VMware View Optimization Guide for Windows 7

OPTIMIZATION GUIDE

vmware® enSYNCH

Table of Contents

About This Guide

The following documentation provides a guideline on configuring a standard Windows 7 image to be used within a VMware View Infrastructure. This guide provides administrators with the information necessary to create a standard image of Windows 7 leveraging the Microsoft Deployment Toolkit or by utilizing a script-based approach to optimize a traditionally installed Windows 7 virtual machine. The recommended configuration settings optimize Windows 7 to help enhance the overall scalability and performance within a VMware View Virtual Desktop Infrastructure.

The first section of the paper will discuss the overall process of optimization and the optimization aids provided. In the next section, step-by-step procedural guidance is given for both methods of optimization. Afterward, the Windows 7 Operating System Customizations section provides background information on the specific optimizations and techniques used by the optimization aids. Finally, the Managing VMware View Desktops section provides guidance and considerations for optimizing the environmental aspects on an ongoing basis.

Process Overview

The goal of building your standard image and applying desired customizations can be accomplished in a number of ways. This guide provides two methods for IT organizations to utilize, each requiring a different level of effort and yielding different benefits. "Diagram 1" illustrates the workflow of both methods.

Traditional Install Method
A traditional install can be optimized with a minimum set of tools, and requires very little effort to create a standardized and optimized process for customizing a Windows 7 virtual machine. Administrators create the virtual machine with the specified parameters, load the operating system from media, and then apply optimizations through the use of a command script, Commands.bat, attached to this guide (distributed as a choice of CommandsPersonaManagement.txt or CommandsNoPersonaManagement.txt) and provided in Appendix B.

Microsoft Deployment Toolkit Method
The Microsoft Deployment Toolkit (MDT) provides a framework to build and maintain a defined process that is modular and applicable to both physical and virtual desktops. The benefits of this solution are driven from the prescriptive guidance and repeatable processes included in the tool to build and maintain standardized images. While you may invest more time up front when using this method, there are long-term advantages. In many cases, an IT organization may already use some of the tools and processes described. This method involves leveraging the MDT and Windows Automated Installation Kit (WAIK) to create a standard image build and customization process that leverages a robust Task Sequence engine. You can use the MDT approach to automate application installation, manage driver injection into different operating system versions, and use a GUI to create system builds and customize events.

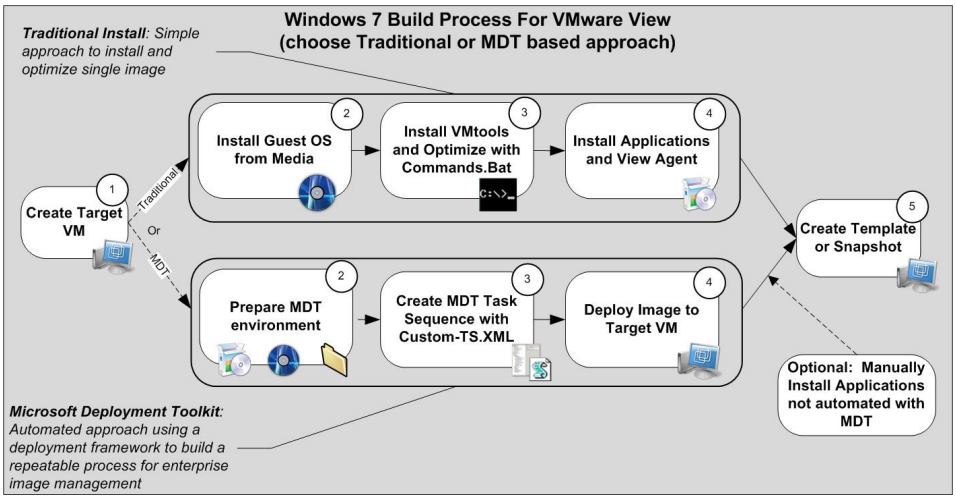


Diagram 1

Optimization Aids Provided

This guide provides two mechanisms to optimize the Windows 7 image. As shown in Diagram 1, customers have the choice of leveraging a script file or the MDT to implement the customizations. While these optimization aids contain recommended configurations, IT organizations should investigate and determine their benefit, as there is sometimes a trade-off between productivity and optimization. Review Appendix A, which lists all of the optimizations where an asterisk ('*') has been used to highlight discretionary changes. You should review these for applicability to your organization's specific use cases.

Commands.bat

The Commands.bat is a script file that can be executed manually or by using an automated scripting mechanism. The script utilizes standard operating system mechanisms to manipulate the registry using REG syntax, adjust services using PowerShell, and optimize other miscellaneous items such as Scheduled Tasks. The exact syntax is provided in Appendix B. The script is distributed as a choice of CommandsPersonaManagement.txt or CommandsNoPersonaManagement.txt, included as an attachment to this guide. (You can save the commands text file by going to the Adobe Reader View menu, selecting Navigation Panels, Attachments, and then Save As. After saving, rename to Commands.bat.)

If you are implementing View Persona Management, use the text file called CommandsPersonaManagement.txt. If you are not implementing Persona Management, use the text file called CommandsNoPersonaManagement.txt.

If you have an existing desktop image without Persona Management, and you wish to deploy Persona Management on that desktop image, create a BAT file on your virtual machine template from the supplied CommandsDesktopsReadyForPersonaManagement.txt file. Run this script as Admin (right-click > Run as Administrator). Reboot the computer when the BAT file completes. For details of the script, see Appendix C.

Microsoft Deployment Toolkit and TS.xml

The TS.xml file is used by the Task Sequence engine of the MDT. Replacing the default TS.xml with the one provided with this guide will provide a GUI interface for viewing and editing the recommended customizations. The customizations included in the provided TS.xml are equivalent to the Commands.bat script file mentioned above. The TS.xml file is referenced in Appendix D and included as an attachment to this guide. (You can save the TS.xml by going to the Adobe Reader View menu, selecting Navigation Panels, Attachments, and then Save As.)

Procedure for Creating an Optimized Windows 7 Image

Administrative Rights for Users

It should be noted that the methods and optimization aids provided in this guide will customize the parent virtual machine, upon which end users' desktops will be based. However, these optimizations can be "undone" if end users have administrative rights to start services and modify the registry. For this reason, it is important to reinforce these settings via GPOs for control of desktops for which end users have administrative rights.

Administrative Note on Image Version Tracking and Managing Windows 7 Updates

Optimizing the operating system configuration is an iterative process. As images progress through the normal life cycle, it can become difficult to determine which image configuration and subsequent optimizations a particular VMware View guest virtual machine is leveraging. As VMware View desktops are updated using the View Composer Recompose and Refresh, the virtual machines are linked to parent virtual machines and snapshots. Careful management of snapshot names allows some track-back ability, but an identifier in the operating system can also be used for identification using script or system management processes. For this reason, add an additional registry setting to track the version of an image, as well as any other helpful information an organization may find useful (version, date, type, author, and so on). The modifications provided in the TS.xml and Commands.bat file include a marker key in HKEY Local Machine\Software\Image for this purpose.

Applying Windows Updates is an important step in the process to ensure that your parent virtual machine stays as up to date as possible. It is recommended that the "Windows Update" service be set to "Disabled" by default to avoid pulling updates down to virtual machines in your View environment once they are deployed. The custom Task Sequence provided with this document applies all applicable Windows Updates that are available at the time the target virtual machine is built and subsequently disables the Windows Update Service to avoid your View virtual machines from downloading updates from Microsoft. It is considered a Best Practice to manage your updates for your virtual machines on the parent virtual machine and recompose that virtual machine to update all linked clones. To apply updates manually to your parent virtual machine, re-enable the Windows Update service, and run Windows updates or apply updates leveraging your enterprise patch management process.

Creating the Target Virtual Machine

The initial virtual machine parameters create a virtual hardware profile, which will be used for subsequent virtual machines. You can convert an existing physical or virtual machine using VMware Converter, but it is best to create a new virtual machine using the Virtual Infrastructure Client. Administrators can use the built-in VMware vCenter™ wizard to create a new virtual machine or select the parameters on their own. Specific recommendations are listed in the following table.

Virtual Machine Parameters Table

PARAMETER	COMMENTS
Guest Operating System	Microsoft Windows 7 (32-bit or 64-bit)
SCSI Controller	LSI Logic SAS or Parallel

PARAMETER	COMMENTS
Hard Disk	Disks for Templates or parent virtual machines can utilize Thin Provisioning
Video Card	No need to specify as settings are provided by View Manager
Floppy	Remove the floppy drive
CD/DVD	Set to Client Device Used for VMware Tools install, Windows 7 ISO, or Windows PE boot ISO with MDT
NIC Adaptor Type	VMXNET 3. Apply the Microsoft hotfix patch (see the VMware View Administration guide).
Memory Specs	32-bit, 1 – 3GB (no more than 3GB); 64-bit, 1 – 4GB (depends on use case)
Bios - Disable Ports	Go to the Options tab of virtual machine properties and select force entry into bios to disable unnecessary LPT and COM ports

Virtual Machine Parameters Explained

Disk Controller

VMware recommends using the LSI Logic SAS or Parallel controller for Windows 7 virtual machines.

NIC Type

The Network Interface Card (NIC) needs to be VMXNET 3. Failure to set the proper NIC type prevents Windows PE from correctly acquiring an IP address and gaining access to the network for resources required during imaging. The traditional install method uses the VMXNET 3 virtual network adaptor to provide the most efficient networking stack for Windows 7. Apply the Windows hotfix (see the VMware View Administration guide).

Video Parameters

Setting specific video parameters of the video card is not necessary in the virtual machine properties. Leave the video card settings at Auto-detect video settings. The values used for video memory will be set and managed by VMware View Manager.

Memory Specifications

For Windows 7 x86, no more than 3GB of memory should ever be allocated. Memory specifications are dependent upon the supporting virtualization infrastructure. However, you should provide at least 1GB of memory to the standard virtual machine template leveraged for Windows 7. 2GB of memory would be ideal and provide for more bursting of memory when needed for heavier end-user applications. This setting is completely dependent upon the environment and use case scenarios. Sufficient use case mappings should be done to determine the optimum memory settings for your organization.

Choosing Your Windows 7 Installation Method

At this point in the guide, administrators should determine whether to do a traditional installation (proceed to "Traditional Install" section) of Windows 7 by mounting the media to the virtual machine, or to utilize the MDT (proceed to "Using the Microsoft Deployment Toolkit to Optimize Windows 7" section) for installation of Windows 7 into the target virtual machine.

Why Use the Microsoft Deployment Toolkit 2010?
The MDT can best be described as a collection of scripts and processes that supports a defined framework to create a standard, repeatable, and flexible image for an organization. This approach creates a prescriptive and standardized build process. The benefits are summarized below.

- **Flexible:** Enable, disable, or build on logic when certain commands are executed, depending upon existing scenarios.
- **Easy:** The Task Sequencer provides pre-built components for adding reboots, partitioning, command lines, and other logic, all within an intuitive GUI interface.
- **Updatable:** As drivers, applications, and other updates are needed within the standard build process, the Task Sequencer can be updated in a point-and-click configuration for all new image builds in one interface.
- **Cross Platform:** The same MDT framework can be leveraged for both virtual and physical machine builds.

Note: Proceed to the "Using the Microsoft Deployment Toolkit to Optimize Windows 7" section if you wish to follow that method.

Traditional Install of Windows 7

The following section outlines the process for a traditional install of Windows 7 using an ISO image mounted on a datastore accessible by the target virtual machine. After the installation of the operating system is complete, Commands.bat is used to optimize the configuration. Installation of applications and the VMware View Agent can either be performed automatically or manually.

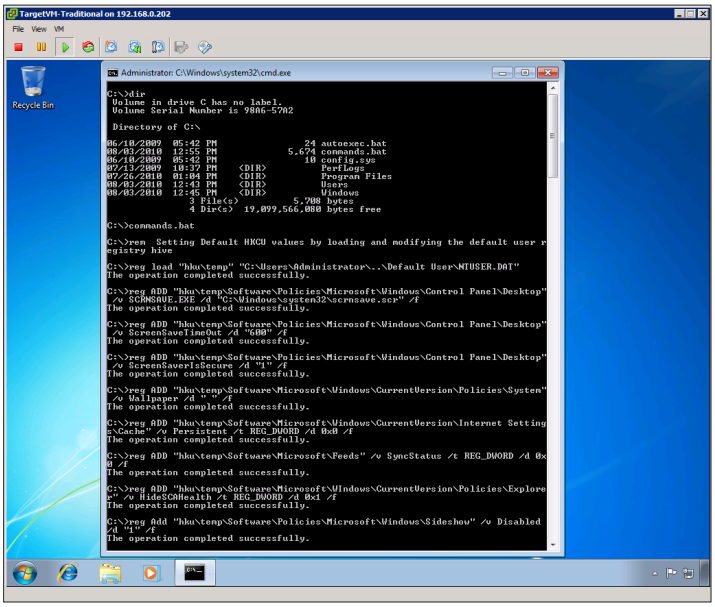
Install Guest OS from Media

1. Ensure that the CD/ROM device is set to **Connect at Power on** and directed to the Windows 7 ISO image.
2. Connect to the virtual machine console and answer the prompts for the operating system Setup Wizard.
3. Restart as necessary.
4. Remove any unnecessary components from the operating system; for example, Tablet PC components.

Install VMware Tools and Optimize with Commands.bat

1. Once the operating system installation is complete, perform Windows Update as necessary.
2. From the virtual machine console menu or from VMware vCenter, initiate and complete the installation of VMware Tools.
3. Restart as necessary.
4. Use the Adobe attachment panel to save and copy the Commands.bat included with this guide to the local OS, and execute or run from a network share. Monitor the command window to ensure the commands complete successfully.

5. Restart to affect the changes in Windows services.



Install Applications and VMware View Agent

1. Install applications as needed in the base image.

   You can either join the Active Directory domain or not to install applications. If you do not join the domain, mount the application installers on a protected share outside the domain so that you can load them while not in the domain.

2. Install the VMware View Agent manually or utilize a silent installation command as provided, substituting the appropriate values.

   For example: `VMware-viewagent.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1 ADDLOCAL=ALL"`

3. Restart as necessary.

4. In vCenter, edit the properties of the virtual machine to disconnect the installation media and remove the CD/DVD Drive from the virtual machine.

Note: For more information on how to install the VMware View Agent, please refer to the section "Install View Agent Silently" within the VMware View Administrative Guide.

Proceed to the "Using the Target Virtual Machine to Create VMware View Desktops" section.

Using the Microsoft Deployment Toolkit to Optimize Windows 7

The MDT 2010 is a free toolkit provided by Microsoft to organizations wishing to build and deploy a standard image in a Lite-Touch process. The toolkit enables organizations to standardize and automate the process of creating golden master images.

Using Windows System Image Manager with the MDT

Some organizations may already be leveraging the Windows System Image Manager to customize their Windows 7 images via the unattend.xml. This is most often done through the MDT framework and can be integrated into this process. Some of the settings referenced in this document can be accommodated through that tool and applied directly to the unattend.xml file if desired. For more information on the features and capabilities of WSIM, please reference the following URL. http://technet.microsoft.com/en-us/library/cc722301%28WS.10%29.aspx

Prepare the Microsoft Deployment Toolkit 2010 Environment

Preparation of an MDT environment may require the creation of a separate virtual machine that utilizes the MDT, WAIK, and the customized TS.xml included with this guide. This section covers the MDT installation, creating the Deployment Share, staging the OS media, and injecting drivers from VMware Tools into the image. The deployment share is used for storing all the standard configurations and customizations leveraged for building a Windows 7 image. This process was tested on both MDT 2010 and MDT 2010 with Update 1.

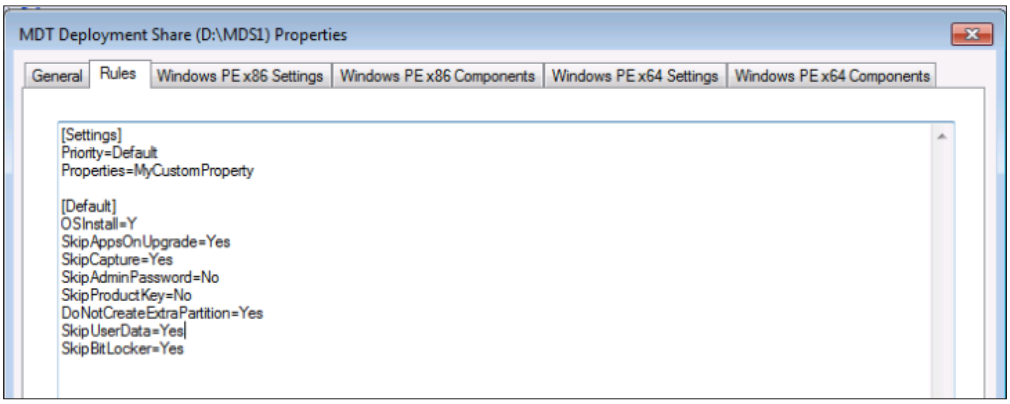
1. (Optional) Create a separate virtual machine for the MDT, unless an MDT environment already exists.
2. Review the system requirements and ensure that the system being leveraged meets the minimum: http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en#Requirements

   Note: Check the Solution Accelerators site for the latest links and information on MDT: http://technet.microsoft.com/en-us/solutionaccelerators/dd407791.aspx
3. Download and install the Windows Automated Installation Kit, latest PowerShell version, and the appropriate version of the MDT for your operating system (x86, x64) from the link above.

   Note: Pay close attention to the installation directory for MDT during the install, and ensure it is on a drive with sufficient space to hold images, source media, and any line of business applications needed for your standard image.
4. Once the installation for MDT is complete, launch the Workbench by going to the Start Menu and navigating to **Start > All Programs > Microsoft Deployment Toolkit** and selecting **Deployment Workbench**.
5. Validate that all required components are installed by navigating to **Information Center > Components** within the Deployment Workbench and ensuring that any item marked with **Required** in the **Status** column is showing under the Installed section.

   Note: Components can be downloaded and installed from inside the Workbench if not already installed.
6. Next, navigate to the node **Deployment Shares** within the Deployment Workbench, right-click and select **New Deployment Share**.
7. Name the Deployment Share, e.g., MDS1. Defaults can be leveraged for this wizard, but pay close attention to **Deployment Share Path** to ensure you are placing your source files in a location with sufficient space. If you selected an OS drive for the installation of the MDT, during this step you should select a data volume (non-boot partition) to store deployment data.
8. Select **Deployment Share**, just created, and click **Properties**. On the Rules tab, add or edit the following lines and click **Apply**. These settings will streamline the process of building the Target Virtual machine.

   ```
   SkipCapture=Yes
   SkipUserData=Yes
   SkipBitLocker=Yes
   DoNotCreateExtraPartition=Yes
   ```
   (This line prevents adding the 100-300MB system partition for BitLocker)



Staging OS Media

This section describes the process of importing Volume License source media for Windows 7. In order to build the initial Windows 7 image, source media needs to be obtained and imported into the Deployment Workbench.

1. To import Volume License media for Windows 7, navigate to **Deployment Shares > MDT Deployment Share > Operating Systems**, right-click **Operating Systems**, and select **Import Operating System**.
2. Select **Full set of source files** and click **Next**.
3. Mount the Windows 7 ISO to the MDT virtual machine or point to a network location that houses the extracted Windows 7 source files. The media will be validated on import to ensure files at the root directory represent an install source for Windows 7.
4. You can select **Move the files to the deployment share instead of copying them**. This is useful if you are leveraging a virtual machine for your MDT server and want to avoid copying data, as moves are instant and copying could take several minutes. Select **Next** to continue.
5. The destination directory is the directory that will be created under the directory **Deployment Share\ Operating Systems**. Name the directory, and select **Next** through the remaining screens to finish the import; for example, **OS-Win7forView**.

Importing Drivers into the Workbench to Support VMware Virtual Machines

In order to successfully connect to the network and see storage when booting to Windows PE, NIC and storage drivers may need to be imported into the workbench. Once drivers are imported, they will be injected into the Windows PE boot media when the Deployment Share is updated (discussed in a later step).

1. Locate the drivers by browsing to the VMware Tools drivers directory on an existing Windows 7 or Server 2008 virtual machine installed with VMware Tools. Ordinarily the directory is located at: `C:\Program files\VMware\VMware Tools\Drivers`.
2. Copy the Drivers directory to a location that can be accessed from the virtual machine running MDT. We are specifically concerned about **Network** and **Storage** (virtual machinexnet and scsi directories, respectively).
3. Next, within the Deployment Workbench, navigate to **Deployment Shares > MDT Deployment Share > Out-of-Box Drivers**, right-click **Out-of-Box Drivers**, and select **Import Drivers**.
4. Point to the directory containing the VMware drivers, and select **Next** to import the drivers into the Deployment Workbench.

   Note: This process automatically interrogates the .inf and .cab files to locate the appropriate driver files that are required and imports them.

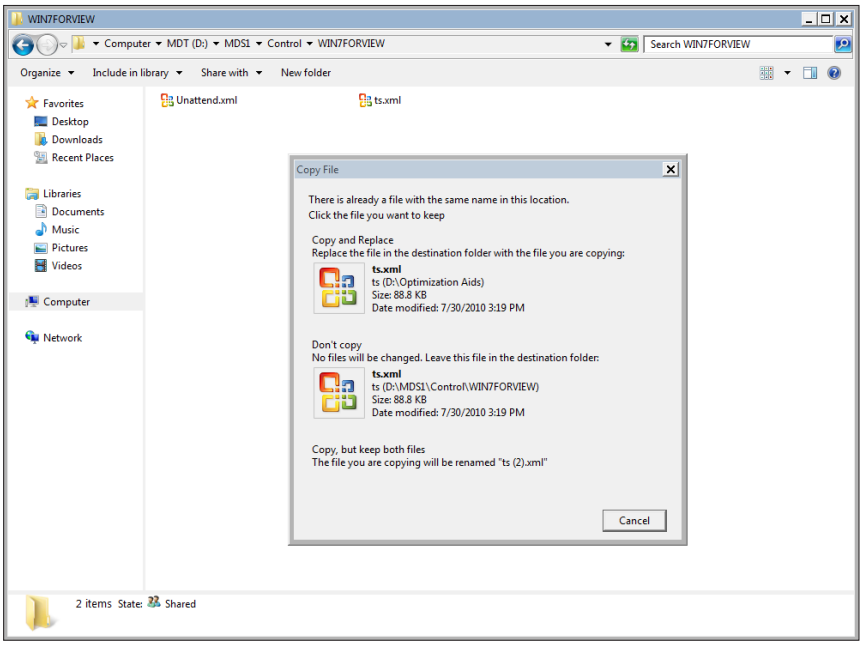
Create a Custom Task Sequence with TS.xml

This section discusses leveraging the MDT to create a Task Sequence. A Task Sequence is a series of commands combined together to create an automated process directly from inside the Deployment Workbench interface. The primary benefit of this process and strategy is to generate a repeatable process that is easily updated as the environment changes. This process also removes much of the manual effort required in generating a customized image for a VMware View environment. The steps that follow step through the process of creating a Task Sequence for the Windows 7 operating system image, then utilizing the TS.xml file included in this document to import a customized Task Sequence that optimizes this image for VMware View environments.

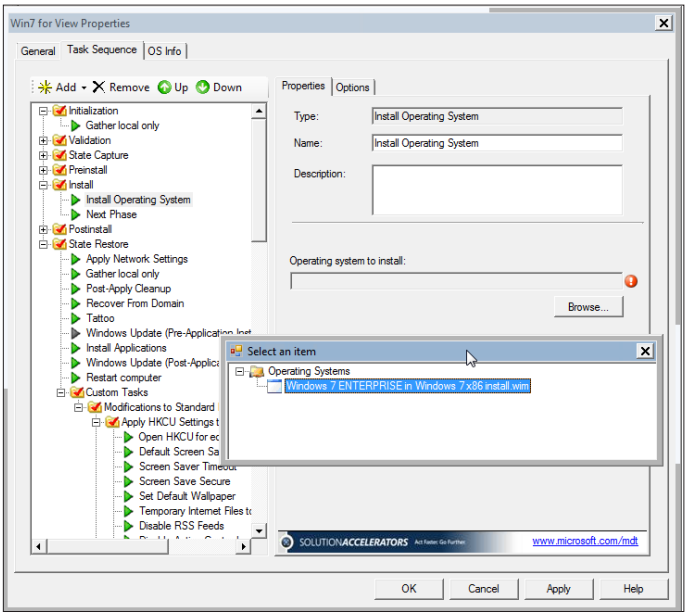
1. Within the Deployment Workbench, navigate to **Deployment Shares > MDT Deployment Share > Task Sequences,** right-click **Task Sequences** and select **New Task Sequence**.
2. Enter a **Task Sequence ID**. This ID needs to be unique and will determine the directory name that gets created with customizations in the `\\MDT\MDS1\control` folder.

   Example: Using Win7forView as the Task Sequence ID will create the directory `\\MDT\MDS1\control\Win7forView`
3. Next, enter a **Task Sequence name**. This name needs to be unique and will be the name that shows up in a list of Task Sequences to choose from when building the golden image. Click **Next**.

   Example: Use Win7forView as the Task Sequence name.
4. Select **Standard Client Task Sequence** and click **Next**.
5. Select the operating system that you imported in a previous step described in the "Staging OS Media" section. Click **Next**.
6. Answer the remaining questions, and finalize the Task Sequence definition.
7. **IMPORTANT:** Replace the default TS.xml (created in the Win7forView custom task sequence directory) with the customized TS.xml attached to this guide. Use the Adobe attachment panel to save and copy the customized TS.xml to the correct location, for example, \\MDT\MDS1\control\Win7forView.



8. Return to the Deployment Workbench, select the Task Sequence, and right-click to see the properties. Select the Task Sequence tab (you will receive an error.) Click OK, then navigate to **Install > Install Operating System** and set **Operating System to Install** to your imported OS media referenced in the "Staging OS Media" section.



9. The final part of this process is ensuring the Deployment Share is updated. This step generates the boot image that will be used for booting to Windows PE and initiating the OS Build. To update the **Deployment Share, navigate to Deployment Shares > MDT Deployment Share**, right-click **Deployment Share**, and select **Update Deployment Share**.

10. Select **Next** and **Next** to start the process of updating the Deployment Share.

Customize the "Win7forView" Task Sequence (optional)

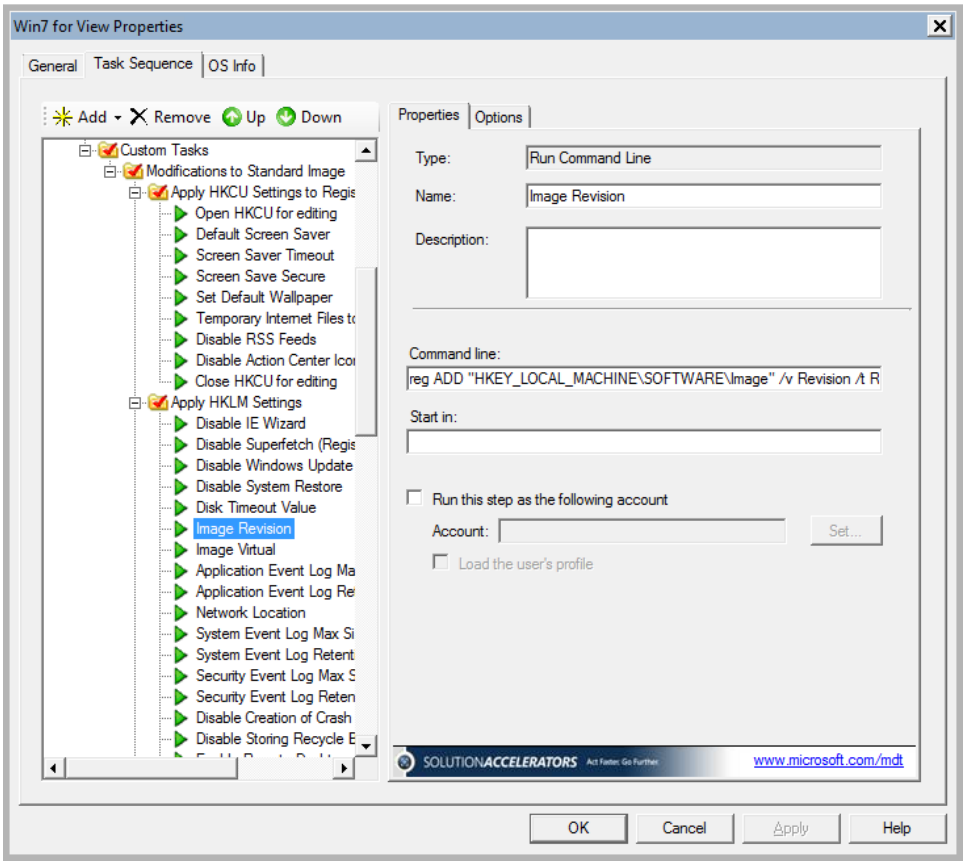
Customizations done to the registry, services, applications, and so on can be applied programmatically to a Windows 7 image through the Task Sequence process of the MDT. This white paper documents the configurations that customize HKCU (Current User Settings), and HKLM (Computer Local Machine Settings), as well as those service states that need to be **disabled**. All these changes can be programmatically applied through the Task Sequencer. The TS.xml file provided with this white paper creates a starting point for moving forward with different customizations.

Note: This section discusses the process of implementing your own configuration changes directly in the MDT Task Sequencer (optional).

1. Within the Deployment Workbench, navigate to Deployment Shares > MDT **Deployment Share > Task Sequences**, right-click **Task Sequences**, and select **Win7ForView**. Right-click **Task Sequence** to modify in the right-hand pane, and select **Properties**.

2. Select any of the recommended customizations and enable, disable, or change the settings by editing the **Properties** tab. Additionally, you can add tasks or settings that are particular to your environment to the appropriate phase. These changes will be written to the TS.xml file and become part of the standardized build process.

3. You can add a custom task, using the Task Sequence editor to navigate to the **State Restore > Custom Tasks** section. With **Custom Tasks** highlighted, click **Add** and navigate to **Add > General > Run Command Line**. This option provides the ability to run command lines during OS installation.



Here is a screenshot that illustrates how a custom task is utilized to run a command line-based customization.

Installing Applications with the Microsoft Deployment Toolkit

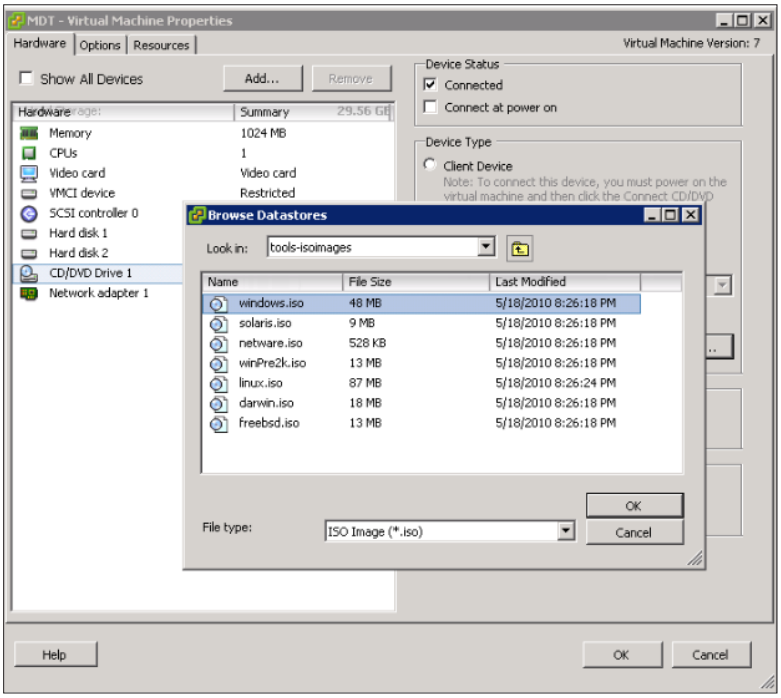
The decision to include or not include software packages into a standard image depends upon the organizational need and strategy for application deployment and management. It may be beneficial to create a custom image with the packages already coupled into the image. The MDT can accommodate existing packages that have been created within your organization and enable them to be deployed using a Task Sequence to a standard image. Ideally, these packages would be silently deployable and created leveraging MSI technology (in cases where HKCU application-specific settings need to be included).

The MDT provides the ability to deploy software to a target system during OS deployment as long the installation supports silent switches. The process detailed below will add VMware Tools and VMware View Agent as applications to be used later by a Task Sequence for automated installation:

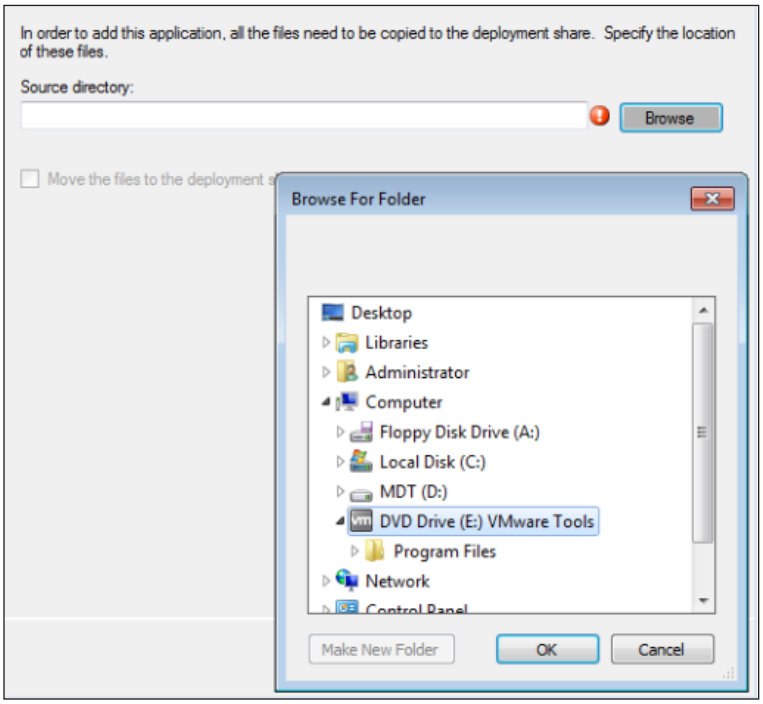
Note: The order that you add applications is important as the task sequence will by default install them in the same order they were added. VMware Tools must be added first as it is required for the View Agent to be installed correctly.

1. Within the Deployment Workbench, navigate to **Deployment Shares > MDT Deployment Share > Applications**, right-click **Applications** and select **New Application**.
2. Select **Application with source files** and click **Next**.

3. Provide details about the VMware Tools and click **Next**.
   a. Publisher: VMware
   b. Application Name: VMware Tools
   c. Version: 4.1
   d. Language: English
4. Select your source directory by mounting the Windows.ISO to the MDT virtual machine.
   a. Mount the Windows.ISO by browsing the Datastores to \vmimages\tools-isoimages and click **Connected**



b. **IMPORTANT:** Select the root of the drive where Windows.ISO is mounted



5. Specify the name of the directory that will be created within your Deployment Share.

   Example: VMwareTools

6. Specify the command line and click **Next**.

   Example: `: msiexec /i "VMware Tools.msi" /qn /norestart`

7. Click **Next and Finish** to complete the process.

8. Select the VMware View Tools application, right click to view **Properties**, select the **Details** tab, and place a check on **Reboot the computer after installing this application**.

Follow a similar process to add the VMware View Agent application.

1. Within the Deployment Workbench, navigate to **Deployment Shares > MDT Deployment Share > Applications**, right-click **Applications** and select **New Application**.

2. Select **Application with source files** and click **Next**.

3. Provide details about the VMware View Application and click **Next**.

   a. Publisher: VMware

   b. Application Name: View Agent

   c. Version: 4.5

   d. Language: English

4. Select your source directory and click **Next**.

   a. Browse to the location of the VMware View Agent application

5. Specify the name of the directory that will be created within your Deployment Share.

   Example: VMwareViewAgent45

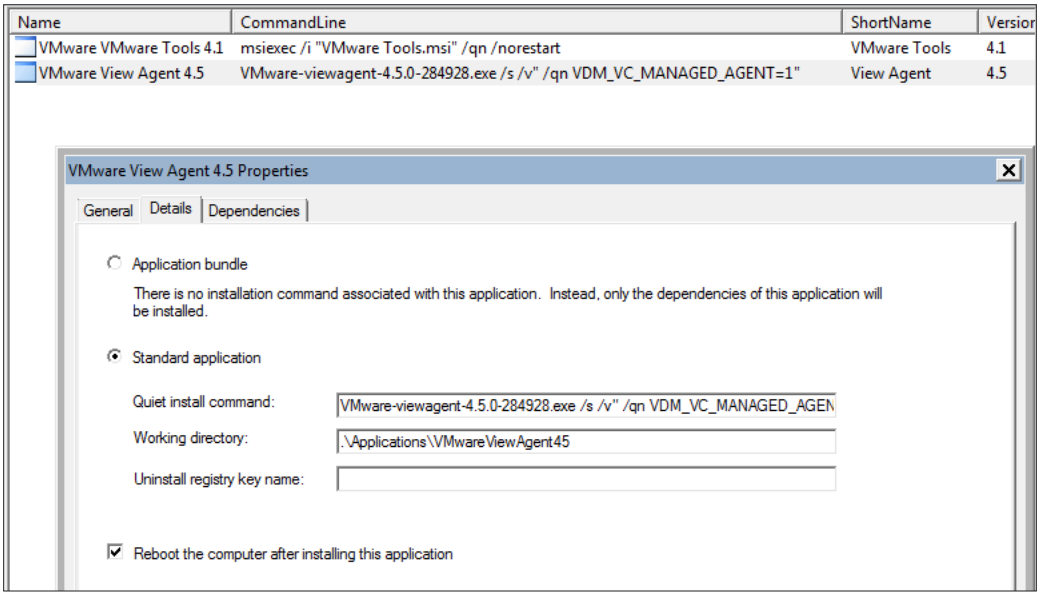
6. Specify the command line.

   Example: `VMware-viewagent-BUILDXXXXX.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1"`

7. Click **Next** to complete the process.

8. Select the VMware View Agent application, right click to view Properties, select the Details tab, and place a check on Reboot the computer after installing this application.

Note: For more information on how to install the View Agent, please refer to the section titled "Install View Agent Silently" within the VMware View Administrative Guide.



Deploy the "Win7 for View" OS Instance into the Target Virtual Machine

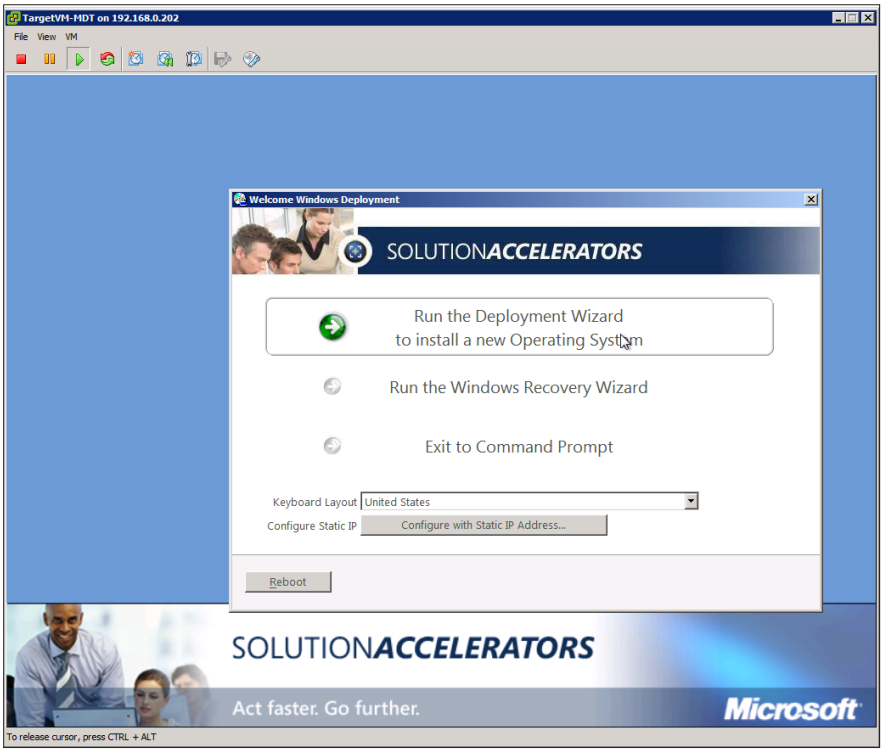
The following section describes the process for deploying the customized image into the target virtual machine. Now that the Deployment Share has been updated and the Task Sequence for the build has been prepared, it is time to deploy the OS instance into the target virtual machine and apply the optimizations.

1. From the MDT virtual machine, copy the appropriate Lite-Touch PE ISO (x86 or x64) from the deployment share (D:\DeploymentShare\Boot) to a datastore that can be utilized by the target virtual machine.

2. From the target virtual machine created in the earlier section, modify the CD/DVD properties to locate and connect at power on the appropriate platform Lite-Touch PE boot CD.

3. Boot your virtual machine from the bootable media selected above.

4. Select **Run the Deployment Wizard**, enter credentials to connect to the Microsoft Deployment Share, and then press **Enter**.



5. Select the Win7 for View Task Sequence and click **Next**.
6. Enter Product Key information.
7. Specify a computer name and click **Next**.
8. Select **Join a Workgroup**.

   Note: VMware View Composer or vCenter customization will join the virtual machine to the domain at a later time.
9. Click **Next** on **Language** and other preferences.
10. Select **Time Zone** and click **Next**.
11. Click to Select both the “VMware Tools” and “View Agent” application from the Application Install Window.
12. Enter **Administrator Password** to be used for logon after restart.
13. Click **Next** to begin the process of installing the operating system. The virtual machine will restart as necessary and provide visual updates as it progresses through the various stages.
14. Right-click on the target virtual machine in vCenter and under the Guest submenu, install VMware Tools, then shutdown the virtual machine.
15. In vCenter, edit the properties of the virtual machine to disconnect the WinPE bootable ISO, and remove the CD/DVD Drive from the virtual machine.

Using the Target Virtual Machine to Create VMware View Desktops

At this point, the target virtual machine will be an optimized Windows 7 installation that is ready to be utilized in the VMware View environment. When utilizing this image for full- or linked-clone pools in VMware View, the operating system will need to be customized to generate a unique instance for each user. This customization can be accomplished using sysprep, using VMware vCenter customizations settings, or with the QuickPrep tool used by VMware View Manager.

Preparation of the Parent Virtual Machine

1. To utilize this virtual machine as a parent virtual machine for full clones, you will need to power down the virtual machine and then convert it to a template. Administrators can then select this virtual machine through View Manager as the parent virtual machine for a full clone desktop pool.
2. To utilize the target virtual machine as a parent virtual machine for linked clone pools, you must run ipconfig/release, power down the virtual machine, and then create a snapshot. For linked clone-based pools, administrators will select the parent virtual machine and then the specific snapshot for creating or recomposing desktop pools.

Note: See the VMware View Administrator Guide for specifics on preparing the parent virtual machine for creation of desktop pools.

Windows 7 Operating System Customizations

The following modifications are provided as recommendations for how to optimize the configuration of the Windows 7 operating system in a VMware View Virtual Desktop Infrastructure. Appendix A provides a complete reference of the recommended customizations, and lists the methods available for implementation (GPO, registry, service, command line).

Note: If you apply customizations to the master image, they are persistent only if users cannot change them. If individual users have administrative rights, they can override these customizations. To preserve your customizations, modify the desktops by GPO so that the customizations are enforced. Refer to *Appendix A* for the list of customizations that can be set by GPO.

Windows 7 Service Modifications

The following table outlines the recommended state of services for a Windows 7 virtual machine. Even if a service is by default configured as manual, you should still disable the service to avoid any potential issues. These services can all be disabled in your initial image prior to capturing. You should analyze each service for applicability within your corporate environment. Some services detailed below (for example: Themes) may actually be desired and left at default values. Discretionary changes are marked with an asterisk ('*').

Windows 7 Services Parameters Table

SERVICE	DEFAULT	STATE	COMMENTS
BitLocker Drive Encryption Service	Manual	Disable	Not recommended to encrypt VDI virtual machines
Block Level Backup Engine Service	Manual	Disable	Leveraged for backing up data on a workstation
*Desktop Window Manager Session Manager	Auto	Disable	Disable if Aero is not necessary / desired
Disk Defragmenter	Manual	Disable	Provides disk defragmenting services for hard drives and can impact performance if run on a virtual machine
Diagnostic Policy Service	Auto	Disable	Problem detection and troubleshooting resolution
Home Group Listener	Manual	Disable	Leveraged for Home Networking
Home Group Provider	Manual	Disable	Leveraged for Home Networking
*IP Helper	Auto	Disable	Disable if IPv6 is not leveraged
Microsoft iSCSI Initiator Service	Manual	Disable	Not needed for virtual machines

SERVICE	DEFAULT	STATE	COMMENTS
Microsoft Software Shadow Copy Provider	Manual	Disable/ Enable	Leveraged by the VSS for backups. Disable if you are not using System Restore and not using View Persona Management. Required for Persona Management, and is automatically enabled with Persona Management.
Secure Socket Tunneling Protocol Service	Manual	Disable	Used to provide VPN capability
Security Center	Auto	Disable	Monitors configuration of security-related services
Superfetch	Auto	Disable	Loads applications into memory for faster reload over time. Non-persistent virtual machines will likely not benefit from this setting being enabled. Full testing is recommended to determine the optimum setting for this service.
Tablet PC Input Service	Manual	Disable	Table PC Services
*Themes	Auto	Disable	Only if you want to run as “Classic” interface (no “Orb” for start button)
UPnP Host Service	Manual	Disable	Dependent on SSDP Service
Volume Shadow Copy Service	Manual	Disable/ Enable	Disable if you are not using System Restore and not using View Persona Management. Required for Persona Management, and is automatically enabled with Persona Management.
Windows Backup	Manual	Disable	Backs up workstation data
*Windows Defender	Auto	Disable	Disable if Anti Spyware / Malware isn’t needed
Windows Error Reporting Service	Manual	Disable	Windows Error Reporting
*Windows Firewall	Auto	Disable	Disable unless you are setting exceptions using GPO
Windows Media Center Receiver Service	Manual	Disable	Used by Media Center
Windows Media Center Scheduler Service	Manual	Disable	Used by Media Center

SERVICE	DEFAULT	STATE	COMMENTS
*Windows Search	Auto	Disable	Disable if you are not doing a lot of searching on a virtual machine
*Windows Update	Auto	Disable	Disable unless needed for updates
WLAN AutoConfig	Manual	Disable	Wireless LAN Configuration
WWAN AutoConfig	Manual	Disable	Used for Mobile Broadband Devices
*Offline Files	Manual	Disable	Used for maintenance of Offline Files cache
SSDP Discovery	Manual	Disable	Used to discover UPNP Devices

Note: Any of the services above can be programmatically disabled using a script prior to an image being Sysprep'd and captured by executing the following PowerShell syntax for each service. Ensure that the Service Name is being used (not the Display Name) for best results:

```
Powershell Set-Service 'Service name' -startuptype "disabled"
```

Windows 7 Customizations Available Using Group Policy

Customizations can be dynamically applied through the use of GPOs post build. Many organizations prefer to use GPOs because of existing policies that manage physical machines, which can be leveraged for virtual desktops as well. GPOs provide many benefits for desktop management, but care should be taken in the design and implementation. The following sections describe recommended practices for utilizing GPOs for VMware View desktops.

Dedicated OU

The recommended approach is to place virtual machines in a dedicated OU within Active Directory, block inheritance, and enforce loopback processing for user-based GPOs, so that any user GPOs that are applied at your dedicated OU will override any other user-based GPOs applied previously.

Blocking Inheritance on an OU

Blocking inheritance is a potentially important step if you wish to manage virtual machines. In some cases, a Group Policy being applied for computer accounts in other OUs may have a direct conflict with a setting you wish to apply in your Virtual Desktop Infrastructure environment (for example, a wallpaper policy). Additional information describing inheritance for Group Policies is located here: http://blogs.technet.com/b/grouppolicy/archive/2010/01/07/tales-from-the-community-enforced-vs-block-inheritance.aspx

Loopback Policy Processing

Loopback policy processing is useful when you want to have Group Policies applied to users according to where the computer account is located in Active Directory. If a computer account is located in a special OU that has certain Group Policy settings applied for end users of those systems, leverage loopback policy processing to ensure Group Policies are applied in the expected and preferred fashion. More on implementing loopback policy processing can be found here: http://technet.microsoft.com/en-us/library/bb742376.aspx#EDAA

Windows 7 Group Policy Table

POLICY	POLICY LOCATION	SETTINGS
Action Center Icon Removal	User Configuration > Administrative Templates > Start Menu and Taskbar	• Remove the Action Center icon = Enabled
Event Logs	Computer Configuration > Administrative Templates > Event Log Service > Specific Event Log	• Maximum application log size = 1024 • Maximum security log size = 1024 • Maximum system log size = 1024 Note: If you are attempting to set the Security log size to 1024 via this Group Policy setting, you are restricted to 20480 unless you set this using the previous Group Policy Setting valid for Windows XP SP2 and Server 2003 and above located here – Computer Configuration > Windows Settings > Security Settings > Event Log
*Firewall	Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties	• Firewall State = On (Recommended), or Off Note: If the Windows Firewall Service is Disabled, this is not necessary
Internet Explorer Settings (cache)	User Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page	• Empty Temporary Internet Files folder when browser is closed = Enabled
Internet Explorer Settings (first run wizard)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer	• Prevent performance of First Run Customize settings = Enabled
Recycle Bin	User Configuration > Administrative Templates > Windows Components > Windows Explorer	• Do not move deleted files to the recycle bin = Enabled
Remote Desktop	Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections	• Enables users to connect remotely using Remote Desktop Services = Enabled
Remote Desktop	Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security	• Require user authentication for remote connections by using Network Level Authentication = Enabled

POLICY	POLICY LOCATION	SETTINGS
RSS Feeds	User Configuration > Administrative Templates > Windows Components > RSS Feeds	• Turn off background sync for feeds and Web Slices = Enabled
*Screen Saver	User Configuration > Administrative Templates > Control Panel > Personalization	• Password protect the screen saver = Enabled • Screen saver timeout = 600 • Force specific screen saver = %windir%\system32\scrnsave.scr
System Restore	Computer Configuration > Administrative Templates > System > System Restore	• Turn off System Restore = Enabled
User Access Control	Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options	• User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode = Elevate without prompting • User Account Control: Detect application installations and prompt for elevation = Disabled • User Account Control: Only elevate UIAccess applications that are installed in secure locations = Disabled • User Account Control: Run all administrators in Admin Approval Mode = Disabled
Wallpaper	User Configuration > Administrative Templates > Desktop > Desktop	• Desktop Wallpaper = “ ” Note: A “space” is required to set the wallpaper to none in the above setting. Optionally, setting to a file that does not exist will actually prevent a user from setting wallpaper at all.
Windows Defender	Computer Configuration > Administrative Templates > Windows Components > Windows Defender	• Turn off Windows Defender = Enabled
Windows Sideshow	Computer Configuration > Administrative Templates > Windows Components > Windows Sideshow	• Turn off Windows Sideshow = Enabled
*Windows Update	Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings	• Turn Off Access to All Windows Update Features = Enabled • Turn off Windows Update Device Driver Searching = Enabled Note: If the Windows Update Service is Disabled, this is not necessary

Windows 7 Customizations Available Using the Registry

Many optimizations can be programmatically applied by modifying the registry. Most of the modifications that directly affect the operating system are contained in the HKEY Local Machine hive. However, there are a number of changes that can be made in the users' registry, which will reduce repetitive tasks and visual desktop characteristics. The visual desktop settings, such as screensavers and background, can unnecessarily introduce significant bandwidth into the display stream, which is why they are included as recommended optimizations.

COMPUTER (LOCAL MACHINE) SETTINGS
WINDOWS REGISTRY EDITOR VERSION 5.00

```
;Disables First Run Wizard for Internet Explorer
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main]
"DisableFirstRunCustomize"=dword:00000001
;Disables Windows Update
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"NoAutoUpdate"=dword:00000001
;Disables System Restore
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore]
"DisableSR"=dword:00000001
;Sets size and retention for Event Logs to 1 MB and no retention
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application]
"MaxSize"=dword:00100000
"Retention"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security
"MaxSize"=dword:00100000
"Retention"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\System]
"MaxSize"=dword:00100000
"Retention"=dword:00000000
;Disables the crash dump file
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]
"CrashDumpEnabled"=dword:00000000
;Removes the option to store files in the recycle bin and deletes them immediately
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoRecycleFiles"=dword:00000001
;Allows RDP to be used - ensure firewall is configured or turned off
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"fDenyTSConnections"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\
RDP-Tcp]
"UserAuthentication"=dword:00000000
;Disables User Access Control (UAC)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"EnableLUA"=dword:00000000
;Set Superfetch for boot files only
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters]
"EnableSuperfetch"=dword:00000000
;Turn off Default Network Location Dialogue
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\
NewNetworkWindowOff]
; Extend Disk Time-Out Value to 200
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk]
"TimeOutValue"=dword:000000c8
[HKEY_LOCAL_MACHINE\SOFTWARE\Image]
"Revision"="1.0"
"Virtual"="Yes"
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Sideshow]
"Disabled"=dword:00000001
```

Windows Aero is a feature that is automatically enabled in most versions of Windows 7, through the registry. VMware View supports 3D graphics such as Windows Aero. If Aero is not evident in Windows 7, see What is the Aero desktop experience? and Open the Aero troubleshooter. To enable 3D graphics in VMware View, see *3D Graphics over LAN and WAN* in the VMware View Evaluator's Guide. You enable 3D graphics through View Administrator in desktop pool settings.

Creating and Modifying the Default User Profile

For years, administrators have been customizing the default profile for a standard image by customizing the profile of the local administrator, and then copying that profile to the default user profile directory, complete with all customizations required for each user that logs into a system. This process was problematic and not officially supported by Microsoft. This paper will concentrate on one method that can be leveraged to alter the default user profile. The best method for an organization is determined by reviewing the available supported solutions and picking the one that is most suited for its needs.

USER (DEFAULT USER) SETTINGS
WINDOWS REGISTRY EDITOR VERSION 5.00

```
;Sets the screensaver default to "blank", timeout 10 mins, protected
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop]
"SCRNSAVE.EXE"="%windir%\\system32\\scrnsave.scr"
"ScreenSaveTimeOut"="600"
"ScreenSaverIsSecure"="1"
;Sets default wallpaper to nothing
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"Wallpaper"=""
;Ensures that temporary internet files are always purged
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache]
"Persistent"=dword:00000000
;Hide the Action Center Task Tray Icon
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"HideSCAHealth"=dword:00000001
;Disable RSS Feeds for Internet
[HKEY_CURRENT_USER\Software\Microsoft\Feeds]
"SyncStatus"=dword:00000000
```

Note: Default user profile settings for the HKCU\.Default hive need to be imported prior to the image being Sysprep'd and captured. The above user default settings can be applied to the default user profile programmatically by following the process defined in the "Creating and Modifying the Default User Profile" section of this white paper.

Supported Methods for Modifying the Default User Profile

- Automated Profile Copy with Sysprep (CopyProfile):
  http://technet.microsoft.com/en-us/library/cc748953(WS.10).aspx

  http://support.microsoft.com/kb/973289
- Scripted Approach:
  http://support.microsoft.com/?id=284193

  http://blogs.technet.com/b/deploymentguys/archive/2009/10/29/configuring-default-user-settings-full-update-for-windows-7-and-windows-server-2008-r2.aspx
- Group Policy Preferences:
  http://www.microsoft.com/downloads/details.aspx?FamilyID=42e30e3f-6f01-4610-9d6e-f6e0fb7a0790&displaylang=en

Scripted Approach for Modifying the Default User Profile

Commands.bat and TS.xml utilize the following approach to modify the default user profile, as it provides the most flexibility in how settings can be applied and be executed programmatically with advanced techniques discussed in the "Deployment Section" of this paper.

Note: This process is only intended to incorporate default user settings into a standard image.

1. First, identify the HKCU settings that are needed to be included in the default user profile for a Windows 7 standard image. Keep these settings specific to Windows, such as those presented in this white paper (default screensaver settings, default wallpaper behavior, and so on).

   Note: Microsoft states that not all HKCU settings can be applied programmatically using registry inserts, so your mileage may vary. Whenever possible, establish defaults for your VMware View virtual machines using Group Policy to ensure consistent results.

2. Next, create a batch file, script, or PowerShell command that initiates loading the NTUser.DAT file for the default user profile into regedit in order to update.

   ```
   REG LOAD "hku\Test" "%USERPROFILE%\..\Default User\NTUSER.DAT"
   ```

   The above example assumes the hive for default user will be loaded into **Test** under `HKEY_Users` within the registry. This command must be executed exactly as it is shown, changing only the `hku\Test` to another location such as `hku\TEMP` if desired.

3. Next, while the hive is open for editing, insert any registry updates required for `HKU\.Default` using either `REG, PowerShell`, or `regedit /s` commands. REG is used below to illustrate one way of inserting values.

   ```
   REG ADD "hku\Test\ Software\Microsoft\Windows\CurrentVersion\Policies\
   System" /v Wallpaper /d "" /f
   ```

4. Finally (very important), the registry hive needs to be unloaded to save the changes imported into the default user profile. Failure to do this will hold the hive open by the currently logged on user and not append updates.

   ```
   REG unload "hku\Test"
   ```

5. Now, your batch file should look similar to the following:

   ```
   REG LOAD "hku\Test" "%USERPROFILE%\..\Default User\NTUSER.DAT"

   REG ADD "hku\Test\ Software\Microsoft\Windows\CurrentVersion\Policies\
   System" /v Wallpaper /d "" /f

   REG unload "hku\Test"
   ```

   Note: The above commands may be word-wrapped due to formatting.

Managing VMware View Desktops

The goal of optimizing Windows 7 extends beyond the initial build and deployment of optimized virtual machines. The following section reviews settings that are relevant to the ongoing management of VMware View desktops, and optional settings to modify the default behavior of the PCoIP display protocol.

View Manager Idle Settings

View Manager provides settings that determine the length of time that idle or disconnected VMware View desktops will utilize system resources before going into suspended mode or powering down. These settings can be modified per desktop pool or managed by View policies. Determining an acceptable length of time can significantly reduce the load on the system hardware. However, putting machines into suspension or setting up users to constantly power on their desktops will be counterproductive, so address these settings carefully.

Managing PCoIP using GPOs

In some cases, part of optimization can include limiting or tuning the PCoIP protocol for certain network environments. The PCoIP.ADM file is provided with VMware View and can be used to deploy these settings using GPOs to VMware View clients. For further details, see the VMware View 5 with PCoIP Network Optimization Guide.

GPO PCoIPImagingMaximumInitialImageQuality
In a limited bandwidth scenario, this setting can be used to configure a preference between higher initial image quality, with larger peaks in bandwidth during large screen changes; or lower initial image quality, with smaller peaks in bandwidth during large screen changes.

Note: If used, consider adjusting the maximum imaging quality before applying a bandwidth limit or adjusting the minimum image quality.

Set to a value between 0 - 100 (default is 90). This value must be set lower than the PCoIPImagingMinimumInitialQuality value.

GPO PCoIPMaxLinkRate
The PCoIP protocol is designed to take advantage of available network bandwidth and share bandwidth fairly across active users on a link. You should not change this setting unless you have carefully determined the overall effect to be beneficial. Be careful not to set a maximum bandwidth limit so low that individual sessions cannot take advantage of additional link bandwidth when available.

Note: If used, this setting should be configured for all users that share a particular network link.

Set `PCoIPMaxLinkRate` to the desired maximum PCoIP session bandwidth in kilobits per second (that is, 1000 = 1000Kbps = 1Mbps). Default is 1Gbps, 0 = no bandwidth constraints.

References

Group Policy Registry Settings
http://www.microsoft.com/downloads/details.aspx?FamilyID=18c90c80-8b0a-4906-a4f5-ff24cc2030fb&displaylang=en

http://msdn.microsoft.com/en-us/library/ms815238.aspx

Using REG to Update the Registry
http://technet.microsoft.com/en-us/library/cc732643(WS.10).aspx

Configuring PCoIP for Use with View 4.x (Knowledge Base article)
http://kb.VMware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1018158

VMware View 5 with PCoIP Network Optimization Guide
http://www.vmware.com/technical-resources/products/view.html

VMware View Persona Management Deployment Guide
http://www.vmware.com/technical-resources/products/view.html

About the Authors

Ensynch
Jim Britt currently holds the role of Solutions Architect at Ensynch, Inc. and has been a specialist in the areas of systems management and virtualization for over 15 years. His range and versatility are showcased in his experience with supporting companies ranging from 250 seats nationally to 120,000 seats globally. Jim's deep technical abilities in systems management and virtualization make him a highly sought after resource as an engineer and speaker. His specialties include desktop imaging and deployment, software delivery, virtualization, patch management, systems monitoring and reporting, and team building and mentorship.

Founded in 2001, Ensynch, Inc. is a leading professional services consulting firm providing information technology, business optimization, and project management consulting services, as well as IT resourcing and staffing. Ensynch has earned consecutive spots on the Inc. 500, and numerous Microsoft distinctions, including Worldwide Partner Award Recognition. It is headquartered in, Tempe, Arizona with offices across Southern California and in New York. Ensynch serves growing midmarket and enterprise companies in the U.S. and select clients across the globe.

VMware
Aaron Black is a Senior Technical Marketing Manager at VMware®. In this role, his primary focus is to develop technical content to aid in evaluation and implementations of VMware View™ and VMware ThinApp™. Aaron's background includes roles as a systems engineer and solutions consultant in the Technical Services organization. His previous positions include systems engineer with Citrix Systems, leading a technical corporate IT team at Sprint, and solutions design for customers of Choice Solutions, a platinum reseller of VMware products.

Tina de Benedictis, Technical Marketing Manager in End User Computing at VMware, updated this document to accommodate the Persona Management and 3D graphics features in View 5.

Appendix A (Customizations Reference)

The Customizations Reference table lists all recommended settings to optimize Windows 7 for your VMware View virtual desktop infrastructure. The Method column represents the available mechanisms to apply these settings. The Method chosen should be based upon organizational restrictions and preferences. Discretionary changes are marked with an asterisk ('*').

TYPE	DESCRIPTION	STATUS	METHOD	HIVE
Customization	Action Center Icon	Disable	GPO, Registry	HKCU
Customization	Set Boot to "No GUI"	Disable	Command Line	HKLM
Customization	Crash Dump	Disable	Registry	HKLM
Customization	Disk Timeout Value	Modify	Registry	HKLM
Customization	Event Logs	Modify	GPO, Registry	HKLM
Customization	Hibernation	Disable	Command Line	HKLM
Customization	IE Cache	Disable	GPO, Registry	HKCU
Customization	IE First Run Wizard	Disable	GPO, Registry	HKLM
Customization	IE RSS Feeds	Disable	GPO, Registry	HKCU
Customization	Image Revision	Modify/Create	Registry	HKLM
Customization	Last Access Timestamp	Modify	Command Line	HKLM
Customization	Network Location Dialogue	Modify	Registry	HKLM
Customization	Recycle Bin	Disable Deleted File Retention	GPO, Registry	HKLM
Customization	Registry Idle Backup	Disable	Command Line	HKLM
Customization	Screensaver	Enable and Configure	GPO, Registry	HKCU
Customization	Wallpaper	Disable	GPO, Registry	HKCU
Customization	WinSAT (Windows System Assessment Tool)	Disable	Command Line	HKLM
Feature	User Access Control	Turn off or Configure	GPO, Registry	HKLM
Feature	Windows Sideshow	Disable	GPO, Registry	HKLM
Feature/Service	System Restore	Disable	GPO, Registry, Services, Command Line	HKLM

TYPE	DESCRIPTION	STATUS	METHOD	HIVE
Windows Service	*Desktop Window Manager Session Manager	Disable	Services	HKLM
Windows Service	*IP Helper	Disable	Services	HKLM
Windows Service	*Superfetch	Disable	Registry, Services	HKLM
Windows Service	*Themes	Disable	Services	HKLM
Windows Service	*Windows Defender	Disable	GPO, Services, Command Line	HKLM
Windows Service	Tablet	PC Input	Services	HKLM
Windows Service	*Windows Firewall	Configure/ Disable	GPO, Services, Command Line	HKLM
Windows Service	BitLocker Drive Encryption Service	Disable	Services	HKLM
Windows Service	Block Level Backup Engine Service	Disable	Services	HKLM
Windows Service	Diagnostic Policy Service	Disable	Services	HKLM
Windows Service	Disk Defragmenter	Disable	Services, Command Line	HKLM
Windows Service	Home Group Listener	Disable	Services	HKLM
Windows Service	Home Group Provider	Disable	Services	HKLM
Windows Service	Microsoft iSCSI Initiator Service	Disable	Services	HKLM
Windows Service	Microsoft Software Shadow Copy Provider	Disable/ Enable for Persona Management	Services	HKLM
Windows Service	Offline Files	Disable	Services	HKLM
Windows Service	Remote Desktop	Enable	GPO, Registry, Services	HKLM
Windows Service	Secure Socket Tunneling Protocol Service	Disable	Services	HKLM
Windows Service	Security Center	Disable	Services	HKLM
Windows Service	SSDP Discovery	Disable	Services	HKLM

TYPE	DESCRIPTION	STATUS	METHOD	HIVE
Windows Service	Volume Shadow Copy Service	Disable/ Enable for Persona Management	Services	HKLM
Windows Service	Windows Backup	Disable	Services	HKLM
Windows Service	Windows Error Reporting Service	Disable	Services	HKLM
Windows Service	Windows Media Center Receiver Service	Disable	Services	HKLM
Windows Service	Windows Media Center Scheduler Service	Disable	Services	HKLM
Windows Service	Windows Search	Disable	Services	HKLM
Windows Service	Windows Update	Disable	GPO, Registry, Services	HKLM
Windows Service	WLAN AutoConfig	Disable	Services	HKLM
Windows Service	WWAN AutoConfig	Disable	Services	HKLM

Appendix B (Commands.bat)

To optimize a Windows 7 desktop template, you can create a Commands.bat file from one of two files attached to this guide: CommandsPersonaManagement.txt or CommandsNoPersonaManagement.txt. To save one of these text files, go to the Adobe Reader menu, select **View**, then **Navigation Panels**, **Attachments**, the text file of your choice, and then select **Save Attachment.** Choose the CommandsPersonaManagement.txt file if you plan to implement View Persona Management. Choose CommandsNoPersonaManagement.txt if you do not plan to implement View Persona Management. Rename to Commands.bat for batch file execution. The contents of the batch file are displayed below.

Note: The commands below may be word-wrapped due to formatting.

Administrator Note: Any HKEY users setting applied to the default user will only apply to new profiles created. The administrators default profile will be left untouched. To see the effects of modifications to the default user profile, you must login as another user other than the local administrator.

***Important:** If you are implementing Persona Management, these two lines have been deleted from the CommandsNoPersonaManagement.txt file to create the CommandsPersonaManagement.txt file:*

```
Powershell Set-Service 'VSS' -startuptype "disabled"
...
vssadmin delete shadows /All /Quiet
```

By deleting these lines, you are making these desktops ready for Persona Management enablement.

CommandsNoPersonaManagement.txt

```
rem Use this script for desktops _without_ View Persona Management implemented.

rem  Setting Default HKCU values by loading and modifying the default user registry hive
reg load "hku\temp" "%USERPROFILE%\..\Default User\NTUSER.DAT"
reg ADD "hku\temp\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v
SCRNSAVE.EXE /d "%windir%\system32\scrnsave.scr" /f
reg ADD "hku\temp\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v
ScreenSaveTimeOut /d "600" /f
reg ADD "hku\temp\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v
ScreenSaverIsSecure /d "1" /f
reg ADD "hku\temp\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
Wallpaper /d " " /f
reg ADD "hku\temp\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache" /v
Persistent /t REG_DWORD /d 0x0 /f
reg ADD "hku\temp\Software\Microsoft\Feeds" /v SyncStatus /t REG_DWORD /d 0x0 /f
reg ADD "hku\temp\Software\Microsoft\WIndows\CurrentVersion\Policies\Explorer" /v
HideSCAHealth /t REG_DWORD /d 0x1 /f
reg unload "hku\temp"

rem Making modifications to the HKLM hive
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main" /v
DisableFirstRunCustomize /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters" /v EnableSuperfetch /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v
NoAutoUpdate /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v
DisableSR /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk" /v TimeOutValue /t
REG_DWORD /d 200 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Image" /v Revision /t REG_SZ /d 1.0 /f

reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Image" /v Virtual /t REG_SZ /d Yes /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application" /v
MaxSize /t REG_DWORD /d 0x100000 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application" /v
Retention /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Network\
NewNetworkWindowOff" /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\System" /v
MaxSize /t REG_DWORD /d 0x100000 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\System" /v
Retention /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security" /v
MaxSize /t REG_DWORD /d 0x100000 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security" /v
Retention /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl" /v
CrashDumpEnabled /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer"
/v NoRecycleFiles /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
```

```
fDenyTSConnections /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\
RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\system" /v
EnableLUA /t REG_DWORD /d 0x0 /f
reg Add "HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Sideshow" /v Disabled /t
REG_DWORD /d 0x1 /f

rem Using Powershell to perform Windows Services modifications
Powershell Set-Service 'BDESVC' -startuptype "disabled"
Powershell Set-Service 'wbengine' -startuptype "disabled"
Powershell Set-Service 'DPS' -startuptype "disabled"
Powershell Set-Service 'UxSms' -startuptype "disabled"
Powershell Set-Service 'Defragsvc' -startuptype "disabled"
Powershell Set-Service 'HomeGroupListener' -startuptype "disabled"
Powershell Set-Service 'HomeGroupProvider' -startuptype "disabled"
Powershell Set-Service 'iphlpsvc' -startuptype "disabled"
Powershell Set-Service 'MSiSCSI' -startuptype "disabled"
Powershell Set-Service 'swprv' -startuptype "disabled"
Powershell Set-Service 'CscService' -startuptype "disabled"
Powershell Set-Service 'SstpSvc' -startuptype "disabled"
Powershell Set-Service 'wscsvc' -startuptype "disabled"
Powershell Set-Service 'SSDPSRV' -startuptype "disabled"
Powershell Set-Service 'SysMain' -startuptype "disabled"
Powershell Set-Service 'TabletInputService' -startuptype "disabled"
Powershell Set-Service 'Themes' -startuptype "disabled"
Powershell Set-Service 'upnphost' -startuptype "disabled"
Powershell Set-Service 'VSS' -startuptype "disabled"
Powershell Set-Service 'SDRSVC' -startuptype "disabled"
Powershell Set-Service 'WinDefend' -startuptype "disabled"
Powershell Set-Service 'WerSvc' -startuptype "disabled"
Powershell Set-Service 'MpsSvc' -startuptype "disabled"
Powershell Set-Service 'ehRecvr' -startuptype "disabled"
Powershell Set-Service 'ehSched' -startuptype "disabled"
Powershell Set-Service 'WSearch' -startuptype "disabled"
Powershell Set-Service 'wuauserv' -startuptype "disabled"
Powershell Set-Service 'Wlansvc' -startuptype "disabled"
Powershell Set-Service 'WwanSvc' -startuptype "disabled"

rem Making miscellaneous modifications
bcdedit /set BOOTUX disabled
vssadmin delete shadows /All /Quiet
Powershell disable-computerrestore -drive c:\
netsh advfirewall set allprofiles state off
powercfg -H OFF
net stop "sysmain"
fsutil behavior set DisableLastAccess 1

rem Making modifications to Scheduled Tasks
schtasks /change /TN "\Microsoft\Windows\Defrag\ScheduledDefrag" /Disable
schtasks /change /TN "\Microsoft\Windows\SystemRestore\SR" /Disable
schtasks /change /TN "\Microsoft\Windows\Registry\RegIdleBackup" /Disable
schtasks /change /TN "\Microsoft\Windows Defender\MPIdleTask" /Disable
schtasks /change /TN "\Microsoft\Windows Defender\MP Scheduled Scan" /Disable
schtasks /change /TN "\Microsoft\Windows\Maintenance\WinSAT" /Disable
```

CommandsPersonaManagement.txt

```
rem Use this script for desktops _with_ View Persona Management implemented.

rem Setting Default HKCU values by loading and modifying the default user registry hive
reg load "hku\temp" "%USERPROFILE%\..\Default User\NTUSER.DAT"
reg ADD "hku\temp\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v
SCRNSAVE.EXE /d "%windir%\system32\scrnsave.scr" /f
reg ADD "hku\temp\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v
ScreenSaveTimeOut /d "600" /f
reg ADD "hku\temp\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v
ScreenSaverIsSecure /d "1" /f
reg ADD "hku\temp\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
Wallpaper /d " " /f
reg ADD "hku\temp\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache"
/v Persistent /t REG_DWORD /d 0x0 /f
reg ADD "hku\temp\Software\Microsoft\Feeds" /v SyncStatus /t REG_DWORD /d 0x0 /f
reg ADD "hku\temp\Software\Microsoft\WIndows\CurrentVersion\Policies\Explorer" /v
HideSCAHealth /t REG_DWORD /d 0x1 /f
reg unload "hku\temp"

rem Making modifications to the HKLM hive
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main" /v
DisableFirstRunCustomize /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters" /v EnableSuperfetch /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v
NoAutoUpdate /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v
DisableSR /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk" /v TimeOutValue
/t REG_DWORD /d 200 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Image" /v Revision /t REG_SZ /d 1.0 /f

reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Image" /v Virtual /t REG_SZ /d Yes /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application"
/v MaxSize /t REG_DWORD /d 0x100000 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application"
/v Retention /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Network\
NewNetworkWindowOff" /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\System" /v
MaxSize /t REG_DWORD /d 0x100000 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\System" /v
Retention /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security" /v
MaxSize /t REG_DWORD /d 0x100000 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security" /v
Retention /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl" /v
CrashDumpEnabled /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\
Explorer" /v NoRecycleFiles /t REG_DWORD /d 0x1 /f
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0x0 /f
```

```
reg ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\
WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0x0 /f
reg ADD "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\system"
/v EnableLUA /t REG_DWORD /d 0x0 /f
reg Add "HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Sideshow" /v Disabled /t
REG_DWORD /d 0x1 /f

rem Using Powershell to perform Windows Services modifications
Powershell Set-Service 'BDESVC' -startuptype "disabled"
Powershell Set-Service 'wbengine' -startuptype "disabled"
Powershell Set-Service 'DPS' -startuptype "disabled"
Powershell Set-Service 'UxSms' -startuptype "disabled"
Powershell Set-Service 'Defragsvc' -startuptype "disabled"
Powershell Set-Service 'HomeGroupListener' -startuptype "disabled"
Powershell Set-Service 'HomeGroupProvider' -startuptype "disabled"
Powershell Set-Service 'iphlpsvc' -startuptype "disabled"
Powershell Set-Service 'MSiSCSI' -startuptype "disabled"
Powershell Set-Service 'swprv' -startuptype "disabled"
Powershell Set-Service 'CscService' -startuptype "disabled"
Powershell Set-Service 'SstpSvc' -startuptype "disabled"
Powershell Set-Service 'wscsvc' -startuptype "disabled"
Powershell Set-Service 'SSDPSRV' -startuptype "disabled"
Powershell Set-Service 'SysMain' -startuptype "disabled"
Powershell Set-Service 'TabletInputService' -startuptype "disabled"
Powershell Set-Service 'Themes' -startuptype "disabled"
Powershell Set-Service 'upnphost' -startuptype "disabled"
Powershell Set-Service 'SDRSVC' -startuptype "disabled"
Powershell Set-Service 'WinDefend' -startuptype "disabled"
Powershell Set-Service 'WerSvc' -startuptype "disabled"
Powershell Set-Service 'MpsSvc' -startuptype "disabled"
Powershell Set-Service 'ehRecvr' -startuptype "disabled"
Powershell Set-Service 'ehSched' -startuptype "disabled"
Powershell Set-Service 'WSearch' -startuptype "disabled"
Powershell Set-Service 'wuauserv' -startuptype "disabled"
Powershell Set-Service 'Wlansvc' -startuptype "disabled"
Powershell Set-Service 'WwanSvc' -startuptype "disabled"

rem Making miscellaneous modifications
bcdedit /set BOOTUX disabled
Powershell disable-computerrestore -drive c:\
netsh advfirewall set allprofiles state off
powercfg -H OFF
net stop "sysmain"
fsutil behavior set DisableLastAccess 1

rem Making modifications to Scheduled Tasks
schtasks /change /TN "\Microsoft\Windows\Defrag\ScheduledDefrag" /Disable
schtasks /change /TN "\Microsoft\Windows\SystemRestore\SR" /Disable
schtasks /change /TN "\Microsoft\Windows\Registry\RegIdleBackup" /Disable
schtasks /change /TN "\Microsoft\Windows Defender\MPIdleTask" /Disable
schtasks /change /TN "\Microsoft\Windows Defender\MP Scheduled Scan" /Disable
```

Appendix C (CommandsDesktopReadyForPersonaManagement.txt)

If you have an existing desktop image without Persona Management, and you wish to deploy Persona Management on that desktop image, create a `BAT` file on your virtual machine template from the attached `CommandsDesktopsReadyForPersonaManagement.txt` file. From the Adobe Reader View menu, select **Navigation Panels**, **Attachments**, and then **Save As** a `BAT` file. Run this script as Admin (right-click > Run as Administrator). Reboot the computer when the `BAT` file completes.

CommandsDesktopReadyForPersonaManagement.txt

```
rem To implement View Persona Management on desktops that previously did not use Persona
Management, convert this text file to a BAT file and run it on your virtual machine
template.

rem You must run this script as Admin (right-click > Run as Administrator).
rem Reboot the computer after script completes.
Powershell Set-Service 'VSS' -startuptype "automatic"
Powershell Set-Service 'swprv' -startuptype "automatic"
pause
```

Appendix D (TS.xml)

Example Task Sequence XML (TS.xml)

The `TS.xml` file has been attached to this guide and can be saved by going to the Adobe Reader menu, selecting **View**, then **Navigation Panels**, **Attachments**, and **TS.xml**, then selecting **Save Attachment**. Refer to the "Using the Microsoft Deployment Toolkit" section for step-by-step guidance.

vmware

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