CITRIX®

Smart Card Configuration for Citrix Environments

Version 1.1

Table of Contents

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Introduction

This document provides a step-by-step guide for configuring a complete smart card deployment on Citrix XenDesktop. Instructions are included for Windows, Macintosh and Linux clients.

Obtaining a Smart Card

The deployment is based on the NIST PIV smart card standard. Smart card driver software for PIV cards is supplied by the Operating System vendors. Note that some organisations require more advanced Smart card driver software which can be installed according to the smart card driver vendor's documentation.

For the purposes of this document, the Yubikey 4 smart card is used. The Yubikey 4 is an all-in-one USB CCID PIV device that can be purchased from Amazon or other vendors. The Yubico software referenced in this document is open source and available as a free download from their website.

Note that it is possible to test with other types of PIV smart cards, but the details of the process will vary according to the smart card vendor's documentation.

Required hardware

This deployment requires three Windows 2012 R2 servers, which may be installed in a Virtual Machine environment, including the:

- Domain Controller
- XenDesktop VDA server
- XenDesktop DDC server

The machines must be installed on a private network, completely isolated from external systems.

Physical computers or Thin Client devices are used to test the smart card integration with HDX Receiver; Windows 10, Linux and Macintosh clients will be connected.

This document includes the following sections:

- Setting up a Windows Domain. Includes a step-by-step guide to configuring a Windows domain to allow smart card authentication. It covers installation and configuration of the Microsoft Certificate Authority.
- Configuring the Smart card. Provides a step-by-step guide to installing a smart card user certificate onto a Yubikey 4 device. The process will be similar for other types of PIV smart cards.
- Enabling Smart cards on Windows. Includes a step-by-step guide to enabling smart card logins on Windows. This can be done per server, or by applying a Smart card Group Policy.

- Configuring Microsoft IIS for HTTPS. This section is a step-by-step guide to enabling HTTPS with smart card client authentication on a Microsoft IIS server. This server will then then be used to host the Citrix StoreFront Web Application.
- Configuring Citrix StoreFront. Provides This a step-by-step guide to creating a StoreFront store that is enabled for Smart card Authentication
- Configuring the XenDesktop DDC. Describes describes how to enable Smart card authentication in the XenDesktop DDC, through to making a connection to the VDA using the HDX Smart card Virtual Channel.
- Configuring Citrix Receiver for Windows. Includes information describing how to configure Windows Receiver, Internet Explorer and Firefox to run on a Windows machine.
- Configuring Citrix Receiver for Linux. This section describes how to configure Linux Receiver and Firefox to run on a Linux machine.
- Configuring Citrix Receiver for Apple OS X. Describes how to configure Citrix Receiver and Firefox to run on an OSX machine.

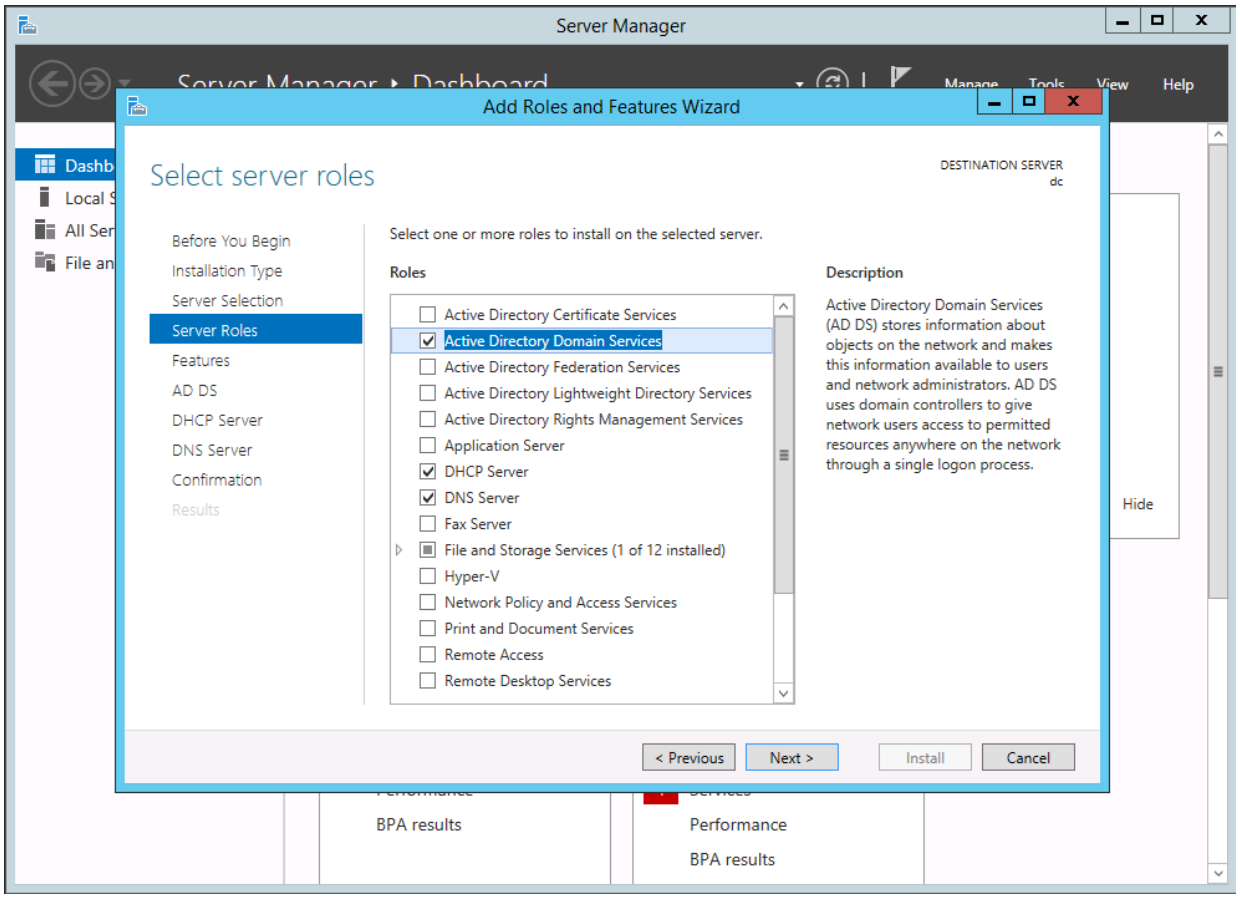
Setting up a Windows Domain

The Windows Domain Controller runs the DHCP server and DNS server for the isolated network. This section covers the promotion of a Windows 2012 R2 machine to a domain controller, and the configuration of the Microsoft Certificate Authority component.

Installing Domain Controller Roles

To configure the Domain Controller, run the Microsoft Server Manager tool and install the following roles:

- Active Directory Domain Services
- DHCP Server
- DNS Server
- Active Directory Certificate Services (must be installed after installing the above)

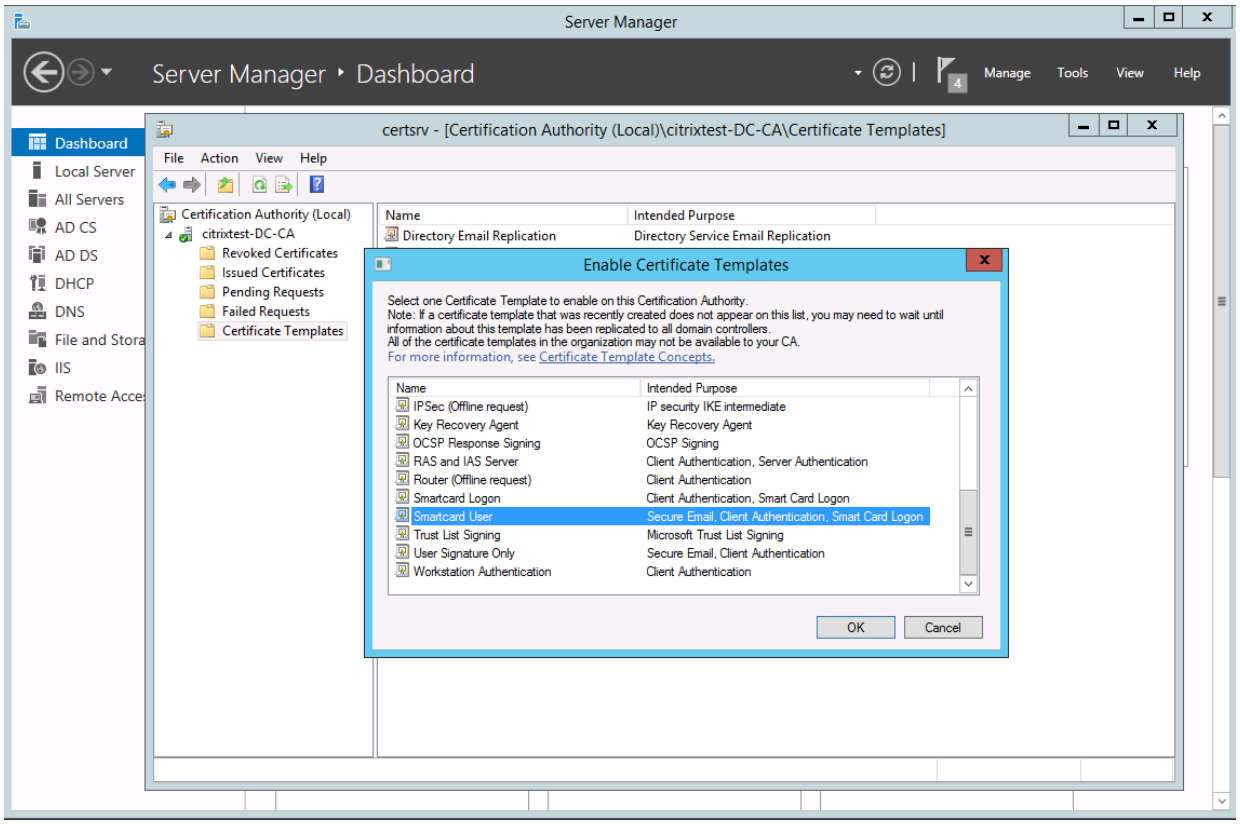


Note that it is possible to configure the Domain Controller as a Router to a public network at this stage using the Remote Access role, but care should be taken to maintain the isolation of the domain deployment network.

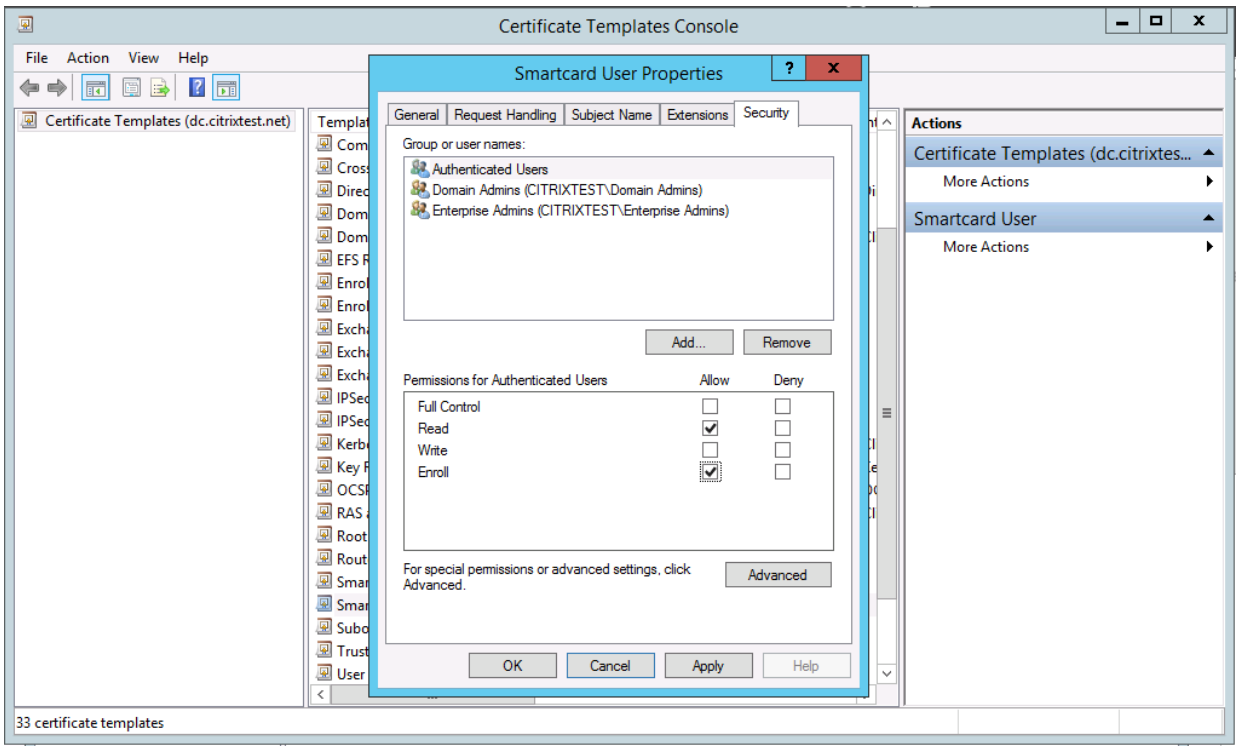
When the Domain Controller is fully installed, join the XenDeskop DDC and VDA servers to the domain. Ensure that all DHCP and DNS services are retrieved from the Domain Controller.

Preparing the Certificate Authority for Smart card usage

In the Server Manager tool open the “Certificate Authority” GUI from the “Tools” menu. In the “Certificate Templates” node, check that the “Smart card User” template is shown. If not, right click and choose “New -> **Certificate template to Issue**” and add it from this list.

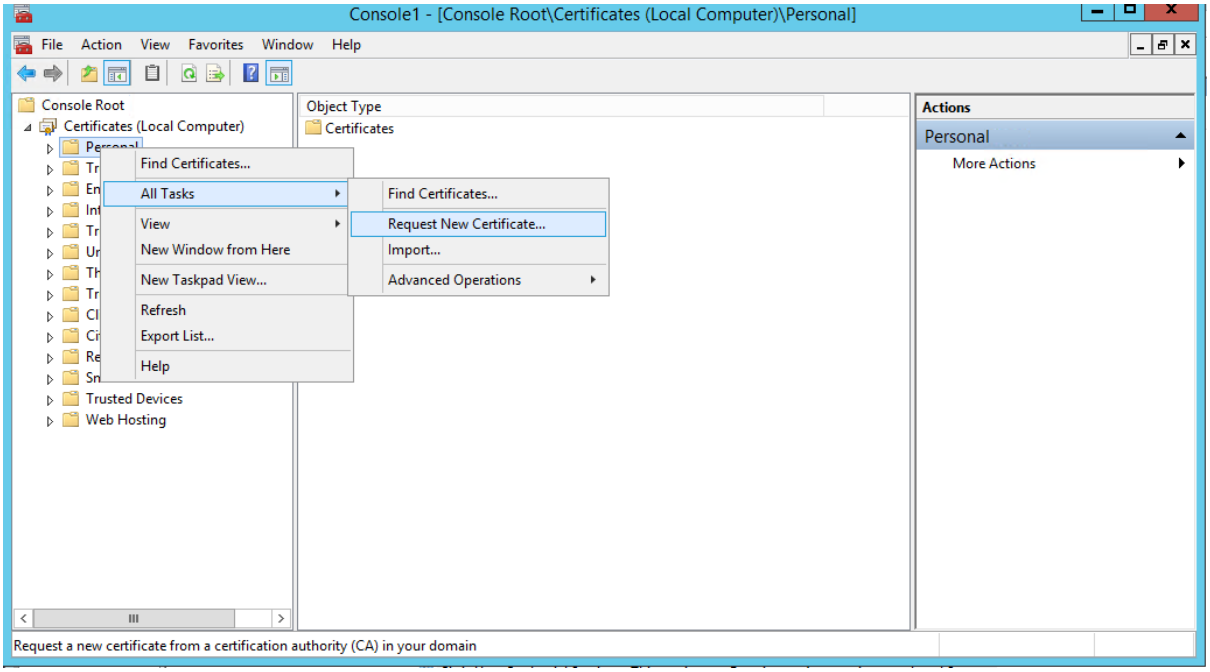


Next, right click the "**Certificate Templates**" node and choose "**Manage**". This will bring up the "Certificate Templates Console". Double click the "**Smart card User**" template and go to the Security tab. Grant the "**Enroll**" permission to "**Authenticated Users**" and click OK.

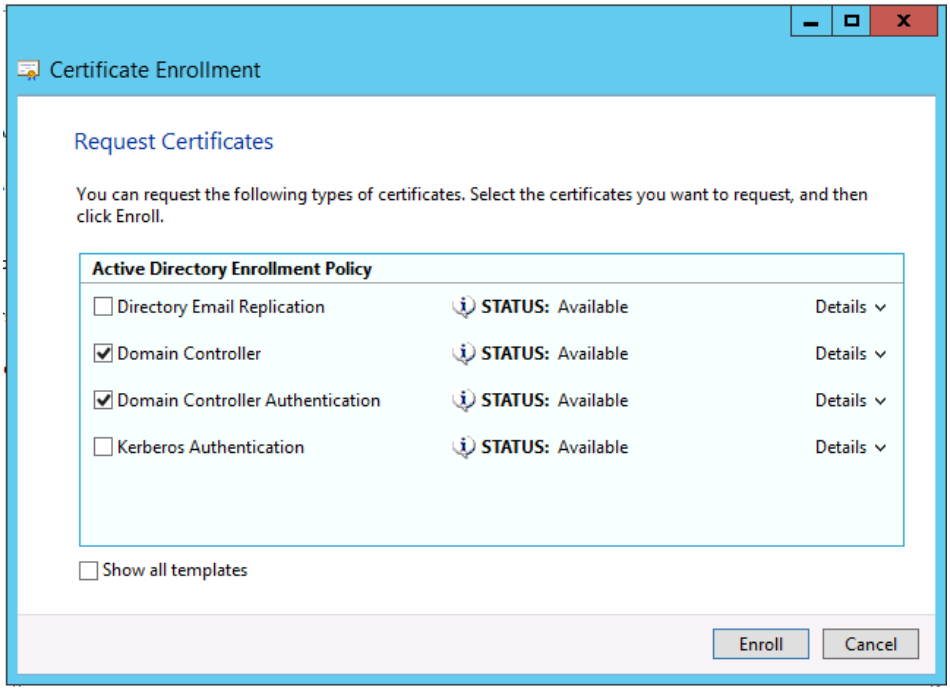


Issuing a Domain Controller Certificate

To authenticate users with a smartcard, the domain controller must be issued with X509 certificates to handle the Kerberos protocol. To do this, run the Microsoft Management Console (mmc.exe), choose **Add/Remove Snapins**, and select Certificates for the "**Computer account**".

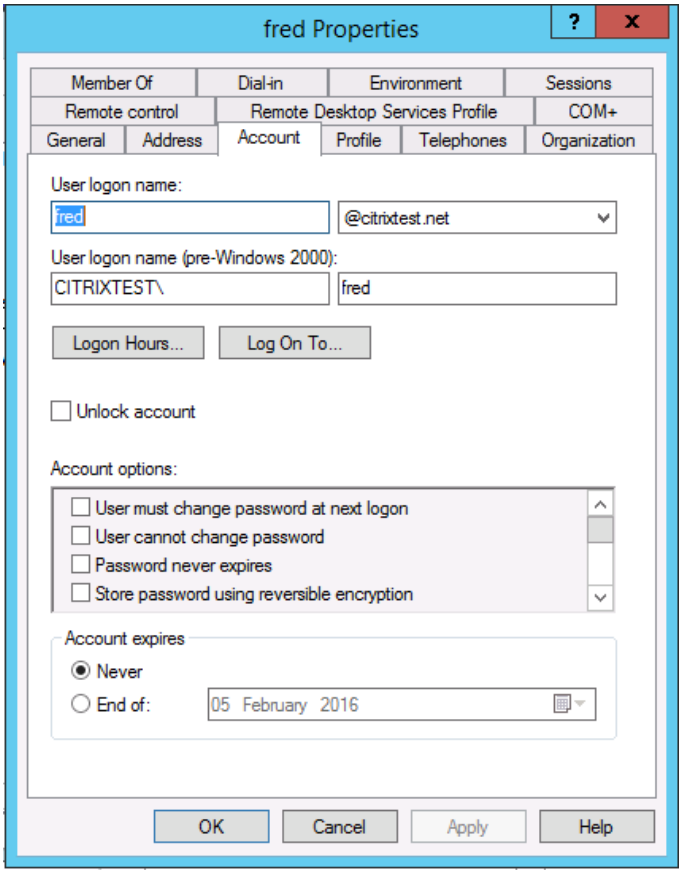


Select "All Tasks → Request New Certificate..." and request "Domain Controller" and "Domain Controller Authentication" certificates.



Creating a test user

Return to the Server Manager and launch the "**Active Directory Users and Computers**" tool from the **Tools** menu. Create a test user (note the username and @citrixtest.net sections). For the purposes of the document, we will create a user account of fred@citrixtest.net.

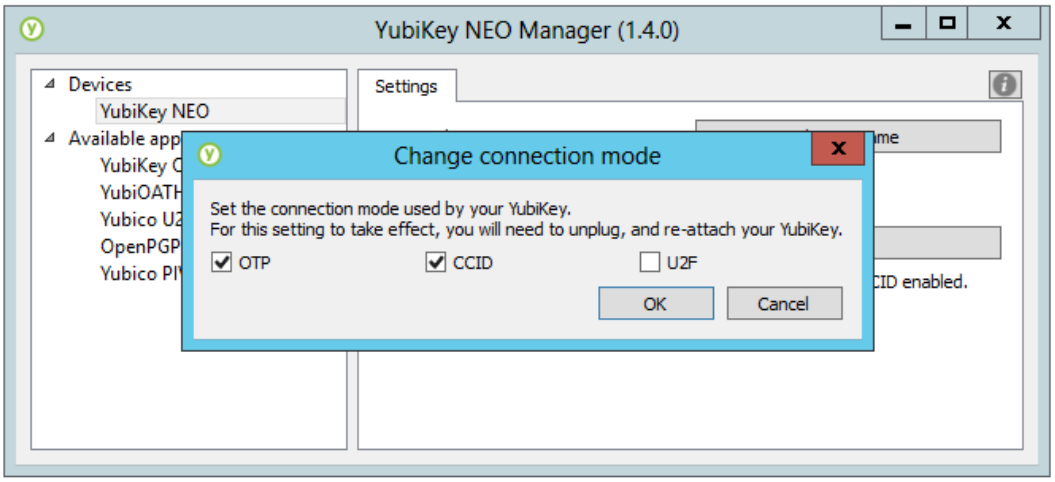


Configuring the Smart card

This section details the process of creating a user smart card certificate and using it to configure a smart card. If you are using a different vendor's PIV smart card, you should refer to the vendor documentation.

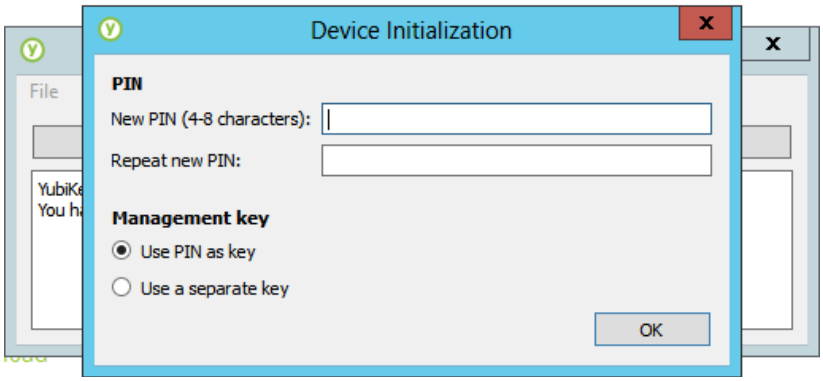
Enable PIV CCID Mode for the Yubikey 4

Yubikey 4s devices are usually shipped with PIV CCID mode disabled. To enable smartcard mode, download and install the "Yubikey NEO Manager" tool from the downloads page of Yubico's website; this can be done on a separate machine. Run the tool and insert the **Yubikey 4** device. Click "Change connection mode" and enable CCID. This only needs to be done once.

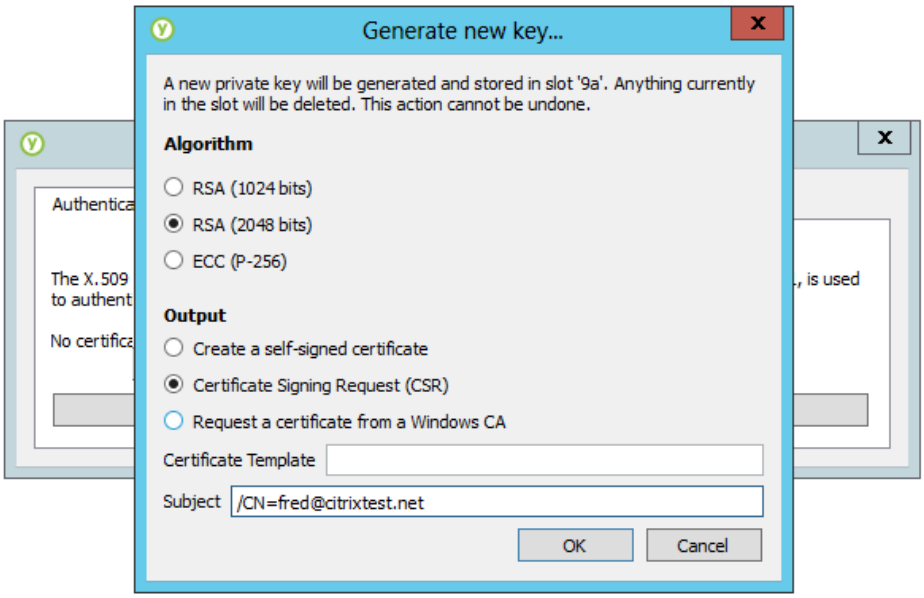


Yubikey PIV Manager Tool

Download and install the "Yubikey PIV Manager" tool from the downloads page of Yubico's website. Run the tool and insert the **Yubikey 4** device. The tool will prompt for you to setup a user PIN and management key for the **Yubikey 4**.



Click the "**Certificates**" button, and choose "**Generate new key**" on the "**Authentication**" tab.



Choose "RSA (2048 bits)" and "Certificate Signing Request". For the Subject select "/CN=fred@citrixtest.net", replacing fred with an appropriate username and citrixtest.net with the UPN suffix of your domain, matching the user account created in the previous step.

Click OK and save the .csr file when requested. You will be prompted to enter the PIN that you specified at "Device Initialization" stage.

Issuing the certificate

Copy the .csr file to the Domain Controller machine. Log in as the user matching the subject (fred@citrixtest.net in this example). Run the command line:

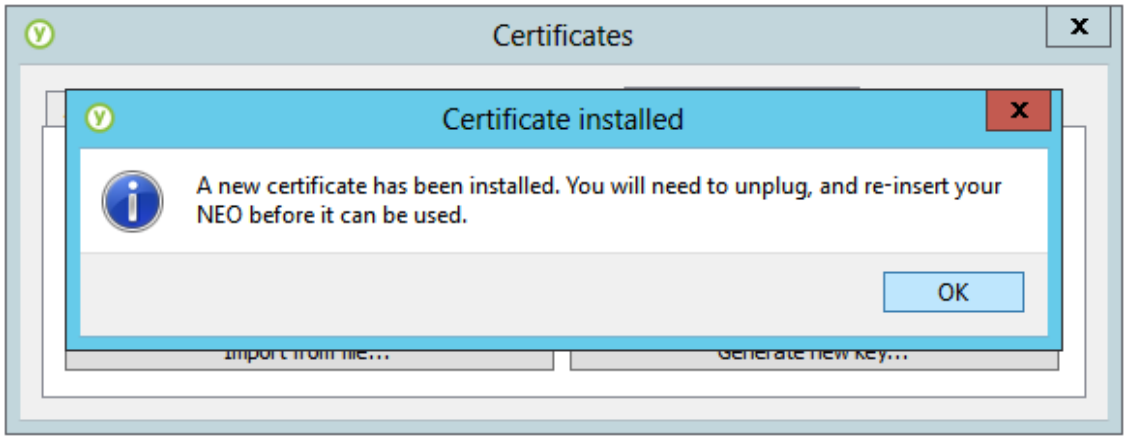
```
certreq -submit -attrib "CertificateTemplate:SmartcardUser" <file.csr>
```

If this step fails check the "Enroll" security permission set on the "Certificate Template Console" above and log out/in. The list of available certificate template names can be seen by running "`certutil -template`".

If the certificate request submission is successful, you are prompted to select your certificate authority and then save a .crt file. Copy the .crt file back to the computer running the YubiKey PIV Manager tool.

Importing the certificate to the Yubikey

On the "Authentication" tab of the YubiKey PIV Manager, Select the "Import from File…" option. Import the .crt file retrieved from the domain controller.



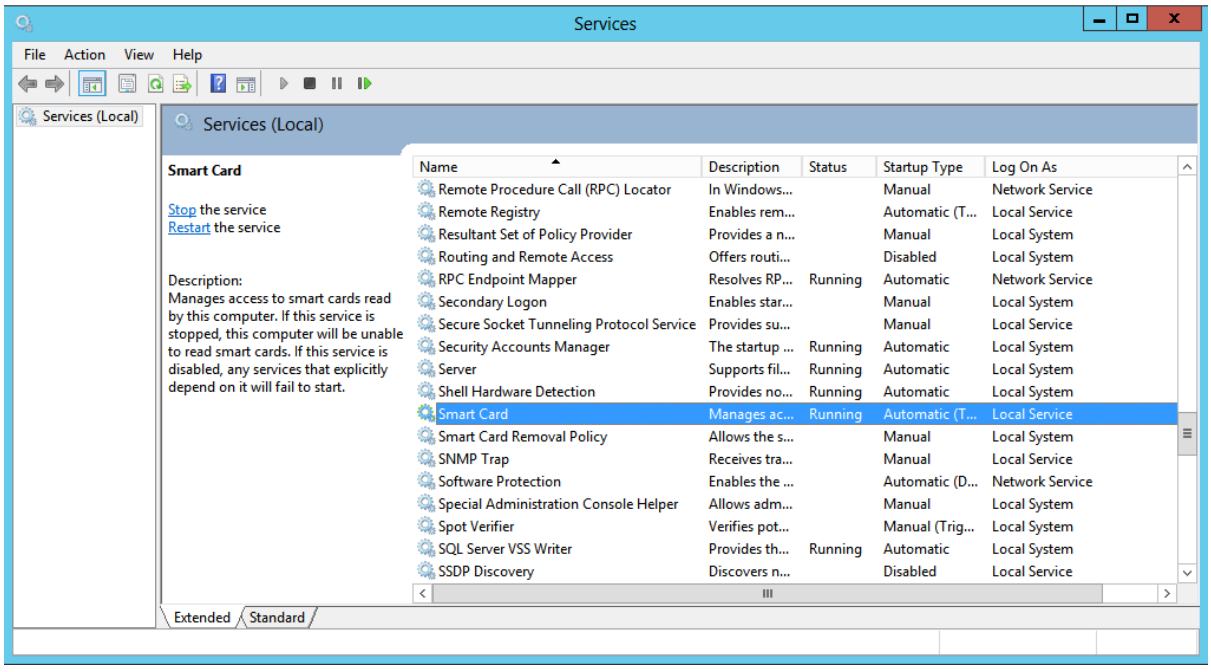
Setting CHUID and CCC objects

Older versions of the Yubikey software do not set the Card Holder Unique Identifier (CHUID) and Card Capability Container (CCC) PIV fields automatically. This will result in the device not be detected on Windows and OSX. Use the command line "set-chuid" and "set-ccc" features of the yubico-piv-tool to correct this (see Yubico documentation if you encounter this issue).

The Yubikey smart card device is now ready for use.

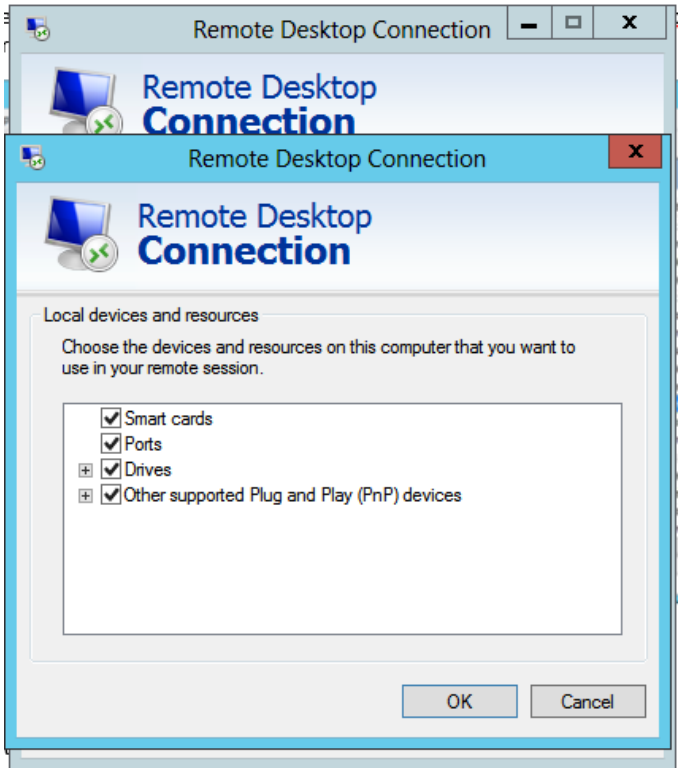
Enabling Smart cards on Windows

Smart card authentication can be enabled through the Services control panel (run services.msc on the command line). Simply enable and start the "Smart card Service".



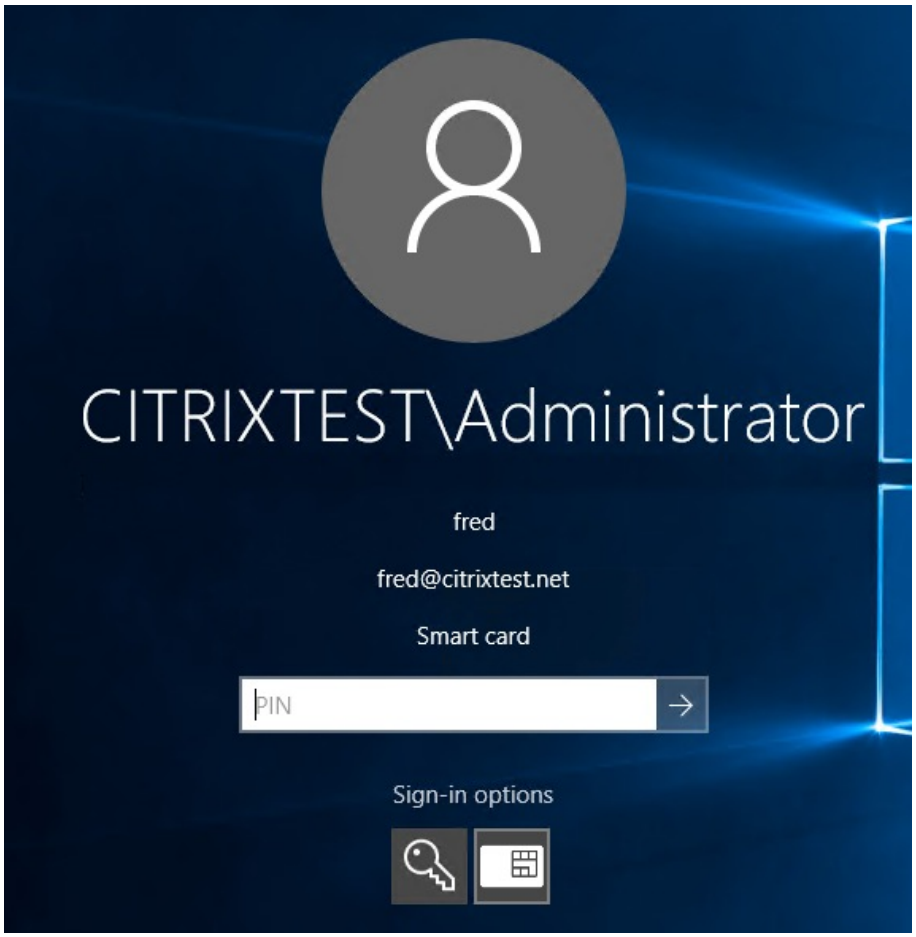
On your XenDesktop VDA machine, enable this service and log out. Connect the Yubikey to the VDA machine, or connect remotely using RDP.

If connecting remotely, remember to enable Smart card devices in the RDP "Local Resources" tab.



You must log in as an Administrator to allow the smart card drivers to load.

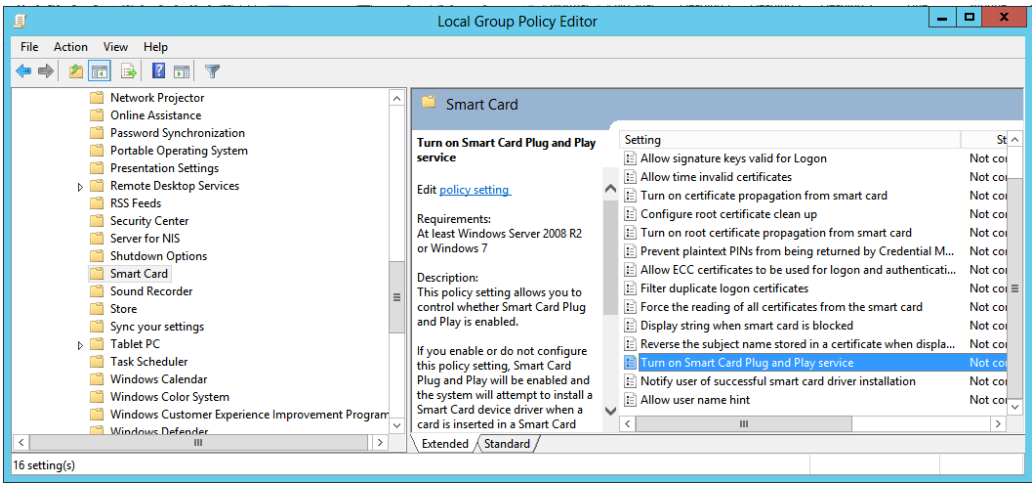
Next, lock the computer and check that the smart card logon icon is available:



You should now be able to log on using the PIN that was specified in the Yubikey PIV Manager tool.

Configuring Smart cards by Group Policy

Note that in addition to manually enabling the Smart card service, Microsoft provides a Group Policy to remotely enable smart card logon (Windows Components/Smart card).

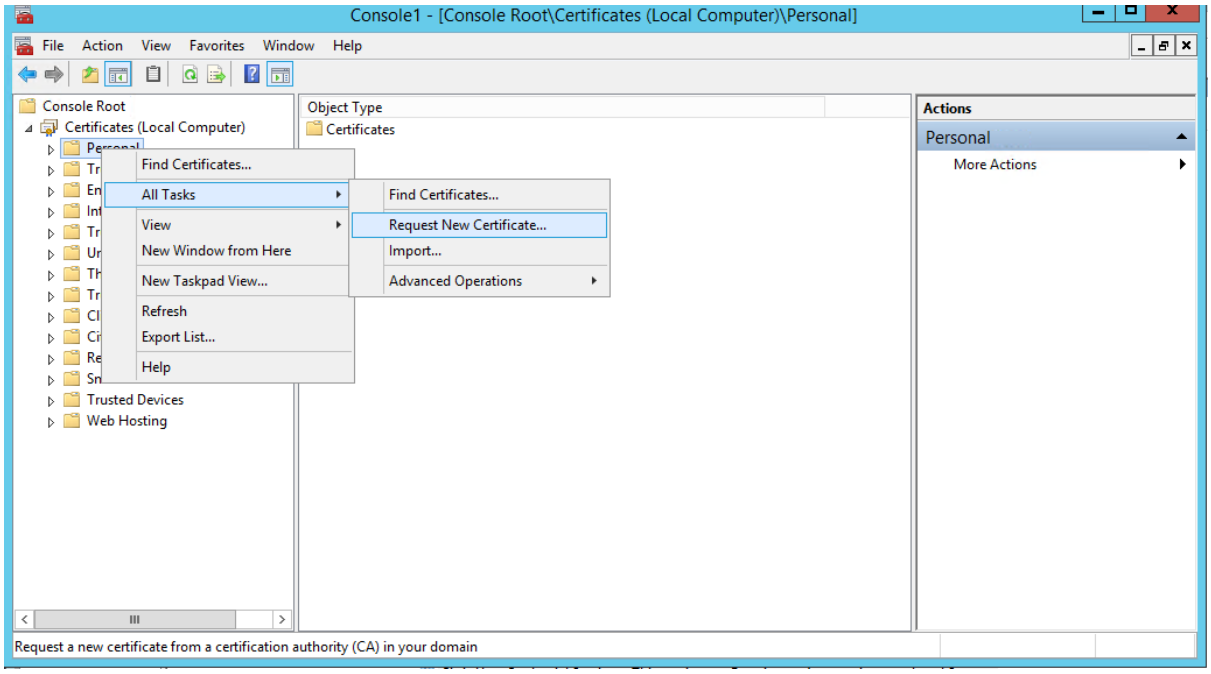


Configuring Microsoft IIS for HTTPS

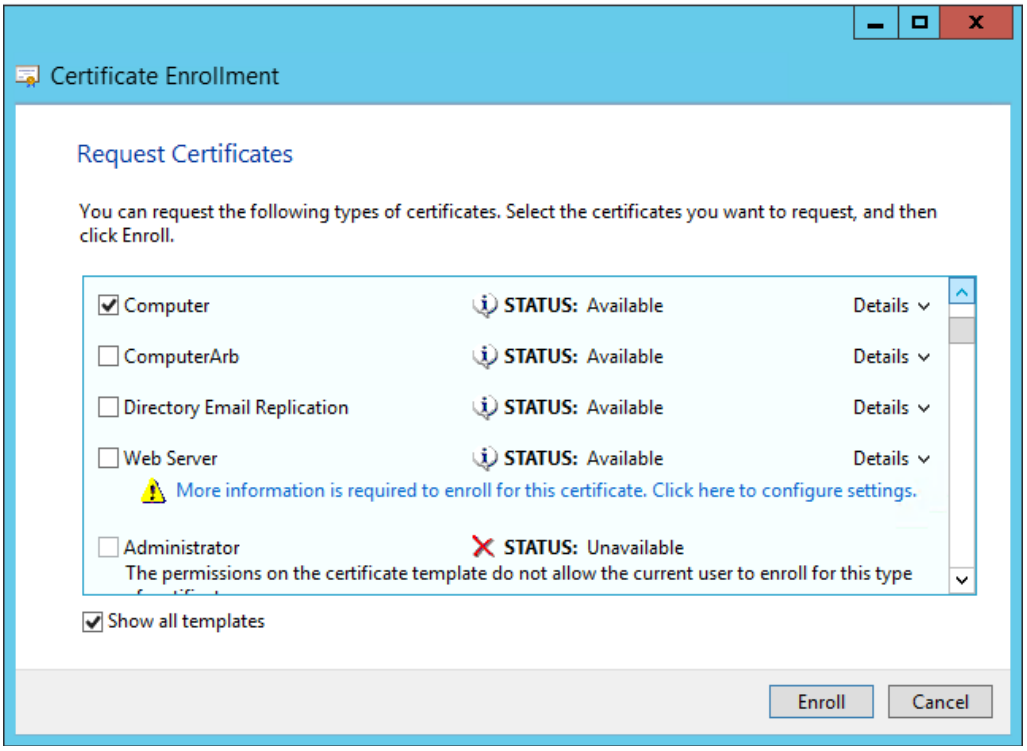
This section describes configuring Microsoft IIS for HTTPS smart card authentication.

Configuring HTTPS on Microsoft IIS

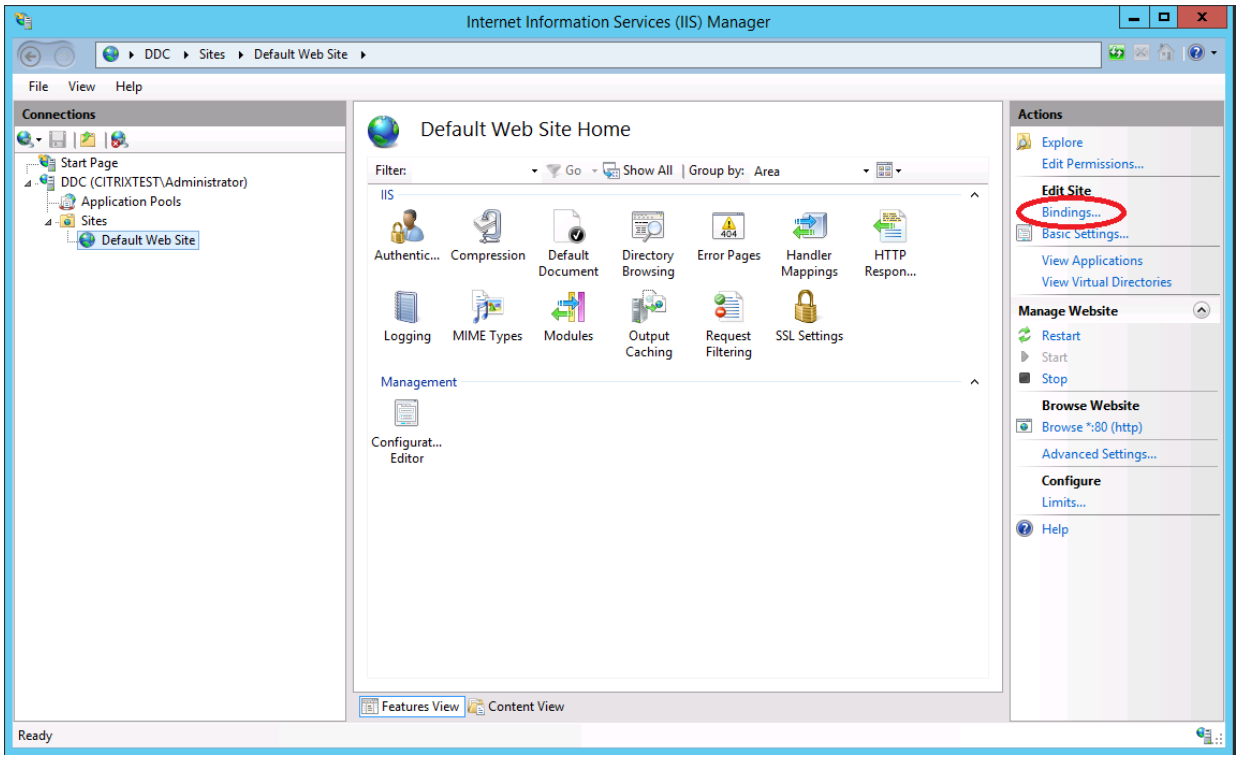
On the XenDesktop DDC server that will host StoreFront, run the Microsoft Management Console (mmc.exe), choose Add/Remove Snapins, and select Certificates for the "Computer account".



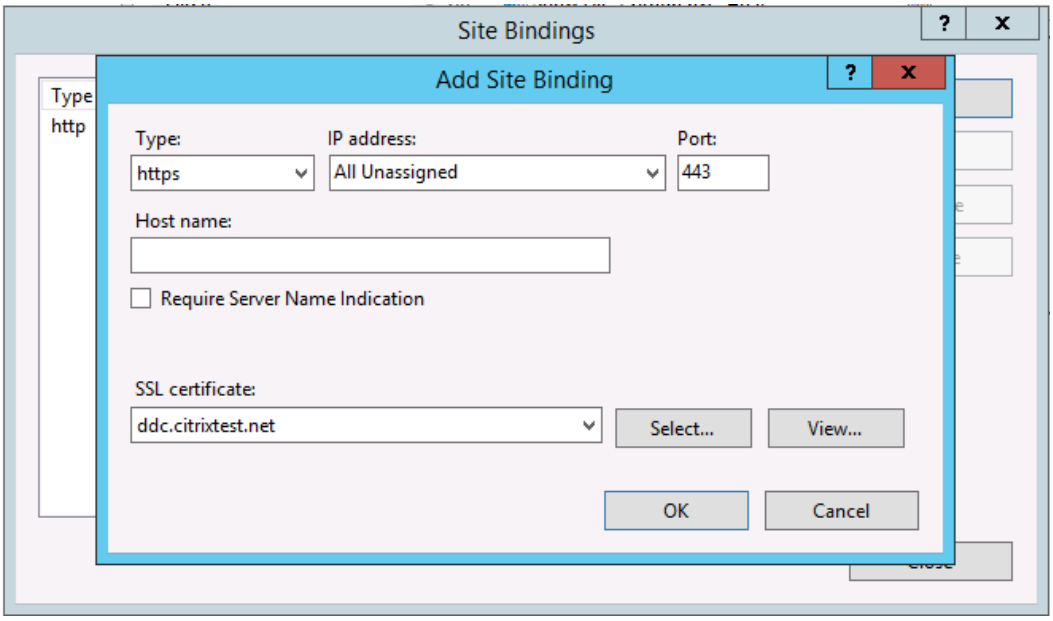
Select "All Tasks → Request New Certificate..." and generate a Computer certificate.



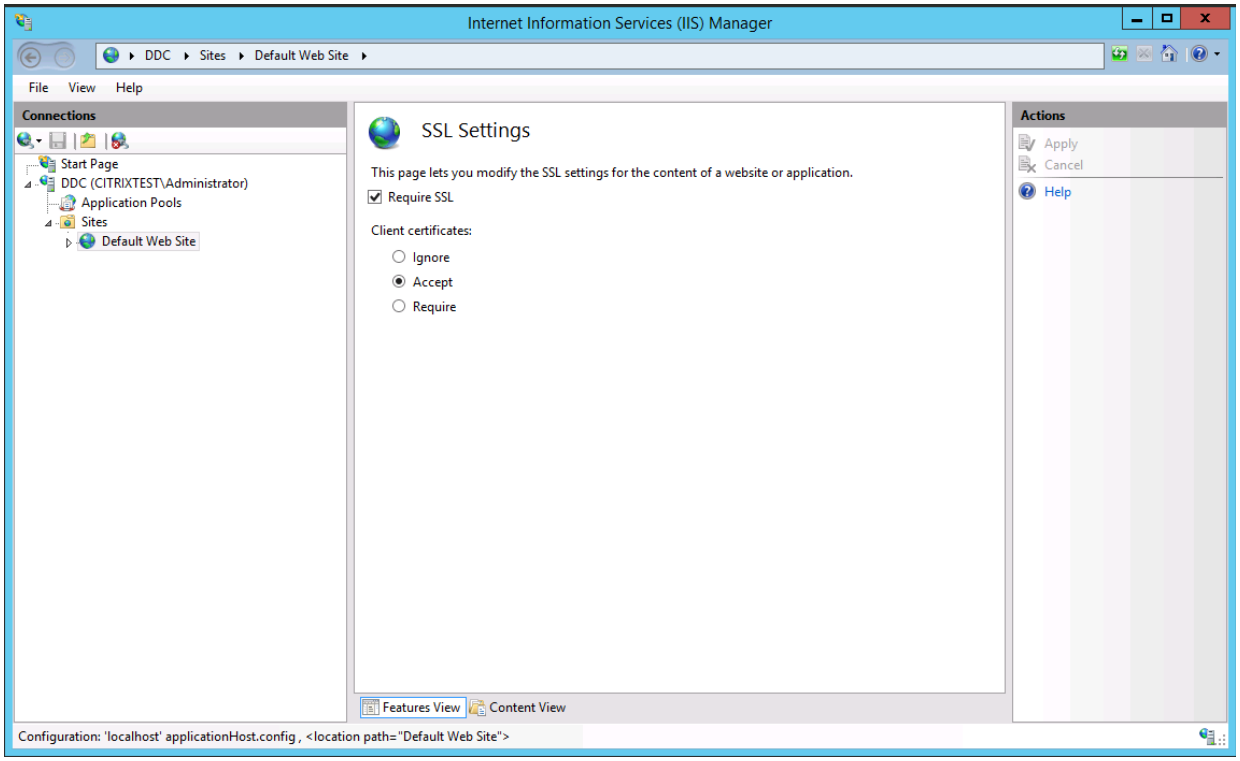
Next start the "IIS Manager" console and choose the "**Bindings**..." option for the default website:



Add HTTPS bindings, selecting the certificate that was created in the MMC:



Finally go to the "**SSL Settings**" for the web-site and select "**Require SSL**" and "**Accept Client Certificate**" for the appropriate endpoints. Note that this step may need to be done after creating the StoreFront store (see the next section):



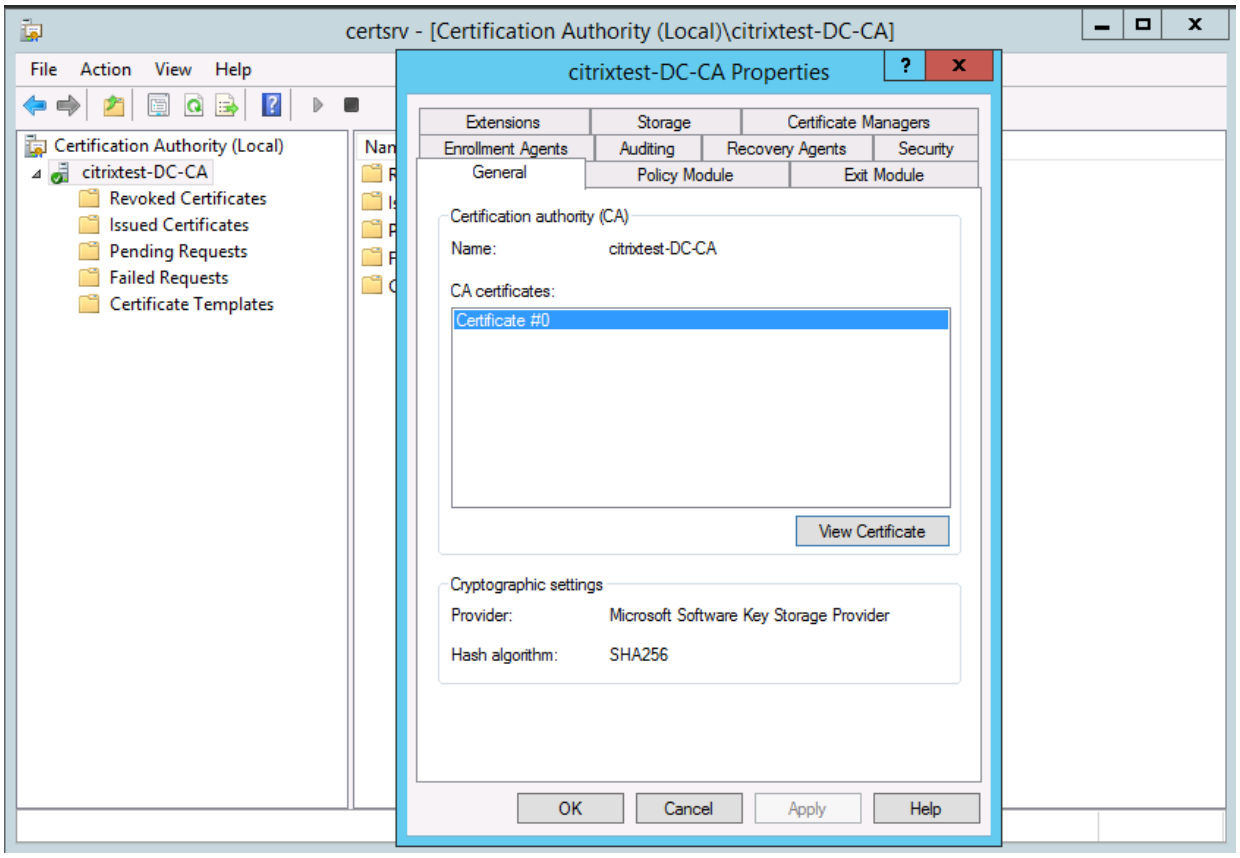
Non-Domain Joined Computers

When a Windows computer joins a domain, it automatically downloads and installs the "Trusted CA" certificates used to authorize the Microsoft Certificate Authority. For non-Windows computers, and for computers not joined to a domain, this can be done manually.

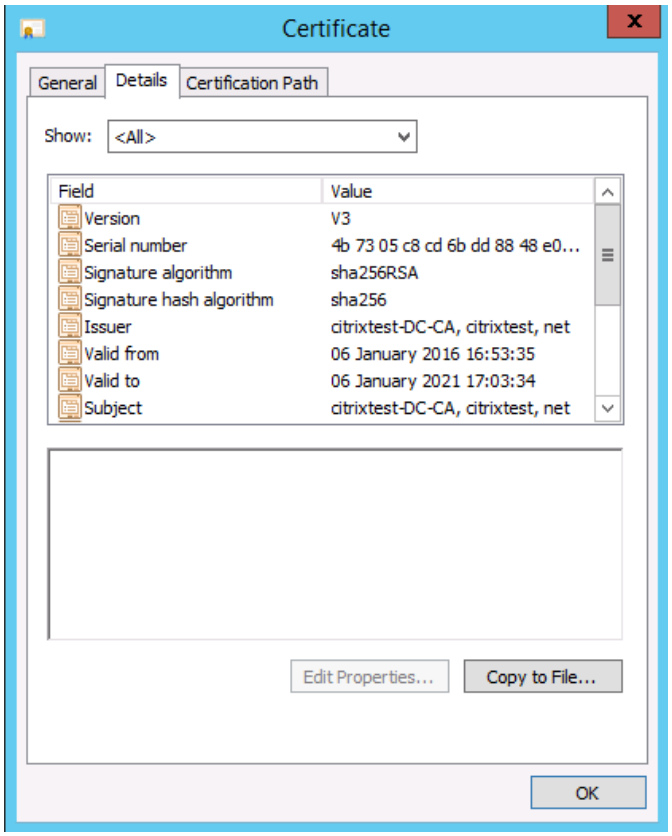
If a CA is not trusted, Web browsers and other security systems will prompt with security warnings whenever visiting Web pages protected by certificates issued by the CA.

Retrieving the CA Certificate from the Microsoft CA

In the Microsoft Certificate Authority, select the CA node and choose "**Properties**..." The CA certificates are shown on the "**General**" tab. Note that you will, in general, only need the most recent CA certificate.

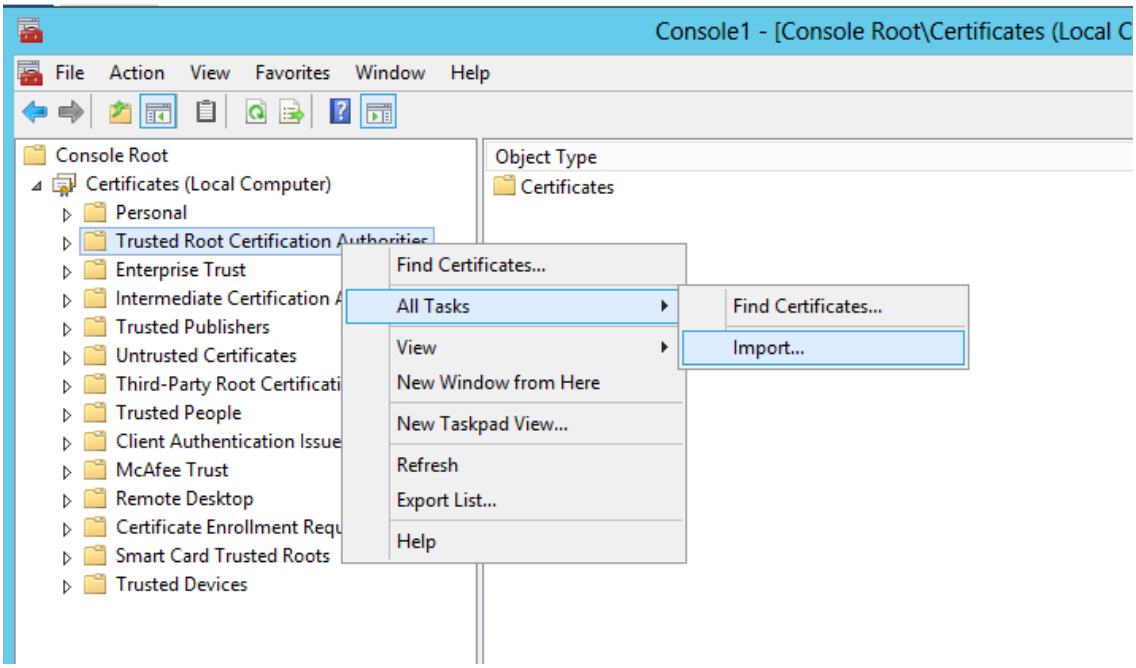


Click "**View Certificate**". On the "**Details**" tab, there is an option to "**Copy to File**". Use this to export the root certificate (use the DER/.cer options). This file can be manually copied to non-domain joined computers.



Installing the Trusted CA Certificate on Windows

To install a trusted CA certificate, run the mmc.exe as Administrator. Add the "**Certificates**" snapin for the Computer Account. Right-click the "**Trusted Root Certification Authorities**" and **Import** the file.

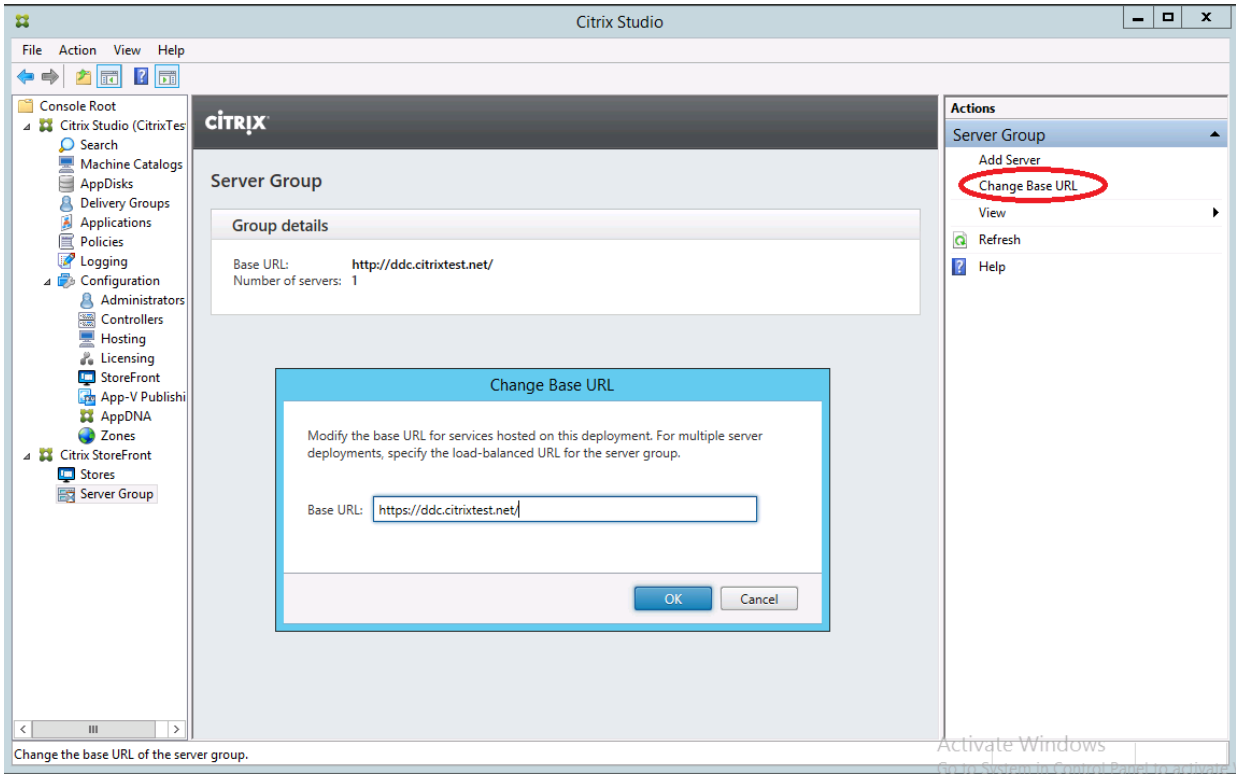


Configuring Citrix StoreFront

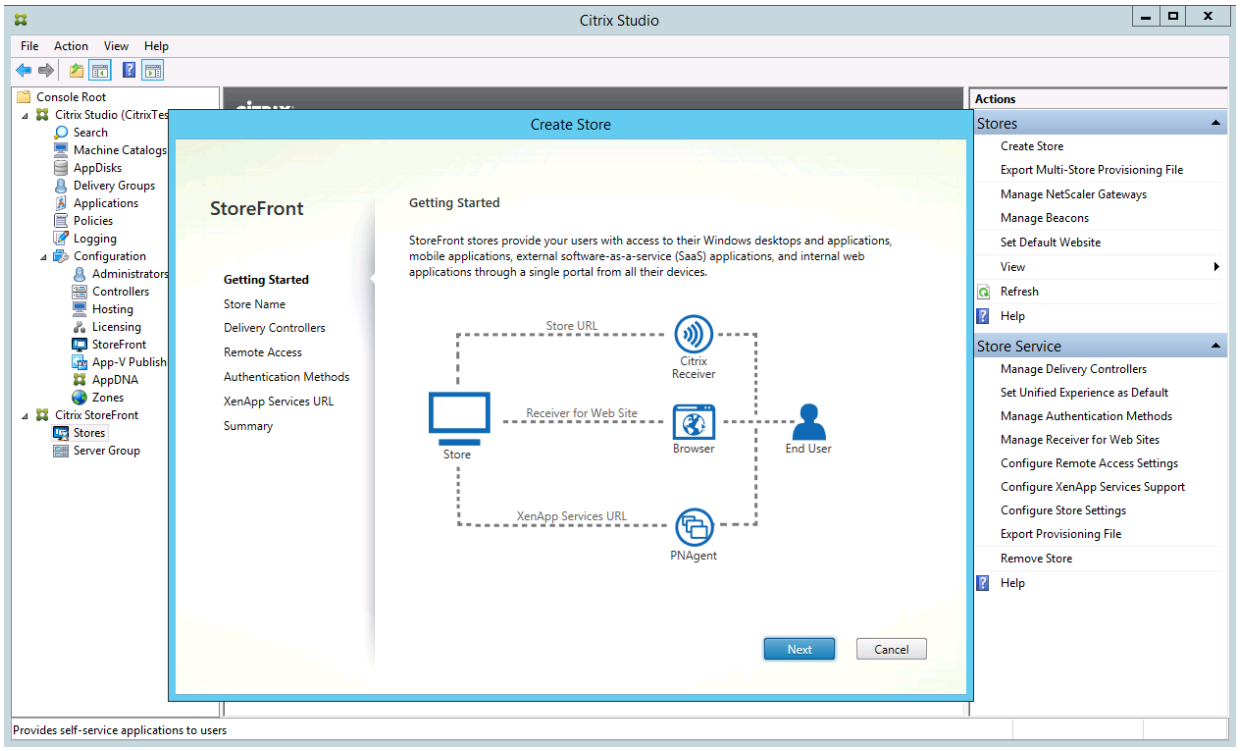
This section describes enabling StoreFront smart card authentication on an IIS server configured for smart card authentication

Creating the Store

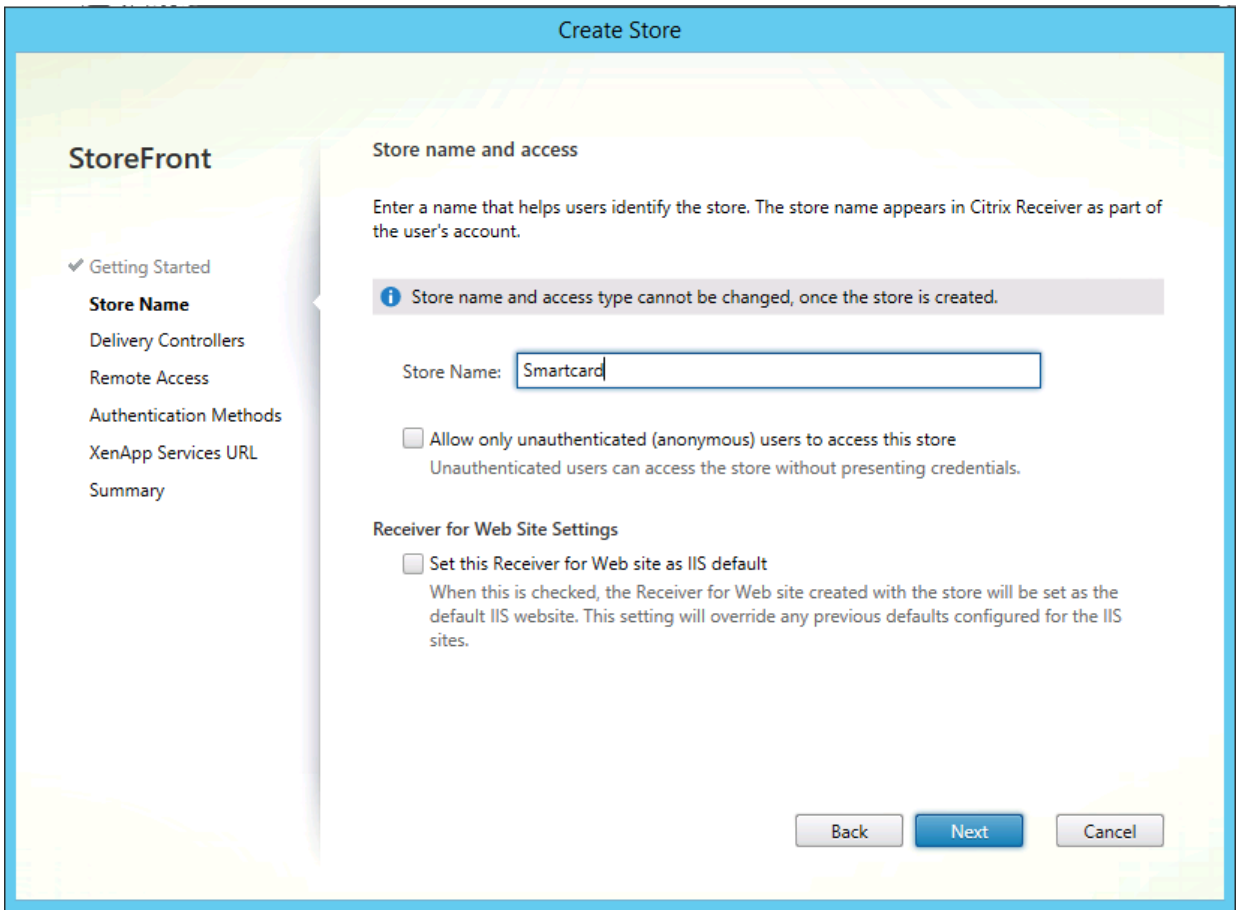
Start the StoreFront Management console. Go to the "**Server Group**" page and select "**Change Base URL**". Ensure that the base URL is set to *https://* rather than ***http://***.



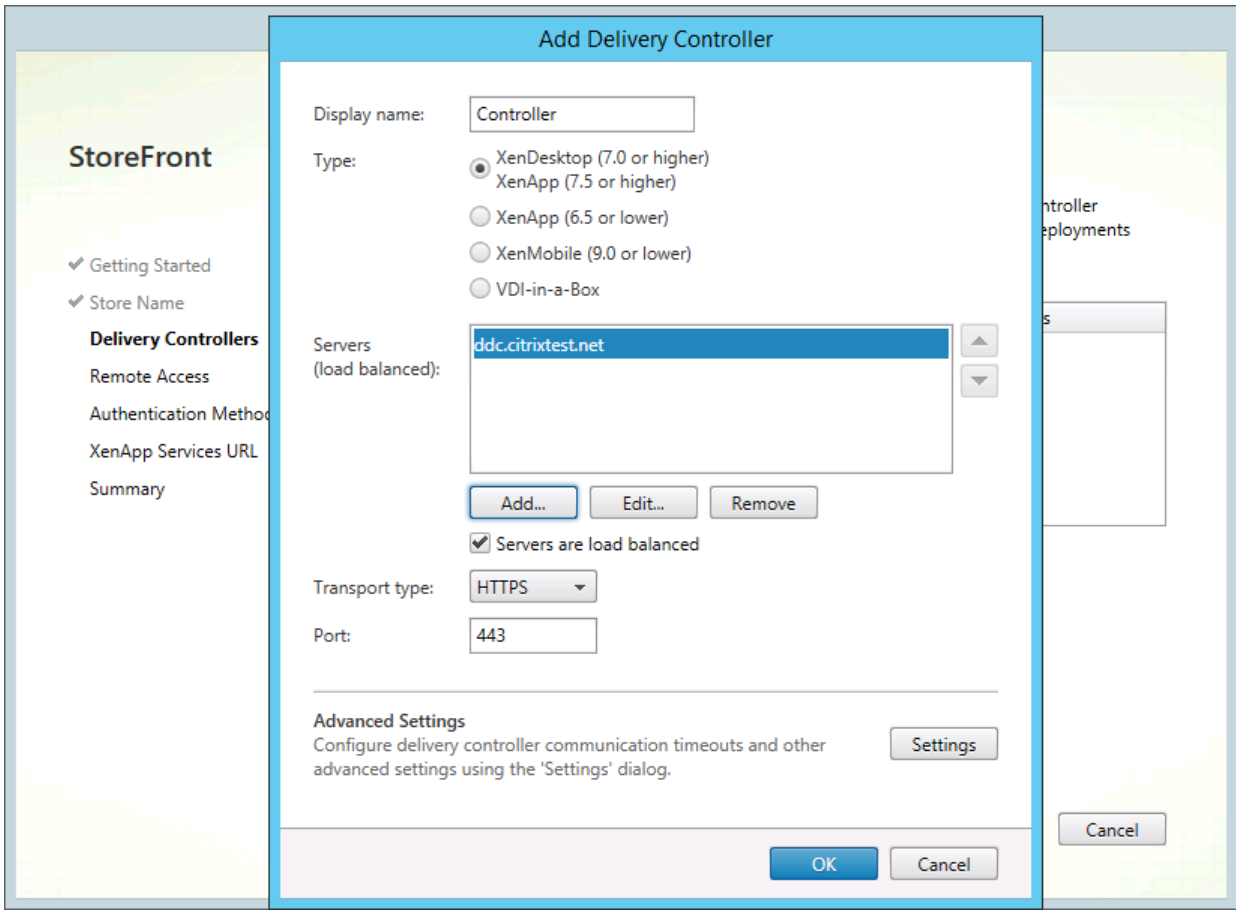
Next select "**Create New Store**..." and follow the wizard:



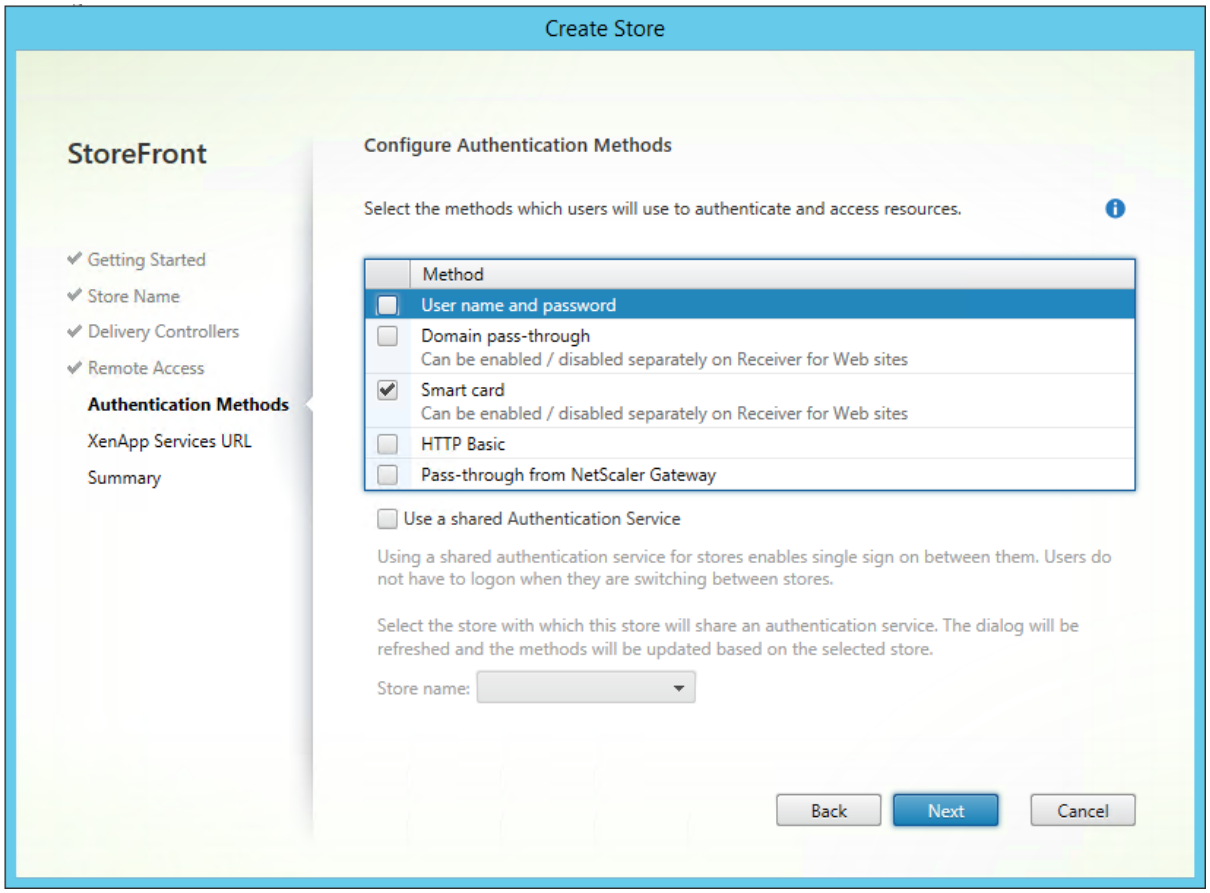
Here we create a store named “Smartcard”, this results in a Web site named “SmartcardWeb” being accessible from a web-browser.



Note that the XenDesktop DDC should be configured for HTTPS by following the instructions to configure IIS. If this has been done, for example: StoreFront and the XenDesktop DDC are running on the same machine, then the Transport Type should be set to HTTPS and the address is the same as that used in a Web browser: computer.fqdn.com.



Finally, configure the smart card authentication for this store, disabling any other options.

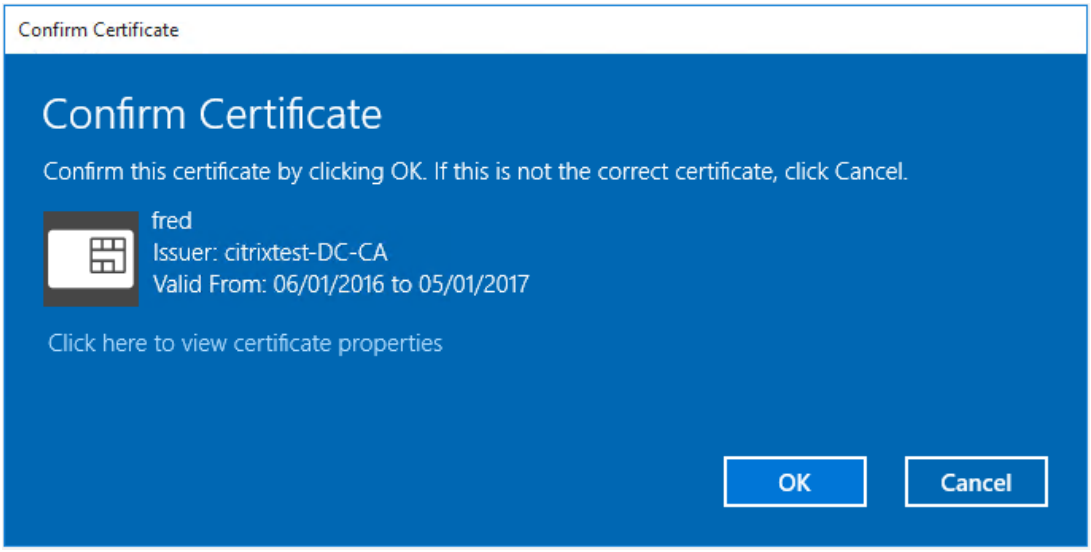


Confirm that Smart card HTTPS authentication is working

From the domain joined machine where the smart card is inserted start Internet Explorer and connect to:

https://computer.fqdn/Citrix/SmartcardWeb

Note that the storename must have Web appended. The Web browser should request the smart card PIN.



Check that the fred@citrixtest.net can log in to StoreFront.

Configuring the XenDesktop DDC

In a standard deployment, StoreFront uses the end user's password credentials to authenticate the end user to the XenDesktop DDC. With a smart card the XenDesktop server must be instructed to "trust" the StoreFront server to validate the smart card.

Note that this does not affect authentication to the end VDA, only the authentication for the session brokering logic.

Trusting Storefront to authenticate users

On the DDC machine, run PowerShell as Administrator and type:

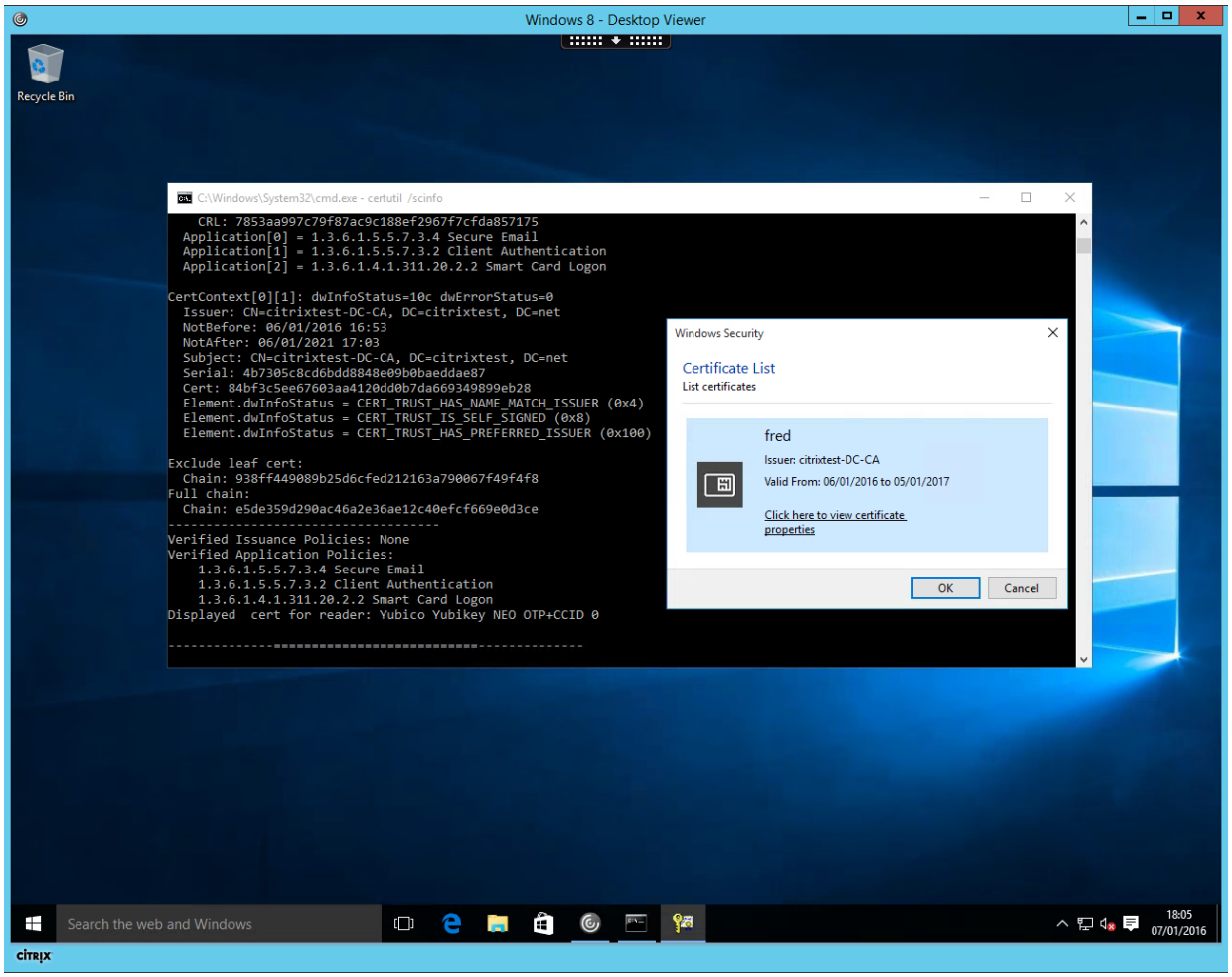
```
Add-PSSnapin Citrix.*

Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $True
```

The broker will now "trust" the StoreFront server to correctly authenticate the user. Note that this may not be appropriate for all deployment options of StoreFront.

Launching a smart card session from a web browser

Return to the machine where the smart card is inserted and launch a published Desktop. Once logged in, ensure that the smart card is correctly remoted by running:

```
Certutil /scinfo
```

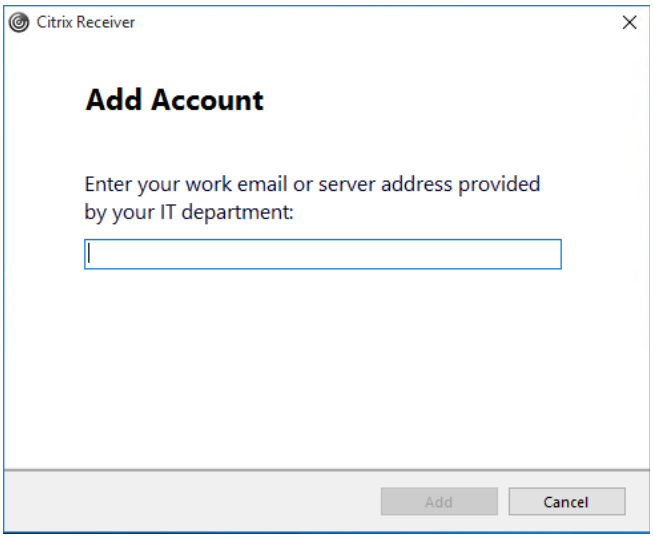


Configuring Citrix Receiver for Windows

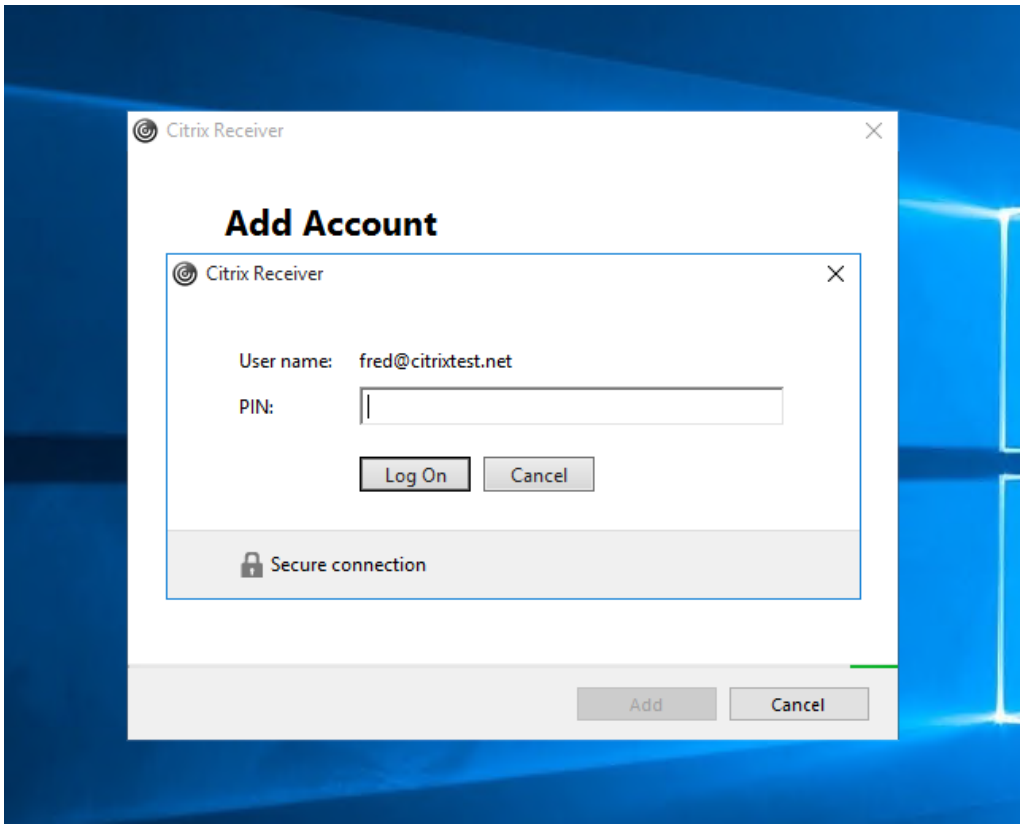
When run on domain joined machines, Internet Explorer should work without further configuration. For non-domain joined machines, Internet Explorer will display security warnings unless the domain root certificate into the computer's Trusted Root Certificate store.

Configuring the Citrix Receiver

Locate the Citrix Receiver icon in the Task bar and choose "Open" from the context menu:



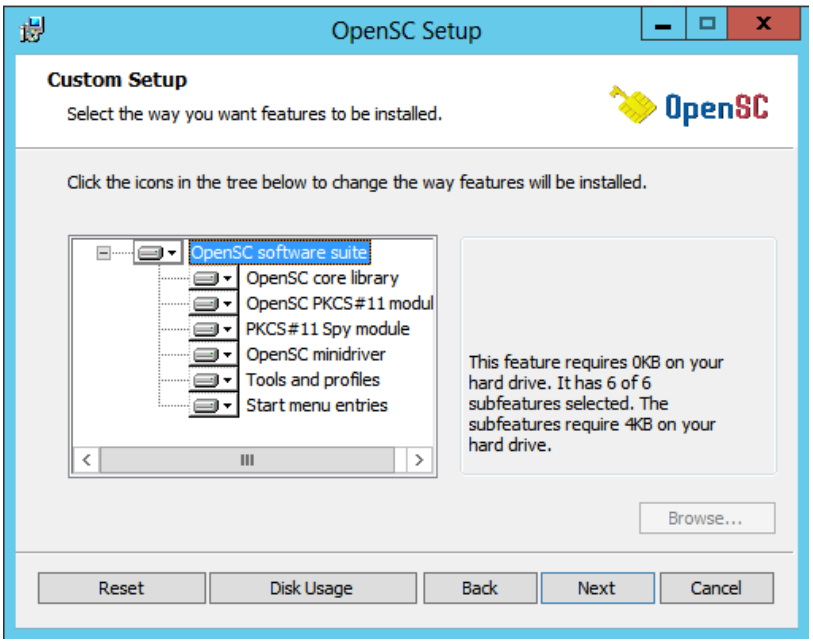
Enter https://<serverfqdn>/Citrix/Smartcard (note that the SmartcardWeb extension is not used here). Check that the tool performs smart card prompts.



As before, ensure that the connection launches and runs with an HDX connection by checking the output of `certutil /scinfo`.

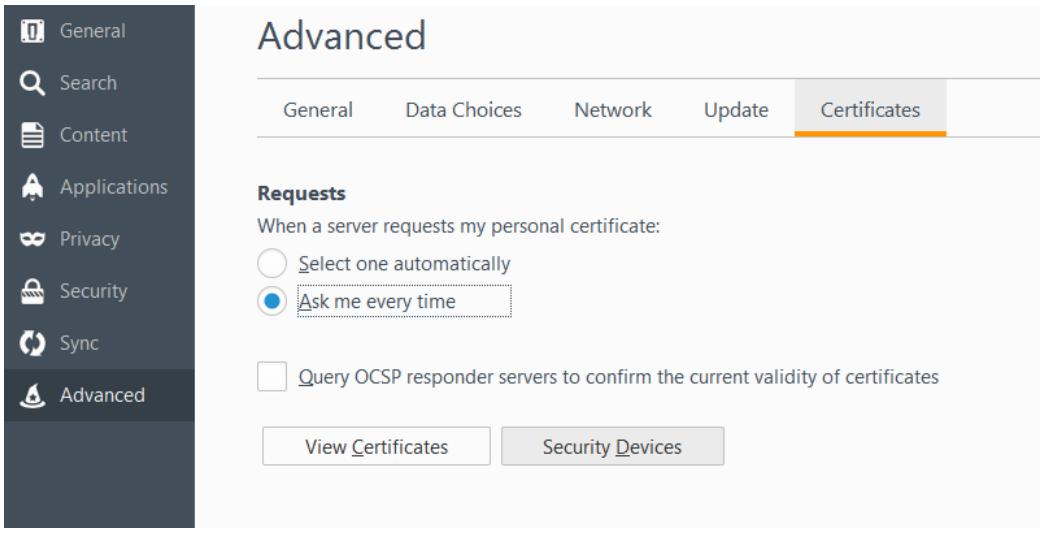
Firefox for Windows

Download the **opensc-xxxx-win32.msi** installer from the OpenSC project website and install, checking the MD5 checksum of the downloaded file. Ensure that the **OpenSC PKCS#11 module** is included in the installer.

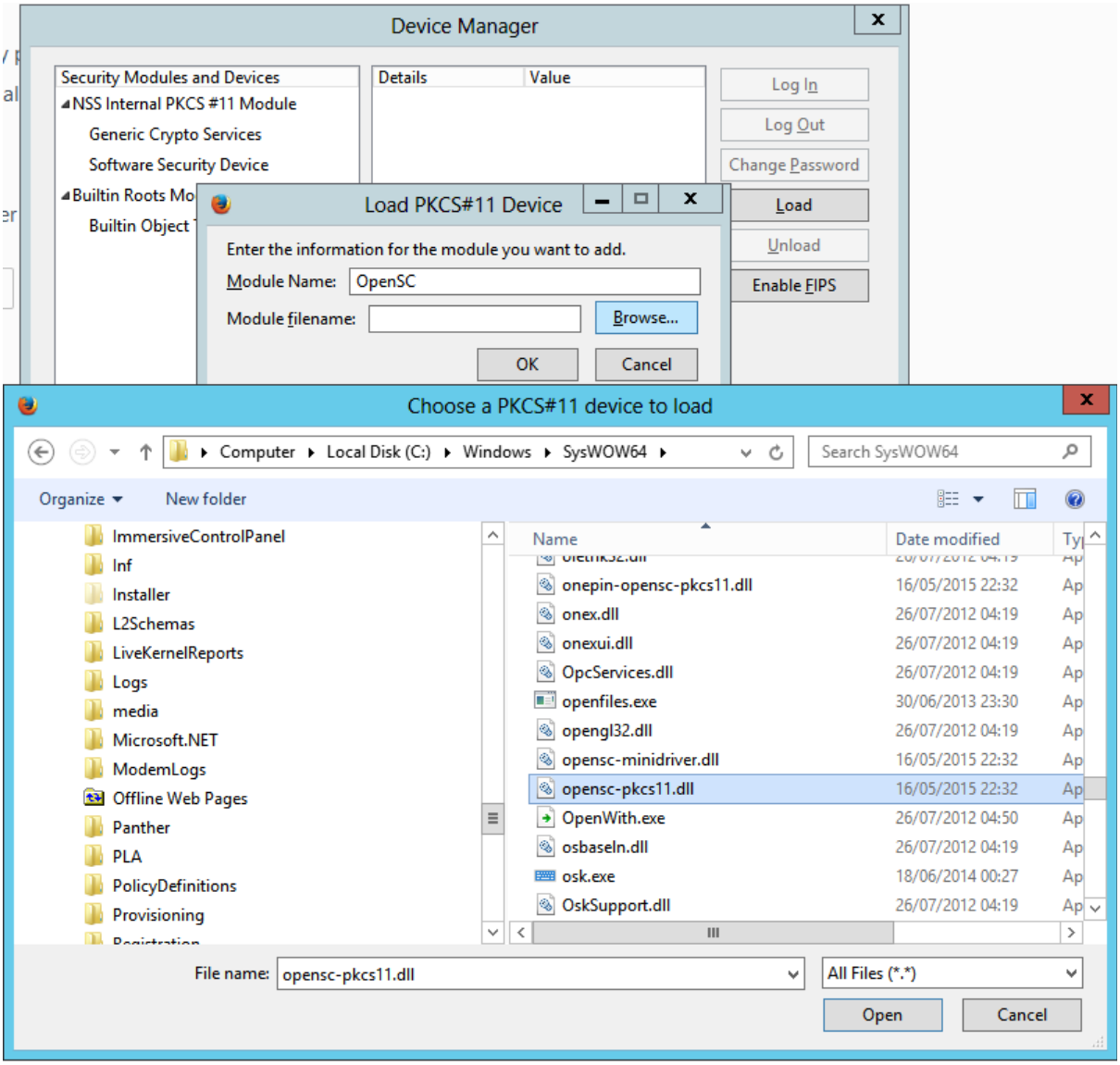


Note that the **opensc-pkcs11.dll** is installed to the **c:\Windows\SysWOW64** directory on 64bit Windows.

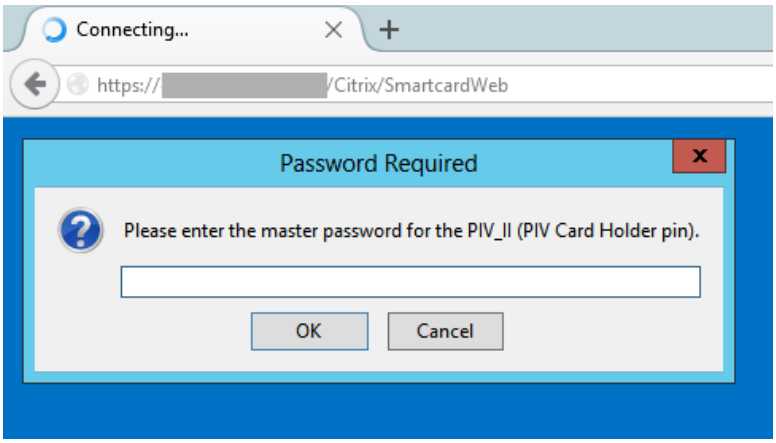
Open Firefox's Preferences dialog and go to the Advanced->Certificates tab. Select "**Security Devices**":



"Load" a new device named "**OpenSC**" and locate the opensc-pkcs11.dll file



Finally exit and **restart** Firefox to confirm that it can authenticate to the StoreFront server.



Configuring Citrix Receiver for Linux

To configure Citrix Receiver for Linux, including Rasperry Pi versions, ensure that the OpenSC package is installed:

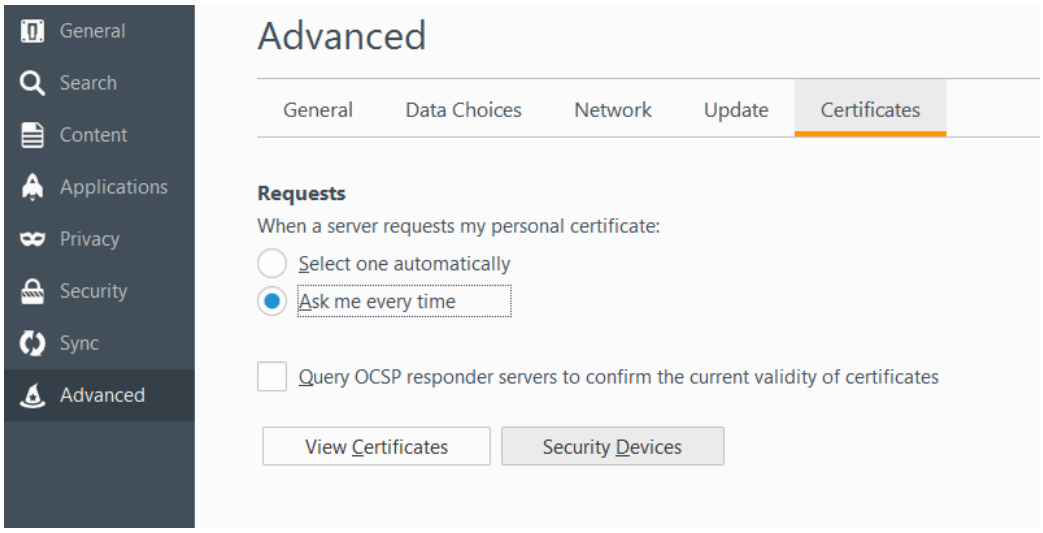
- RedHat and derivatives: `sudo yum install pcsc-lite opensc`
- Debian and derivatives: `sudo apt-get install pcscd opensc`

For Linux Native Receiver

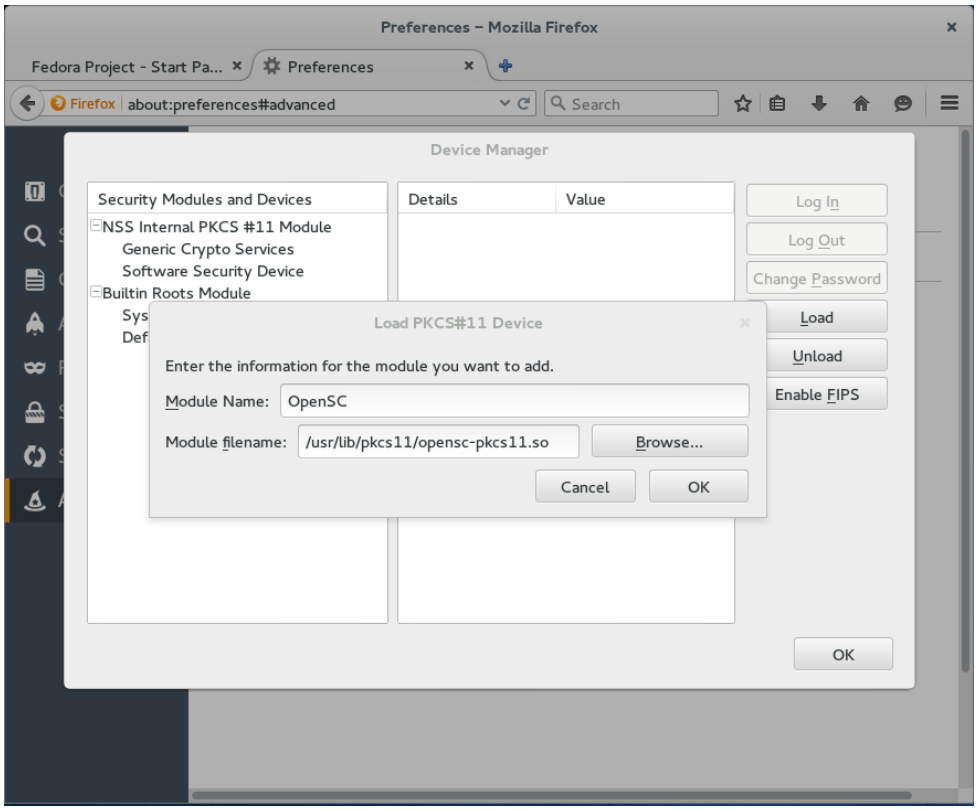
Citrix Receiver for Linux will automatically detect and configure smart cards through OpenSC. Older versions can be configured to use opensc-pkcs11.so through AuthManConfig.xml.

Configure Firefox on Linux

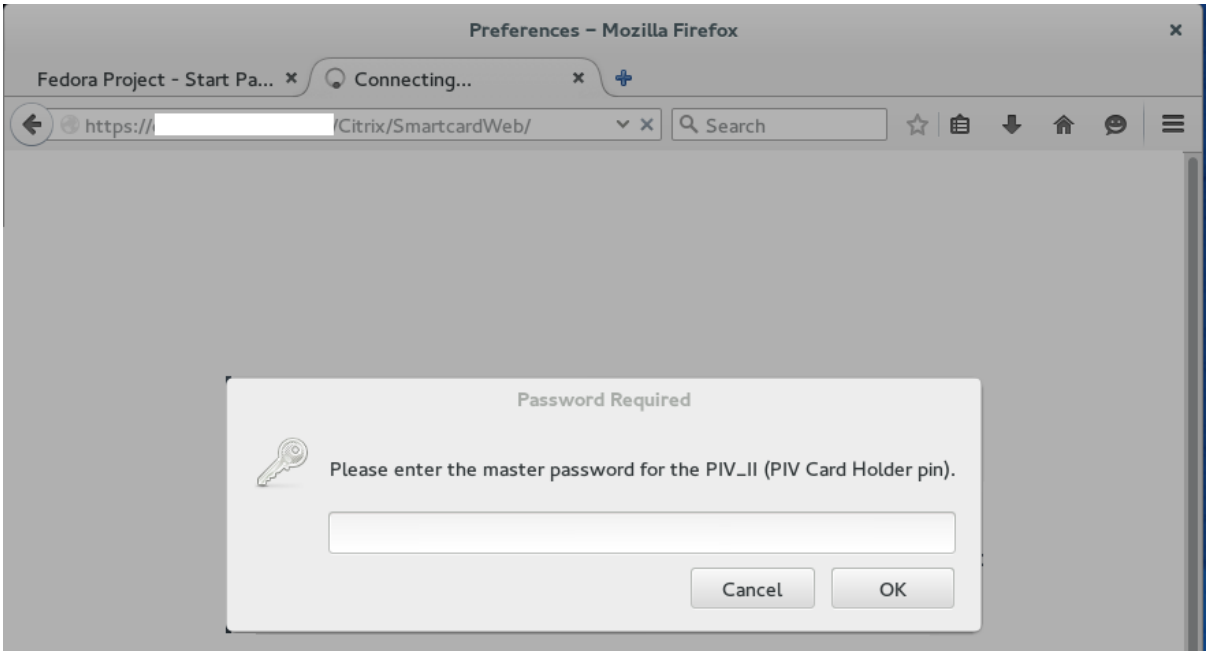
Open the Firefox preferences dialog. Select the "Security Devices" option in Advanced/Certificates



Click "Load" and specify a new module name. Use "Browse" to locate the file "/usr/lib/pkcs11/opensc-pkcs11.so"



Check that StoreFront for Web is functioning by restarting Firefox and visiting https://computer.fqdn/Citrix/SmartcardWeb .



Configuring Citrix Receiver for OSX

Smart card support in OSX is an optional add-on using packages that can be easily downloaded from an appropriate Web site. Always check the cryptographic identity of software before installing.

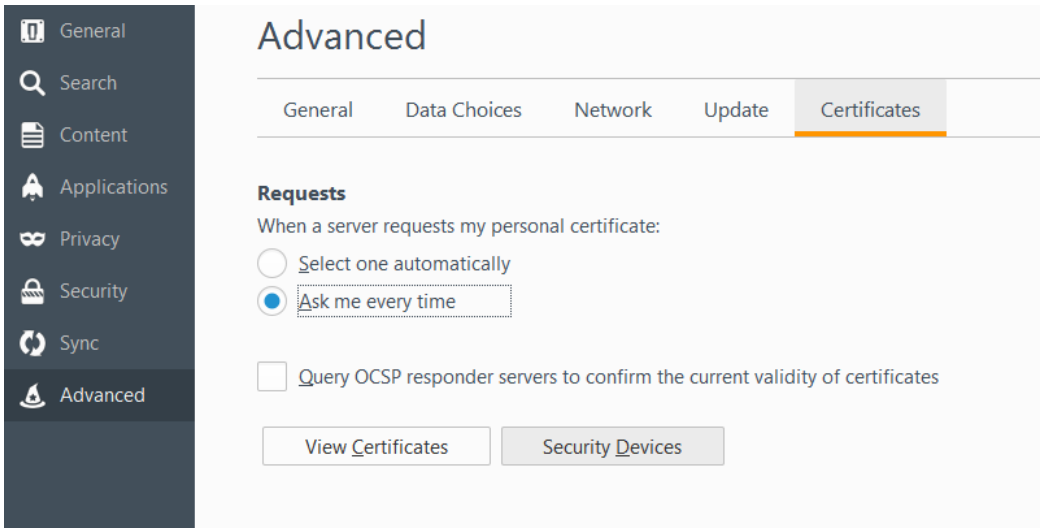
Installing smart card support for Safari

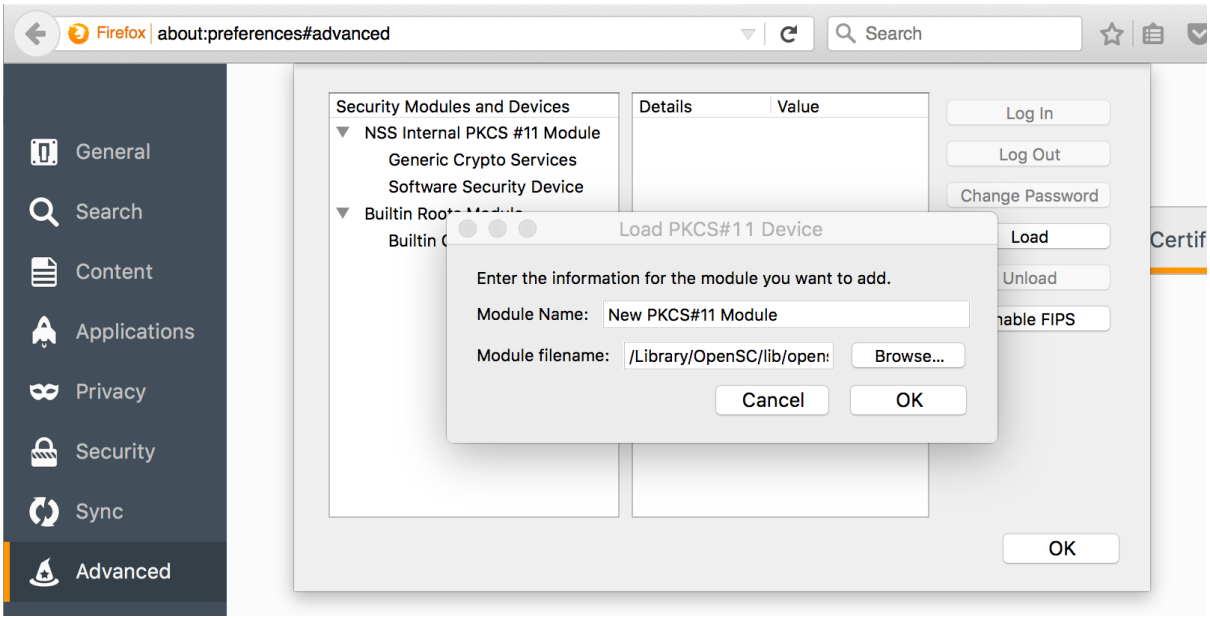
Install the Apple Smart Card Services package from smartcardservices.macosforge.org, ensuring that the files are correctly signed by Apple. PIV smart cards should automatically be available to Safari through the Keychain Access tool.

Firefox on Mac OSX

Download the OpenSC installer for Mac OSX, ensuring that the files are correctly signed. Run the install Wizard to install the PKCS#11 APIs:

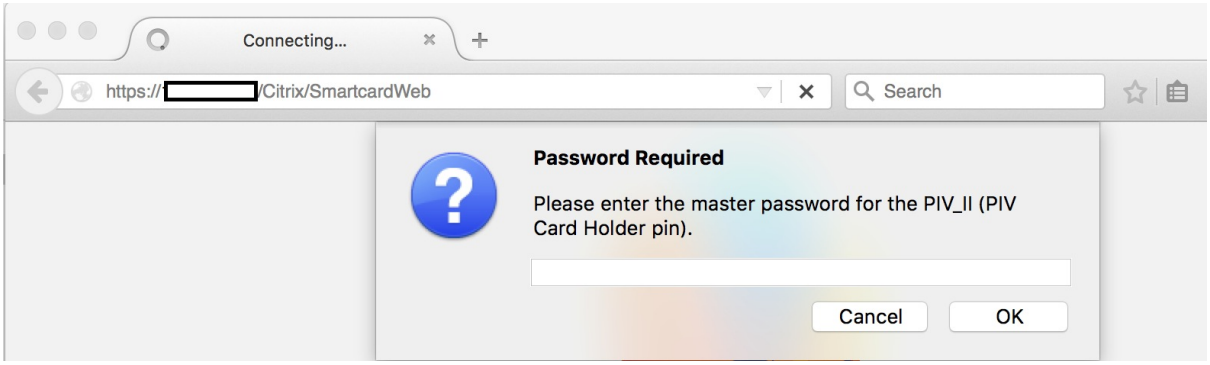
Open the Firefox preferences dialog. Select the "Security Devices" option in Advanced/Certificates:





The opensc-pkcs11.so library is installed in [/System]/Library/OpenSC/lib/pkcs11/opensc-pkcs11.so.

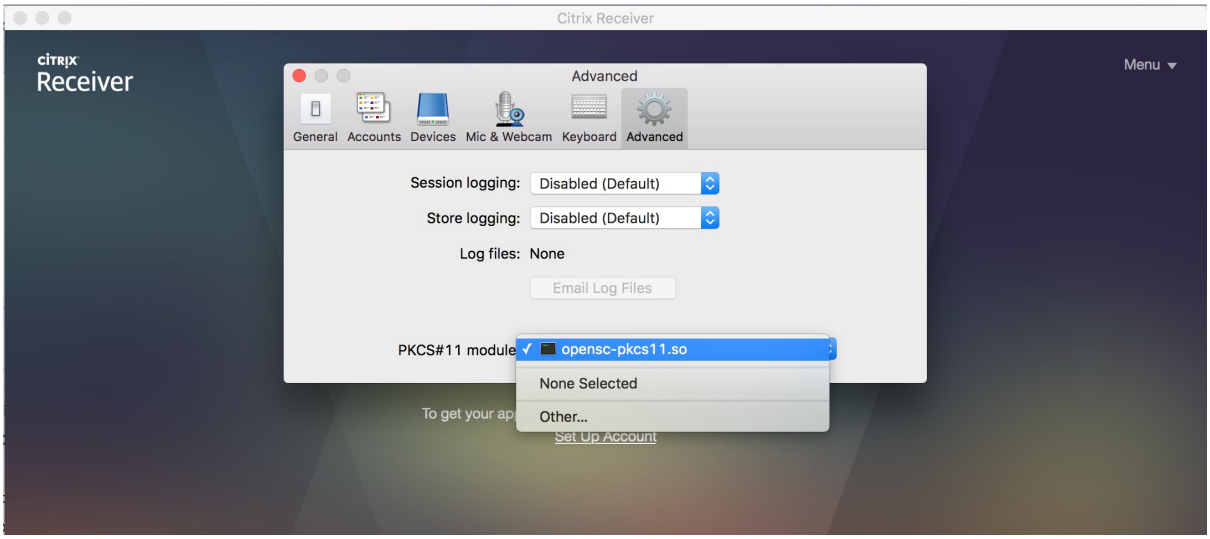
Exit and restart Firefox before checking that the smart card is working correctly.



Configuring Citrix Receiver for Mac to use NetScaler Authentication

If you wish to use your smart card to authenticate with NetScaler, install OpenSC as described in the "Firefox on Macintosh" section.

Open Citrix Receiver and go to the "Citrix Receiver → Preferences…" GUI.



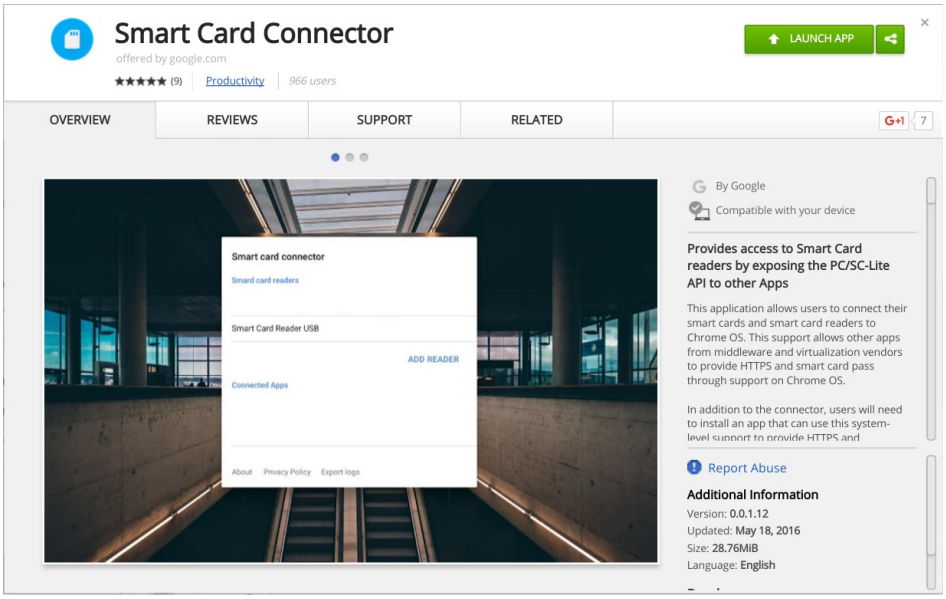
The opensc-pkcs11.so library is installed in [/System]/Library/OpenSC/lib/pkcs11/opensc-pkcs11.so.

Configuring Citrix Receiver for ChromeOS

Smart card support in ChromeOS is packaged as an extension in the Google Play Store. There are two components to install, the smart card connector and CACKey smart card driver.

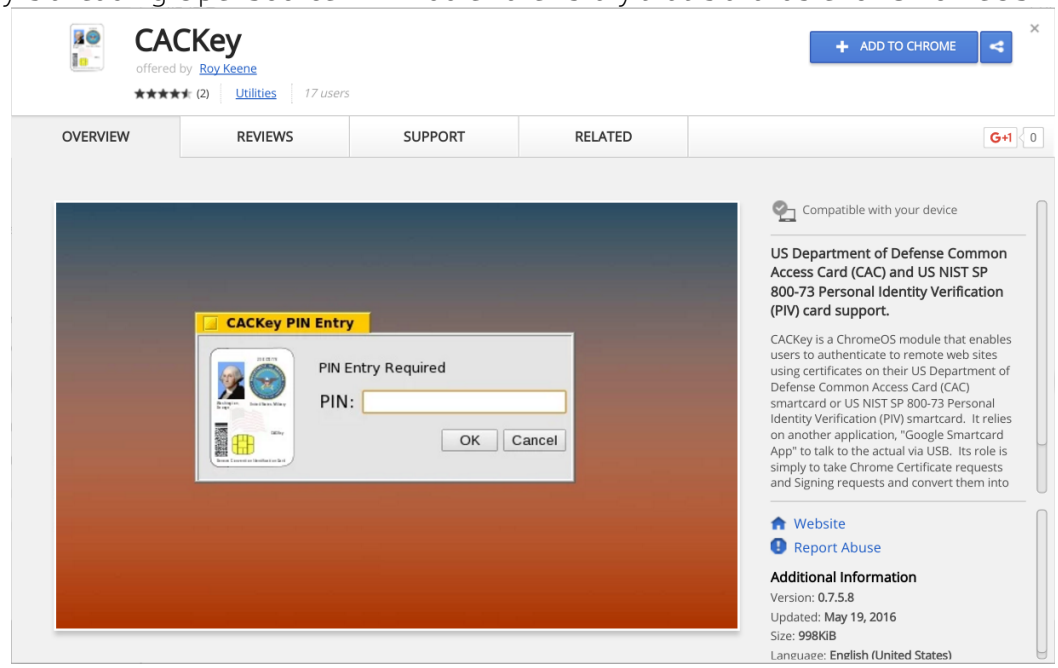
Installing the "Smart Card Connector"

Install the Google Smart Card Connector application. This provides direct access to the smartcard reader:

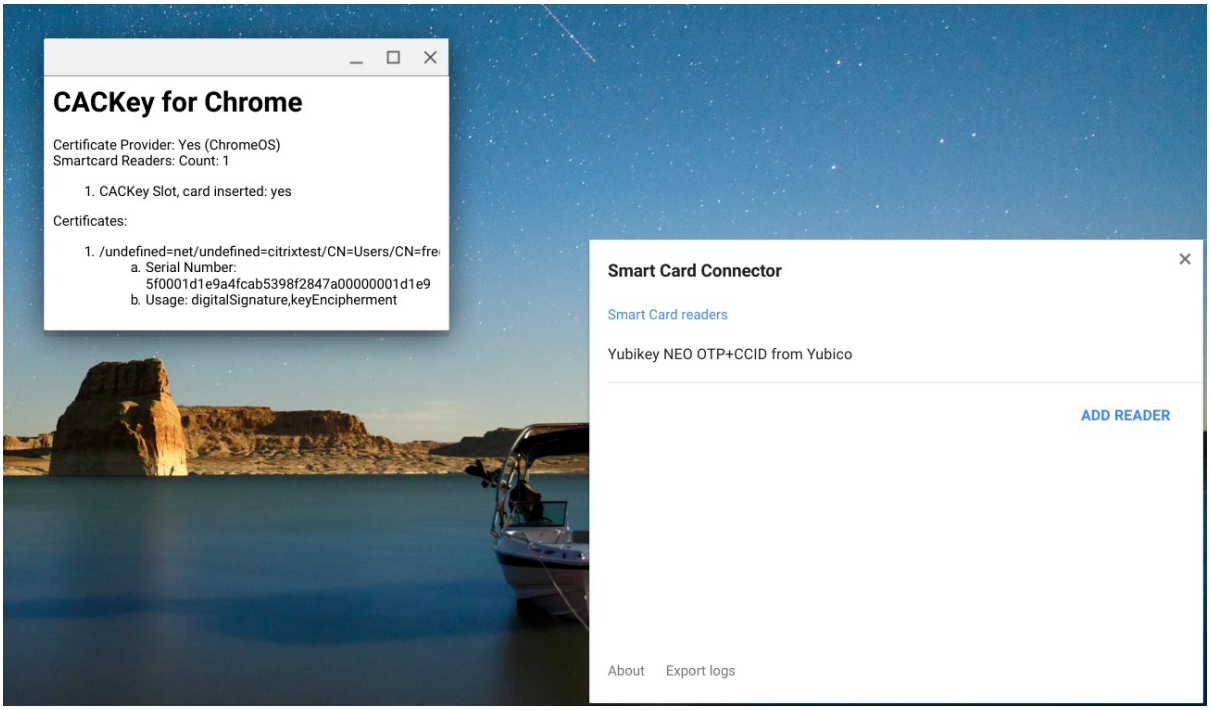


Installing the "CACKey" Smart Card driver

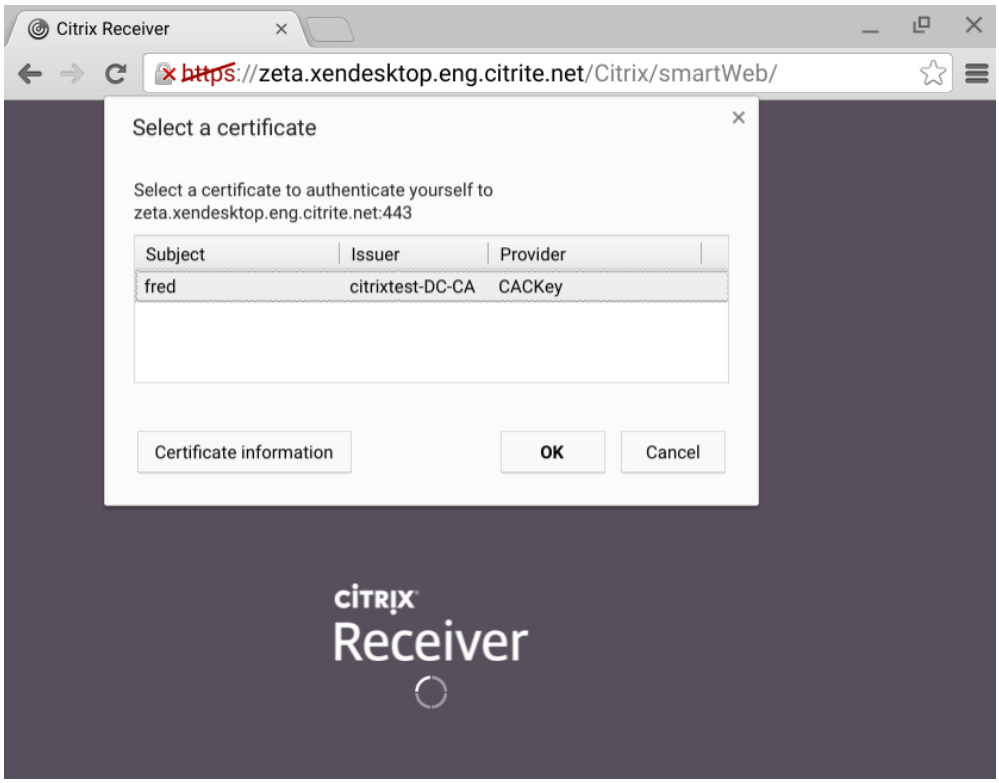
CACKey is a leading OpenSource PIV middleware library that is available for ChromeOS:



Once installed, reboot the ChromeOS device, insert the Yubikey and launch the Smart Card Connector first, followed by the CACKey extension.



The web browser automatically uses the CACKey to authenticate to StoreFront:



References

PIV specifications:	http://csrc.nist.gov/groups/SNS/piv/standards.html
NIST PIV test cards:	http://csrc.nist.gov/groups/SNS/piv/testcards.html
Yubikey 4:	https://www.yubico.com/products/yubikey-hardware/yubikey4/
OpenSC:	https://github.com/OpenSC/OpenSC/wiki
SC Services for OSX:	https://smartcardservices.macosforge.org/
CACKey	http://cackey.rkeene.org/fossil/index