# Windows XP Deployment Guide

VMware Virtual Desktop Infrastructure

VMware® Virtual Desktop Infrastructure (VDI) transforms the way customers use and manage desktop operating systems. Desktop instances can be deployed rapidly in secure data centers to facilitate high availability and disaster recovery, protect the integrity of enterprise information, and remove data from local devices that are susceptible to theft or loss. Isolating each desktop instance in its own virtual machine eliminates typical application compatibility issues and improves users' personal computing environments.

## About This Guide

This guide offers best practices for creating Windows XP-based templates for VMware VDI-based solutions and for preparing the same templates for use with Virtual Desktop Manager 2.

## Creating the Initial Virtual Machine

The initial virtual machine establishes a virtual hardware profile to be used for rapid deployment of other virtual desktop instances. You can create the initial virtual machine from scratch, as in this guide, or convert a physical machine to a virtual machine, using either the standalone version of VMware Converter or the version integrated with VirtualCenter 2.5. Use VMware converter to convert the physical PC to a virtual machine and migrate it to VI3, convert it to a template, and use it as the baseline for deploying future virtual desktops.

To create the initial virtual machine from scratch, use the Virtual Infrastructure Client to connect to your VirtualCenter server, then use the console to configure the initial virtual machine or template, and install the OS using the console.

When you establish a connection with your Virtual Infrastructure datacenter, a new virtual machine should be created from inventory. When you create a new virtual machine, the wizard for the new virtual machine appears. Use the Custom Configuration Parameters as baseline settings for a template. If you use a Virtual Desktop Manager, such as VDM 2, to create pools of desktops, you can change many of these settings, such as the Host/Cluster, Datastore, and Resource Pool, at deployment time.

**Table 1.** Custom Configuration Parameters

| Parameter | Comments |
|---|---|
| Name and Location | This can be a generic name such as `xptemplate`. The location can be any folder within your datacenter inventory. |
| Host/Cluster | Host/Cluster is the ESX server or cluster of server resources that will be used to run this virtual machine. It can be changed at anytime. The location of the initial virtual machine or template does not necessarily specify where future virtual machines created from this template will reside. |
| Resource Pool | If the physical ESX server resources are divided granularly using resource pools, they can be assigned to this virtual machine |
| Datastore | This is the location where files associated with the virtual machine should be stored. |
| Guest Operating System | The operating system that will be installed. |

**Table 1.** Custom Configuration Parameters

| Parameter | Comments |
|---|---|
| CPUs | The number of virtual processors that will be presented to the virtual machine. For most VDI users, a single processor should be sufficient. |
| Memory | The amount of memory to allocate to each virtual machine e created from this template, in most cases, 512MB |
| Network | The number of virtual network adapters that will be used. One is usually enough. As a best practice, the network name should be consistent across virtual infrastructures. An incorrect network name in a template can cause failures during the instance customization phases. |
| I/O Adapters | The LSI Logic adapter issued for VDI-based deployments is recommended; however, the LSI Logic driver is not included as part of the Windows XP install procedure. Download and add it during the OS installation. |
| Disk | Create a new disk when creating the initial virtual machine or template, based on the amount of local storage you decide to allocate to each user. Allow at least enough for the OS installation, patches, and locally installed applications. Best Practice is to store as much of the user's information, profile, and documents on network shares rather than locally. Doing so can greatly reduce the need for disk space and management of the local data. |

# Installing Windows XP

## Preparation

Virtual machines behave like physical machines, so Windows XP installation is essentially the same on both. Although it is possible to image your virtual machine using some type of legacy or existing cloning technology, this guide focuses on a fresh Windows XP installation.

**NOTE**: LSI storage controller drivers are not available on the Windows XP installation CD, so be sure to complete the following items before starting the installation:

- Download the LSI 53C1030 drivers from the LSI Web site.
- Using MagicISO or other third-party solutions, create a `.flp` image containing the LSI Logic drivers.
- SCP the floppy image to the virtual machine's ESX host. If you are using VirtualCenter 2.5, you can use the VIC to upload the file to the desired datastore.
- Have a Windows XP CD or ISO image that is accessible form the virtual machine.

## Pre-installation Virtual Machine Modifications

Make the following modifications to the virtual machine hardware profile before starting the Windows XP installation. Using the VIC connect to VirtualCenter, locate the virtual machine that was initially created and edit the following hardware settings:

- Ensure there is a floppy drive present.
- Ensure the floppy drive is configured to connect at Power On.
- If using a floppy image, ensure the Device Type is set to use a floppy image and is pointing to the LSI Driver image.
- Ensure the CD/DVD drive is present and configured to connect at power on.
- Ensue the CD/DVD Device Type is configured to point at the Windows XP CD or ISO image.

## Installation

Once you complete the pre-installation preparation and modifications, you can install Windows XP. The basic general steps and best practices for installing and preparing Windows XP are:

- From the Virtual Infrastructure client, connect to VirtualCenter.
- Power on the virtual machine created earlier.

- Use the console to view the boot process and to send input to the virtual machine.
- As the Windows Setup process begins, press F6 to add an additional SCSI driver. This lets you specify the LSI Logic driver on the floppy image.

The Windows setup process copies all the necessary files to the virtual disk. Complete the setup just as you would for any normal Windows XP installation. However, because this image will be used as a template, it is a good idea to make the configuration as generic as possible. For instance customization, see "Creating a Guest Customization Specification" on page 4).

After completing the Windows setup, perform the following tasks before finalizing the image. Some of these steps will vary from organization to organization, depending on your Windows imaging standards; some are optional and noted as such. Many can be managed using a group policy (see "Common GPOs for Managing Virtual Desktops" on page 5).

### Recommended Steps

- If not applied to the installation CD, Install SP2 and the most recent Microsoft updates.
- Install and configure the VMware Tools.
- If using Virtual Desktop Manager 2 as your connection broker, install the VDM 2 agent.
- Install and configure any additional third-party or in-house applications needed.
- Set the Windows screensaver to blank.
- Configuring the default color setting for RDP.

By default, Windows XP uses 16-bit color for Remote Desktop. You can enable and manage 24-bit color centrally using group policy or by making the following registry change:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\/
RDP-Tcp – Change the color depth to 4
```

### Optional Steps

- Disable any unused hardware, such as COM1 and COM2.
- Turn off theme enhancements.
- Adjust My Computer>Properties>Advanced Tab>Performance Section>Settings for best performance.
- Set the blank screen saver to password protect on resume.
- Ensure hardware acceleration is enabled.
- Start>Control Panel>Display>Settings Tab>Advanced Button>Troubleshooting Tab.
- Delete any hidden update uninstall folders — C:\WINDOWS.
  For example: `$NtUninstallKB893756$`
- Disable Indexing Services
  Indexing improves searches by cataloging files. For users who search a lot, this may be beneficial and should not be disabled.
- Start>Control Panel>Add Remove Windows Components>Indexing Service.
- Disable indexing of the C: drive from the properties.
- Remove or minimize System restore points.
- Start>Control Panel>System>System Restore.
- Disable any unwanted services.
- Run Disk Cleanup.
- My Computer>C: properties.
- Run Disk Defrag.
- My Computer>C: properties>Tools.

After the preparations and installation are complete, you can power the virtual machine off and get ready to enable it as a deployment template for other virtual desktops.

## Converting the Virtual Machine to a Template

Using templates standardizes the creation of virtual desktops and reduces the risk of human error. Many organizations may have more than one template. For example, you may decide to create separate templates for Finance, HR, and Sales, each group using a unique software or virtual hardware configuration. Ultimately, the use of templates with VDM 2 and VI3 gives you a fast, automated way to provision desktops.

You can convert any virtual machine to a template. Connect to VirtualCenter using the VIC. From the inventory, locate the virtual machine, and select Convert to Template. You can also clone the virtual machine to a template. Cloning creates a copy, leaving the original virtual machine in place. You may find this helpful if you update the template and redeploy desktops often, for instance, when deploying non-persistent desktops or in an environment where a profile solution is used to separate the user profiles from the desktop environment. You can convert a template to a virtual machine, update it, and then convert it back to a template again at any time.

## Creating a Guest Customization Specification

Guest customization allows you to customize virtual desktop as they are created. Using Microsoft sysprep, VirtualCenter guest customization automates several configuration tasks such as:

- Registration Information
- Assigning a unique computer name
- Adding your product key
- Setting the Administrator password
- Setting the time zone
- Any custom run-once scripts
- Network configuration
- Joining a domain
- Generating a new SID

If you use VDM 2 as your virtual desktop manager, it works in conjunction with any existing pre-defined guest customization specifications. You have the option of selecting which guest customization file, if any, to customize the pool of virtual desktops it will create.

To create a guest customization specification, connect with VirtualCenter using the VIC, then select Edit, Customization Specifications. Once the Customization Specification Manger starts, select New. If you prefer, you may import an existing custom sysprep.ini file and use it in the guest customization wizard. As a best practice when using VDM 2 and Guest Customization Specification, set the Computer Name portion of the guest specification to Use the Virtual Machine Name. This ensures that the computer name is consistent across VDM 2, VirtualCenter, Active Directory, and Local Computer Name.

When your initial virtual machine, template, and guest customization are complete, the virtual desktop template is ready to use for deploying virtual desktops. The following sections focus on common best practices for simplifying and standardizing some common desktop management tasks.

# Managing VMware VDI-Based Windows XP Desktops

## Adding Users to the Local Remote Desktop Users Group

When you add users to the Windows XP local group, Remote Desktop Users, they will not be able to access individual or pooled desktops unless they belong to this local group. There are several ways to add users or groups to the local Remote Desktop Users. One is to use a login script. Another approach leverages the Restricted Groups GPO in Active Directory.

When leveraging Restricted Groups, you can add users individually or create a group, add users it, then add that group to the Restricted Group you are managing. Restricted Group GPOs can exist at several GPO levels. Here are the steps for configuring a Restricted Group using the Default Domain Policy:

- Using a MMC console for your domain, create a new group called VDI Users under Active Directory>Users and Computers.
- Add to this group the users who need to access virtual desktops.
- Edit your Default Domain Policy.
- Under Computer Configuration>Windows Settings>Restricted Groups, add the Remote Desktop Users Group.
- Add the VDI users group to the members of the Restricted Remote Desktop Users.

This approach ensures that the VDI Users group is always added to the local Remote Desktop Users group of each virtual desktop joined to the domain. When provisioning new users, a help desk or administrator only needs to ensure that users are added to the Active Directory, VDI Users group.

## Common GPOs for Managing Virtual Desktops

There are several GPOs that can be used for central control of the configuration of your virtual desktops. Because users access their virtual desktops with Remote Desktop, the most common and often used GPOs are the Terminal Server GPOs under Computer or User Configuration>Administrative Templates>Windows Components>Terminal Services. Several of the GPOs are specific to Terminal Server and do not apply to remote desktops sessions. Some of the more commonly used GPOs for deploying Windows XP in a VDI environment are described below. Many of these are optional but recommended. Naturally, use cases and environments vary depending on your organization's standards and policies.

**Table 2. GPOs Under Terminal Services**

| | |
|---|---|
| Enforce Removal of Remote Desktop Wallpaper = Enable | This can greatly enhance the user experience, especially over low-bandwidth connections |
| Limit maximum color depth = Enable | This lets you set the color depth for Remote Desktop sessions. |
| Allow users to connect remotely using Terminal Services = Enable | Setting this ensures that the local policy enabling Remote Desktop connections is configured. |
| Remote Windows Security Item from Start Menu = Disable | Setting this to Disable ensure that users have a log off mechanism. |
| Remove Disconnect option from Shut down dialog = Enable | Setting this minimizes the possibility of users disconnecting rather than logging off. |

**Table 3. GPOs Under Terminal Services >Sessions**

| | |
|---|---|
| Set time limit for disconnected sessions = Enable | Setting this logs off any disconnected sessions that occur after the specified time. Combined with VDM 2 virtual machine power policies, this can be used to create a dynamic and powerful solution for suspending or powering off disconnected virtual desktops. When unneeded desktops are suspended or powered off, the resources are made available to other desktops. |
| Set a time limit for active but idle Terminal Services sessions = Enable | Setting this logs off any idle sessions that occur after the specified time. Combined with VDM 2 virtual machine power policies, this can be used to create a dynamic and powerful solution for suspending or powering off disconnected virtual desktops. When unneeded desktops are suspended or powered off, the resources are made available to other desktops. |

1. Note: Windows XP has a bug where the idle tracker will not work. A hotfix is available from Microsoft upon request. See KB890864.

## Managing the VDM Client Using GPOs

One of the components provided with Virtual Desktop Manager 2 is the VDM Client, a Win32 application that can be installed on most Windows platforms, such as XP Embedded, Windows 2000 Pro, XP Professional, and Vista. It provides the client side component for connecting with virtual desktops. On Embedded XP, Windows XP, and Vista clients, it also enables the ability to redirect additional USB devices not supported by native RDP device redirection.

Also included with VDM 2 is a Group Policy Administrative Template for managing and configuring the VDM Client settings from a central location with Group Policy. The client side settings that can be managed using this administrative template are:

- Enable the shade
- Pin the shade
- Don't check monitor alignment on spanning
- Color depth
- Desktop background
- Show contents of window while dragging
- Menu and window animation
- Themes
- Cursor shadow
- Font smoothing
- Desktop composition
- Audio redirection
- Redirect drives
- Redirect printers
- Redirect serial ports
- Redirect smart cards
- Redirect clipboard
- Redirect supported plug-and-play devices
- Bitmap caching
- Shadow bitmaps
- Cache persistence active
- Enable compression
- Windows key combination redirection
- Bitmap cache file size

Take the he following steps to start configuring the VDM Client settings:

- Locate the `vdm_client.adm` file in C:\Program Files\VMware\VMware VDM\Server\ADM. This is located on any connection broker that has been installed.
- Copy this file to the management station you use to mange Group Policy Objects. By default, Group Policy looks for administration templates in C:\WINDOWS\inf. You can copy the `vdm_client.vdm` file to that location or any other location accessible from your management station.
- Using your MM with the Group Policy Editor snap-in loaded, locate the Group Policy you want to add the template to.
- From the policy, expand User Configuration, Select Administrative Templates, and Add/Remove Templates.
- Locate the `vdm_client` template and add it to the policy.

Once you complete these steps, you are ready to configure your policy for setting VDM client settings. When managing the VDM Client settings or another device, such as a thin client using its own RDP client and configuration, note that any GPO settings for the Remote Desktop will override the client side. For example, if the client is configured to use 24-bit color and the Remote Desktop GPO is configured for a maximum of 16-bit color, the connection will connect using 16-bit color.

# Miscellaneous Information

## Multi-Monitor Support

Using the latest Microsoft Remote Desktop client command line option, `/span`, a Remote Desktop Session can span multiple displays with a maximum resolution of 4096 x 2048. However, spanning does not achieve the identical desktop experience to that of a workstation with a multi-port graphics card. In order to achieve a true multi-monitor experience, you need a third-party tool, such as SplitView or iShadow - Remote Desktop Manager.

VDM 2 also provides the ability for users to configure their desktops by spanning the Remote Desktop session across multiple monitors. Individual users can configure this preference with the VDM Client or VDM WebAccess.

# About the Author

Warren Ponder is a Senior Technical Marketing Engineer at VMware. In this role, he works as part of the product marking team developing alternative approaches to traditional desktop architectures and solutions. Much of his time is spent speaking, writing white papers, and developing technical content focused on thin client computing, Windows interoperability, and virtual desktop solutions that leverage the benefits of VMware's leading virtualization technologies.

# References

http://technet.microsoft.com/en-us/sysinternals/default.aspx

http://technet.microsoft.com/en-us/windowsxp/default.aspx?wt.svl=leftnav

http://technet2.microsoft.com/windowsserver/en/library/b9546edf-751f-4a09-835a-f3397caef2361033.mspx?mfr=true

http://technet2.microsoft.com/windowsserver2008/en/library/fc0b405b-07ef-4767-8716-198d7f0949011033.mspx?mfr=true

http://www.ishadow.com/

http://www.splitview.com/

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



Revision 20080128 Item DG-042-SLN-01-01