



## VIRTUALIZING DESKTOPS WITH SUN RAY™ SOFTWARE AND VMWARE VIEW MANAGER

David Fong, Sun Microsystems  
Matthias Müller-Prove, Sun Microsystems  
Adam Workman, Sun Microsystems

Sun BluePrints™ Online

Part No 820-7120-10  
Revision 1.0, 3/3/09



## Table of Contents

<b>The Desktop Management Challenge</b> .....	1
<b>Desktop Virtualization with Sun and VMware Software</b> .....	2
Architecture Overview .....	3
Virtualization Layer .....	4
Session Management Layer .....	4
Virtual Desktop Access Layer .....	5
Key Capabilities .....	5
<b>Software Installation and Configuration</b> .....	7
Software Installation .....	7
Configure VMware View Manager .....	7
Install and Configure Sun Ray Connector for VMware View Manager .....	10
Enabling SSL .....	12
Generate the Certificate .....	12
Enable the Certificate .....	13
Install the Certificate on Sun Ray Servers .....	14
Troubleshooting .....	16
<b>Best Practices for Deployment</b> .....	18
<b>For More Information</b> .....	19
About the Authors .....	19
Acknowledgments .....	19
References .....	19
Ordering Sun Documents .....	20
Accessing Sun Documentation Online .....	20

## Chapter 1

# The Desktop Management Challenge

Coping with a never-ending stream of software upgrades and patches, dealing with personal software on desktop PCs, and managing a variety of software versions and hardware failures all present challenges to system administrators. As the number of desktops grows, management and operational costs rise. Ensuring that every system is protected against the latest security attacks is a time-consuming task, and energy budgets inflate as more desktops are added to the environment. In addition, demonstrating compliance with industry or government legislation and internal policies is difficult when applications reside on individual PCs. Perhaps most importantly, sensitive data and critical applications on desktops and laptops are vulnerable to theft and data loss — a problem that is exacerbated by poor backup procedures.

With more users needing the ability to work remotely, enterprises are recognizing the need to let people move from place to place without losing the functionality of traditional fixed asset environments. Unfortunately, traditional PC-based approaches to desktop computing struggle to support mobility, and pose a variety of challenges that even the most advanced system management tools often fail to address.

Desktop virtualization applies well-known datacenter expertise to hosting desktop PC environments. It enables isolation, encapsulation, and mobility, helping organizations to run different operating systems side-by-side, run legacy Win32 applications next to Web 2.0 applications, and move operating systems, applications, and desktops to different devices. In fact, desktop environments can be moved off individual desktops and centralized on dedicated servers in the datacenter. As a result, organizations can take advantage of client device independence, provide true mobility for workers, streamline management, and keep information secure.

This Sun BluePrints™ article describes a reference implementation for desktop virtualization deployments developed by technology leaders in desktop virtualization and thin client technology, and explains how to install and configure key software components. Combining the Sun Ray™ Software, Sun Ray thin clients, and VMware View Manager, the reference implementation gives clients access to resilient and secure desktop environments.

Building on over 10 years of experience delivering desktops over the network, Sun continues to work with VMware to deliver high-performance virtualization solutions that can help organizations make better use of valuable resources. By utilizing a feature-rich virtual desktop infrastructure solution with some of the most secure thin clients available, the reference implementation provides a highly secure solution that can help simplify desktop management.

## Chapter 2

## Desktop Virtualization with Sun and VMware Software

To be effective, enterprise desktop virtualization solutions must be able to:

- Ease desktop environment management — Hosting virtualized desktop images in datacenters can help reduce the challenges associated with upgrading and patching applications and operating systems.
- Scale to meet demand — Every tier of an enterprise virtualization solution must be able to grow and handle hundreds or thousands of desktops.
- Deliver needed performance and security — Whether users are working locally on a LAN or accessing virtual desktops remotely via WAN or Internet connections, systems must provide secure access to the environment, keep transmitted information safe, and deliver adequate performance to support productivity.
- Assign desktops effectively — Because users employ various tools to perform job functions and handle responsibilities, virtualized desktop environments must be able to provision different, or multiple, desktops to users. For example, some users require personally assigned desktops, while others can use desktops from a shared pool.

VMware software can be combined with Sun software, servers, and thin clients to create a dynamic platform that brings virtualization to the desktop and enables user mobility through a server-centric model that simplifies desktop access and management (Figure 2-1).

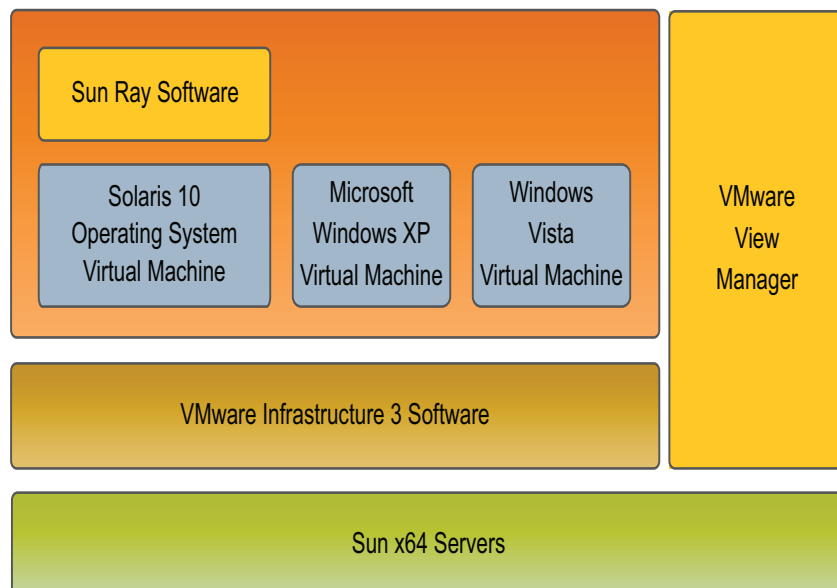


Figure 2-1. Sun Ray technology and VMware View Manager solution stack

Sun Ray Connector for VMware View Manager is a free, add-on component for Sun Ray Software that is available for download at:  
[http://sun.com/software/sunray/get\\_addons.jsp](http://sun.com/software/sunray/get_addons.jsp)

- *Sun Ray Software*  
 Sun Ray Software enables users to access applications and services from any location using Sun Ray compatible thin client devices. Since Sun Ray thin clients do not contain any local processing or storage resources, these functions are performed centrally on servers. The Sun Ray Connector for VMware View Manager allows Sun Ray users to connect to Windows virtual machines via the VMware View Manager software.
- *VMware Infrastructure Software*  
 VMware Infrastructure 3, comprised of VMware ESX Server and VMware vCenter, is virtual machine technology for partitioning, consolidating, and managing systems in mission-critical environments. VMware ESX Server provides a highly-scalable virtual machine platform with advanced resource management capabilities, all of which is managed through VMware vCenter.
- *VMware View Manager*  
 VMware View Manager is an enterprise-class desktop management broker that securely connects remote users to virtual desktops in the datacenter. An easy to use, Web-based interface provides management of the centralized environment.

## Architecture Overview

The Sun Ray technology and VMware View Manager solution uses a multilayered approach that centralizes and facilitates access to services and applications to bona fide users while denying entry to those that are unknown or have insufficient privileges (Figure 2-2).

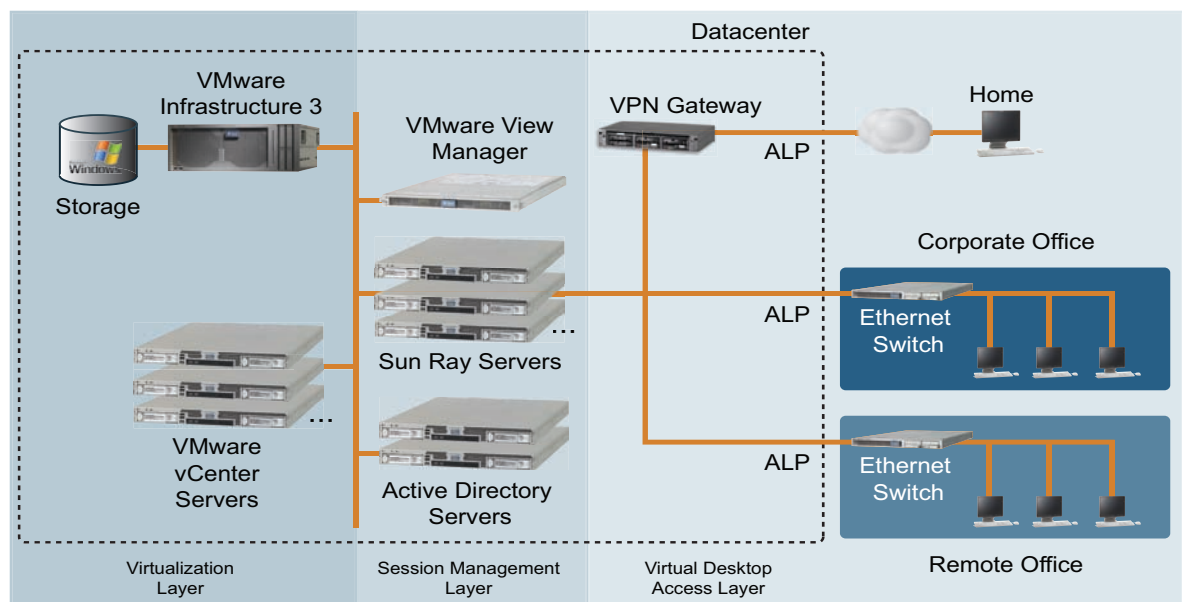


Figure 2-2. Sun Ray technology and VMware View Manager solution architecture

## Virtualization Layer

The virtualization layer consists of one or more servers dedicated to hosting desktops for users, and is typically housed in a datacenter or other secure environment. To support simultaneous access to multiple desktops on a client, the virtualization layer can consist of a heterogeneous collection of servers linked to clients through a session management layer.

Virtualization is made possible by a hypervisor in the physical server that encapsulates each virtual machine, letting the operating system function in an emulated hardware environment that provides needed resources. Encapsulated virtual machines can be moved from one physical host to another without concern for differences in hardware or device driver capabilities. Once encapsulated, virtual machines are isolated from one another to ensure problems that occur in one environment do not affect other virtual machine instances.

## Session Management Layer

Sun Ray servers act as a management layer between virtual desktop servers in the virtualization layer and client desktop environments in the desktop access layer. These session management layer servers enable desktop virtualization by decoupling client devices that deliver application-generated video, audio, and user interfaces from the actual provisioning and processing of application software. Session management layer servers can be horizontally scalable servers from Sun or other vendors with UltraSPARC®, AMD Opteron™, or Intel® Xeon® processors running the Solaris™ Operating System (Solaris OS).

Session management layer servers are often bound together in failover groups of two or more servers to increase availability in the event of a network or system failure. If a server is rendered unavailable, each Sun Ray desktop unit connected to the server reconnects to an available server in the failover group, and to a previously existing desktop session. Since the desktops are hosted in the virtualization layer, users are presented with the same system state without data loss.

Active Directory servers authenticate users and implement access policies, such as restricting the permitted hours for login and password expiration dates. Sun Ray Connector for VMware View Manager forwards user names and passwords to VDM, and the authentication occurs between the VMware View Manager and Active Directory software.

## Virtual Desktop Access Layer

The client tier includes Sun Ray devices used to access services that are connected to the server via a wired or wireless LAN or WAN over a modem, cable modem, digital subscriber line (DSL), WiFi, or other communications channel.

## Key Capabilities

The desktop virtualization reference implementation provides several key capabilities.

- **Session mobility (hot-desking)**  
Desktop virtualization gives users the ability to move from one Sun Ray client to another and resume the desktop session. Because the user session executes on a server rather than the client device, users can migrate from one Sun Ray thin client to another — without pausing or saving applications — and access the session from a different Sun Ray client. The session appears instantly in the new location once the user is identified through the insertion of an optional smart card. This hot-desking capability is possible whether a user moves to the next cubicle, works from a remote or home office, or checks in from a Sun Ray device on the other side of the world.
- **Regional hot-desking**  
Regional hot-desking gives users access to desktop sessions across a wide domain and longer distance than a single failover group. Enterprises with multiple failover groups and users that move from one location to another — such as between corporate headquarters and various branch offices — can take advantage of regional hot-desking.
- **Stateless delivery of desktops and applications**  
The Sun Ray technology and VMware View Manager solution provides stateless connectivity to Sun Ray thin clients. Changes to the client device, such as a reboot or power outage, do not affect desktop environments or applications running in the virtualization layer. Upon restart, clients reconnect to the back-end servers and sessions resume where users left off.
- **Simplified deployment and administration**  
The Sun Ray technology and VMware View Manager solution centralizes software installation and management. Organizations only need to install and maintain a single instance of an operating system on a virtualization layer server. The operating system is made available to qualified users over the network, eliminating the need to install and maintain environments on every client platform. Because operating systems are maintained in the datacenter, upgrade and patch installation processes are simplified, reducing administrative burden as well as the impact of malware attacks.
- **Data security**  
While users gain freedom in how, where, and when they access enterprise IT services, managers retain full control over who has what kind of access to specific resources and information. Security features help maintain process and data integrity. In addition, Sun Ray thin clients do not contain disk drives. Data is stored

on central storage and cannot be compromised if the device is stolen.

Furthermore, copying data to external USB devices is possible only if enterprise data management policies permit.

- Performance

Many companies allow users to work from home or at a variety of office locations. With users working under a variety of network conditions, it is important for the system to provide the performance needed for users to be productive. The Sun Ray technology and VMware View Manager solution takes advantage of the high-performance Sun Ray Appliance Link Protocol (ALP) to transmit user input and screen updates from datacenters to the client over local and wide area networks. Additionally, Sun Ray multimedia enhancements for Windows Media Player provide increased performance of corporate communications and training videos by leveraging client-side compute resources, conserving server network bandwidth.

- Scalability

When multiple Sun Ray servers are configured as a failover group, Sun Ray thin clients can connect to any Sun Ray server. Such a configuration provides high availability as well as scalability for Sun Ray clients. In addition, the reference implementation lets administrators store and manage thousands of virtual desktops on hundreds of physical servers from a single management console.

- Reliability

With less complex designs and no moving parts, Sun Ray devices contain fewer components that are likely to fail. Sun Ray thin clients can be simply replaced if needed, without the need to reload software, recover files, and configure network settings and user preferences.

## Chapter 3

# Software Installation and Configuration

This chapter describes the overall process for installing and configuring the VMware View Manager to provide Windows desktops to Sun Ray clients.

## Software Installation

Several software packages must be installed and running prior to connecting the Sun Ray Software and VMware View Manager. If the software is to be deployed in front of a working View Manager environment, some of the installations steps below may not be required.

1. Install the VMware ESX Server software. Detailed instructions can be found at [http://www.vmware.com/support/pubs/vi\\_pages/vi\\_pubs\\_35.html](http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html)
2. Install the VMware vCenter software. Detailed instructions can be found at [http://www.vmware.com/support/pubs/vi\\_pages/vi\\_pubs\\_35.html](http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html)
3. Install the VMware View Manager Connection Server. Detailed instructions can be found at [http://www.vmware.com/pdf/viewmanager3\\_admin\\_guide.pdf](http://www.vmware.com/pdf/viewmanager3_admin_guide.pdf)
4. Install Windows XP with the VMware View Manager Agent. Detailed instructions can be found at [http://www.vmware.com/pdf/viewmanager3\\_admin\\_guide.pdf](http://www.vmware.com/pdf/viewmanager3_admin_guide.pdf)
5. Install the Solaris 10 Operating System on a separate system or on a virtual machine. See [http://blogs.sun.com/acworkma/entry/how\\_to\\_install\\_solaris\\_10](http://blogs.sun.com/acworkma/entry/how_to_install_solaris_10) for instructions.
6. Install the Sun Ray Software. Instructions can be found at [http://blogs.sun.com/acworkma/entry/how\\_to\\_build\\_a\\_sun1](http://blogs.sun.com/acworkma/entry/how_to_build_a_sun1)

## Configure VMware View Manager

VMware View Manager settings need to be adjusted for the Sun environment. The following steps configure the software not to use the Secure Sockets Layer (SSL). If the environment requires the use of SSL, configure the system without SSL first, and then use steps in subsequent sections to enable the use of SSL.

1. Configure View Manager to accept non-SSL connections. Log into your View Manager administrative Web site.
2. Go to the *Configurations* tab.

3. Edit the global settings to turn *Require SSL* to *Off*. View Manager states the software needs to be restarted. Do not restart the software at this time.

The screenshot shows the VMware View Administrator interface. The 'Global Settings' tab is active, and the 'Require SSL for client connections' setting is set to 'No'. A blue arrow points to this setting. Other settings include 'Session timeout: 600 minutes', 'Reauthenticate after network interruption: No', 'Message security mode: Disabled', 'Direct connection for Offline Desktop operations: No', and 'Require SSL for Offline Desktop operations: No'.

4. Deselect *Require SSL* on the pop-up screen.

The screenshot shows the 'Global Settings' dialog box. The 'Require SSL for client connections' checkbox is unchecked, and a blue arrow points to it. Other settings include 'Session timeout: 600 minute(s) \*', 'Reauthenticate after network interruption' (unchecked), 'Message security mode: Disabled', 'Direct connection for Offline Desktop operations' (unchecked), 'Require SSL for Offline Desktop operations' (unchecked), 'Disable SSO for Offline Desktop operations' (unchecked), 'Display a pre-login message' (unchecked), and 'Display warning before forced logoff' (checked). The warning message is: 'Your desktop is scheduled for an important update and will be restarted in 5 minutes. Please save any unsaved work now.' The dialog box has 'OK' and 'Cancel' buttons.

- Change View Manager to use a direct connection rather than the default mode of tunneling the connection. On the *Configuration* tab in the View Manager Administrator, select the server and click *Edit*.

The screenshot shows the VMware View Administrator interface. The 'Configuration' tab is selected. The 'View Servers' section is expanded, showing a table with one server listed: 'DONAU'. The 'Edit...' button for this server is highlighted with a blue arrow.

Session Type	Current	Highest
Total Active	0	1
Active - Non linked clone	0	1
Active - linked clone	0	0
Offline	0	0

Name	Activation	Enabled Settings
✓ DONAU	Enabled	Smart card authentication: Optional

- Click on *Direct connection to desktop* on the pop-up screen.

The screenshot shows the 'View Server Settings' dialog box. The 'Direct connection to desktop' checkbox is checked and highlighted with a blue arrow. Below it, there is a note: 'This change will take effect on next login for each user.' Other options include 'Smart card authentication' (set to 'Not allowed') and 'RSA SecurID 2-Factor Authentication' (with sub-options for 'Enable', 'Enforce SecurID and Windows user name matching', and 'Clear node secret'). There is also a field for 'Upload RSA authentication agent configuration file (sdconf.rec):' with a 'Browse...' button. 'OK' and 'Cancel' buttons are at the bottom.

- Restart the View Manager service. The service can be found in the Windows Service Manager under the name VMWare View Connection Server.

## Install and Configure Sun Ray Connector for VMware View Manager

Once the View Manager and Sun Ray Software environments are running and configured, the two can be tied together.

1. Download Sun Ray Connector for VMware View Manager software to the Sun Ray server. The software can be found at [sun.com/software/sunray/get\\_addons.jsp](http://sun.com/software/sunray/get_addons.jsp)
2. Install the Sun Ray Connector for VMware View Manager software using the commands below. Be sure to accept the defaults. A message displays when the install process completes without error.

```
# unzip srvdm_1.0.zip
# cd srvdm_1.0

/* On x64 systems */
# pkgadd -d Packages/Solaris_10+/i386/

/* On SPARC systems */
# pkgadd -d Packages/Solaris_10+/sparc/
```

3. Configure the kiosk. The following steps use the Sun Ray Software Web interface to configure the Sun Ray Software to present Windows desktops.
4. Login to the Web administration port at <http://sun-ray-server:1660> using the username *admin* and the password assigned during software setup.
5. Click on the *Advanced* tab.
6. Click on the *Kiosk Mode* sub-tab. If Kiosk mode is being set up for the first time, a message displays about missing Kiosk Mode settings. Click the *Edit* button on the right. If Kiosk mode is configured already, skip to the next step.

The screenshot shows the Sun Ray Administration web interface. At the top, there is a header with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below the header, it shows 'User: admin Server: loghost' and the 'Sun Ray Administration' title. The main navigation area includes tabs for 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', and 'Log Files'. Under the 'Advanced' tab, there are sub-tabs for 'Security', 'System Policy', 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The 'Kiosk Mode' sub-tab is selected. A message box with an information icon (i) states: 'No Kiosk Mode Settings Exist in Sun Ray Data Store' and 'Click the Edit button to specify Kiosk Mode settings.' A blue arrow points to the 'Edit' button located at the bottom right of the message box.

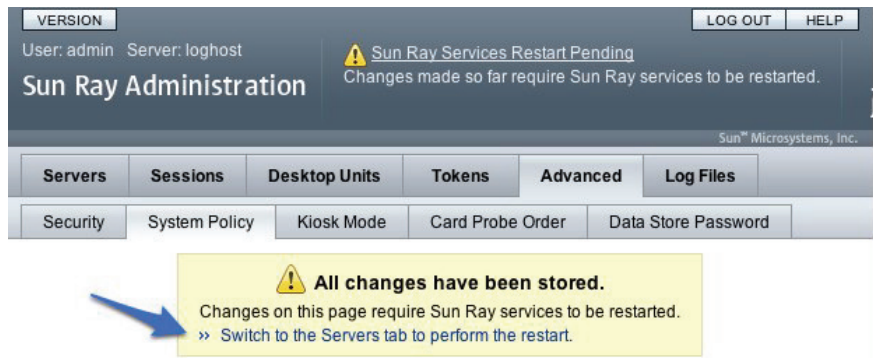
- Modify the session parameters. In the Sessions pull down, select *VMWare Virtual Desktop Manager Session*. Because we are going to start the configuration without SSL enabled, add `-http -s servername` in the arguments field and click *OK*.

The screenshot shows the Sun Ray Administration interface. The 'Advanced' menu is open, and the 'Kiosk Mode' sub-tab is selected. The 'Edit Kiosk Mode' dialog box is displayed, allowing configuration of session parameters. The 'Session' dropdown is set to 'VMWare Virtual Desktop Manager Session'. The 'Timeout' is set to 12000 seconds. The 'Arguments' field contains '-http -s donau'. The 'Default' value is '-s localhost -https -- -m'. 'OK' and 'Cancel' buttons are at the bottom right.

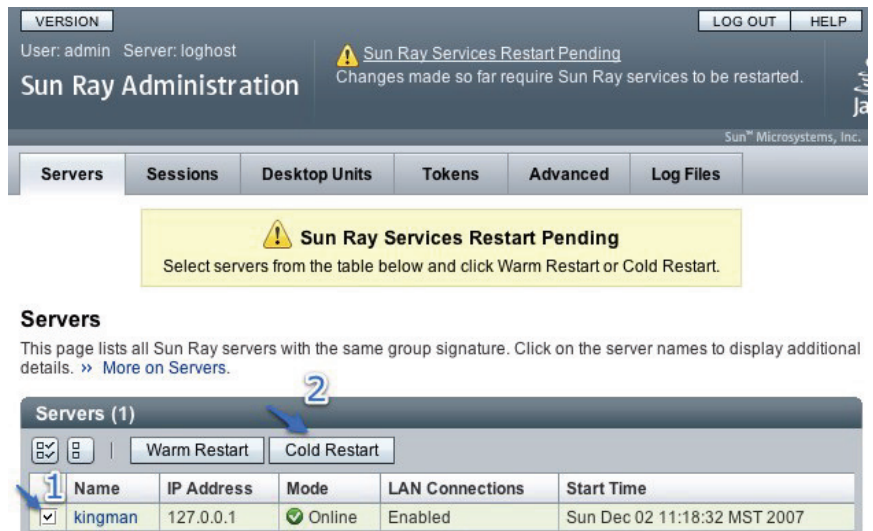
- Instruct the server when to use Kiosk Mode for card and non-card users. Click on the *System Policy* sub-tab on the *Advanced* menu. In the dialog box, check the *Enabled* box for Kiosk Mode for both card and non-card users.

The screenshot shows the Sun Ray Administration interface with the 'Advanced' menu open and the 'System Policy' sub-tab selected. The 'System Policy' page is displayed, showing configuration options for Card Users and Non-Card Users. Under 'Card Users', 'Access' is set to 'All Users' and 'Kiosk Mode' is checked 'Enabled'. Under 'Non-Card Users', 'Access' is set to 'All Users' and 'Kiosk Mode' is checked 'Enabled'. There are 'Save' and 'Reset' buttons at the top right.

9. Click *Save* when done. A message displays indicating the changes are stored.
10. Restart the server. Click on the link in the message dialog to switch to the *Servers* tab.



11. Select the server and click *Cold Restart*.



12. Enter your credentials into the View Manager login screen displayed on the Sun Ray device. Once logged in, the Windows desktop displays.

## Enabling SSL

The default SSL certificate that results from the VMware View Manager installation must be replaced in order to enable the Sun Ray Connector for VMware View Manager to connect to the system. Either a valid certificate must be put in place, or a self-signed certificate must be created. Failure to do so can result in hostname mismatch errors for VMware clients or connection errors for Sun Ray clients.

### Generate the Certificate

The following steps outline how to create a self-signed certificate. If a signed certificate exists, this step can be eliminated.

1. Start a command prompt on the VMware View Manager server.

2. Move to the `C:\Program Files\VMware\VMware View\Server\jre\bin` directory.
3. Execute the `keytool` command with the following options.

```
> keytool -genkey -keyalg "RSA" -keystore keys.p12 -storetype pkcs12
-validity 360
```

4. Answer the questions posed to create the certificate. Note that the first question asks for your name. Be sure to enter the server name as the reply, and make note of the password entered.

### Enable the Certificate

The next step in the process is to enable the newly created certificate.

1. Move the `keys.12` certificate just created from the `C:\Program Files\VMware\VMware View\Server\jre\bin` directory to the `C:\Program Files\VMware\View Manager\Server\sslgateway\conf` directory.
2. Create the `C:\Program Files\VMware\View Manager\Server\sslgateway\conf\locked.properties` file.
3. Add the following two lines to the `locked.properties` file. Be sure to replace `password` with the password created for the certificate.

```
keyfile=keys.p12
keypass=password
```

4. Restart the VMware View Manager Connection Server.
5. Look in the event log in the View Manager administration site for a line regarding the use of the `keys.p12` file.

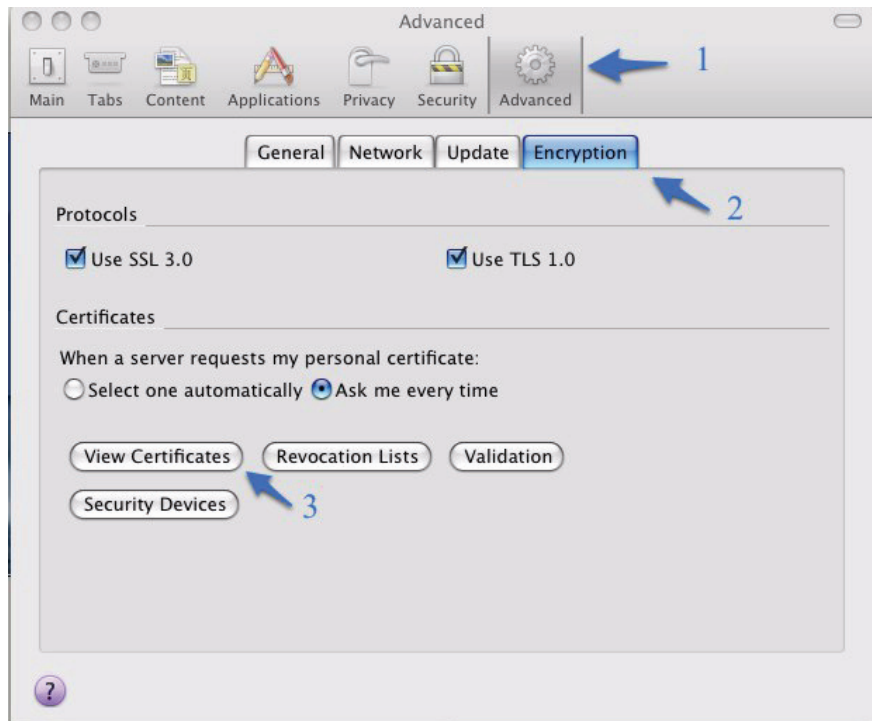
Message	Type	Time
Setting VC Poll Delay to 60000 ms (more ...)	Info	1/6/09 10:39:27 PM
Setting Missing VM Scan Delay to 60000 ms (more ...)	Info	1/6/09 10:39:27 PM
Scanner started (more ...)	Info	1/6/09 10:39:26 PM
Finished validating VMs (more ...)	Info	1/6/09 10:39:26 PM
Validating VMs (more ...)	Info	1/6/09 10:39:26 PM
User administrator has successfully authenticated to View Administrator (more ...)	Info	1/6/09 10:39:16 PM
AJP services are now ready (more ...)	Info	1/6/09 10:39:08 PM
Smart Card/Certificate Authentication will not be used (more ...)	Info	1/6/09 10:39:08 PM
Logging HTTP processor installed (more ...)	Info	1/6/09 10:39:06 PM
AJP services are now ready (more ...)	Info	1/6/09 10:39:06 PM
The Secure Gateway Server is listening on https://443 (more ...)	Info	1/6/09 10:39:07 PM
Smart Card Authentication mode: OPTIONAL (more ...)	Info	1/6/09 10:39:06 PM
The Secure Gateway Server is using SSL certificate store keys.p12 with password of 6 characters (more ...)	Info	1/6/09 10:39:05 PM
Setting chunkedResponseAcknowledged to 4 (more ...)	Info	1/6/09 10:39:04 PM
Setting maxUnacknowledgedDataSize to 307200 (more ...)	Info	1/6/09 10:39:04 PM
Changing message security mode to: OFF (more ...)	Info	1/6/09 10:39:04 PM
The Secure Gateway Server will be accessed using URL https://donau.wb.midwestco.com:443 (more ...)	Info	1/6/09 10:39:04 PM
The VDM Security Server subsystem is starting (more ...)	Info	1/6/09 10:39:03 PM
The VDM Broker subsystem is starting (more ...)	Info	1/6/09 10:39:02 PM
Plugin 'rs_invoke' - VDM Framework Java Diagnostics' loaded, version=3.0.0 build=127642, buildType=release (more ...)	Info	1/6/09 10:38:59 PM

6. Go back to the VMware View Manager site and use the Web interface to connect.

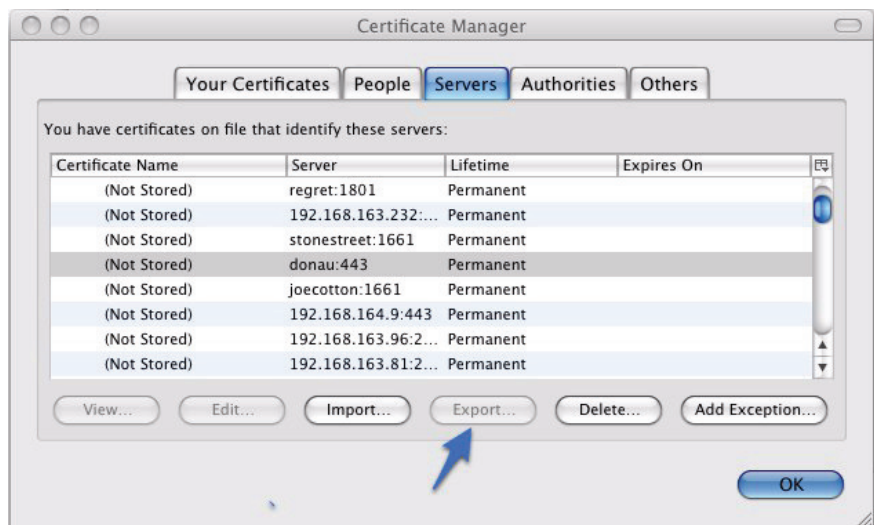
### Install the Certificate on Sun Ray Servers

Before the certificate can be imported into the system, it must be obtained and stored. This process involves exporting the certificate using a Web browser, such as Firefox. The export must be done while adding a security exemption in the View Manager administration site for the self-signed certificate.

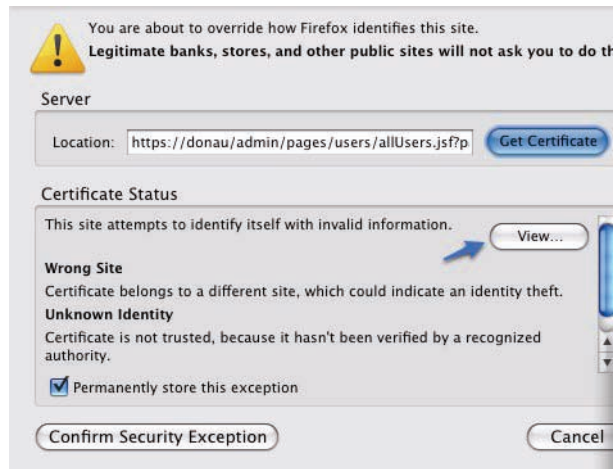
1. Go to Preferences in the Firefox Web browser.
2. Click on *Advanced*->*Encryption*->*View Certificates*.



3. Notice that the *Export* button is grayed out.



4. Click *Delete* and start the process over to obtain the certificate.
5. Return to the View Manager administration site once the certificate is deleted. A certificate error is displayed.
6. Click on *Add Exception*.
7. Click on *Get Certificate*.
8. Click the *View* button before confirming the exception.



9. Click on the *Details* tab and then push the *Export* button.



10. Name the certificate and save it.

11. Close the windows and confirm the security exemption to get back into the View Manager Web site.

Now that the certificate is obtained, it can be imported into Sun Ray servers.

1. Copy the saved certificate to the Sun Ray server using the `scp` command.
2. Run the `keytool` command to change the certificate the software uses to the saved certificate.

```
# keytool -import -file certificate -trustcacerts -v -keystore
/etc/opt/SUNWkio/sessions/vdm/keystore
```

3. Edit the `/etc/opt/SUNWkio/sessions/vdm/vdm` file and insert the certificate password. Line 17 includes the word `javaKeyStorePass`. Add the password for the certificate into the file.
4. Execute the following commands.

```
# sed 's/trustStore=$javaKeyStorePass
/trustStorePassword=$javaKeyStorePass /'
/etc/opt/SUNWkio/sessions/vdm/vdm > /tmp/vdm
# cp /tmp/vdm /etc/opt/SUNWkio/sessions/vdm/vdm
```

5. Restart the kiosk sessions on the Sun Ray server. Once rebooted, the Sun Ray Connector for VMware View login screen appears.

```
# /opt/SUNWut/sbin/utrestart -c
```

## Troubleshooting

In the event the software does not work as expected, look at the log messages located in the `/var/opt/SUNWut/log/messages` file. Error messages related to the software begin with `kiosk:vdm`. Table 3-1 describes key error messages and solutions.

Table 3-1. Key error messages and solution suggestions

Error Message	Description	Solution or Issue to Resolve
Error connecting to VDM server: javax.net.ssl.SSLException:java.lang.RuntimeException: Unexpected error: java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be non-empty	The SSL certificate is not set up correctly on the Sun Ray server.	<ul style="list-style-type: none"> <li>Follow the instructions at: <a href="http://blogs.sun.com/sjf/entry/setting_up_ssl_and_sun">http://blogs.sun.com/sjf/entry/setting_up_ssl_and_sun</a></li> </ul>
<p>This desktop is currently not available. Please try connecting to this desktop again later or contact your system administrator.</p> <p>The desktop sources for this desktop are not responding. Please try connecting to the desktop again later, or contact your system administrator.</p>	The desktop is not set up properly, or is already in use	<ul style="list-style-type: none"> <li>Someone is logged in the machine (over remote desktop or via the console in VMware vCenter). The machine is powering on/off or suspending.</li> <li>No free desktops exist for that user.</li> <li>The VDM tools are not installed on the desktop, or are not working correctly. Check that the desktop status is available in the VDM Web administration.</li> <li>Active Directory and/or DNS is not setup properly on the desktop.</li> <li>There is a network communication problem between the VDM server and the desktop.</li> <li>A Windows firewall is blocking connections to the desktop.</li> </ul>
Connection tunneling is required to connect to the desktop but it is not supported by this client.	Connection tunneling provides security across a WAN. It allows an encrypted connection from the client to the desktop, by tunneling it through the VDM server.	<ul style="list-style-type: none"> <li>Disable connection tunneling.</li> <li>For VDM 2/2.1, open the VDM Web administration, go to <i>Configuration</i>, and enable <i>Direct Connect to virtual desktop</i>.</li> <li>For View Manager 3, open the VDM Web administration, go to <i>Configuration-&gt;VDM Servers-&gt;Edit</i>, and enable <i>Direct connection to desktop</i>.</li> </ul>
Exception in thread "main" java.lang.NoClassDefFoundError	An incorrect version of Java software is in use.	<ul style="list-style-type: none"> <li>Install Java version 1.5.</li> </ul>
Desktop tries to open but immediately disconnects.	Desktop fails to open.	<ul style="list-style-type: none"> <li>Diagnose the problem further. Try to connect to the desktop manually from the Sun Ray Server using the <code>/opt/SUNWuttsc/bin/uttsc desktop-IP</code> command. A remote desktop connection to the virtual machine should open. If it fails, it can provide an error message with further information.</li> </ul>

## Chapter 4

# Best Practices for Deployment

Taking into account user and system requirements and following best practices can help ease deployment and foster consistent solution performance characteristics.

- Gather user, application, and operating system statistics to determine CPU, memory, disk, and network usage patterns and size systems appropriately. Decide whether to size systems for average or peak utilization rates.
- Consider the resources needed by different types of users and operating systems when determining how many concurrent users can be handled by a single server.
- Factor in capacity, I/O operations, and data throughput when estimating needed storage capacity and evaluating storage systems for use. Be sure to include the base size of the virtual machine (operating system, applications, and local data) and add capacity for page and log files and additional headroom.
- Plan the order in which desktops are virtualized based on performance metrics, hardware refresh rates, operating system upgrade plans for applications needs, and maintenance schedules.
- Optimize the image size of desktop golden images by adjusting operating system settings and application sets. Operating systems can be streamlined by removing unnecessary features. Application set sizes can be reduced by storing only a single copy that can be used by multiple users.
- Place user data on network-based file systems on centralized storage to simplify virtual desktop golden image update processes.
- Keep roaming profiles as small as possible by using folder redirection.
- Conserve computing resources by turning off graphical screensavers and GUI enhancements, and disabling COM ports and offline files and folders.
- Locate virtual machine swap files separately from snapshot files to mitigate performance degradation due to intensive disk activity and memory page swapping.
- Run virtualized environments on multicore servers to increase the number of virtual machines per host to support more users.
- Load balance session management layer and virtualization layer servers to further increase performance and scalability and provide additional fault tolerance.

## Chapter 5

# For More Information

Rapidly increasing performance, sophisticated applications, and the growth and exploitation of networks are changing the way people work. Hardware, software, and networking advancements are enabling geographically dispersed users to collaborate in real time, and mobile computing and communications technologies are enabling workers to take their virtual offices on the road. With the convergence of compact computing devices, ubiquitous communications, and changes to the IT infrastructure, remote computing is becoming mainstream.

The Sun Ray technology and VMware View Manager solution makes the concept of secure access to applications at any time, in any location, a practical reality. It brings together Sun and VMware technologies to deliver enterprise computing services to local and remote, desktop clients. It grants access to applications and services to qualified users, and gives organizations the ability to select the hardware, software, and services that best suit business needs. By centralizing administration, support, service provisioning and network management activities are significantly reduced, thereby lowering the cost of IT service delivery while creating a more agile and secure IT infrastructure.

### About the Authors

With over 10 years of experience in desktop solutions, David W. Fong, P. Eng. is a member of the technical enablement team in Sun's Global xVM Practice specializing in desktop virtualization. Before joining Sun, David was a Senior Systems Engineer with Tarantella. Prior to that, he held Channel Sales Manager, Consulting Engineer, and Product Development Manager positions with various companies.

With over 15 years of experience in practical application of information technology solutions, Adam Workman is a member of the Desktop Virtualization Team and the MySQL Technical Lead for Sun's U.S. Software Practice. Before joining his current team, Adam was a member of Sun's Global Systems Engineering team. Prior to that he was the Chief Architect for messaging systems for a major telecommunications provider.

Matthias Müller-Prove is a user experience architect for desktop virtualization at Sun. During 15 years in the industry, Matthias also worked on the user interface of the open source office suite OpenOffice.org, and shaped the Adobe GoLive Web editor. More information from Matthias can be found at <http://blogs.sun.com/mprove>.

### Acknowledgments

The authors would like to thank Stephanie Lewellen for her contributions to this article.

## References

Sun Ray Software:

<http://sun.com/software/sunray>

VMware View:

<http://vmware.com/products/view>

## Ordering Sun Documents

The SunDocs<sup>SM</sup> program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals through this program.

## Accessing Sun Documentation Online

The docs.sun.com web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is <http://docs.sun.com/>

To reference Sun BluePrints Online articles, visit the Sun BluePrints Online Web site at: <http://www.sun.com/blueprints/online.html>

**Sun Microsystems, Inc.** 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN (9786) **Web** [sun.com](http://sun.com)



© 2009 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Solaris, Sun BluePrints, Sun Ray, and SunDocs are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the US and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Intel Xeon is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. AMD and Opteron are trademarks or registered trademarks of Advanced Micro Devices. Information subject to change without notice. Printed in USA 03/09