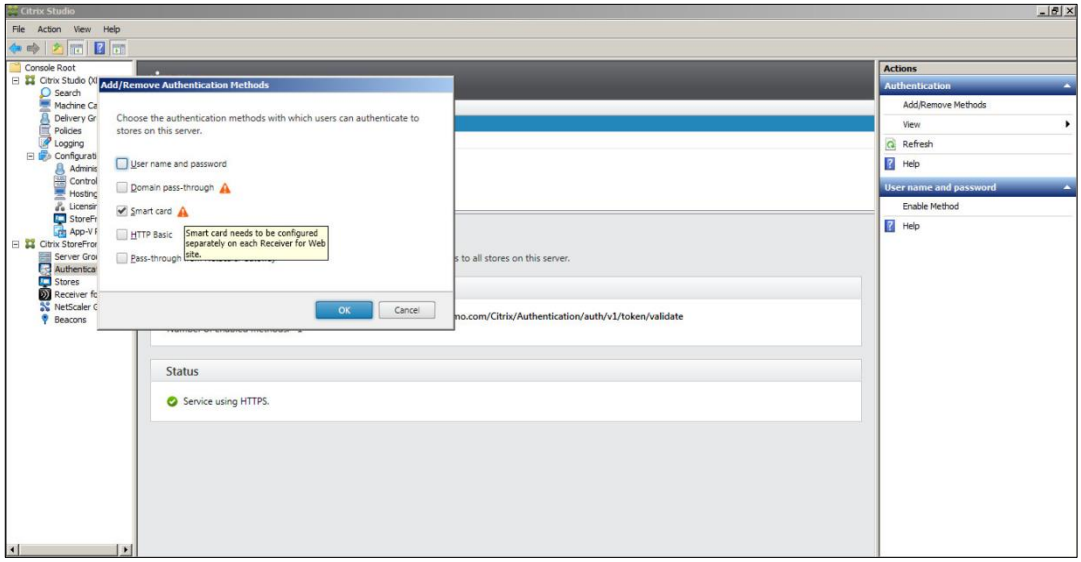
To configure a smart card for the Citrix Receiver:

1. Open Citrix Studio.
2. In the left pane, click **Citrix Storefront -> Authentication**.



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

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

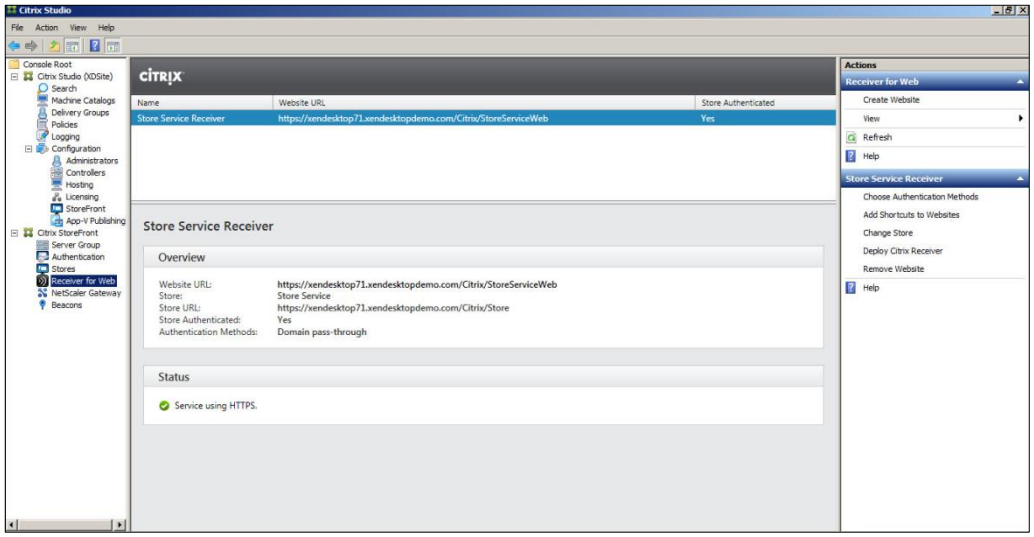


(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)

4. Select the **Smart Card** check box, and then click **OK**.

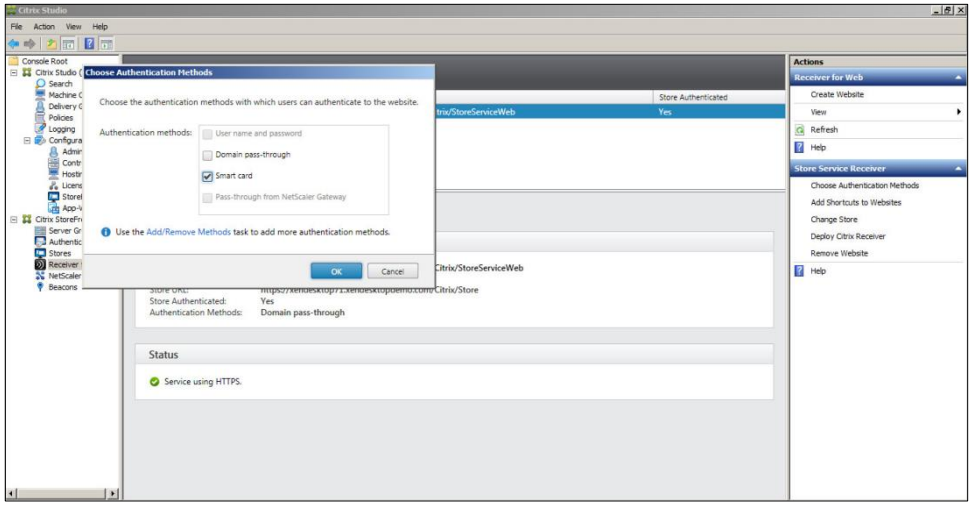
To configure a smart card for the StoreFront Receiver for Web:

1. In the left pane, click **Receiver for Web**.



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

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



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

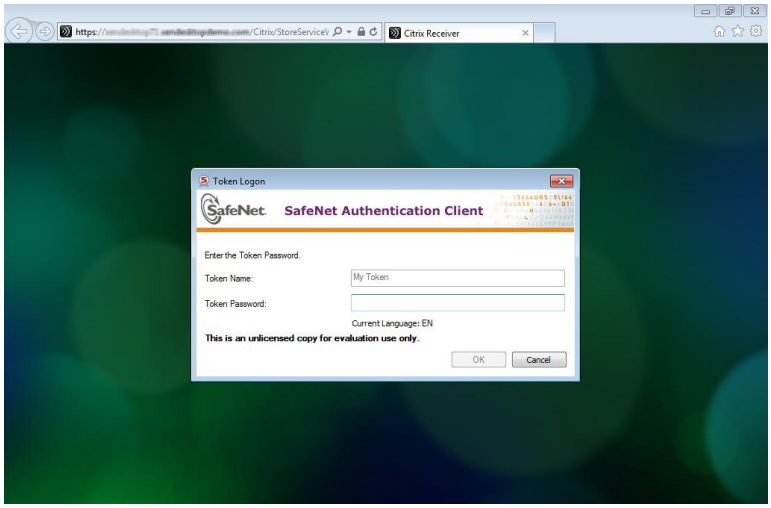
3. Select **Smart Card**, and then click **OK**.

Typical Certificate-based Authentication Scenario

In this scenario, a user connects a SafeNet USB token to the Windows client computer. When the StoreFront web interface connects to the Citrix XenDesktop Server, the user is prompted to enter their token password. Upon successful authentication, the user is prompted to select a published application.

Logging On to StoreFront Web Receiver

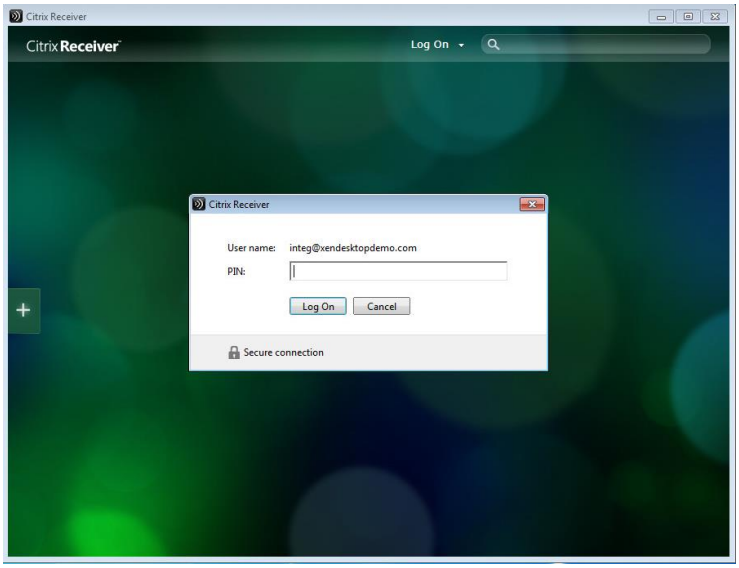
1. Connect your SafeNet USB token to the computer.
2. Open a browser and type https://<XenDesktopServer.Your_Domain>/Citrix/StoreServiceWeb/.
3. The **SAC Token Logon** dialog box is displayed.



4. Type the token password, and then click **OK**.
5. The StoreFront Web Receiver application page is displayed.

Logging-On to Citrix Receiver:

1. Connect your SafeNet USB token to the computer.
2. Open Citrix Receiver.
3. The Log On window opens together with Citrix Receiver PIN code logon window.



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

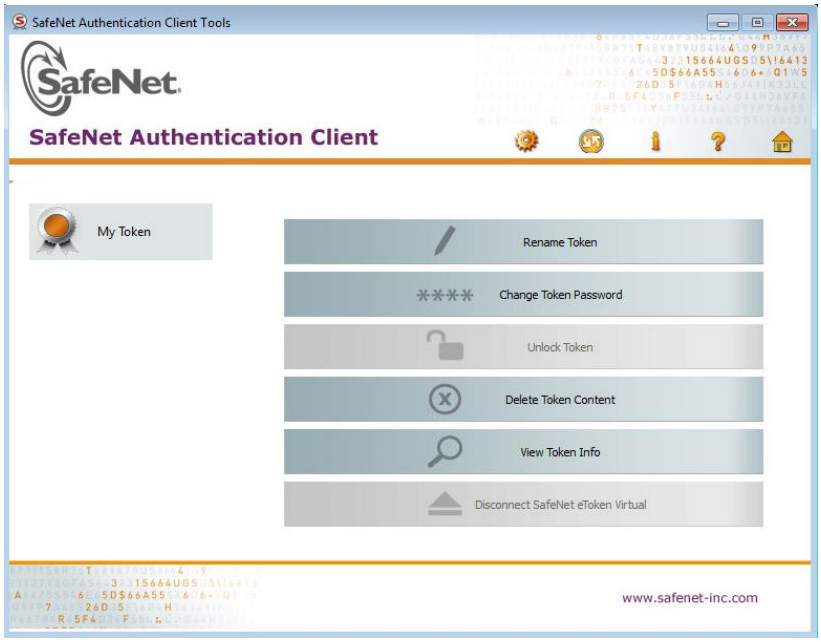
4. Type the token password, and then click **OK**.
5. The Citrix Receiver application window opens:

Configuring Citrix StoreFront 2.5 to Use Smart Card Pass-through Authentication

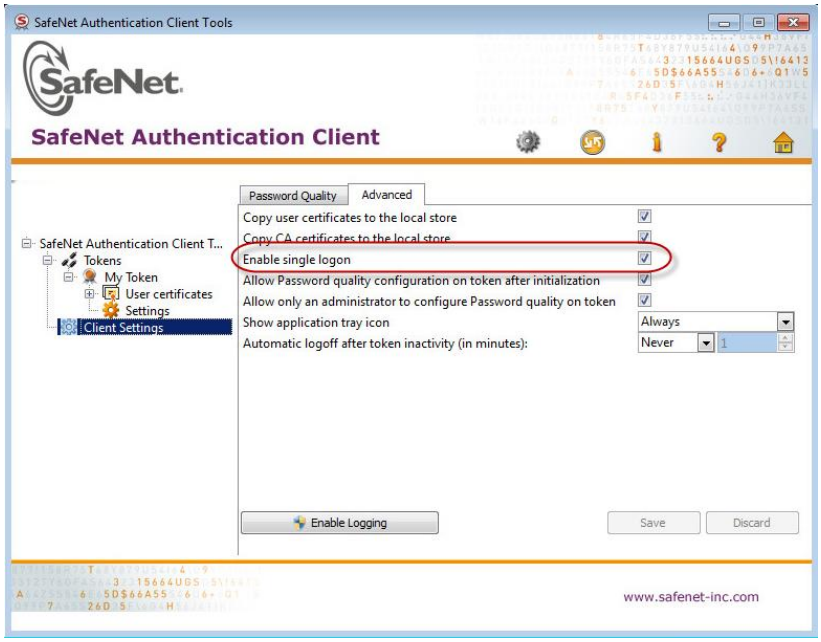
To configure Citrix StoreFront to use smart card pass-through authentication:

On SafeNet Authentication Client:

1. Open the SAC console.



2. Click **Advanced View > Client Settings**, and then click the **Advanced** tab.
3. Select the **Enable single logon** check box.



4. Click **Save**.
5. Open the Windows Registry by typing **regedit** on the command line.
    a. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC** and create a new key called **General**.
    b. In the new key, create a new DWORD (32-bit) with the name **SingleSignOn**. Specify a value of **1**.
    c. Exit the Windows Registry.

On StoreFront 2.5 Server:

To configure StoreFront to use smart card pass-through authentication, you must first configure the **default.ica** file on the IIS:

1. Open the file **default.ica** with a text editor. The file can typically be found at the following location:

    C:\inetpub\wwwroot\Citrix\<Store_Name>\App_Data\)
2. Under **Application**, add the following: **DisableCtrlAltDel=Off**
3. Save the file.

More information can be found at:

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

On Citrix Receiver Client Machine:

On the client machine where the Citrix Receiver is installed, you need to modify the default Citrix CSP dialogue PIN prompt to use SAC instead.

To change the default Citrix CSP PIN behavior prompt:

1. Press **Start > Run** and type **regedit.exe** to open the Windows Registry on the client machine.
2. Add the key value shown below to the following Registry key:

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

More information can be found at the following link:

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

Support Contacts

If you encounter a problem while installing, registering or operating this product, make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	
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 SafeNet Knowledge Base.	