VMware View
Thin Client Certification
Guide v11

Please note that you can always find the most up-to-date technical documentation on our website at http://www.vmware.com/support/.

The VMware website also provides the latest product updates.

VMware, Inc.

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

1. Introduction

1.1 *About This Guide*

VMware's certification process is designed to validate proper client integrations and compatibility with VMware View product versions. This guide describes the certification Procedure and test cases for certifying thin client devices and software image compatibility with VMware View 5.0.1.

Thin Client Integration Types

Hardware Submission

This guide provides the certification tests that apply to thin clients based one of the following integration scenarios.

1. Microsoft Windows XPe SP3, Microsoft Windows Embedded Standard or Microsoft Windows Embedded Standard 7 running the VMware View Client for Windows (Provided by VMware)
2. Hardware or software thin clients running the VMware View Client for Linux (Provided by VMware)
3. Hardware or software thin clients running custom View Clients based on the VMware View Open Client. Please see http://code.google.com/p/vmware-view-open-client/ for more information about the View Open Client.

Beginning with the release of VMware View 4.5, VMware requires that the thin client device's operating system support all the hardware features of the thin client device being submitted for certification. For example, if the thin client device has two video outputs, it is mandatory for the thin client's OS to support both video outputs in View. If the thin client device has a built-in Smart Card reader, then support for Smart Card in View is also mandatory. If the thin client device supports USB, then USB Redirection in View is also required.

VMware View XML API Custom Clients

Beginning with the release of VMware View 4.0, certifications of custom View clients based on the VMware View XML API can only be accepted if either the VMware provided commercial View clients or a client based on the View Open Client cannot be used. Please contact VMware for more information before developing or submitting custom View XML API clients.

Software Thin Client for Re-purposed PC

A software image for re-purposed PC is a self-contained, loadable image containing an operating system and either the VMware View Client for Linux or a client based on the VMware View Open Client. The VMware View Client for Windows is prohibited from being used in a re-purposed PC solution. Please submit certifications for a software thin client for re-purposed PCs just like a hardware thin client. Perform either the View Client for Linux test cases or the View Open Client test cases, and submit the results to VMware for review. The software image must also be provided to VMware along with the certification submission form. For VMware validation purposes, this software image must be installable on a virtual environment or a hardware platform is required.

VMware strongly recommends naming your thin client solution for re-purposed PC with a specific product name that is different from the thin client's OS. From our experience, we believe that a product with the same name as the thin client OS will cause confusion with customers and potentially prove a disadvantage in the market place. There are many benefits that your thin client product provides, including bundling with the VMware View client and different install options. Having a product name that reflects this would greatly help customers identify and purchase your software.

1.1.1 Documentation Sources

This certification guide does not replace VMware’s installation and administration guides for vSphere or View products.

For detailed setup and configuration guides for VMware products, see the following documentation on the VMware website:

http://www.vmware.com/support/pubs/

1.1.2 Before You Begin

Before you can certify your thin client with VMware View, make sure that:

- Your VMware TAP Select membership is up to date.
- Your VDI Redistribution Agreement has been signed and accepted by VMware.
- Production level versions of your thin client devices or software images are available.
- An RC or GA release of the target VMware View product is available from VMware.
- Your thin client device meets the minimum hardware and software requirements for the VMware View release.

1.1.3 What’s New

- Added new RADIUS 2-Factor Authentication test cases to all client types

1.1.4 Revision History

This document applies to VMware View. This guide is revised with each revision of the thin client certification program guide or when deemed necessary. A revised version can contain minor or major changes.

Product Version	Release Number	Date	Description
VMware Thin Client Certification Guide for VMware View 4.5 v2	V1	July 15, 2010	Initial v2 release. Updated Graphics Guidelines test case. Updated test case 5.7 and test case 6.10.
VMware Thin Client Certification Guide for VMware View 4.5 v3	V2	July 22, 2010	Updated GUI Guidelines test cases with example commands to execute as well as make it less restrictive. Added requirement that hardware sample models must match what is indicated in the submission form.
VMware Thin Client Certification Guide for VMware View 4.5 v3	V3	Sept. 9, 2010	Removed power policy test case for the View Open Client. Clarified PcoIP support policy test cases. Added graphics guideline test cases to View Linux Client and View Open Client.
VMware Thin Client Certification Guide for VMware View 4.5 v4	V4	Sept. 24, 2010	Added more tests for Open Client to bring it into parity with the Linux client. Added specific Windows 7 test cases.
VMware Thin Client Certification Guide for VMware View 4.5 v5	V5	Dec. 22, 2010	Revise test cases (5.1, 5.14 & 5.15) for WES 7 thin client. Clarify software certification image submission.
VMware Thin Client Certification Guide for VMware View 4.5\4.6	V6	Feb. 24, 2011	View 4.6 release Revise test cases for USB Redirection Add Certification Process Flow Chart Clarification on RSA Test Cases
VMware Thin Client Certification Guide for VMware View 5	V7	July 29, 2011	- Change footer - New graphics for OpenView - Update PCoIP Requirements (Section 5.20 pg 96 & Section 6.24 pg 133) - Revise Test Cases 4.3 to 4.7 & 5.4 to 5.8 for View 5 - Update test case 2.3.4 Minimum Thin Client Software requirement for View 5 - Change XP SP2 requirement to SP3 for Thin Client - Remove test case 5.21 as View 5 no longer support RGS protocol - Add a note on changing default image cache GPO on thin client of 512MB & 1920x1200 resolution
VMware Thin Client Certification	V8	Sept 14, 2011	- Revise test cases 4.3 - 4.11 (Open Client)

Guide for VMware View 5			- Revise test cases 5.4-5.11 (Win Client)
VMware Thin Client Certification Guide for VMware View	V9	Feb 7, 2012	- Updated test cases around different SSL options for Linux CRT 1.4 & Custom\Open Clients - Added client-side cache test cases to Windows & Linux clients - Update kiosk mode test case for Linux
VMware Thin Client Certification Guide for VMware View 5.0.1	V10	March 29, 2012	- Remove non-SSL test cases for Windows client - Remove splash screen test cases for Open Client
VMware Thin Client Certification Guide for VMware View Connection Server v5.1, Windows Client 5.1 and Linux Client 1.5	V11	May 1, 2012	- Added new RADIUS 2-Factor Authentication test cases to all clients

1.2 How to Use This Guide

- Review **Section 2** and make sure you have everything you need to set up and configure the View certification test bed.
- Perform all tests in **Section 3** to set up the View certification test bed and record your results in the **Pre-Certification** checklist as you proceed.
- To certify a hardware thin client or a re-purposed PC software solution based on the View Open Client, perform all tests in **Section 4** and record your results in the **View Open Client** checklist. When finished, proceed to **Section 7** for information on submitting certification test results.
- To certify a Windows XPe/Windows Embedded Standard thin client running the View Client for Windows, perform all tests in **Section 5** and record your results in the **Windows View Client** checklist. When finished, proceed to **Section 7** for information on submitting certification test results.
- To certify a hardware thin client or a re-purposed PC software solution running the View Client for Linux, perform all tests in **Section 6** and record your results in the **Linux View Client** checklist. When finished, proceed to **Section 7** for information on submitting certification test results.

1.3 Certification Process Overview

1.3.1 Section Descriptions

Section 2 provides further details on the hardware, software, and expertise necessary for successfully setting up and configuring the View test bed required for certification.

Section 3 provides test cases that walk through the setup of the View test bed environment.

Section 4 provides the test cases to perform for the View Open Client certification.

Section 5 provides the test cases to perform for the Windows View Client certification.

Section 6 provides the test cases to perform for the Linux View Client certification.

Section 7 provides details on the certification submission Procedure and what to expect from VMware.

1.3.2 Certification Support

If you have any questions about the thin client certification program or experience issues related to VMware View software, test bed setup, certification tests, or the submission process, please e-mail vdi-cert-support@vmware.com

1.4 Certification Best Practices

1.4.1 Training

The partner performing the certification tests should be a VMware Certified Professional (VCP). Please see the following link for more information:

http://mylearn.vmware.com/portals/certification/

The partner should also be familiar with administering Microsoft operating systems, Microsoft network services, and Microsoft Active Directory.

1.4.2 Thin Client Integration

Review the guidelines on client integration and what optional components are needed. Please see Section 2.3 for more details. Once the requirements are understood, perform the integration of the Windows, Linux, or View Open Client with your thin client.

1.4.3 Test Bed Validation

To help ensure that the thin client certification process goes as smoothly as possible, VMware suggests that you completely validate the View test bed configuration before performing the actual thin client certification test cases.

1.4.4 Pre-Certification

Perform a complete pre-certification test cycle before performing the actual thin client certification tests for submission. By performing a pre-certification test cycle, you'll gain experience about how the actual test Procedure are executed as well as a high confidence that all tests can pass without issue.

1.4.5 Perform One-Pass

Once you are ready to perform the thin client certification tests for submission, execute the thin client certification test suite in one pass.

1.4.6 Isolated Network

VMware recommends configuring the View certification test bed on an isolated network. Using an isolated network ensures that the thin client certification tests are not interfering or competing with other network resources that might be in use on a production network. It also greatly simplifies the network setup and configuration of the thin client certification test bed.

2. Certification Requirements and Deliverables

2.1 Basic Requirements

- A Gigabit ethernet switch.
- A domain controller (Active Directory).
- A DNS server.
- A DHCP server.
- A VirtualCenter Server or vCenter Server.
- An ESX/ESXi 4.0 U4 or later server with at least 184 GB of disk storage. ESXi 5.0 is highly recommended.
- A server to host VMware View Connection Server.
- A laptop or desktop system running Windows XP Professional SP3 with Virtual Infrastructure Client (VI Client) or vSphere Client and View Client.
- Installation media and licenses for Microsoft Windows 2003 Server Enterprise SP2 32-bit or Windows Server 2008\R2.
- Installation media and licenses for Microsoft Windows XP Professional SP3 32-bit.
- Installation media and licenses for Microsoft Windows 7 (32-bit and 64-bit).
- Microsoft Windows XP SP3 Deployment Tools from http://www.microsoft.com.
- Installation media for vSphere 4 or 5.
- Installation media for View Connection Server, View Agent (32-bit and 64-bit), and View Clients.
- VMware SCSI drivers from http://www.vmware.com/download/server/drivers_tools.html.
- VMware Thin Client Certification submission form.
- A good understanding of basic network configuration, Microsoft Windows XP/Windows Server 2003\2008, Windows 7 administration, and VMware Virtual Infrastructure and vSphere administration.
- USB Flash drive
- Computer speakers or headphones.

2.2 Test Environment Hardware Configuration

The certification test bed can be assembled in one of two ways –

(1) on physical systems or

(2) on virtual machines in ESX Server.

2.2.1 Dedicated Systems or Virtual Machines

If you choose to host the certification test bed on separate systems, the minimum hardware requirements for the ESX Server would be lower.

Storage for the virtual machines on the ESX Server system can be any of the storage options supported by ESX Server (local storage, SAN, iSCSI, NFS, NAS, etc.). Ensure there is enough free disk space on the appropriate storage device for hosting the virtual machines needed for the test bed.

Below is a typical ESX Server configuration for hosting all VMware View services on a single ESX Server. See the *Systems Compatibility Guide for ESX Server* for a list of systems that support ESX Server.

- **Server –** An Intel or AMD based server. The server must meet the minimum requirements for ESX/ESXi 4.0 U4 or later outlined on the VMware website at http://www.vmware.com/support/pubs/vi_pubs.html
- **Processor** – At least 2 processors. 1.5 GHz minimum. Support for AMD-V or Intel VT required.
- **Memory** – 4 GB RAM minimum.
- **Storage** – A SCSI disk, Fibre Channel LUN, or RAID LUN. 184 GB of disk space minimum.
- **Networking** – 1 single-port Gigabit Ethernet card minimum.

In addition to the standalone physical systems or ESX Server, you will also need:

- **Network Switch** – Gigabit network switch with at least 4 ports.
- **Network Cables** – Cat5e network cables.
- **Thin Client System** – Thin client system being certified.

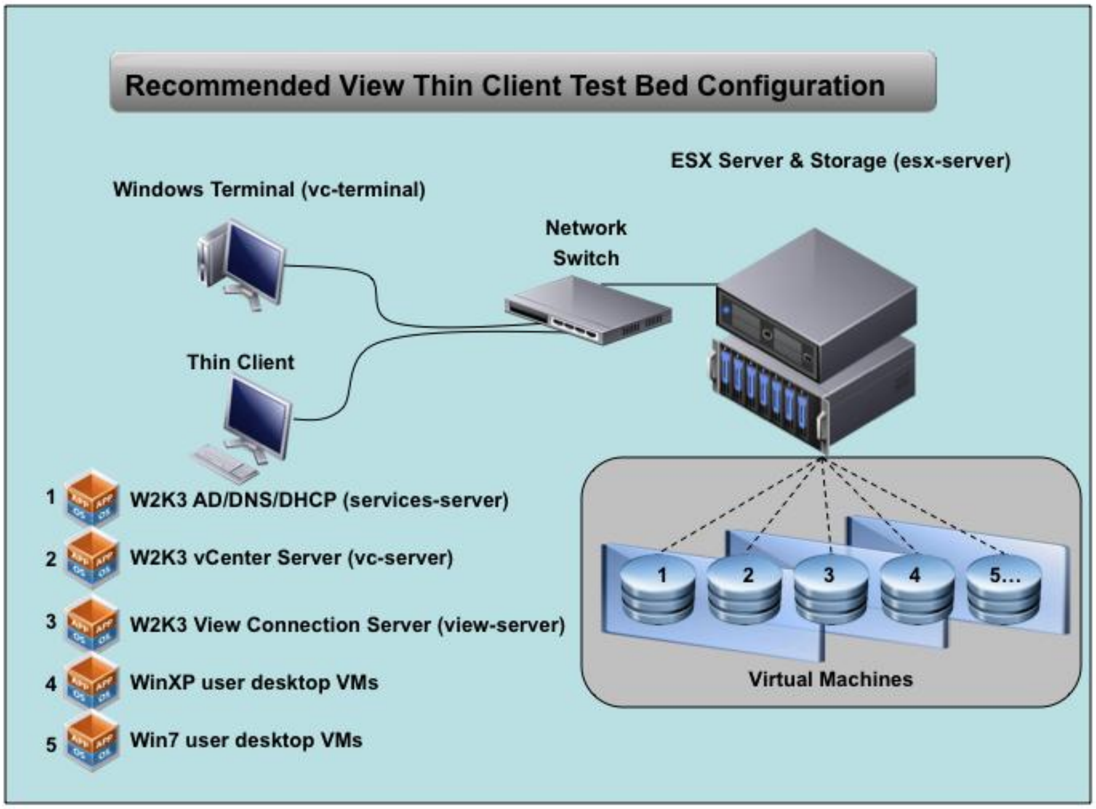

Recommended View Thin Client Test Bed Configuration
ESX Server & Storage (esx-server)
Windows Terminal (vc-terminal)
Network Switch
Thin Client
1 W2K3 AD/DNS/DHCP (services-server)
2 W2K3 vCenter Server (vc-server)
3 W2K3 View Connection Server (view-server)
4 WinXP user desktop VMs
5 Win7 user desktop VMs
1
2
3
4
5...
Virtual Machines

Figure 1 – Test Bed Diagram – ESX Server Hosted Configuration

2.2.2 Required Software

- ESX/ESXi 4.0 U4 or higher. ESXi 5.0 is highly recommended
- If you are using vSphere, you must have vSphere 4.0 Update 1 or Update 2 or vSphere 4.1 of the minimum
- View Connection Server
- View Agent (32-bit and 64-bit)
- View Clients
- Microsoft Windows 2003 Server Enterprise SP2 32-bit
- Microsoft Windows 2008\R2 Server
- Microsoft Windows XP Professional SP3 32-bit
- Microsoft Windows 7 (32-bit and 64-bit)

2.3 Thin Client Integration Requirements

The following sections provide minimum thin client requirements for VMware’s thin client certification program. The listed requirements are the minimum environments required to fully support the View Client for Windows, the View Client for Linux, or custom View clients based on the View Open Client.

Please refer to the README file that accompanies each VMware View client package for the most up-to-date hardware and software requirements for the View client as well as instructions for installing and integrating the View client with the thin client device.

2.3.1 Custom View Clients

Custom View clients based on the View Open Client or the View XML API must meet VMware's branding guidelines outlined in the **VMwareViewGraphicsUsage.pdf** document. The default open source non-VMware icons must be replaced with the approved VMware icons provided in the **VMwareViewGraphics.zip** package and the color scheme and appearance of the custom View client's GUI must match VMware's guidelines before being submitted to VMware for certification review.

2.3.2 Optional VMware View Features and Test Cases

Some features of the VMware View clients are optional. These optional features appear as optional test cases in this certification guide. However, if the thin client hardware or software supports a particular feature, then the feature and test case are mandatory. For example, not all thin clients can support the PCoIP protocol, Smart Card authentication, multi-monitor, kiosk mode, or multimedia redirection (MMR). When the thin client cannot support one of these features, the test case covering the feature is optional. When a thin client meets all the hardware and software requirements to support an optional feature, then the test case for the optional feature is mandatory and must be executed.

VMware may, at its discretion, accept certification submissions for thin clients that do not meet all the minimum requirements on a case-by-case basis. Please contact VMware for more information.

Please review the next section before proceeding with setting up the thin client test bed or executing actual certification test cases.

2.3.3 Minimum Thin Client Hardware

Thin Client Hardware requirements for the View Client for Windows:

Required

- **Processor**
    - **Without PCoIP support:** x86 processor compatible with Microsoft Windows
    - **With PCoIP support:** 800 MHz x86 processor with SSE2 extensions
- **Memory**
    - **Without PCoIP support:** 256 MB of SDRAM
    - **With PCoIP support:** Please see Test Case 5.25.
- Chipset compatible with Microsoft Windows
- 512 MB of local persistent storage
- Super VGA (800x600) or higher resolution video adapter
- 10/100 Mbps or faster Ethernet adapter
- Mouse and keyboard or equivalent

Optional

- USB
- Support for multiple monitors
- Serial, parallel, or PS/2 ports
- Audio

Thin Client Hardware requirements for the View Client for Linux or View Open Client:

Required

- **Processor**
    - **Without PCoIP support:** x86 or ARM processors
    - **With PCoIP support:** 800 MHz x86 processor with SSE2 extensions
- **Memory**
    - **Without PCoIP support:** 128 MB of SDRAM
    - **With PCoIP support:** Please see Test Case 6.22.
- Chipset compatible with Linux
- Super VGA (800x600) or higher resolution video adapter
- 10/100 Mbps or faster Ethernet adapter
- Mouse and keyboard or equivalent

Optional

- USB
- Support for dual monitors
- Serial, parallel, or PS/2 ports
- Audio

2.3.4 Minimum Thin Client Software

Thin Client Software requirements for the View Client for Windows:

Required

- Microsoft Windows XPe SP3 or higher,Microsoft Windows Embedded Standard or Microsoft Windows Embedded Standard 7.
- Microsoft Windows XPe SP3, Windows Embedded Standard or Windows Embedded Standard 7 should be completely loaded into the Flash RAM of the thin client.
- Microsoft Windows XPe SP3, Windows Embedded Standard or Windows Embedded Standard 7 must be configured with follow options:
    - USB enabled
    - Microsoft Internet Explorer

VMware highly recommends using RDP 7 in thin client devices running the View Client for Windows. However, VMware also fully supports RDP 6 on certain versions of Windows such as Windows Vista (Home/Business/Enterprise).

Thin Client Software requirements for the View Client for Linux or View Open Client:

Required applications and libraries

Required Version	**Libraries**
glibc 2.x	libc.so.6, libdl.so.2
gcc 3.4.x	libstdc++.so.6, libgcc_s.so.1
glib 2.22	libglib-2.0.so.0, libgobject-2.0.so.0
gtk+ 2.18	libgtk-x11-2.0.so.0, libgdk-x11.2.0.so.0, libgdk_pixbuf-2.0.so.0
libpng 1.2.x	libpng12.so.0
openssl 0.9.8	libssl.so.0.9.8, libcrypto.so.0.9.8
libxml 2.6.x	libxml2.so.2
zlib 1.2.3	libz.so.1

rdesktop 1.4.x or higher

rdesktop 1.5.x or higher to connect to a Microsoft Windows Vista desktop or to support Wyse MMR

2.4 Test Failure Information

If a test case fails, please provide the following information so that VMware can help address the problem:

- Configuration information of all the systems running in the certification environment.
- A description of the failure scenario and how to reproduce it.
- View Connection Broker version and build.
- View Agent version and build.
- View Client version and build.
- Logs for View Connection Broker, View Client, and View Agent. Please see the “Collecting Diagnostic Information for VMware View” section in the *VMware View Administrator’s Guide.*
- Any additional information that can help VMware analyze the problem.

3. Setting Up The Thin Client Test Environment

Use the following test cases to set up your VMware View thin client certification test environment. As each test case runs and passes, mark the results in the *Pre-Certification* checklist of the submission form. The *Pre-Certification* checklist must be submitted to VMware as part of the thin client certification submission.

3.1 View:Setup:IsolatedNetwork

Test Purpose

The thin client certification environment should be set up on an isolated Gigabit ethernet switch. An isolated network will prevent conflicts from services that may be running on an existing network.

Expected Results

An isolated network switch will host the thin client certification environment.

Procedure

1. Procure a Gigabit network switch to host the thin client certification environment.
2. The network switch will host addresses in the **192.168.23.xxx** range and the **vdi-test1.com** domain.

3.2 View:Setup:Terminal

Test Purpose

Set up a laptop or desktop system as a terminal for administering VirtualCenter Server or vCenter Server and View Connection Server. The terminal should run Microsoft Windows XP Professional SP3 32-bit and have vSphere Client and View Client for Windows installed.

Expected Results

A Windows XP Professional SP3 system with vSphere Client and View Client for Windows installed is connected to the network.

Procedure

1. Procure a laptop or desktop system running Microsoft Windows XP Professional SP3 32-bit. Be sure to have Administrator privileges to this system.
2. Log in to the machine as an administrator.
3. Set the following parameters on the system:
    - **Server name** – vc-terminal
    - **Password** – vmware
    - **Static IP** – 192.168.23.9
    - **Netmask** – 255.255.255.0
    - **Default Gateway** – 192.168.23.254
    - **DNS Server** – 192.168.23.10
    - **DNS Suffix –** vdi-test1.com
4. Attach **vc-terminal** to the network switch with a network cable.
5. Disable Windows Firewall on **vc-terminal**.
6. Procure the vSphere 4 installation media.
7. Install vSphere Client on **vc-terminal**.
8. Procure the View Client for Windows installation media.
9. Install View Client for Windows on **vc-terminal**.

3.3 View:Setup:NetworkServicesServer

Test Purpose

Install Microsoft Windows 2003 Server Enterprise SP2 32-bit on a physical machine or a virtual machine. This server will be attached to the network switch and will host a primary domain controller (Active Directory), a DHCP server, and a DNS server.

Expected Results

A server running Windows 2003 Server Enterprise SP2 is connected to the network switch.

Procedure

1. Procure a physical machine or set up a virtual machine with the following hardware specifications:
    - **Processor** – 2 GHz or higher Intel/AMD x86 processor
    - **Memory** – 2 GB RAM minimum
    - **Storage** – 10 GB
    - **Networking** – 100/1000 Mbps Ethernet
2. Procure the installation media for Microsoft Windows 2003 Server Enterprise SP2 32-bit along with a valid license.
3. Install Microsoft Windows 2003 Server Enterprise SP2 32-bit on the server.
4. Set the following parameters on the server:
    - **Server name** – services-server
    - **Administrator password** – vmware
    - **Static IP** – 192.168.23.10
    - **Netmask –** 255.255.255.0
    - **Default Gateway** – 192.168.23.254
5. Attach the **services-server** to the network switch.
6. Log into **services-server** as the Administrator and disable Windows Firewall.

3.4 View:Setup:NetworkServices

Test Purpose

Set up an Active Directory domain controller, DNS, and DHCP services on **services-server** for the thin client certification environment.

Expected Results

Active Directory domain controller, DNS, and DHCP services are running on **services-server**.

Procedure

1. Log into **services-server** as the Administrator.
2. Choose **Start > Manage Your Server**.
3. Choose **Add or remove a role**.
4. Use the setup wizard to add Domain Controller (Active Directory), DNS server, and DHCP server to the roles.
5. For the Domain Controller and DNS server:
    - Choose to install a domain controller for a new domain
    - Create a new domain in a new forest
    - Set the new Active Directory domain name to **vdi-test1.com**
    - Choose to install a DNS server along with the domain controller
6. For the DHCP server:
    - If a current Address Pool scope already exists, please delete it and create a new one.
    - Set the Address Pool from 192.168.23.100 – 192.168.23.200
    - Set the Router to 192.168.23.254 in Server Options
    - Set the DNS Servers to 192.168.23.10 in Server Options
    - Set the DNS Domain Name to **vdi-test1.com** in Server Options
7. Log into **vc-terminal** and join it to the **vdi-test1.com** domain, and make sure **vc-terminal** resolves to 192.168.23.9 in DNS.
8. Make sure **services-server** is in the **vdi-test1.com** domain and resolves to 192.168.23.10 in DNS.
9. In **vc-terminal**, change the Windows network settings to obtain an IP address and DNS automatically with DHCP.

3.5 View:Setup:VCServer

Test Purpose

Install Microsoft Windows 2003 Server Enterprise SP2 32-bit on a physical machine or a virtual machine. This server will be attached to the network switch and will host VirtualCenter Server or vCenter Server.

Expected Results

A server running Windows 2003 Server Enterprise SP2 is connected to the network switch.

Procedure

1. Procure a physical machine or set up a virtual machine with the following hardware specifications:
    - **Processor** – 2 GHz or higher Intel/AMD x86 processor
    - **Memory** – 2 GB RAM minimum
    - **Storage** – 10 GB
    - **Networking** – 100/1000 Mbps Ethernet
2. Procure the installation media for Microsoft Windows 2003 Server Enterprise SP2 32-bit along with a valid license.
3. Install Microsoft Windows 2003 Server Enterprise SP2 32-bit on the server.
4. Set the following parameters on the server:
    - **Server name** – vc-server
    - **Administrator password** – vmware
    - **Static IP** – 192.168.23.20
    - **Netmask** – 255.255.255.0
    - **Default Gateway** – 192.168.23.254
    - **DNS Server** – 192.168.23.10
5. Attach the **vc-server** to the network switch.
6. Log into **vc-server** as the Administrator and disable Windows Firewall.
7. Join **vc-server** to the vdi-test1.com domain.

3.6 View:Setup:VC

Test Purpose

Install VirtualCenter Server or vCenter Server on **vc-server** to manage the ESX Server that will run on the thin client certification environment.

Expected Results

VirtualCenter Server or vCenter Server will be running on **vc-server**.

Procedure

1. Procure thevSphere installation media from VMware.
2. Log into **vc-server** as the Administrator.
3. Refer to the the appropriate VMware documentation at http://www.vmware.com/support/pubs/ and install vCenter Server.
4. Log out of **vc-server**.

3.7 View:Setup:ESXServer

Test Purpose

VMware View requires an ESX Server to host desktop virtual machines. At least 184 GB of disk storage is recommended for the ESX Server.

Expected Results

ESX Server will be installed on a physical machine attached to the certification network.

Procedure

1. Procure the ESX/ESXi 4.0 U4 or later installation media from VMware. ESXi 5.0 is highly recommended.
2. Refer to the appropriate VMware documentation at http://www.vmware.com/support/pubs/ and install ESX/ESXi.
3. Set the following parameters on the ESX/ESXi Server:
    - **Server name** – esx-server
    - **root password** – vmware
    - **Static IP** – 192.168.23.11
    - **Netmask** – 255.255.255.0
    - **Default Gateway** – 192.168.23.254
    - **DNS Server** – 192.168.23.10
    - **DNS Domain** – vdi-test1.com
4. Configure the network settings on the ESX Server so that its virtual machines are connected to the thin client certification network switch.
5. Log into **services-server** as the Administrator.
6. Choose **Start > Manage Your Server** and add a host entry in the **vdi-test1.com** domain in DNS for **esx-server**.

3.8 View:Setup:AddESXToVC

Test Purpose

Configure the VirtualCenter Server or vCenter Server to manage the ESX Server on the thin client certification environment. The View Connection Server uses VirtualCenter Server or vCenter Server to provision desktop virtual machines on the ESX Server.

Expected Results

The vCenter Server will manage the ESX Server.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch the vSphere Client.
3. Connect to **vc-server** and provide the Administrator credentials.
4. Add **esx-server** to the vCenter Server.
5. Quit the VI Client.

3.9 View:Setup:InstallDeploymentTools

Test Purpose

Microsoft Windows guest operating systems that are cloned in vCenter Server require Microsoft's Sysprep tool to properly set up. Install Microsoft Windows XP SP3 Deployment Tools for the provisioning of user desktop virtual machines.

Expected Results

Microsoft Windows XP SP3 Deployment Tools installed in vCenter Server.

Procedure

1. Log into **vc-server** as the Administrator.
2. Procure the Microsoft Windows XP SP3 Deployment Tools CAB file from http://www.microsoft.com and copy it to **vc-server**.
3. Open the CAB file and copy all the files in it to the directory, C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\sysprep\xp or C:\Documents and Settings\All Users\Application Data\VMware\VMware vCenter\sysprep\xp.

3.10 View:Setup:DesktopVMTemplate

Test Purpose

Create a Windows XP Professional SP3 32-bit guest OS template on the ESX Server along with a guest customization specification to serve as a base desktop to deploy to VMware View users.

Expected Results

A Windows XP Professional SP3 guest OS template with a guest customization specification will be created on the ESX Server.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch the VI Client or vSphere Client.
3. Connect to **vc-server** and provide the Administrator credentials.
4. Create a new virtual machine on the ESX Server with the following specifications:
    - **Virtual machine name** – Windows XP Pro 32-bit
    - **ESX host** – esx-server.vdi-test1.com
    - **Number of virtual processors** – 1
    - **Memory** – 256 MB
    - **Networking** – 1 NIC
    - **Storage** – 10 GB, BusLogic SCSI controller
5. Install Windows XP Professional SP3 32-bit on the new virtual machine.
6. After installing the OS, join the virtual machine to the vdi-test1.com domain.
7. Make sure **vdi-test1.com/domain users** are allowed to log in through Remote Desktop in the **System Properties > Remote** tab.
8. Install VMware Tools on the guest OS.
9. Install VMware View Agent on the guest OS.
10. Disable Windows Firewall.
11. Shutdown the guest OS and the virtual machine.
12. Convert the Windows XP virtual machine to a template.
13. Deploy a new virtual machine from the Windows XP Pro 32-bit template.
14. Use the Customization Wizard to create a new customization specification with the following settings:
    - **Name** – your name
    - **Organization** – your organization
    - **Computer name** – use the virtual machine name
    - **Windows License** – enter the Microsoft Windows license information
    - **Administrator password** – vmware

- **Automatically log in as the Administrator** – disabled
- **Time zone** – your time zone
- **Run once** – keep the defaults
- **Network Interface settings** – typical settings
- **Domain** – vdi-test1.com
- **Generate new SID** – enabled

15. Save the customization specification as “view-xp-spec”.
16. Finish the deployment of the Windows XP virtual machine, and verify that the guest OS was cloned and set up correctly.
17. Shutdown the guest OS and delete the virtual machine from the disk.

3.11 View:Setup:IndividualDesktops

Test Purpose

Deploy two individual desktop virtual machines from the Windows XP Pro 32-bit guest OS template in vCenter Server. These two desktop virtual machines will be used in the thin client certification tests.

Expected Results

Two individual desktop virtual machines are deployed.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch the VI Client or vSphere Client.
3. Connect to **vc-server** and provide the Administrator credentials.
4. Select the Windows XP Pro 32-bit guest OS template and choose **Deploy Virtual Machine from this Template**.
5. Use the **Deploy Template Wizard** and set the following configuration for the new virtual machine:
    - **Virtual machine name** – individual1
    - **ESX host** – esx-server.vdi-test1.com
    - **Guest customization option** – view-xp-spec
    - **Power on this virtual machine after creation** - enabled
6. Verify that the desktop OS was set up correctly.
7. Repeat the deployment process on a second virtual machine and name it **individual2**.

3.12 View:Setup:Individual_Windows7_32

Test Purpose

Deploy an individual desktop virtual machine running Windows 7 32-bit in vCenter Server. This desktop virtual machine will be used in the thin client certification tests.

Expected Results

A Windows 7 individual desktop virtual machine is deployed.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch the VI Client or vSphere Client.
3. Connect to **vc-server** and provide the Administrator credentials.
4. Deploy a new virtual machine on **esx-server** to run Windows 7 32-bit.
5. Use the **Create New Virtual Machine Wizard** and set the following configuration for the new virtual machine:
    - **Typical configuration**
    - **Virtual machine name** – win7_32
    - **Guest OS Type** – Microsoft Windows 7 (32-bit)
6. Obtain installation media and a license for Windows 7 32-bit.
7. Install Windows 7 32-bit on the virtual machine.
8. During the installation, make **vmware** the default user and a system administrator with the password vmware.
9. After the installation is complete, log into the OS as **vmware**.
10. Verify that the desktop OS was set up correctly.
11. Choose **VM -> Guest -> Install/Upgrade VMware Tools** to install VMware Tools for Windows 7.
12. Disable the Windows Firewall.
13. Install the 32-bit VMware View Agent.
14. Join the **win7_32** VM to the vdi-test1.com domain.
15. In **System Properties -> Remote** tab, add vdi-test1.com Domain Users to the list of users allowed to connect remotely.
16. Log out of the **win7_32** VM.

3.13 View:Setup:Individual_Windows7_64

Test Purpose

Deploy an individual desktop virtual machine running Windows 7 64-bit in vCenter Server. This desktop virtual machine will be used in the thin client certification tests.

Expected Results

A Windows 7 64-bit individual desktop virtual machine is deployed.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch the vSphere Client.
3. Connect to **vc-server** and provide the Administrator credentials.
4. Deploy a new virtual machine on **esx-server** to run Windows 7 64-bit.
5. Use the **Create New Virtual Machine Wizard** and set the following configuration for the new virtual machine:
    - **Typical configuration**
    - **Virtual machine name** – win7_64
    - **Guest OS Type** – Microsoft Windows 7 (64-bit)
6. Obtain installation media and a license for Windows 7 64-bit.
7. Install Windows 7 64-bit on the virtual machine.
8. During the installation, make **vmware** the default user and a system administrator with the password vmware.
9. After the installation is complete, log into the OS as **vmware**.
10. Verify that the desktop OS was set up correctly.
11. Choose **VM -> Guest -> Install/Upgrade VMware Tools** to install VMware Tools for Windows 7.
12. Disable the Windows Firewall.
13. Install the 64-bit VMware View Agent.
14. Join the **win7_64** VM to the vdi-test1.com domain.
15. In **System Properties -> Remote** tab, add vdi-test1.com Domain Users to the list of users allowed to connect remotely.
16. Log out of the **win7_64** VM.

3.14 View:Setup:ViewConnectionServer

Test Purpose

Install View Connection Server on a physical machine or a virtual machine running Windows Server 2003 Enterprise SP2 32-bit or Windows 2008R2 if you'd like to have the PCoIP Secure Gateway feature installed.

Expected Results

View Connection Server installed and attached to the network switch.

Procedure

1. Procure a physical machine or set up a virtual machine with the following hardware specifications:
    - **Processor** – 2 GHz or higher Intel/AMD x86 processor minimum
    - **Memory** – 2 GB RAM
    - **Storage** – 8 GB
    - **Networking** – 100/1000 Mbps Ethernet card
2. Procure the installation media for Microsoft Windows Server 2003 Enterprise SP2 32-bit or Windows 2008R2 along with a valid license.
3. Install Microsoft Windows Server 2003 Enterprise SP2 or Windows 2008R2 on the server.
4. Set the following parameters on the server:
    - **Server name** – view-server
    - **Administrator password** – vmware
    - **Static IP** – 192.168.23.12
    - **Netmask** – 255.255.255.0
    - **Default Gateway** – 192.168.23.254
    - **DNS** – 192.168.23.10
5. Attach the server to the network switch.
6. Log in to **services-server** as the Administrator.
7. Add a new host entry in DNS for **view-server**.
8. Log out of **services-server**.
9. Log in to **view-server** as the Administrator.
10. Disable Windows Firewall.
11. Join **view-server** to the **vdi-test1.com** domain.
12. Procure the View Connection Server installation media and license key from VMware.
13. Refer to the *VMware View Installation and Administration Guide* and follow the instructions to install View Connection Server on **view-server**.
14. On **view-server,** launch Internet Explorer and go to https://view-server/admin. If you do not have Adobe Flash installed on your web browser, install it.
15. Log into the View Administrator portal with the **view-server** administrator credentials and make sure the license key is installed in View Connection Server in View Configuration.
16. Set up the View Connection Server to use the vCenter Server running on **vc-server**.

17. Add the domain administrator as an administrator of the View Connection Server in the View Administrator Configuration panel.

3.15 View:Setup:AddIndividualDesktopsToView

Test Purpose

Add pre-existing individual desktop virtual machines to the View Connection Server's inventory of desktops and entitle the desktops to all domain users.

Expected Results

Pre-existing individual desktop virtual machines are added to View Connection Server's inventory and entitled to all domain users.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
3. Log in to the **View Administrator** as the domain administrator.
4. In **Inventory -> Pools**, click **Add** to add a Manual Pool.
5. Click Next and choose a Dedicated assignment. Check Enable automatic assignment.
6. Click Next and choose vCenter virtual machines.
7. Click Next and choose **vc-server**.
8. Click Next and name the Pool ID and Display name **individual1**.
9. Click Next and use the following configuration:
    - **General -> State** – Enabled
    - **General -> Connection Server restrictions** – None
    - **Remote Settings -> Remote Desktop Power Policy** – Don't change
    - **Remote Settings -> Automatically logoff after disconnection** – Never
    - **Remote Settings -> Allow users to reset their desktop** - Yes
    - **Remote Display Protocol -> Default display protocol** – PCoIP
    - **Remote Display Protocol -> Allow users to choose protocol** – Yes
    - **Remote Display Protocol -> Max number of monitors** - 2
    - **Remote Display Protocol -> Max resolution of any one monitor** – 1920x1200
    - **Adobe Flash Settings -> Adobe Flash quality** – Do not control
    - **Adobe Flash Settings -> Adobe Flash throttling** - Disabled
10. Click **Next** and choose the **individual1** VM.
11. After the VM has been added to the pool, entitle it to all domain users in **vdi-test1.com.**
12. Repeat for the **individual2** VM but make it floating assignment and name the Pool ID and Display name individual2.
13. Repeat for the **win7_32** VM but make it floating assignment and name the Pool ID and Display name win7_32.

14. Repeat for the **win7_64** VM but make it floating assignment and name the Pool ID and Display name win7_64.
15. Log out of **View Administrator**.
16. Launch the View Client and connect to **view-server**.
17. Log in as the domain Administrator on the **vdi-test1.com** domain.
18. Make sure all the individual VMs are listed as available desktops to connect to.
19. Connect to **individual1**, and verify that the desktop is launched in View Client.
20. Log out of **individual1**.
21. Launch the View Client again and connect to **individual2**.
22. Verify that the desktop is launched in View Client.
23. Log out of **individual2**.
24. Launch the View Client again and connect to **win7_32**.
25. Verify that the desktop is launched in View Client.
26. Log out of **win7_32.**
27. Launch the View Client again and connect to **win7_64**.
28. Verify that the desktop is launched in View Client.
29. Log out of **win7_64.**

3.16 View:Setup:DedicatedPool

Test Purpose

Deploy an automated pool with dedicated assignment from the Windows XP Pro 32-bit guest OS template. Dedicated desktop pools allow users to log into the same desktop every time. Automated desktop pools are created and customized by the View Connection Server.

Expected Results

An automated pool with dedicated assignment is deployed.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
3. Log in to the **View Administrator** as the domain administrator.
4. Go to Inventory -> Pools and add a new Automated pool.
5. Click Next and choose Dedicated assignment. Check Enable automatic assignment.
6. Click Next and choose vCenter full virtual machines.
7. Click Next and name the Pool ID and Display name **dedicated**.
8. Click Next and use the following configuration:
   - **General -> State** – Enabled
   - **General -> Connection Server restrictions** – None
   - **Remote Settings -> Remote Desktop Power Policy** – Don’t change
   - **Remote Settings -> Automatically logoff after disconnection** – Never
   - **Remote Settings -> Allow users to reset their desktop** - Yes
   - **Remote Display Protocol -> Default display protocol** – PCoIP
   - **Remote Display Protocol -> Allow users to choose protocol** – Yes
   - **Remote Display Protocol -> Max number of monitors** - 2
   - **Remote Display Protocol -> Max resolution of any one monitor** – 1920x1200
   - **Adobe Flash Settings -> Adobe Flash quality** – Do not control
   - **Adobe Flash Settings -> Adobe Flash throttling** - Disabled
9. Click Next and enable provisioning.
10. Set the naming pattern to **dedicated**.
11. Set the max number of desktops to 2.
12. Set the number of spare desktops to 1 and provision all desktops up-front.
13. Click Next and select the Windows XP Pro 32-bit template, select the VM folder, host, resource pool, and datastore for the pool.
14. Click Next and choose the **view-xp-spec** for guest customization.

15. Finish deploying the pool.
16. Launch the vSphere Client.
17. Connect to **vc-server** as the Administrator.
18. Monitor the cloning and customization of the virtual machines in the new dedicated pool. This process will take several minutes to complete.
19. Log out of **vc-server**.
20. Go back to **View Administrator**.
21. Entitle the new dedicated pool to all domain users in the **vdi-test1.com** domain.
22. Launch View Client and connect to **view-server**.
23. Log in as the domain administrator on the **vdi-test1.com** domain.
24. Make sure the new dedicated pool is listed as available to connect to.
25. Connect to the dedicated pool, and verify that the desktop is launched in View Client.
26. Log out of the dedicated pool desktop.

3.17 View:Setup:FloatingPool

Test Purpose

Deploy an automated pool with floating assignment from the Windows XP Pro 32-bit guest OS template. Automated pools with floating assignment are available to users when they log in but are returned to the pool when users log off. Users log into a different desktop every time. Automated desktop pools are created and customized by View Connection Server. These two desktop virtual machines will be used in the thin client certification tests.

Expected Results

An automated pool with floating assignment is deployed.

Procedure

1. Log into **vc-terminal** as the Administrator.
2. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
3. Log in to the **View Administrator** as the domain administrator.
4. Go to Inventory -> Pools and add a new Automated pool.
5. Click Next and choose Floating assignment.
6. Click Next and choose vCenter full virtual machines.
7. Click Next and name the Pool ID and Display name **floating**.
8. Click Next and use the following configuration:
    - **General -> State** – Enabled
    - **General -> Connection Server restrictions** – None
    - **Remote Settings -> Remote Desktop Power Policy** – Don't change
    - **Remote Settings -> Automatically logoff after disconnection** – Never
    - **Remote Settings -> Allow users to reset their desktop** - Yes
    - **Remote Display Protocol -> Default display protocol** – PCoIP
    - **Remote Display Protocol -> Allow users to choose protocol** – Yes
    - **Remote Display Protocol -> Max number of monitors** - 2
    - **Remote Display Protocol -> Max resolution of any one monitor** – 1920x1200
    - **Adobe Flash Settings -> Adobe Flash quality** – Do not control
    - **Adobe Flash Settings -> Adobe Flash throttling** - Disabled
9. Click Next and enable provisioning.
10. Set the naming pattern to **floating**.
11. Set the max number of desktops to 2.
12. Set the number of spare desktops to 1 and provision all desktops up-front.
13. Click Next and select the Windows XP Pro 32-bit template, select the VM folder, host, resource pool, and datastore for the pool.

14. Click Next and choose the **view-xp-spec** for guest customization.
15. Finish deploying the pool.
16. Launch the vSphere Client.
17. Connect to **vc-server** as the Administrator.
18. Monitor the cloning and customization of the virtual machines in the new floating pool. This process will take several minutes to complete.
19. Log out of **vc-server**.
20. Go back to **View Administrator**.
21. Entitle the new floating pool to all domain users in the **vdi-test1.com** domain.
22. Launch View Client and connect to **view-server**.
23. Log in as the domain administrator on the **vdi-test1.com** domain.
24. Make sure the new floating pool is listed as available to connect to.
25. Connect to the floating pool, and verify that the desktop is launched in View Client.
26. Log out of the floating pool desktop.

3.18 View:Setup:DomainPasswordPolicy

Test Purpose

Set the domain password policy to support thin client certification testing. Modify the Active Directory password policy to allow 0-character passwords and disable password complexity requirements.

Expected Results

The domain password policy will be modified.

Procedure

1. Log into **services-server** as the Administrator.
2. Choose **Start > Manage Your Server > Manage users and computers in Active Directory**.
3. Right-click the **vdi-test1.com** domain and choose **Properties**.
4. Go to the **Group Policy** tab and edit the **Default Domain Policy**.
5. Navigate to **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.**
6. Set the minimum password length to 0 characters.
7. Disable “Password must meet complexity requirements”.
8. Log out of **services-server**.

3.19 View:Setup:RSASecurIDAuthenticationManager (Optional)

Test Purpose

Install Microsoft Windows 2003 Server Enterprise (SP2) 32-bit on a physical or virtual machine. This server will be attached to the network switch & will serve as the RSA Authentication Manager Server.

Expected Results

A server with the RSA Authentication Manager installed & is able to assign, generate and import token.

Procedure

1. Procure a physical machine or set up a virtual machine with the following hardware specifications:
    - Memory = 2GB
    - Hard Disk = 30GB
2. Procure the installation media for Microsoft Windows 2003 Server Enterprise SP2 32-bit along with a valid license
3. Install Microsoft Windows 2003 Server Enterprise 32-bit on the server
4. Set the following parameters on the server:
    - Server name: rsa
    - Administrator password: vmware
5. Attach the rsa server to the network switch
6. Join the rsa server to vdi-test1.com domain
7. Install & set up an RSA Authentication Manager. Refer to the documentation that accompies the RSA SecurID Authentication Manger software for more information on how to do this.
8. Install RSA SecurID Software Token Administration (http://www.rsa.com/node.aspx?id=2525)

3.20 View:Setup:RSASecurIDToken (Optional)

Test Purpose

Using the RSA Authentication Manager server to assign, generate & import token key

Expected Result

RSA Authentication Manager server can assign token key & passcode is successfully generated for users

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userrsa**”
2. Set the password to “**vmware**” and disable “User must change password at next logon”
3. Log into the rsa server as a domain administrator & launch the RSA Security Console & perform the following….
    a. Creating a new user
        i. Clicking on Identity > Users > Add New & enter “**userrsa**”
    b. Importing the token
        i. Clicking on Authentication > SecurID Tokens > Import Tokens Job > Add New
        ii. Click Browse & navigate to the RSA License XML file
        iii. Click Submit Job
    c. Assigning Token
        i. Clicking on Authentication > SecurID Tokens > Manage Existing
        ii. Click the Unassigned tab
        iii. Click the down arrow besides the token serial number & select Assign to user from the context menu
        iv. Click Search to list users
        v. Select “**rsauser”** user & click Assign
    d. Distributing Token File
        i. Clicking on Authentication > SecurID Tokens > Distribute Software Token Jobs > Add New > Distribute Token Files
        ii. In the Software Token Device Type, select (Passcode) Desktop PC AES 128-bit 3.0x
        iii. Click Next
        iv. Click Next
        v. Select one token per file & click Next
        vi. Click Next & select No Password
        vii. Click Submit Job
        viii. Click Compeleted tab
        ix. Click the down arrow besides the job & select Download Output File from the context menu
        x. Save software_token.zip to your local disk drive
    e. Using the Token File
        i. Extract *.sdtid from software_token.zip
        ii. Launch the RSA SecurID Software Token Administration application
        iii. Click Import from Files
        iv. Browse to the sdtid file & click OK
    f. Adding the Authentication Agent
        i. Launch the RSA Security Console
        ii. Click Access > Authentication Agents > Add New
        iii. Input View Connection Server’s IP address & click Resolve Hostname. This should resolve to your View Connection Server Hostname.
        iv. Click Save
    g. Generating the Configuration File
        i. From the RSA Security, click Access > Authentication Agents > Generate Configuration File
        ii. Click Generate Configuration File
        iii. Click Download Now
        iv. Save the AM_Config.zip on local disk
        v. Extract sdconf.rec from the zip file
        vi. Launch the View Connection Server Admin Portal

vii. Click View Configuration > Servers
viii. Select the View server & click Edit > Authentication tab
ix. Enable RSA SecurID 2-Factor Authentication
x. Click Browse and select sdconf.rec
xi. Click OK

3.21 View:Setup:RADIUS 2-Factor Authentication Manager (Optional)

Test Purpose

Install Microsoft Windows 2008R2 or any Windows Server version required to run the 2-Factor Authentication Manager There are a few different Authentication Managers that VMware View support. Depending on what you have setup, this authentication server can be attached to the network switch or as a standalone and will serve as the 2-Factor Authentication Manager Server.

Expected Results

A server with the Authentication Manager installed & is able to assign, generate and import token.

Procedure

1. Procure the installation media for Microsoft Windows 2008R2 along with a valid license
2. Install Microsoft Windows 2008R2 on the server
3. Set the following parameters on the server:
    a. Server name: radius
    b. Administrator password: vmware
4. Attach the radius server to the network switch
5. Join the radius server to vdi-test1.com domain if necessary
6. Install & set up an Radius Authentication Manager. Refer to the documentation that accompies the 2-Factor Authentication Manger software for more information on how to do this.

4. VMware View Open Client Test Cases

There are two options to certify a thin client utilizing a custom View client based on the VMware View Open Client.

A. Run the VMware View Open Client Test Cases

If the production-level custom View client source code changes cannot be submitted to VMware for review, please perform the View Open Client Test Cases below. As each test case runs and passes, mark the results in the *View Open Client* checklist of the submission form. The *View Open Client* checklist will be submitted to VMware as part of the certification submission.

B. Submit Source Code Changes to VMware for Review

VMware will only accept certification requests for production-level custom View clients. For the production-level custom View client, please submit the source code changes to the base VMware View Open Client to VMware for review along with the *Device and Company Information* sheet of the Submission Form and two production samples of the thin client. VMware will review the source code changes within two weeks after receiving the two thin client production samples. Once VMware approves the certification request, the thin client will be listed on the VMware Thin Client HCL.

4.1 View:OpenClient:LoginInvalid

Test Purpose

A user with an invalid username or invalid password cannot log into an entitled desktop.

Expected Results

An invalid user will not be allowed to log into the entitled desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userinvalid**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. With the View Open Client, connect to **view-server.vdi-test1.com**.
4. Enter the correct username but incorrect password, select the **vdi-test1.com** domain, and log in.
5. The user authentication should fail and an error message must be displayed indicating invalid credentials.
6. With the View Open Client, connect to **view-server.vdi-test1.com** again.
7. Enter the username incorrectly but enter the password correctly, select the **vdi-test1.com** domain, and log in.
8. The user authentication should fail and an error message must be displayed indicating invalid credentials.

4.2 View:OpenClient:ConnectionBrokerDisabled

Test Purpose

A user cannot log in to an entitled desktop when the connection broker is disabled.

Expected Results

A user cannot connect to the disabled connection broker.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usernobroker**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. In the **View Administrator**, go to the **View Configuration -> Servers** and disable **view-server** under the **View Connection Servers** section.
7. With the View Open Client, connect to **view-server.vdi-test1.com**.
8. The user will not be allowed to connect.
9. An error message must be displayed indicating a failure to connect to a View Connection Server.
10. Go back to the **View Administrator** and re-enable the **view-server**.

4.3 View:OpenClient:ConnectSSLDefault

Test Purpose

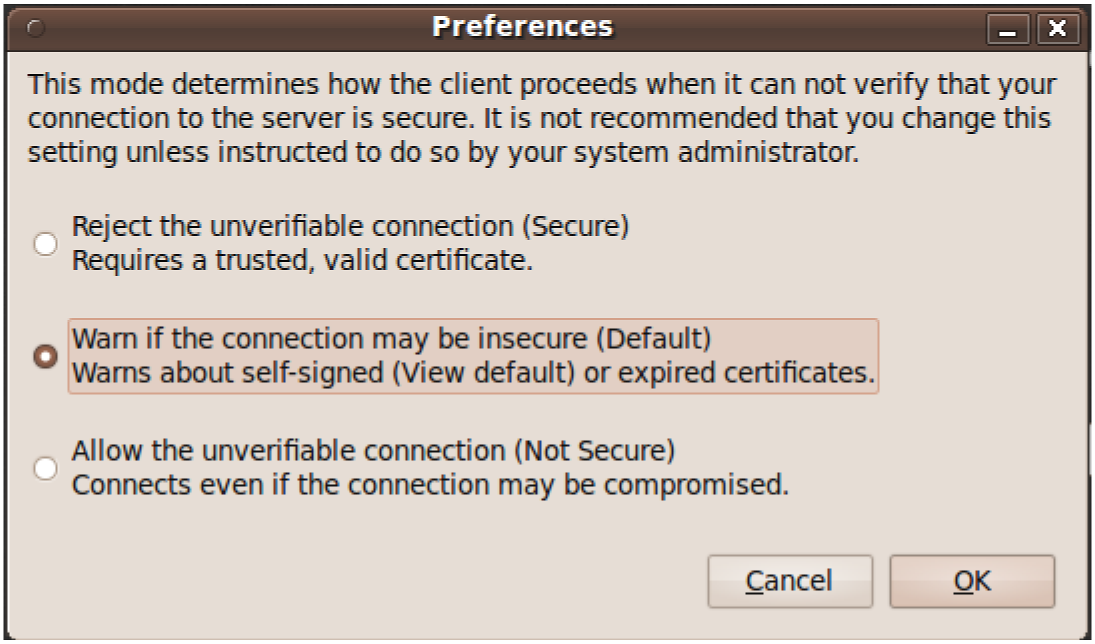
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL default security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userssl**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Global Settings** and make sure **Use SSL for client connections** is enabled.
7. Log into **view-server** as the Administrator.
8. Restart the View Connection Server service.
9. Log in to the thin client and launch the View Client.
10. Make sure **Use secure connection (SSL) option** is checked certificate checking mode is set to the default “**Warn if the connection may be insecure**.” Below is an example of what the SSL configuration window may look like.



This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

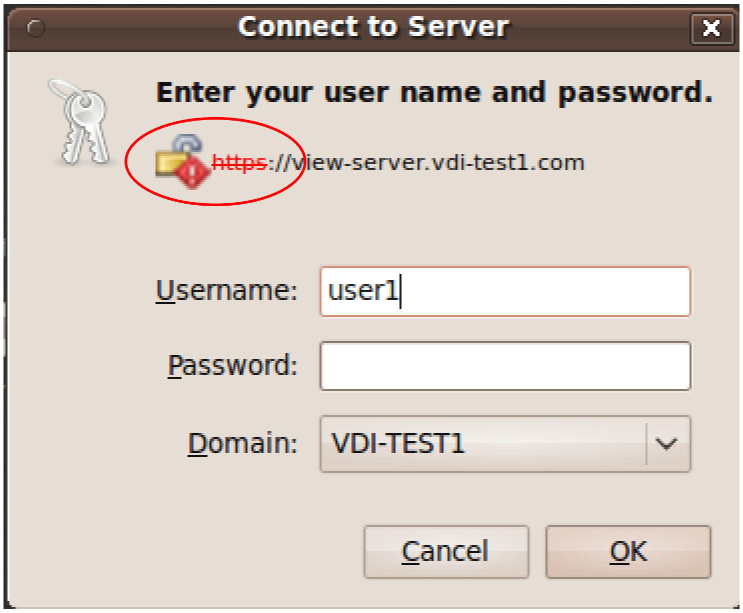
● Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

11. Connect to **view-server.vdi-test1.com** with the View Client.

12. You should get a prompt indicating that the View cannot verify the identity of the server. Choosing to “**Connect Insecurely**” should allow you to proceed with the username & password log-in screen.

13. Make sure the dialog shows the orange unlocked icon as shown below



Enter your user name and password.

~~https~~://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

14. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.

15. Verify that the desktop selector dialog box appears.

16. Choose the **individual1** desktop and connect.

17. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.

18. Log out of the desktop virtual machine.

19. Quit the View Client.

4.4 View:OpenClient:ConnectNotSecure

Test Purpose

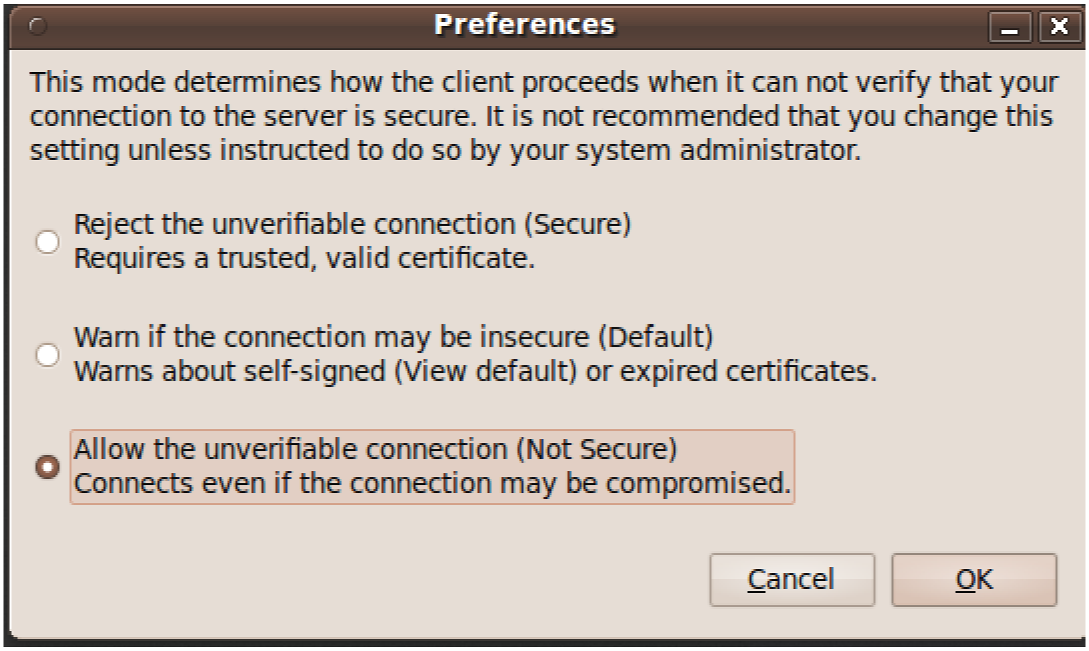
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop without any security check.

Procedure

1. Log in to the thin client and launch the View Client.
2. Ensure that the certificate checking mode is set to "**Allow the unverifiable connection (Not Secure)**." Below is an example of what the configuration window may look like.



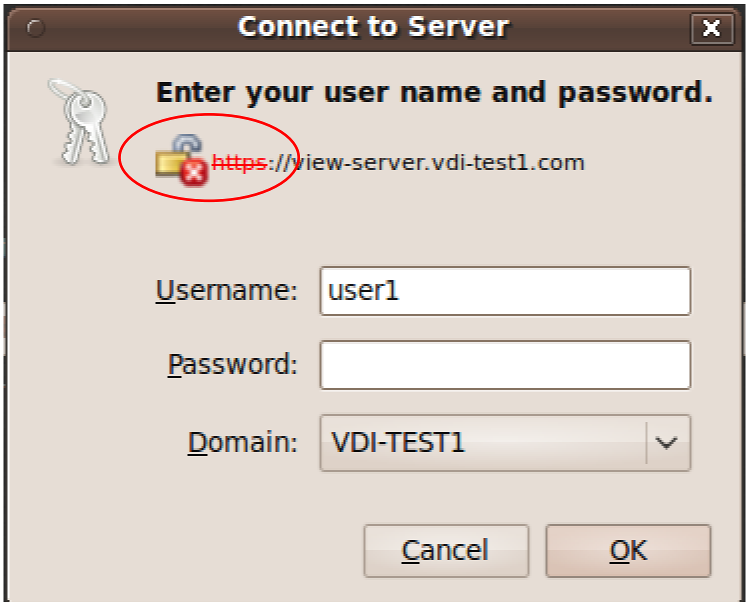
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

● Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are seeing the log-in screen as follows



Connect to Server

Enter your user name and password.

~~https~~://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Individual2** desktop and connect.
8. The user successfully connects to the **Individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

4.5 View:OpenClient:ConnectSSLSecure

Test Purpose

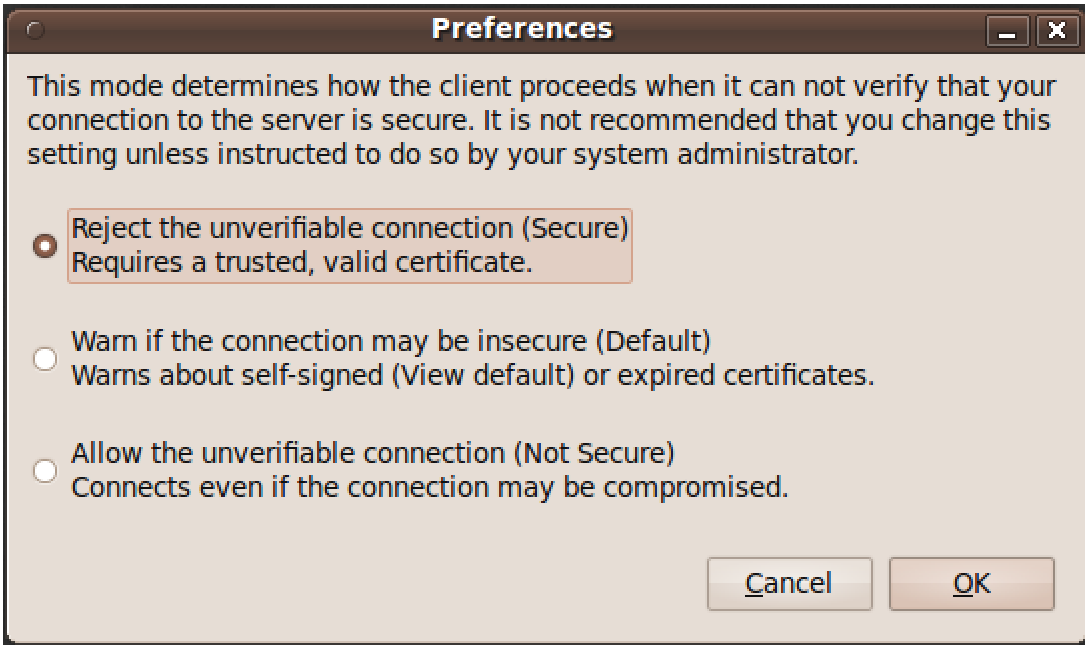
An attempt to connect to the View Connection Server without a valid certificate should result in an error.

Expected Results

Conneciton to the View Server should fail

Procedure

1. Log in to the thin client and launch the View Client.
2. Ensure that the certificate checking mode is set to “**Reject the unverifiable connection (Secure)**.” Below is an example of what the SSL configuration window may look like.



This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

● Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. You should get “the certificate authority is invalid or incorrect” error message as the valid certificate is not yet installed.
5. Quit the View Client application

4.6 View:OpenClient:SecurityCertificateSetup

Test Purpose

The root certificate is generated, signed & added to the server truststore so that the View Connection Server can authenticate users & permit them to connect to their View desktops.

NOTE: Please note that the certificate that you are installing to the server needs to be issued to the hostname "**view-server.vdi-test1.com**" If the security keystore is not generated or imported properly, you will not be able to pass the subsequent test cases.

Expected Results

Certificate is signed & imported to View Connection Server successfully.

Procedure

1. Please refer to the **VMware View Administration guide** and the **VMware View Installation guide** on how to generate, sign & import the root certificate to the View Connection Server

4.7 View:OpenClient:ConnectNotSecureWithCert

Test Purpose

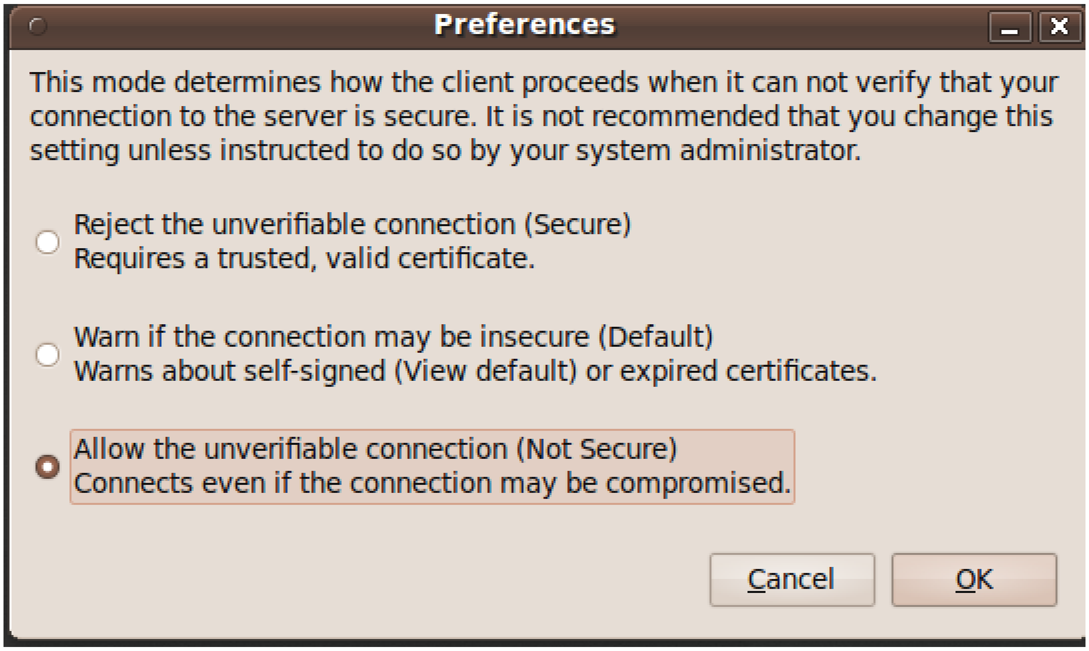
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Ensure that the certificate checking mode is set to “**Allow the unverifiable connection (Not Secure)**.” Below is an example of what the SSL configuration window may look like.



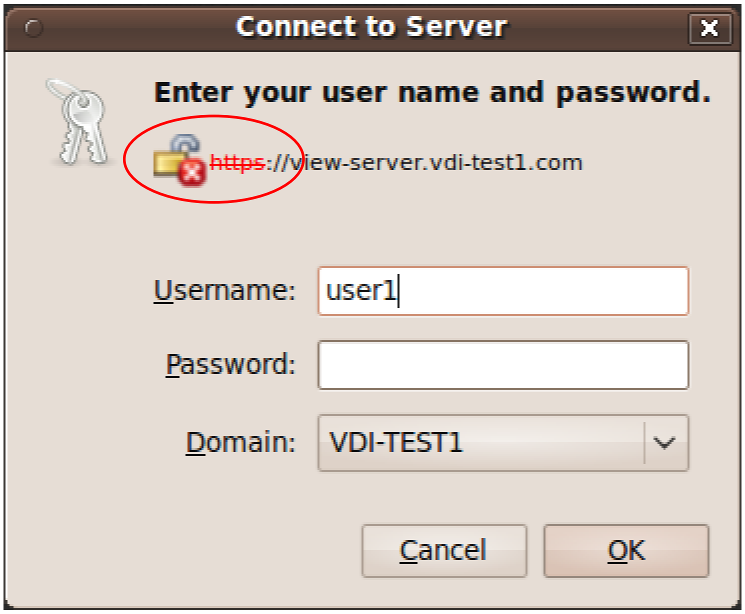
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

● Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are NOT getting any error message & that you are seeing the log-in screen as follows



Enter your user name and password.

~~https~~://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Dedicated1** desktop and connect.
8. The user successfully connects to the **Dedicated1** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

4.8 View:OpenClient:ConnectDefaultWithCert

Test Purpose

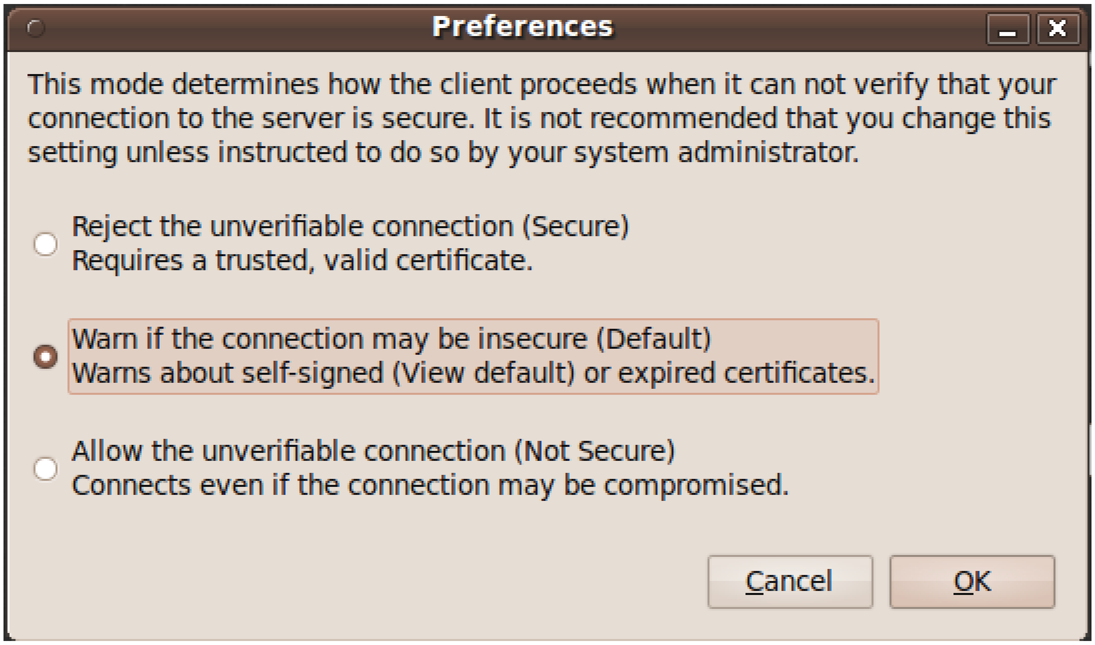
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL security set to default after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Ensure that the certificate checking mode is set to the default "**Warn if the connection may be insecure**." Below is an example of what the SSL configuration window may look like.



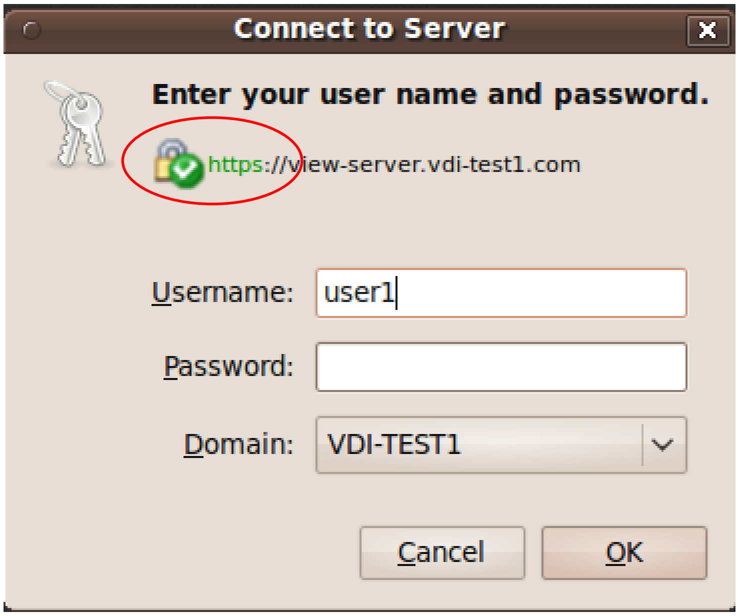
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

● Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are not getting any error message & that you are seeing the log-in screen with **green lock icon** as follows



Connect to Server

Enter your user name and password.

https://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Win7 64-bit** desktop and connect.
8. The user successfully connects to the **Win7 64-bit** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

4.9 View:OpenClient:ConnectSecureWithCert

Test Purpose

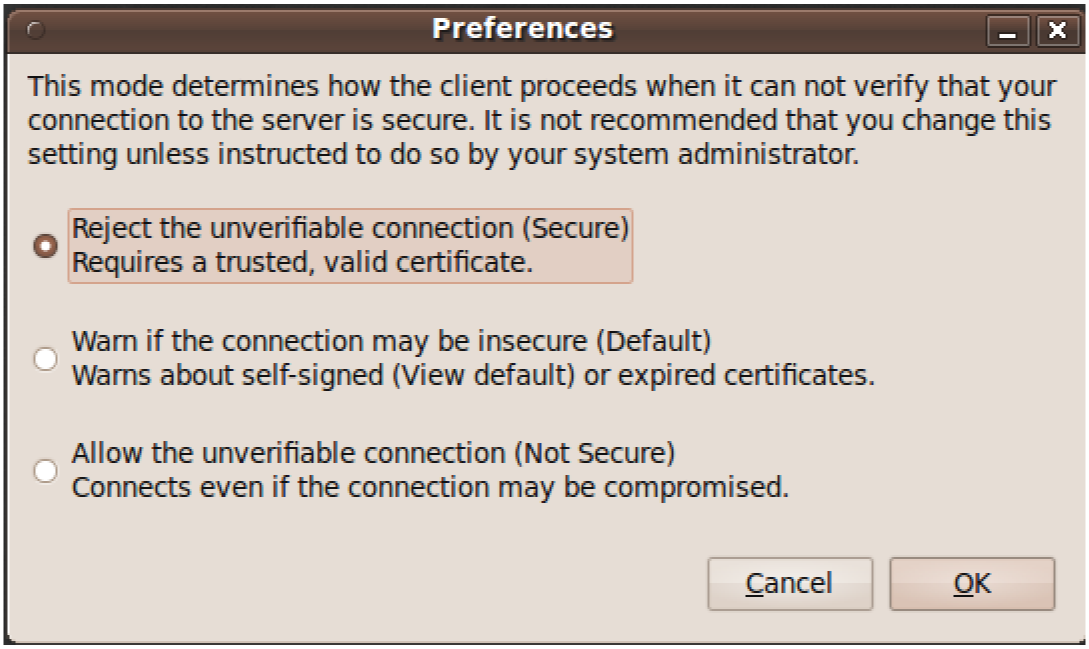
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL security set to full security after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Ensure that the certificate checking mode is set to “**Reject the unverifiable connection (Secure).**” Below is an example of what the SSL configuration window may look like.



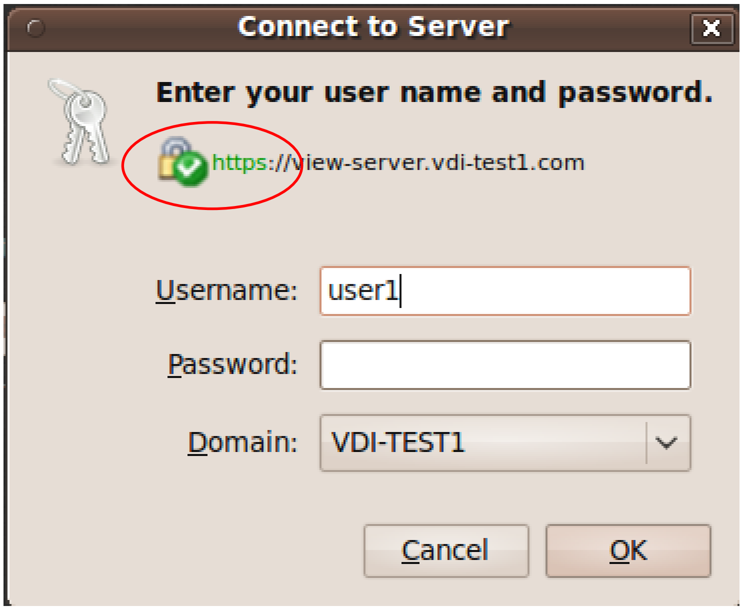
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

● Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are not getting any error message & that you are seeing the log-in screen with the **green lock icon** as follows



Connect to Server

Enter your user name and password.

https://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Win7 32-bit** desktop and connect.
8. The user successfully connects to the **Win7 32-bit** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

4.10 View:OpenClient:Non-SSLNotSupported

Test Purpose

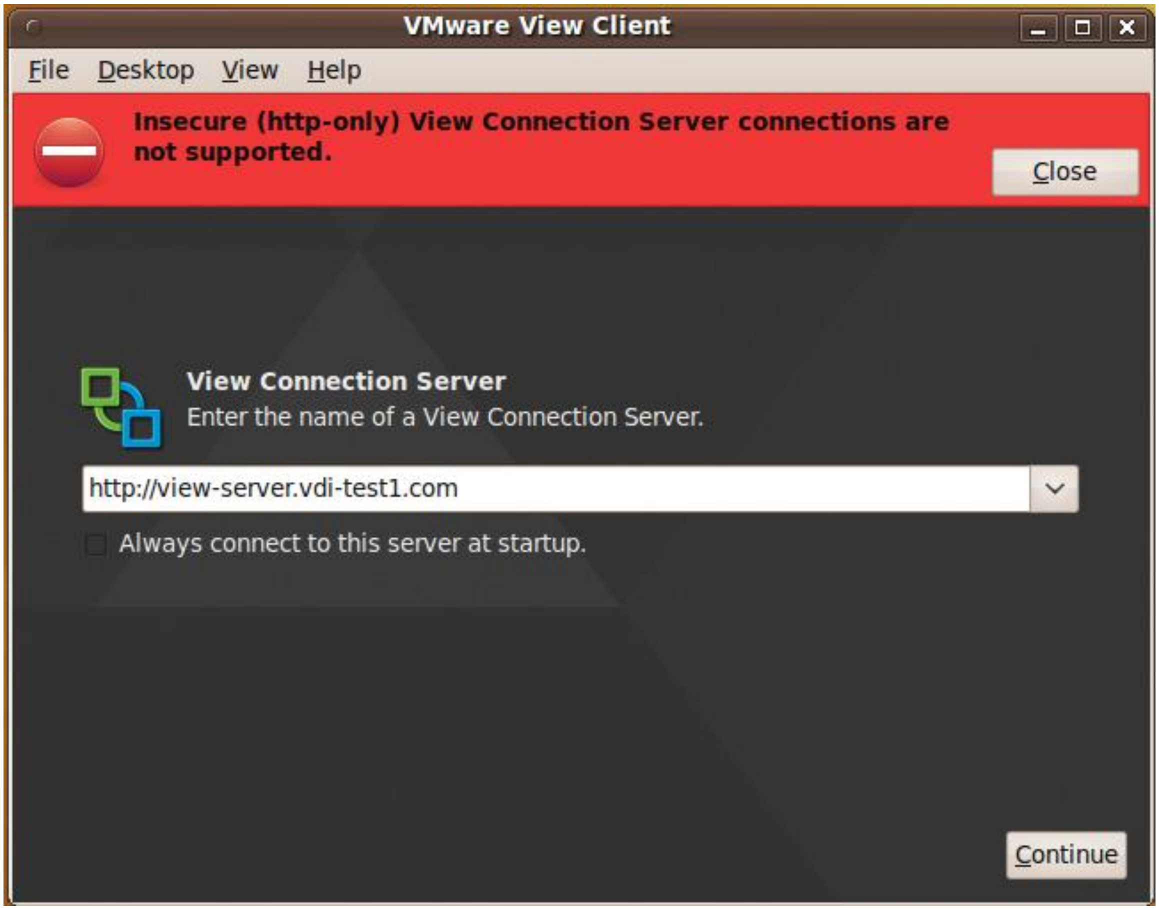
View Client fails to connect to View Connection Server in non-SSL mode

Expected Results

The user should be prompted that non-SSL (http-only) mode is not supported

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to **http://view-server.vdi-test1.com**
3. Connection attempt should fail & user should get the similar message as below



Insecure (http-only) View Connection Server connections are not supported.

View Connection Server

Enter the name of a View Connection Server.

http://view-server.vdi-test1.com

☐ Always connect to this server at startup.

4.11 View:OpenClient:ConnectXPFullscreen

Test Purpose

A valid user can connect to the View Connection Server and a Windows XP desktop virtual machine with the View client in fullscreen mode.

Expected Results

The user will successfully connect to a Windows XP desktop virtual machine in fullscreen mode.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userfullscreen**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View client with the fullscreen option.
5. Verify that the View client is in fullscreen mode and no other thin client operating system UI elements are visible.
6. Connect to **view-server.vdi-test1.com** with the View client.
7. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
8. Verify that the desktop selector dialog box appears.
9. Choose the **individual1** desktop and connect in fullscreen.
10. The user successfully connects to the **individual1** desktop virtual machine in fullscreen and will be automatically logged in to the OS.
11. Log out of the desktop session.
12. Quit the View client.

4.12 View:OpenClient:ConnectWin7Fullscreen

Test Purpose

A valid user can connect to the View Connection Server and a Windows 7 desktop virtual machine with the View client in fullscreen mode.

Expected Results

The user will successfully connect to a Windows 7 desktop virtual machine in fullscreen mode.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userfullscreen**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View client with the fullscreen option.
5. Verify that the View client is in fullscreen mode and no other thin client operating system UI elements are visible.
6. Connect to **view-server.vdi-test1.com** with the View client.
7. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
8. Verify that the desktop selector dialog box appears.
9. Choose the **win7_64** desktop and connect in fullscreen.
10. The user successfully connects to the **win7_64** desktop virtual machine in fullscreen and will be automatically logged in to the OS.
11. Log out of the desktop session.
12. Quit the View client.

4.13 View:OpenClient:BasicSessionDirectConnect

Test Purpose

A valid user can connect to the View Connection Server and an entitled desktop with the View client for without a secure tunnel.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop without a secure tunnel.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userdirectconnect**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Servers** and edit **view-server**.
7. Disable **Use secure tunnel connection to desktop**.
8. Log into the thin client.
9. Launch the View client and connect to **view-server.vdi-test1.com**.
10. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
11. Choose the **win7_32** desktop and connect using both RDP and PCoIP.
12. The user successfully connects to the **win7_32** desktop virtual machine and will be automatically logged in to the OS. No additional user validation was needed.
13. Log out of the desktop virtual machine.
14. Go back to the **View Administrator**.
15. Go to **View Configuration -> Servers** and edit **view-server**.
16. Enable **User secure tunnel connection to desktop**.

4.14 View:OpenClient:NoDesktopEntitlement

Test Purpose

A user cannot log in to a desktop that has not been entitled.

Expected Results

A user cannot connect to the unentitled desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usernoentitle**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. In **Inventory -> Pools**, remove the entitlement for domain users from the **individual2** pool.
7. With the View Open Client, connect to **view-server.vdi-test1.com**.
8. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
9. The user will not be allowed to connect to the un-entitled **individual2** desktop. Verify that the **individual2** desktop does not appear in the **Available Desktops** window.
10. Go back to the **View Administrator** and re-entitle domain users to the **individual2** pool.

4.15 View:OpenClient:SSONotMapped

Test Purpose

An entitled desktop that is not joined to the domain will require a second local authentication.

Expected Results

A desktop not joined to the domain will ask for a second local authentication.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usernosso**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch the VI Client or vSphere Client and connect to **vc-server**.
5. Log in as the Administrator.
6. Log into the **win7_32** desktop as an Administrator and remove it from membership in the domain.
7. Restart the **win7_32** desktop.
8. Quit the VI Client or vSphere Client.
9. With the View Open Client, connect to **view-server.vdi-test1.com**.
10. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
11. Choose the **win7_32** desktop and connect.
12. The user successfully connects to the desktop virtual machine but will not be automatically logged in to the OS. The OS will request local authentication.
13. Provide the local user authentication for the **win7_32** desktop.
14. The user will successfully log into the **win7_32** desktop.
15. Log out of the desktop virtual machine session.
16. Go back to **vc-terminal,** launch VI Client or vSphere Client, and reconnect to **vc-server** as the Administrator.
17. Log into the **win7_32** desktop as a local administrator and re-join the desktop to the domain.
18. Log out of the desktop.
19. Quit the VI Client or vSphere Client.

4.16 View:OpenClient:SessionTimeout

Test Purpose

A user will be disconnected from an entitled desktop after the View session timeout limit is reached.

Expected Results

A user will be disconnected from a desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usersessiontimeout**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Global Settings** and edit the Session timeout to 2 minutes.
7. With the View Open Client, connect to **view-server.vdi-test1.com**.
8. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
9. Choose a desktop that has been entitled to all domain users and connect.
10. The user successfully connects to the desktop virtual machine and will be automatically logged in to the OS.
11. Remain logged into the desktop.
12. Verify that the user is disconnected from the desktop after 2 minutes with a session timeout message.
13. Go back to the **View Administrator** portal and set the session timeout to the default of 600 minutes.

4.17 View:OpenClient:SessionForceDisconnect

Test Purpose

A user can be forcibly disconnected from an entitled desktop by the View Administrator.

Expected Results

A user will be disconnected from a desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userforceoff**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. With the View Open Client, connect to **view-server.vdi-test1.com**.
4. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
5. Choose a desktop that has been entitled to all domain users and connect.
6. The user successfully connects to the desktop virtual machine and will be automatically logged in to the OS.
7. Remain logged into the desktop.
8. Log into **vc-terminal** as the Administrator.
9. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
10. Log in to the **View Administrator** as Administrator.
11. Go to **Monitoring** -> **Remote Sessions**.
12. Click on the session used by “**userforceoff**”.
13. Then click **Disconnect Session** and confirm the action.
14. Verify that the user is forcibly disconnected from the desktop on the View Open Client.

4.18 View:OpenClient:DesktopReconnect

Test Purpose

A user can resume a desktop virtual machine session after a View client disconnect.

Expected Results

The user will resume the previous desktop virtual machine session.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userdisconnect**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **Inventory -> Desktops** and select the **individual1** desktop. Click **More Commands** and choose “Logoff Session” if a user is already logged on.
7. Log into the thin client.
8. Launch the View client and connect to **view-server.vdi-test1.com**.
9. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
10. Choose the **individual1** desktop and connect.
11. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
12. Open an Explorer window on the desktop virtual machine.
13. Physically disconnect the network cable from the thin client.
14. Verify that the desktop session disconnects.
15. Reconnect the network cable to the thin client.
16. Launch the View client and connect to **view-server.vdi-test1.com** again.
17. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
18. Choose the **individual1** desktop and connect.
19. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
20. Verify that the Explorer window is still open on the desktop.
21. Log out of the desktop virtual machine.

4.19 View:OpenClient:Keyboard

Test Purpose

The keyboard works correctly in the View client.

Expected Results

The keyboard works correctly in the View client.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userkeyboard**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View client and connect to **view-server.vdi-test1.com**.
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop and connect.
7. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
8. Launch the Notepad application.
9. Type the following:

   Virtual Machine’s are gr8at!

   #They are s000 cool!&%
10. Verify that the text entry works correctly.
11. Log out of the desktop virtual machine.

4.20 View:OpenClient:MinimumMemory

Test Purpose

A valid user can connect to the View Connection Server with the View client for with a minimum memory configured thin client.

Expected Results

The user will successfully connect to the View Connection Server.

Procedure

1. Use a thin client device configured with the minimum amount of memory that will be available to customers.
2. In the **vdi-test1.com** domain, create a new user with the username "**userminmem**".
3. Set the password to "**vmware"**, and disable "User must change password at next logon".
4. Log into the thin client.
5. Launch the View client and connect to **view-server.vdi-test1.com**.
6. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
7. Choose the **win7_64** desktop and connect.
8. The user successfully connects to the **win7_64** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the **win7_64** desktop.
10. Quit the View client.

4.21 View:OpenClient:MultiMonitor

Test Purpose

Verify that the View client will utilize all the displays in a multi-monitor thin client configuration. If the thin client device does not meet the hardware requirements to support multi-monitor, this test case can be skipped.

Expected Results

The View client will work with a multi-monitor thin client configuration.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usermultimon**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into the thin client.
4. Launch the View client and connect to **view-server.vdi-test1.com**.
5. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
6. In the **Display** option, choose Multimonitor.
7. Choose the **individual2** desktop and connect.
8. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Verify that the desktop spans across multiple displays.
10. Open a file manager window on the desktop virtual machine.
11. Drag the file manager window around all the displays and verify that the file manager window can be seen on all displays.
12. Log out of the desktop virtual machine.

4.22 View:OpenClient:AudioVideoRedirection (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client device will support some form of accelerated redirection of audio and video from the desktop VM to the thin client device. Verify the View client can play accelerated multimedia files in a connected session.

Expected Results

The View client plays multimedia files in a connected session.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usermmr**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Connect computer speakers or headphones to the thin client device.
4. Log into **vc-terminal** as the Administrator.
5. Launch the VI Client or vSphere Client and connect to **vc-server** as an Administrator.
6. Open a console to the **individual2** virtual machine, log in as **usermmr**, and copy the test multimedia files to the desktop. The following files should be copied: OLYMPICS.MPG, flowergarden320.avi, Damien.wmv, vandread_ep13_op_wm8_ver.wmv, Amazon_350k.wmv, and mediaexample.mp3.
7. Quit the VI Client or vSphere Client.
8. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
9. Log in to the **View Administrator** as Administrator.
10. Go to **Policies -> Global Policies** and make sure **Multimedia redirection (MMR)** is set to Allow in the View Policies section.
11. Log out of **View Administrator**.
12. Log into the thin client.
13. Launch the View client and connect to **view-server.vdi-test1.com**.
14. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
15. Choose the **individual2** desktop and connect.
16. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
17. Open Task Manager and monitor the CPU Usage. When accelerated audio and video redirection is utilized, CPU usage should be low during multimedia playback.
18. Launch Windows Media Player and complete the setup process if necessary.
19. Play mediaexample.mp3 in Windows Media Player.
20. The audio should stream smoothly from the desktop virtual machine to the thin client’s speakers or headphones.
21. Click Pause and the audio should pause.
22. Click Play and the audio should resume.

23. Play OLYMPICS.MPG in Windows Media Player. The playback should be smooth.
24. Click Pause and the video should pause.
25. Click Play and the video should resume.
26. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
27. While the video is playing, rewind and the video should rewind and continue playing without issue.
28. Play flowergarden320.avi in Windows Media Player. The playback should be smooth.
29. Click Pause and the video should pause.
30. Click Play and the video should resume.
31. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
32. While the video is playing, rewind and the video should rewind and continue playing without issue.
33. Play Damien.wmv in Windows Media Player. The playback should be smooth.
34. Click Pause and the video should pause.
35. Click Play and the video should resume.
36. Play vandread_ep13_op_wm8_ver.wmv in Windows Media Player. The playback should be smooth.
37. Click Pause and the video should pause.
38. Click Play and the video should resume.
39. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
40. While the video is playing, rewind and the video should rewind and continue playing without issue.
41. Play Amazon_350k.wmv in Windows Media Player. The playback should be smooth.
42. Click Pause and the video should pause.
43. Click Play and the video should resume.
44. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
45. While the video is playing, rewind and the video should rewind and continue playing without issue.
46. Log out of the View client.

4.23 View:OpenClient:USBFlashDrive (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client device will support some form of USB redirection from the thin client to the desktop VM. Verify that the View client on the thin client device can use a USB flash drive with the desktop virtual machine.

Expected Results

The View client on the thin client device connects and uses a USB flash drive with the desktop virtual machine.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userusb**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Enable USB redirection for the thin client.
5. Connect a USB flash drive to the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
8. Choose the **individual2** desktop and connect.
9. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
10. Verify that the USB flash drive is recognized by the **individual2** desktop virtual machine.
11. Edit and save a notepad file on the desktop.
12. Copy the notepad file to the USB flash drive.
13. Open the notepad file on the USB flash drive and verify the contents.
14. Perform the read & write tests to the flash drive by copying flowergarden320.avi to & from the USB flash drive
15. Play the flowergarden320.avi from the USB flash drive. Verify the video plays smoothly and the audio is synced.
16. Unplug & replug the USB flash drive from the thin client while still connecting to the desktop session and ensure that the USB flash drive unmounts & remounts properly (without having to disconnect and reconnect to the desktop session).
17. Log out of the desktop virtual machine.
18. Repeat the same tests with Win7 x86 & Win 7 x64 virtual desktops.

4.24 View:OpenClient:BasicSessionRSASecurID (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RSA SecurID authentication. A valid user can connect to the View Connection Server and an entitled desktop with the View client using RSA SecurID authentication.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Log into the thin client.
2. Launch the View client and connect to **view-server.vdi-test1.com**.
3. Provide the username and RSA SecurID token PIN.
4. Provide the user's domain login password.
5. Connect to the **individual2** desktop.
6. The user successfully connects to the **individual2** desktop virtual machine.
7. Log out of the desktop virtual machine.

4.25 View:OpenClient:Valid2-FactorAuthentication (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RADIUS 2-Factor Authentication. There are a few different Authentication Managers that VMware View support. Depending on what you have setup, please perform the tests below. A valid user can connect to the View Connection Server and an entitled desktop with the View client using RADIUS 2-Factor Authentication.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Launch the web browser and go to the **View Administrator** portal at https://view-server/admin
2. Log into the **View Administrator** as an Administrator
3. Go to **View Configuration -> Servers.** Click on **Connection Servers** tab and highlight your **View Connection Server** name and select **Edit**. This should bring up the "**Edit View Connection Server Settings**"
4. Select the **Authentication** tab and setup the **Authenticator** but DO NOT enable "**Enforce 2-factor and Windows user name matching" and "Use the same User name and password for RADIUS and Windows Authentication" options**
5. Log into the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Provide the valid username and passcode if you're using **VASCO Authentication Manager** (Note: the passcode consists of PIN & token generated by the Vasco Authentication Manager)

   OR

   Provide AD user name and password, which is imported into **SMSPASSCODE server** if you're using **SMSPASSCODE Authentication Manager**
8. Provide the static passcode is using **SMSPASSCODE Authentication Manger**
9. Provide the user's domain login password
10. Connect to the **individual2** desktop.
11. The user successfully connects to the **individual2** desktop virtual machine.
12. Log out of the desktop virtual machine.

4.26 View:OpenClient:AD Matching 2-Factor Authentication (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RADIUS 2-Factor Authentication. There are a few different Authentication Managers that VMware View support. Depending on what you have setup, please perform the tests below. A valid user can connect to the View Connection Server and an entitled desktop with “Enforce 2-Factor and Windows user name matching” option enabled.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Launch the web browser and go to the **View Administrator** portal at https://view-server/admin
2. Log into the **View Administrator** as an Administrator
3. Go to **View Configuration -> Servers.** Click on **Connection Servers** tab and highlight your **View Connection Server** name and select **Edit**. This should bring up the “**Edit View Connection Server Settings**”
4. Select the **Authentication** tab and enable “**Enforce 2-factor and Windows user name matching”** but NOT the **“Use the same User name and password for RADIUS and Windows Authentication” option**
5. Log into the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Provide the valid username and passcode if you are using **VASCO Authentication Manager** (Note: the passcode consists of PIN & token generated by the **VASCO Authentication Manager**)

   OR

   Provide AD user name and password, which is imported into **SMSPASSCODE server** if you’re using **SMSPASSCODE Authentication Manager**
8. Provide the static passcode if you are using **SMSPASSCODE Authentication Manger**
9. Provide the user’s domain login password
10. Connect to the **Win7 x64** desktop.
11. The user successfully connects to the **Win7 x64** desktop virtual machine.
12. Log out of the desktop virtual machine.

4.27 View:OpenClient:BasicSessionSmartCard (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. A valid user can connect to the View Connection Server and an entitled desktop with the View client for using Smart Card authentication and both the RDP and PCoIP protocol.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usersmartcard**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Install the Smart Card reader on the thin client along with the necessary drivers and libraries. Refer to the documentation that accompanies the Smart Card reader for more information about how to do this.
4. Set up the Active Directory server and View Connection Server to support Smart Card authentication for the “**userlinuxsmartcard”** user. Refer to the “Smart Card Authentication” section of the ***VMware View Manager Administration Guide*** for more information about how to do this at http://www.vmware.com/support/pubs/view_pubs.html.
5. Enable Smart Card support in the View client.
6. Log into the thin client.
7. Plug the Smart Card into the Smart Card reader.
8. Launch the View client and connect to **view-server.vdi-test1.com**.
9. Provide the Smart Card PIN.
10. Connect to the **individual2** desktop using the RDP protocol.
11. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS with no additional authentication.
12. Log out of the desktop session.
13. Repeat logging into the **individual2** desktop with the Smart Card and the PCoIP protocol.
14. Log out of the desktop session.
15. Log off the thin client.

4.28 View:OpenClient:SmartCardRemovalPolicy (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. Verify that a Smart Card authenticated user is automatically disconnected from a desktop virtual machine when the Smart Card is removed.

Expected Results

A Smart Card authenticated user will automatically be disconnected from a desktop virtual machine when the Smart Card is removed.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userscremoval**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Servers,** highlight **view-server** and click **Edit.** In the **Authentication** tab**,** enable **Disconnect user sessions on smart card removal**.
7. Log out of **View Administrator**.
8. Set up the thin client and user for Smart Card authentication in the vdi-test1.com domain.
9. Log in to the thin client.
10. Insert the Smart Card.
11. Launch the View client and connect to **view-server.vdi-test1.com**. Provide the login PIN if necessary.
12. Choose the **individual2** desktop.
13. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
14. Remove the Smart Card from the Smart Card reader.
15. Verify that the user is automatically disconnected from the desktop virtual machine session.
16. Log out of the thin client.

4.29 View:OpenClient:ClientInfo

Test Purpose

Verify that local system information from the system running the View Open Client is passed to the View Agent on the desktop virtual machine and saved in the Windows Registry.

Expected Results

System information from the thin client is stored in the desktop virtual machine's Windows Registry.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usersysinfo**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. With the View Open Client, connect to **view-server.vdi-test1.com**.
4. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
5. Choose a desktop that has been entitled to all domain users and connect.
6. The user successfully connects to the desktop virtual machine and will be automatically logged in to the OS.
7. On the desktop virtual machine, run the "regedit" command to open the Windows System Registry.
8. Navigate to **My Computer\HKEY_CURRENT_USER\Volatile Environment.**
9. Verify that all the following data exists in the Windows System Registry:
    - **ViewClient_IP_Address** = the IP address of the thin client device
    - **ViewClient_MAC_Address** = the MAC address of the thin client device
    - **ViewClient_Machine_Name** = the machine name of the thin client device
    - **ViewClient_LoggedOn_Username** = usersysinfo
    - **ViewClient_Type** = the thin client name or operating system type of the thin client device
10. Log off the desktop virtual machine.

4.30 View:OpenClient:ApplicationIcon

Test Purpose

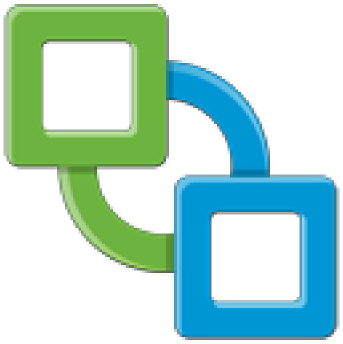
The View Open Client should have an application icon consistent with the current View icon illustrated in the **VMware View Graphics Guide** pdf file.

Expected Results

The View Open Client application icon is consistent with the guidelines in the **VMware View Graphics Guide** pdf file.

Procedure

1. Refer to the **VMware Graphics Guide** pdf file for the most up-to-date information about the View graphics guidelines.
2. Log into the thin client.
3. Verify that the View Open Client application icon on the desktop and in menus looks like this:



4.31 View:OpenClient:LoginBanner

Test Purpose

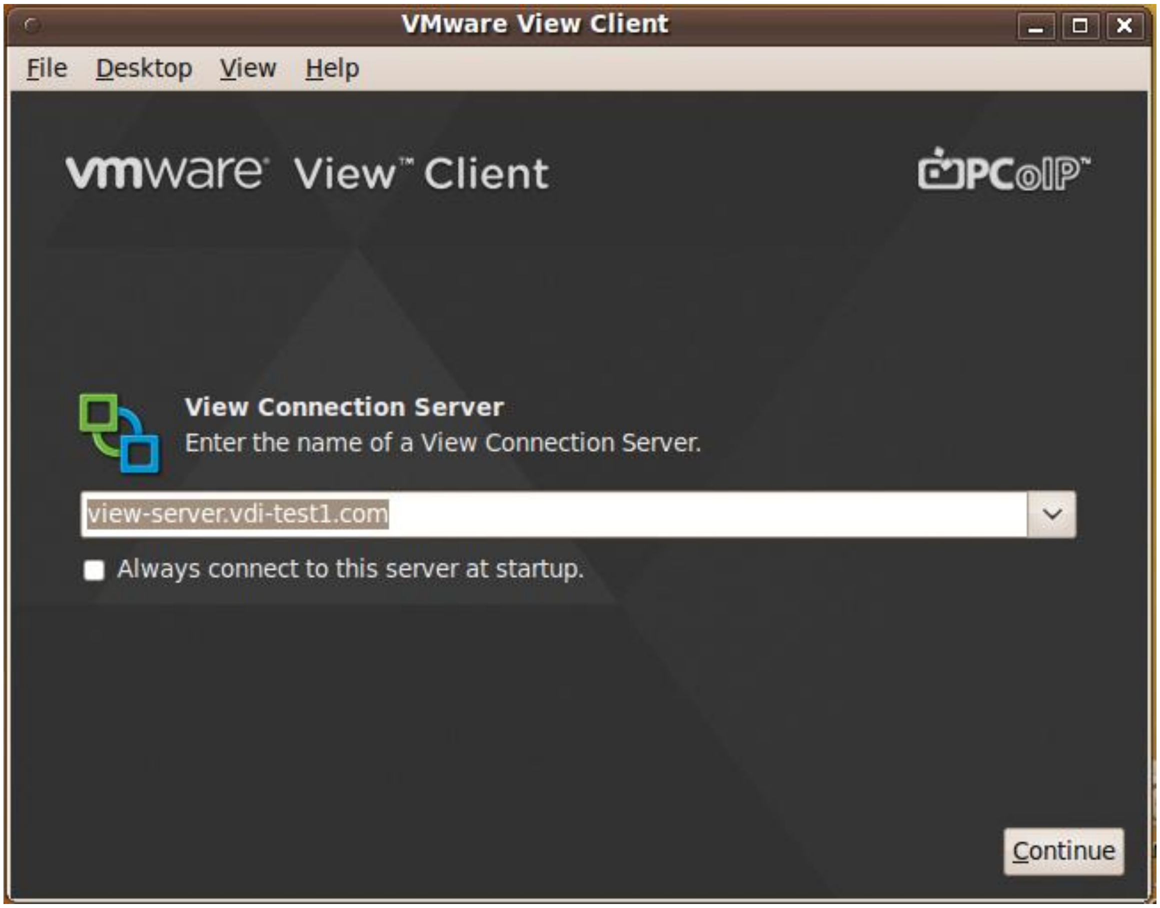
The View Open Client should have a login screen banner consistent with the current View login screen banner illustrated in the **VMware Graphics Guide** pdf file.

Expected Results

The View Open Client login screen banner is consistent with the guidelines in the **VMware View Graphics Guide** pdf file.

Procedure

1. Refer to the **VMware View Graphics Guide** pdf file for the most up-to-date information about the View graphics guidelines.
2. Log into the thin client.
3. Verify that the View Open Client login screen banner looks similar to this:



View Connection Server

Enter the name of a View Connection Server.

view-server.vdi-test1.com

☐ Always connect to this server at startup.

4. No other logos besides VMware logos may be present on the View Client login screen.
5. The VMware and View Manager logos must be present on the same login screen where user credentials are presented.

6. The VMware and View Manager logos must be a minimum of 48 x 48 pixels.
7. The copy “VMware View” must be present and located on the top banner.
8. The Typeface for “VMware View” must be Myriad Pro Condensed.
9. For the Login screen; Username, Password, and Windows Domain name are required. The SecurID login prompt is optional.
10. There must be a “Connect” button to connect to a virtual machine and a “Cancel” button which exits the client placed at the bottom of the login screen.
11. If available, “Help” - a button linked to a help document and “Options” - a button which provides advanced options for client must be labeled “Help” and “Options”.
12. The charcoal gradient background used for the login screen must use exact same values as described in the graphics guide. Please refer to the guide posted on Partner Central.
13. The light gray background used for the login screen must be exactly as described in the graphics guide. Please refer to the guide posted on Partner Central.

4.32 View:OpenClient:PreLoginMessage

Test Purpose

A View Connection Server pre-login message can be displayed on the View Open Client.

Expected Results

A pre-login message will be displayed on the View Open Client.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userpremessage**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin
5. Log into the **View Administrator** as an administrator.
6. Edit **View Configuration -> Global Settings** and enable “Pre-login message”.
7. Set the pre-login message to be “Hello, VMware!”.
8. Log into the thin client.
9. With the View Open Client, connect to **view-server.vdi-test1.com**.
10. Verify that the pre-login message is displayed.
11. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
12. The user successfully connects to the desktop virtual machine and will be automatically logged in to the OS.
13. Log off the desktop virtual machine.

4.33 View:OpenClient:UIGuidelines

Test Purpose

Verify that the thin client conforms to VMware’s user interface guidelines for running the View Open Client.

Expected Results

The thin client conforms to VMware’s user interface guidelines for running the View Open Client.

Procedure

1. Verify that it is possible for a non-Administrative user to launch the View Client without use of the ‘--nonInteractive’ commandline option. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which ‘--nonInteractive’ mode is not used.
2. Verify that it is possible for a non-Administrative user to launch the View Client with custom options provided via the commandline and options file. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which custom options can be supplied. The user must be able to supply all the custom options that the View Client supports.
3. Verify that it is possible for a non-Administrative user to launch the View Client using the ‘--unattended’ commandline option. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which the ‘--unattended’ commandline option is supplied. When the View Client is launched with the ‘--unattended’ commandline option, it must also support the user-supplied ‘--serverURL’, ‘--userName’, ‘--password’, and ‘--domainName’ options.

5. VMware View Client for Windows Test Cases

Use the following test cases to certify a Microsoft Windows XPe, Windows Embedded Standard, Windows Embedded Standard 7 thin client running the VMware View Client for Windows. As each test case runs and passes, mark the results in the *Windows View Client* checklist. The *Windows View Client* checklist will be submitted to VMware as part of the thin client certification submission.

5.1 View:WinClient:SWRequirements

Test Purpose

Verify that the Microsoft Windows thin client meets the minimum software requirements for the VMware View Client for Windows application.

Expected Results

The thin client device meets the minimum software requirements for View Client for Windows.

Procedure

1. Log into the thin client as an Administrator.
2. Verify that Microsoft Windows has the following minimum components required by View Client for Windows:
    - Common Control Libraries Version 5
    - Common Control Libraries Version 6 [1.0.0.0]
    - Common Control Libraries Version 6 [1.0.10.0]
    - Primitive: Iphlpapi
    - Primitive: Msimg32
    - Primitive: Ole32
    - Primitive: Oleaut32
    - Primitive: Secur32
    - Primitive: Setupapi
    - Primitive: Shell32
    - Primitive: WinHttp
    - Primitive: Ws2_32
    - Primitive: Wtsapi32
    - DbgHelp Library
    - RPC Local Support (not applicable to WES 7)
    - Terminal Services Client ActiveX Core
    - Urlmon Library
    - Win32 API – Advanced
    - Win32 API – GDI
    - Win32 API – Kernel
    - Win32 API – User
    - WinHTTP
    - Wininet Library

- Workstation Service

3. Verify that Microsoft Windows has the following optional components in order to run the View Client for Windows Support Tool:
    - WMI Scripting
    - WMI Core
    - WMI Win32 Provider
    - WMI Correlation (not applicable to WES 7)
4. Verify that Microsoft Windows has the following optional component in order to view Help documentation:
    - Internet Explorer
5. Verify that Microsoft Windows has the following optional component in order to install the USB driver:
    - Add Hardware Control Panel (newdev.dll)

5.2 View:WinClient:SetupNetworking

Test Purpose

Verify that the Microsoft Windows thin client can connect to the thin client certification environment.

Expected Results

The thin client connects to the thin client certification environment.

Procedure

1. Connect the thin client to the thin client certification network switch.
2. Log into the thin client as an Administrator.
3. Verify the thin client has an IP address.
4. Disable Windows Firewall if it is active.

5.3 View:WinClient:Install

Test Purpose

Install the View Client for Windows on the thin client.

Expected Results

The View Client for Windows installs on the thin client without any issues.

Procedure

1. Log in to the thin client as an Administrator.
2. Procure the View Client for Windows installer from VMware.
3. Copy the View Client installer to the thin client.
4. Refer to the *VMware View Installation and Administration Guide* and follow the instructions to install the View Client.
5. Verify that the View Client installed on the thin client without any error message.
6. Launch the View Client and verify that the View Client dialog box appears.
7. Quit the View Client.

5.4 View:WinClient:ConnectSSLDefault

Test Purpose

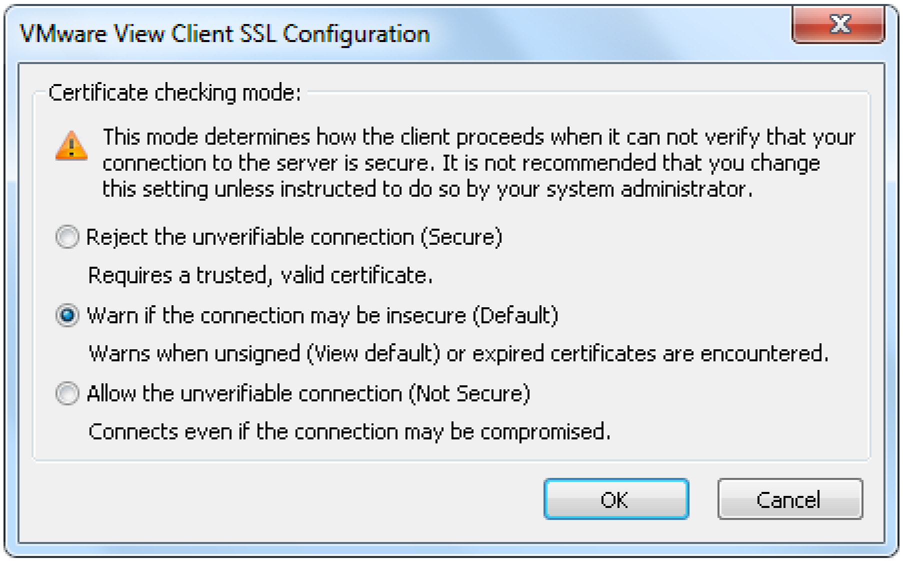
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL default security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userssl**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Global Settings** and make sure **Use SSL for client connections** is enabled.
7. Log into **view-server** as the Administrator.
8. Restart the View Connection Server service.
9. Log in to the thin client and launch the View Client.
10. Click on **Configure SSL.** This should bring up the **VMware View Clie**nt **SSL Configuration window**. In this window, keep the default setting (“**Warn if the connection may be insecure**”) shown below.



VMware View Client SSL Configuration

Certificate checking mode:

This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)

Requires a trusted, valid certificate.

● Warn if the connection may be insecure (Default)

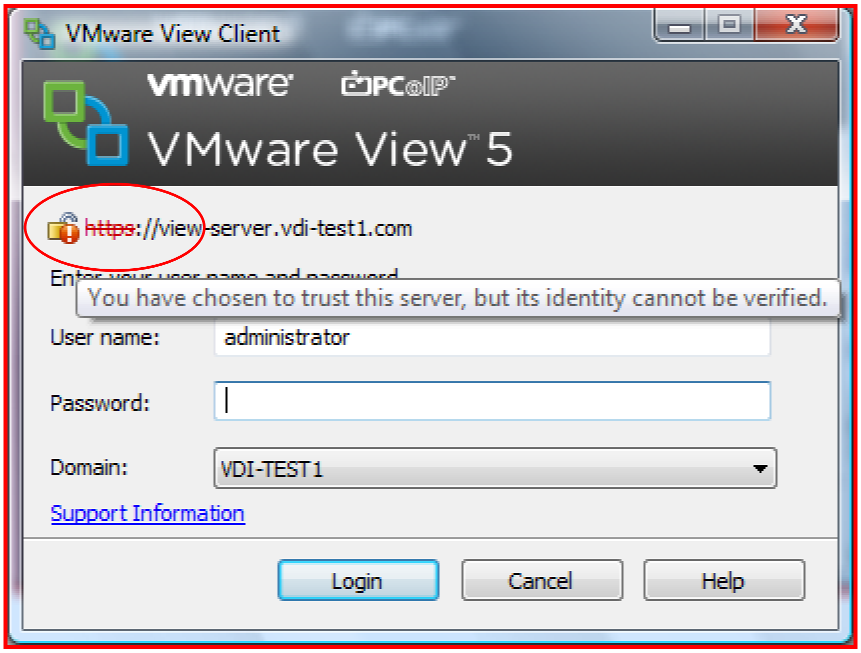
Warns when unsigned (View default) or expired certificates are encountered.

○ Allow the unverifiable connection (Not Secure)

Connects even if the connection may be compromised.

11. Connect to **view-server.vdi-test1.com** with the View Client.
12. You should get a prompt indicating that the View cannot verify the identity of the server. Click **Continue** on this prompt. It should allow you to enter the user’s credentials to connect to the View Server

13. Please verify that the username/password dialog shows the orange unlocked icon as shown below



~~https~~://view-server.vdi-test1.com

You have chosen to trust this server, but its identity cannot be verified.

User name: administrator

Password:

Domain: VDI-TEST1

14. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.

15. Verify that the desktop selector dialog box appears.

16. Choose the **individual1** desktop and connect.

17. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.

18. Log out of the desktop virtual machine.

19. Quit the View Client.

5.5 *View:WinClient:ConnectSSLNotSecure*

Test Purpose

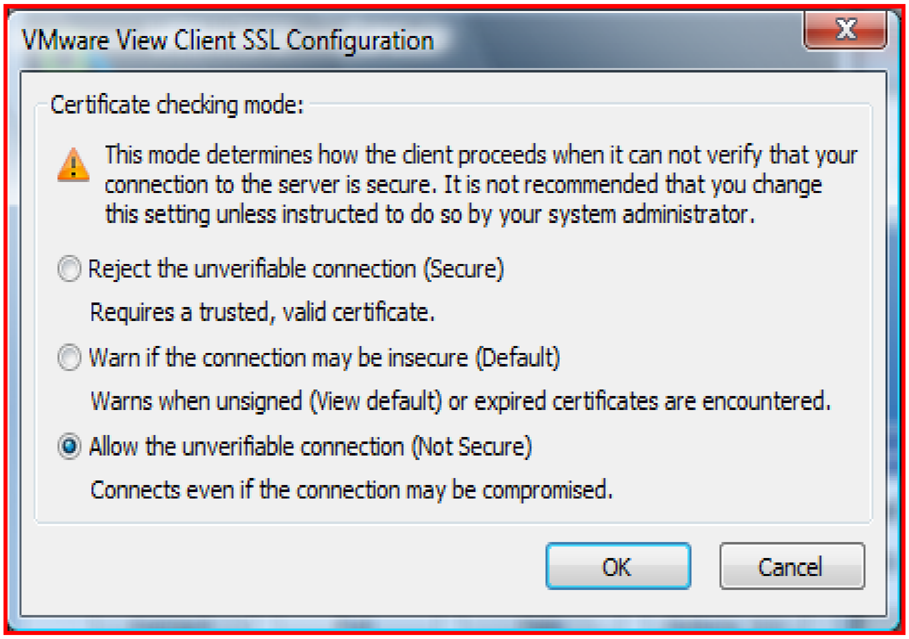
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop without any security check.

Procedure

1. Log in to the thin client and launch the View Client.
2. Click on **Configure SSL.** This should bring up the **VMware View Client SSL Configuration window**. In this window, check "**Allow the unverifiable connection (Not Secure)** option & click **Ok**



VMware View Client SSL Configuration

Certificate checking mode:

This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)

Requires a trusted, valid certificate.

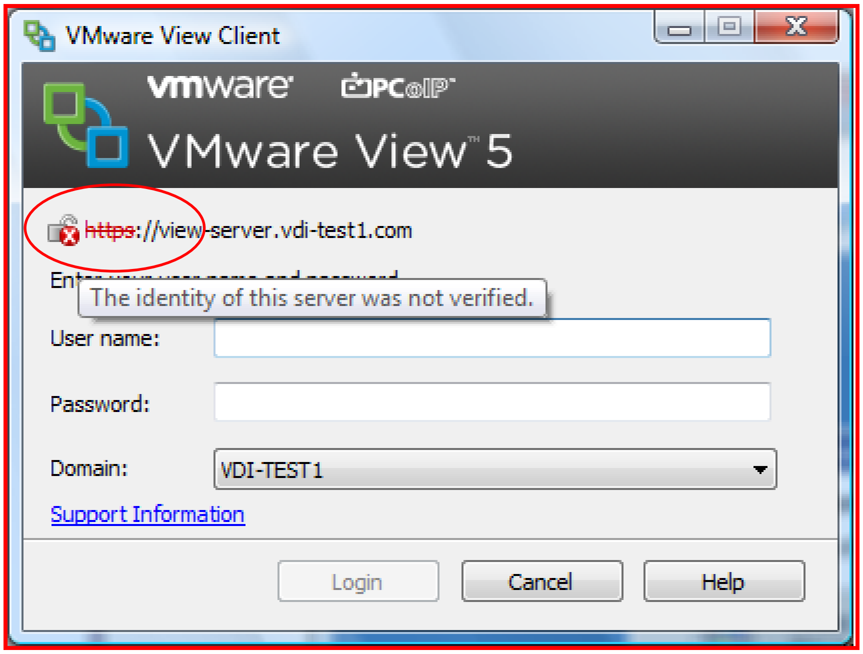
○ Warn if the connection may be insecure (Default)

Warns when unsigned (View default) or expired certificates are encountered.

● Allow the unverifiable connection (Not Secure)

Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are seeing the log-in screen as follows



~~https~~://view-server.vdi-test1.com

The identity of this server was not verified.

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Individual2** desktop and connect.
8. The user successfully connects to the **Individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

5.6 *View:WinClient:ConnectSSLSecure*

Test Purpose

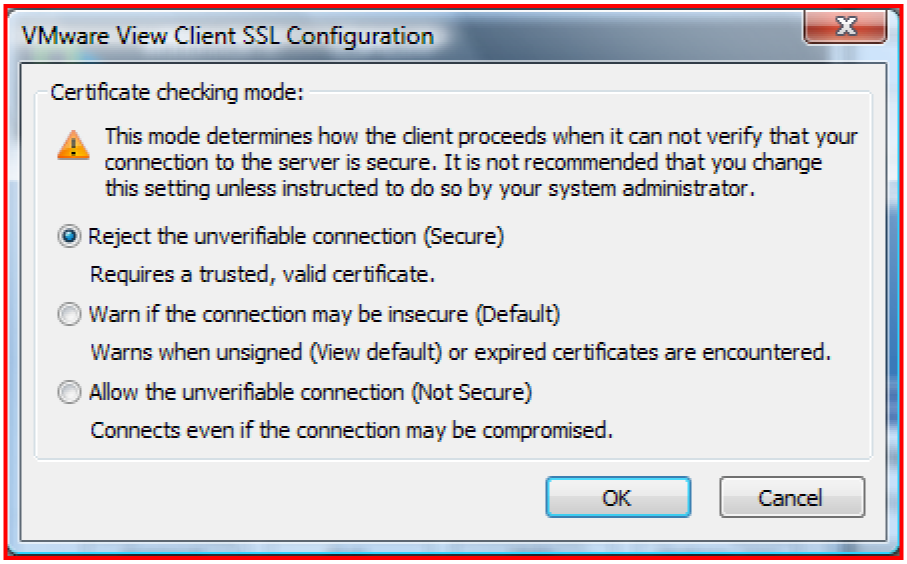
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop without any security check.

Procedure

1. Log in to the thin client and launch the View Client.
2. Click on **Configure SSL.** This should bring up the VMware View Client SSL Configuration window. In this window, check "Reject the unverifiable connection (Secure)" option & click Ok



VMware View Client SSL Configuration

Certificate checking mode:

This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

● Reject the unverifiable connection (Secure)

Requires a trusted, valid certificate.

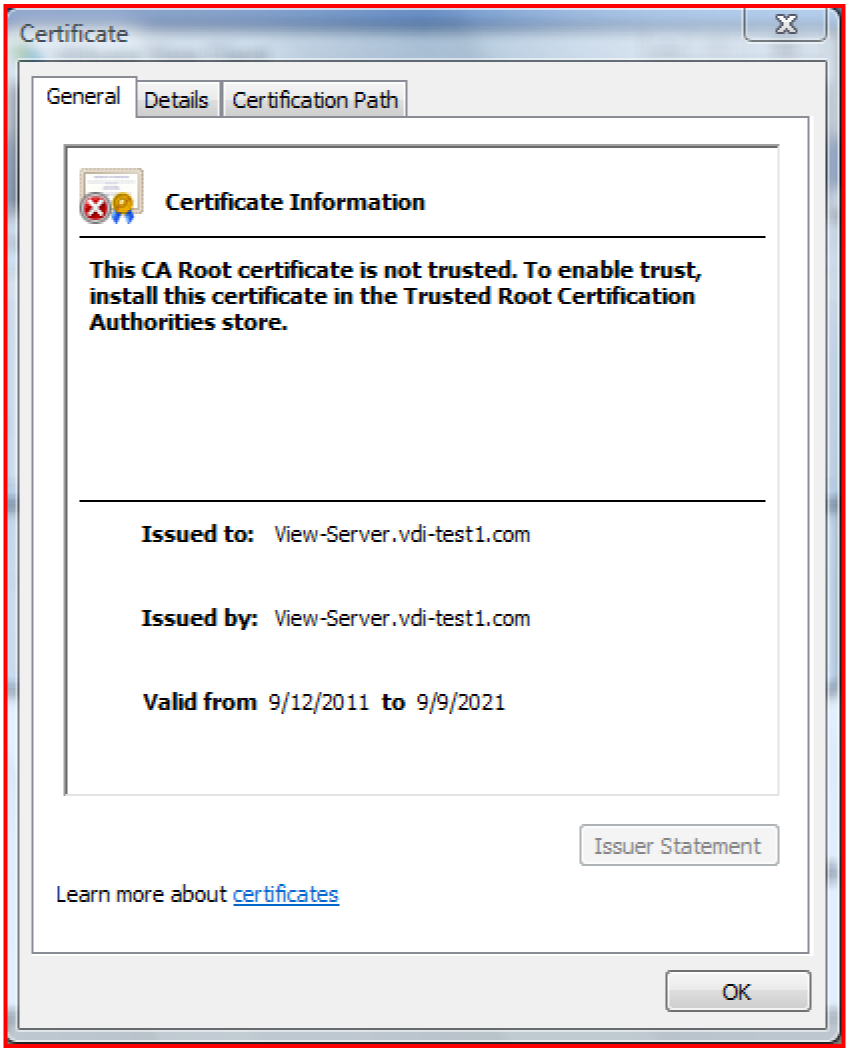
○ Warn if the connection may be insecure (Default)

Warns when unsigned (View default) or expired certificates are encountered.

○ Allow the unverifiable connection (Not Secure)

Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. You should get the "**Failed to connect…..**" error message. Click on "**Show Certificate**" button & verify that it launches the certificate details window as follows.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: View-Server.vdi-test1.com

Issued by: View-Server.vdi-test1.com

Valid from 9/12/2011 **to** 9/9/2021

5. Click **OK** on the message & quit the View Client application

5.7 View:WinClient:SecurityCertificateSetup

Test Purpose

The root certificate is generated, signed & added to the server truststore so that the View Connection Server can authenticate users & permit them to connect to their View desktops.

NOTE: Please note that the certificate that you are installing to the server needs to be issued to the hostname "**view-server.vdi-test1.com**" If the security keystore is not generated or imported properly, you will not be able to pass the subsequent test cases.

Expected Results

Certificate is signed & imported to View Connection Server successfully.

Procedure

1. Please refer to the VMware View Administration guide and the VMware View Installation guide on how to generate, sign & import the root certificate to the View Connection Server.

5.8 View:WinClient:ConnectNotSecureWithCert

Test Purpose

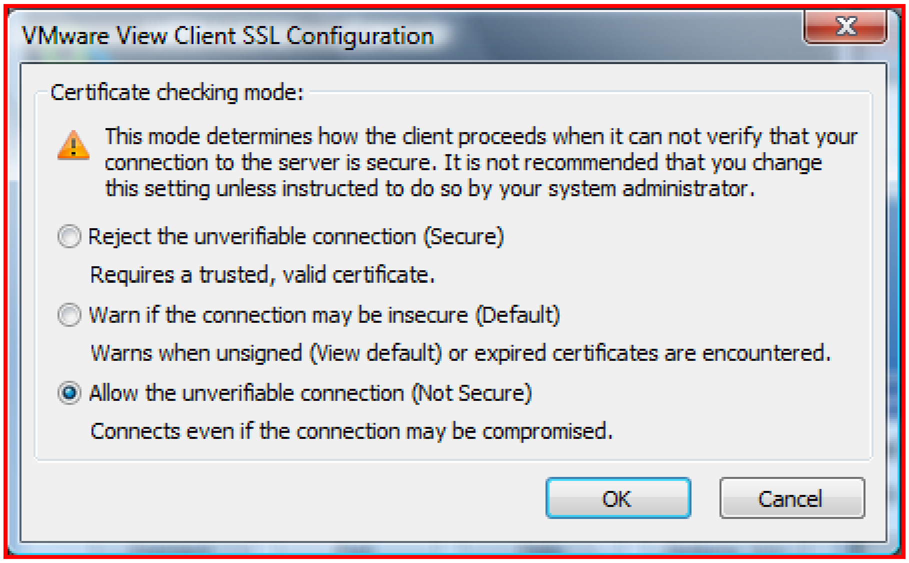
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Click on **Configure SSL.** This should bring up the **VMware View Client SSL Configuration window**. In this window, check "**Allow the unverifiable connection (Not Secure)**" option & click **Ok**



VMware View Client SSL Configuration

Certificate checking mode:

This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)

Requires a trusted, valid certificate.

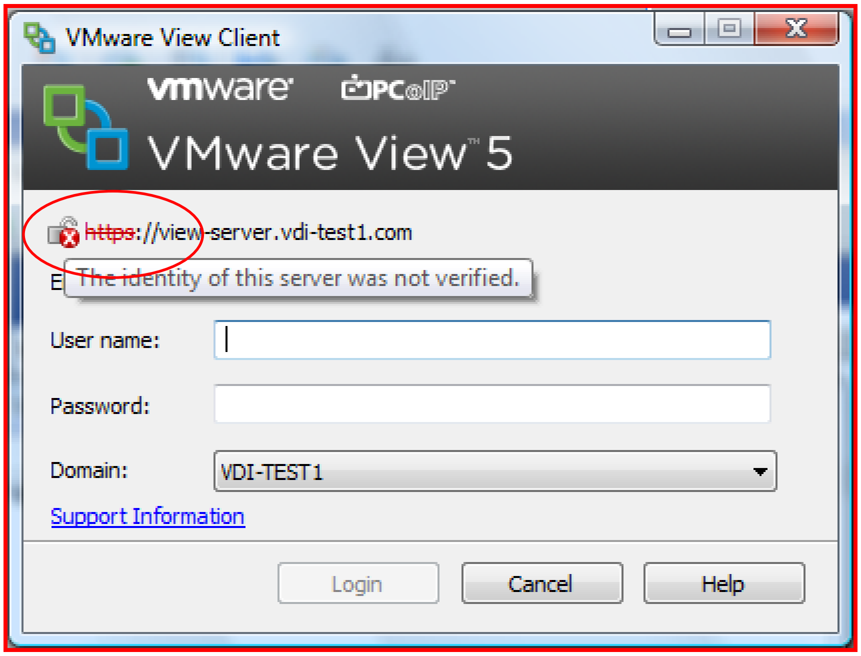
○ Warn if the connection may be insecure (Default)

Warns when unsigned (View default) or expired certificates are encountered.

● Allow the unverifiable connection (Not Secure)

Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are NOT getting any error message & that you are seeing the log-in screen as follows



~~https~~://view-server.vdi-test1.com

The identity of this server was not verified.

User name:

Password:

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Dedicated1** desktop and connect.
8. The user successfully connects to the **Dedicated1** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

5.9 View:WinClient:ConnectDefaultWithCert

Test Purpose

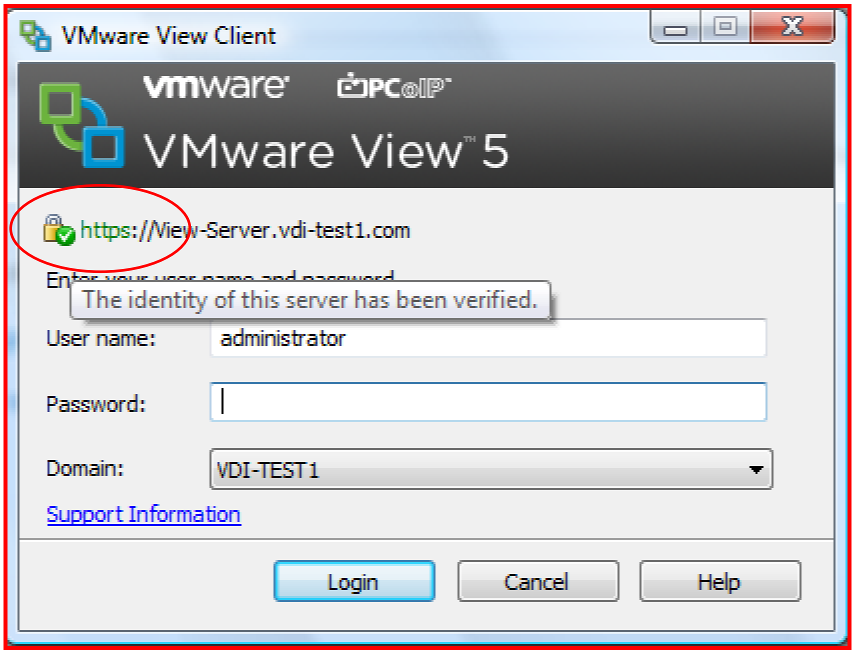
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL security set to default after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Click on **Configure SSL.** This should bring up the **VMware View Client SSL Configuration window**. In this window, check "**Warn if the connection may be insecure (Default)**" option & click **Ok**
3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are not getting any error message & that you are seeing the log-in as follows



https://View-Server.vdi-test1.com

Enter your user name and password

The identity of this server has been verified.

User name: administrator

Password:

Domain: VDI-TEST1

5. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Win7 64-bit** desktop and connect.
8. The user successfully connects to the **Win7 64-bit** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

5.10 View:WinClient:ConnectSecureWithCert

Test Purpose

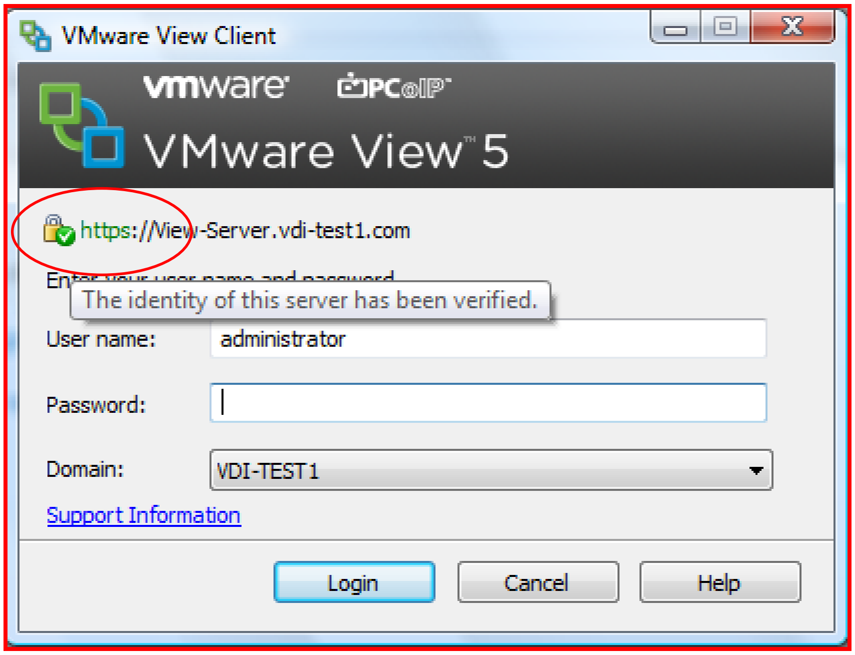
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL security set to full security after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Click on **Configure SSL.** This should bring up the **VMware View Client SSL Configuration window**. In this window, check "**Reject the unverifiable connection (Secure)**" option & click Ok
3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are not getting any error message & that you are seeing the log-in with the green lock icon as follows



https://View-Server.vdi-test1.com

The identity of this server has been verified.

User name: administrator

Password:

Domain: VDI-TEST1

5. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Win7 32-bit** desktop and connect.
8. The user successfully connects to the **Win7 32-bit** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

5.11 View:WinClient:Invalid

Test Purpose

A user with an invalid username or invalid password cannot log into a desktop virtual machine.

Expected Results

An invalid user will not be allowed to log into the desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userinvalid**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log in to the thin client.
4. Launch the View Client and connect to **view-server.vdi-test1.com**.
5. Enter the correct username but incorrect password, select the **vdi-test1.com** domain, and log in.
6. The user authentication should fail, and an error dialog box should appear.
7. Enter the username incorrectly but enter the password correctly, select the **vdi-test1.com** domain, and log in.
8. The user authentication should fail, and an error dialog box should appear.
9. Quit the View Client.

5.12 View:WinClient:DesktopReconnect

Test Purpose

A user can resume a desktop virtual machine session after a View Client disconnect.

Expected Results

The user will resume the previous desktop virtual machine session.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userdisconnect**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **Inventory -> Desktops** and select the **individual1** desktop. Click **More Commands** and choose "Logoff Session" if a user is already logged on.
7. Log in to the thin client.
8. Launch the View Client and connect to **view-server.vdi-test1.com**.
9. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
10. Choose the **individual1** desktop and connect.
11. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
12. Open an Explorer window on the desktop virtual machine.
13. Click **Options > Disconnect** from the View Client menu.
14. Verify that the View Client quits.
15. Launch the View Client and connect to **view-server.vdi-test1.com** again.
16. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
17. Choose the **individual1** desktop and connect.
18. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
19. Verify that the Explorer window is still open on the desktop.
20. Log out of the desktop virtual machine.

5.13 View:WinClient:OSRestart

Test Purpose

A user can restart and shutdown the desktop virtual machine’s operating system using the View Client for Windows.

Expected Results

The user will restart and shutdown the desktop virtual machine’s operating system.

Procedure

1. Log in to the thin client.
2. Launch the View Client and connect to **view-server.vdi-test1.com**.
3. Log in as a **vdi-test1.com** domain Administrator.
4. Choose the **individual2** desktop and connect.
5. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
6. Restart the desktop. Open a command prompt and type:

   ```
   shutdown -r -t 00
   ```

7. Verify that the desktop virtual machine begins the restart process and the View Client disconnects and quits. Wait a few minutes for the desktop to restart.
8. Launch the View Client and connect to **view-server.vdi-test1.com** again.
9. Log in as a **vdi-test1.com** domain Administrator again.
10. Choose the **individual2** desktop and connect.
11. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
12. Shutdown the desktop. Open a command prompt and type:

    ```
    shutdown -s -t 00
    ```

13. Verify that the desktop virtual machine begins the shutdown process and the View Client disconnects and quits. Wait a few minutes for the desktop to shutdown.
14. Launch the View Client and connect to **view-server.vdi-test1.com** again.
15. Log in as a **vdi-test1.com** domain Administrator again.
16. Choose the **individual2** desktop and connect.
17. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
18. Log out of the desktop virtual machine.

5.14 View:WinClient:DesktopUI

Test Purpose

The basic user interface of the View Client for Windows functions correctly.

Expected Results

The basic user interface of the View Client functions correctly.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usergui**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log in to the thin client.
4. Launch the View Client and connect to **view-server.vdi-test1.com**
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop and connect in full screen mode.
7. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
8. Click **Options > Switch Desktop > Other Desktop…** from the View Client menu.
9. Verify that the View Client desktop selector appears.
10. Click **Options > Help** from the View Client menu.
11. Verify that a web browser opens a help page.
12. Click **Options > About VMware View Client** from the View Client Menu.
13. Verify that an informational window about the View Client appears.
14. Toggle the pin icon on the full screen toolbar.
15. Verify that the toolbar slides up and hides itself leaving only a sliver.
16. Mouse over the toolbar sliver.
17. Verify that the toolbar un-hides.
18. Toggle the pin icon on the toolbar.
19. Verify that the toolbar is locked in place.
20. Double-click the toolbar.
21. Verify that the desktop goes into windowed mode.
22. Re-size the window.
23. Verify that the desktop window can be resized.
24. Double-click the window toolbar.
25. Verify that the desktop goes into full screen mode.
26. Click the X in the toolbar and acknowledge quitting View Client.
27. Verify that the View Client disconnects and quits.

5.15 View:WinClient:Keyboard

Test Purpose

The keyboard works correctly in the View Client for Windows.

Expected Results

The keyboard works correctly in the View Client.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userkeyboard**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log in to the thin client.
4. Launch the View Client and connect to **view-server.vdi-test1.com**.
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop and connect.
7. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
8. Launch Notepad and type some text.
9. Verify that the text entry works correctly.
10. Log out of the desktop virtual machine.

5.16 View:WinClient:MinimumMemory

Test Purpose

A valid user can connect to the View Connection Server with the View Client for Windows with a minimum memory configured thin client device.

Expected Results

The user will successfully connect to the View Connection Server.

Procedure

1. Use a thin client configured with the minimum amount of memory that will be available to customers.
2. In the **vdi-test1.com** domain, create a new user with the username “**userminmem**”.
3. Set the password to “**vmware”**, and disable “User must change password at next logon”.
4. Log in to the thin client and launch the View Client.
5. Connect to **view-server.vdi-test1.com** with the View Client.
6. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
7. Choose the **individual2** desktop and connect.
8. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the **individual2** desktop.
10. Quit the View Client.

5.17 View:WinClient:MMRSupport

Test Purpose

Verify that the installation of the View Client for Windows includes support for Wyse Multimedia Redirection (MMR).

NOTE: This particular test is not applicable to WES 7 Thin Client as MMR support is not yet available on View Client 4.5. This failure is acceptable on WES 7 until VMware View supports MMR. Please note this on your submission log when making a certification request.

Expected Results

The View Client supports multimedia redirection.

Procedure

1. Log in to the thin client where View Client for Windows has been installed.
2. Go to **C:\Program Files\VMware\VMware View\Client\bin\**
3. Verify that **MMRClientSrcFilter.dll** is present.
4. Verify that **MMRVCClientDLL.dll** is present.

5.18 View:WinClient:MMRPlayVideo

Test Purpose

The View Client for Windows can play multimedia files in a connected session with MMR.

NOTE: Since MMR support is not yet available on View Client 4.5, video playback will not be as smooth. This failure is acceptable on WES 7. Please note this on your submission log when making a certification request.

Expected Results

The View Client plays multimedia files in a connected session with MMR.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usermmr**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Connect speakers or headphones to the thin client so that you can hear audio output.
4. Log into **vc-terminal** as the Administrator.
5. Launch the VI Client or vSphere Client and connect to **vc-server** as an Administrator.
6. Open a console to the **individual2** virtual machine, log in as **usermmr**, and copy the test multimedia files to the desktop. The following files should be copied: OLYMPICS.MPG, flowergarden320.avi, Damien.wmv, vandread_ep13_op_wm8_ver.wmv, Amazon_350k.wmv, and mediaexample.mp3.
7. Log off the desktop virtual machine.
8. Quit the VI Client or vSphere Client.
9. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
10. Log in to the **View Administrator** as Administrator.
11. Go to **Policies -> Global Policies** and make sure **Multimedia redirection (MMR)** is set to Allow under the View Policies section.
12. Log out of **View Administrator**.
13. Log in to the thin client.
14. Launch the View Client and connect to **view-server.vdi-test1.com**.
15. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
16. Choose the **individual2** desktop and connect.
17. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
18. Open Task Manager and monitor the CPU Usage. When MMR is utilized, CPU usage should hover around 5%.
19. Launch Windows Media Player and complete the setup process if necessary.
20. Play mediaexample.mp3 in Windows Media Player.
21. The audio should stream smoothly from the desktop virtual machine to the thin client's speakers or headphones.

22. Click Pause and the audio should pause.
23. Click Play and the audio should resume.
24. Play OLYMPICS.MPG in Windows Media Player. The playback should be smooth.
25. Click Pause and the video should pause.
26. Click Play and the video should resume.
27. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
28. While the video is playing, rewind and the video should rewind and continue playing without issue.
29. Play flowergarden320.avi in Windows Media Player. The playback should be smooth.
30. Click Pause and the video should pause.
31. Click Play and the video should resume.
32. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
33. While the video is playing, rewind and the video should rewind and continue playing without issue.
34. Play Damien.wmv in Windows Media Player. The playback should be smooth.
35. Click Pause and the video should pause.
36. Click Play and the video should resume.
37. Play vandread_ep13_op_wm8_ver.wmv in Windows Media Player. The playback should be smooth.
38. Click Pause and the video should pause.
39. Click Play and the video should resume.
40. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
41. While the video is playing, rewind and the video should rewind and continue playing without issue.
42. Play Amazon_350k.wmv in Windows Media Player. The playback should be smooth.
43. Click Pause and the video should pause.
44. Click Play and the video should resume.
45. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
46. While the video is playing, rewind and the video should rewind and continue playing without issue.
47. Log out of the View Client.

5.19 View:WinClient:MultiMonitor

Test Purpose

Verify that the View Client will utilize all the displays in a multi-monitor thin client configuration. If the thin client device does not meet the hardware requirements to support multi-monitor, this test case can be skipped.

Expected Results

The View Client will work with a multi-monitor thin client configuration.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usermultimon**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log in to the thin client.
4. Launch the View Client and connect to **view-server.vdi-test1.com**.
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. In the **Display** option, choose **Multimonitor**.
7. Choose the **individual2** desktop and connect.
8. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Verify that the desktop spans across multiple displays.
10. Open an **Explorer window** on the desktop virtual machine.
11. Drag the Explorer window around all the displays and verify that the Explorer window can be seen on all displays.
12. Log out of the desktop virtual machine.

5.20 View:WinClient:USBFlashDrive

Test Purpose

Verify that the View Client on the thin client can use a USB flash drive with the desktop virtual machine.

Expected Results

The View Client on the thin client connects and uses a USB flash drive with the desktop virtual machine.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userusb**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. On the thin client, launch the View Client and connect to **view-server.vdi-test1.com**.
4. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
5. Choose the **individual2** desktop and connect.
6. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
7. Connect a USB flash drive to the thin client device.
8. If USB autoconnect is not set on the View Client, choose Connect USB Device and connect the USB flash drive to the desktop virtual machine.
9. Verify that the USB flash drive is recognized by the desktop virtual machine.
10. Edit and save a notepad file on the desktop.
11. Copy the notepad file to the USB flash drive.
12. Open the notepad file on the USB flash drive and verify the contents.
13. Perform the read & write tests to the flash drive by copying the flowergarden320.avi to and from the USB flash drive.
14. Play the flowergarden320.avi from the USB flash drive. Verify the video plays smoothly and the audio is synced.
15. In the View Client menu bar, disconnect the USB flash drive from the thin client by choosing **Connect USB Device** and unchecking the connected USB flash drive.
16. Unplug & replug the USB flash drive from the thin client while still connecting to the desktop session & ensure that the USB flash drive unmounts & remounts properly (without having to disconnect and reconnect to the desktop sessison).
17. Log out of the desktop virtual machine.
18. Repeat the same tests with Win7 x86 & Win7 x64 virtual desktops.

5.21 View:WinClient:BasicSessionRSASecurID (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RSA SecurID authentication. A valid user can connect to the View Connection Server and an entitled desktop with the View Client using RSA SecurID authentication.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Log into the thin client.
2. Launch the View Client and connect to **view-server.vdi-test1.com**.
3. Provide the username and RSA SecurID token PIN.
4. Provide the user's domain login password.
5. Connect to the **individual2** desktop.
6. The user successfully connects to the **individual2** desktop virtual machine.
7. Log out of the desktop virtual machine.

5.22 View:WinClient:Valid2-FactorAuthentication (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RADIUS 2-Factor Authentication. There are a few different Authentication Managers that VMware View support. Depending on what you have setup, please perform the tests below. A valid user can connect to the View Connection Server and an entitled desktop with the View client using RADIUS 2-Factor Authentication.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Launch the web browser and go to the **View Administrator** portal at https://view-server/admin
2. Log into the **View Administrator** as an Administrator
3. Go to **View Configuration -> Servers.** Click on **Connection Servers** tab and highlight your **View Connection Server** name and select **Edit**. This should bring up the "**Edit View Connection Server Settings**"
4. Select the **Authentication** tab and setup the **Authenticator** but DO NOT enable "**Enforce 2-factor and Windows user name matching" and "Use the same User name and password for RADIUS and Windows Authentication" options**
5. Log into the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Provide the valid username and passcode if you're using **VASCO Authentication Manager** (Note: the passcode consists of PIN & token generated by the Vasco Authentication Manager)

   OR

   Provide AD user name and password, which is imported into **SMSPASSCODE server** if you're using **SMSPASSCODE Authentication Manager**
8. Provide the static passcode is using **SMSPASSCODE Authentication Manger**
9. Provide the user's domain login password
10. Connect to the **individual2** desktop.
11. The user successfully connects to the **individual2** desktop virtual machine.
12. Log out of the desktop virtual machine.

5.23 View:WinClient:AD Matching 2-Factor Authentication (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RADIUS 2-Factor Authentication. There are a few different Authentication Managers that VMware View support. Depending on what you have setup, please perform the tests below. A valid user can connect to the View Connection Server and an entitled desktop with “Enforce 2-Factor and Windows user name matching” option enabled.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Launch the web browser and go to the **View Administrator** portal at https://view-server/admin
2. Log into the **View Administrator** as an Administrator
3. Go to **View Configuration -> Servers.** Click on **Connection Servers** tab and highlight your **View Connection Server** name and select **Edit**. This should bring up the “**Edit View Connection Server Settings**”
4. Select the **Authentication** tab and enable “**Enforce 2-factor and Windows user name matching”** but NOT the **“Use the same User name and password for RADIUS and Windows Authentication” option**
5. Log into the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Provide the valid username and passcode if you are using **VASCO Authentication Manager** (Note: the passcode consists of PIN & token generated by the **VASCO Authentication Manager**)

   OR

   Provide AD user name and password, which is imported into **SMSPASSCODE server** if you’re using **SMSPASSCODE Authentication Manager**
8. Provide the static passcode if you are using **SMSPASSCODE Authentication Manger**
9. Provide the user’s domain login password
10. Connect to the **Win7 x64** desktop.
11. The user successfully connects to the **Win7 x64** desktop virtual machine.
12. Log out of the desktop virtual machine.

5.24 View:WinClient:PCoIPHWRequirements

Test Purpose

Verify that the thin client meets the hardware requirements for utilizing the PCoIP protocol. If the thin client device does not meet the hardware requirements to support the PCoIP protocol, this test case can be skipped.

Expected Results

The thin client meets the hardware requirements for using the PCoIP protocol.

Procedure

1. Verify that the thin client device has an x86 based processor with SSE2 extensions.
2. Verify that the thin client device has a minimum 800 MHz processor.
3. In addition to the RAM requirements for the thin client operating system, the thin client must also have the following additional amount of RAM to support the PCoIP protocol. The amount of additional RAM is determined by the maximum number of displays and the maximum resolution the thin client will support. Please see the table below.

Display Setting	**Width**	**Height**	**Pixels**	**Additional RAM @ 1 Display**	**Rounded Up**	**Additional RAM @ 2 Displays**	**Rounded Up**
VGA	640	480	307200	Not Tested	**N/A**	Not Tested	**N/A**
SVGA	800	600	480000	160 MB	**196 MB**	310 MB	**512 MB**
720p	1280	720	921600	150 MB	**196 MB**	320 MB	**512 MB**
UXGA	1600	1200	1920000	300 MB	**512MB**	380 MB	**512 MB**
1080p	1920	1080	2073600	330 MB	**512 MB**	380 MB	**512 MB**
WUXGA	1920	1200	2304000	330 MB	**512 MB**	380 MB	**512 MB**
QXGA	2048	1536	3145728	350 MB	**512 MB**	440 MB	**512 MB**
WQXGA	2560	1600	4096000	Not Tested	**N/A**	Not Tested	**N/A**

5.25 View:WinClient:PCoIP

Test Purpose

Verify that the thin client can connect to a desktop virtual machine using the View Client and the PCoIP protocol.

NOTES:

- If the thin client device does not meet all the hardware or software requirements to support the PCoIP protocol, this test case can be skipped. The thin client will only be certified for RDP.
- (View 5.0 only) If the thin client memory is 512MB, in order to support 1920x1200 resolution with PCoIP, you need to change the default image cache size from 250MB to 50MB.

However, if the thin client device meets all the requirements to support PCoIP, then it is mandatory to support PCoIP.

Expected Results

The thin client will connect to a desktop virtual machine using the PCoIP protocol.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userpcoip**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log in to the thin client.
4. Launch the View Client and connect to **view-server.vdi-test1.com**.
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop.
7. Choose PCoIP as the Display Protocol and connect to the desktop.
8. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Verify that the desktop VM’s display resolution is automatically adjusted to match the thin client device’s display resolution.
10. Log out of the desktop virtual machine.

5.26 View:WinClient:PCoIPMiniClientImageCacheSize

Test Purpose

The default image cache size is set at 250MB. This test is to ensure that when the variable is changed to the minimum of 50MB, performance is still good. It should still work with good user experience.

Expected Results

With direct connection between Client & Agent using PCoIP, video playing is still smooth. Users should not experience any image crashing.

Procedure

1. Copy the pcoip.admin from your View Conneciton Server (**<install_directory>\VMware\VMware View\Server\extras\GroupPolicyFiles\pcoip.admin>**) to your thin client
2. On your thin client system, run **gpedit.msc**. This should launch the **Local Group Policy Editor** window
3. Under **Computer Configuration**, right click on **Administrative Templates** & select **Add/Remove Templates**
4. Click **Add** & select the **pcoip.admin** then close out of this window
5. Go to **Computer Configuration** -> **Administrative Templates** -> select **Classic Administrtive Templates (ADM)** -> **PCoIP Session Variables** -> **Overridable Administrator Defaults,** set the value of "**Configure PCoIP client image cache size policy**" to 50MB
6. Click **Apply** and **OK** to close out of this window
7. Launch the **View Client** application & connect to **view-server.vdi-test1.com**
8. Select **PCoIP Protocol** and connect to **Win7x86** desktop
9. Play a video file. As the video is playing, move back & forth the screen. Video playing should be smooth with no image crashing.

5.27 View:WinClient:PCoIPMaxClientImageCacheSize

Test Purpose

The default image cache size is set at 250MB. This test is to ensure that when the variable is changed to the max of 300 MB, performance is still good. It should still work with good user experience.

Expected Results

With direct connection between Client & Agent using PCoIP, video playing is still smooth. Users should not experience any image crashing.

Procedure

1. Copy the pcoip.admin from your View Conneciton Server (**<install_directory>\VMware\VMware View\Server\extras\GroupPolicyFiles\pcoip.admin>**) to your thin client
2. On your thin client system, run **gpedit.msc**. This should launch the **Local Group Policy Editor** window
3. Under **Computer Configuration,** right click on **Administrative Templates** & select **Add/Remove Templates**
4. Click **Add** & select the **pcoip.admin** then close out of this window
5. Go to **Computer Configuration** -> **Administrative Templates** -> select **Classic Administrtive Templates (ADM)** -> **PCoIP Session Variables** -> **Overridable Administrator Defaults,** set the value of "**Configure PCoIP client image cache size policy**" to 300MB
6. Click **Apply** and **OK** to close out of this window
7. Launch the **View Client** application & connect to **view-server.vdi-test1.com**
8. Select **PCoIP Protocol** and connect to **Win7x64** desktop
9. Play a video file. As the video is playing, move back & forth the screen. Video playing should be smooth with no image crashing.

5.28 View:WinClient:BasicSessionSmartCard (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. A valid user can connect to the View Connection Server and an entitled desktop with the View Client using Smart Card authentication with both the RDP and PCoIP protocol.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usersmartcard**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Install the Smart Card reader on the thin client along with the necessary drivers and libraries. Refer to the documentation that accompanies the Smart Card reader for information about how to do this.
4. Set up the Active Directory server and View Connection Server to support Smart Card authentication for the "**usersmartcard"** user. Refer to the "Smart Card Authentication" section of the ***VMware View Manager Administration Guide*** for more information about how to do this at http://www.vmware.com/support/pubs/view_pubs.html.
5. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
6. Log in to the **View Administrator** as Administrator.
7. Go to **View Configuration -> Servers,** highlight **view-server** and click **Edit.** On the **Authentication** tab, verify that **Smart card authentication** is set to Optional or Required.
8. Log out of **View Administrator**.
9. Log into the thin client.
10. Plug the Smart Card into the Smart Card reader.
11. Launch the View Client and connect to **view-server.vdi-test1.com**.
12. Provide the Smart Card PIN.
13. Connect to the **individual2** desktop with the RDP protocol.
14. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS with no additional authentication.
15. Log out of the desktop session.
16. Repeat logging into the **individual2** desktop with the Smart Card and the PCoIP protocol.
17. Log out of the desktop session.
18. Log off the thin client.

5.29 View:WinClient:TripleSSO

Test Purpose

Verify that a domain user can connect to the thin client, View Connection Server, and the desktop virtual machine with a single domain sign on.

Expected Results

A domain user can connect to the thin client, View Connection Server, and the desktop virtual machine with a single domain sign on.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usertriplesso**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. As the thin client administrator, join the thin client to the vdi-test1 domain. The thin client must be a member of the domain in order to utilize Triple SSO.
4. Log in to the thin client as the domain user **usertriplesso**.
5. Launch the View Client and connect to **view-server.vdi-test1.com**. Make sure “**Log in as current user: VDI-TEST1\usertriplesso**” is checked.
6. Verify that the View Client automatically authenticates with the View Connection Server using the thin client user credentials.
7. Choose the **individual2** desktop.
8. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Remove the thin client from membership in the domain.
11. Log out of the thin client.

5.30 View:WinClient:UPNTripleSSO

Test Purpose

Verify that a domain user can connect to the thin client, View Connection Server, and the desktop virtual machine with a UPN (User Principal Name) and single sign on.

Expected Results

A domain user can connect to the thin client, View Connection Server, and the desktop virtual machine with a UPN and single sign on.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userupn**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. As the thin client administrator, join the thin client to the vdi-test1 domain. The thin client must be a member of the domain in order to utilize UPN.
4. Log into **services-server** as the Administrator.
5. Choose **Start > Manage Your Server > Manage domains and trusts**.
6. Right-click **Active Directory Domains and Trusts** and choose **Properties**.
7. Add **vdi.int** as an alternative UPN suffix and click **OK**.
8. Choose **Start > Manage Your Server > Manage users and computers in Active Directory.**
9. Right-click **userupn** and choose **Properties**.
10. Choose **Account**, change the User logon name suffix to vdi.int, and click **OK**.
11. Log out of **services-server**.
12. Log in to the thin client with the UPN userupn@vdi.int and provide the password. The domain field should automatically gray out.
13. Launch the View Client and connect to **view-server.vdi-test1.com**. Make sure "**Log in as current user**" is checked.
14. Verify that the View Client automatically authenticates with the View Connection Server using the thin client user credentials.
15. Choose the **individual2** desktop.
16. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
17. Log out of the desktop virtual machine.
18. Remove the thin client from membership in the domain.
19. Log out of the thin client.

5.31 View:WinClient:SmartCardTripleSSO (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. Verify that a domain user can connect to the thin client, View Connection Server, and the desktop virtual machine with a single Smart Card sign on.

Expected Results

A Smart Card user can connect to the thin client, View Connection Server, and the desktop virtual machine with a single sign on.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userscsso**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. As the thin client administrator, join the thin client to the vdi-test1 domain. The thin client must be a member of the domain in order to utilize Triple SSO.
4. Set up the thin client and user for Smart Card authentication in the vdi-test1.com domain.
5. Log in to the thin client using Smart Card authentication. Provide the Smart Card PIN if necessary.
6. Launch the View Client and connect to **view-server.vdi-test1.com**. Make sure "**Log in as current user: VDI-TEST1\userscsso**" is checked.
7. Verify that the View Client automatically authenticates with the View Connection Server.
8. Choose the **individual2** desktop.
9. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
10. Log out of the desktop virtual machine.
11. Remove the thin client from membership in the domain.
12. Log out of the thin client.

5.32 View:WinClient:SmartCardRemovalPolicy (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. Verify that a Smart Card authenticated user is automatically logged off of a desktop virtual machine when the Smart Card is removed.

Expected Results

A Smart Card authenticated user will automatically be forced to log off of a desktop virtual machine when the Smart Card is removed. At the next login, the user will start a new session instead of continuing the previous session.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userscremoval**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Servers,** highlight **view-server** and click **Edit.** In the **Authentication** tab, verify that **Disconnect user sessions on smart card removal** is enabled.
7. Log out of **View Administrator**.
8. Set up the thin client and user for Smart Card authentication in the vdi-test1.com domain.
9. Log in to the thin client.
10. Insert the Smart Card.
11. Launch the View Client and connect to **view-server.vdi-test1.com**. Provide the login PIN if necessary.
12. Choose the **individual2** desktop.
13. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
14. Remove the Smart Card from the Smart Card reader.
15. Verify that the user is disconnected from the desktop virtual machine session.
16. Log out of the thin client.

5.33 View:WinClient:TimezoneRedirection

Test Purpose

The VMware View Client for Windows can forward the thin client's time zone setting to the desktop virtual machine.

Expected Results

The desktop virtual machine will have the same time zone setting as the thin client running the VMware View Client for Windows.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usertimezone**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into **vc-terminal** as the Administrator.
4. Launch the VI Client or vSphere Client.
5. Connect to **vc-server** and provide the Administrator credentials.
6. Open a console to the **individual2** desktop and log in as the Domain Administrator.
7. Set the time zone to US Pacific time.
8. Log out of the **individual2** desktop.
9. Quit the VI Client or vSphere Client.
10. Log into the thin client as a user with Administrator privileges.
11. Set the time zone to US Eastern time on the thin client.
12. Log out of the thin client.
13. Log back into the thin client as a non-Administrator.
14. Launch the VMware View Client for Windows and connect to **view-server.vdi-test1.com.**
15. Enter the **usertimezone** credentials, select the **vdi-test1.com** domain, and log in.
16. Choose the **individual2** desktop and connect.
17. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
18. Verify that the desktop virtual machine's time zone is automatically set to US Eastern time to match the thin client.
19. Log out of the **individual2** desktop.
20. Quit the View Client.

5.34 View:WinClient:PCoIPCopyAndPaste

Test Purpose

Verify that the thin client device's operating system can copy and paste text to the desktop session via the View Client for Windows using the PCoIP protocol.

Expected Results

The thin client device's operating system can copy and paste text to the desktop session via the View Client for Windows using the PCoIP protocol.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usercopypaste**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into the thin client.
4. On the thin client, open a web browser or a text file.
5. Highlight some text with the mouse, click the right mouse button, and choose **Copy**.
6. Launch the VMware View Client for Windows and connect to **view-server.vdi-test1.com.**
7. Enter the **usercopypaste** credentials, select the **vdi-test1.com** domain, and log in.
8. Choose the **individual2** desktop and connect with the PCoIP Display Protocol.
9. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
10. In the desktop session, create a new text document with Wordpad.
11. In the Wordpad window, click the right mouse button and choose **Paste**.
12. Verify that the text is copied correctly from the thin client to the desktop session.
13. Quit Wordpad.
14. Log out of the **individual2** desktop.
15. Quit the View Client.

5.35 View:WinClient:KioskMode (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support the View client's kiosk mode. Verify that the thin client can function in Kiosk Mode with the View Client for Windows and the View Connection Server. For more detailed information about Kiosk Mode requirements, please see the Kiosk Mode whitepaper available as an addendum to the end of this document.

Expected Results

The thin client functions in Kiosk Mode with the View Client for Windows and the View Connection Server.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**kioskadmin**". Make this user a member of the **Account Operators** group in the domain.
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Administrators** and create a new administrator role called "**Kiosk_Admin**". Give this new role **Direct Interaction** and **View Configuration and Global Policies** privileges.
7. Add the "**kioskadmin**" user as a View administrator with the **Kiosk_Admin** role.
8. Log into the thin client device with the View Client installed and open a new Windows command prompt. Go to **C:\Program Files\VMware\VMware View\Client\bin\** and execute the following command:

   ```
   wswc.exe –printEnvironmentInfo
   ```

   Note the MAC address of the thin client. The MAC address of the thin client will be used to identify it with the View Connection Server during Kiosk Mode login.
9. Log into **vc-terminal** as the Administrator.
10. Launch the VI Client or vSphere Client.
11. Connect to **vc-server** and provide the Administrator credentials.
12. Open a console to the **view-server** and log in as "kioskadmin".
13. Enable Kiosk Mode on the View Connection Server. Open a new Windows command prompt and go to **C:\Program Files\VMware\VMware View\Server\tools\bin\** and execute the following command:

   ```
   vdmadmin.exe –Q –enable –s view-server
   ```

   Verify that kiosk mode is enabled. Execute:

   ```
   vdmadmin.exe –Q –clientauth –list
   ```

   For **view-server**, the **Client Authentication Enabled** field should be true.

14. Add the thin client to the View Connection Server as a kiosk. At the **view-server** command prompt, go to **C:\Program Files\VMware\VMware View\Server\tools\bin\** and execute the following command:

    ```
    vdmadmin.exe –Q –clientauth –add –domain vdi-test1.com –clientid <THIN_CLIENT_MAC_ADDRESS> -genpassword –description “Windows kiosk user”
    ```

    Verify that the thin client was added as a kiosk. At the command prompt, execute:

    ```
    vdmadmin.exe –Q –clientauth –list
    ```

    The **Client Authentication User List** should contain a **clientID** with the thin client’s MAC address.

15. Log back into the thin client and execute the View client in Kiosk Mode. Open a new Windows command prompt and go to **C:\Program Files\VMware\VMware View\Client\bin\** and execute the following command:

    ```
    wswc.exe –unattended –serverURL view-server.vdi-test1.com
    ```

    The thin client should automatically connect to the View Connection Server and log into a desktop entitled to all domain users without any user intervention.

16. Log out of the entitled desktop and quit the View client.

5.36 View:WinClient:UIGuidelines

Test Purpose

Verify that the thin client conforms to VMware's user interface guidelines for running the View Client for Windows.

Expected Results

The thin client conforms to VMware's user interface guidelines for running the View Client for Windows.

Procedure

1. Verify that an Administrative user can launch the View Client without use of the '`-nonInteractive`' commandline option. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which '`-nonInteractive`' mode is not used. From the Windows command prompt, go to C:\Program Files\VMware\VMware View\Client\bin\ and execute this command:

   ```
   wswc.exe
   ```

   The View Client should launch without any issues.

2. Verify that an Administrative user can launch the View Client with custom options provided via the commandline, options file, and registry property. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which custom options can be supplied. The list of commandline options can be viewed by executing '`wswc.exe /?`'. The user must be able to supply all the custom options that the View Client supports. From the Windows command prompt, go to C:\Program Files\VMware\VMware View\Client\bin\ and execute this command:

   ```
   wswc.exe –nonInteractive –serverURL view-server.vdi-test1.com –username
   usercopypaste –password vmware –domainName vdi-test1 –desktopProtocol
   rdp –desktopName win7_64
   ```

   The View Client should launch and connect to the win7_64 desktop without interaction from the user or error messaging of any kind.

6. VMware View Client for Linux Test Cases

Use the following test cases to certify a Linux thin client running the VMware View Client for Linux. As each test case runs and passes, mark the results in the *Linux View Client* checklist. The *Linux View Client* checklist will be submitted to VMware as part of the thin client certification submission.

6.1 View:LnxClient:SWRequirements

Test Purpose

Verify that the thin client's Linux operating system meets the software requirements for the VMware View Client for Linux.

Expected Results

The thin client's OS meets the software requirements for VMware View Client for Linux.

Procedure

1. Log into the thin client.
2. Verify that the Linux OS has the following components required by the View Client for Linux:

Required Version	Libraries
glibc 2.x	libc.so.6, libdl.so.2
gcc 3.4.x	libstdc++.so.6, libgcc_s.so.1
glib 2.22	libglib-2.0.so.0, libgobject-2.0.so.0
gtk+ 2.18	libgtk-x11-2.0.so.0, libgdk-x11.2.0.so.0, libgdk_pixbuf-2.0.so.0
libpng 1.2.x	libpng12.so.0
openssl 0.9.8	libssl.so.0.9.8, libcrypto.so.0.9.8
libxml 2.6.x	libxml2.so.2
zlib 1.2.3	libz.so.1

   rdesktop 1.4.x or higher

   rdesktop 1.5.x or higher to connect to a Microsoft Windows Vista desktop or to support Wyse MMR

3. If the thin client will support multiple monitors, the Xinerama extension to the X Window System must be enabled with more than one display defined. The thin client must also run a window manager that supports the _NET_WM_FULLSCREEN_MONITORS window manager protocol defined in freedesktop.org's Extended Window Manager Hints.

6.2 View:LnxClient:SetupNetworking

Test Purpose

Verify that the Linux thin client can connect to the View thin client certification environment.

Expected Results

The thin client connects to the View thin client certification environment.

Procedure

1. Connect the thin client to the View thin client certification network switch.
2. Log into the thin client as a user without root privileges.
3. Verify that the thin client has a valid IP address.

6.3 *View:LnxClient:ConnectSSLDefault*

Test Purpose

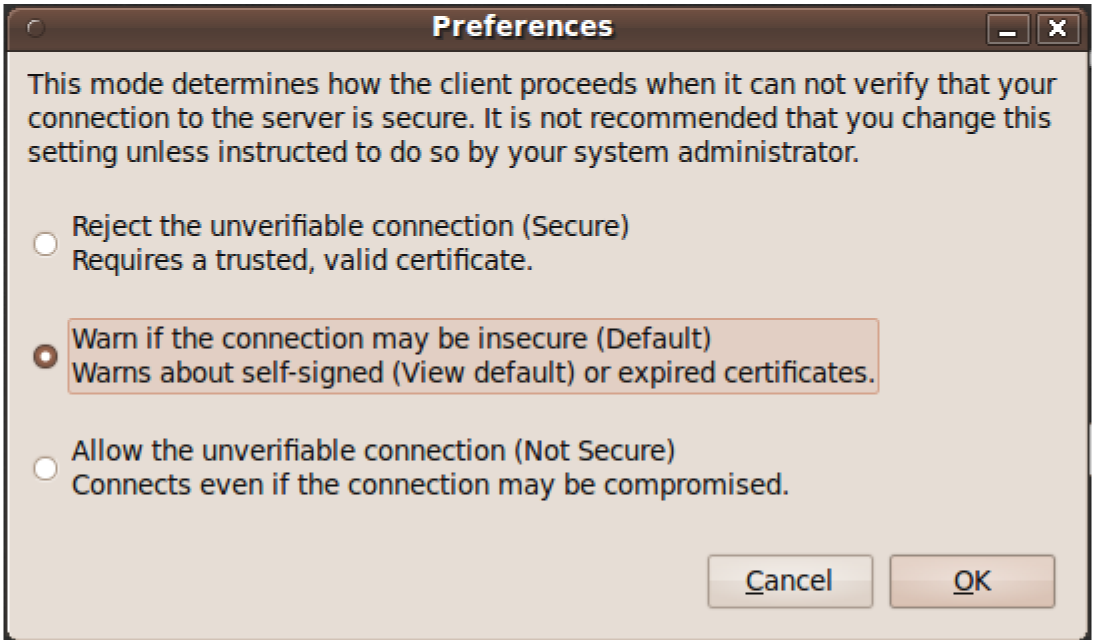
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL default security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userssl**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Global Settings** and make sure **Use SSL for client connections** is enabled.
7. Log into **view-server** as the Administrator.
8. Restart the View Connection Server service.
9. Log in to the thin client and launch the View Client.
10. Under the **File menu** -> **Preferences**, make sure “**Warn if the connection may be insecure**” is checked



This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

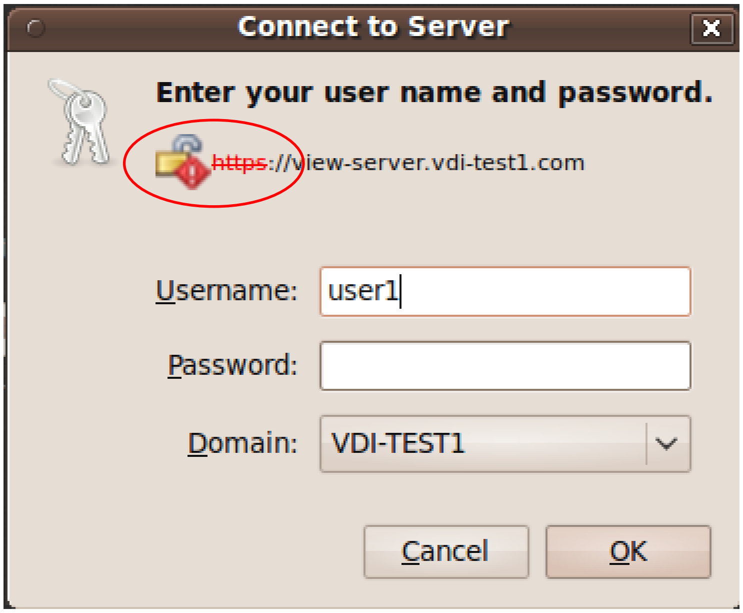
○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

● Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

11. Connect to **view-server.vdi-test1.com** with the View Client.
12. You should get a prompt indicating that the View cannot verify the identity of the server. Choosing to “**Connect Insecurely**” should allow you to proceed with the username & password log-in screen.

13. Make sure the dialog shows the **orange unlocked icon** as shown below



Connect to Server
Enter your user name and password.
~~https~~://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

14. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
15. Verify that the desktop selector dialog box appears.
16. Choose the **individual1** desktop and connect.
17. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
18. Log out of the desktop virtual machine.
19. Quit the View Client.

6.4 View:LnxClient:ConnectSSLNotSecure

Test Purpose

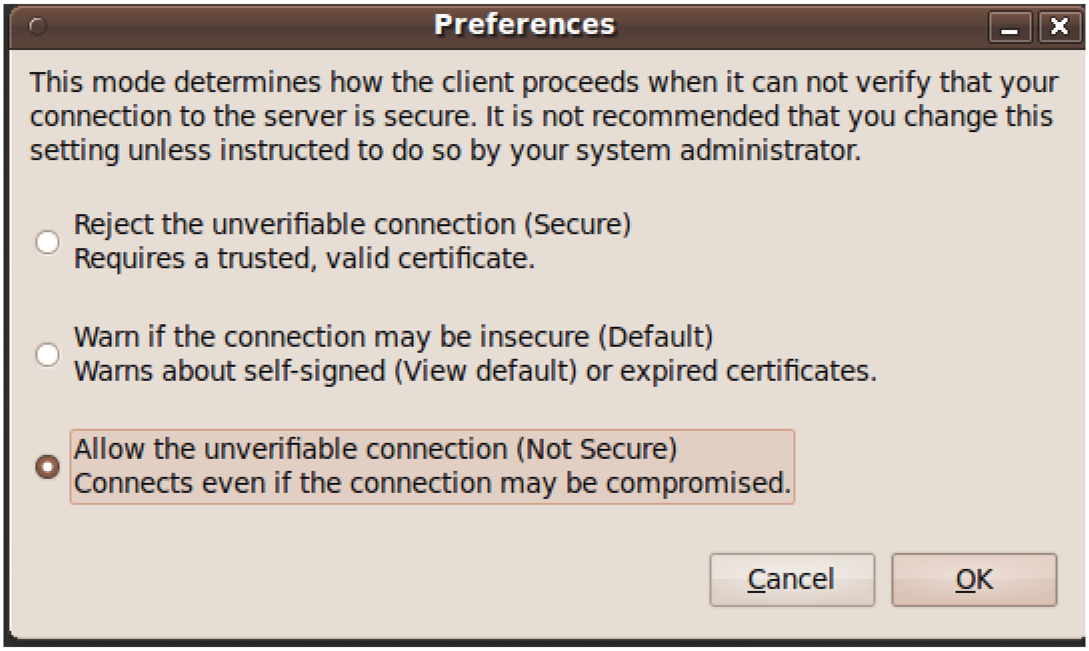
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop without any security check.

Procedure

1. Log in to the thin client and launch the View Client.
2. Under the **File menu** -> **Preferences**, make sure "**Allow the unverifiable connection (Not Secure)**" is checked



This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

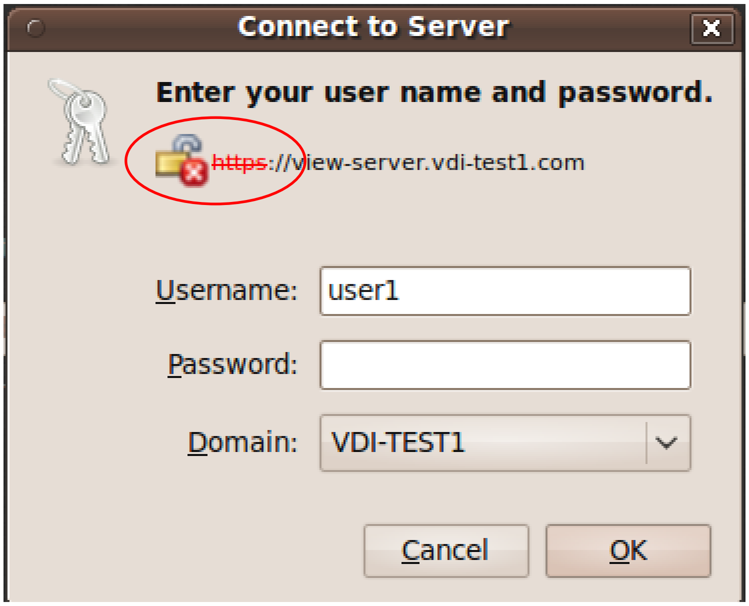
○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

● Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.

4. Please verify that you are seeing the log-in screen as follows


Connect to Server
Enter your user name and password.
~~https~~://view-server.vdi-test1.com
Username:
user1
Password:
Domain:
VDI-TEST1
Cancel
OK

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Individual2** desktop and connect.
8. The user successfully connects to the **Individual2** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

6.5 *View:LnxClient:ConnectSSLSecure*

Test Purpose

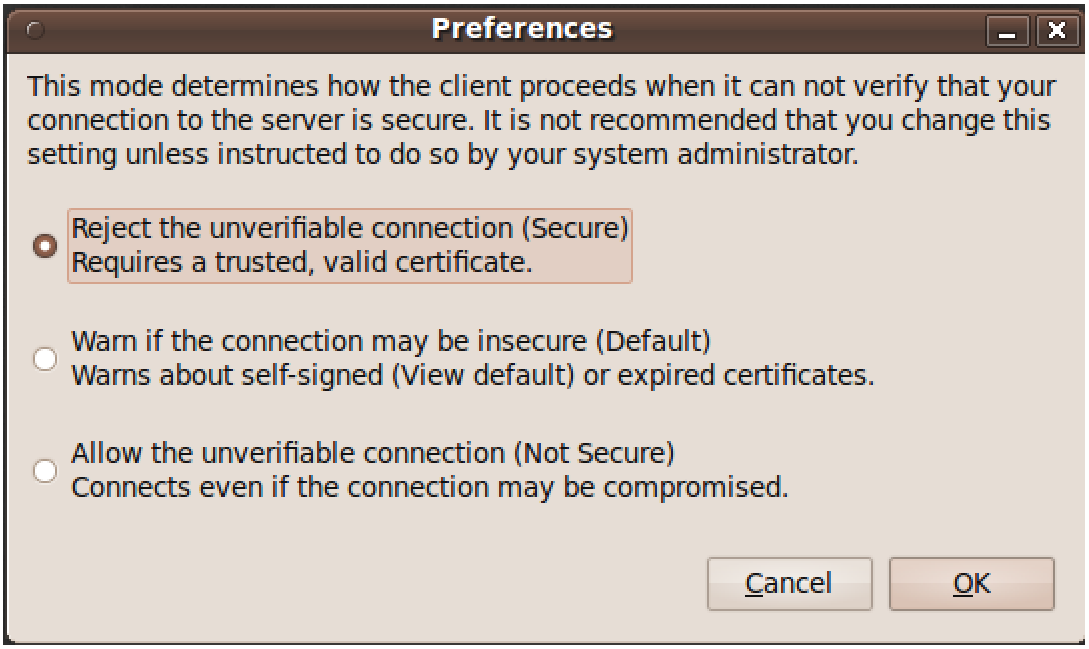
An attempt to connect to the View Connection Server without a valid certificate should result in an error.

Expected Results

Connection to View Server should fail.

Procedure

1. Log in to the thin client and launch the View Client.
2. Under the **File menu** -> **Preferences**, make sure “**Reject the unverifiable connection (Secure)**” is checked



Preferences

This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

● Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. You should get “the certificate authority is invalid or incorrect” error message as the valid certificate is not yet installed.
5. Quit the View Client application

6.6 View:LnxClient:SecurityCertificateSetup

Test Purpose

The root certificate is generated, signed & added to the server truststore so that the View Connection Server can authenticate users & permit them to connect to their View desktops.

NOTE: Please note that the certificate that you are installing to the server needs to be issued to the hostname “**view-server.vdi-test1.com**” If the security keystore is not generated or imported properly, you will not be able to pass the subsequent test cases.

Expected Results

Certificate is signed & imported to View Connection Server successfully.

Procedure

1. Please refer to the **VMware View Administration guide** and the **VMware View Installation guide** on how to generate, sign & import the root certificate to the View Connection Server

6.7 View:LnxClient:ConnectNotSecureWithCert

Test Purpose

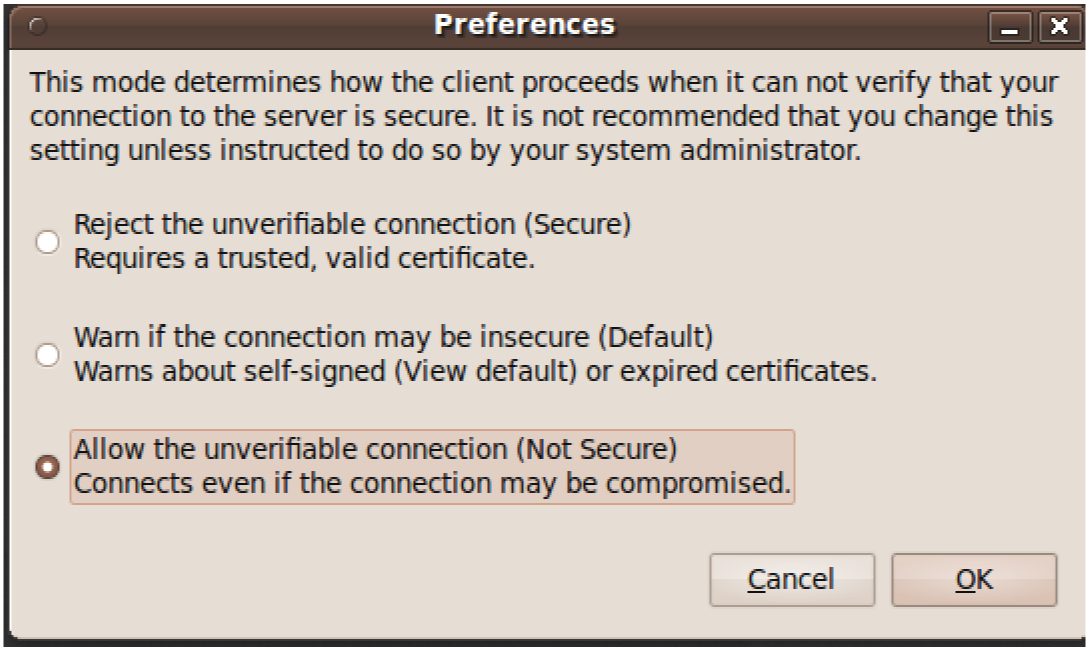
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL Not Secure security setting after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Under the **File menu** -> **Preferences**, make sure “**Allow the unverifiable connection (Not Secure)**” is checked



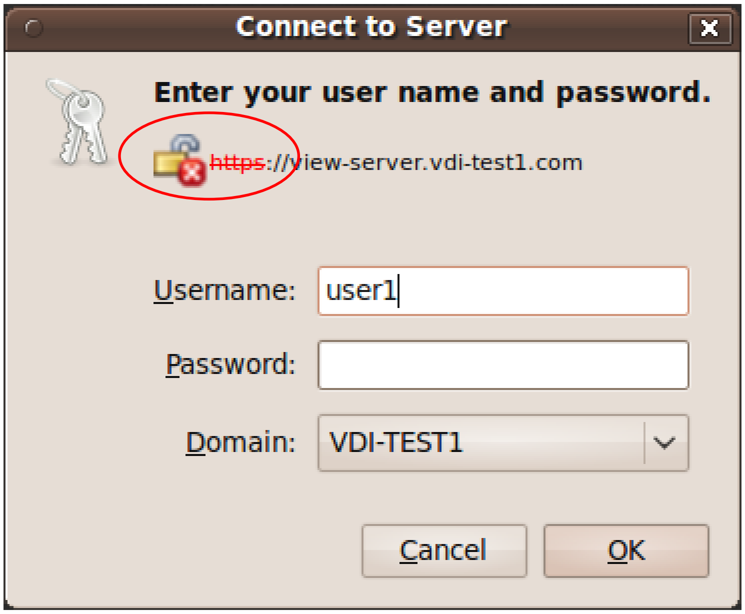
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

● Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are NOT getting any error message & that you are seeing the log-in screen as follows



Enter your user name and password.

~~https~~://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Dedicated1** desktop and connect.
8. The user successfully connects to the **Dedicated1** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

6.8 View:LnxClient:ConnectDefaultWithCert

Test Purpose

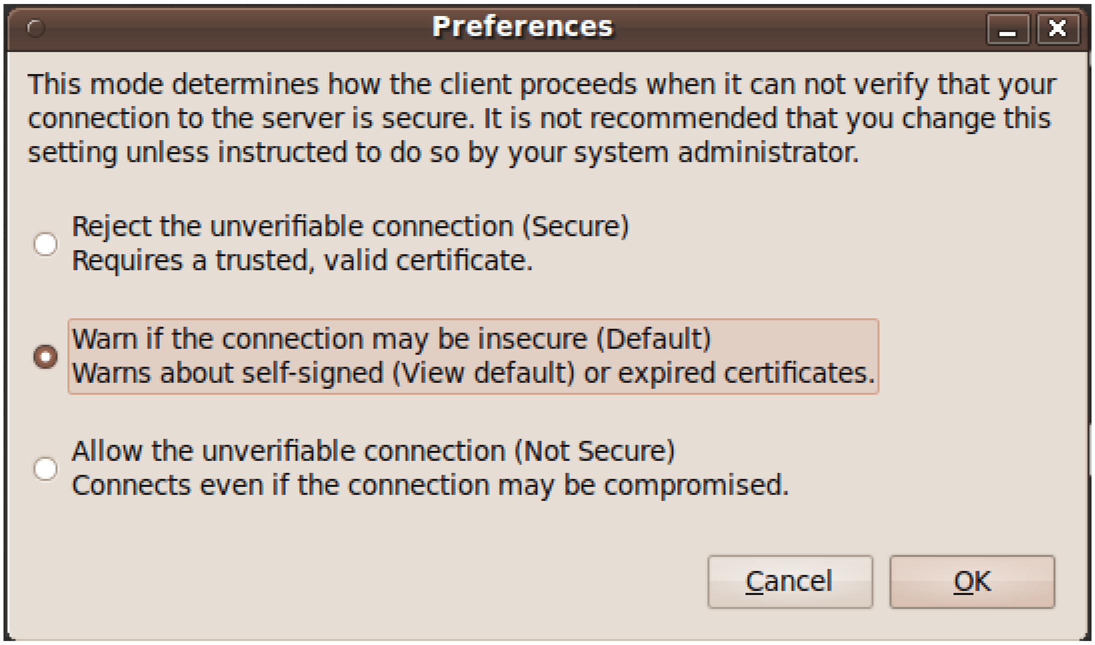
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL security set to default after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Under the **File menu** -> **Preferences**, make sure “**Warn if the connection may be insecure**” is checked



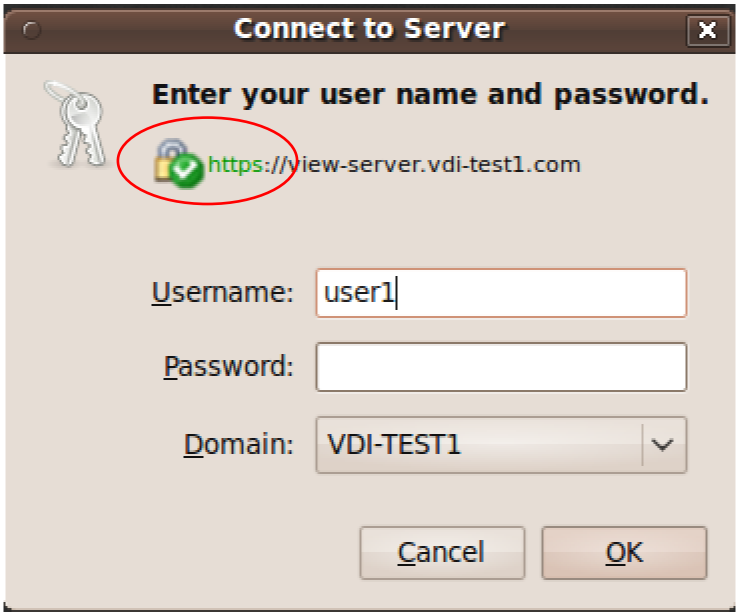
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

● Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are not getting any error message and that you are seeing the log-in as follows



Connect to Server

Enter your user name and password.

https://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Win7 64-bit** desktop and connect.
8. The user successfully connects to the **Win7 64-bit** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

6.9 View:LnxClient:ConnectSecureWithCert

Test Purpose

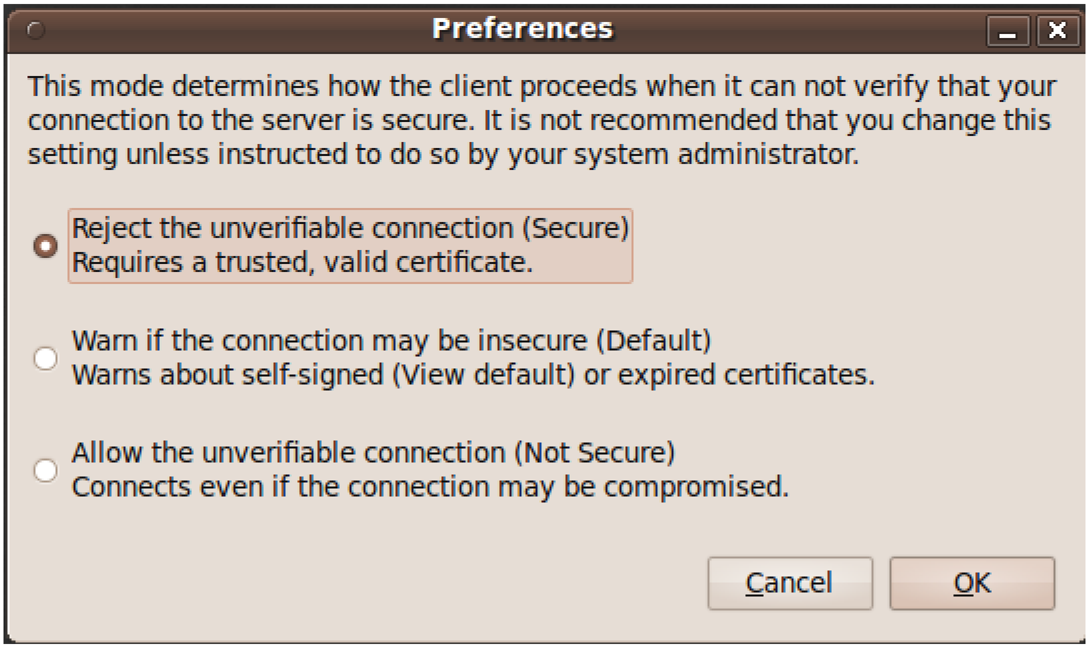
A valid user can connect to the View Connection Server and a remote desktop with the View Client using SSL security set to full security after importing the certificate.

Expected Results

The user will successfully connect to the View Connection Server and a remote desktop.

Procedure

1. Log in to the thin client and launch the View Client.
2. Under the **File menu** -> **Preferences**, make sure “**Reject the unverifiable connection (Secure)**” is checked



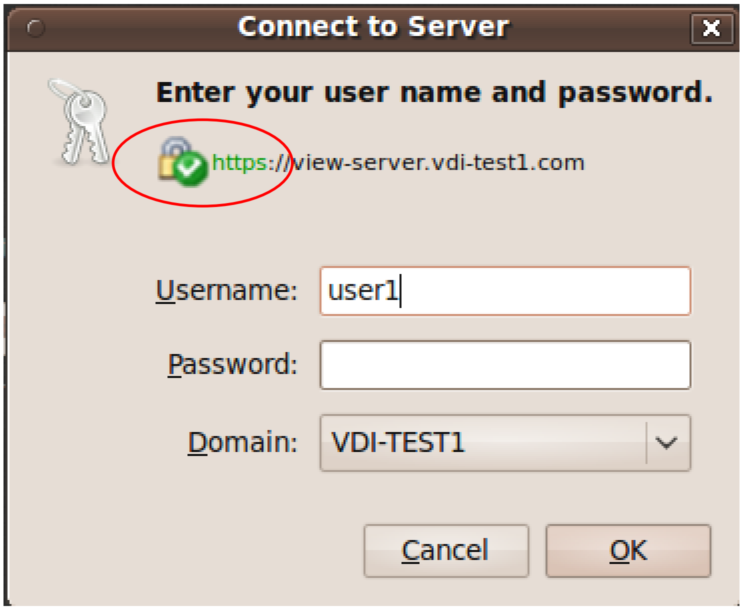
This mode determines how the client proceeds when it can not verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

● Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

○ Warn if the connection may be insecure (Default)
Warns about self-signed (View default) or expired certificates.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

3. Connect to **view-server.vdi-test1.com** with the View Client.
4. Please verify that you are not getting any error message & that you are seeing the log-in with the **green lock icon** as follows



Enter your user name and password.

https://view-server.vdi-test1.com

Username: user1

Password:

Domain: VDI-TEST1

5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Verify that the desktop selector dialog box appears.
7. Choose the **Win7 32-bit** desktop and connect.
8. The user successfully connects to the **Win7 32-bit** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the desktop virtual machine.
10. Quit the View Client.

6.10 View:LnxClient:Non-SSLNotSupported

Test Purpose

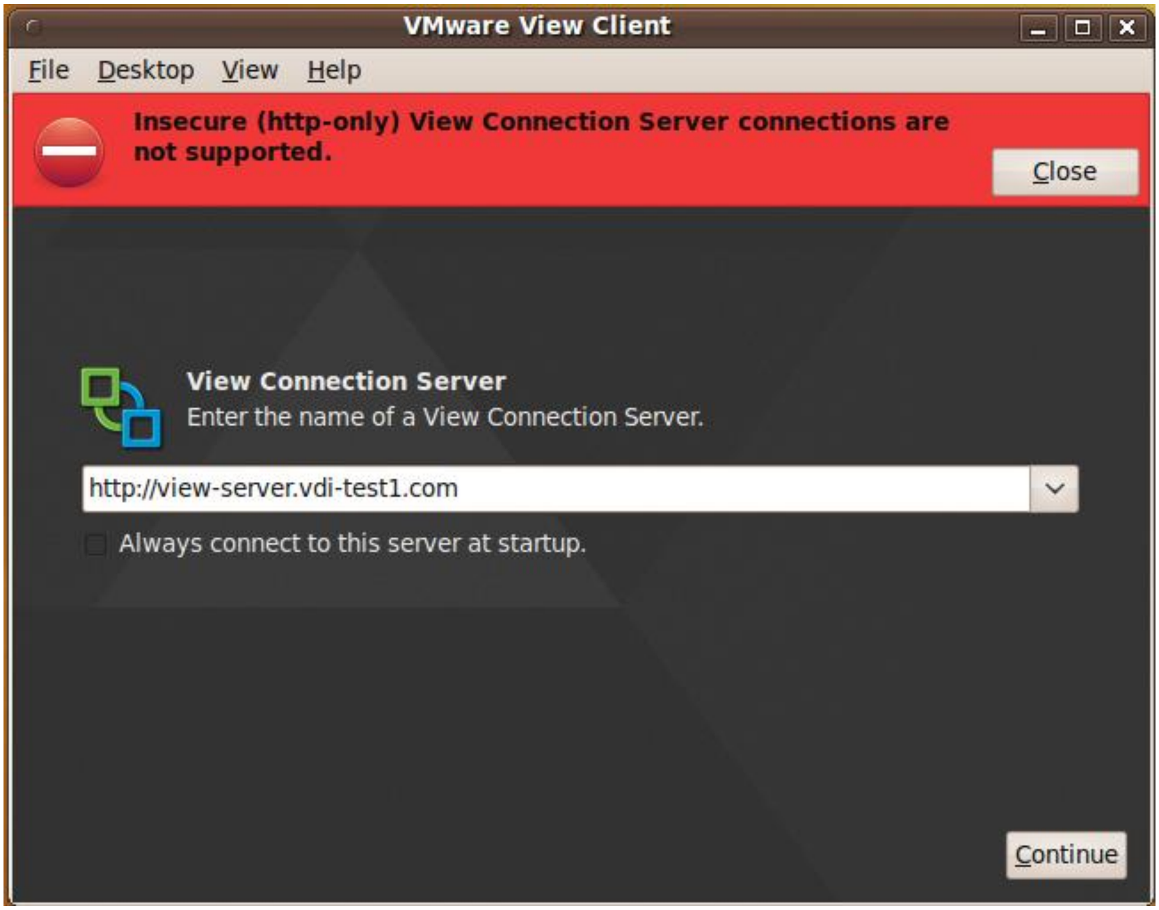
View Client fails to connect to View Connection Server in non-SSL mode

Expected Results

The user should be prompted that non-SSL (http-only) mode is not supported

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to http://view-server.vdi-test1.com
3. Connection attempt should fail & user should get the error message **“Insecure (http-only) View Connection Server connections are not supported.”**



Insecure (http-only) View Connection Server connections are not supported.

View Connection Server

Enter the name of a View Connection Server.

http://view-server.vdi-test1.com

☐ Always connect to this server at startup.

6.11 View:LnxClient:Invalid

Test Purpose

A user with an invalid username or invalid password cannot log into an entitled desktop virtual machine with the View Client for Linux.

Expected Results

An invalid user will not be allowed to log into the entitled desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userinvalid**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
5. Enter the correct username but incorrect password, select the **vdi-test1.com** domain, and log in.
6. The user authentication should fail, and an error dialog box should appear.
7. Quit the View Client for Linux.
8. Launch the View Client for Linux again and connect to **view-server.vdi-test1.com**.
9. Enter the username incorrectly but enter the password correctly, select the **vdi-test1.com** domain, and log in.
10. The user authentication should fail, and an error dialog box should appear.
11. Quit the View Client for Linux.

6.12 View:LnxClient:ConnectFullscreen

Test Purpose

A valid user can connect to the View Connection Server with the View Client for Linux in fullscreen mode.

Expected Results

The user will successfully connect to the View Connection Server in fullscreen mode.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userfullscreen**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View Client for Linux with the –fullscreen option.
5. Verify that the View Client for Linux is in fullscreen mode and no other thin client operating system UI elements are visible.
6. Connect to **view-server.vdi-test1.com** with the View Client for Linux.
7. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
8. Verify that the desktop selector dialog box appears.
9. Quit the View Client for Linux.

6.13 View:LnxClient:BasicSessionDirectConnect

Test Purpose

A valid user can connect to the View Connection Server and an entitled desktop with the View Client for Linux without a secure tunnel.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop without a secure tunnel.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userdirectconnect**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Servers** and edit **view-server**.
7. Disable **Use secure tunnel connection to desktop**.
8. Log into the thin client.
9. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
10. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
11. Choose the **win7_32** desktop and connect using both RDP and PCoIP.
12. The user successfully connects to the **win7_32** desktop virtual machine and will be automatically logged in to the OS. No additional user validation was needed.
13. Log out of the desktop virtual machine.
14. Go back to the **View Administrator**.
15. Go to **View Configuration -> Servers** and edit **view-server**.
16. Enable **User secure tunnel connection to desktop**.

6.14 View:LnxClient:BasicSessionRSASecurID (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RSA SecurID authentication. A valid user can connect to the View Connection Server and an entitled desktop with the View Client for Linux using RSA SecurID authentication.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
3. Provide the username and RSA SecurID token PIN.
4. Provide the user’s domain login password.
5. Connect to the **individual2** desktop.
6. The user successfully connects to the **individual2** desktop virtual machine.
7. Log out of the desktop virtual machine.

6.15 View:LnxClient:Valid2-FactorAuthentication (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RADIUS 2-Factor Authentication. There are a few different Authentication Managers that VMware View support. Depending on what you have setup, please perform the tests below. A valid user can connect to the View Connection Server and an entitled desktop with the View client using RADIUS 2-Factor Authentication.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Launch the web browser and go to the **View Administrator** portal at https://view-server/admin
2. Log into the **View Administrator** as an Administrator
3. Go to **View Configuration -> Servers.** Click on **Connection Servers** tab and highlight your **View Connection Server** name and select **Edit**. This should bring up the "**Edit View Connection Server Settings**"
4. Select the **Authentication** tab and setup the **Authenticator** but DO NOT enable "**Enforce 2-factor and Windows user name matching" and "Use the same User name and password for RADIUS and Windows Authentication" options**
5. Log into the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Provide the valid username and passcode if you're using **VASCO Authentication Manager** (Note: the passcode consists of PIN & token generated by the Vasco Authentication Manager)

   OR

   Provide AD user name and password, which is imported into **SMSPASSCODE server** if you're using **SMSPASSCODE Authentication Manager**
8. Provide the static passcode is using **SMSPASSCODE Authentication Manger**
9. Provide the user's domain login password
10. Connect to the **individual2** desktop.
11. The user successfully connects to the **individual2** desktop virtual machine.
12. Log out of the desktop virtual machine.

6.16 View:LnxClient:AD Matching 2-Factor Authentication (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support RADIUS 2-Factor Authentication. There are a few different Authentication Managers that VMware View support. Depending on what you have setup, please perform the tests below. A valid user can connect to the View Connection Server and an entitled desktop with "Enforce 2-Factor and Windows user name matching" option enabled.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. Launch the web browser and go to the **View Administrator** portal at https://view-server/admin
2. Log into the **View Administrator** as an Administrator
3. Go to **View Configuration -> Servers.** Click on **Connection Servers** tab and highlight your **View Connection Server** name and select **Edit**. This should bring up the "**Edit View Connection Server Settings**"
4. Select the **Authentication** tab and enable "**Enforce 2-factor and Windows user name matching"** but NOT the **"Use the same User name and password for RADIUS and Windows Authentication" option**
5. Log into the thin client.
6. Launch the View client and connect to **view-server.vdi-test1.com**.
7. Provide the valid username and passcode if you are using **VASCO Authentication Manager** (Note: the passcode consists of PIN & token generated by the **VASCO Authentication Manager**)

   OR

   Provide AD user name and password, which is imported into **SMSPASSCODE server** if you're using **SMSPASSCODE Authentication Manager**
8. Provide the static passcode if you are using **SMSPASSCODE Authentication Manger**
9. Provide the user's domain login password
10. Connect to the **Win7 x64** desktop.
11. The user successfully connects to the **Win7 x64** desktop virtual machine.
12. Log out of the desktop virtual machine.

6.17 View:LnxClient:BasicUI

Test Purpose

Under normal use, the UI of the thin client OS does not interfere with the UI of the desktop virtual machine.

Expected Results

The UI of the thin client OS does not interfere with the UI of the desktop virtual machine.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userbasicui**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop and connect.
7. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS in fullscreen mode.
8. Press the Windows key.
9. Verify that this key press is interpreted within the context of the desktop virtual machine and not the underlying thin client OS. The Windows Start Menu should appear.
10. Launch several application windows in the desktop virtual machine.
11. Press Alt-Tab.
12. Verify that this key press is interpreted within the context of the desktop virtual machine and not the underlying thin client OS. This action should switch windows on the desktop virtual machine and not the thin client OS.
13. Log out of the desktop virtual machine.

6.18 View:LnxClient:DesktopReconnect

Test Purpose

A user can resume a desktop virtual machine session after a View Client for Linux disconnect.

Expected Results

The user will resume the previous desktop virtual machine session.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userdisconnect**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **Inventory -> Desktops** and select the **individual1** desktop. Click **More Commands** and choose “Logoff Session” if a user is already logged on.
7. Log into the thin client.
8. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**
9. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
10. Choose the **individual1** desktop and connect.
11. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
12. Open an Explorer window on the desktop virtual machine.
13. Physically disconnect the network cable from the thin client.
14. Verify that the desktop session disconnects.
15. Reconnect the network cable to the thin client.
16. Launch the View Client for Linux and connect to **view-server.vdi-test1.com** again.
17. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
18. Choose the **individual1** desktop and connect.
19. The user successfully connects to the **individual1** desktop virtual machine and will be automatically logged in to the OS.
20. Verify that the Explorer window is still open on the desktop.
21. Log out of the desktop virtual machine.

6.19 View:LnxClient:OSRestart

Test Purpose

A user can restart and shutdown the entitled desktop’s operating system.

Expected Results

The user will restart and shutdown the entitled desktop’s operating system.

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
3. Log in as a **vdi-test1.com** domain Administrator.
4. Choose the **individual2** desktop and connect.
5. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
6. Restart the desktop OS. Open a command prompt and type:

   ```
   shutdown -r -t 00
   ```

7. Verify that the entitled desktop begins the restart process and the View Client for Linux disconnects and quits.
8. Wait a short period of time while the entitled desktop restarts.
9. Launch the View Client for Linux and connect to **view-server.vdi-test1.com** again.
10. Log in as a **vdi-test1.com** domain Administrator again.
11. Choose the **individual2** desktop and connect.
12. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
13. Shutdown the OS. Open a command prompt and type:

    ```
    shutdown -s -t 00
    ```

14. Verify that the entitled desktop begins the shutdown process and the View Client should go back to the Desktop Selector window
15. Wait a short period of time while the entitled desktop shuts down.
16. Wait a short period of time while the desktop OS boots up. Choose the **individual2** desktop and reconnect.
17. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
18. Log out of the entitled desktop.

6.20 View:LnxClient:Keyboard

Test Purpose

The keyboard works correctly in the View Client for Linux.

Expected Results

The keyboard works correctly in the View Client for Linux.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userkeyboard**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
5. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop and connect.
7. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
8. Launch the Notepad application.
9. Type the following:

   Virtual Machine’s are gr8at!

   #They are s000 cool!&%

10. Verify that the text entry works correctly.
11. Log out of the desktop virtual machine.

6.21 View:LnxClient:MinimumMemory

Test Purpose

A valid user can connect to the View Connection Server with the View Client for Linux with a minimum memory configured thin client.

Expected Results

The user will successfully connect to the View Connection Server.

Procedure

1. Use a thin client device configured with the minimum amount of memory that will be available to customers.
2. In the **vdi-test1.com** domain, create a new user with the username “**userminmem**”.
3. Set the password to “**vmware”**, and disable “User must change password at next logon”.
4. Log into the thin client.
5. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
6. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
7. Choose the **win7_64** desktop and connect.
8. The user successfully connects to the **win7_64** desktop virtual machine and will be automatically logged in to the OS.
9. Log out of the **win7_64** desktop.
10. Quit the View Client for Linux.

6.22 View:LnxClient:MultiMonitor

Test Purpose

Verify that the View Client for Linux will utilize all the displays in a multi-monitor thin client configuration. If the thin client device does not meet the hardware requirements to support multi-monitor, this test case can be skipped.

Expected Results

The View Client for Linux will work with a multi-monitor thin client configuration.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userlinuxmultimon**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Verify that the Xinerama extension to the X Window System has been enabled with more than one display defined.
5. Verify that the thin client is running a window manager that supports the _NET_WM_FULLSCREEN_MONITORS window manager protocol defined in freedesktop.org’s Extended Window Manager Hints.
6. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
7. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
8. In the **Display** option, choose Multimonitor.
9. Choose the **individual2** desktop and connect.
10. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
11. Verify that the desktop spans across multiple displays.
12. Open a file manager window on the desktop virtual machine.
13. Drag the file manager window around all the displays and verify that the file manager window can be seen on all displays.
14. Log out of the desktop virtual machine.

6.23 View:LnxClient:MMRSupport (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Wyse Multimedia Redirection (MMR). Verify that a thin client can support Wyse MMR with the addition of MMR libraries, codecs, and a patch to rdesktop.

Expected Results

MMR libraries and codecs are installed on the thin client device and rdesktop is patched.

Procedure

1. Log in to the thin client with the View Client for Linux already installed.
2. Obtain the wyse-mmr libraries package from VMware and copy it to the thin client.
3. Uncompress the wyse-mmr tar.gz file and read the README file.
4. Follow the instructions in the README file and install and setup MMR support.
5. Recompile and re-install rdesktop.

6.24 View:LnxClient:MMRPlayVideo (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client device will support Wyse MMR. Verify the View Client for Linux can play multimedia files in a connected session.

Expected Results

The View Client for Linux plays multimedia files in a connected session.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usermmr**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Connect computer speakers or headphones to the thin client device.
4. Log into **vc-terminal** as the Administrator.
5. Launch the VI Client or vSphere Client and connect to **vc-server** as an Administrator.
6. Open a console to the **individual2** virtual machine, log in as **usermmr**, and copy the test multimedia files to the desktop. The following files should be copied: OLYMPICS.MPG, flowergarden320.avi, Damien.wmv, vandread_ep13_op_wm8_ver.wmv, Amazon_350k.wmv, and mediaexample.mp3.
7. Quit the VI Client or vSphere Client.
8. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
9. Log in to the **View Administrator** as Administrator.
10. Go to **Policies -> Global Policies** and make sure **Multimedia redirection (MMR)** is set to Allow in the View Policies section.
11. Log out of **View Administrator**.
12. Log into the thin client.
13. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
14. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
15. Choose the **individual2** desktop and connect.
16. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
17. Open Task Manager and monitor the CPU Usage. When MMR is utilized, CPU usage should hover around 5%.
18. Launch Windows Media Player and complete the setup process if necessary.
19. Play mediaexample.mp3 in Windows Media Player.
20. The audio should stream smoothly from the desktop virtual machine to the thin client’s speakers or headphones.
21. Click Pause and the audio should pause.
22. Click Play and the audio should resume.
23. Play OLYMPICS.MPG in Windows Media Player. The playback should be smooth.

24. Click Pause and the video should pause.
25. Click Play and the video should resume.
26. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
27. While the video is playing, rewind and the video should rewind and continue playing without issue.
28. Play flowergarden320.avi in Windows Media Player. The playback should be smooth.
29. Click Pause and the video should pause.
30. Click Play and the video should resume.
31. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
32. While the video is playing, rewind and the video should rewind and continue playing without issue.
33. Play Damien.wmv in Windows Media Player. The playback should be smooth.
34. Click Pause and the video should pause.
35. Click Play and the video should resume.
36. Play vandread_ep13_op_wm8_ver.wmv in Windows Media Player. The playback should be smooth.
37. Click Pause and the video should pause.
38. Click Play and the video should resume.
39. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
40. While the video is playing, rewind and the video should rewind and continue playing without issue.
41. Play Amazon_350k.wmv in Windows Media Player. The playback should be smooth.
42. Click Pause and the video should pause.
43. Click Play and the video should resume.
44. While the video is playing, seek forward and the video should fast forward and continue playing without issue.
45. While the video is playing, rewind and the video should rewind and continue playing without issue.
46. Log out of the View Client for Linux.

6.25 View:LnxClient:MMRPlayVideoClipping (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Wyse MMR. Verify the View Client for Linux can play multimedia files in a connected session. The video should play normally and should be clipped by an application that is on top of Media Player.

Expected Results

The View Client for Linux plays multimedia files in a connected session normally and should be clipped by an application that is on top of Media Player.

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
3. Enter the "**usermmr**" credentials, select the **vdi-test1.com** domain, and log in.
4. Choose the **individual2** desktop and connect.
5. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
6. Open Task Manager and monitor the CPU Usage. When MMR is utilized, CPU usage should hover around 5%.
7. Launch Windows Media Player.
8. Play OLYMPICS.MPG in Windows Media Player.
9. The audio should stream smoothly from the desktop virtual machine to the thin client's speakers or headphones.
10. Open Notepad and place Notepad over part of Media Player.
11. Verify that Notepad correctly clips out the portion of the video that it is over.
12. Log out of the View Client for Linux.

6.26 View:LnxClient:MMRPlayVideoSync (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Wyse MMR. Verify the View Client for Linux can play multimedia files in a connected session. The video should play normally and should not leave trailing still images when Media Player is moved.

Expected Results

The View Client for Linux plays multimedia files in a connected session normally and should not leave trailing still images when Media Player is moved around the desktop.

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
3. Enter the "**usermmr**" credentials, select the **vdi-test1.com** domain, and log in.
4. Choose the **individual2** desktop and connect.
5. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
6. Open Task Manager and monitor the CPU Usage. When MMR is utilized, CPU usage should hover around 5%.
7. Launch Windows Media Player.
8. Play OLYMPICS.MPG in Windows Media Player.
9. The audio should stream smoothly from the desktop virtual machine to the thin client's speakers or headphones.
10. Drag Media Player around the desktop while the video is playing.
11. Verify that Media Player does not leave trailing still images on the desktop as it is being dragged. The video should be wholly contained within Media Player.
12. Log out of the View Client for Linux.

6.27 View:LnxClient:MMRPlayVideoResize (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Wyse MMR. Verify the View Client for Linux can play multimedia files in a connected session. The video should get resized when Media Player gets resized.

Expected Results

The View Client for Linux plays multimedia files in a connected session. When Media Player gets resized, the video being played should also be resized.

Procedure

1. Log into the thin client.
2. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
3. Enter the “**usermmr**” credentials, select the **vdi-test1.com** domain, and log in.
4. Choose the **individual2** desktop and connect.
5. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
6. Open Task Manager and monitor the CPU Usage. When MMR is utilized, CPU usage should hover around 5%.
7. Launch Windows Media Player.
8. Play OLYMPICS.MPG in Windows Media Player.
9. The audio should stream smoothly from the desktop virtual machine to the thin client’s speakers or headphones.
10. Resize Media Player to fullscreen.
11. Verify that the video plays back in fullscreen mode.
12. Log out of the View Client for Linux.

6.28 View:LnxClient:USBFlashDrive

Test Purpose

Verify that the View Client for Linux on the thin client device can use a USB flash drive with the desktop virtual machine.

Expected Results

The View Client for Linux on the thin client device connects and uses a USB flash drive with the desktop virtual machine.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userlinuxusb**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into the thin client.
4. Make sure that system permissions for USB redirection have been set. See the README file for USB redirection.
5. Connect a USB flash drive to the thin client.
6. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
7. Enter the user’s credentials, select the **vdi-test1.com** domain, and log in.
8. Choose the **individual2** desktop and connect.
9. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
10. Verify that the USB flash drive is recognized by the desktop virtual machine.
11. Edit and save a notepad file on the desktop.
12. Copy the notepad file to the USB flash drive.
13. Open the notepad file on the USB flash drive and verify the contents.
14. Perform the read & write tests to the flash drive by copying the flowergarden320.avi to and from the USB flash drive
15. Play the flowergarden320.avi from the USB flash drive. Verify the video plays smoothly and the audio is synced.
16. Unplug & replug the USB flash drive from the thin client while still connecting to the desktop session and ensure that the USB flash drive unmounts & remounts properly (without having to disconnect and reconnect to the desktop session).
17. Log out of the desktop virtual machine.
18. Repeat the same tests with Win7 x86 & Win7 x64 virtual desktops.

6.29 View:LnxClient:ClientInfo

Test Purpose

Verify that local Linux system information is passed to the View Agent on the desktop virtual machine and saved in the Windows Registry.

Expected Results

System information from the View Client for Linux machine is stored in the desktop virtual machine's Windows Registry.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userlinuxinfo**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into the thin client.
4. Launch the View Client for Linux and connect to **view-server.vdi-test1.com.**
5. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
6. Choose the **individual2** desktop and connect.
7. The user successfully connects to the desktop virtual machine and will be automatically logged in to the OS.
8. On the desktop virtual machine, run the "regedit" command to open the Windows System Registry.
9. Navigate to **My Computer\HKEY_CURRENT_USER\Volatile Environment.**
10. Verify that all the following data exists in the Windows System Registry:
    - **ViewClient_IP_Address** = the IP address of the thin client device
    - **ViewClient_MAC_Address** = the MAC address of the thin client device
    - **ViewClient_Machine_Name** = the machine name of the thin client device
    - **ViewClient_LoggedOn_Username** = the username that was entered in the View Client
    - **ViewClient_Type** = the thin client name or operating system type of the thin client device
    - **ViewClient_TimeOffset_GMT** = the thin client device's time offset from GMT
11. Log off the desktop virtual machine.

6.30 View:LnxClient:PCoIPHWRequirements

Test Purpose

Verify that the thin client meets the hardware requirements for utilizing the PCoIP protocol. If the thin client device does not meet the hardware requirements to support the PCoIP protocol, this test case can be skipped.

Expected Results

The thin client meets the hardware requirements for using the PCoIP protocol.

Procedure

1. Verify that the thin client device has an x86 based processor with SSE2 extensions.
2. Verify that the thin client device has a minimum 800 MHz processor.
3. In addition to the RAM requirements for the thin client operating system, the thin client must also have the following additional amount of RAM to support the PCoIP protocol. The amount of additional RAM is determined by the maximum number of displays and the maximum resolution the thin client will support. Please see the table below.

Display Setting	Width	Height	Pixels	Additional RAM @ 1 Display	Rounded Up	Additional RAM @ 2 Displays	Rounded Up
VGA	640	480	307200	Not Tested	**N/A**	Not Tested	**N/A**
SVGA	800	600	480000	160 MB	**196 MB**	310 MB	**512 MB**
720p	1280	720	921600	150 MB	**196 MB**	320 MB	**512 MB**
UXGA	1600	1200	1920000	300 MB	**512MB**	380 MB	**512 MB**
1080p	1920	1080	2073600	330 MB	**512 MB**	380 MB	**512 MB**
WUXGA	1920	1200	2304000	330 MB	**512 MB**	380 MB	**512 MB**
QXGA	2048	1536	3145728	350 MB	**512 MB**	440 MB	**512 MB**
WQXGA	2560	1600	4096000	Not Tested	**N/A**	Not Tested	**N/A**

6.31 View:LnxClient:PCoIP

Test Purpose

Verify that the Linux View Client can connect to a desktop virtual machine using the PCoIP protocol.

NOTE: If the thin client device does not meet all the hardware or software requirements to support the PCoIP protocol, this test case can be skipped. The thin client will only be certified for RDP.

However, if the thin client device meets all the requirements to support PCoIP, then it is mandatory to support PCoIP.

Expected Results

The Linux View Client will connect to a desktop virtual machine using the PCoIP protocol.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userpcoip**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log in to the thin client.
4. Install the additional VMware-view-pcoip package if it has not already been installed. Please see the README file included in the package for installation instructions.
5. Launch the Linux View Client and connect to **view-server.vdi-test1.com**.
6. Enter the user's credentials, select the **vdi-test1.com** domain, and log in.
7. Choose the **win7_32** desktop.
8. Choose PCoIP as the Display Protocol and connect to the desktop.
9. The user successfully connects to the **win7_32** desktop virtual machine and will be automatically logged in to the OS.
10. Verify that the desktop VM's display resolution is automatically adjusted to match the thin client device's display resolution.
11. Log out of the desktop virtual machine.

6.32 View:LnxClient:PCoIPSmallClientImageCacheSize

Test Purpose

The default image cache size is set at 250MB. This test is to ensure that the variable is set 10 (smaller than the minimum of 50MB), performance is still good & that correct cache size is recorded in the log.

Expected Results

With direct connection between Client and Agent using PCoIP, user should be able to see the rectangles around every tile (32x32 pixels) on the picture. This means those content in every rectangle comes from cache and the log reports the client cache size at 4750.

Procedure

1. Look to see if ".pcoip.rc" file exists in ~/ directory. If not create this hidden file
2. Add the following to the .pcoip.rc file

   pcoip.show_image_cache_hits = 1

   pcoip.image_cache_size_mb = 10
3. Launch the **View Client application** and connect to the **Win7x64** desktop via **PCoIP protocol**.
4. Once connected, user should see the rectangles around every tile (**32x32 tile**)
5. View a Windows sample picture using Windows Photo Viewer
6. Go to the next picture & back to previous
7. On your thin client system, browse to **/tmp/teradici-user**. There should be a pcoip log file.
8. Launch this log file & verify that the client cache size is set correctly to **4750**

   IPC :cSW_CLIENT_IPC: Creating client cache (*size = 4750*, physical memory = 3275MB)

6.33 View:LnxClient:PCoIPLargeClientImageCacheSize

Test Purpose

The default image cache size is set at 250MB. This test is to ensure that the variable is set 1000MB (larger than the max of 300MB), performance is still good & that correct cache size is recorded in the log.

Expected Results

With direct connection between Client and Agent using PCoIP, user should be able to see the rectangles around every tile (32x32 pixels) on the picture. This means those content in every rectangle comes from cache and the log reports the client cache size at 28500.

Procedure

1. Repeat the previous test but change the **pcoip.image_cache_size_mb** to **1000** in the **.pcoip.rc** log
2. Launch the **View Client application** and connect to the **Win7x64** desktop via **PCoIP protocol**.
3. Once connected, user should see the rectangles around every tile (**32x32 tile**)
4. View a Windows sample picture using Windows Photo Viewer
5. Go to the next picture & back to previous
6. On your thin client system, browse to **/tmp/teradici-user**. There should be a pcoip log file.
7. Launch this log file & verify that the client cache size is set correctly to **28500**

   IPC :cSW_CLIENT_IPC: Creating client cache (*size = 28500*, physical memory = 3275MB)

6.34 View:LnxClient:BasicSessionSmartCard (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. A valid user can connect to the View Connection Server and an entitled desktop with the View Client for Linux using Smart Card authentication and both the RDP and PCoIP protocol.

Expected Results

The user will successfully connect to the View Connection Server and an entitled desktop.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**userlinuxsmartcard**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Install the Smart Card reader on the thin client along with the necessary drivers and libraries. Refer to the documentation that accompanies the Smart Card reader for more information about how to do this.
4. Set up the Active Directory server and View Connection Server to support Smart Card authentication for the "**userlinuxsmartcard"** user. Refer to the "Smart Card Authentication" section of the ***VMware View Manager Administration Guide*** for more information about how to do this at http://www.vmware.com/support/pubs/view_pubs.html.
5. Enable Smart Card support in the VMware View Client for Linux. Refer to the "SMART CARD SUPPORT" section of README.txt included with the View Client for Linux for more information about how to do this.
6. Log into the thin client.
7. Plug the Smart Card into the Smart Card reader.
8. Launch the View Client for Linux and connect to **view-server.vdi-test1.com**.
9. Provide the Smart Card PIN.
10. Connect to the **individual2** desktop using the RDP protocol.
11. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS with no additional authentication.
12. Log out of the desktop session.
13. Repeat logging into the **individual2** desktop with the Smart Card and the PCoIP protocol.
14. Log out of the desktop session.
15. Log off the thin client.

6.35 View:LnxClient:SmartCardRemovalPolicy (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support Smart Card authentication. Verify that a Smart Card authenticated user is automatically disconnected from a desktop virtual machine when the Smart Card is removed.

Expected Results

A Smart Card authenticated user will automatically be disconnected from a desktop virtual machine when the Smart Card is removed.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**userscremoval**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Servers,** highlight **view-server** and click **Edit.** In the **Authentication** tab**,** enable **Disconnect user sessions on smart card removal**.
7. Log out of **View Administrator**.
8. Set up the thin client and user for Smart Card authentication in the vdi-test1.com domain.
9. Log in to the thin client.
10. Insert the Smart Card.
11. Launch the Linux View Client and connect to **view-server.vdi-test1.com**. Provide the login PIN if necessary.
12. Choose the **individual2** desktop.
13. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
14. Remove the Smart Card from the Smart Card reader.
15. Verify that the user is automatically disconnected from the desktop virtual machine session.
16. Log out of the thin client.

6.36 View:LnxClient:TimezoneRedirection

Test Purpose

Verify the VMware Linux View Client can forward the thin client’s time zone setting to the desktop virtual machine.

Expected Results

The desktop virtual machine will have the same time zone setting as the thin client running the VMware Linux View Client.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username “**usertimezone**”.
2. Set the password to “**vmware”**, and disable “User must change password at next logon”.
3. Log into **vc-terminal** as the Administrator.
4. Launch the VI Client or vSphere Client.
5. Connect to **vc-server** and provide the Administrator credentials.
6. Open a console to the **individual2** desktop and log in as the Domain Administrator.
7. Set the time zone to US Pacific time.
8. Quit the VI Client or vSphere Client.
9. Log into the thin client as a user with root privileges.
10. Set the time zone to US Eastern time on the thin client.
11. Log out of the thin client.
12. Log back into the thin client device as a user without root privileges.
13. Launch the Linux View Client and connect to **view-server.vdi-test1.com.**
14. Enter the **usertimezone** credentials, select the **vdi-test1.com** domain, and log in.
15. Choose the **individual2** desktop and connect.
16. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
17. Verify that the desktop virtual machine’s time zone is automatically set to US Eastern time.
18. Log out of the **individual2** desktop.

6.37 View:LnxClient:PCoIPCopyAndPaste

Test Purpose

Verify that the thin client device's operating system can copy and paste text to the desktop session via the View Client for Linux using the PCoIP protocol.

Expected Results

The thin client device's operating system can copy and paste text to the desktop session via the View Client for Linux using the PCoIP protocol.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**usercopypaste**".
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into the thin client.
4. Install the additional VMware-view-pcoip package if it has not already been installed. Please see the README file included in the package for installation instructions. Verify that the **libmksvchanclient.so** file included in the package is copied to /usr/lib/pcoip/vchan_plugins/.
5. On the thin client, open a web browser or a text file.
6. Highlight some text and copy it. The exact Procedure for doing this will depend on your Linux configuration.
7. Launch the VMware View Client for Linux and connect to **view-server.vdi-test1.com.**
8. Enter the **usercopypaste** credentials, select the **vdi-test1.com** domain, and log in.
9. Choose the **individual2** desktop and connect using the PCoIP Display Protocol.
10. The user successfully connects to the **individual2** desktop virtual machine and will be automatically logged in to the OS.
11. Paste the copied text in Wordpad or the copied image in Paint or other photo editing software
12. Verify that the text or image is copied correctly from the thin client to the desktop session.
13. Quit Wordpad.
14. Log out of the **individual2** desktop.
15. Quit the View Client.

6.38 View:LnxClient:KioskMode (Optional)

Test Purpose

This test case is optional and will only need to be run if the thin client will support the View client's kiosk mode. Verify that the thin client can function in Kiosk Mode with the View Client for Linux and the View Connection Server. For more detailed information about Kiosk Mode requirements, please see the Kiosk Mode whitepaper available as an addendum to the end of this document.

Expected Results

The thin client functions in Kiosk Mode with the View Client for Linux and the View Connection Server.

Procedure

1. In the **vdi-test1.com** domain, create a new user with the username "**kioskadmin**". Make this user a member of the **Account Operators** group in the domain.
2. Set the password to "**vmware"**, and disable "User must change password at next logon".
3. Log into **vc-terminal** as the Administrator.
4. Launch a web browser and go to the **View Administrator** portal at https://view-server/admin.
5. Log in to the **View Administrator** as Administrator.
6. Go to **View Configuration -> Administrators** and create a new administrator role called "**Kiosk_Admin**". Give this new role **Direct Interaction** and **View Configuration and Global Policies** privileges.
7. Add the "**kioskadmin**" user as a View administrator with the **Kiosk_Admin** role.
8. Log into the thin client device with the View Client installed and and execute the following command:

   ```
   vmware-view --printEnvironmentInfo –s view-server.vdi-test1.com
   ```

   Note the MAC address of the thin client. The MAC address of the thin client will be used to identify it with the View Connection Server during Kiosk Mode login.
9. Log into **vc-terminal** as the Administrator.
10. Launch the VI Client or vSphere Client.
11. Connect to **vc-server** and provide the Administrator credentials.
12. Open a console to the **view-server** and log in as "kioskadmin".
13. Enable Kiosk Mode on the View Connection Server. Open a new Windows command prompt and go to **C:\Program Files\VMware\VMware View\Server\tools\bin\** and execute the following command:

   ```
   vdmadmin.exe –Q –enable –s view-server
   ```

   Verify that kiosk mode is enabled. Execute:

```
vdmadmin.exe –Q –clientauth –list
```

For **view-server**, the **Client Authentication Enabled** field should be true.

14. Add the thin client to the View Connection Server as a kiosk. At the **view-server** command prompt, go to **C:\Program Files\VMware\VMware View\Server\tools\bin\** and execute the following command:

    ```
    vdmadmin.exe –Q –clientauth –add –domain vdi-test1.com –clientid
    <THIN_CLIENT_MAC_ADDRESS> -genpassword –description “Linux kiosk user”
    ```

    Verify that the thin client was added as a kiosk. At the command prompt, execute:

    ```
    vdmadmin.exe –Q –clientauth –list
    ```

    The **Client Authentication User List** should contain a **clientID** with the thin client’s MAC address.

15. Log back into the thin client and execute the View client in Kiosk Mode. At the commandline execute the following command:

    ```
    vmware-view --kioskLogin --fullscreen --once --nonInteractive --nomenubar –s
    view-server.vdi-test1.com
    ```

    The thin client should automatically connect to the View Connection Server and log into a desktop entitled to all domain users without any user intervention.

    NOTE: If you have more than one desktop, you need to add the –n <desktop name> option to your command.

16. Log out of the entitled desktop and quit the View client.

6.39 View:LnxClient:UIGuidelines

Test Purpose

Verify that the thin client conforms to VMware's user interface guidelines for running the View Client for Linux.

Expected Results

The thin client conforms to VMware's user interface guidelines for running the View Client for Linux.

Procedure

1. Verify that an Administrative user can launch the View Client without use of the '`--nonInteractive`' commandline option. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which '`--nonInteractive`' mode is not used. From the commandline, go to the directory containing the View Client binary and execute this command:

   ```
   ./vmware-view
   ```

   The View Client should launch without issue.

2. Verify that an Administrative user can launch the View Client with custom options provided via the commandline and options file. If a configuration manager is used instead of a general-purpose desktop UI, there must be a configuration in which custom options can be supplied. The list of commandline options can be viewed by executing '`vmware-view --help`'. The user must be able to supply all the custom options that the View Client supports. From the commandline, execute this command:

   ```
   ./vmware-view --nonInteractive  --serverURL view-server --userName
   usercopypaste --password vmware --domainName vdi-test1.com --desktopName
   win7_64
   ```

   The View Client should launch and connect to the win7_64 desktop without interaction from the user or error messaging of any kind.

6.40 View:LnxClient:ApplicationIcon

Test Purpose

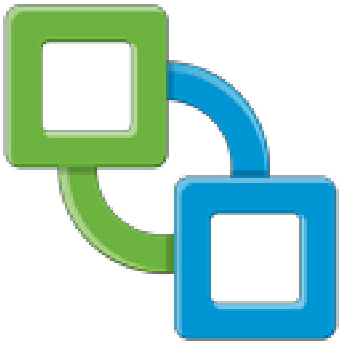
The View Linux Client should have an application icon consistent with the current View icon illustrated in the **VMware View Graphics Guide** pdf file.

Expected Results

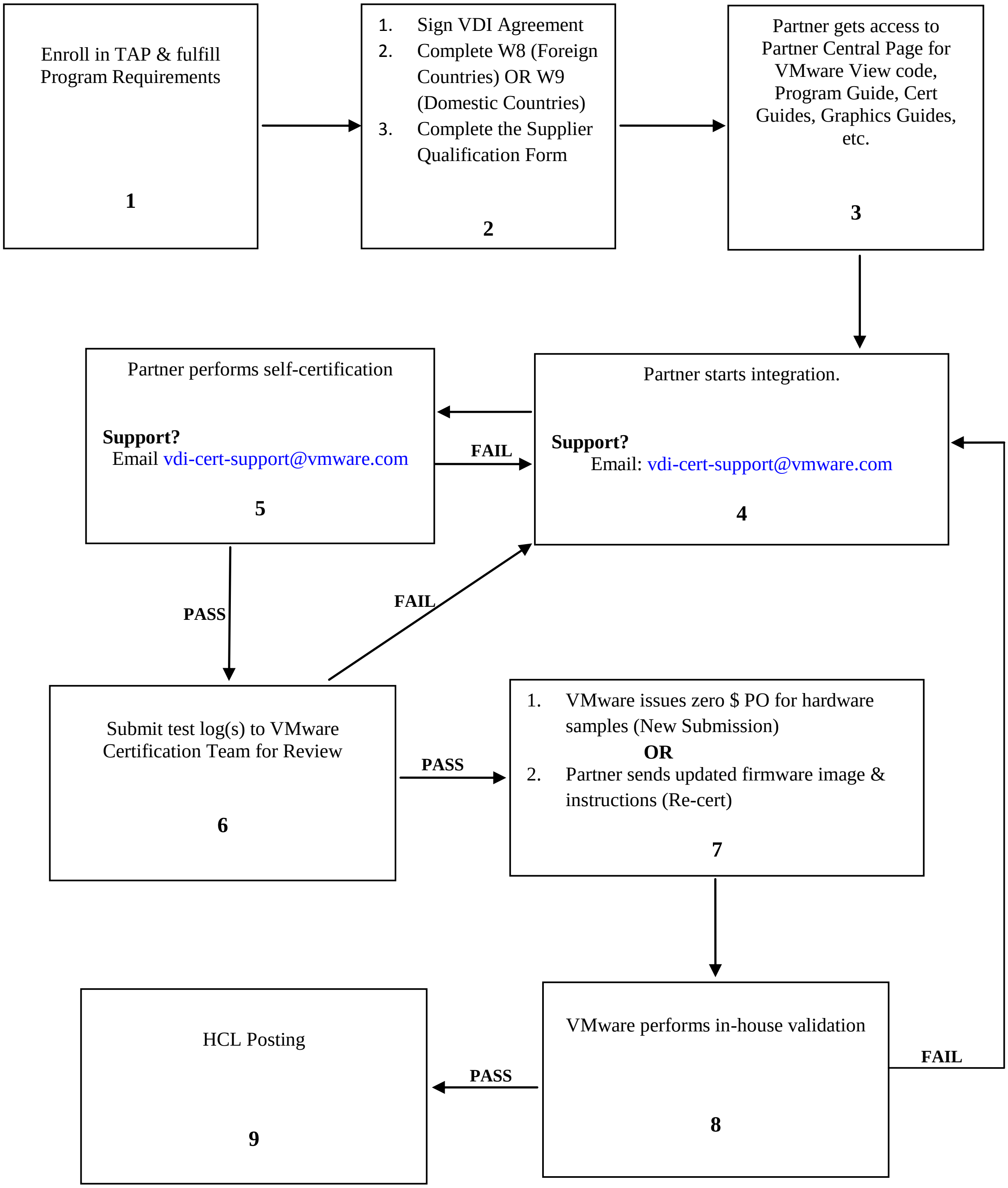
The View Linux Client application icon is consistent with the guidelines in the **VMware View Graphics Guide** pdf file.

Procedure

1. Refer to the **VMware View Graphics Guide** pdf file for the most up-to-date information about the View graphics guidelines.
2. Log into the thin client.
3. Verify that the View Linux Client application icon on the desktop and in menus looks like this:



1. Thin Client Certification Process Flow


Enroll in TAP & fulfill Program Requirements
1
1. Sign VDI Agreement
2. Complete W8 (Foreign Countries) OR W9 (Domestic Countries)
3. Complete the Supplier Qualification Form
2
Partner gets access to Partner Central Page for VMware View code, Program Guide, Cert Guides, Graphics Guides, etc.
3
Partner starts integration.
Support?
Email: vdi-cert-support@vmware.com
4
Partner performs self-certification
Support?
Email vdi-cert-support@vmware.com
5
FAIL
PASS
FAIL
Submit test log(s) to VMware Certification Team for Review
6
PASS
1. VMware issues zero $ PO for hardware samples (New Submission)
OR
2. Partner sends updated firmware image & instructions (Re-cert)
7
VMware performs in-house validation
8
FAIL
PASS
HCL Posting
9

8. Certification Submission Procedure

Hardware Certification:

After successfully completing and passing all the test cases, submit the VMware View Thin Client Certification Submission form to VMware for review. Once the log review has passed, VMware will notify you with a zero $ PO for you to send in the hardware samples. Please do not send in hardware without a zero $ PO. You must also send 2 production samples of the thin client device to VMware for validation if VMware does not already have sample devices onsite. The 2 thin client production samples must contain the same software load used in the certification tests. The 2 thin client production samples must contain the same model identification as indicated on the submission form. An incorrectly configured thin client device may delay the validation process and the posting to the VMware View Thin Client Hardware Compatibility List. Once VMware receives the 2 thin client production samples, VMware will review the submission form, validate the 2 thin client production samples, and post the thin client device to the VMware View Thin Client Hardware Compatibility List within 2 weeks.

Certifications will remain open for 30 days after the submission. After 30 days, if VMware has not received equipment or technical issues with a submission have not been addressed, the certification will be closed.

If you are certifying a new View client version with a thin client device that you have already submitted to VMware from a prior certification submission, VMware can update the thin client device with your new software image to verify your submission. Instead of submitting hardware samples, please submit the new software image and detailed instructions for updating the device to VMware along with your Thin Client Certification Submission form.

Software Certification:

After successfully completing and passing all the test cases for your software, submit the VMware View Thin Client Certification Submission form to VMware for review along with your OS image. This can be in a form of an iso. This iso must be installable on a virtual environment or a hardware platform is required for VMware validation purposes. If a hardware platform is required, please contact VMware for a zero $ PO before shipping the hardware to us.

Submission Procedure:

1. Complete the ***Device & Company Information*** sheet of the Thin Client Certification Submission form.
2. Perform all the test cases in Section 3 to set up the View certification environment and mark the results in the ***Pre-Certification*** sheet of the Thin Client Certification Submission Form.
3. **View Open Client:** To certify a thin client based on the View Open Client either (1) perform the tests in Section 4 and fill out the ***View Open Client*** sheet of the submission form or (2) submit code changes to VMware for review.
4. **View Windows Client:** To certify a Windows XPe/Windows Embedded Standard, Windows Embedded Standard 7 thin client running the View Client for Windows, perform the tests in Section 5 and fill out the ***Windows View Client*** sheet of the submission form.
5. **View Linux Client:** To certify a Linux thin client running the View Client for Linux, perform the tests in Section 6 and fill out the ***Linux View Client*** sheet of the submission form.
6. E-mail the following items to vdi-cert-support@vmware.com
    a. VMware View Thin Client Certification Submission Form
    b. For a custom client based on the View Open Client, screenshots or pictures of the View client splash screen and login screen.

    c. Optionally, for a custom client based on the View Open Client, the source code changes to the base View Open Client.

7. Wait for VMware's acknowledgement of receiving the submission form and/or other files.
8. VMware will review the submission form.
9. If the review finds issues with the submission, VMware will work with the partner to correct the issues so that the certification submission review will pass.
10. Once the review passes, VMware will request 2 production samples or the new device image.
11. a) For a hardware thin client, VMware will request the 2 production samples with a Zero Cost Purchase Order (PO) Number, a mailing address, and a VMware contact. You will not need to provide production samples to VMware if you have already done so in a prior certification submission. The thin client samples' model identification (labeling on the device) must match the "Hardware Model" field in the ***Device & Company Information*** section of the submission form.

    b) For software certification, partners will need to either provide VMware with the OS image or a hardware platform for validation.
12. If you have already submitted thin client device samples to VMware for a prior certification, you will only need to provide the new software image and detailed instructions for updating the device to VMware.
13. Send 2 production samples of the hardware thin client or new device image to VMware.
14. Upon receiving the 2 hardware thin client production samples or new device image, VMware will:
    a. Perform a validation of the thin client within 2 weeks.
    b. Notify the partner via e-mail whether the thin client passes or fails certification.
15. If the thin client device passes certification, VMware will e-mail the partner the "VMware Ready Certified" logo usage guidelines along with the VMware Ready Certified logos if necessary. VMware will also provide the date when the approved submission will first appear on the VMware Thin Client Hardware Compatibility List.