

SafeNet Authentication Client Integration Guide

Using SAC CBA for VMware Horizon 6
(View Administrator)



THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012983-001, Rev. A
Release Date	April 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

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

Third-Party Software Acknowledgement.....	4
Description.....	4
Applicability.....	5
Environment	5
Audience.....	5
CBA Flow using SAC	5
Prerequisites.....	6
Supported Tokens in SAC.....	6
Certificate-based USB tokens.....	6
Smart Cards.....	6
Certificate-based Hybrid USB Tokens	6
Software Tokens	6
Configuring VMware Horizon 6	7
Setting Certificates in VMware Horizon 6 Environment	9
Obtaining the Root Certificate from the CA	9
Adding the Root Certificates to the Connection Server	13
Configuring View Connection Server Configuration Properties.....	14
Configuring Active Directory for Smart Card Authentication	14
Creating Certificate Templates	14
Running the Solution	15
Support Contacts.....	16

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as VMware Horizon 6 (View Administrator).

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 (CAs) and enterprises to ease the administration of SafeNet's hardware or software token 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 meet different organizations' PKI device 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*.

VMware Horizon™ 6 (with View) is a virtual desktop infrastructure (VDI) platform that delivers virtualized and remote desktops and applications through a single platform, giving end users access to all of their online resources through one unified workspace.

This document describes how to:

- Perform certificate-based authentication (CBA) to VMware Horizon 6 using SafeNet tokens.
- Configure the VMware Horizon 6 environment to work with SafeNet tokens.

It is assumed that the VMware Horizon 6 (View Administrator) environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

VMware Horizon 6 (View Administrator) 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.
- VMware Horizon 6 (View Administrator)

Environment

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

- SafeNet Authentication Client (SAC)—Version 9.0
- VMware Horizon 6 (View Administrator)

Audience

This document is targeted to system administrators who are familiar with VMware Horizon 6 (View Administrator), and are interested in adding certificate-based authentication (CBA) using SafeNet tokens.

CBA Flow using SAC

The diagram below illustrates the flow of certificate-based authentication:



1. An Administrator would like to connect to VMware Horizon 6 View Administrator.
2. The Administrator connects the SafeNet eToken containing the certificate.
3. The Administrator browses to VMware Horizon 6 Administration Console to connect using the certificate on the token.
4. The Administrator enters his token's credentials.
5. If the credentials are successfully authenticated, the Administrator is logged in to the VMware Horizon 6 View Administrator.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for VMware Horizon 6 (View Administrator) 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 further 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 (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 VMware Horizon 6 (View Administrator).

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)

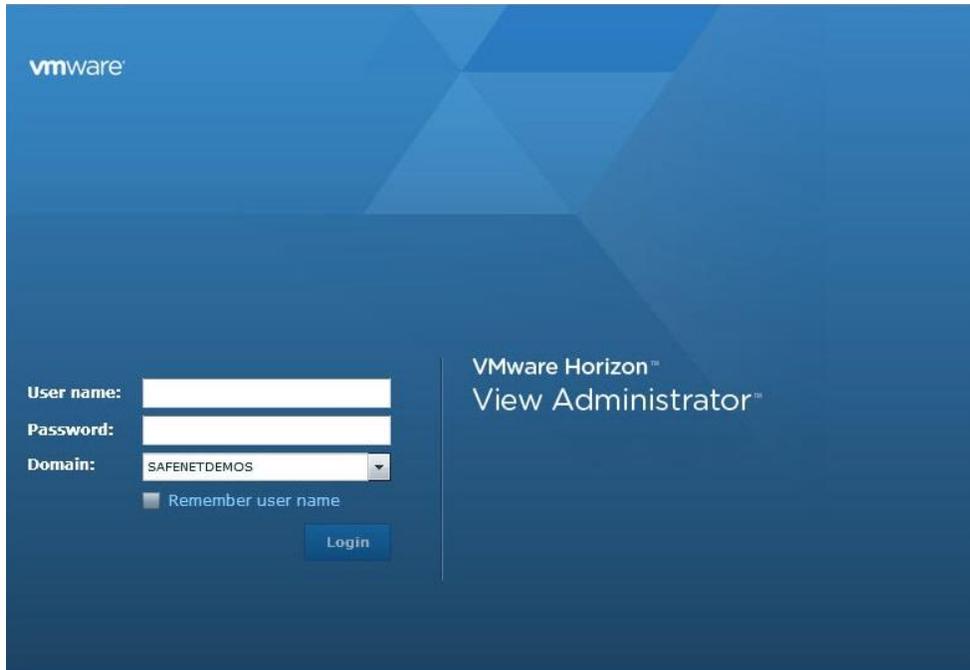
Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring VMware Horizon 6

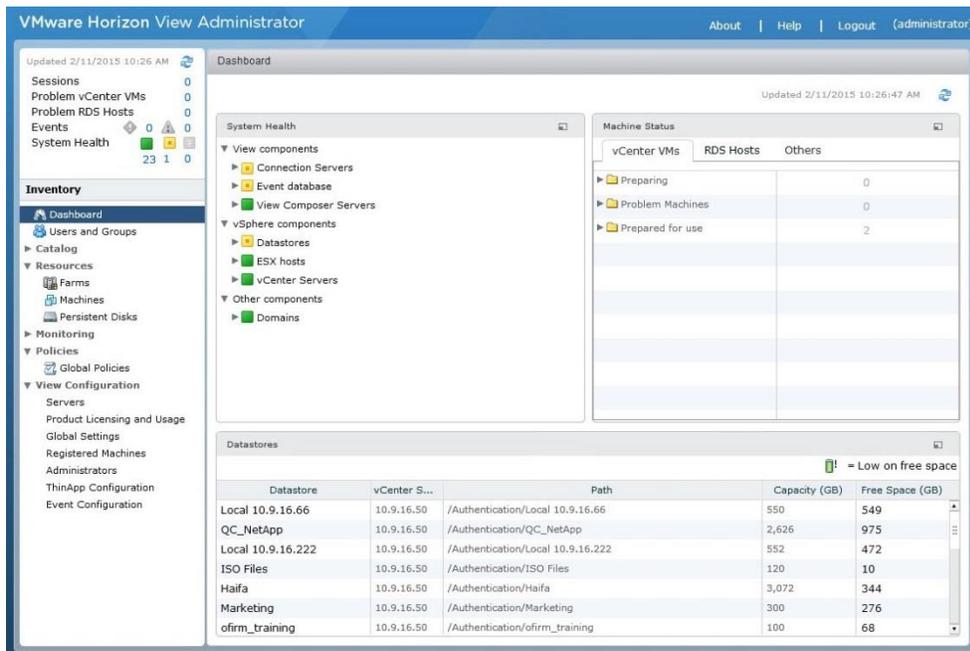
Configure the VMware Horizon 6 environment through the VMware Horizon View Server for two-factor authentication so users can authenticate using certificates on their eTokens.

1. Log in to the VMware Horizon View Administrator using the URL <http://<ViewServer>/admin>.



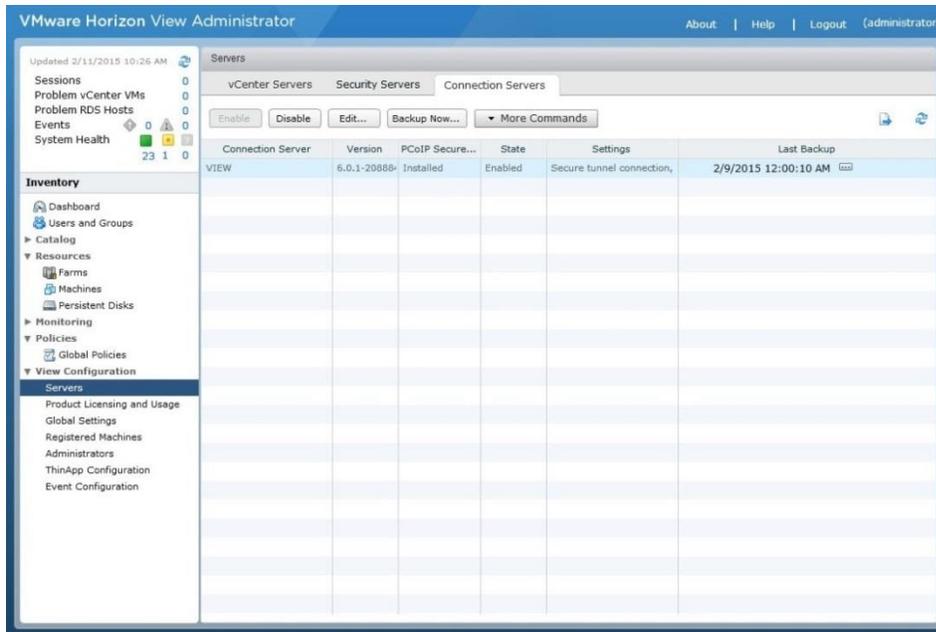
(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners).

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



(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners).

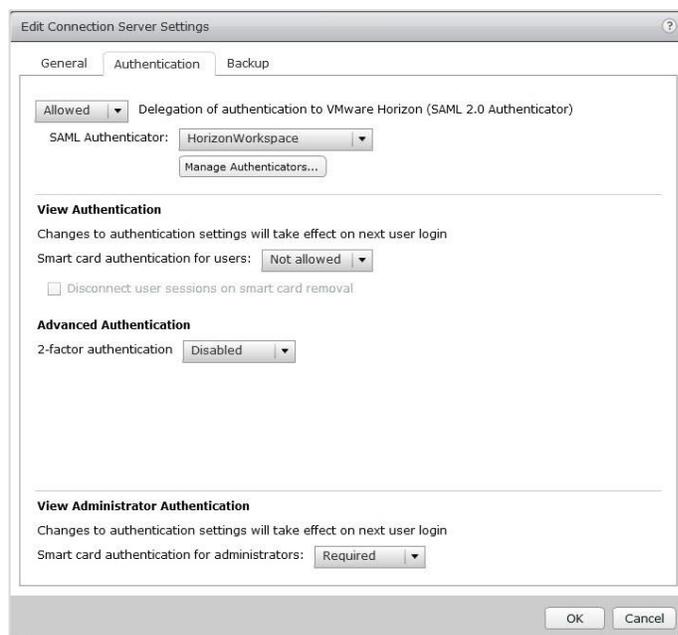
- In the **Servers** window, click the **Connection Servers** tab.



(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners).

- Click the **Connection Server**, and then click **Edit**
- On the **Edit Connection Server Settings** window, click the **Authentication** tab.
- Under **View Authentication**, complete the following, and then click **OK**.

Smart card authentication for users	Select Required .
Disconnect user sessions on smart card removal	(Optional) Select this option.



(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners).

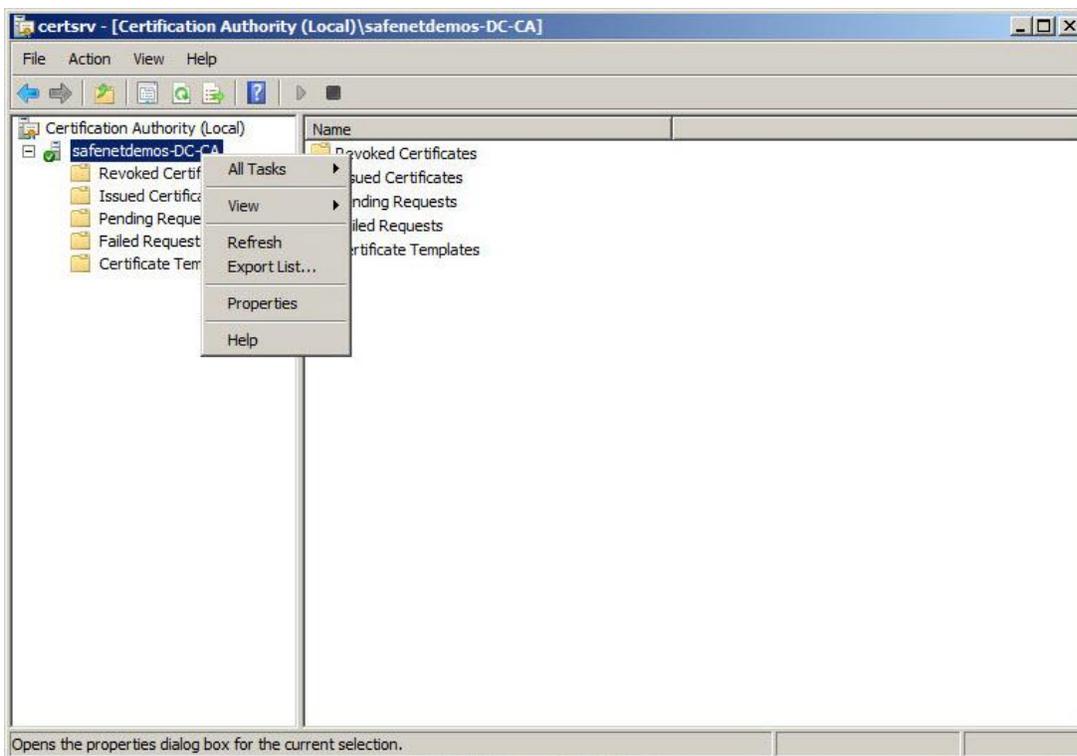
Setting Certificates in VMware Horizon 6 Environment

Complete the procedures in this section to configure VMware Horizon for two-factor authentication so users can authenticate using certificates on their eTokens.

- Obtaining the Root Certificate from the CA, page 9
- Adding the Root Certificates to the Connection Server, page 13
- Configuring View Connection Server Configuration Properties, page 14
- Configuring Active Directory for Smart Card Authentication, page 14
- Creating Certificate Templates, page 14

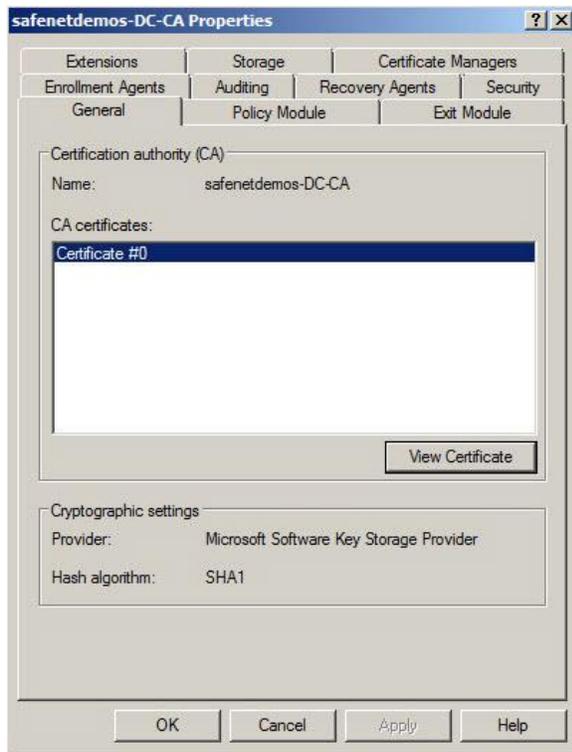
Obtaining the Root Certificate from the CA

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



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

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



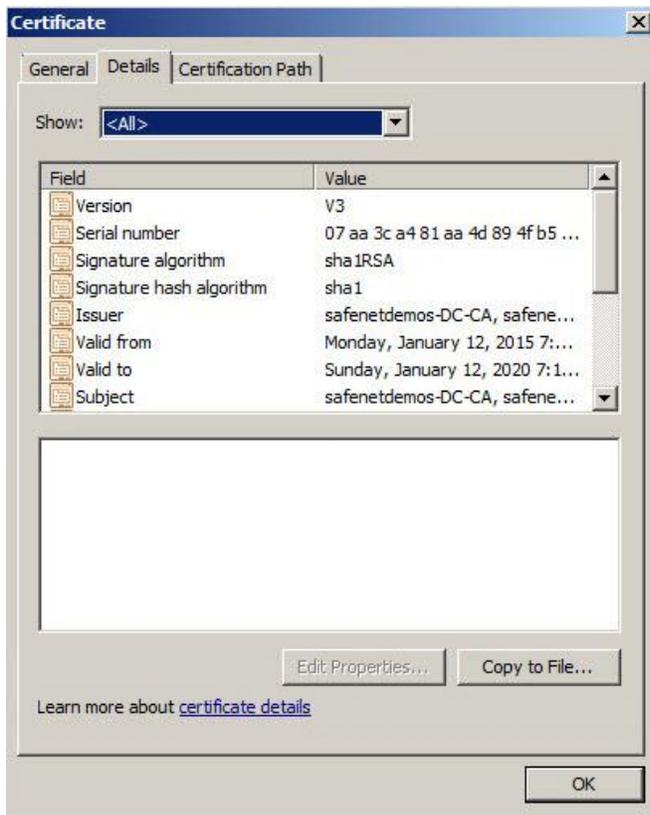
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

3. On the **Certificate** window, click the **Details** tab.



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

4. On the **Details** tab, click **Copy to File**.



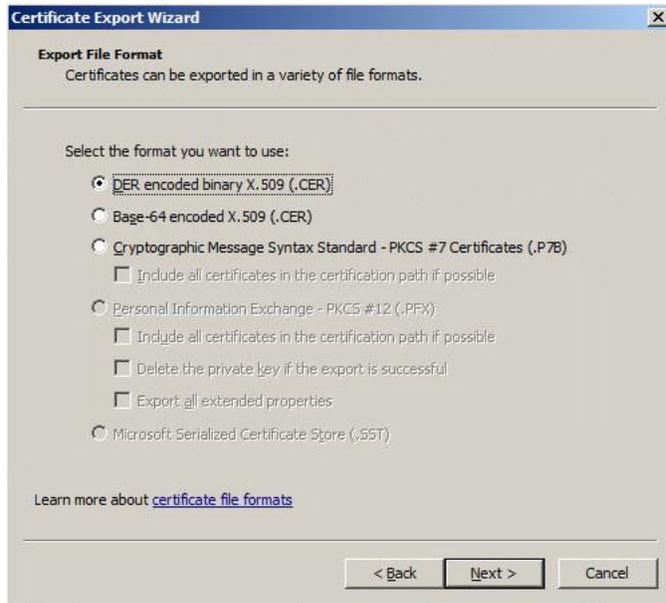
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

5. The **Certificate Export Wizard** is displayed. On the **Welcome** window, click **Next**.



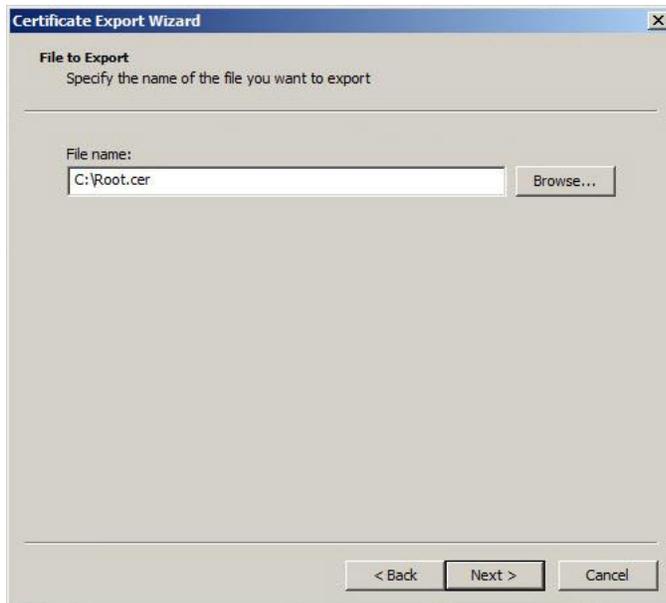
The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

6. Select the **DER encoded library X.509 (CER)** file format, and then click **Next**.



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

7. Click **Browse**, select the file to export, and then click **Next**.



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

- Click **Finish** to close the Certificate Export Wizard.



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

- Click **OK** when the export successfully completes.



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

Adding the Root Certificates to the Connection Server

Add the root certificate to a server truststore file so that VMware Horizon View Connection Server instances and security servers can validate and authenticate smart card users to their View desktops.

For this procedure, you will need the **keytool** utility, which is located in the VMware View installation folder (for example, C:\Program Files\VMware\VMware View\Server\jre\bin).

- On the View Connection Server or security server host, use the **keytool** utility to import the root certificate into the server truststore file—run the following command:

```
keytool.exe -import -alias alias -file c:\certnew.cer -keystore trust.key
```

The value of the **<keystore>** parameter is the file to store the imported key. In this procedure, the value is **trust.key**

- Provide a password for the keystore file. You will need this password if you add certificates to the keystore file later.
- Copy the truststore file that you just created to the SSL gateway configuration folder on the View Connection Server—run this command:

```
copy trust.key ..\..\sslgateway\conf\trust.key
```

Configuring View Connection Server Configuration Properties

To enable smart card authentication, you must modify the View Connection Server configuration properties on your View Connection Server or security server host.

1. Browse to **C:\Program Files\VMware\VMware View\Server\sslgateway\conf**, and locate the **locked.properties** file.

If the **locked.properties** file does not exist in this configuration folder on the View Connection Server or security server host, create a blank text file and name it **locked.properties**.

2. Assign the following values to the properties:

- **trustKeyfile=trust.key**
- **trustStoretype=JKS**
- **useCertAuth=true**

3. Save the file.
4. Restart the system.

Configuring Active Directory for Smart Card Authentication

Smart card logins rely on user principal names (UPNs), so the Active Directory accounts of smart card users must have valid UPNs for authentication before the smart card enrollment.

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory.

If the Windows domain controller acts as the root CA, you do not need to add it to the Trusted Root Certification Authorities.

If you use an intermediate certification authority to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

Creating Certificate Templates

Smartcard Logon or Smartcard User templates must be available to authenticate with the smart card. In addition, VMware Horizon 6 with View requires a minimum certificate key size of 1024 bits.

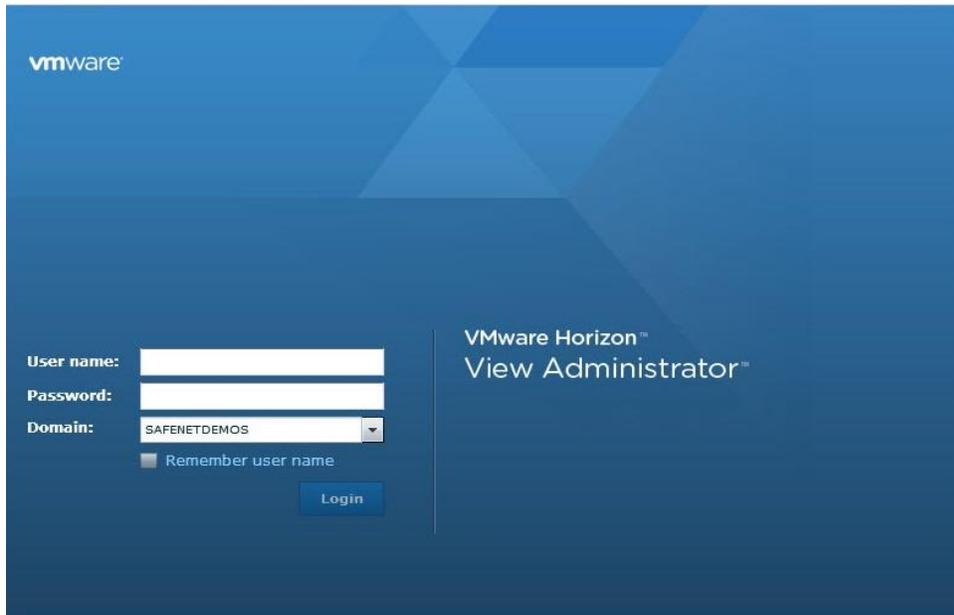
If you already have these templates, you can skip this step.

Follow this procedure to create (duplicate) the existing SmartCard Logon or Smartcard User template, and modify the minimum key size of the new certificate template.

1. Open the **Certificate Authority** window, and expand the CA directory.
2. Right-click on **Certificates**, and then select **Manage**.
3. Right-click on either **Smartcard User** or **Smartcard Logon**, and then select **Duplicate Template**.
4. Make sure the **Minimum key size** is set to **1024**.
5. Return to the **Certificate Authority** window, right-click on **Certificates**, and then select **New > Certificate Template to Issue**.
6. On the **Enable Certificate Templates** window, select the new duplicate certificate, and then click **OK**.

Running the Solution

1. Insert the SafeNet eToken into the machine.
2. Log in to the VMware Horizon View Administrator.



(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners).

3. Select the certificate to use, and then click **OK**.

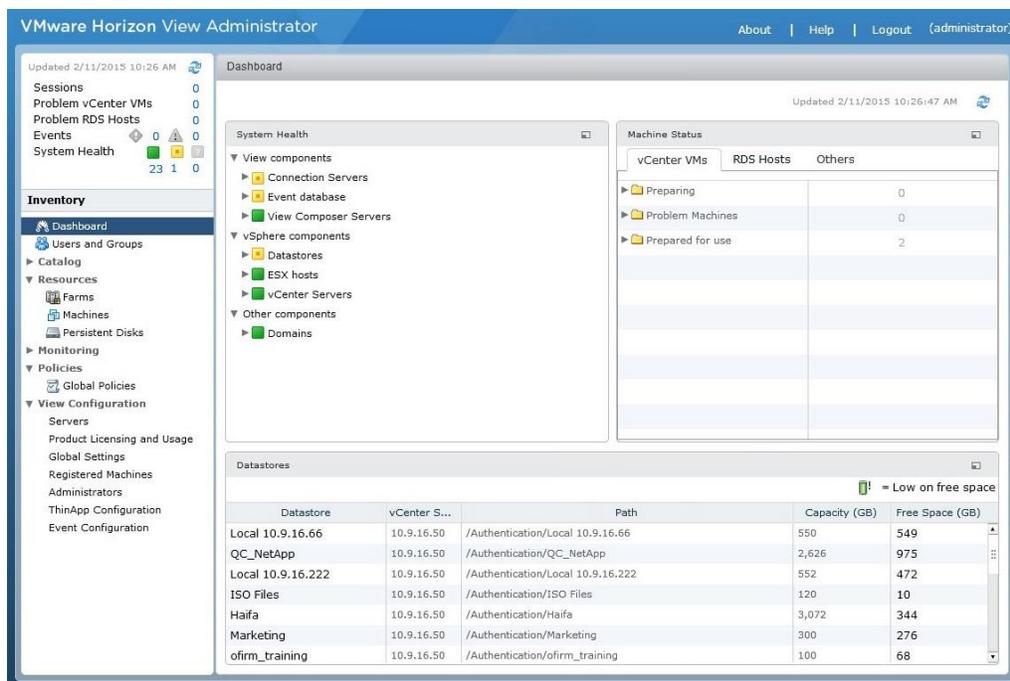


The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

4. Enter the **Token Password**, and then click **OK**.



After successful authentication, the user is logged in to VMware Horizon 6 View Administrator.



(The screen image above is from VMware® Horizon View™. 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 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.

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
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.	