

# Intel® vPro™ Technology Use Case Reference Design

Desktop Virtualization: Dual OS Deployment – Type 2 Hypervisor

Revision 1.0  
December, 2010  
Document ID: 1089

# Revision History

Revision	Revision History	Date
1.0	First release.	December, 2010

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see [www.intel.com/technology/platform-technology/intel-amt/](http://www.intel.com/technology/platform-technology/intel-amt/)

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel® Virtualization Technology (Intel® VT), Intel® Trusted Execution Technology (Intel® TXT), and Intel® 64 architecture require a computer system with a processor, chipset, BIOS, enabling software and/or operating system, device drivers and applications designed for these features. Performance will vary depending on your configuration. Contact your vendor for more information.

Intel, the Intel logo, Intel® AMT, and Intel® vPro™ are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

\*Other names and brands may be claimed as the property of others.

Copyright © 2010 Intel Corporation. All rights reserved.

# Contents

---

<b>1</b>	<b>Preface .....</b>	<b>5</b>
1.1	Document Scope .....	5
1.2	Intended Audience .....	5
1.3	Related Documentation .....	5
<b>2</b>	<b>Introduction .....</b>	<b>6</b>
2.1	Intel® Virtualization Technology (Intel® VT) .....	6
2.1.1	Intel® VT-x .....	6
2.1.2	Intel® VT-d .....	6
2.2	Hardware and Software Considerations .....	7
<b>3</b>	<b>Choosing and Configuring the Host System .....</b>	<b>9</b>
3.1	Choosing the Platform .....	9
3.2	BIOS Settings .....	9
3.2.1	Host OS .....	9
<b>4</b>	<b>Configuring the VM Application .....</b>	<b>10</b>
4.1	Installing the VM Application .....	10
4.2	Installing the IT OS Build .....	10
4.2.1	Installing a VM from the OS Installation Disc .....	11
4.2.2	Exporting a VM .....	18
4.2.3	Importing a VM .....	18
4.3	Enabling Intel VT-x with EPT and AES-NI .....	19
4.4	Unity Mode .....	23
4.4.1	Enabling Unity Mode in VMWare* .....	23
4.4.2	Using Unity Mode in VMWare .....	25
4.5	Security Between Host OS and Guest OS .....	28

## Figures

Figure 1:	VMWare* Workstation Home Tab .....	11
Figure 2:	Choosing the VM Hardware Compatibility .....	12
Figure 3:	Easy Install Information Screen .....	13
Figure 4:	Virtual Machine Name and Location .....	14
Figure 5:	VM Memory Configuration .....	15
Figure 6:	Selecting a Disk to Use for the VM .....	16
Figure 7:	Specifying Disk Capacity .....	17
Figure 8:	Summary of Configuration and Finish Button .....	18
Figure 9:	The VM Devices Tab .....	19
Figure 10:	Selecting the Preferred Mode .....	20
Figure 11:	Selecting Encryption .....	21
Figure 12:	Setting Password .....	21
Figure 13:	Option to Change Password or Remove Encryption .....	22
Figure 14:	Select Install VMWare Tools .....	23
Figure 15:	Run setup.exe .....	24
Figure 16:	Choose an Installation Type .....	25
Figure 17:	The Unity Button .....	25
Figure 18:	VM Start Button .....	26
Figure 19:	Example of Open Folders in Both VM and Host OS .....	26
Figure 20:	Aero™ Desktop Display for VM and Host Applications .....	27

Figure 21: Security Options ..... 28

Figure 22: Further Security Options..... 29

**Tables**

Table 1: Desktop Virtualization System Considerations ..... 7

# 1 Preface

---

Data security and user flexibility are competing forces for IT groups supporting users in their environment. On one hand, IT is tasked with making sure corporate data is secure. On the other hand, users demand the freedom to install applications that fall outside of the “standard IT build” to remain productive and up to date with the latest trends in the given industry. Locking the user image down makes the users upset and can impact productivity, but giving every user administrator rights on the system could allow for an unacceptable amount of risk to the corporate data.

This is where Desktop Virtualization comes into play. The corporate IT group loads a locked down version of the IT build on the system. As part of this OS image, a Type 2 hypervisor is available that end users are able to install a personal OS that they have full administrative rights to use. Within this OS they can load all of the applications that they need that aren’t part of the normal IT image.

In order to successfully support a dual OS deployment model, IT needs to be aware that not all clients are capable of this type of deployment. This Use Case Reference Design document discusses Intel® vPro™ technology based clients as the platform of choice and focuses on the setup and configuration of a type 2 hypervisor to satisfy a dual OS deployment.

## 1.1 Document Scope

This document discusses considerations when choosing a platform for running a dual OS deployment as well as some of the options available in a virtualization environment that make working in this manner easy for the end user. This document also discusses new features in the Intel® processor code named Westmere that help enhance performance and security when using virtualization.

## 1.2 Intended Audience

This document is intended for IT professionals who are deploying or are thinking about deploying a dual OS virtualization solution.

## 1.3 Related Documentation

For more information about Intel® Virtualization Technology (Intel® VT), visit the Intel® Virtualization Technology web site:

[http://www.intel.com/technology/virtualization/technology.htm?iid=tech\\_vt+tech](http://www.intel.com/technology/virtualization/technology.htm?iid=tech_vt+tech)

## 2 Introduction

---

When deciding what type of system to purchase for desktop virtualization, there are several aspects to the system configuration that must be considered. A system that will be running applications locally in both the host OS and a guest OS (running in a virtual machine or VM) will need to have higher than average system specifications to be able to deliver a quality user experience. This system will also need to have some key features that aren't available in all systems. The following sections discuss these key features and requirements in order to identify the right system to purchase.

### 2.1 Intel® Virtualization Technology (Intel® VT)

Intel® Virtualization Technology or Intel® VT is a feature that, along with the processor, chipset, BIOS, and enabling software, improves traditional software-based virtualization. Taking advantage of offloading workloads to system hardware, these integrated features enable virtualization software to provide more streamlined software stacks and “near native” performance characteristics. Virtualization solutions enhanced by Intel VT allow a platform to run multiple operating systems (OSs) and applications as independent virtual machines, allowing one computer system to function as multiple “virtual” systems. For example, IT managers can create a single build with multiple and different OSs, software, and legacy applications (Intel Corporation, 2007).

For more details regarding Intel Virtualization Technology, visit

[http://www.intel.com/technology/virtualization/technology.htm?iid=tech\\_vt+tech](http://www.intel.com/technology/virtualization/technology.htm?iid=tech_vt+tech)

#### 2.1.1 Intel® VT-x

Intel® Virtualization Technology for IA32, Intel® 64 and Intel® Architecture (Intel VT-x) pertains to CPU virtualization. This is the type of virtualization that most client virtualization applications make use of to increase performance of the virtual machines. Without this feature, all of the CPU processing would have to be emulated in software, paying a huge performance tax in any virtual machine running in this manner.

#### 2.1.2 Intel® VT-d

Intel® Virtualization Technology for Directed I/O (Intel VT-d) is the ability to give virtual machines direct access to devices in the chipset, allowing the I/O traffic between the virtual machine and the device to flow directly and not have to be managed by the hypervisor. Devices that are assigned to a virtual machine are only available to the specific virtual machine they are assigned. For example, if a graphics device is assigned to a virtual machine, it can only be used by that specific virtual machine; however, the performance of that graphics device in the virtual machine will be “near native”.

## 2.2 Hardware and Software Considerations

Systems that are tasked with running one or more virtual environments need to have higher system specifications in order to run each environment at a user acceptable performance level. The system will need to have the total minimum system requirements of all host and virtual operating systems added together in order to operate at the minimum performance level. The Windows\* 7 64-bit OS minimum requirements are 2 GB of RAM and 20 GB of hard disk drive (HDD). So, for example, a system that will be running Windows 7 64-bit as both the host OS and the guest OS will need to have a total of 4 GB of RAM and at least a 40 GB HDD in order to meet the minimum requirements for both operating systems running concurrently. Below is a chart listing the specific hardware and software considerations that need to be taken into account when looking for a client platform to support a virtualization environment:

**Table 1: Desktop Virtualization System Considerations**

CPU	<p>Any processor that supports Intel® Virtualization Technology. A complete list of processors that have this support is listed here:</p> <ul style="list-style-type: none"> <li>▪ <a href="http://ark.intel.com/VTList.aspx">http://ark.intel.com/VTList.aspx</a></li> </ul> <p>All Intel® vPro™ branded platforms support Intel Virtualization Technology</p>
Memory (RAM)	<p>Each virtual machine dedicates a set amount of memory based on what is specified in the virtual machine settings. When the virtual machine starts up, that amount of memory is allocated from the host machine to the virtual machine.</p> <p>For most configurations that have a host OS running a single virtual machine, 4 GB of system memory is suggested for a good user experience. If multiple virtual machines need to run simultaneously or applications that require large amounts of memory need to run, consider increasing the amount of system memory to 8 GB or more to maintain performance.</p> <p>It is suggested that a 64-bit OS is used as the host OS as that will allow the OS to address greater than 3 GB of memory, making that memory available to both the host and guest OS environments.</p>
Hard Drive	<p>When a virtual machine is created, a hard drive size is set that limits the amount of hard drive space that a virtual machine can use. This virtual hard drive is stored as a file on the physical hard drive. Some virtualization applications allocate all of this space immediately and some allow the drive to grow as needed, but either way the hard drive in the platform needs to be large enough to accommodate both the host OS as well as any virtual machines (running or not) on the platform.</p> <p>Solid state drives provide an increase in I/O performance and may be another way to help increase performance in both the host and guest OS environments.</p>

Operating System and Virtualization Software	<p>The host OS running on the platform needs to support running the virtualization software that the IT department specifies. Most virtualization software runs on the major OS types (Windows, Linux*, and OSX).</p> <p>The host OS must also support Intel VT in order for the virtualization software to operate at peak performance.</p>
--	--



## 3 Choosing and Configuring the Host System

---

### 3.1 Choosing the Platform

Probably the most critical part of deploying a desktop virtualization configuration is choosing which platform to buy. The platform must support Intel VT and it must be able to run an operating system that is supported by the virtualization software. Most virtualization software packages have support for all of the major OSs: Windows, Linux, and OSX. For Windows and Linux users, the Intel® vPro™ technology based platforms offer the best performance and feature set for virtualization. The deciding factors should be:

1. Does the system fit well with the current platform management solution
2. Intel Virtualization Technology support in the platform
3. The host and guest OSs supported by the chosen virtualization application
4. System performance

IT departments should choose a virtualization application that has a broad list of supported host and guest OSs.

### 3.2 BIOS Settings

Before installing the virtualization software on the host OS, the BIOS settings must be configured so that the hardware is in a state that can be used by the virtualization software.

1. Enter your systems BIOS configuration menu.
2. Within the BIOS settings you'll need to enable the Intel VT setting.
  - a. Some BIOS may show both an Intel VT-x and an Intel VT-d setting. For the purposes of this document, Intel VT-x is the critical piece. However, if you are also interested in exploring chipset virtualization, then you should enable Intel VT-d as well.
  - b. Having Intel VT-d enabled should not affect the procedures discussed in this document.
3. Save the settings and exit the BIOS.

#### 3.2.1 Host OS

The IT group generally has a pre-set build that has all of the supported applications and tools already installed. In order to support users running a virtual machine for their personal applications, a type 2 hypervisor will also need to be added to this image with permissions for the user to install a new VM on the hypervisor. Alternatively, the IT group could provide a base OS image that gives the users full administrator rights to modify as they see fit.

## 4 Configuring the VM Application

---

There are many different virtualization applications available to implement a desktop virtualization strategy. In this next section, the document will cover details around how to setup and configure a virtualization application. The examples used in this section will be based on the VMWare\* Workstation 7.1 software application. The reason this application was chosen was due to its implementation of Intel VT-x w/EPT and AES-NI, both of which are new features that are currently available only on Intel® processors code named Westmere. Intel® vPro™ technology based platforms are the only business clients that make this processor and these new features available to customers.

### 4.1 Installing the VM Application

Installing VMWare Workstation 7.1 is a straightforward process. There is nothing special that needs to be done during the installation process to ensure the Intel VT-x w/EPT or AES-NI features are enabled. To purchase or get a trial version of the software along with the full instructions on how to install and use VMWare Workstation 7.1, please go to the VMWare Workstation web site:

<http://www.vmware.com/products/workstation/>

### 4.2 Installing the IT OS Build

This next section will cover what is needed to be done to install a new VM on the hypervisor. If the IT group provides the base image for users, then it is assumed that the IT group already performed these steps.

## 4.2.1 Installing a VM from the OS Installation Disc

Before you can install a fresh OS onto a virtual machine (VM) you need to configure the properties of the VM. The following steps will walk through the creation process using VMWare Workstation 7.1. Most virtualization software follows very similar steps and should have similar settings.

1. In VMWare Workstation, on the Home tab, click **New Virtual Machine**.

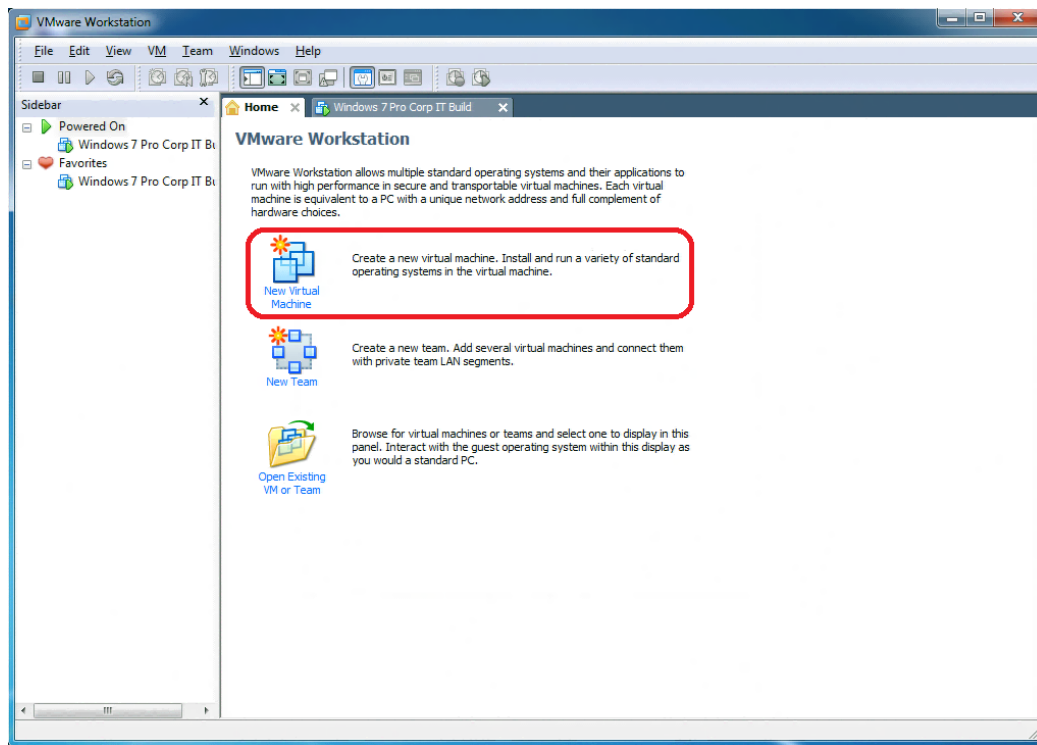
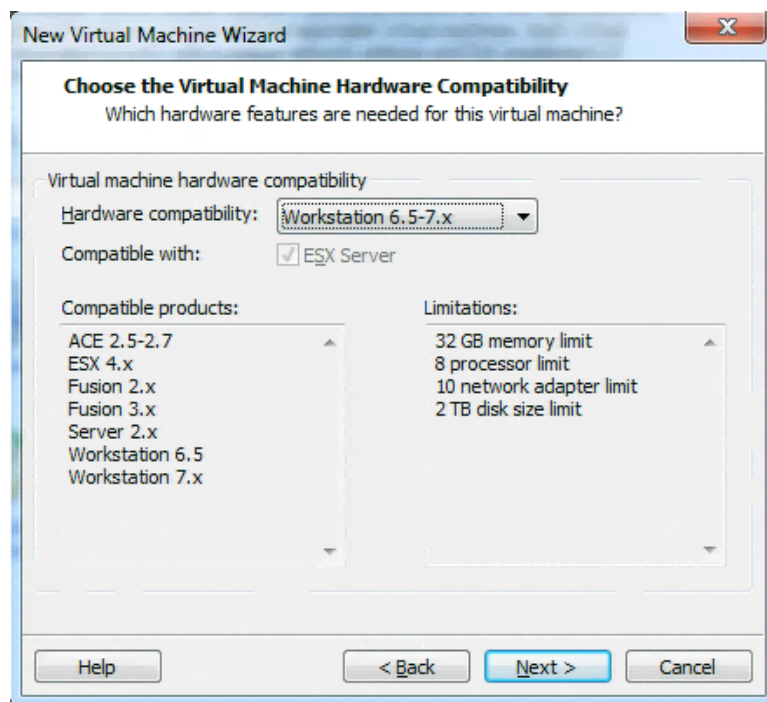


Figure 1: VMWare\* Workstation Home Tab

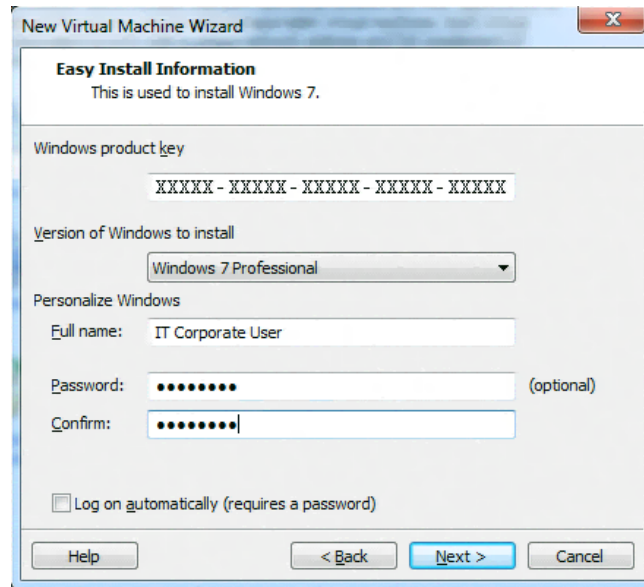
2. The New Virtual Machine Wizard dialogue box appears. There are two options available: Typical and Custom. Typical is fairly straightforward and skips some options such as processor and memory configuration that may be important for a knowledgeable user or IT shop to consider. These options can be modified after the VM is created, however. For the purposes of this document, we'll examine the "Custom" flow. Select **Custom (advanced)** and click **Next**.
3. The hardware compatibility page provides options to enable compatibility with previous versions of VMWare Workstation. Adjusting this setting impacts the hardware limitations that are available as well as compatibility with other VMWare products. Unless you have a need to be backwards compatible, select **Workstation 6.5-7.x** and click **Next**.



**Figure 2: Choosing the VM Hardware Compatibility**

4. The Guest Operating System Installation page asks where the install media is located. Either physical media or .iso files are acceptable. There is also an option to create the VM without installing an OS. This document will follow the "install from physical media" route. Select **DVD RW Drive** for **Installer disc** and click **Next**.
5. The Easy Install option in VMWare Workstation allows for an unattended installation of the OS. By entering in the activation key, username and password (optional), the OS is able to be installed without any user input. If a corporate build disc is being used that already has all of the information and scripts needed to configure the client on a fresh installation, then you only need to specify the

**Version of Windows to install** and **Full name** fields. The product key, password, and automatic log on do not need to be entered or selected. Click **Next** to proceed.



**Figure 3: Easy Install Information Screen**

6. The virtual machine name is used to identify the virtual machine in the VMWare Workstation application. This name is not used as part of the guest OS. Enter the virtual machine name and use **Browse** to enter the location, then click **Next**.

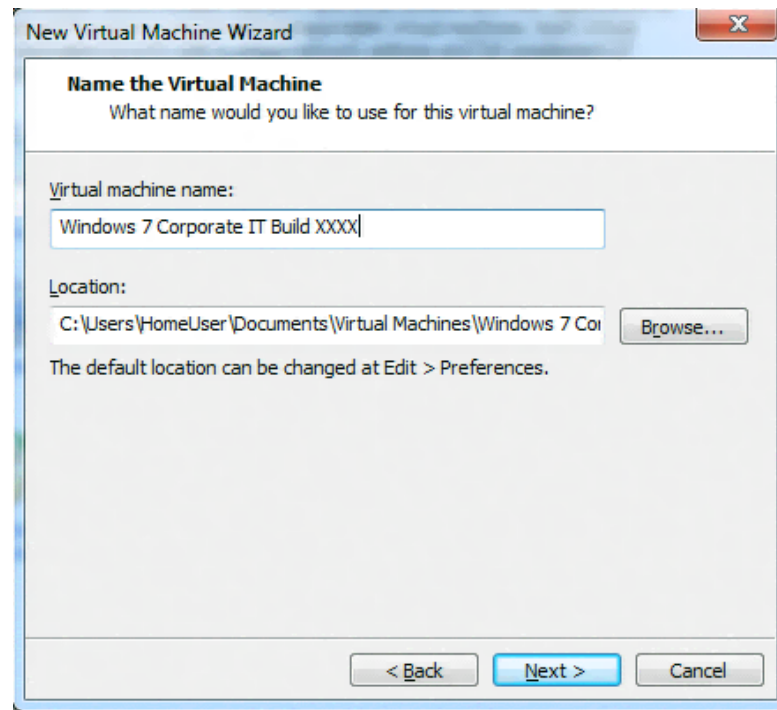


Figure 4: Virtual Machine Name and Location

7. The processor configuration page allows you to configure the number of processors and number of cores per processor that will be available in the virtual machine. This setting can have significant effect on whether a VM boots or not. If more virtual processors or cores are assigned to the VM than are available on the physical system, the VM will not boot. When creating a VM that will be imported to other machines of unknown hardware configuration, it is better to assign the minimum number of processors and cores. This setting can be increased after importing the VM to the specific machine based on the hardware capabilities of the machine. Specify the number of processors and cores, then click **Next** to continue.
8. The memory configuration page allows you to configure how much memory will be allocated to the virtual machine when it is started up. Again, it is usually best to set this value at the minimum when creating a new VM that will be imported to systems with unknown hardware configurations. However, IT policy could more easily set a minimum memory requirement for new system purchases that could allow memory size assumptions to be made. Unlike the processor configuration, exceeding available host memory will not prevent a VM from powering up; however, performance may be impacted.

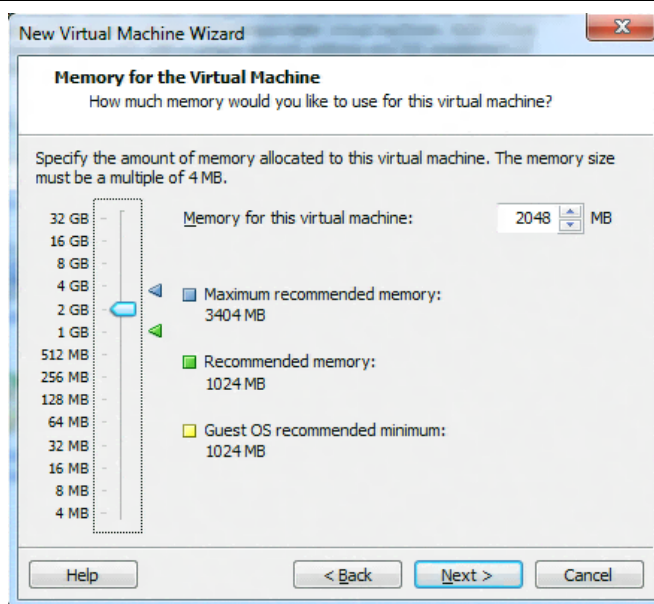
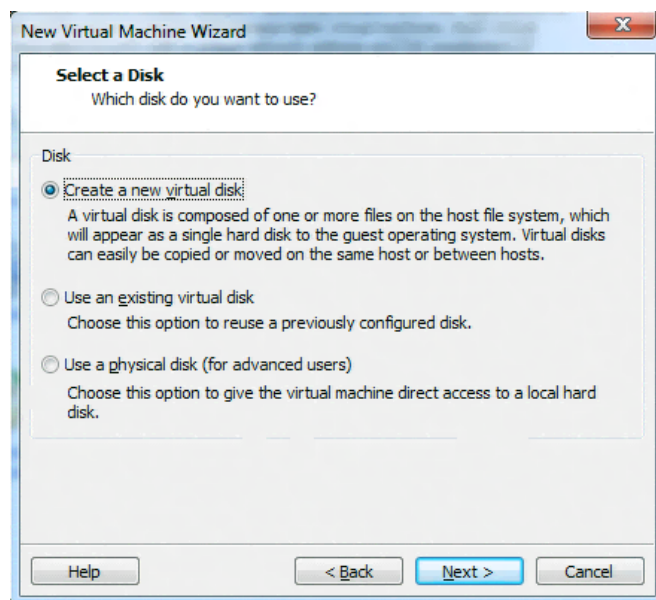


Figure 5: VM Memory Configuration

9. The Network Type screen allows you to specify how network packets are handled between the host OS and the guest OS. Bridged networking allows the guest OS to directly access the network hardware and makes it so the guest OS must have its own IP address on the network. Network Address Translation (NAT) shares the network connection between the host OS and the guest OS, both sharing the same IP address. Select a network connection type and click **Next**.
10. I/O controller type automatically marks the recommended selection based on the type of controller in your system. Click **Next** to accept the automatically selected choice.
11. Disk selection allows you to specify whether to create a new virtual disk, reuse an existing virtual disk, or assign a physical disk to be used. Virtual disks are essentially files that are stored on the physical disk and take up the amount of space specified for the virtual disk. From a performance consideration, virtual disks will have slightly lower performance than assigning a physical disk due to having to share the I/O bandwidth between both the guest and host OS. However, having a separate physical disk just for the virtual machine may not be practical in a mobile system. Select the desired type of disk to use and click **Next**.

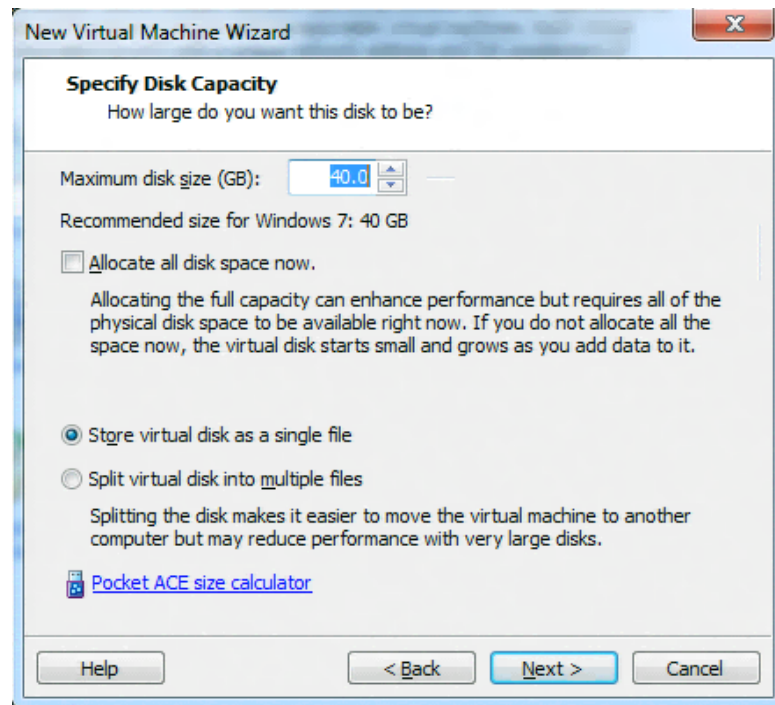


**Figure 6: Selecting a Disk to Use for the VM**

12. The disk type selection is automatically marked based on your controller type. Click **Next** to accept the automatic selection and proceed.



13. On the Specify Disk Capacity page, be sure to assign enough disk space to accommodate the guest OS plus all of the applications that will need to be stored there. The recommended size for Windows 7 is only 40 GB, but with large documents and email folders added in addition to other applications, drive size can easily exceed this. Allocate drive space accordingly, then click **Next** to continue.



**Figure 7: Specifying Disk Capacity**

14. The Specify Disk File page allows you to specify where the virtual disk file will be saved. Click **Browse** to specify the location, then click **Next** to continue.
15. The Ready to Create VM page provides a summary of the options selected and gives a final opportunity to change these settings by clicking the **Customize Hardware** button. Click **Finish** to create the VM and begin installing the OS using the information provided on the Easy Installation page.

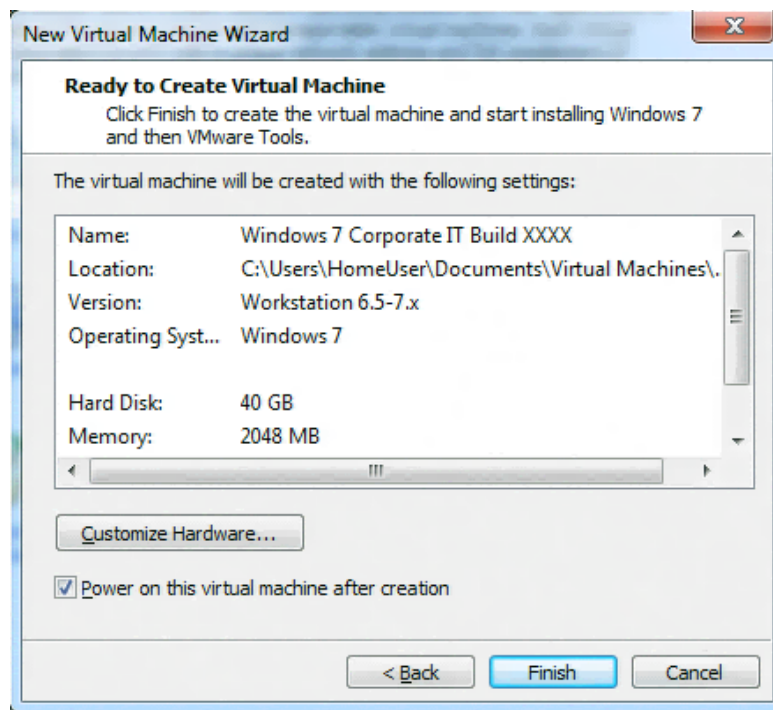


Figure 8: Summary of Configuration and Finish Button

## 4.2.2 Exporting a VM

Once the OS installation has completed, some finalization options may need to be configured if they weren't already provided in as part of the build disk. Once the image is completed, the VM can be saved off as a golden image. In VMWare Workstation 7.1 this can be done by copying the VM directory and all of the contents. The default location for this in Windows 7 is <OS Drive Letter>:\Users\<User Name>\My Documents\Virtual Machines\.

## 4.2.3 Importing a VM

Importing a VM onto a machine is similar to exporting a VM. Saving the VM files into the <OS Drive Letter>:\Users\<User Name>\My Documents\Virtual Machines\ location is preferred but is not required for a VM to function. In order to add a VM to VMWare Workstation 7.1, click **File -> Open** and navigate to the location of the VM files. Select the .vmx file and click **Open** to add the VM to VMWare Workstation 7.1.

## 4.3 Enabling Intel VT-x with EPT and AES-NI

Whether the IT OS Build is installed manually or imported, there are a couple settings that will need to be configured in order to take full advantage of the Intel VT-x with EPT and AES-NI features.

1. Using VMWare Workstation 7.1 and with the virtual machine turned off, locate the virtual machine tab that you want to make changes to.
2. On the selected virtual machine's information page, select the **Devices** tab.

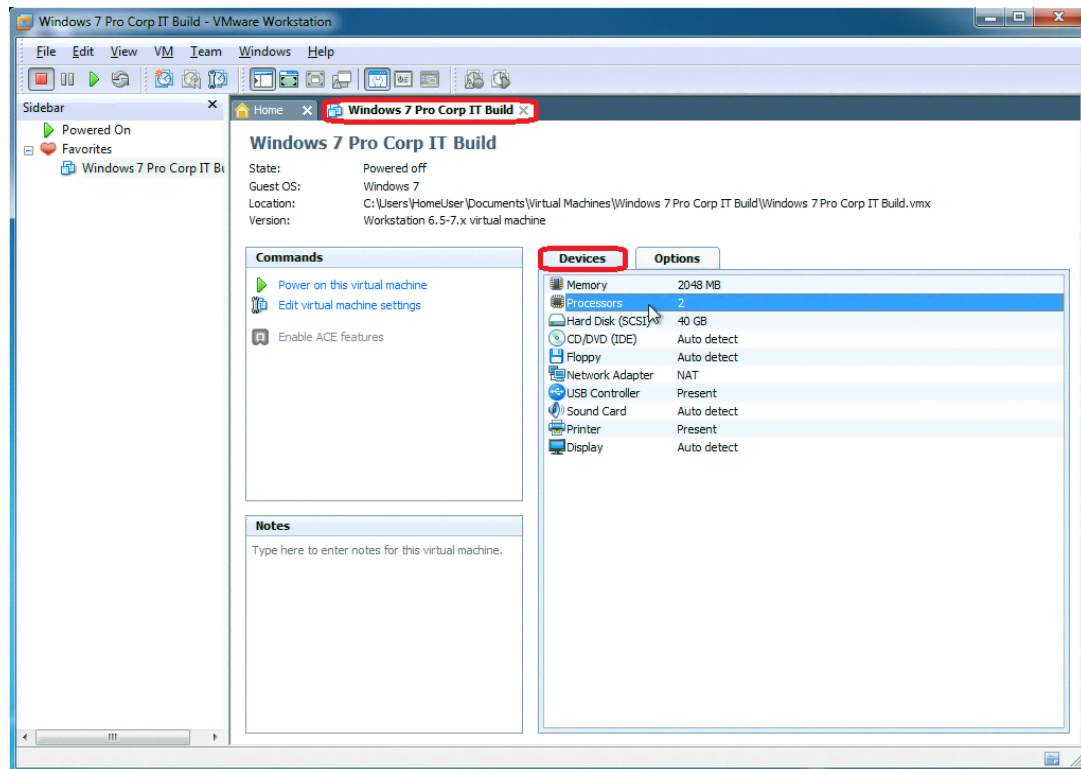
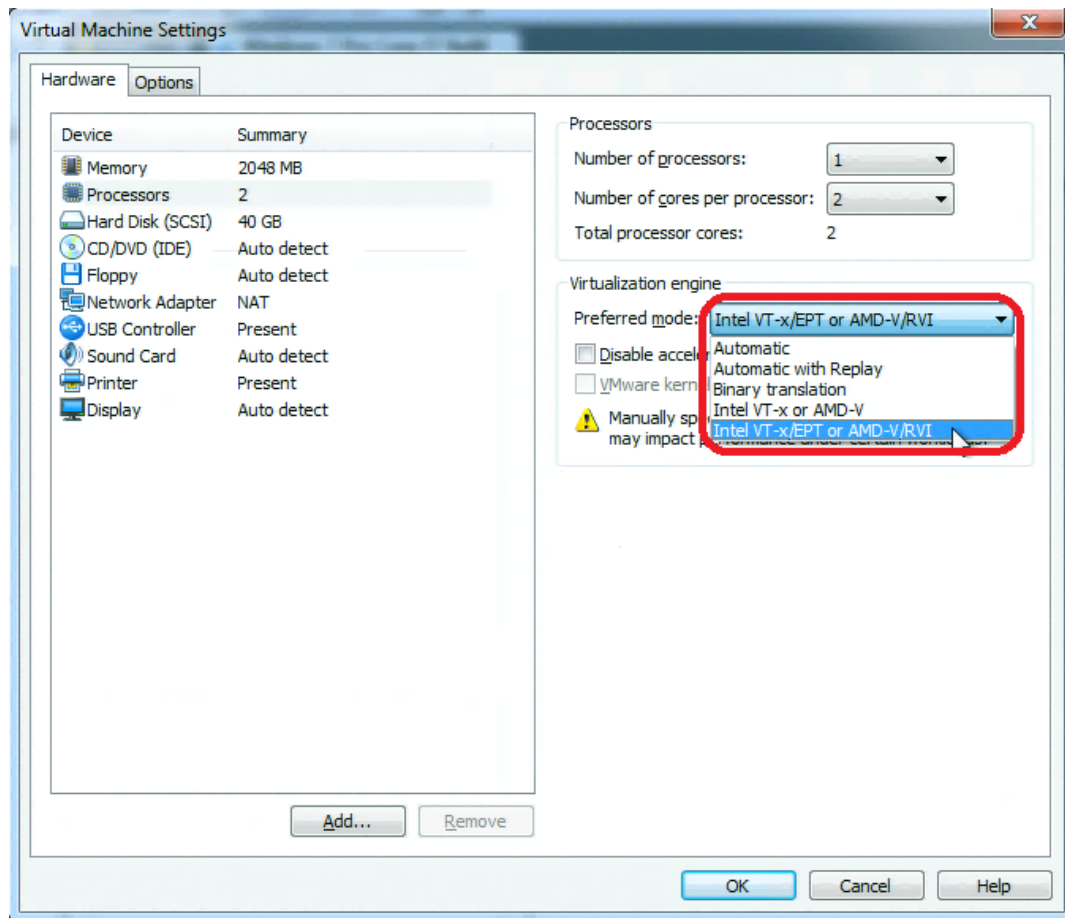


Figure 9: The VM Devices Tab

3. On the Devices tab, double-click the **Processors** item. A new window is displayed with the processors settings highlighted.

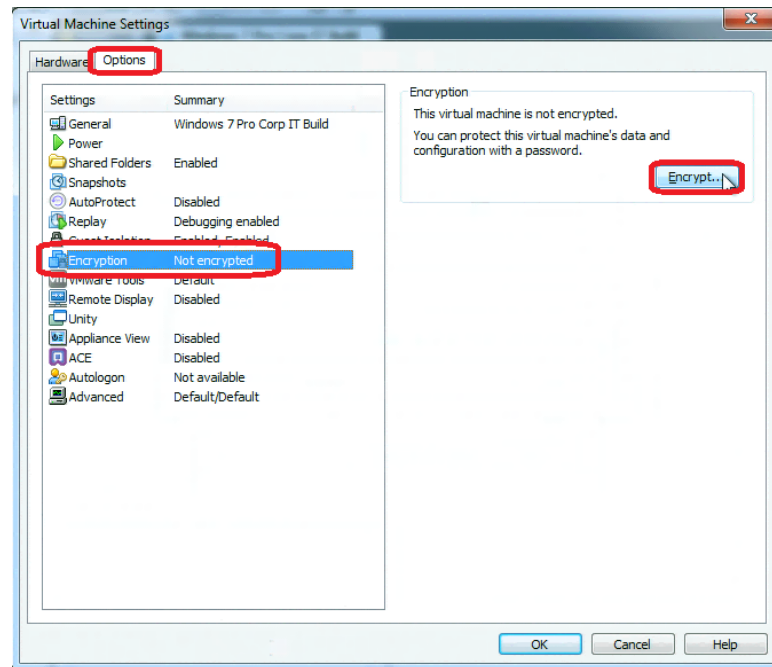
4. Select **Intel VT-x/EPT or AMD-V/RVI** for **Preferred mode** as shown below. You may see a warning below stating that manually specifying the virtualization mode engine may impact performance under certain workloads.



**Figure 10: Selecting the Preferred Mode**

5. At the top of the Virtual Machine Settings window, select the **Options** tab.

6. Under **Settings**, select **Encryption** and click **Encrypt** in the right-hand pane.



**Figure 11: Selecting Encryption**

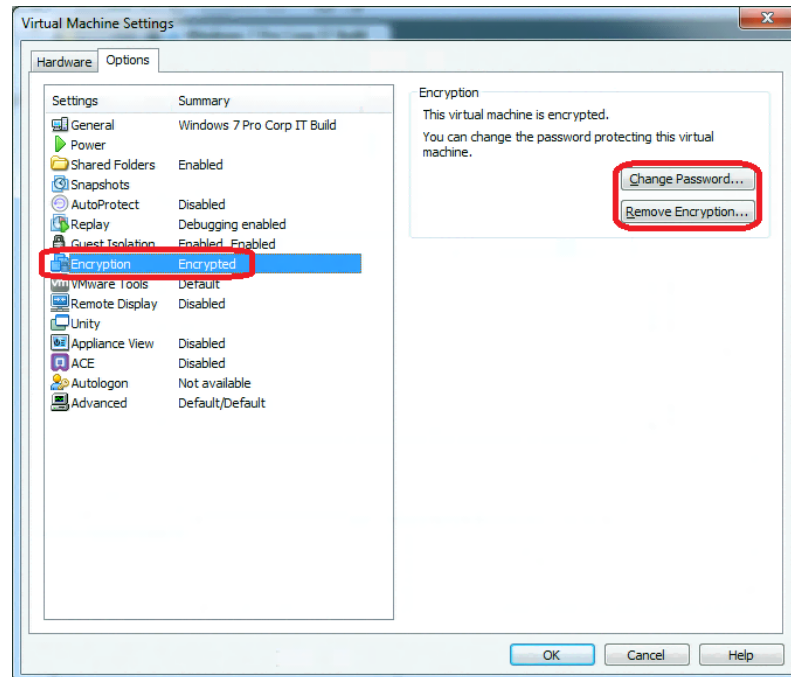
7. A dialog is displayed asking you to enter a password. Enter in a password that meets the IT password policy strength requirements and click **Encrypt**.



**Figure 12: Setting Password**

8. A progress bar is displayed showing the progress of the encryption process.

9. Once complete, you'll have the option to change the encryption password or remove encryption on this same page. Click **OK** to close the virtual machine settings window.



**Figure 13: Option to Change Password or Remove Encryption**

Once a VM is encrypted the encryption password will have to be entered when the VM is started or added to a machine.

There is no specific setting for AES-NI, but by using encryption on the virtual machine, VMWare makes use of the new instructions to speed up the performance of encryption/decryption tasks. For more information about the specific AES-NI functions, refer to this article on the Intel web site: <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/>

## 4.4 Unity Mode

VMWare includes a feature called Unity mode in which all open windows, whether launched from the VM or from the host OS, appear to be running on the host OS desktop. Other virtualization packages have similar features (some vendors refer to this as “coherence” mode, others as “seamless” mode, etc.).

In this mode, the virtual machine desktop is hidden and moving between applications running in the virtual machine and host OS is seamless. Features such as “cut and paste” and “drag and drop” are even enabled for some items. Notable exceptions are potential security and vulnerability items such as web addresses.

### 4.4.1 Enabling Unity Mode in VMWare\*

In order to enable this mode, the virtual machine must have the virtual application software's tools installed. In VMWare, this software toolset is VMWare Tools, which can be pushed from the virtual application software. Other virtualization software products may differ from the following instructions.

1. In VMWare Workstation 7.1, right-click on the virtual machine that is running and select **Install VMWare Tools...** from the menu, as shown in Figure 14 below.

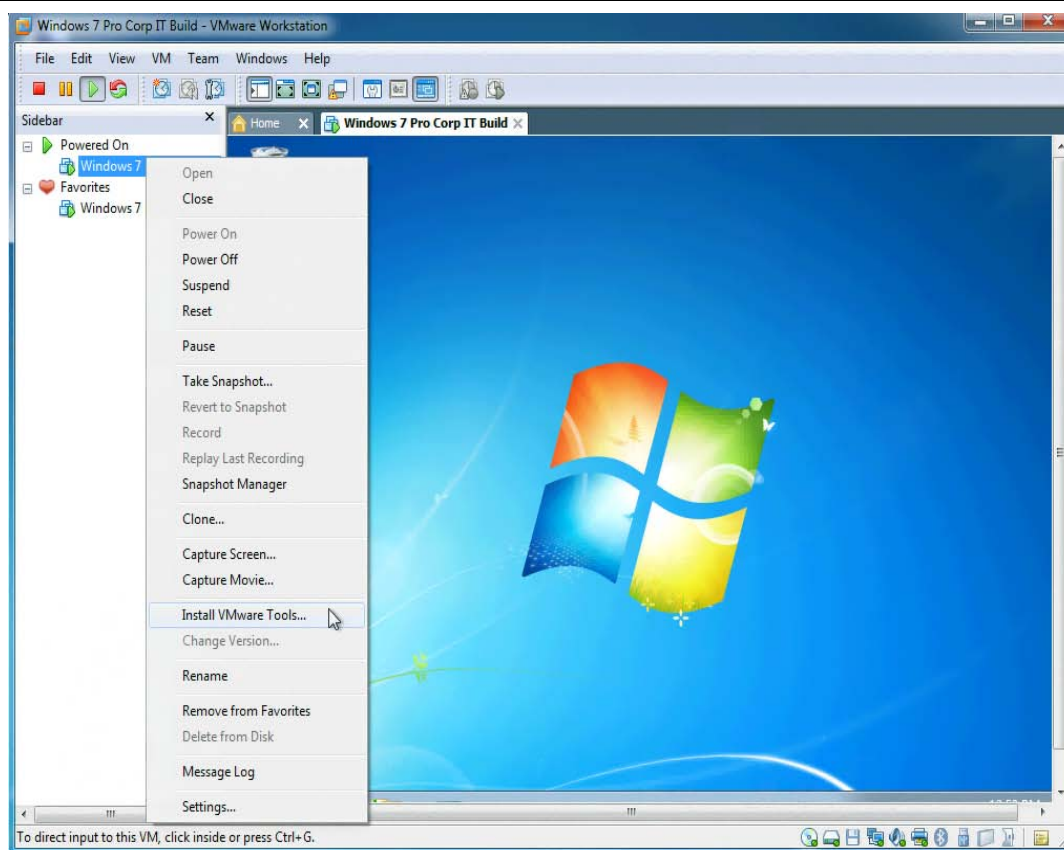


Figure 14: Select Install VMWare Tools

- 
2. A dialog box is displayed. Note the dialog's message and then click **Install**.
3. An auto-run window is displayed. Click **Run Setup.exe**.

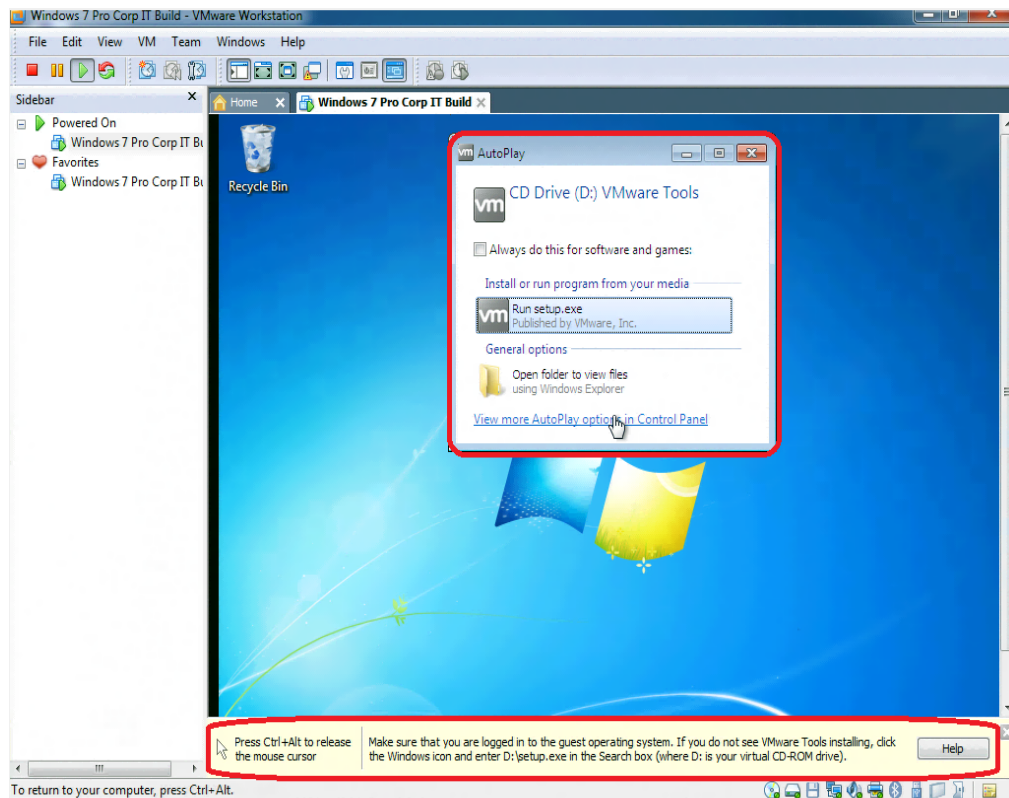


Figure 15: Run setup.exe

- 
- 
- 
4. If you have User Account Control enabled, a dialog box asking for permission to install the software is displayed. Click **Yes** to continue.
5. A splash screen is displayed while the tools are extracted.
6. On the Installation Wizard Welcome screen, click **Next**.



7. On the Setup Type page, choose the type of installation you want to perform.  
**Typical** will install all of the features needed to run on VMWare Workstation 7.1. If you want to use this virtual machine with other VMWare products, such as VMWare Viewer, then choose **Complete** installation.

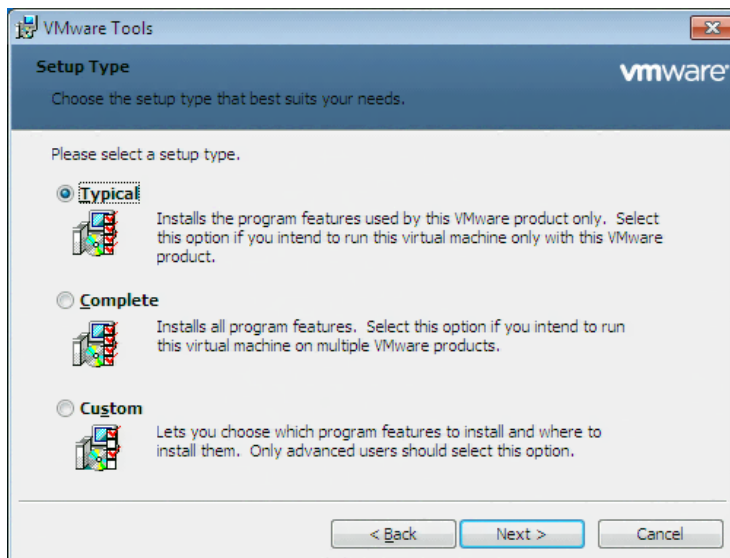


Figure 16: Choose an Installation Type

8. On the final page of the wizard, click **Install**. A progress bar is displayed showing the status of the installation. Once the installation is complete, click **Finish**.
9. After installation, you will be required to reboot the virtual machine before the tools can be used.

#### 4.4.2 Using Unity Mode in VMWare

At this point the Unity feature is now available to use. Click the **Unity** button, as shown in Figure 17, to begin using this feature.

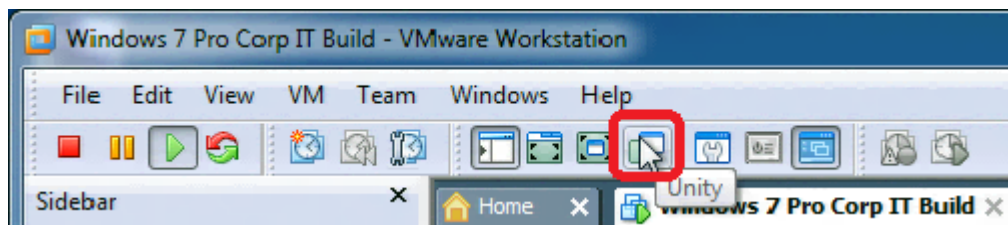


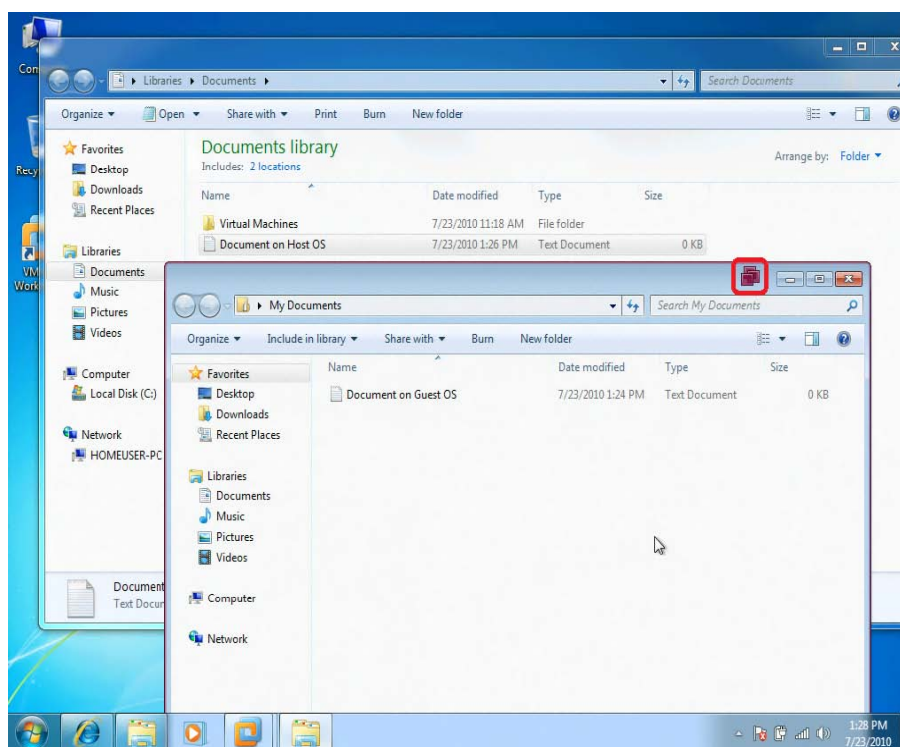
Figure 17: The Unity Button

The VMware window will minimize to the desktop and it will appear as though the client only has the host OS desktop. However, if you hover over the **Start** button, a separate **Start** button will appear as shown below.



**Figure 18: VM Start Button**

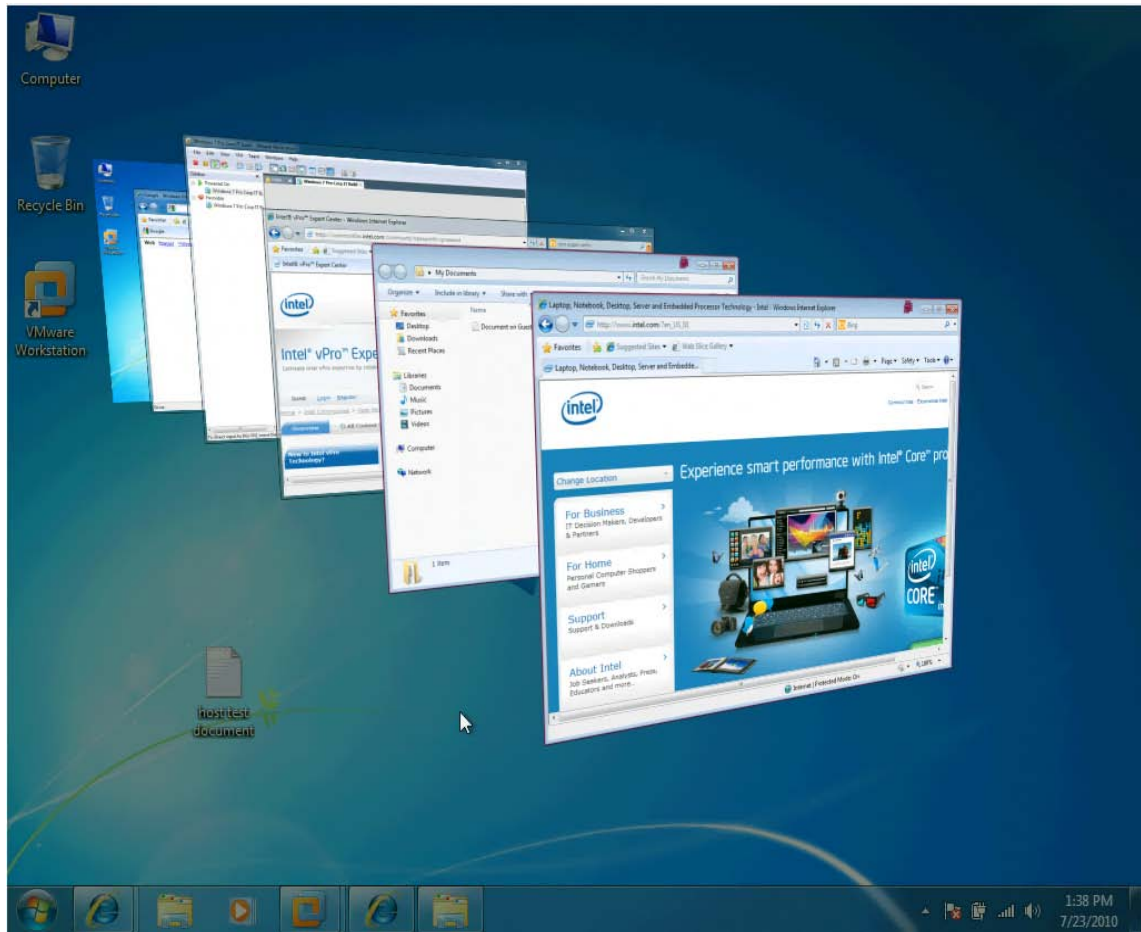
This **Start** button is for the virtual machine. Running applications from this menu will launch the applications in the virtual machine, but show them on the host OS desktop as if the application was running on the host OS.



**Figure 19: Example of Open Folders in Both VM and Host OS**

In Figure 19 above you see the desktop of the host OS with the documents folder and in front of that the documents folder of the virtual machine. With VMWare, virtual machine windows have a special icon as highlighted in red in Figure 19.

Also, the entire window is outlined in the same color as the icon. This color is configurable and can be unique to each virtual machine running on the host OS so you can tell which window belongs to which virtual machine when multiple virtual machines are running at the same time.



**Figure 20: Aero™ Desktop Display for VM and Host Applications**

This mode also works well with the Aero™ Desktop method of quickly switching between open applications and windows, shown in Figure 20 above. The applications running in the virtual machine show up on the task bar of the host OS allowing those windows to be access easily from a single task bar.

## 4.5 Security Between Host OS and Guest OS

Depending on the security policies of the IT department, there are varying amounts of sharing that can happen between the host OS and the guest OS. This can range from no sharing at all between the two environments up to allowing “cut and paste” and file sharing. Most virtualization applications have some amount of configurability with regard to security. Below are a couple of screen shots of the options found in VMWare Workstation 7.1.

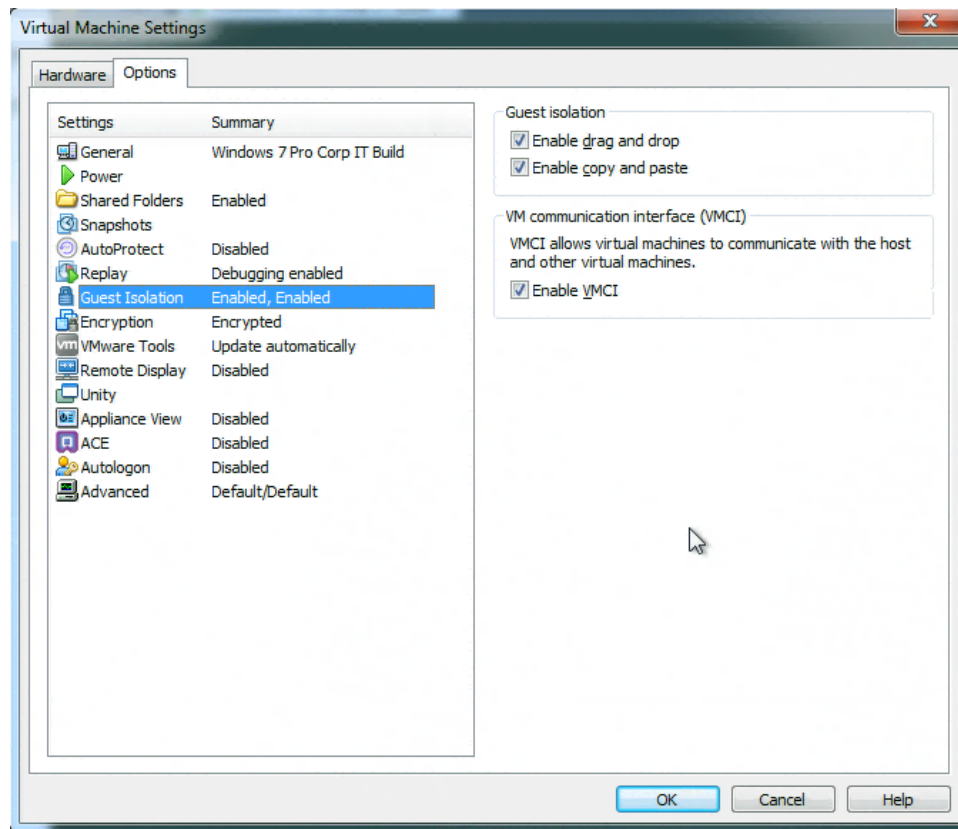


Figure 21: Security Options

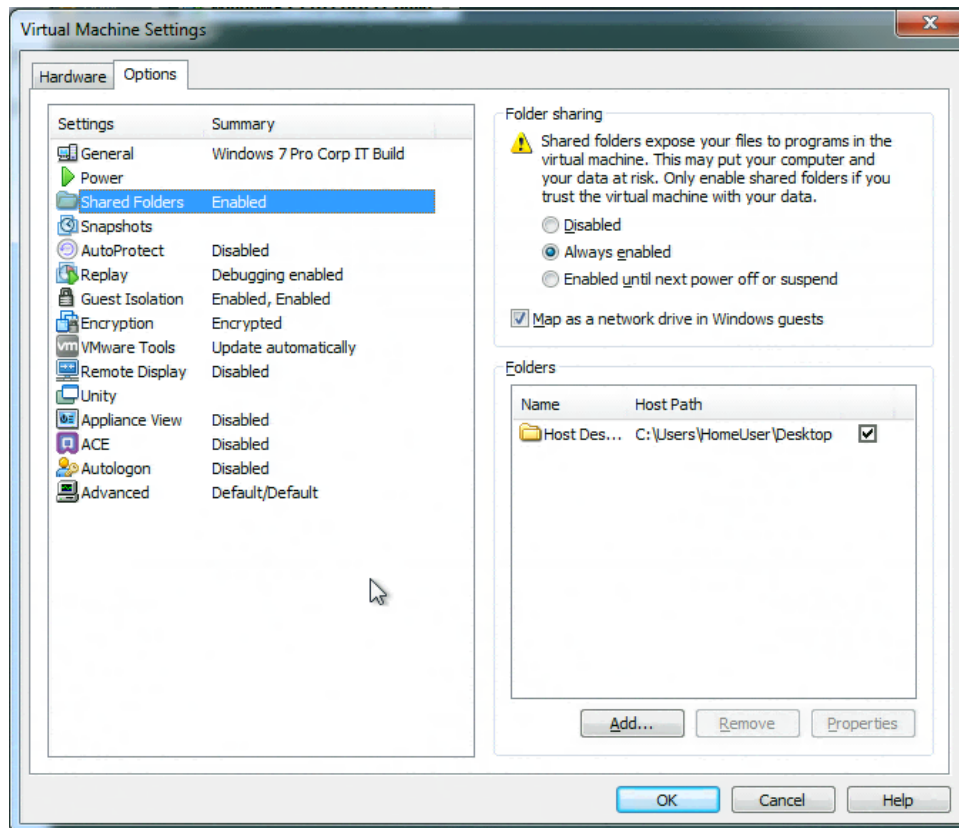


Figure 22: Further Security Options