PC Re-purposing with VMware® View:

Turning a PC into a Thin Desktop

A Whitepaper

Introduction

Built on the industry-leading VMware virtualization platform, VMware View enables you to deliver rich, personalized virtual desktops to any device with all the benefits of centralized enterprise desktop management. The VMware View portfolio of products lets you run virtual desktops in the datacenter while giving end users a single view of all their applications and data in a familiar, personalized environment on any device at any location.

VMware View transforms the way you use and manage desktop operating systems by helping you centralize the control of desktop PC images, applications, and data. You can deploy virtual desktop instances 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. By isolating each desktop instance in its own virtual machine, you eliminate typical application compatibility issues and deliver a more personal computing environment.

Other benefits of VMware View include simplified regulatory compliance. You no longer need to track security patches and back up data for a diverse mix of end user computers. Instead, updates and backups take place in the datacenter, in the VMware View environment.

Migrating physical desktops to virtual desktops powered by VMware View can be done in several different ways.

In one scenario, you simply replace all your users' physical PCs with thin or zero clients. Thin and zero clients are simple, single-purpose devices that connect to a monitor, keyboard, mouse and network. When powered on, the only application to which the user has access is the View client software that allows the user to connect to her virtual View desktop. Thin or zero clients are easy to deploy, are secure and easy to manage.

However, not all organizations want to invest in new thin or zero client hardware when they embark on a physical to virtual desktop migration.

In many organizations, the physical PCs on users' desks are still in good condition. Replacing them may not only incur additional cost, but also result in accounting complications. Therefore, there is interest in many organizations to convert these physical PCs to thin desktops instead of purchasing new thin or zero clients. This conversion process is referred to as "PC re-purposing".

PC re-purposing can be the initial phase in physical to virtual desktop migration. Then as these re-purposed PCs are fully depreciated or otherwise need replacement, they can be replaced by thin or zero client devices.

There are several approaches you can use to turn a physical PC into a thin client or locked down device with direct access to virtual desktops. This technical note highlights some of your options. It is not all-inclusive, and you may prefer to achieve the same objective using different methods.

This paper provides information for Windows platforms. It does not constitute an endorsement or product validation of any third-party tools.

To use this guide, you should have a good understanding of the system administration techniques involved in configuring system policy and the local registry and should have a basic understanding of how a thin client works.

How Thin Clients Function

To reduce the overhead of device management and meet security policies, thin clients are generally diskless workstations centrally managed from administrative servers.

Instead of booting from a hard drive as a traditional desktop computer does, a thin client can boot from PXE, flash, optical media, or USB devices. The best-known thin client operating systems are Windows XP Embedded, Windows CE, Linux, and various proprietary operating systems. What makes a thin client different from a Windows PC is that the user does not have access to the underlying operating system e.g. the Windows login screen or the Start menu. The applications that the user can run on the thin client are also limited. Finally, the user is unable to change configuration settings, install/remove software, modify the operating system or download files on a thin client. In this way, the thin client is able to provide a secure access to the user's virtual desktop environment that is unaffected by malware.

When repurposing a legacy PC as a thin client, your goal is to turn the PC into a locked down device and provide users with simple access to a virtualized desktop client, such as VMware View. When the user powers on the PC, the only application she is able to access is VMware View. The only action she can do is to log onto her virtual desktop environment via VMware View.

In most respects, users interact with a virtual desktop environment as they would with a local operating environment. However, if the hardware used for the thin client is not on the remote protocol hardware compatibility list, users might experience some incompatibility on physical hardware such as sound cards and USB devices.

To configure a PC as a thin client, you must carry out two main tasks:

- Replace and lock down the default shell, using the VMware View client as the shell.
- Lock down the login profile and policy.

PC Re-Purposing on Windows Platforms

You have several options when re-purposing a Windows PC:

1. Keep the current version of Windows that is already on the hard disk of the PC
2. Install Windows Thin PC on the hard disk of the PC
3. Use another operating system such as Linux either by installing it on the hard disk of the PC or PXE booting the PC

This paper focuses on the first two options.

The advantage of continuing to use Windows as the operating system is that device drivers are already available for the particular PC that you are re-purposing.

You can turn a Windows PC into a thin device by changing the shell from explorer.exe to the VMware View client(wswc.exe).

You can allow the user to log in to the PC normally, or you can remove the PC login to minimize user confusion and the number of times the user has to log in. The only application that can be launched directly on the computer is the application listed as the shell.

Before you modify the registry settings or enforce a new policy for the system, you must make sure the PC has network connectivity and has the VMware View client installed.

After you confirm that the client is operational, make the registry changes described in "Changing the Default Shell (All Users)" or "Changing the Default Shell (Only Current User)". The first registry modification locks down all users who log in to the environment, including administrators.

The procedures in this paper describe the steps you need to take to convert a Windows XP computer.

Changing the Default Shell (All Users)

Take the following steps to change the default shell for all users, including administrators:

1. Start the Windows Registry Editor by entering regedit at a command prompt.
2. Locate the following subkey:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`
3. In the right pane, select **Shell.**
4. Select **Edit** > **Modify.**
5. Change the value data from explorer.exe to the new shell path—for example,
   `C:\Program Files\VMware\VMware View\client\bin\wswc.exe`
6. Click **OK,** and then exit Registry Editor, log out, and log back in.

Changing the Default Shell (Only Current User)

You may prefer to lock down the shell for specific users. This approach allows administrators to make changes as necessary without using a boot disk to change the registry.

Take the following steps to change the default shell for only the current user:

1. Log in to Windows as the user whose shell you want to change.
2. Start the Windows Registry Editor by entering regedit at a command prompt.
3. Locate the following subkey:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

4. Select **Edit** > **New** > **String Value** and give the new value the name Shell.
5. With the new value selected, select **Edit** > **Modify.**
6. Set the value data to the path of the new shell— for example

```
C:\Program Files\VMware\VMware View\client\bin\wswc.exe
```

7. Click **OK,** and then exit Registry Editor, log out of the user's account, and log back in.

You can also change the default shell using a group policy that is enforced for the users when they log in. A group policy is easier to push out to large groups of users if you have the appropriate management infrastructure in place.

Take the following steps to set up a group policy that changes the default shell:

1. Working at the workstation you normally use for setting group policies, start the Group Policy Editor by entering gpedit.msc at a command prompt.
2. Select and expand **User Configuration.**
3. Select and expand **Administrative Templates.**
4. Select **System.**
5. Select **Custom User Interface** in the right pane.
6. Select **Action** > **Properties.**
7. Select **Enabled,** and then in the **Interface file name** field enter the path to the View client—for example

```
C:\Program Files\VMware\VMware View\client\bin\wswc.exe
```

8. Click **OK,** and then exit Group Policy Editor.
9. Push the updated policy to the affected users using the procedures appropriate for your management tools.

When the affected end users log in, they see only the VMware View login.

When the user's shell is restricted in this way and the user logs out of the virtual desktop, nothing remains on the screen but a blank Windows environment with no shell at all. You can avoid this frustrating experience by setting up the appropriate restart logic in the View client.

Take the following steps to set up the PC where you are working so that it presents a View login if the user logs out of the virtual desktop:

1. Use Notepad or another text editor to create a file named View.cmd with the following content:

   ```
   @echo off
   :View
   "C:\Program Files\VMware\VMware View\Client\bin\wswc.exe"
   goto View
   ```

2. Save the file in a location of your choice—for example, C:\BatchFiles
3. Create a VBScript script named view.vbs with the following content:

   ```
   Set WshShell = CreateObject("WScript.Shell")

   WshShell.Run Chr(34) & "C:\BatchFiles\view.cmd" & Chr(34), 0

   Set WshShell = Nothing
   ```

4. Save the script in the C:\BatchFiles directory.
5. Start the Windows Registry Editor by entering regedit at a command prompt.
6. Locate the following subkey:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
   ```

   NOTE Modifying this subkey affects all users, including administrators, and leaves all users with no interface except the View client. You can modify the registry setting that affects a specific user by logging in as that user and modifying the corresponding subkey under HKEY_CURRENT_USER, instead.

7. In the right pane, select **Shell.**
8. Select **Edit > Modify.**
9. Change the value data from explorer.exe to the Windows scripting command and the new shell path—for example:

   ```
   wscript c:\BatchFiles\view.vbs
   ```

10. Click **OK,** and then exit Registry Editor. Reboot the system.

Windows Options

Another approach is to use a Microsoft tool kit called Windows Fundamentals for Legacy PCs. Windows Fundamentals is derived from Windows XP Professional with SP2. It is software based and has enhanced write filter (EWF) functionality like that in XP Embedded. EWF allows all changes to be written to a disposable part of the drive so anything a user changes is lost when the client is rebooted.

Windows Fundamentals strips out most of the standard Windows XP functionality, leaving a core operating system designed to run the RDP and ICA clients, a browser, management and security agents, document viewers, and the .NET framework.

Because Windows Fundamentals is built on Windows XP Pro, you can add Windows Fundamentals machines to your domain and lock them down using group policies or manage them using SMS. To SMS, they appear as Windows XP Professional SP2 systems. You can also manage and patch them in the same way that you do standard Windows XP workstations.

More recently, Microsoft introduced Windows Thin PC for the expressed purpose of enabling IT organizations to convert existing PCs to thin devices. According to Microsoft, Windows Thin PC is a “smaller footprint, locked down version of Windows 7”.

The procedures described in this paper can also apply to Windows Thin PC.

Summary

Repurposing a PC by turning it into a thin desktop can help you extend the life of a legacy PC by three to five years. With no disruptions, you can move to secure and managed virtual desktops that meet your key regulatory compliance mandates.

Thin desktop features are also beneficial in such use cases as

- Providing access for external partners or contractors who need to connect to a dedicated virtual desktop using View
- Restricting students to the curriculum-specific applications in a training organization

A thin desktop is not prone to data loss or viruses as a PC would be. At the same tine, the thin desktop can use a wide variety of virtual desktop applications. Because those applications are running on datacenter servers, end users gain access to applications that they might not be able to run on their older PCs and operating systems.

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