Smart Card Certificate Authentication with VMware® View™ 4.5 and Above

WHITE PAPER

vmware®

Table of Contents

About This Paper

This document provides a technical overview on smart cards and certificate authentication in VMware® View™ 4.5 and above. It is not a tutorial; it is intended for security administrators with basic knowledge of authentication techniques. The paper summarizes certificate authentication and provides advice about using VMware View 4.5 and above to perform a variety of authentication and other security-related administration tasks with smart cards on Windows or Linux machines.

Introduction

The concept of the virtual desktop has enormous appeal to companies that are looking to cut costs and provide more flexible access to resources for authorized users. However, security and access control remain paramount concerns, particularly in industries with stringent regulatory requirements such as the public sector, healthcare, and financial services.

Secure authentication via smart card certificates in Common Access Card (CAC), Two Factor Authentication, or eToken form factor can provide a solution. VMware View offers full-fledged smart card certificate authentication for both PCoIP and RDP protocols in either online/remote mode or offline/local mode.

VMware View was developed to provide rich, personalized, complete virtual desktops as a managed service. The product makes it possible to consolidate virtual desktops on datacenter servers and manage operating systems, applications and data independently for greater business agility while providing a flexible high-performance desktop experience for end users, over any network.

In VMware View 4.5 and above, certificate authentication is supported in the remote display protocol (RDP), PC-over-IP (PCoIP). VMware View 4.5 and above also enhances the offline authentication using smart card.

Specifically, VMware View 4.5 and above can provide:

- Seamless integration of authentication
- Active Directory object clean up with spontaneous revocation
- “Walkaway” or “coffee break” smart card removal policy
- Multiple readers and multiple card support
- Full security for either online or offline desktops
- A full range of guest OS support, including Windows 7, Vista, and XP

Smart Card Overview

A smart card is a small tamper-proof computer containing a CPU and a small amount of non-volatile storage for public key certificates and associated keys. Smart cards are commonly used in secure Web access, VPN, Windows login, or digital signing applications.

Smart cards provide a way to provide user authentication that is different from normal password authentication. With smart card authentication, you simply insert a smart card into the smart card reader and enter a PIN (typically a 4-8 digit string) and you are authenticated. This type of authentication tests the user’s identity by verifying both what they have (the smart card) and what they know (the smart card PIN).

When you insert a smart card into a Windows machine, the certificates that are on the smart card are copied to the local certificate store on the machine. All of the certificates stored on the user's computer are available to all applications running on it, including the View Client. To see this list of certificates, go to **Start > Control Panel > Internet Options > Content > Certificates** and look under the **Personal** tab. These certificates have many complex properties and to view them, simply select the certificate and click the View button.

Getting Started

To use smart cards on any Windows machine, you first need to install a few packages to teach Windows how to talk to smart cards. These modules you will install are called CSPs (cryptographic service providers) and serve as intermediaries between Windows and the smart card.

The most frequently seen cryptographic providers include:

- MS CSP — Microsoft's smart card Cryptographic Service Provider (CSP) module. The CSP facilitates communication between the device and the smart card. The CSP must be signed by Microsoft, or it won't work on Windows. Typically, the manufacturer of the smart card reader provides a CSP; for example, a Gemalto (previously, Gemplus) reader would use a Gemalto CSP, a Schlumberger reader would use the Schlumberger CSP, and so on. The Microsoft .NET framework includes this crypto API by default.
- Java Card — Heavily used by the Department of Defense, Java Card uses the OpenCard framework standard to access the hardware security module. The Java Card API runs Java applets within the card memory. FIPS 201/PIV, FIPS 140-2 certified card, and Common Access Card (CAC) are Java Card.
- Others — There are more than 100,000 types of smart cards from different silicon manufacturers where APDU command is the generic interface used to communicate with the card.

First, you will need to install a hotfix (http://support.microsoft.com/kb/909520) for Windows, which provides the Microsoft Base CSP. This allows you to use smart cards such as Gemalto with Windows.

Optionally, you can install the ActivIdentity ActivClient software suite, which provides helpful tools for interacting with smart cards, as well as another CSP to use for ActivIdentity smart cards.

When you get the blank smart card, you can retrieve a Windows certificate. See the "Setting Up The Certificate" section.

Authenticating into Windows with a Smart Card

The Windows login screen has built-in smart card support, but it waits for you to insert a smart card into your reader even if it's already in there. If you have a smart card reader attached to your machine and are about to log into Windows, you will see a message telling you to insert your smart card. But what Windows listens to is the notification the smart card reader provides to it when a smart card is inserted. So the first thing you need to do is to remove your smart card from your reader and re-insert it. You will now see an entry for a PIN, where you can enter yours. This should log you into Windows.

Using Smart Cards in VMware View

Before setting up smart card authentication in VMware View, you should make sure to have:

- The middleware or driver installed on View Client
- The middleware or driver installed on the virtual desktop
- Smart card enabled within the View Administrator configuration

There are several steps that need to take place to set up smart card authentication for VMware View.

View Connection Server

This is probably the most difficult part. Refer to the VMware View Administration Guide for the View Connection Server and go to the Smart Card Authentication section. This will walk you through what is required to set your broker up to understand smart cards.

Remote Desktop (Agent) and Windows Client

Getting and Managing Certificates

Now that you have set up your infrastructure to support smart cards, you need to actually put some certificates on your smart card. To view certificate info on your current smart card reader, go to https://www.netsolutions. gemalto.com/CertManagement.aspx if you have a Gemalto reader with a Gemalto smart card, or just open the ActivClient software for its supported types of cards and readers.

Storing Certificates on a Smart Card

To install certificates to a smart card, you must first set up a Windows machine (or virtual machine) as an enrollment station. This basically means that, as an administrator, you are giving this machine the authority to issue smart cards for any user. This desktop must be a member of the domain that you are issuing certificates for. The video instructions to set up the machine as an enrollment station and issue the certificates to the smart card are posted at http://vimeo.com/7127297.

Smart Card Authentication Details in Windows View Client

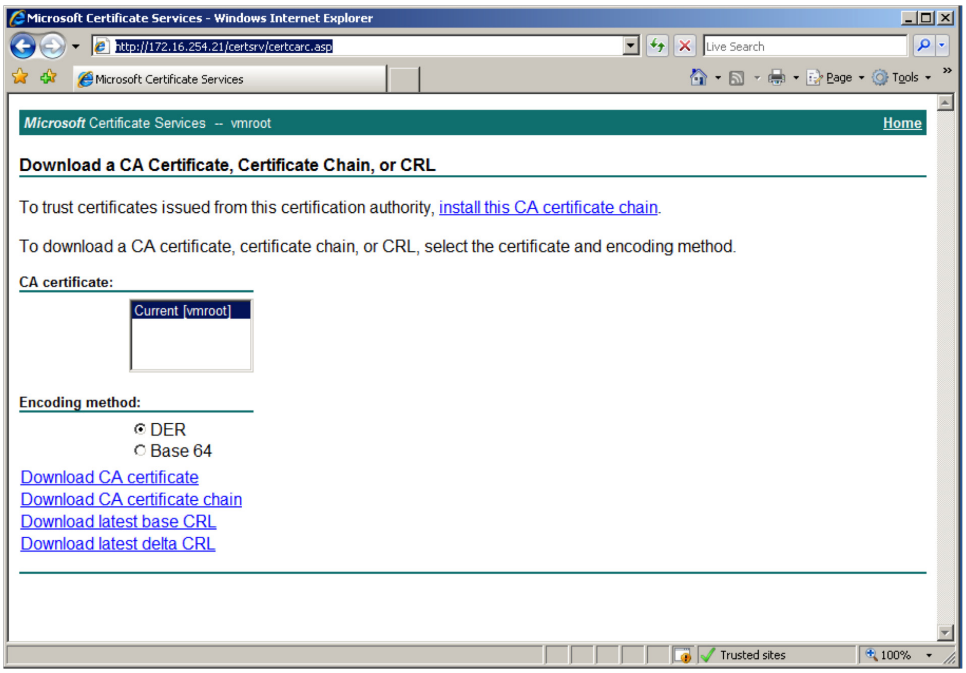
As mentioned earlier, the Windows View Client accesses a list of all certificates installed to the machine and those copied from a smart card. It then filters through this list and removes any certificates that are not relevant. It uses the following rules to filter through the list:

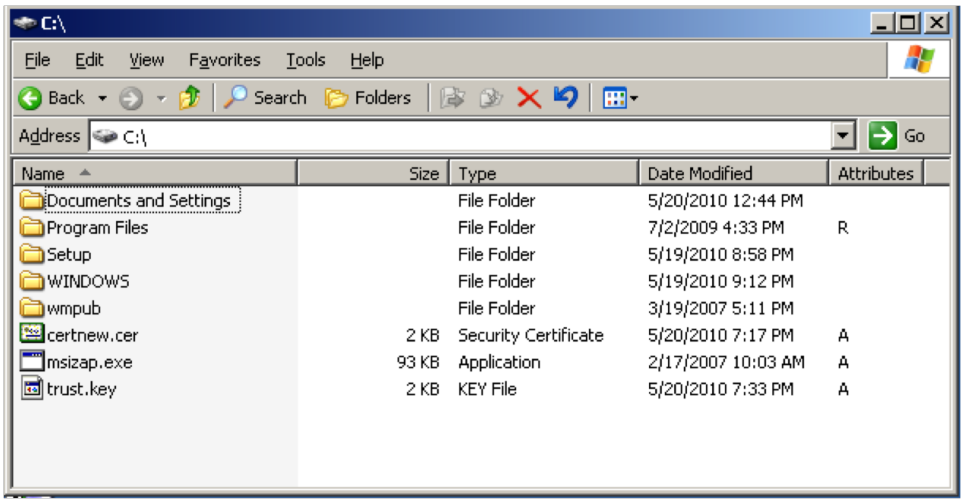
1. The certificate must be valid according to the computer clock (i.e., not expired and not valid in the future).
2. The certificate must have a private key that can be used for authentication. If this is not the case, the Debug logs will show messages indicating so.
3. The certificate must have a valid user principal name or distinguished name. The distinguished name is also known as a Subject in the Certificate Details screen of Windows. The user principal name looks like an e-mail address and can be viewed by looking at the Subject Alternative Name in the Certificate Details screen.
4. The certificate must have the Digital Signature key usage. This can be viewed by looking at the Key Usage field in the Certificate Details screen.
5. The certificate must have the Smart Card Login enhanced key usage. This can be viewed by looking at the Enhanced Key Usage field in the Certificate Details screen.
6. The certificate must be issued by a domain that the View Connection Server allows for authentication. To view this domain, go into the certificate properties, click the Details tab, and look at the issuer field.

Setting Up the Certificate

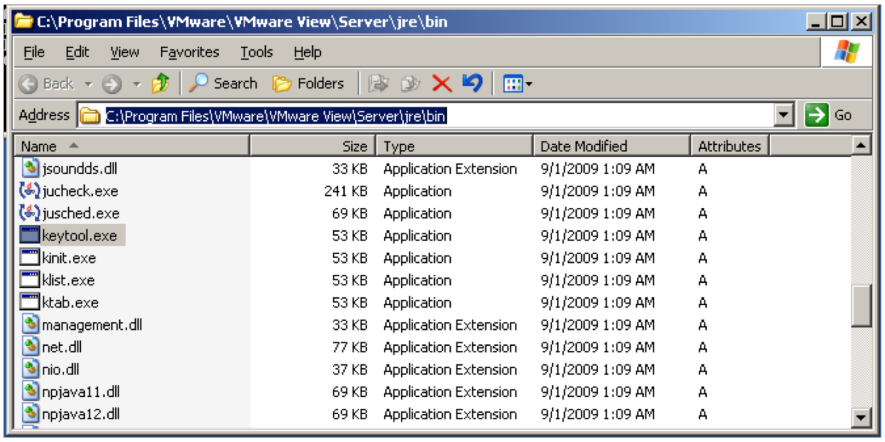
To install certificates on a smart card, you must first set up a Windows computer (or virtual machine) as an enrollment station. In this example, you must have already configured the Certificate Authority (CA) on a Windows Server 2003 or 2008 environment, and the server must be a member of the domain for which you are issuing certificates.

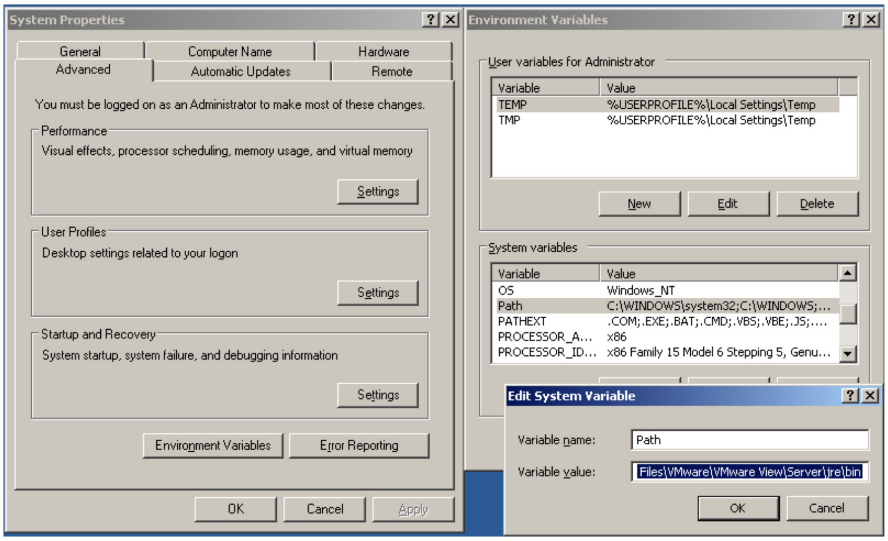
Save CA root certificate to C:\



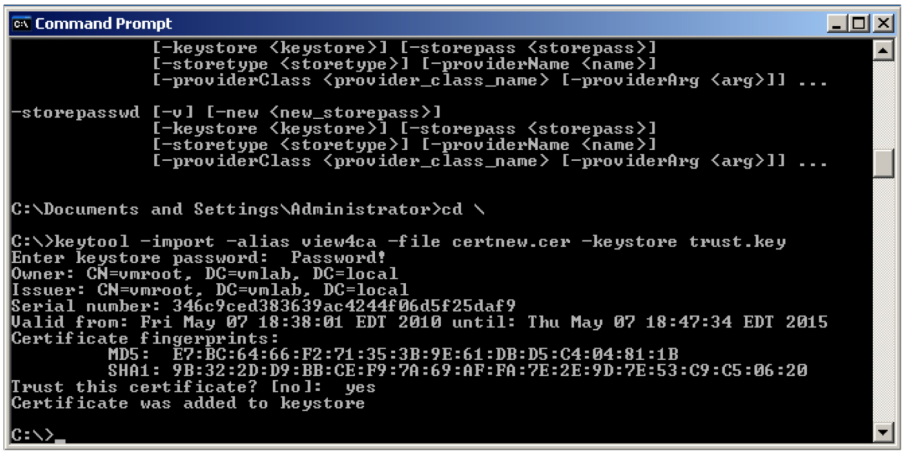


In the **Advanced tab**, select **Environment Variables** and set the **Path** in **System variables** for **keytool.exe**. In this example it is **C:\Program Files\VMware View\Server\jre\bin**.

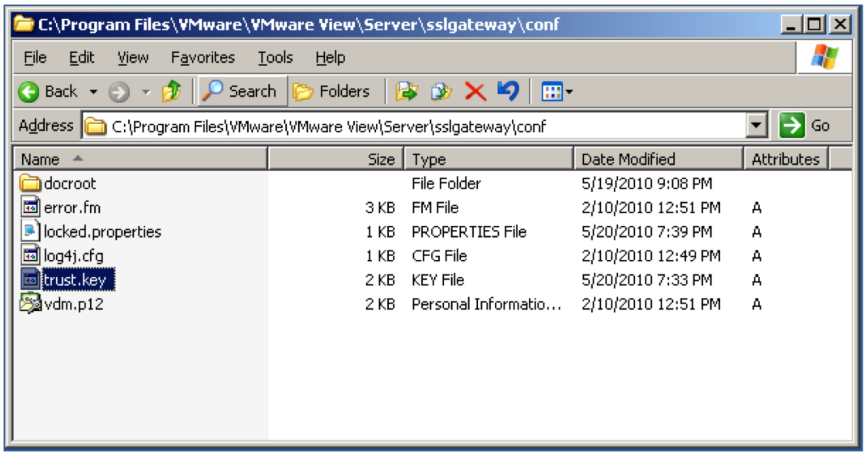




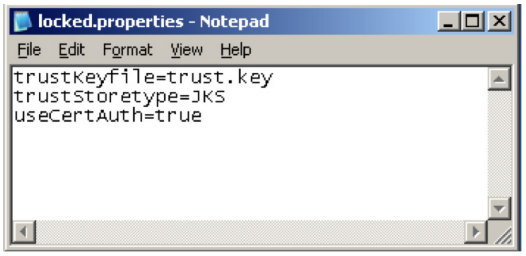
Open a **Command Prompt** and create a **trust.key** using the command **keytool –import –alias –view4ca –file certnew.cer –keystore trust.key** and then answering the prompts.



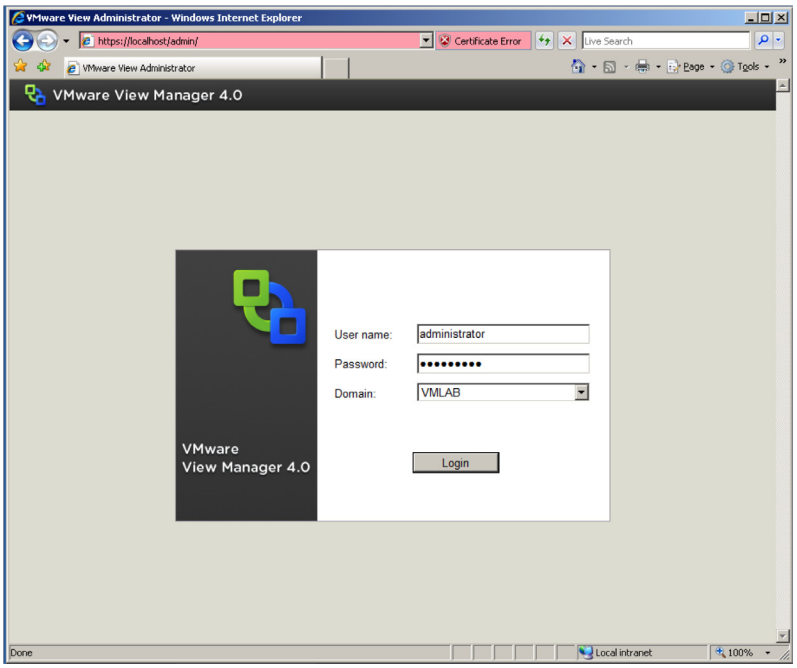
Copy the newly created trust.key to the appropriate location. In this example, it is **C:\Program Files\VMware\VMware View\Server\sslgateway\conf**.

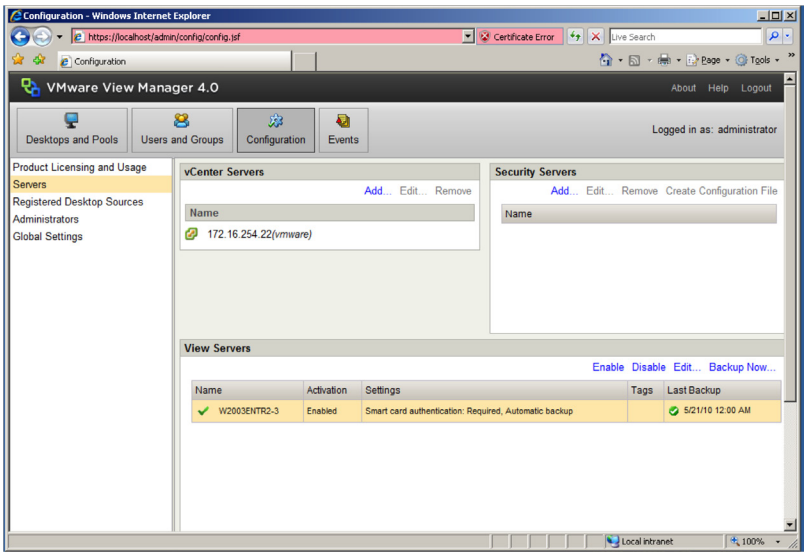


Using Windows Notepad or a similar text editor, create the file **locked.properties**, similar to the screenshot below. Note that it is case sensitive.

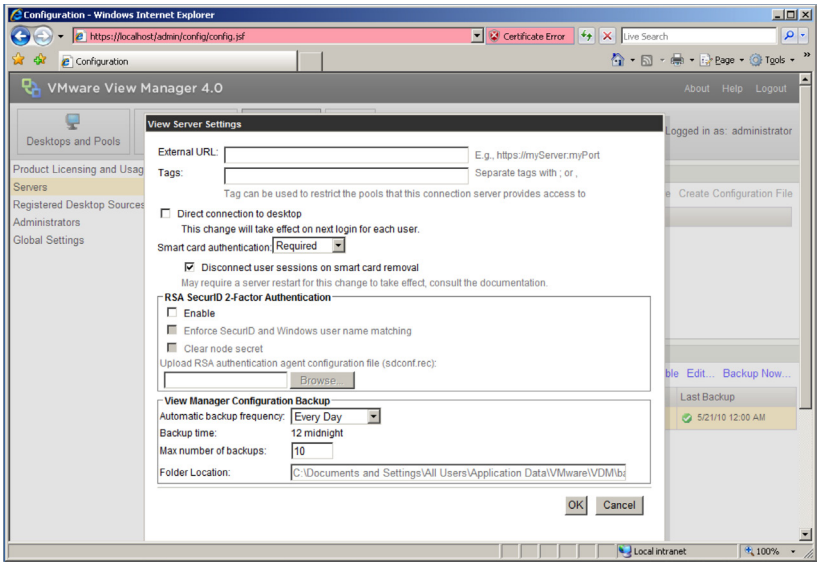


Log in to VMware View Manager, select **Configuration**, and then **Server**.





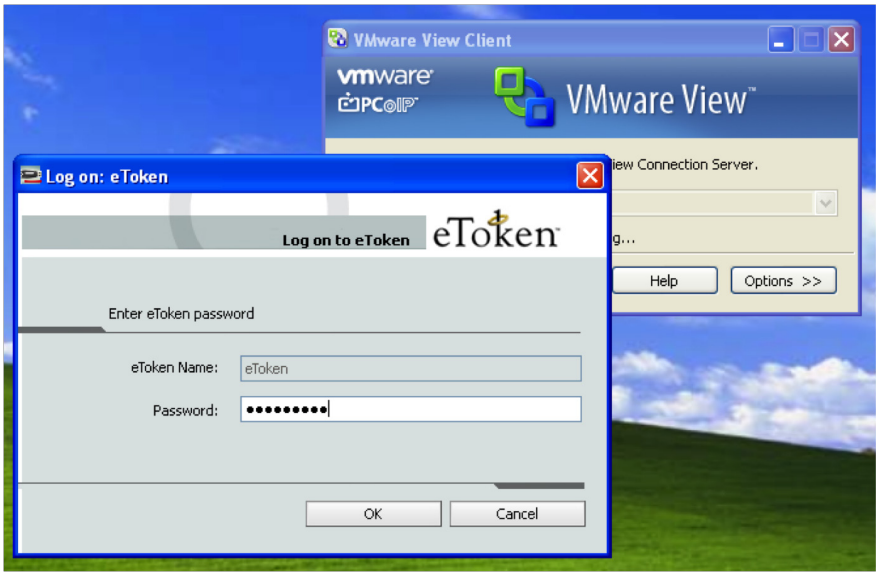
As shown in the screenshot below, configure the settings to meet your security policies. In this example, smart card authentication is required, and the user session is disconnected on smart card removal.



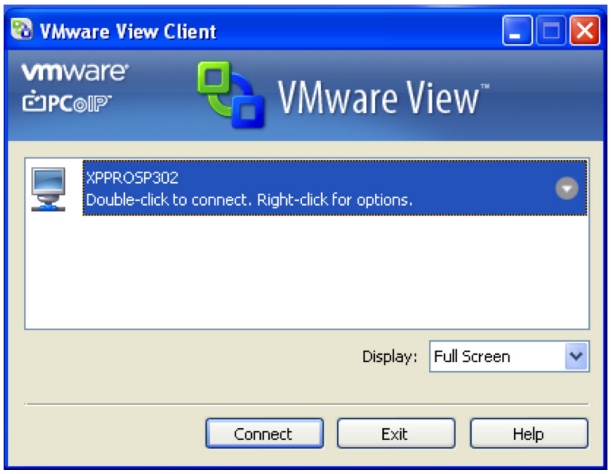
After clicking on OK, reboot the server.

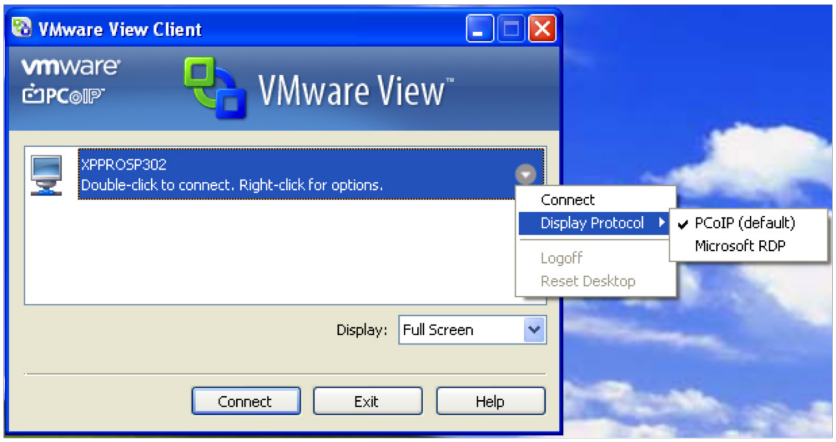
Using the View Client

In addition to PKI smart cards, VMware View also supports USB eToken. In this example, you log in using eToken.

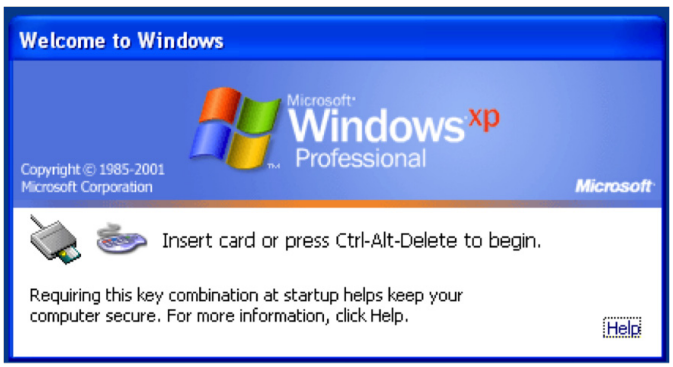


Next, select the virtual machine, and right-click for options, such as Display Protocol.



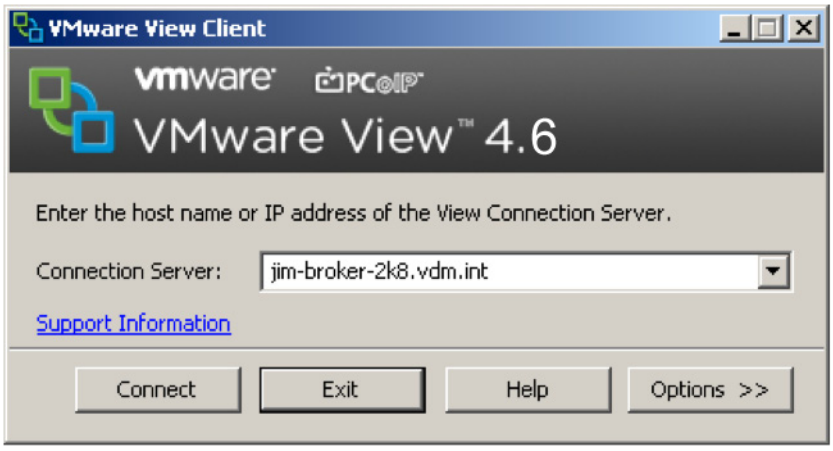


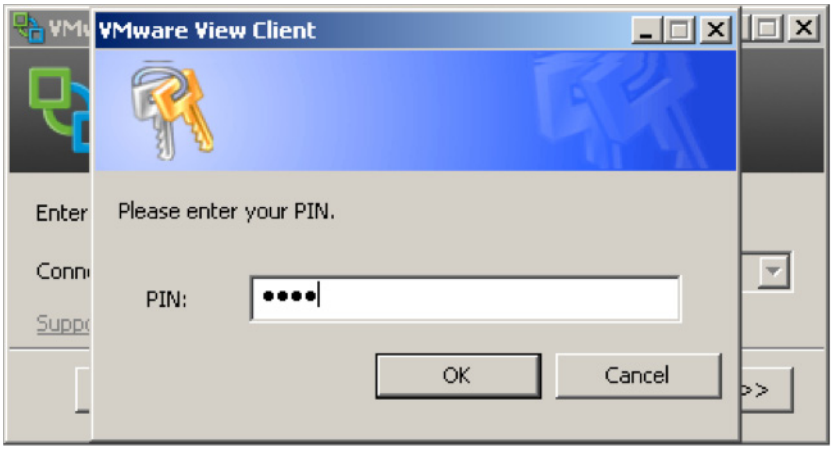
Next, log on to Windows.



Multiple Certificates in a Smart Card

If there are multiple valid certificates, VMware View displays a prompt asking the user to select the certificate they would like to use. If there is only one valid certificate, it is used automatically without prompting the user. If certificate authentication fails for any reason, VMware View will automatically default to the normal password authentication if smart card authentication was set to Optional. If it's set to "Required" in the View Manager administration console, you will not be able to log in without a legitimate certificate.

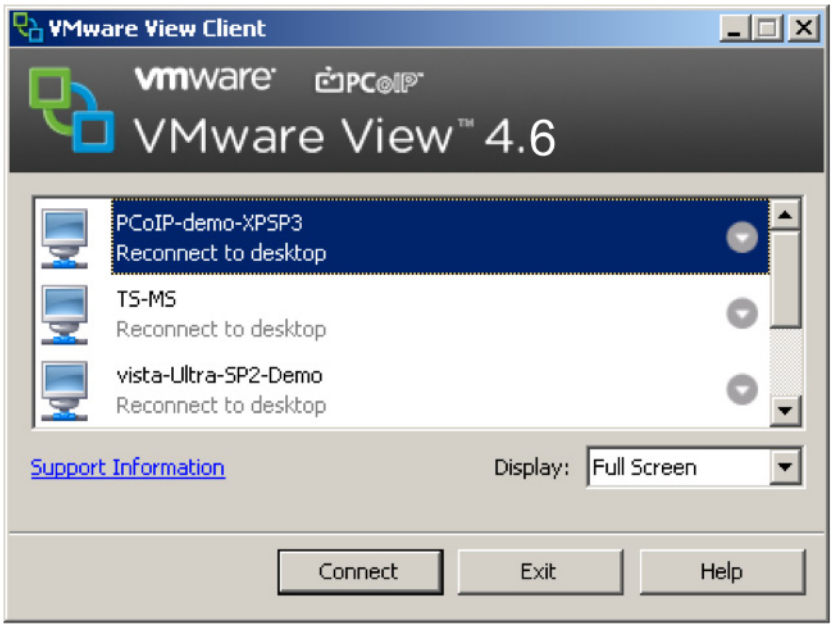




In VMware View 5, users enter the PIN and single signon directly onto the guest desktop in either PCoIP or RDP connection.

Smart Card Single Signon

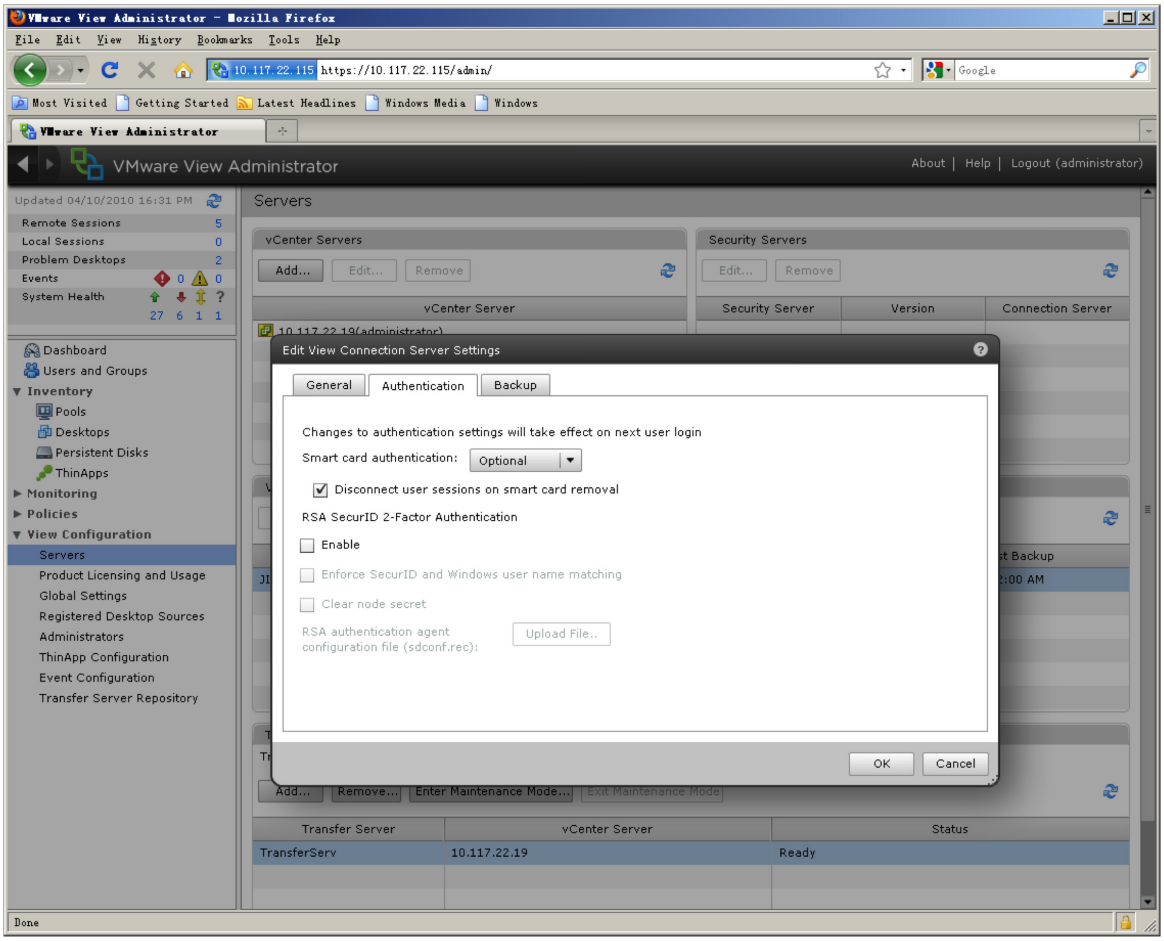
In VMware View 4.5 and above, you can use smart card for single signon, which means that after the user enters their PIN to authenticate to the View Connection Server, VMware View will not require them to enter their PIN again to log into their remote desktop. The smart card PIN is transmitted to the broker during authentication, where the broker remembers this encrypted PIN while the session is active.



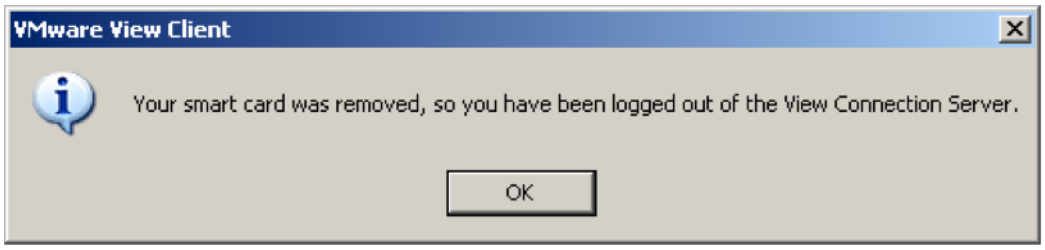
When the user connects to a remote desktop, the broker sends the encrypted PIN to the remote desktop and our custom login module automatically logs the user in using the redirected smart card and the PIN sent to it by the View Connection Server.

Smart Card Removal Policy

This feature, introduced in VMware View 4.0, allows the system to be configured to lock the user desktop upon smart card removal. You can use View Administrator to specify settings to accommodate different smart card authentication scenarios. The detailed step-by-step instructions can be found in the View Manager Administrator Guide, on page 103.



If you configure View Client to access Connection Server with the "Log in As Current User" option checked, smart card removal policy will not apply.

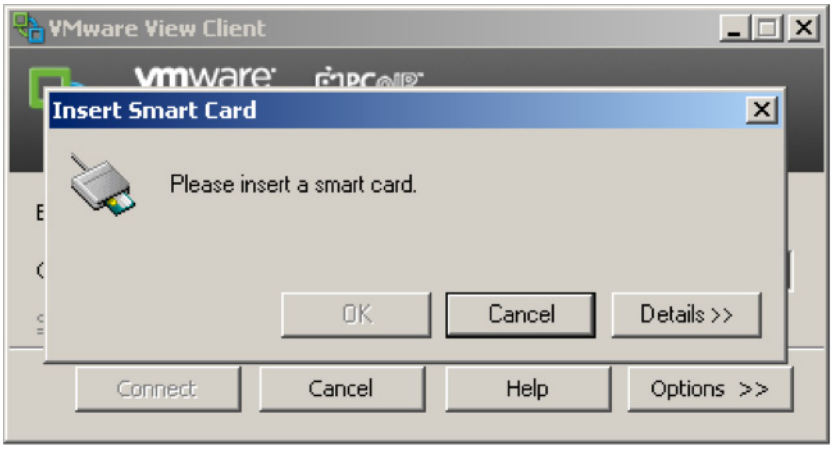


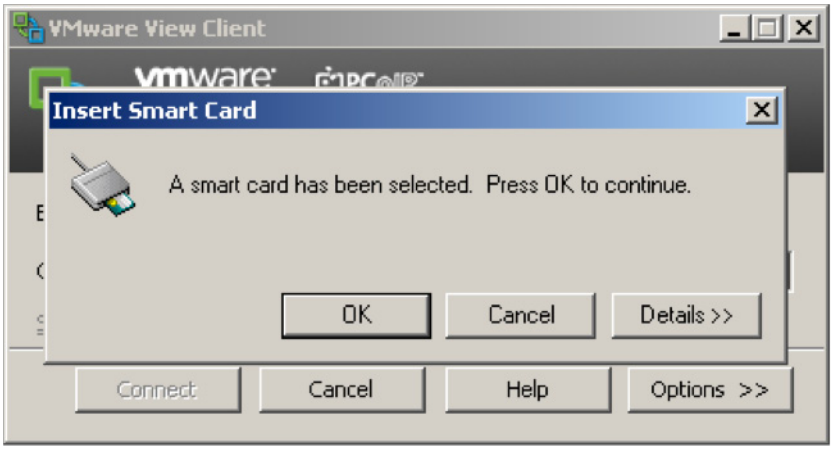
Once the smart card is removed during online mode, the remote desktop just disconnects; it does not logout. So the unsaved contents should be still there. However, if you have configured the pool settings "logout immediately after disconnect," your session will first disconnect, then logout, and the contents will not be saved.

For the local/offline mode, removing the smart card will cause the local desktops to be suspended/ disconnected; however, all unsaved contents will still be saved.

Local Mode / Offline Smart Card Authentication

If you configure the View Connection Server to log in with smart card in the online mode, it will impact the "checked-out" offline desktop login session to log in with smart card as well. The local mode authentication method will use or "remember" the last known good log in method.

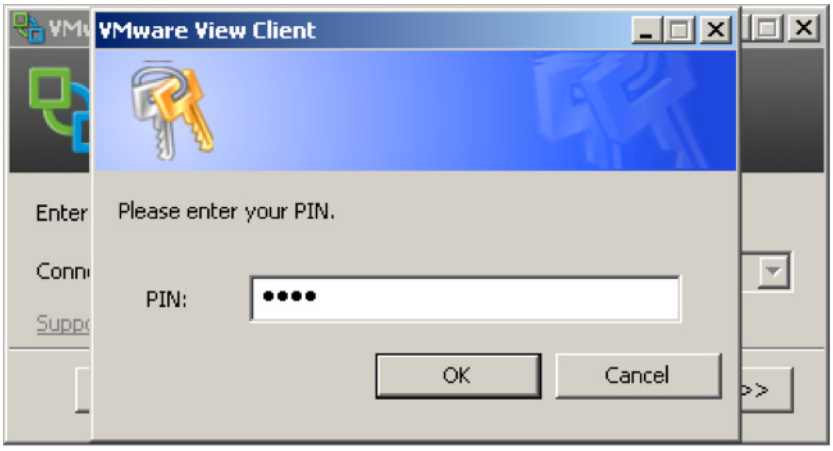




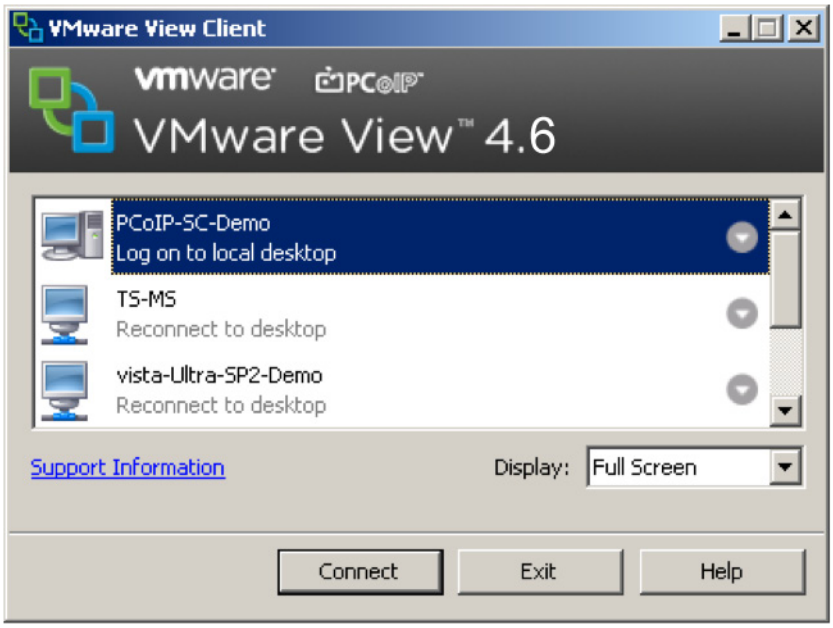
For offline smart card authentication, using a cached credential login along with a smart card certificate will allow you single signon to the guest desktop.

Please note the USB redirection for smart card drop-down menu item is not available in the local mode configuration for the smart card reader (to avoid pass-through reader and virtual reader conflict).

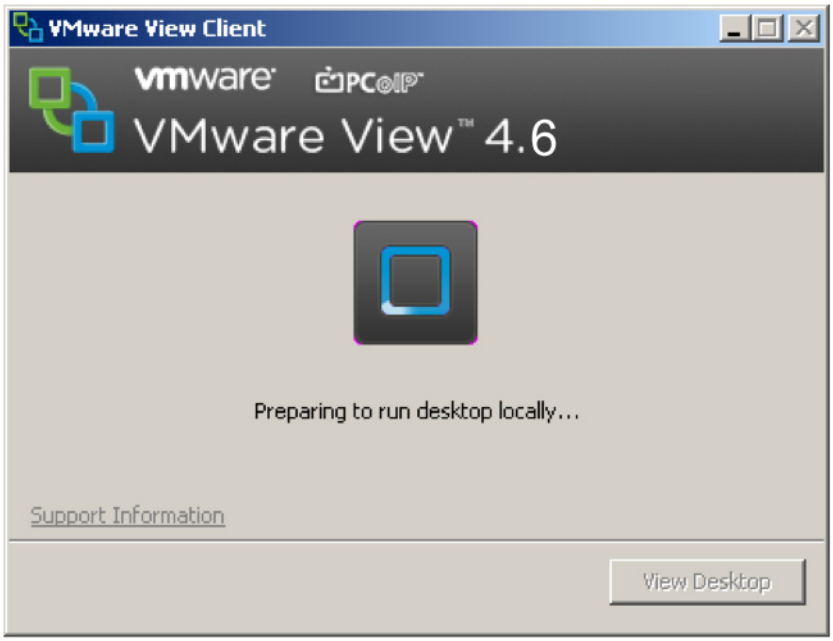
In the offline desktop session, you connect the View Client as you would in establishing a regular session. During the authentication, View Client notices the View Connection Server is not online and will default to the cached credentials. It is critical that your smart card with valid certificate is authenticated and logged into the View environment once before you use it in the offline mode. If it's a brand new smart card, it will not be usable in offline without a previous successful login.



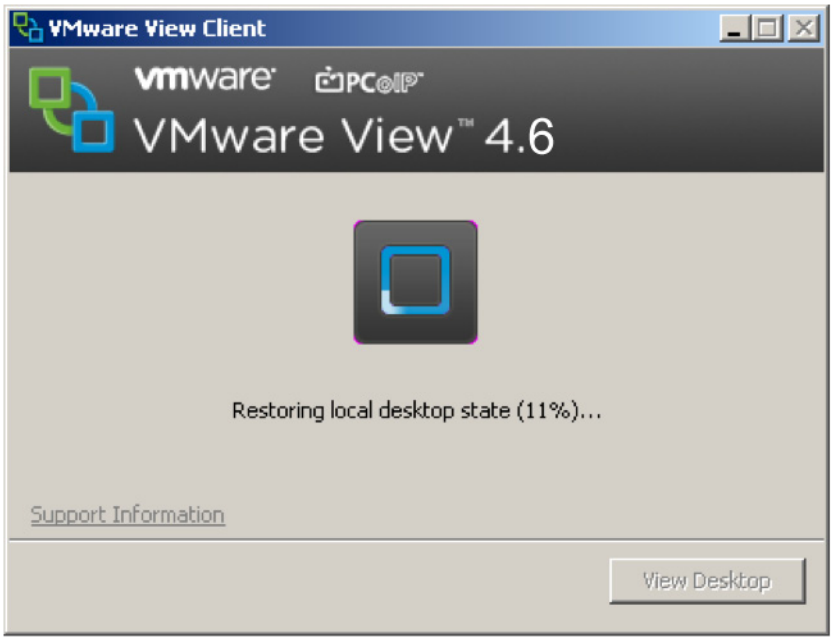
The initial launch of View Client requires a PIN entry.



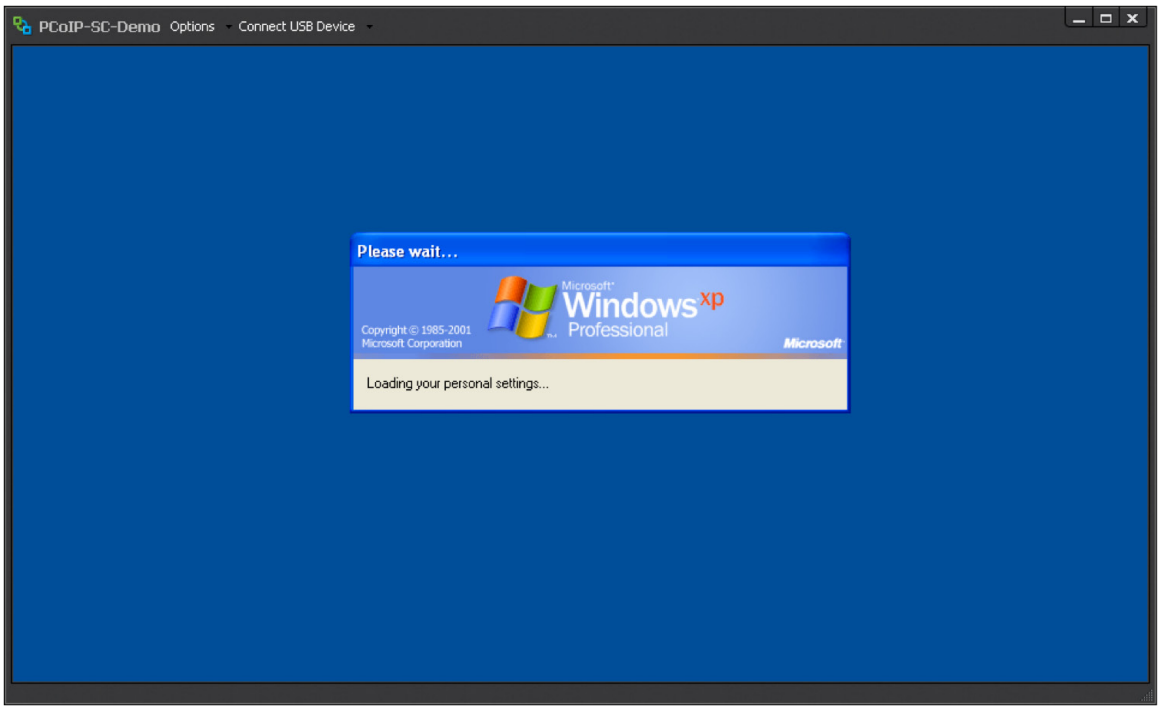
Reconnecting back to "checked-out" desktop using smart card in local mode with PIN entry.



Log in to local mode session.



Smart card removed during local mode session.



When the smart card is removed during the session, the desktop is suspended immediately if the smart card removal policy is set at the View Manager Administration console.

Certification Revocation Lists / Online Certificate Status Protocol (OCSP)

In the event that workers leave the company and their smart card certificates are no longer valid, a certificate revocation list (CRL) is generated and published periodically, after a clearly defined timeframe (Wikipedia: http://en.wikipedia.org/wiki/Revocation_list). A CRL can also be published immediately after a certificate has been revoked. CRL has a known minor drawback in that it tends to be slow.

View Manager supports certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates that is published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

To enable CRL in View environment, you can edit the locked.properties file on the View Connection Server or security server host. The detailed information can be found in the Configure Smart Card Authentication section from the VMware View Administrator's Guide.

For example: <install_directory>\VMware\VMware View\Server\sslgateway\conf\locked.propertiesenabledRevocationChecking=true

crlLocation = "http://root.ocsp.net/CertEnroll/ocsp-ROOT-CA.crl

OCSPURL=http://root.ocsp.net/ocsp

ocspsigningcert=ocsp-signing.cer

If OCSP is not configured or not working, VMware View will fall back to CRL for the revocation policy. The detailed instructions are available in the VMware View Manager Administration Guide.

Summary

VMware View offers full-fledged smart card certificate authentication for both PCoIP and RDP protocols in either online/remote mode or offline/local mode. VMware View is also available on the Linux platform. The Linux commercial client is only available to our thin client partners with full support of PCoIP and RDP. For the open Linux client, users can use the smart card authentication with RDP.

As public sector, healthcare, and financial verticals evaluate the virtual desktop concept and its benefits and challenges, they will find that VMware View offers an excellent solution that helps cut costs while improving access control and security.

References

070520 WP Gemalto .NET 2.0 Smart Card Certificate Enrollment using Microsoft Certificate Services

View Manager Administration Guide

Smart Card Infrastructure MSDN Blog

About the Author

Cynthia Hsieh is a Senior Technical Marketing Manager at VMware. She focuses on application integration, proof of concepts, and security subjects. Hsieh's previous background includes product management positions at Wyse, Trend Micro, Oracle, and Yahoo.

Information in this document is adapted from internal Wiki pages by Adam Gross, who is a Member of the Technical Staff responsible for smart card authentication development at VMware. Thanks also to Jim Zhang (Sr. QA Engineer, VMware) for validating the content accuracy and for providing subject expertise.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com