Using Certificate-based Authentication with SafeNet Authentication Client for Citrix XenApp 6.5

Contents
Description...............................................................................................................................................2
The Multi-Factor Authentication Dilemma: Security over Convenience.........................................................2
Multi-Factor Authentication Dataflow and Environment ..................................................................................2
Preparation and Perquisites................................................................................................................................3
  Server Side ..................................................................................................................................................3
  Client Side ..................................................................................................................................................4
Citrix Configuration for Certificate-Based Authentication ..............................................................................4
  Next we will configure the different Citrix components to work with certificate-based authentication.  Citrix Web Interface Management Configuration........................................................................................................4
  Smart card authentication methods for Citrix XenApp Web sites:.................................................................4
  Smart card authentication methods for Citrix XenApp Services sites:.........................................................5
SafeNet Authentication Client Configuration.................................................................................................6
  Typical Certificate Based Authentication Scenario ..........................................................................................7
  Logging-on to Citrix Web Interface..................................................................................................................7
Description

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

SafeNet’s certificate-based authenticators provide secure remote access, as well as other advanced applications including: digital signing, password management, network logon, and combined physical/logical access, in a single authenticator. 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. SafeNet Authentication Client manages SafeNet’s extensive portfolio of certificate-based authenticators, ensuring full support for all currently deployed eToken and iKey devices.

Citrix XenApp is an application delivery solution that enables any Windows application to be virtualized, centralized and managed in the datacenter and instantly delivered as a service to users anywhere on any device. As users connect remotely to the virtual server, multi-factor authentication is a fundamental capability.

The Multi-Factor Authentication Dilemma: Security over Convenience

As you set up to deploy certificate-based multi-factor authentication solution with your Citrix XenApp solution, one of the most frequent deployment questions pops up. Citrix XenApp allows users to have a session single-logon capability, where, once the user was authenticated to the smart-card device, the user stays authenticated until the end of the session, regardless of the number of times the user accesses the application. This provides a better user-experience for those using the system. However on the same note, this single-logon capability, called “Pass Through” may impose security risks in ultra-sensitive use-cases and environments.

Before deploying the system you should decide whether your organization can deploy the user-friendly single-logon, :Pass Through” feature, or alternatively users will need to authenticate each time they interface with Citrix XenApp application.

Multi-Factor Authentication Dataflow and Environment

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

- **SafeNet Authentication Client** – A unified middleware client for all SafeNet certificate based authenticators. This document describes SafeNet Authentication Client version 8.2.
- **Citrix Receiver** - A client application installed on the end point device (e.g.: PCs, tablets, smartphones, etc.) that interfaces with Citrix-enabled IT infrastructure.
- **Citrix Web Interface** - Citrix Web Interface provides secure access to XenApp and XenDesktop resources from anywhere through any device with a Web browser or through the Citrix Receiver. This document describes Citrix Web Interface version 5.4.

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 XenDesk using SafeNet’s certificate-based authenticator. SafeNet’s authenticator is deployed with a user unique client certificate that is used to authenticate the user. When the user is authenticated the user needs to provide a PIN to access the authenticator.
2. The credentials provided are passed to Citrix XenApp which returns a response to the Citrix Receiver client or Citrix Web Interface to accept or to reject the user authentication request.

![Deployment and dataflow of SafeNet's multi-factor authentication solution with Citrix XenApp](image)

**Figure 1:** Deployment and dataflow of SafeNet’s multi-factor authentication solution with Citrix XenApp

## Preparation and Perquisites

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

**NOTE**

This document assumes that Citrix XenApp Server is already installed and interfaced using Citrix Web Interface and that the solution is working using static passwords, or any other user-authentication method.

Follow these steps:

### Server Side

2. Ensure that Citrix Web Interface version 5.4 is installed. Citrix Web Interface should be configured to work with two sites:
   - A web site for accessing Citrix XenApp via a Web browser
   - A service site for accessing Citrix XenApp via the Citrix Receiver

For more information on Citrix management web sites, please refer to [Citrix Configuration for Certificate-Based Authentication](#)
3. Based on the decision whether to use smart-card authentication or smart-card pass through authentication, ensure that your domain environment supports the appropriate method.

For more information on Citrix smart card pre-requirements please refer to http://support.citrix.com/article/CTX129096

Client Side

1. Ensure that Citrix Receiver version 3.4 Enterprise is installed on each client machine that needs to use certificate-based authentication.

2. Install SafeNet Authentication Client version 8.2.
   Configure Single logon in SafeNet Authentication Client version 8.2 if "Pass Through with Smart Card" authentication method is selected in XenApp Services site.

   For more information on Citrix management web sites, please refer to SafeNet Authentication Client Configuration

Citrix Configuration for Certificate-Based Authentication

Next we will configure the different Citrix components to work with certificate-based authentication.

Citrix Web Interface Management Configuration

Citrix web interface introduces XenApp Web Sites (for Web Interface users) and XenApp Services Sites (for users of the Citrix Receiver).

Configure the authentication method to “Smart Card” or “Pass Through with Smart Card”, based on your preference and in conjunction with the description described above. When configuring the authentication method to be “Smart Card” the user will be asked to enter the smart card PIN / Password again when logging in to the Citrix site. If the authentication method is configured to be "Pass Through with Smart Card" The user will be asked for the smart card PIN once: on the client-login and will not be to re-enter the PIN again during the same session.

Smart card authentication methods for Citrix XenApp Web sites:

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.

3. In the Action pane, click Authentication Methods
4. Select the **Smart card** or **Pass-through with smart card** check box, as appropriate.

5. Click **Properties** to configure further settings for smart card authentication.

**Smart card authentication methods for Citrix XenApp Services sites:**

1. On the Windows **Start** menu, click **All Programs > Citrix > Management Consoles > Citrix Web Interface Management**.

2. In the left pane of the Citrix Web Interface Management console, click **XenApp Services Sites** and select your site in the results pane.

3. In the **Action** pane, click **Authentication Methods**
4. Select the **Smart card** or **Pass-through with smart card** check box, as appropriate.

5. Click **Properties** to configure further settings for smart card authentication.

### SafeNet Authentication Client Configuration

If the authentication method is configured to be “Pass Through with Smart Card” in Citrix Web Interface XenApp Services Sites, it is necessary to enable single logon in SafeNet Authentication Client version 8.2.

**To enable Single logon in the SafeNet Authentication Client**

1. Open SafeNet Authentication Client Tools **Advanced View**.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab
4. Select Enable single logon.

5. To save your changes, click **Save**.

---

**NOTE**

To make sure that SafeNet Authentication Client Single logon settings have been applied correctly following check that in the client machine registry settings that the below key exists and is set to ‘1’:

```
HKLM\Software\SafeNet\Authentication\SAC\GENERAL\SingleLogon
```

---

**Typical Certificate Based Authentication Scenario**

User connects a SafeNet USB token to the Windows client computer. When the Web Interface connects to the Citrix XenApp 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 Citrix Web Interface:**

1. Connect your SafeNet USB token to the computer.
2. Open Internet Explorer and type `https://Domain_Name/Citrix/XenApp`  
The Log On window opens.
3. Select **Smart Card** and Click **Log On**. The Token Logon window opens:

![Token Logon window](image)

4. Enter the Token Password value and click **Ok**.
5. The Citrix XenApp application window opens: