SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for VMware Horizon 7

gemalto
security to be free

Document Part Number: 007-013751-001, Rev. A

Release Date: February 2017

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as VMware Horizon 7.

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*.

Horizon 7 provides a streamlined approach to delivering, protecting and managing virtual desktops (VDI) and apps while containing costs and ensuring that end users can work anytime, anywhere, across any device.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to VMware Horizon 7 using Gemalto tokens and smart cards.

It is assumed that the VMware Horizon 7 environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

VMware Horizon 7 can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode** - SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode** - IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.
- **VMware Horizon 7**

For more details about the different SAC installation modes, refer to the SafeNet Authentication Client Administration Guide.

Environment

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

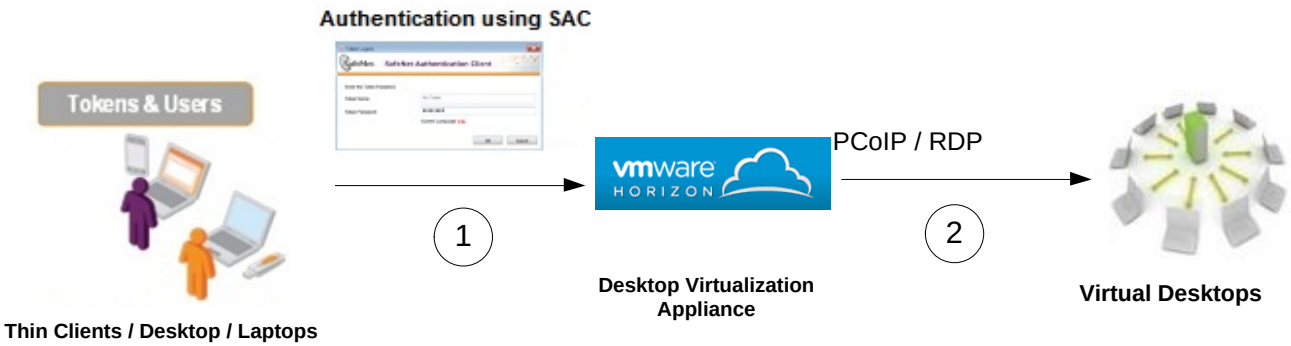
- **SafeNet Authentication Client (SAC)**— *version 10.2*
- **VMware Horizon 7**

Audience

This document is intended for system administrators who are familiar with VMware Horizon 7, and are interested in adding certificate-based authentication capabilities using Gemalto tokens and smart cards.

CBA Flow using SafeNet Authentication Client

1. A user attempts to connect to the VMware Horizon 7 server using the VMware Horizon 7 client application. The user inserts the Gemalto token/smart card on which his certificate resides, and, when prompted, enters the token/smart card 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 VMware Horizon 7 using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. In this guide, the integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) must be configured with an MS CA Connector. For further details, refer to the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a Gemalto token/smart card enrolled with an appropriate certificate.
- SafeNet Authentication Client 10.2 must be installed on all client machines.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of authenticators that can be used as a second authentication factor for users who authenticate to VMware Horizon 7.

SafeNet Authentication Client 10.2 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

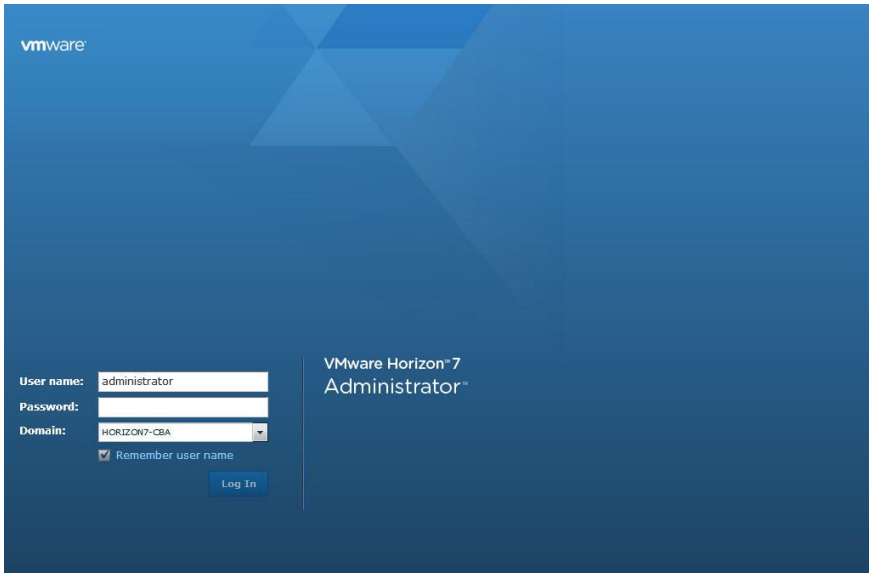
For a complete list of supported authenticators, refer to the *SafeNet Authentication Client Customer Release Notes*.

Configuring VMware Horizon 7

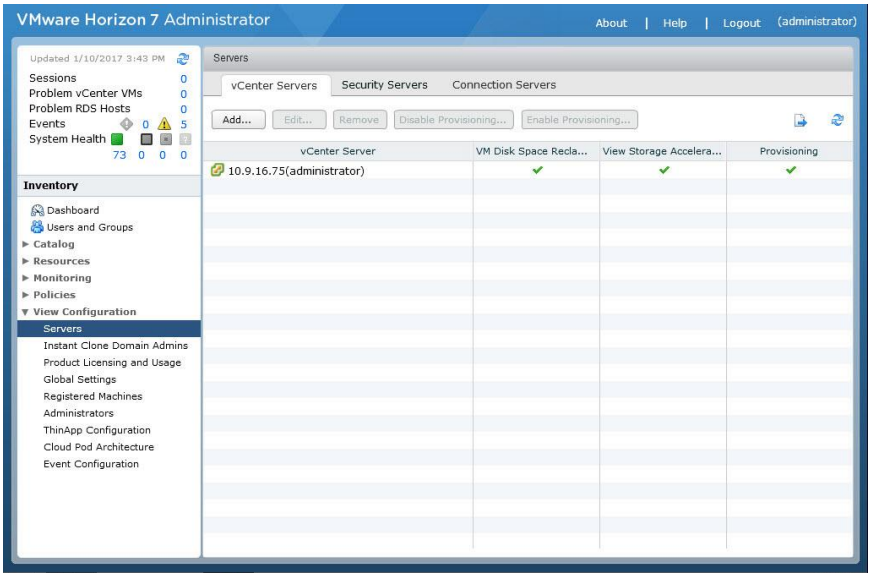
This section describes configuration VMware Horizon 7 to authenticate with Gemalto tokens and smart cards using SafeNet Authentication Client.

This document assumes that VMware Horizon 7 environment is configured with standard LDAP authentication (username and password).

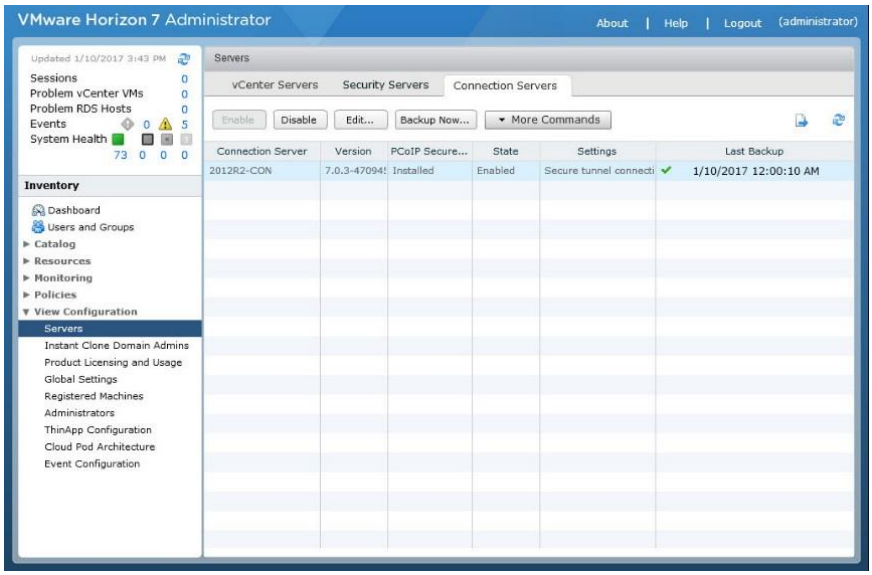
1. Login to the VMware Horizon 7 administrator console using the url: https://<HorizonServer>/admin



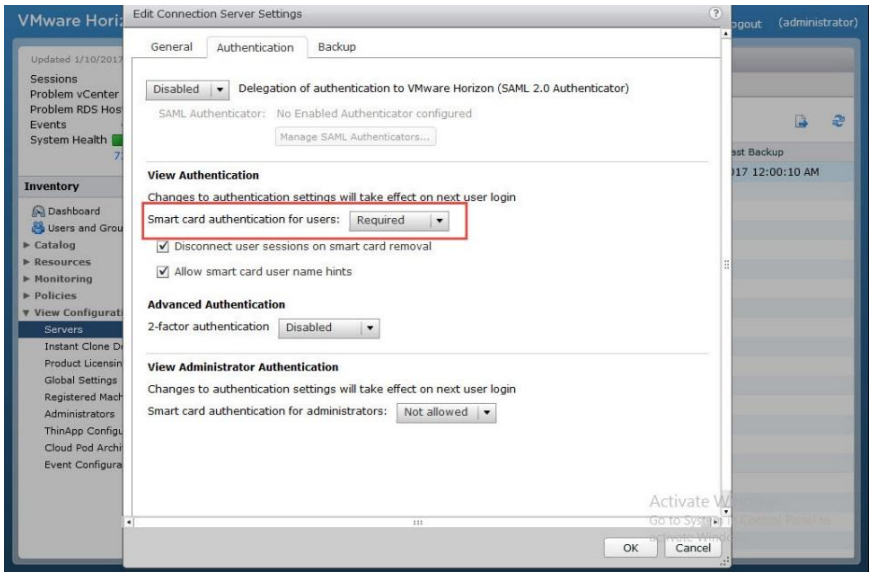
2. Under Inventory, select **View Configuration > Servers**



3. In the Servers window, select the **Connection Servers** tab,



4. Select your Connection Server and click **Edit**.
5. On the Edit Connection Server Settings, click on the **Authentication** tab
6. Under **View Authentication** > **Smart card authentication for users** select **Required**.



7. Click **OK.**

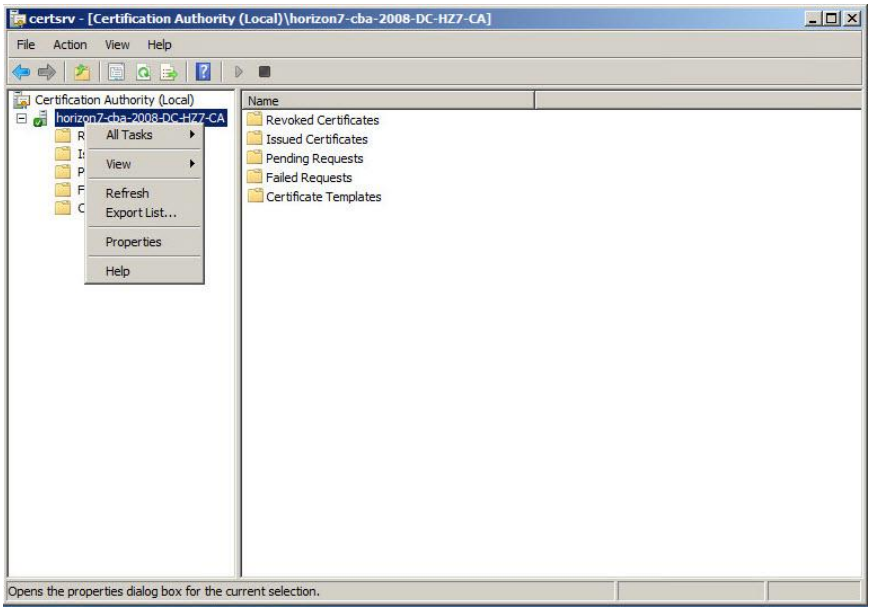
Setting Certificates in VMware Horizon 7

In this section we will obtain and import the CA certificate to the VMware Horizon 7 connection server in order to enable CBA, by performing the following steps:

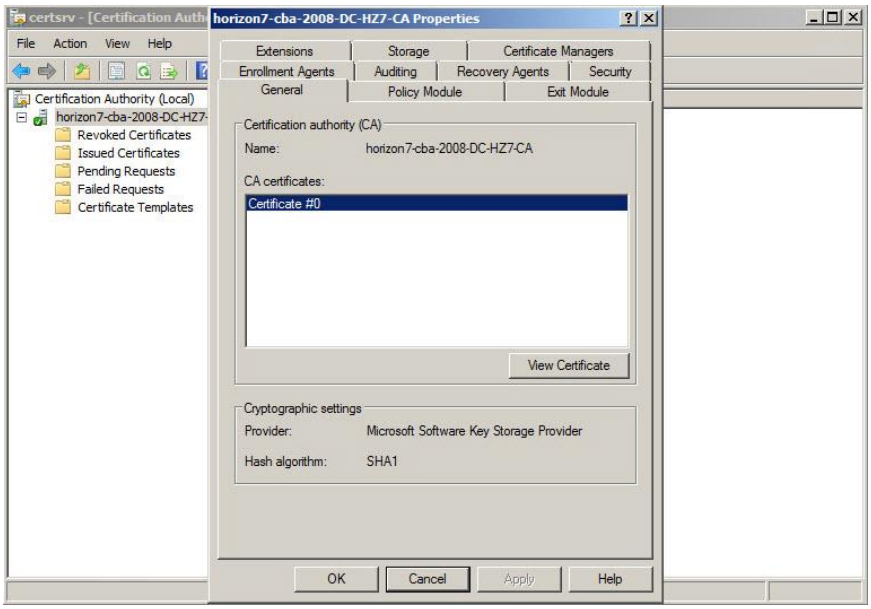
- Obtaining the Root CA certificate
- Adding the Root CA certificate to the connection server
- Configuring VMware Horizon connection server properties

Obtaining the Root CA Certificate

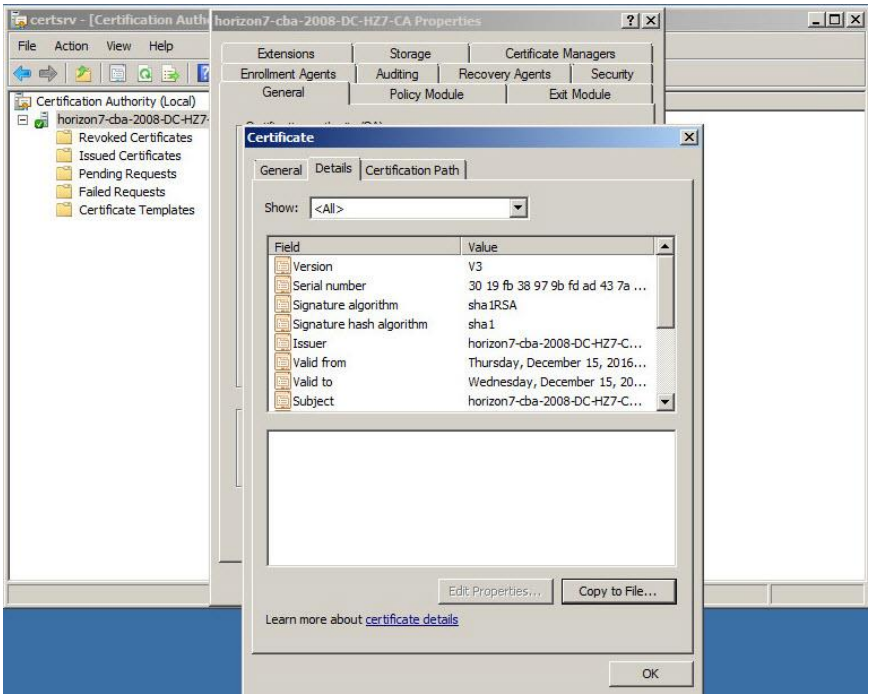
1. Open the **Certificate Authority** window, right-click on the requested CA and then click **Properties.**



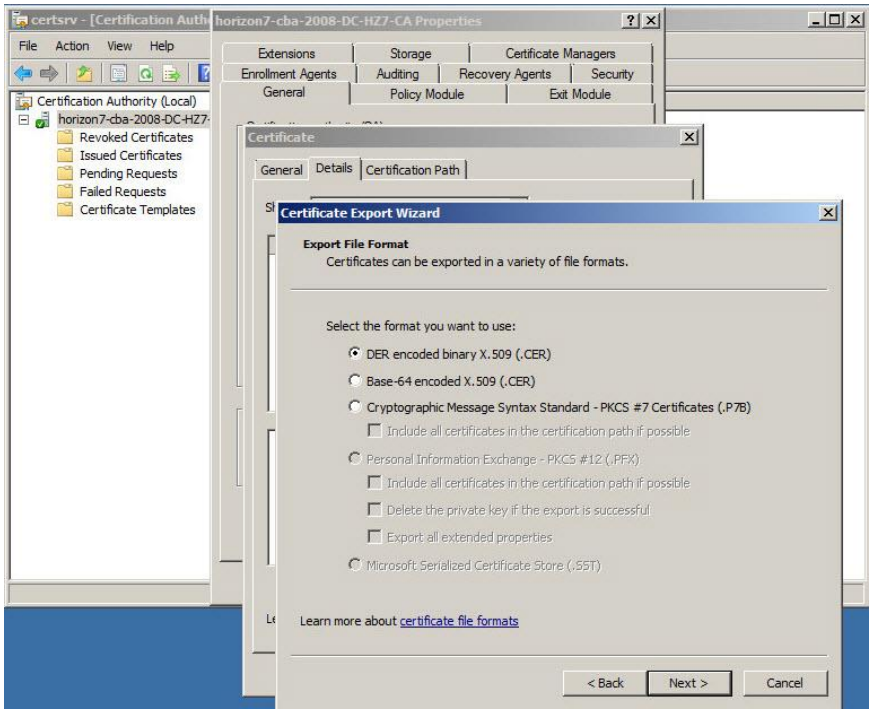
2. On the **General** tab, click **View Certificate**.



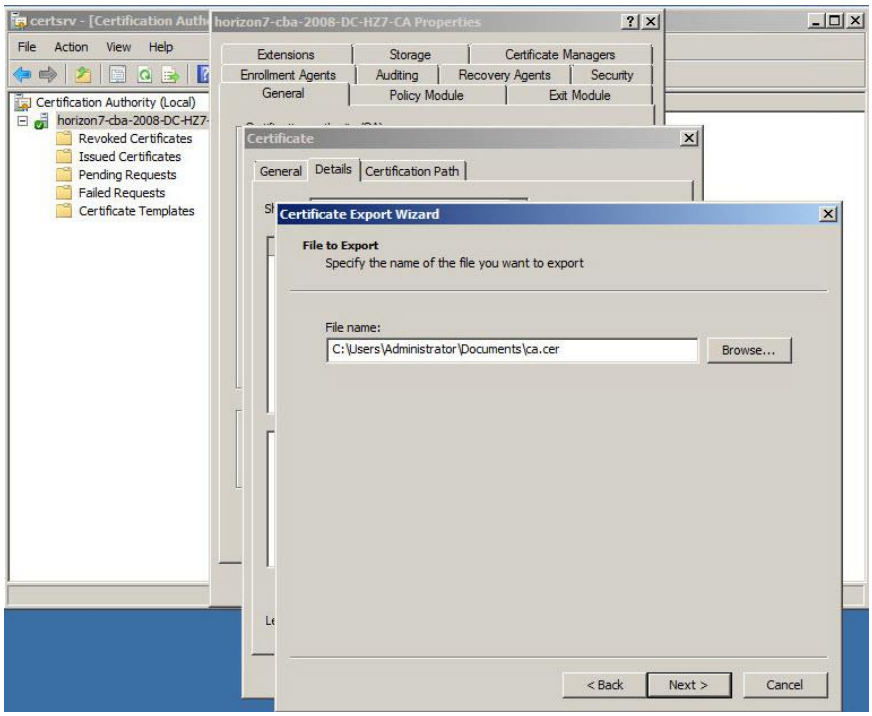
3. On the **Certificate** window, click on the **Details** tab and press on **Copy to File…**



4. The **Certificate Export Wizard** window opens. Select **Next**. On the second window select **DER encoded** and click **Next.**



5. On the **File to Export** window, select a path and file name and click **Next.**



6. Click **Finish**.

Adding the Root CA Certificate to the Connection Server

In this section we add the Root CA certificate to the truststore file which will enable the VMware Horizon 7 connection server to validate and authenticate smart cards.

1. To import the Root CA certificate, use the **keytool** utility, located in the VMware Horizon 7 installation folder (For example: c:\Program Files\VMware\VMware View\Server\jre\bin)
2. Copy the Root CA certificate from the previous section to a known folder (in our integration we copied it to the root of C drive).
3. Use the **keytool** utility to import the root certificate into the server's truststore file by running the following:

   keytool.exe –import –alias alias –file c:\certnew.cer –keystore trust.key
4. Provide a password for the keystore file.
5. Copy the truststore file that you've created (in our example: trust.key) to the SSL gateway configuration folder on the VMware Horizon 7 connection server.

Configuring VMware Horizon Connection Server Properties

To enable smart card authentication, you must modify the VMware Horizon 7 connection server configuration properties:

1. Edit the file **locked.properties** at **c:\Program Files\VMware\VMware View\Server\sslgateway\conf**
   If the file does not exist, create it.
2. Assign the following values to the properties file:
   - **trustKeyfile=trust.key**
   - **trustStoretype=JKS**
   - **useCertAuth=true**
3. Save the file.
4. Restart the server.

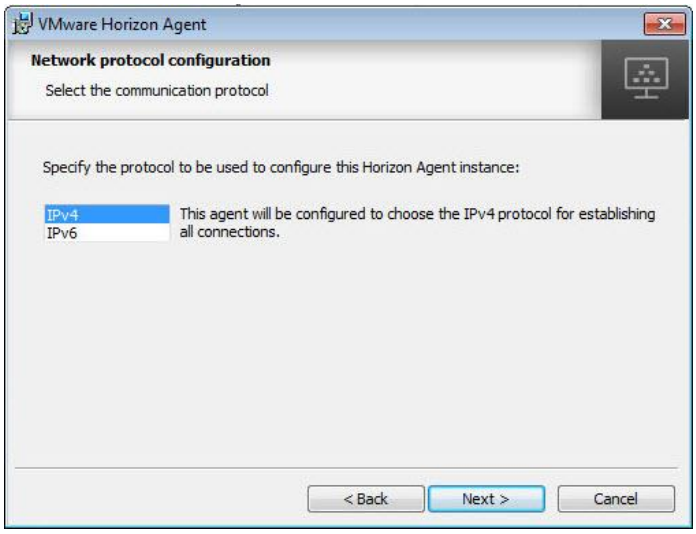
More information about this process can be found here:
https://pubs.vmware.com/view-52/index.jsp#com.vmware.view.administration.doc/GUID-FA1A85D8-07B1-4140-A34B-7F20618083CE.html

Installing the VMware Horizon View Agent

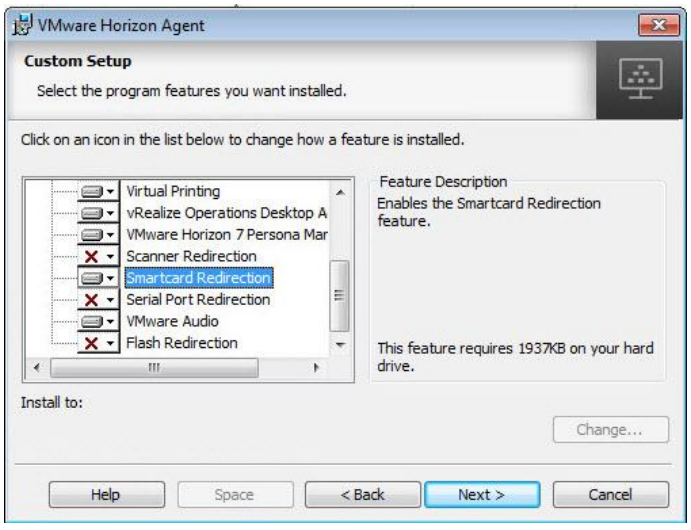
The VMware Horizon View agent needs to be installed on:

- All virtual desktops managed by the VMWare vCenter
- All virtual desktops used as a template for automated desktops
- All virtual machines that publish applications

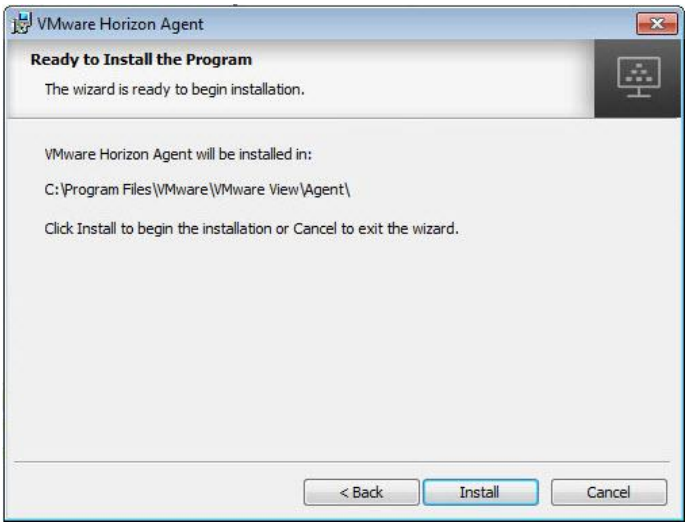
1. Execute the View Agent installer file.
2. Click **Next**, accept the **License Agreement** and click **Next.**
3. On the **Network Protocol Configuration** window select the required **Network Protocol** and click **Next**.



4. On the **Custom Setup** window enable **Smartcard Redirection.**



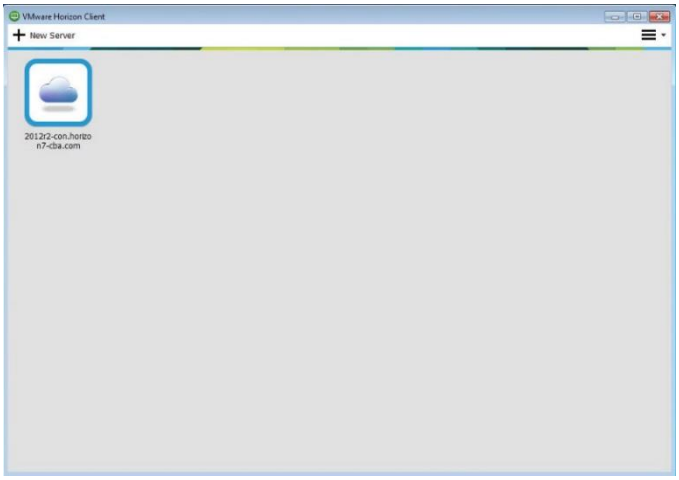
5. Click **Install**



Running the Solution

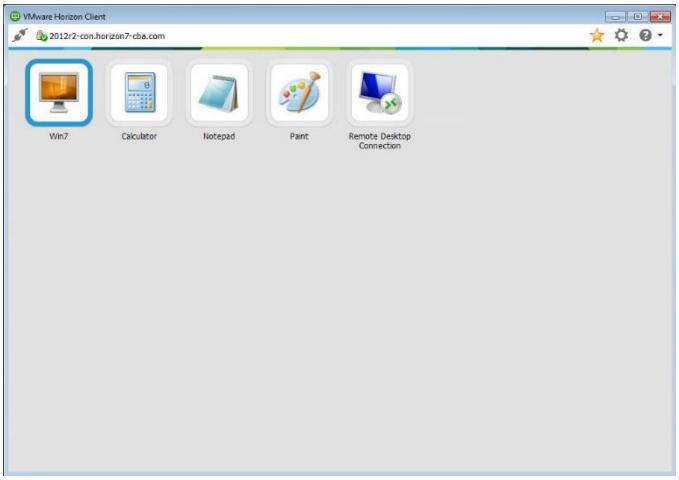
In this section, we will demonstrate the authentication to VMware Horizon 7 with Gemalto token/smart card using the SafeNet Authentication Client.

1. Open the **VMware View** client.



2. Double-click on the VMware View server. The PIN code login window is opened. Enter the PIN code and click **Login**.

After successful authentication, the client machine is connected to the VMware Horizon 7 and the user can access the VM's assigned to him in the VM pool or the published applications.



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 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.	