Pano Virtual Desktop Solution Administrator's Guide

v2.5.1

February 3, 2009

Copyrights and Trademarks

Publication Change Record

The following table records all revisions to this publication. This first entry is always the publication's initial release. Each entry indicates the date of the release and the number of the system release to which the revision corresponds.

Date	System Release
December 2008	v2.5.1

This document uses different typefaces to indicate different kinds of information. The following table explains these typographical conventions.

Font	Meaning
`CourierNew`	Indicates error messages, file name, or screen output.
`Bold`	In a command line, indicates information to be entered exactly as shown.
`Italics`	In a command line, indicates a variable for which you should substitute an appropriate value.

Table of Contents

Preface

About This Book

This book describes the installation and administration of the Pano® Virtual Desktop Solution.

Who Should Use This Book

This book is intended to support System Administrators that need to deploy and maintain the Pano Virtual Desktop Solution.

Related Documentation

The following documents contain additional information relevant to installing, maintaining, and administering Pano Virtual Desktop Solution.

- ***Pano Virtual Desktop Solution Release Notes*** - This book outlines what's new in the release and what known issues were fixed in the release. This book is available online at www.panologic.com and through the *Pano Online Help*.
- ***Pano Virtual Desktop Solution Administrator's Guide*** - This book provides step-by-step instructions about how to install and configure the Pano Virtual Desktop Solution. This book is available online at www.panologic.com and through the *Pano Online Help*.
- ***Pano Logic Quick Start Guide*** - This book provides step-by-step instructions about how to set up the Pano device. This book shipped with the Product Media Kit, and is available online at www.panologic.com.

For additional documentation, go to www.panologic.com.

Typographical Conventions

This document uses different typefaces to indicate different kinds of information. The following table explains these typographical conventions.

Font	Meaning
`CourierNew`	Indicates error messages, file name, or screen output.
`Bold`	In a command line, indicates information to be entered exactly as shown.
`Italics`	In a command line, indicates a variable for which you should substitute an appropriate value.

Contacting Pano Logic

Pano Logic Technical Support:

- support@panologic.com or
- (650) 454-8966

1

Pano VDS Overview

The Pano Virtual Desktop Solution (Pano VDS) comprises physical client devices, centralized management software, software services running within each virtual machine, and underlying virtualization infrastructure.

The Pano VDS enables organizations to centralize user desktop computers inside the IT Data Center. Instead of having user desktops stationed at each user's desk, you can run these desktops as virtual desktops on a server that is hosted inside your data center. The server is based on VMware ESX virtualization platform.

Users connect to their virtual desktops using Pano® devices and Pano VDS. Pano VDS is software that runs inside the data center. The Pano device is only hardware; it does not run any software.

The Pano VDS comprises a few main components:

- Pano Device - a zero client: it has no CPU, no memory, no operating system, no drivers, no software, and no moving parts. The Pano device connects keyboard, mouse, display, audio and USB peripherals over an existing IP network to an instance of Windows XP or Vista running on a virtualized server.
- Pano Manager - Pano Logic's centralized service and web-based management interface that enables administrators to manage the entire virtual desktop installation by integrating with existing directory services and virtual infrastructure managers. Pano Manager also has connection broker functionality. A connection broker integrates with your directory service for user authentication, and is responsible for connecting a Pano device to a user's DVM.
- Pano Desktop Service - A lightweight service residing within each virtual machine links peripherals that are attached to the Pano device to the unmodified Windows drivers residing in the virtual machine. This design guarantees that all existing Windows drivers work without modification.
- Virtualization Layer - Pano Logic's system that leverages server-based virtualization software such as VMware Virtual Infrastructure 3.

Pano Device

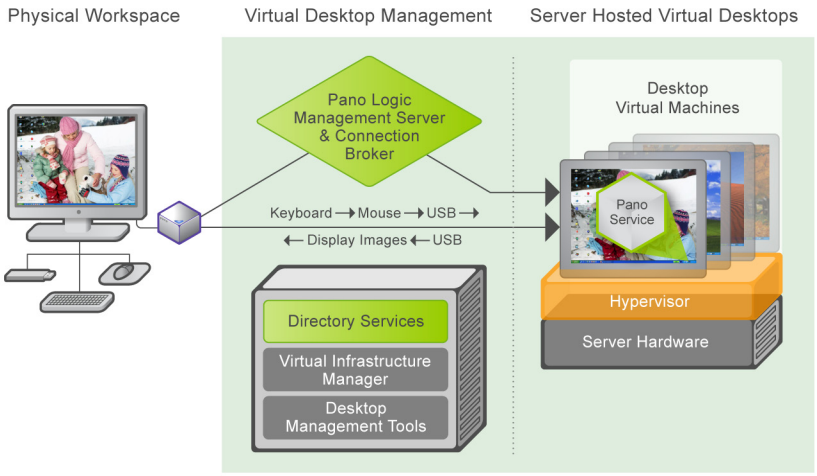
The Pano device is specifically designed for server-based desktop virtualization. Because the Pano device is 100% hardware, all software can now run in the data center, where all your software can be centrally managed and effectively protected.

The Pano device connects to your standard PC peripherals including keyboard, mouse, video monitor, Ethernet network, audio speakers/headphones and a wide variety of USB devices such as thumb drives, CD/DVD drives and additional peripherals. For a list of supported devices, go to "Supported USB Devices" on page 32.

The Pano device is stateless—it contains no intelligence or software memory—and is controlled by centralized services such as the Pano Manager and DHCP. The Pano device includes a single button—the Pano Button™—that initiates out-of-band management of a user's virtual desktop. For example, the user can receive a fresh virtual machine, cloned from a golden image, simply by pushing the Pano Button.

A Pano device consumes only 3% of the energy consumed by a traditional desktop computer and contains no moving parts or compute resources that would require frequent upgrades or replacement.

A Pano device provides a desktop experience to the user by communicating with Pano Manager and DVMs (desktop virtual machines), as shown in the following illustration. The Physical Workspace layer is the only area that is not in the data center; the Virtual Desktop Management and Server Hosted Virtual Desktops layers are hosted within the data center.



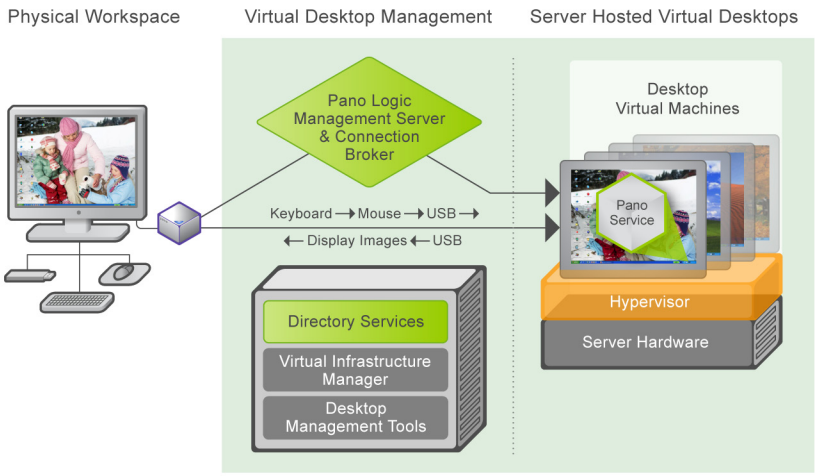
Pano Manager

The Pano Manager is a centrally-hosted server that is delivered in the form of a virtual appliance. The Pano Manager typically runs as a virtual machine located on the same host servers as your desktop virtual machines.

The Pano Manager is the central point of control for all of your Pano devices; it integrates with your directory service and VMware VirtualCenter to manage, deploy, and connect virtual desktops to end users.

The Pano Manager provides secure access to virtual desktops by leveraging Microsoft Active Directory, Novell eDirectory or OpenLDAP for authentication and login.

The Pano Manager also provides a web-based interface that enables users to connect to their desktop virtual machines from traditional PCs or laptops for those times when users are not in front of a Pano device.



Pano Manager has a built-in connection broker functionality. Both the Pano Manager and the connection broker reside on virtual machines that run on the VMware VI3 (Hypervisor).

The connection broker uses the Directory Services (typically Microsoft Active Directory) and the management tools provided by the virtualization provider (VMware VirtualCenter) to connect a Pano device to a user's DVM.

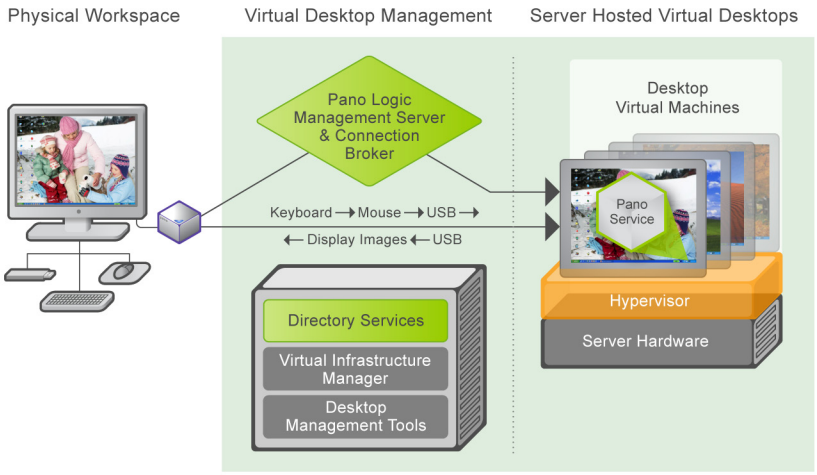
The connection broker is responsible for a couple of important tasks. The connection broker:

- Receives the user credential that users input from the Pano Control Panel, and relays that information to the directory service for authentication.
- Communicates with all desktop agents in the DVMs so that the correct virtual desktops can be associated with the correct user.

Pano Desktop Service

This lightweight Pano Desktop Service (Pano DAS) runs within each DVM. Pano DAS is installed on top of your Windows desktop operating system(s) and allows the desktop session and peripheral I/O to be transmitted securely over your standard IP network.

The Pano Control Panel, which is part of the Pano DAS, allows individual users to set their personal preferences for keyboard, mouse, display and audio settings.



Virtualization Layer

Pano Logic's system leverages server-based virtualization software such as VMware Virtual Infrastructure 3 (VI3) to abstract processor, memory, storage and networking resources into multiple virtual machines, to give you greater hardware utilization and flexibility.

By having the desktops run on top of a hypervisor such as VMware VI3, you can take advantage of VMware technologies such as DRS, VMotion, and HA to provide a more robust and fault tolerant desktop delivery mechanism.

2
Pano VDS Concepts

To understand Pano Virtual Desktop Solution (Pano VDS), let's explore a few key concepts:

DVMs

A desktop virtual machine (DVM) is a virtual machine that runs a desktop operating system such as Windows XP or Vista. DVMs run on top of a virtualized infrastructure hosted on one or more servers.

From the perspective of VMware products (ESX and VirtualCenter) there is no distinction or difference between a DVM and a standard virtual machine. The same types of operations that can be performed on a standard virtual machine can be performed on a DVM. Pano Logic uses the term DVM to specifically refer to virtual machines that are being used as virtual desktops.

- When inside the corporate network, users can connect to DVMs through Pano devices as outlined in "Log On To DVMs as End User" on page 17.
- When outside the corporate network, users can establish a VPN connection from their remote location, then connect through software-based remote desktop connection clients to their DVMs as outlined in "Log On To DVMs as End User" on page 17.

DVM Collections

The Pano VDS introduces the concept of a collection of desktop virtual machines—virtual machines that are being used as virtual desktops. Rather than manage each DVM individually, you can manage a set of desktop virtual machines as a single logical entity. Such a set of DVMs is called a DVM collection.

VMware VirtualCenter provides the Virtual Machines & Templates view to help you organize and manage virtual machines. DVM collections rely on this folder organization. For instance, when you configure a DVM collection, you specify a folder that contains the virtual machines. Pano Manager manages all virtual machines that reside in the specified folder. Go to "Organize DVMs, Templates, Folder in VirtualCenter" on page 107 for tips about how to best organize your folders.

Once defined, you can manage a DVM collection as a logical unit. You can assign users to a DVM collection by simply associating directory objects (groups and users) to the DVM collection using the Management User Interface (MUI). You can also configure DVM collections to grow dynamically as user demand grows.

A key characteristic of a DVM collection is the method by which users or devices are mapped to DVMs. There are two basic methods by which mappings are determined: by *user* and by *device*. Hence, the following collection types:

• User Based Collections

These DVM assignments are based on the user accessing the system. Use User Based collections if you want users to be able to access their DVMs regardless of location. For instance, if you want your users to be able to roam freely throughout the workplace and always have access to their DVM, use one of the User Based collections. For more information, go to "User Based Collections" on page 6.

• Device Based Collections

These DVM assignments are based on the device that is being used to access the system. Use Device Based collections if you want a Pano device to always connect to a specific DVM. For more information, go to "Device Based Collections" on page 7.

• 3rd Party Connection Broker Collections

This special type of collection is used when Pano VDS is used in conjunction with VMware View Manager (formerly known as VMware VDM). Use of VMware View with Pano VDS is optional. For details, go to "Integrate Pano VDS with VMware View" on page 133.

User Based Collections

With User Based collections, Pano devices display the Pano client login screen whenever the device is not connected to a DVM. Users can enter their credentials at the Pano client login screen and be connected to their DVMs.

There are a few User Based collections from which you can choose:

• Pooled Desktops

Within a Pooled Desktops collection type, DVMs are created automatically and temporarily allocated to users upon login. DVM are returned to the pool upon logoff.

DVMs are automatically created from a specified template and assigned to users by the Pano Manager. The set of users that are entitled to use the collection is specified in the Users field of the collection properties.

Assignment of DVMs in a Pooled Desktops collection type is on a per session basis: as soon as the user's Windows session ends (by logging out of Windows), the DVM becomes available for another user. Users of a Pooled Desktops collection type typically run the same set of applications as all other users. Windows roaming profiles and folder redirection can be used to give users a more personalized experience.

• Permanently Assigned Desktops

Desktops are created automatically and permanently assigned to users upon first login. Once assigned, users retain the same dedicated desktop until unassigned by the Administrator.

The set of users that are entitled to use the collection is specified in the Users field of the collection properties. Once a user is assigned to an available DVM, the user is given the same dedicated DVM every time the user logs in to the user's system.

Assignment of the user to the DVM is automatically established the first time the user logs in. Alternatively, the administrator can assign a particular DVM to the user through the Pano Manager's web interface. Permanently Assigned Desktops collection types allow you to leverage automated provisioning, while providing users a dedicated DVM which they can customize and personalize.

• Existing Desktops

The Existing Desktops collection type is created manually by the Administrator and temporarily allocated to users upon login.

DVMs that are part of the VirtualCenter inventory can be manually assigned to users by the Administrator. The set of users that are entitled to use the collection is specified in the Users field of the collection properties.

The Existing Desktops collection type is appropriate when you want to establish a dedicated mapping between a user and a pre-existing or special DVM. A single Existing Desktops collection type should contain only one DVM; however, you can create multiple Existing Desktops collections.

• VMware VDM

When Pano Manager is set up with a VMware View, any credentials that users input through the Pano client login screen's are passed to a VMware View. Provisioning of the DVMs is done through VMware View.

In this scenario, the Pano Manager's function is to is to establish the connection between the Pano device and the DVM. Also, the Pano Manager does not communicate with VirtualCenter to start the DVM; rather, VMware View handles these tasks.

Device Based Collections

Device Based collections allow you to assign Pano devices, rather than users, to specified DVMs. This model is useful if you want to implement special usage scenarios, such as a kiosk or shared computer.

A kiosk is commonly defined as a limited purpose computer that supports multiple users. Kiosks are often placed in open locations where users can simply walk up and start using the device, perhaps without providing any credentials.

Access without user-supplied credentials is implemented by having the system automatically log on to Windows using credentials that are specified in the collection properties. The user experience is such that the user only sees the Windows desktop—not the Pano client login screen or the Windows login screen.

The operating system in a kiosk is generally locked down so that users cannot gain access to applications or networks that are restricted. You can find kiosks in public places such as libraries, company break rooms or corporate lobbies.

Creating a Device Based collection is similar to creating a User Based collection. Device Based collections take advantage of the automated provisioning features of the Pano Manager, allowing you to create and specify a template, while automating the cloning of new DVMs.

Once DVMs have been created, the next step is to assign a device. Device assignment can be performed through the Management User Interface (MUI) or by logging on for the first time from a device through the Pano client login screen.

Once assigned, the Pano Manager allows a device to connect to the designated DVM only. If you later want to use that device with a User Based collection, you must first unassign the device from the designated DVM.

There are three types of Device Based collections, and they are very similar and only differ in their process of logging on to Windows:

• Automatic Login

Use this collection if you want the Pano device to automatically log on to the DVMs using the *same* credentials throughout the collection.

DVMs are automatically created from a specified template. Pano devices are assigned to specific DVMs either through the Management Console or by logging in through the device for the first time. As soon as the Pano device comes up on the network and connects with the Pano Manager, the device automatically connects and logs in to the assigned DVM. The login credentials for the automatic logon into Windows are identical for each and every DVM in the collection. The account can be a local account or a domain account.

• Different Accounts w/ Automatic Login

Use the collection if you want the Pano device to automatically log on to the DVMs using *unique* credentials for each login device.

DVMs are automatically created from a specified template. Pano devices are assigned to specific DVMs either through the Management Console or by logging in through the device for the first time. As soon as the Pano device comes up on the network and connects with the Pano Manager, the device automatically connects and logs in to the assigned DVM. Upon automatically logging in to Windows, a unique account name and password will be used for each DVM in the collection. The accounts must be domain accounts and they must be members of the same security group.

• Windows Login

Use this collection if you only want the Pano device to connect to a DVM, but not log on to the actual DVM (i.e. display the Windows Login prompt).

DVMs are automatically created from a specified template. Pano devices are assigned to specific DVMs either through the Management Console or by logging in through the device for the first time.

As soon as the Pano device comes up on the network and connects with the Pano Manager, the Pano device automatically connects to the assigned DVM. Users must type their credentials at the Windows login prompt (also known as the Windows GINA).

Windows allows a Windows login screen to be displayed for only 2 minutes. If a user has not signed into Windows within 2 minutes, the Pano Manager re-establishes a connection with the DVM. This cycle repeats until a user logs in. Once logged in, the session remains active until the user logs out or disconnects.

Automated Deployment

All collection types, except Existing Desktops collection type, support automated deployment of virtual machines. The conditions under which new DVMs are automatically deployed are based on user demand and the values that you specify when the collection is created or updated.

Because deploying a new DVM from a template can take several minutes or more, depending on the size of the template being copied and the performance of the storage sub-system, the Pano VDS can automatically deploy extra DVMs but not assign them to users right away. When a new user signs into the collection, the Pano VDS automatically assigns that user to one of the extra DVMs, then deploys a new DVM to replenish the extra DVMs so future users do not need to wait for a new DVM to be deployed.

You can specify a certain number of extra DVMs that are pre-provisioned. Within this set of extra DVMs, some can be kept powered on for instant access, while others can be powered off to reduce resource utilization, but still provide fast access.

The **Extra Powered On** and **Extra Powered Off** values in the collection properties dialog determines how many extra DVMs you want the Pano Manager to maintain for the collection, and whether they should be powered on or off:

• If you specify a total of two extra DVMs

The Pano Manager starts deploying a new DVM whenever there are less than two DVMs not assigned to users. If three new users sign in at the same time, one of the users must wait for the Pano VDS to deploy a new DVM.

• If you specify zero extra DVMs

The Pano Manager automatically deploys the new DVMs, but only when a new user logs in. In this case, the user logs in to the Pano client login screen and the Pano Manager asks the user to wait while the Pano VDS deploys a new DVM specifically for that user. Once the DVM is ready, the user can complete the login process.

To turn off automated deployment for a collection, uncheck the **Deploy Enabled** option.

DVM Power Management

The Pano Manager has the ability to power DVMs on and off based on policies. By default, the Pano Manager enforces only the policies that turn DVMs on. If you want the Pano Manager to also enforce the policies that turn DVMs off, select the **Power Off Enabled** option in the collection properties screen.

For the purposes of power management, DVMs can be:

- **Active DVMs** - DVMs that are in use (i.e. a Windows session is in progress) or that have been assigned to users.
- **Extra DVMs** - DVMs that are not in a user session and are not assigned to a user. The Pano Manager allows you to specify how many extra DVMs to create, and how many of these should be powered on. This capability enables users to log on to a DVM quickly without having to wait for a new DVM to be created. If there are more DVMs than the sum of Active and Extra DVMs, those DVMs will be powered off, if the **Power Off Enabled** option is selected.

The power management policies are different for each type of DVM collection:

- **For Pooled Desktops collection type, Automatic Login collection type, Windows Login collection type, and Different Accounts w/ Automatic Login collection type**
  - **Active** - automatically powered on.
  - **Extra** - automatically managed based on the values specified in **Extra Powered On** and **Extra Powered Off** values. If there are more DVMs than the Sum of Active and Extra DVMs then those DVMs will be powered off.
  - **Surplus** - automatically powered off, unless the **Power Off** option is disabled.
- **For Permanently Assigned Desktops collection type**
  - **Active** - the power states of active DVMs (DVMs that have been assigned to users) are not managed by the Pano Manager. The power state of a DVM is controlled by the end user and/or by VirtualCenter. The user of the DVM has the ability to control the power state of the DVM through the Pano Control Panel's Optional screen and when logging on to the DVM via the Pano device. Once logged into the DVM, the user can also use the Windows Security dialog box to control the power state of the DVM. A DVM's power state can also be controlled through VirtualCenter.
  - **Extra** - automatically managed based on the values specified in **Extra Powered On** and **Extra Powered Off** values.
- **For Existing Desktops collection type**

The power states of DVMs in a Existing Desktops collection type are not managed by the Pano Manager. The power state of a DVM is controlled by the end user and/or by VirtualCenter.

The user has the ability to control the power state of the DVM through the Pano Options screen when logging on to the system via the Pano device. Once logged into the DVM, the user can also use the Windows Security dialog box to control the power state of the DVM.

Automated Provisioning

The Pano Manager leverages VMware VirtualCenter's ability to:

- Clone virtual machines using *Templates*
- Automate Windows Sysprep process using a *Customization Specification*

The Pano Manager leverages VirtualCenter through tight integration with their APIs. Such integration enables the Pano Manager to automatically provision new DVMs through the cloning functionality of the template. Also through execution of the customization specification scripts, automated sysprep can be performed on each individual DVM that is generated from the template.

Pano Logic designed its solution to run on top of the VMware Infrastructure. Therefore, it is important to integrate with VMware's management component so that Pano VDS can have full control of the functionality of the DVMs that are available within VirtualCenter.

Automated provisioning lessens the resources required to quickly roll out any large size virtual desktop infrastructures. Automated provisioning also allows for very flexible desktop deployment models.

Templates

Pano Virtual Desktop Solution (Pano VDS) connects to a client OS (windows XP or Vista) desktop virtual machine (DVMs) stored inside a hypervisor. Templates are key to efficient management of DVMs. a template is a VMware VirtualCenter concept (tool) that refers to a virtual machine that is used as a base in Automated Provisioning of DVMs.

In a Pano VDS deployment there can be one or more templates. Typically, a template is associated with a specific role or department profile. It can be customized with specific hardware profile, installed software, etc., to conform to a department's requirements and unique needs. Example of templates might include:

• Nurse Station Template

A Nurse Station template has 512 MBs of RAM, a single CPU, and a 8GB hard disk. Software installed on this virtual machine template includes Medical Records System client software and Scheduling software. This template is used as base to provision DVMs for nurses' stations throughout the hospital.

• Call Center Template

A Call Center template has 384 MBs of RAM, a single CPU, and a 4GB hard disk. Software installed on this virtual machine template includes Call Answer Magic software. This template is used as base to provision DVMs for all the Call Center Agents.

• Help Desk Template

A Help Desk template has 512 MBs of RAM, a single CPU, and a 12GB hard disk. Software installed on this virtual machine template includes MS Office, Helpdesk System ticket tracking and Visio. This template is used as base to provision DVMs for the Help Desk team.

• System Administrator Template

A System Administrator template has 768 MBs of RAM, a single CPU, and a 10GB hard disk. Software installed on this virtual machine template includes MS Office and all the company's IT system management and administration client software and tools. This template is used as base to provision DVMs for the company's IT administrators.

3
The Basics

Switch Connection Modes

This version of the Pano DAS—v2.5.1, supports both Console Direct technology (Console Direct) and Pano Classic. By default the install wizard configures Pano DAS for Console Direct.

The Pano DAS and Pano devices can communicate with each other over a WAN or a LAN. Depending on your operating system, they can use either Pano Logic's Pano Classic application or Pano Logic's Console Direct technology.

Console Direct technology provides better performance because it works at a lower level (the operating system level) whereas RDP works at a higher level than Console Direct technology. Pano Logic has not yet optimized Console Direct technology for connections via WAN (Wide Area Network), but has plans to do so, so "stay tuned".

Console Direct optimizes the end user's experience at the cost of some extra network utilization. If you have 10Mbps of bandwidth or higher between the Pano device and the DVM, Pano DAS v2.5.1 with Console Direct works great. If you have less than 10Mbps end-to-end, Pano Logic recommends that you use Pano DAS v2.5.1 with Pano Classic.

Communication Method	Operating System	Greater than or equal to 10Mbps (LAN)	Less than or equal to 10Mbps
v2.5.1 Console Direct technology	Windows XP	✓	✗
	Vista	✗	✗
v2.5.1 Pano Classic	Windows XP	✓	✓
	Vista	✓	✓

Table 3.1 Console Direct technology vs. Pano Classic application Support

To switch to Pano Classic:

This utility will be replaced by another tool in a future release.

1. Log on to the desktop virtual machine as Administrator.
2. From the DVM, go to `\Program Files\Pano Logic, Inc\Pano Desktop Additions\Bin`.
3. From the command prompt, run the following command:

```
PanoDASCfg -Classic -Reboot
```

To switch to Console Direct:

This utility will be replaced by another tool in a future release.

1. Log on to the desktop virtual machine as Administrator.
2. From the DVM, go to `\Program Files\Pano Logic, Inc\Pano Desktop Additions\Bin`.

3. From the command prompt, run the following command:

```
PanoDASCfg -ConsoleDirect -Reboot
```

Pano Button's Light Indicators

Under normal operation, the Pano Button should have a solid blue color within a few seconds of powering on. Once it is solid blue it should remain in that state till the Pano device is powered off. The sequence is blinking red -> blinking orange -> solid orange -> solid blue. This process should not last for more than 15 seconds. If it doesn't, go to "Troubleshoot Networking Problems" on page 153).

The Pano device has the following states which are indicated by the light on the Pano Button.

Table 3.2 Pano Button Light Indicators: Normal State

Operation		Temporary Color	What's this mean?
1.	Powered on	Blinking red	When the Pano device is powered on, it shows a blinking Red light.
2.	Connected to Network cable	Blinking orange	When a network cable is plugged into the Pano device, the color of the Pano Button changes to blinking orange.
3.	Connected to the Network	Solid orange	When the Pano device gets an IP address, the color on the Pano Button changes to solid orange
4.	Connected to the Pano Manager or a DVM	Solid blue	When the Pano device communicates with the Pano Manager or to a DVM, the color on the Pano device changes to solid blue.

Power On Pano Manager

To power on the Pano Manager:

1. From the Hosts and Clusters view in VirtualCenter, right-click on the Pano Manager VM.
2. Select **Power On**.

There is no default name for the Pano Manager VM. You specified a name for the Pano Manager VM during your initial deployment, when you added the Pano Manager VM to the inventory.

Power Off Pano Manager

To power off the Pano Manager:

1. From the Hosts and Clusters view in VirtualCenter, right-click on the Pano Manager VM.
2. Select **Power Off**.

Log On To Pano Manager

To administer your Pano VDS deployment, use the Management User Interface (MUI).

To launch the Management User Interface (MUI):

Refrain from logging on to the Management User Interface (MUI) with the `root` account; rather, you should use the `admin` account.

1. Go to `http://`***`hostname`***`/admin.jsp` or `http://`***`ipaddress`***`/admin.jsp`, where `hostname` or `ipaddress` is the hostname or IP address of the Pano Manager virtual machine.
2. Log on using one of the following accounts:
   - **Administrator** (Recommended). The default user name for the Pano administrator account is `admin` and the default password is `zerotouch`.
   - **Superuser**. The default user name for the Pano superuser account is `root` and the default password is `password`.

Log Off from Pano Manager

To administer your Pano VDS deployment, use the Management User Interface (MUI).

To log off the Management User Interface (MUI):

From the Pano Manager, click **logout**. Yep, it's that simple!

Log On To DVMs as End User

If want to log on as an Administrator in order to troubleshoot a DVM, go to "Log On To DVMs as Administrator" on page 18. If you are experiencing session timeout issues, go to "Control Session Timeouts" on page 78.

To log on to a DVM through a VPN connection:

If you need to VPN into a DVM from a remote location, use the Pano web access. This client connects to the DVM using RDP.

1. Go to `http://`***`hostname`*** where `hostname` is the hostname of the Pano Manager virtual machine.
2. From the Pano client login screen, type your user name and password, then click **Login.**

To log on to a DVM from a Pano device:

1. Ensure that the Pano Button on your Pano device is solid blue. The Pano client login screen appears on the screen.
2. From the Pano client login screen, type your user name and password, then click **Login.**

Log On To DVMs as Administrator

You can log on to a user's DVM from VMware VirtualCenter. However, if you don't have access to your company's virtual infrastructure, there is an alternative–RDP.

Pano devices use Remote Desktop Protocol (RDP) to connect to the Pano Manager. If you cannot connect to the DVM directly using RDP, then you must fix the RDP problem before you can log on to the DVM. Go to "Troubleshoot RDP Connection Problems" on page 159.

You cannot log on to the DVM from the user's Pano device because you will not necessarily be connected to the same DVM.

To log on to a DVM using RDP:

The user will be disconnected from the DVM as soon as you log on to the DVM as Administrator. While you are logged on, the user receives the `The user Domain\Administrator is currently logged on to this computer. Only the current user or administrator can log on to this computer` message. When you're done, log off the DVM; the user can then log on via the Pano device.

1. Retrieve the DVM's IP address.
2. Retrieve the username associated with the DVM.
3. Open an RDP session into the user's desktop, as Administrator. You're in!

Log Off from DVMs

To log off a DVM from a Pano device:

In general, for a DVM that is assigned to a user (DVM from a Permanently Assigned Desktops collection type) there is no need for a user to log off or power off. The user can simply set the screen saver or press the Pano Button to disconnect from the DVM.

However, if a user logs on to a DVM from a Pooled Desktops collection type, that user must log off; otherwise, the DVM stays assigned to that user and the DVM does not return to the pool. To mitigate this issue, one can implement session timeouts by using an Active Directory group policy.

Hard-Reset DVMs

A shutdown (go to "Shut Down DVMs" on page 19) gracefully closes all running programs and powers the machine off. A hard-reset simply powers off and on, the DVM. A hard-reset might have some undesired effects on some running programs. Perform a hard-reset only if the DVM is unresponsive. To identify the DVM's state, go to "Monitor DVM Status" on page 120.

This task can also be performed using VirtualCenter, but it's much easier to reset the DVM from the Pano device.

To hard-reset a DVM:

1. From the Pano device, type in username and password and click **Options…**.
2. In the pop-up window, click the **Reset** button.

Shut Down DVMs

A shutdown involves a software power-off process. This process is equivalent to shutting down the desktop and bringing it up. This power-off does not bring the Pano Manager VM back on, so you must power on the Pano Manager VM afterward.

This task can also be performed using VirtualCenter, but it's much easier to shut down the DVM from the Pano device.

To shut down a DVM:

1. From the Pano device, type in username and password and click **Options…**.
2. In the pop-up window, click the **Power Off** button.

Retrieve IP Address and Username of DVMs

Only a Permanently Assigned Desktops collection type assigns a DVM to a user.

To retrieve the IP address of a DVM for a Permanently Assigned Desktops collection type:

1. Log on to the Pano Manager.
2. Click the **DVMs** tab.
3. Locate the user id and IP address associated with the DVM.

Log On To Pano Manager VM

The Pano Manager includes a Pano Manager console that allows you to perform the limited set of configuration options for the Pano Manager VM. With this Pano Manager console you can:

- Change Superuser Password
- Change Web Admin Account Password
- Configure Pano Manager VM Network Settings

To log on to Pano Manager VM:

Pano Logic recommends that you always log on as `root`. The default password for the `root` account is `password`.

1. Power on the Pano Manager, if it isn't already.
2. From VirtualCenter, right-click on the Pano Manager VM, then click **Open Console**. You are prompted to log on.
3. Log on using the `root` account. The default password is `password`. Once you are logged in, the Pano Manager console displays.

Log Off from Pano Manager VM

To log off Pano Manager VM:

Do one of the following:

1. From Pano Manager console, select option **5**.
2. From the bash shell, type **`exit`**.

Change Superuser Password

You can change the password for the superuser (`root`) account. The default password for the `root` account is `password`.

To change Pano Manager's superuser password:

1. Power on the Pano Manager.
2. Log on to Pano Manager VM.
3. From the Main Menu, select option **2 - Set Superuser Password**.
4. Follow the on-screen instructions to change the password.

Change Web Admin Account Password

You can change the password for the `admin` account, which is the default account to use when logging on to the Management User Interface (MUI). The default password for the `admin` account is `zerotouch`.

To change web admin password:

1. Power on the Pano Manager.

2. Log on to Pano Manager VM.
3. From the Main Menu, select option **3 - Set Web Admin Password**.
4. Follow the on-screen instructions to change the password.

View Pano Device Information

You might need to get information about a user's Pano device if:

- A particular USB device does not appear to work with the Pano device.
- The Windows desktop experience is not working as expected.

Specific information includes:

- Device Revision
- MAC address

Note: The MAC address of the Pano device can also be obtained from Pano Manager.

- Screen Resolution
- Network Connection Information

To obtain information about a user's Pano device:

1. From the Pano device that you want to troubleshoot, go to the Pano Login. You don't need to log on.
2. In the Pano Login, click **Help**.

View Users' DVM Login Status and DVM Assignment

To view users' information:

1. Log on to the Pano Manager.
2. Click the DVMs tab. The window displays information about which user is logged into a DVM or has been assigned a DVM.
   - For Permanently Assigned Desktops collection type, the Assigned User field will be populated by the user id.
   - For Pooled Desktops collection types, this field will not be populated. Only the Logged in User field will be populated. For more information, go to "Assign Users To DVMs in User Based Collections" on page 113.

Enable Secure Connections

To enable secure connections to any host, you must enable `ssh`. Occasionally you need to connect to the Pano Manager VM using a secure connection. To do so, you must enable `ssh` on the host.

Once you enable `ssh`, you can use non-command line utilities to make secure connections as outlined in "Initiate Secure Connections" on page 24. The `vi` editor isn't the most intuitive editor, but you must use it to enable `ssh`. Once you enable `ssh`, you can use Notepad from that point forward.

To enable ssh for an ESX host:

1. Log on to the ESX host using the superuser (root) credentials:
2. Execute the following commands from a shell:

```
# vi /etc/ssh/sshd_config
```

3. Find `PermitRootLogin` and change to `Yes`: press **ESC**, then press **Insert**.
4. Save the changes: press **ESC** then type **:wq!**. If you make a mistake, you can press the **ESC** key and then type it **:q!** to quit vi without saving the file.
5. Restart the `ssh` daemon:

```
# service sshd restart
```

To enable ssh for an ESXi host:

1. Log on to the ESX host using the superuser (root) credentials:
   a. At the console of the ESXi host, press ALT-F1 to access the console window.
   b. In the console, type **unsupported**, then press Enter. If you typed in the command correctly, you the Tech Support Mode warning and a password prompt appear.
   c. Type the password for the root login. You should then see the prompt of ~ #.
   d. Edit the `inetd.conf` file:

```
# vi /etc/inetd.conf
```

   e. Find the line that begins with #ssh and remove the #. Then save the file. If you're new to using vi, then move the cursor down to #ssh line and then press the Insert key. Move the cursor over one space and then hit backspace to delete the #.
2. Save the changes: press **ESC** then type **:wq!**. If you make a mistake, you can press the **ESC** key and then type it **:q!** to quit vi without saving the file.
3. Do one of the following:
   - (If you edited `sshd_config`) Restart the `ssh` daemon:

```
# service sshd restart
```

   - (If you edited `inetd_config`) Run the following command to determine the process ID for the inetd process:

```
# ps | grep inetd
```

The output of the inetd command will be something like 1299 1299 busybox inetd, and the process ID is 1299. Then, run **kill -HUP** *process_id* (kill -HUP 1299 in this example), and type **inetd** to start it again.

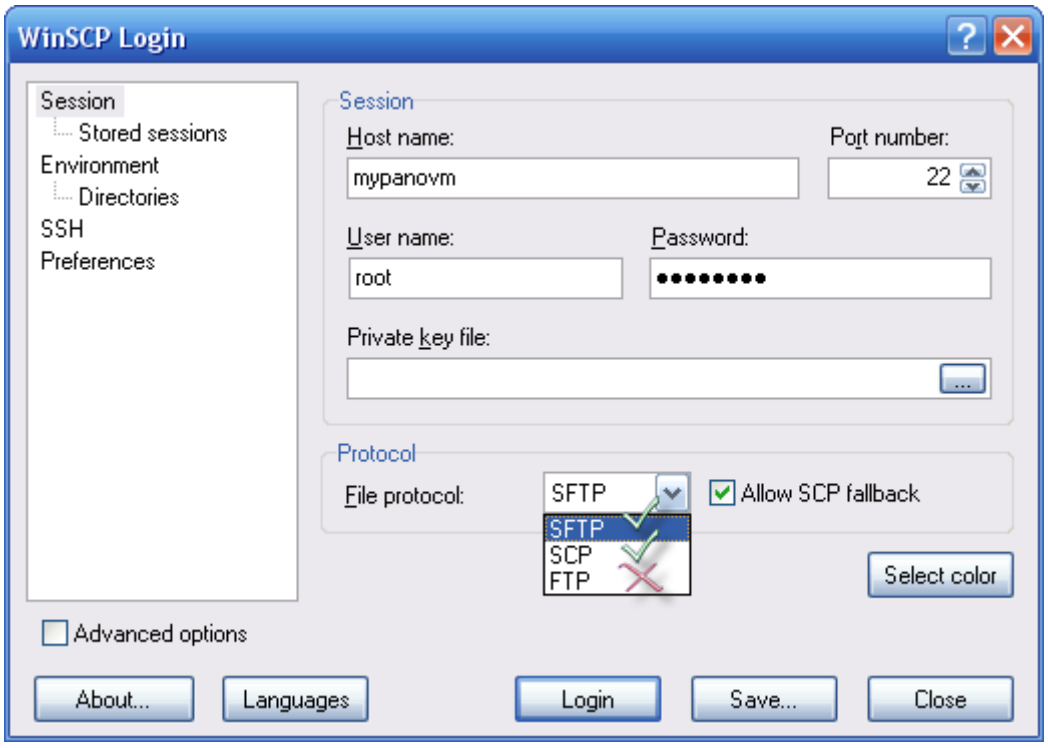
You should now be able to access the host via SSH.

Initiate Secure Connections

Occasionally you need to connect to the Pano Manager VM using a secure connection (for example, `scp` or `sftp`). There are many tools such as WinSCP or putty that enable you to connect without having to use a command line. For security reasons, the Pano Manager VM only allows secure connections.

To initiate a secure connection:

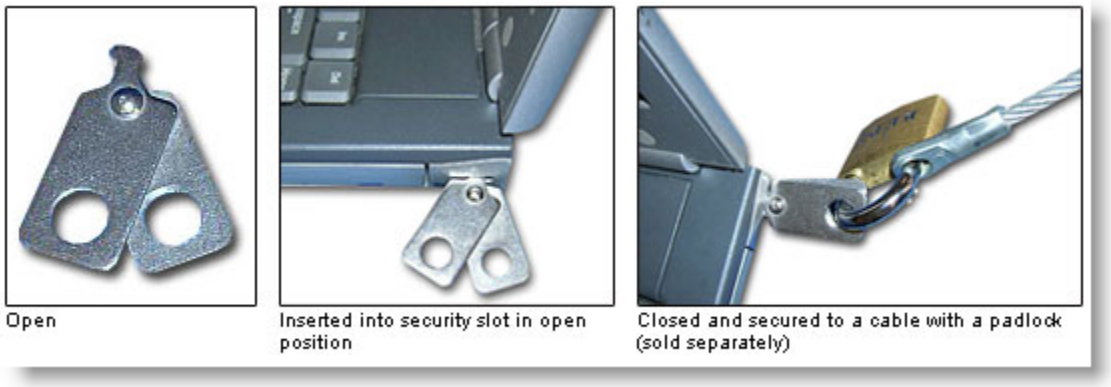
1. Enable ssh.
2. Create your session. Specify the host name and the superuser (root) credentials to which you want to connect (for example, using the Pano Manager VM). You don't need to specify a Private key.
3. Choose a secure file transfer protocol. A secure connection is any connection that uses ssh. FTP isn't a secure protocol, but `sftp` is. If the protocol begins with an "s", then it's probably secure. If you aren't using a secure protocol, the Pano Manager VM will not let you connect.



4. Click **Login**. From here you can copy files from your desktop to the host and from the host to your desktop. If you need to edit any files, simply use the editor of your choice (for example, Notepad).

Secure Pano Devices

All Pano devices have a slot that you can use to secure (lock down) your Pano devices. Consider using the Micro Clip:



Verify VirtualCenter Licenses

An expired license can result in outdated, partial, or missing DVM information in the Pano Manager. Your license(s) might reside on a license server or on the ESX host itself.

To verify VirtualCenter license:

1. Using the VMWare Infrastructure Client, log on to VirtualCenter.
2. Go to **Configuration** tab > **Licensed Features** link > **License Sources** link > **Edit**.

4
Support and System Requirements

Pano Virtual Desktop Solution has specific hardware and software requirements:

Hardware and Resource Requirements

The resources (CPU, memory, disk, network, etc) required to support your environment depend on your:

- Deployment
- Workload requirements
- Network topology
- Number of virtual desktops that you intend to run in your environment

In addition to provisioning for virtual desktops, you need to consider the resource requirements for VMware VirtualCenter and the Pano Manager virtual machine.

Work with your Pano Logic representative or partner to properly size your environment. Meanwhile, let's look at some guidelines and estimates to help you determine your resource requirements:

• Server hardware for VMware VI3

The Pano Virtual Desktop Solution (Pano VDS) requires server hardware to run the virtual infrastructure.

For a deployment based on VMware Virtual Infrastructure 3 (VI3), the server hardware needs to be capable of running VMware ESX Server 3.x. You can find compatible hardware, go to VMware's compatibility guides.

• DVM CPU, Memory, and Disk Space

To estimate your basic requirements, allocate an appropriate amount of CPU and memory to each virtual desktop.

Multiply that amount by the number of desktops that you expect to run. Consider giving every user 512Mb RAM, 1/4 core processor and 1/4 spindle hard disk. For example, if you have 25 users, a Dell 2950 with 2 quad core processors, 32GB RAM and 6 hard drives should more than suffice.

For disk, allocate an appropriate amount of space for each DVM. Also keep in mind disk I/O rates and do not place too many virtual desktops on a single physical drive.

• Network Bandwidth

Ensure that you have sufficient network bandwidth between your server and workgroup switches. You should have 1 Gbps links between your server and workgroup switches. From workgroup switches to Pano devices, 100Mbps links are sufficient.

• VMware VirtualCenter

VirtualCenter is a critical component of the Pano VDS. The minimum recommended configuration for running VirtualCenter with the Pano VDS is as follows:

- At a minimum, a Pentium IV 2.0 Ghz processor.
- At a minimum 2 GB RAM.

Consult the VMware VI3 documentation for complete VirtualCenter requirements. If you choose to run your VirtualCenter as a virtual machine, make sure that you factor VirtualCenter's resource requirements into that host's overall capabilities.

• Pano Manager Virtual Machine

The Pano Manager runs as a virtual machine. You can safely run the Pano Manager on the same host as DVMs; however, you must *reserve* sufficient resources for the Pano Manager VM. Pano Logic recommends that you allocate the following resources for a Pano Manager VM based on the number of Pano devices in your environment:

Deployment	Reserved CPU	Available CPU	# of CPUs	Reserved Memory (mBytes)
0 - 25	512 Mhz	2.0 Ghz	1	1024
25 - 100	1.0 Ghz	4.0 Ghz	2	2048
100 - 250	1.5 Ghz	6.0 Ghz	4	4096

Table 4.1 Pano Manager VM Resource Requirements

- To reserve these resources in VirtualCenter, go to "Reserve Resources for the Pano Manager VM" on page 39.
- To learn about the maximum number of Pano devices that you can deploy, go to "Supported Number of Pano Devices" on page 29.

Supported Number of DVMs

Depending on the collection type, your environment can have either up to 250 DVMs or 250+ DVMs:

- **VMware VDM collection type** - over 250 DVM.
- **All other collection types** - up to 250 DVMs.

If you want to deploy more than 250 DVMs, you must use the VMware VDM collection type.

Irrespective of the collection type that you use, there is a limit to the number of Pano devices (go to "Supported Number of Pano Devices" on page 29) that you can deploy.

Collection	Up to 250 DVMs	Over 250 DVMS
Pooled Desktops	✓	✗
Permanently Assigned Desktops	✓	✗
Existing Desktops	✓	✗
Automatic Login	✓	✗
Different Accounts w/ Automatic Login	✓	✗
Windows Login	✓	✗
VMware VDM	✓	✓

Table 4.2 DVM Support by Collection Type

Supported Number of Pano Devices

A Pano Manager can support up to 250 Pano devices. For larger deployments, you can use Pano VDS scalability feature as outlined in "Configure for Scalability" on page 43. This feature enables you to configure a group of Pano Managers (up to eight) to serve as many as 2000 Pano devices (8 x 250) within a single deployment.

Supported Virtualization Infrastructure

Pano Virtual Desktop Solution requires the following third party software:

• VMware VI3 environment

For a deployment based on VMware VI3, the following environment must be installed and operational.

Product	Release	Supported?
ESX Server	3.5 Update 3	✓
	3.5 Update 2	✓
	3.5 Update 1	✓
	3.5	✓
	3.0.3	✓
VirtualCenter	2.5 Update 3	✓
	2.5 Update 2	✓
	2.5 Update 1	✓
	2.5	✓
	2.02 Update 5	✓

Table 4.3 Supported VMware Infrastructure

• Microsoft Sysprep tools installed on your VirtualCenter server

The Pano Manager automatically provisions DVMs. To utilize these features, you need Microsoft Sysprep tools. Go to “Install Sysprep Tools on VirtualCenter Server” on page 81.

Supported Operating Systems for Pano Desktop Service

You must have valid licenses for Microsoft desktop operating systems. You can install the Pano Desktop Service (Pano DAS) on any of the following operating systems:

- Windows XP Professional, SP2 (32-bit) or SP3 (32-bit) - Pano DAS v2.5.1

  Recommended Updates:

  KB 952132

  KB 959252

- Windows Vista Business Edition (32-bit) - Pano DAS v2.0.4
- Windows Vista Ultimate Edition (32-bit) - Pano DAS v2.0.

The Pano Desktop Service (Pano DAS) v2.5.1 installs a GINA dynamic-link library (DLL). The Pano DAS GINA will overwrite any third-party GINA such as the Novell Netware GINA or Imprivata. If you are running such a GINA, install Pano DAS v2.0.4, or contact Pano Logic Technical Support.

Supported Directory Services

The Pano Virtual Desktop Solution (Pano DAS) supports the following directory services:

- Microsoft Active Directory 2003 or higher
- Novell eDirectory
- OpenLDAP

The Pano Desktop Service (Pano DAS) v2.5.1 installs a GINA dynamic-link library (DLL). The Pano DAS GINA will overwrite any third-party GINA such as the Novell Netware GINA or Imprivata. If you are running such a GINA, install Pano DAS v2.0.4, or contact Pano Logic Technical Support.

Supported Third Party Connection Brokers

Although Pano Manager acts as a full-featured connection broker, Pano VDS supports the following third-party connection brokers. For information, go to Install Pano Device USB Support.

- VMware View 3.0
- VMWare VDM 2.1

Compatibility of Pano Components

The Pano Manager needs to be the same version or later than the Pano Desktop Services (Pano DAS) it manages. The Pano Manager v2.5.1 supports Pano DAS v2.5.1.

The Pano software services v2.5.1 (the Pano Manager and the Pano DAS) are compatible with all released versions of the Pano device.

Supported USB Devices

In addition to support for USB keyboards and mice, this version of Pano Virtual Desktop Solution also includes support for the following USB device types, including composite devices (often called, *all-in-one* solutions). For a list of supported devices by model number, browse the Pano Logic USB Support Matrix.

- USB flash drives
- USB mass storage devices
- USB CD readers/writers
- USB DVD readers/writers
- USB floppy drives
- USB printers
- USB scanners
- USB business card scanners
- USB to serial converters
- USB hubs
- USB RIM BlackBerry
- USB Apple iPod
- USB touch screen display
- USB smart boards

Within each category Pano Logic tests a range of devices to ensure broad support; however it is still suggested that you check with Pano Logic Technical Support at support@panologic.com ahead of time, if you plan to use any supported device. Pano Logic Technical Support can offer guidance on which specific devices have been validated and work best with the solution. The best practice regarding peripherals is for your IT organization to verify interoperability before your company deploys Pano devices with peripherals.

Isochronous USB devices, including web cams, USB speakers, USB handsets, and USB headsets, are not currently supported.

To enable support for all supported devices, go to Install Pano Device USB Support.

Limitations To USB Device Support

• Possible data corruption on USB device

While a USB storage device is inserted into a Pano device, improperly disconnecting the session can cause data corruption on the USB device. This is not a problem that is unique to Pano devices. This is problem is related to USB technology itself.

Keep in mind that there are multiple ways a session can be disconnected (go to “Control Session Timeouts” on page 78). The common ways to disconnect a session include:

- Select disconnect from the Windows Security dialog.
- Press the Pano Button.
- Log on to your original session from another Pano device (also known as session roaming).
- Log on to your original session from another client device, such as through an RDP client running on a laptop computer.

These actions are roughly equivalent to pulling a USB device out of a traditional desktop computer without first selecting **Safely Remove Hardware** from the Windows system tray. When you are not actively using a USB storage device, you should **Safely Remove Hardware** or **Eject** the device.

• Possible operating delay with USB mass storage device

When you insert a USB mass storage device, the amount of time required for the device to become fully operational and appear in the Windows Explorer is proportional to the size of the

storage device. USB thumb drives are generally operational within a few seconds, whereas a 500GB external hard drive might take a minute or longer to become operational.

When you remove a USB mass storage device from a Pano device, you should wait for the device's icon to disappear from the Windows Explorer before reinserting the device. Windows requires some time to fully remove the device.

5
(Start Here) Deploy Pano VDS

Note: Don't worry about installing your Pano devices just yet. We'll get to that part later in the deployment, when you configure the Pano Manager for Pano® Device discovery. If you've already attached your Pano device to the network, it's normal for the Pano Button light color to be amber until they have been discovered by the Pano Manager.

Task			Go to...
If you're meticulous, like us, get acquainted:			
☐	**1.**	Learn a bit about the components with which you'll be working. It won't take long!	"Pano VDS Overview" on page 1
☐	**2.**	Learn some key Pano concepts. You probably already know some of these concepts as a result of your experience with virtualization, but let's review them anyway.	"Pano VDS Concepts" on page 5
If you're impatient, sorry, but there's just no "getting around" this stuff:			
☐	**3.**	Review system requirements and supported configurations.	"Support and System Requirements" on page 27
☐	**4.**	Set up virtual infrastructure. For example, VMware ESX Server 3.x and VMware VirtualCenter. As outlined in "Increase VMware ESX Server Service Console Memory" on page 145 provide the Service Console 800 MB of memory.	VMware Infrastructure documentation
☐	**5.**	Install and configure the Pano Manager VM.	"(Overview) Install and Configure Pano Manager VM" on page 37
☐	**6.**	Configure the Pano Manager for: • Directory Services • Virtualization • Pano Device discovery	"(Overview) Integrate Pano Manager into Your Environment" on page 49
Automated provisioning–a feature you won't want to do without:			
☐	**7.**	Prepare to provision desktop virtual machines. You need to create the virtual machine, template, customization specification, and a few other prerequisites, some of which are optional.	"(Overview) Prepare Desktop Virtual Machines" on page 61
Now for the good stuff:			
☐	**8.**	Create the DVM collections.	"(Overview) Create DVM Collections" on page 105
☐	**9.**	Set user preferences.	"(Overview) Set User Preferences" on page 85
Now here is where you start seeing the fruits of your labor:			

Task		Go to...
☐	**10.** Verify your Pano VDS deployment.	"Verify Pano VDS Deployment" on page 59
☐	**11.** (Optional) Connect the Pano Manager to VMware View Manager.	"(Overview) Integrate Pano VDS with VMware View" on page 134

6
Install and Configure Pano Manager VM

(Overview) Install and Configure Pano Manager VM

Before You Begin: Browse the entire deployment workflow at "(Start Here) Deploy Pano VDS" on page 35.

To install and configure Pano Manager Virtual Machine (Pano Manager VM), perform the following sequence of tasks:

Task		Go to...
1.	Install the Pano Manager VM on VMware VI3	"Install Pano Manager VM on VMware Virtual Infrastructure" on page 38
2.	For security purposes, change superuser (root) password and web admin password. They currently are set to the default.	"Change Superuser Password" on page 20 "Change Web Admin Account Password" on page 20
3.	If necessary, change the Pano Manager VM's port group. By default, the Pano Manager VM belongs to the `VM Network` port group.	"Change Pano Manager VM's Port Group" on page 39
4.	Allocate resources to the Pano Manager.	"Hardware and Resource Requirements" on page 27 "Reserve Resources for the Pano Manager VM" on page 39
5.	Configure the Pano Manager VM's network settings.	"Configure Pano Manager VM Network Settings" on page 41
6.	(Recommended) For more security, add a certificate from a Certified Authority.	"(Overview) Replace Pano Manager's Self-Signed Certificate" on page 171

Next Step(s): If you're performing this workflow as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

Install Pano Manager VM on VMware Virtual Infrastructure

The Pano Manager is delivered as a virtual appliance. This means that the Pano Manager runs within a virtual machine hosted on your virtual infrastructure. The Pano Manager VM can run on any ESX host:

To install Pano Manager VM on VMware VI3:

Before You Begin:

If you have not already installed your VMware Infrastructure, follow the installation instructions provided by VMware. Once you have performed a basic installation of VMware ESX Server 3.x and VMware VirtualCenter, you can install the Pano Manager.

In the following procedure, the `PanoManagerVM-`***`version`***`.tar.gz` file is the Pano Manager VM itself. The Pano Manager VM has the Pano Manager pre-installed.

1. Retrieve the `PanoManagerVM*` file from either the Pano Logic DVD, or Pano Logic's FTP site.
2. Copy the `PanoManagerVM*` file to the ESX host:
   a. From a Windows computer, copy the `PanoManagerVM-`***`version`***`.tar.gz` file from the Pano media disk to your desktop, or download the package to a local file system (a file share).

      Do not extract the file on your desktop or local file system. Extract the file on the Pano Manager VM only.
   b. Use the VMware console or initiate a secure connection to connect to the ESX host on which you intend to load the Pano Manager.
   c. Create a working directory on the Pano Manager VM and into which the compressed file can be copied. For example:

```
# mkdir /vmfs/volumes/storage1/PanoMS-tz/
```

   a. Copy the `PanoManagerVM-`***`version`***`.tar.gz` file from your desktop or local file system to the working directory that you just created.

```
# scp PanoManagerVM-version.tar.gz root@esxhost:/vmfs/volumes/
storage1/PanoMS-gz/
```

3. On the Pano Manager VM, extract the `PanoManagerVM*` file in the `/vmfs/volumes/storage1/PanoMS-tz/` directory.

   Do not extract the file on your desktop or local file system. Extract the file on the Pano Manager VM only.

   For example:

```
# tar -xzvf PanoManagerVM-version.tar.gz
```

   The extraction process typically takes 5-10 minutes and the resulting files total about 15GB.
4. Add the Pano Manager to the inventory:
   a. Use the VMware Infrastructure Client to connect to the ESX host.
   b. In the left browse pane, click on the ESX host.
   c. Click the **Configuration** tab and in the left pane, select **Storage** to navigate to the datastore that contains the copied files (in this example `Storage1` is the datastore).
   d. Right-click on the datastore, then select **Browse**.

e. Browse to the directory that contains the Pano Manager VM file: `/vmfs/volumes/storage1/PanoMS-tz`.

f. Right-click on the `PanoManagerVM.vmx` and select **Add to inventory**. Follow the on-screen prompts.

5. Power on the Pano Manager.

Next Step(s): Do the following

1. Change Superuser Password.
2. Change Web Admin Account Password.
3. Change Pano Manager VM's Port Group.

Change Pano Manager VM's Port Group

When you install your ESX host, a default port group is created, and this port group is `VM Network`. By default, the Pano Manager VM is configured to use the `VM Network` port group. If this port group has been changed or removed, the Pano Manager VM cannot connect to the network. You must edit the Pano Manager VM's settings to configure the network adapter to use your existing port group.

To configure the network adapter to use your existing port group:

1. Log on to VirtualCenter using the VMware Infrastructure Client.
2. Right-click on the Pano Manager VM, then choose **Edit Settings**.
3. Click the **Hardware** tab, then select the network adapter.
4. In the **Network Connection** area, select your existing port group from the Network label drop-down list, then click **OK**.

Next Step(s): "Reserve Resources for the Pano Manager VM" on page 39. Use VMware resource pools and reservations to allocate the Pano Manager VM sufficient resources based on the Pano Manager's resource requirements.

Reserve Resources for the Pano Manager VM

The Pano Manager VM must have sufficient CPU and memory resources available to run effectively. Pano Logic recommends that you set reservations for both CPU and memory to ensure that the Pano Manager VM always has a minimum amount of resources available. For more information, go to "Pano Manager VM Resource Requirements" on page 28.

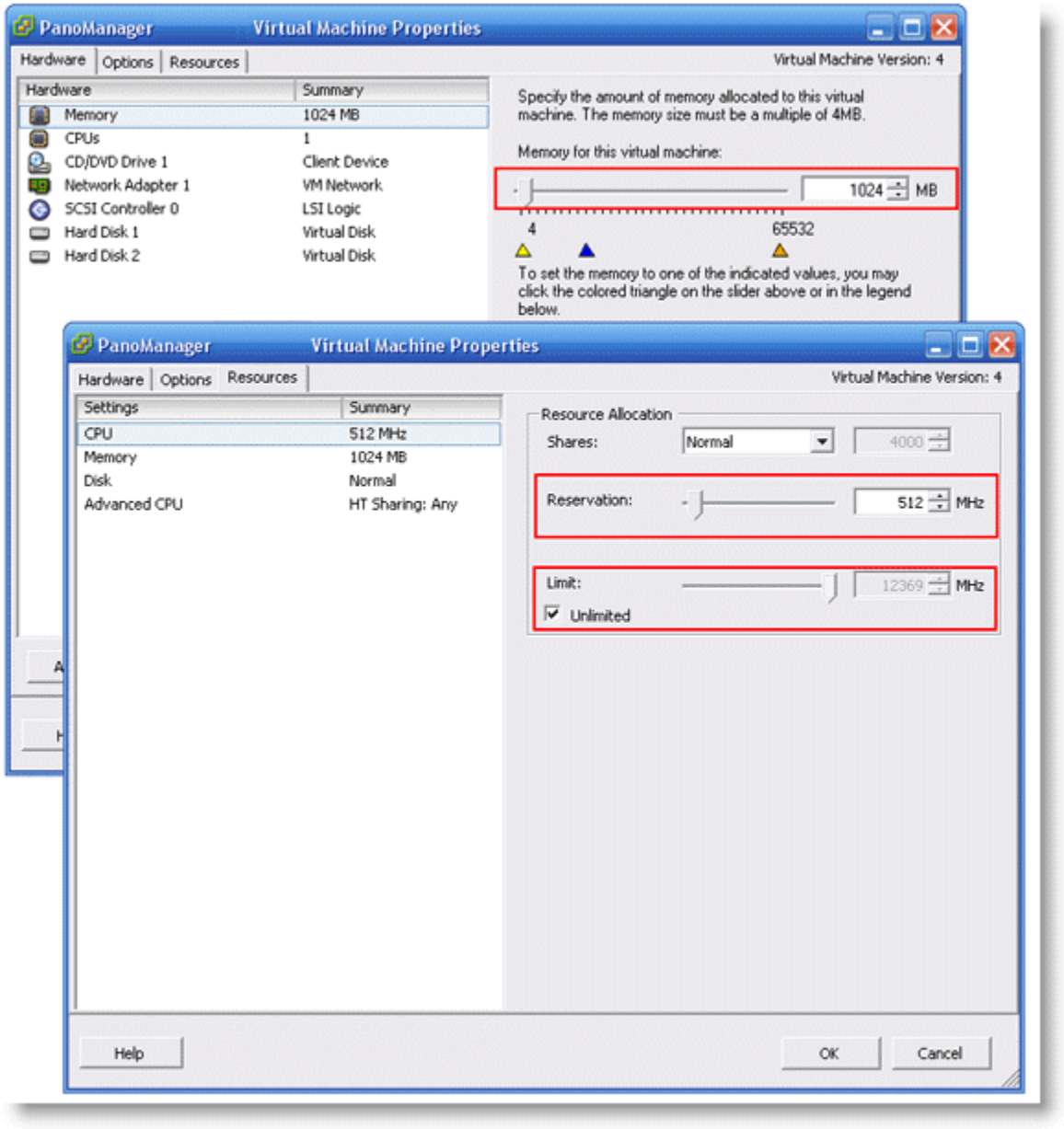
To reserve resources for Pano Manager VM:

1. Determine the CPU and memory resources that your Pano Manager VM requires based on your deployment size. Go to "Pano Manager VM Resource Requirements" on page 28.
2. Reserve CPU and memory resources:
   a. Log on to VirtualCenter using the VMware Infrastructure Client.
   b. Power off the Pano Manager if it isn't already.
   c. Go to **Getting Started** tab > **Basic Tasks** area > **Edit virtual machine settings** link.

Caution: Do not set a maximum limit for CPU or memory. This setting allows the Pano Manager to use additional available resources as needed. The amount of resources consumed by the Pano Manager VM usually varies throughout the day based on your usage patterns. The Pano Manager VM consumes the most resources when Pano devices display the Pano client login

screen. Once users have connected to their DVMs, the Pano Manager incurs practically no load for that device or DVM.

d. In the **Hardware** tab and the **Resources** tab, specify the resource requirements for your deployment, then click **OK**.



e. Power on the Pano Manager VM.

3. Change the number of CPUs for the Pano Manager VM, if necessary:

a. Log on to the Pano Manager console.

b. Select option **4 Drop to bash shell (Power Users)**.

c. Edit the `/etc/grub.conf` file:

- From:

```
  kernel /vmlinuz-2.6.18-53.1.4.el5 ro root=/dev/VolGroup00/
LogVol00 rhgb quietclock=pit nosmp noapic nolapic
```

- To:

```
  kernel /vmlinuz-2.6.18-53.1.4.el5 ro root=/dev/VolGroup00/
LogVol00 rhgb quietclock=pit smp
```

d. Shut down the Pano Manager VM:

```
  # shutdown -h now
```

e. From VirtualCenter, right-click on the Pano Manager VM and select **Edit Settings**.

f. Click the **Hardware** tab, select CPUs, and change number of CPUs for the Pano Manager VM.

g. Power on the Pano Manager VM.

h. Log on to the Pano Manager console.

i. Select option **4 Drop to bash shell (Power Users)**.

j. Type the following command. The number of processor(s) that you added should match the system's `cpuinfo` output:

```
  # cat /proc/cpuinfo | grep processor
```

Next Step(s): "Configure Pano Manager VM Network Settings" on page 41

Configure Pano Manager VM Network Settings

You can configure the Pano Manager VM (Pano Manager VM) to get its network settings from a DHCP Server or you can assign the Pano Manager VM a static IP Address. Setting a static IP address is generally preferred, and is required if you use DHCP-assisted discovery for Pano device as outlined in "(DHCP Method) Set Up Pano Device Discovery" on page 55.

To configure the Pano Manager VM's network settings:

1. Power on the Pano Manager, if not already.
2. Log on to Pano Manager VM.
3. Select option **1**. The **Use DHCP (y/n)?** prompt appears.
4. Specify the network settings for the Pano Manager VM. Set to DHCP or provide static IP.

Next Step(s): Do the following:

1. If you want to upload a self-signed certificate, go to "(Overview) Replace Pano Manager's Self-Signed Certificate" on page 171
2. If you're performing this task as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

7 Configure for Scalability

About Pano VDS Scalability

Note: Pano Logic is working closely with early adopters who need to implement large, scale-out implementations of Pano VDS. If you are deploying hundreds of Pano devices and desktop virtual machines, please contact Pano Logic Technical Support. Pano Logic will work with you to determine your specific requirements and how best to deploy your Pano VDS.

As outlined in "Supported Number of DVMs" on page 29, to deploy more than 250 DVMs you must use a VDM collection type.

The Pano Virtual Desktop Solution can support as many as 2000 Pano devices, using Pano Virtual Desktop Solution scalability feature. This feature enables you to configure a group of Pano Managers (up to eight) to serve as many as 2000 Pano devices (8 x 250) within a single deployment.

Each Pano Manager can provide connection management for up to 250 Pano client login screen. Using a master-slave model, simply create a Pano Manager group, then designate one Pano Manager as the master and the other Pano Managers as slaves. For example, if you want to deploy 400 Pano devices, you need two Pano Managers: the master handles 250 Pano devices, and one slave handles 150.

The master contains all the collections and is used for web logins. Slaves can only be configured to manage Pano client login screen; you cannot configure slaves to perform any other functions. A master Pano Manager coordinates the desktop connections and utilizes resources (distributes load) on the other slave Pano Managers as needed.

Create Pano Manager Group

Note: Pano Logic is working closely with early adopters who need to implement large, scale-out implementations of Pano VDS. If you are deploying hundreds of Pano devices and desktop virtual machines, please contact Pano Logic Technical Support. Pano Logic will work with you to determine your specific requirements and how best to deploy your Pano VDS.

Each Pano Manager that you configure as part of the Pano Manager Group must have sufficient CPU and memory resources available to run effectively.

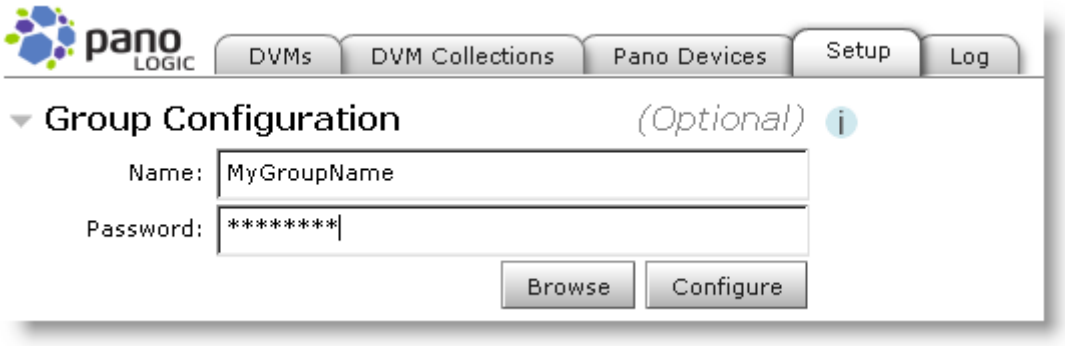
Pano Logic recommends that you set reservations for both CPU and memory to ensure that the Pano Manager VM always has a minimum amount of resources available. For more information, go to "Pano Manager VM Resource Requirements" on page 28.

To create a Pano Manager Group:

Perform this procedure on each Pano Manager. All Pano Managers that are configured with the same group name will form a group together.

1. Log on to the Pano Manager.

2. Click on the **Setup** tab.
3. In the Group Configuration area, type a name and password for the group, then click **Configure**.



4. Click the **Browse** button, then confirm that the newly added Pano Managers appear with the correct status.

That's it! Your Pano Managers are now load balancing.

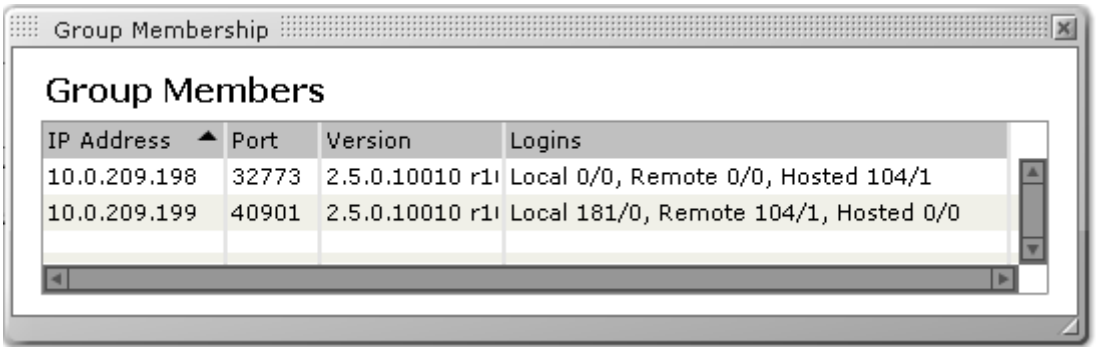
Monitor Pano Manager Group Members' Load

Both the master Pano Manager and slave Pano Managers are considered members. After you configure Pano Managers as part of a Pano Manager Group, the Pano Virtual Desktop Solution discovers the Pano Managers. Discovery requires less than one minute.

To monitor Pano Manager Group members' load:

1. Log on to one of the Pano Managers.
2. Click the **Setup** tab.
3. In the **Group Configuration** area, click the **Browse** button. The members appear in the list. Under the **Logins** column, the load that each is managing also appears:
   - **Local**. Client UI login processes running on the local machine.
   - **Remote**. Client UI login processes running on any remote machine on behalf this local machine.
   - **Hosted**. Client UI login processes running on the remote machines on behalf of some other machine.

   Where the first number is the total number of client UI processes and the second number is the number of those processes that are still starting up.



Identify Master Pano Manager

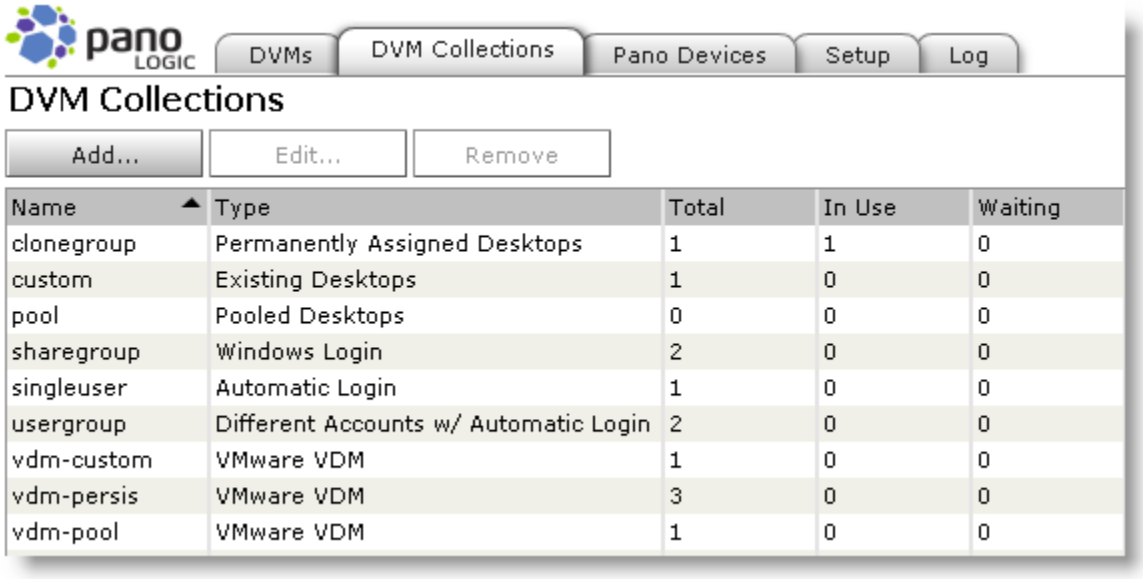
When you need to manage or configure DVMs, do so from the master Pano Manager. As mentioned in "About Pano VDS Scalability" on page 43, slaves can only manage Pano client login screens.

Perform this procedure on each of your Pano Managers until you discover which Pano Manager is the master Pano Manager.

To identify the master Pano Manager:

1. Log on to one of the Pano Managers.
2. Click the **DVM Collections** tab.
   - If your collections appear in the list, then this is the master Pano Manager.

- If your collections do not appear in the list, then this is a slave Pano Manager.



8

Integrate Pano Manager into Your Environment

(Overview) Integrate Pano Manager into Your Environment

Before You Begin: After you've installed and configured the Pano Manager VM as outlined in "(Overview) Install and Configure Pano Manager VM" on page 37, you're ready to integrate it into your existing environment.

To integrate the Pano Manager into your environment, you must connect it to your directory services and virtual infrastructure. Perform the following sequence of tasks.

1.	Prepare to set up the Pano Manager	"Prepare To Integrate Pano Manager" on page 50
2.	If you have a firewall between your data center and your users, open up the appropriate ports for both inbound and outbound traffic.	"Configure Data Center Firewall" on page 50
3.	Connect the Pano Manager to your directory service.	"Connect Pano Manager To Directory Services" on page 50
4.	Connect the Pano Manager to your virtual infrastructure manager.	"Connect Pano Manager To VirtualCenter" on page 51
5.	Select the method for discovering Pano devices on your network.	"Choose a Pano Device Discovery Method" on page 53
6.	Set up Pano Device discovery	"(Broadcast/Probe Method) Set Up Pano Device Discovery" on page 54 "(DHCP Method) Set Up Pano Device Discovery" on page 55

Next Step(s): If you're performing this workflow as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

Prepare To Integrate Pano Manager

To prepare to integrate Pano Manager:

1. Identify an account for the Pano Manager to use to query your directory service.

   Any user who is a member of Domain Users can do AD lookup. The account needs read permissions to the portions of the directory that contain the directory objects (users and groups) for the users of the Pano VDS.
2. Identify an account for the Pano Manager to use to integrate with the VirtualCenter that manages the virtual infrastructure underlying your Pano VDS.

   This account needs to have Administrator permissions in VirtualCenter.

Next Step(s): "Configure Data Center Firewall" on page 50

Configure Data Center Firewall

The Pano DAS communicates with the Pano Manager and Pano devices over certain network ports. If you have a firewall between your users Pano devices and your data center, you must open up these ports for both inbound and outbound traffic. DVMs initiate connections to Pano devices, not the other way around. If these ports are closed, Pano Manager cannot discovery your Pano devices.

Next Step(s): "Connect Pano Manager To Directory Services" on page 50

Connect Pano Manager To Directory Services

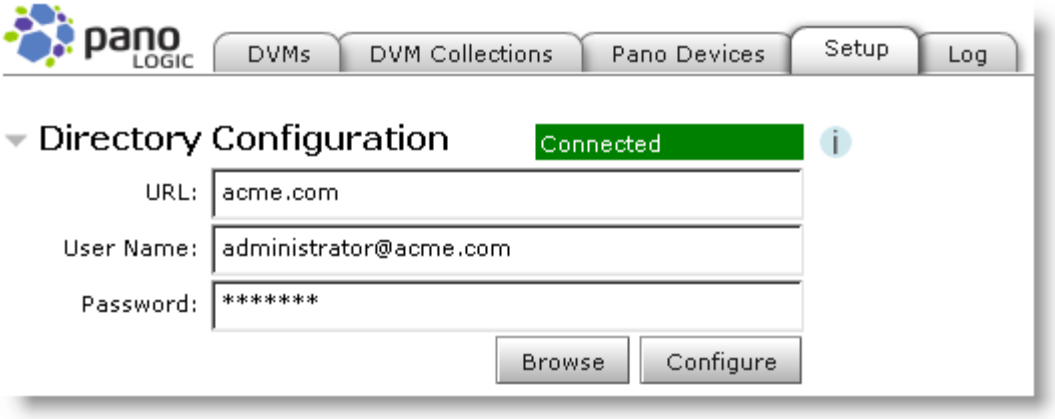
The Pano Manager relies on the directory service for user authentication. (For a list of supported directory services, go to "Supported Directory Services" on page 31.) You need to set up the Pano Manager to read your directory service. Using the standard DNS SRV records (RFC2782), the Pano Manager can automatically determine the best directory servers to contact.

If present, the Active Directory site information is used. Also, the Pano Manager uses the Global Catalog when available for most queries, and only uses other servers for information that is not in the Global Catalog.

To connect Pano Manager to directory services:

3. Log on to the Pano Manager.
4. Click on the Setup tab.
5. In the Directory Configuration area, click the disclosure triangle to open the section if necessary.
6. In the URL field, type your company's internet domain name. The Pano Manager automatically locates the best directory servers to contact.
7. Type the credentials to use when connecting the servers into the user name and password fields, then click **Configure**.
   - The account needs to have read access to all portions of the directory used to authenticate users of the DVMs.
   - When using Active Directory you must use the full User Principal Name (UPN). The UPN is an internet-style login name for the user.

8. When the status changes to `Connected`, click **Browse** to confirm that the account has the proper access privileges to access the directory information.



Troubleshooting: Do the following

- If this procedure didn't work for you, you might have a less common environment, go to (Less Common) Connect Pano Manager To Directory Services.
- If that doesn't work, go to "Troubleshoot Authentication and Directory Services Problems" on page 160.

Next Step(s): "Connect Pano Manager To VirtualCenter" on page 51

Connect Pano Manager To VirtualCenter

The Pano Manager must be able to communicate with VirtualCenter in order to use the Pano Manager's connection brokering and automated deployment features.

If you plan to use VMware View exclusively, then you do not need to perform this procedure (for more information, go to "(Overview) Integrate Pano VDS with VMware View" on page 134.

To enable communication between Pano Manager and VirtualCenter:

Before You Begin: "Prepare To Integrate Pano Manager" on page 50

1. Ensure that VirtualCenter web service is installed and running; otherwise, the Pano Manager can't communicate with VirtualCenter. Go to VMware's "Verifying VirtualCenter Web Service Installation" procedure.
2. Log on to the Pano Manager.
3. Click the **Setup** tab.
4. In the **Virtualization Configuration** area, type the URL for the VirtualCenter interface. The URL can be a FQDN of the computer, IP address, or Netbios name. As long as the URL can resolve to the IP address, it will work.

   For VirtualCenter 2.x:

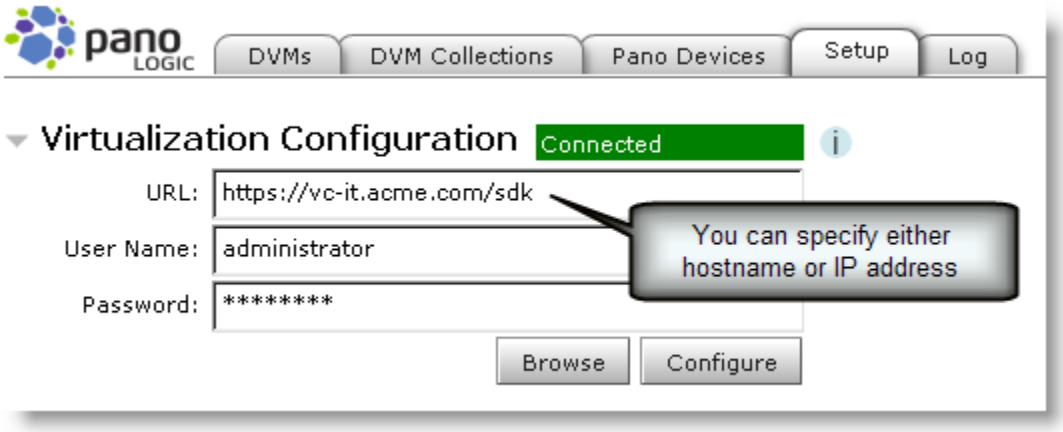
   ```
   http[s]://host/sdk
   ```

   Example:

   ```
   https://vcserver/sdk
   ```

5. Type the user name of the account in VMware VirtualCenter.

   The Pano Manager uses this account to communicate with VirtualCenter. It is recommended that this account be unique–and only used for integration between the Pano Manager and VirtualCenter. The username must be a valid user who has permissions on the Folder hierarchy in VirtualCenter as well as customization scripts and other objects.



6. Type the account's password, then click **Configure**.
7. When connected, In the **Virtualization Configuration** area, click **Browse**, then browse the virtualization hierarchy to confirm that the account has the proper access privileges.

Troubleshooting: "Troubleshoot Communication Problems with VirtualCenter" on page 162

Next Step(s): "Choose a Pano Device Discovery Method" on page 53

Choose a Pano Device Discovery Method

Pano devices need to be discovered before they can be controlled by the Pano Manager. Once discovered, Pano devices receive a name of `PanoDevice-`***`PanoDeviceMacAddress`***. For example, PanoDevice-00-1c-02-40-17-95. As discussed in "Set Up Collections with Device Restrictions" on page 117, you'll eventually decide on a naming convention for your Pano devices to make discovery easier.

There are two ways that the Pano Manager can discovery Pano devices:

- For a *small deployment* (or during a trial), one of the broadcast/probe methods is the easiest option to set up.
- For a *larger-scale production deployment*, DHCP-assisted discovery is the best solution since it is the most efficient on the network. This is the most common method for deploying in production.

Next Step(s): Do one of the following:

- "(Broadcast/Probe Method) Set Up Pano Device Discovery" on page 54
- "(DHCP Method) Set Up Pano Device Discovery" on page 55

(Broadcast/Probe Method) Set Up Pano Device Discovery

Pano devices need to be discovered so they can be controlled by the Pano Manager. If you don't know if the broadcast or probe-based methods are ideal for your deployment, go to "Choose a Pano Device Discovery Method" on page 53.

To set up Pano Device Discovery to use the broadcast/probe method:

1. Log on to the Pano Manager. "Power On Pano Manager" on page 15.
2. Click on the **Devices** tab.
3. In the **Discovery Configuration** area, specify *one* the following discovery parameters:

Note: Avoid specifying an overly broad range of addresses as that causes additional unnecessary broadcasts on your network.

- **Enable Local Broadcast** - Select the check box for this option if your Pano Manager and Pano devices are located on the same subnet.

  When you enable this option, the Pano Manager periodically broadcasts packets on the local subnet to discover new Pano devices.

- **Remote Broadcast Networks** - Use this option when your Pano devices are located on multiple subnets of your network.

  Enter a space-separated list of subnets. For example: 192.168.1.255 191.255.255.255. Subnet IP addresses must end with a value of 255.

- **Probe Address Ranges** - Use this option when you want to specify a range of IP addresses in which the Pano Manager can probe for Pano devices. \

  Use this option only when there is a small defined range of IP addresses for Pano devices as is usually the case during a trial (before you implement Pano VDS in production).

  Enter a dash-separated range of addresses. For example: 10.0.32.100-10.0.32.199. To specify more than one range of addresses to probe, separate the entries with a space. For example: 10.0.32.100-10.0.32.199 10.0.45.1-10.0.45.99. You can use any IP address in this option.

4. Set up the Pano devices, if you haven't already. Simply connect them to your network using the Pano devices' Ethernet port. To verify that the Pano devices are connected to the network, go to "Pano Button's Light Indicators" on page 15.
5. Locate the new Pano devices that the Pano Manager VM just discovered. From the Pano Manager, click on the Pano devices tab. The default name for Pano devices is `PanoDevice-`*`MACAddress`*.

Next Step(s): If you're in the process of deploying the Pano Manager VM, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

(DHCP Method) Set Up Pano Device Discovery

Pano devices need to be discovered so they can be controlled by the Pano Manager. If you don't know if the broadcast or probe-based methods are ideal for your deployment, go to "Choose a Pano Device Discovery Method" on page 53.

Rather than using one of the broadcast or probe discovery methods outlined in "(Broadcast/Probe Method) Set Up Pano Device Discovery" on page 54, you can configure a DHCP server to provide the address of the Pano Manager to the Pano device. This method relies on a DHCP feature called vendor-specific options. Vendor-specific options allow DHCP to return additional data to a DHCP client based on the clients vendor class.

- If you have an Linux DHCP server, go to "Add Pano Logic Vendor Class for Linux DHCP Server" on page 26.
- If you have a Netware DHCP server, go to "Add Pano Logic Vendor Class for Netware DHCP Server" on page 27.
- If you have a Cisco DHCP server, go to "Add Pano Logic Vendor Class for Cisco IOS DHCP Server" on page 27.

To set up Pano Device Discovery to use DHCP method:

You're about to configure your DHCP Server. The example outlined in this procedure is based on a Windows DHCP Server.

On the server, you'll define a vendor class called `Pano Logic`, and this class is identified by the ASCII string `Pano Logic`. For this vendor class you'll use vendor specific option, `Code 1`, Type IP address, Value: ***`PanoManagerServerIPAddress`*** where `PanoManagerServerIPAddress` is the static IP address of the Pano Manager VM.

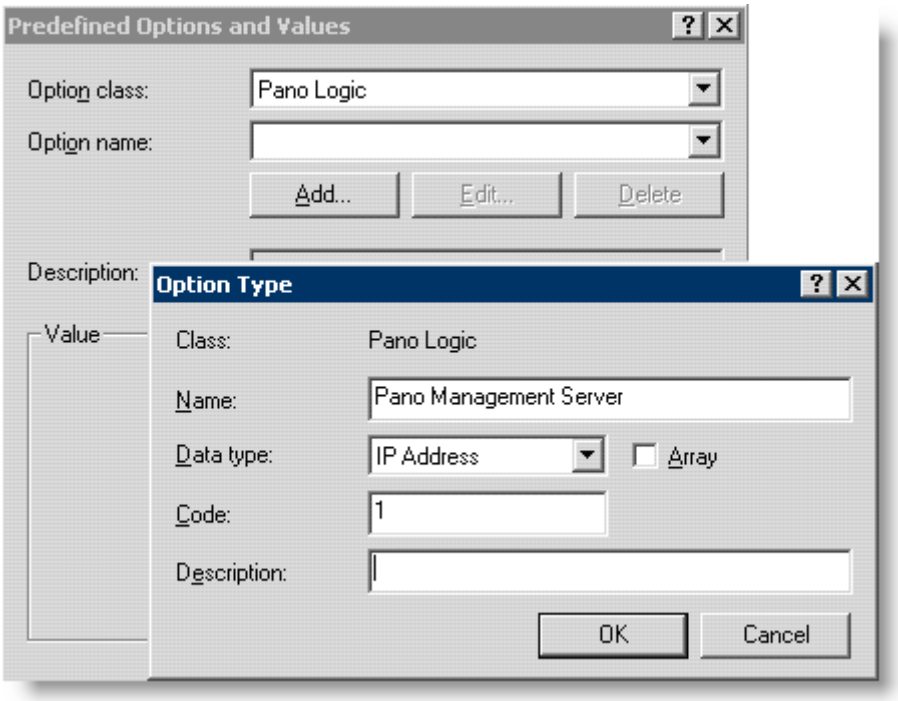
1. From the Windows Server running the DHCP Server, launch the Manage Your Server tool:
   a. Go to **Start** > **Administrative Tools** folder.
   b. Select **Manage Your Server**.
2. Click on **Manage the DHCP server**.
3. Right-click on the domain controller and click **Define Vendor Classes…**.

<Reviewer: Mike thinks that Step 3 might be incorrect--that we don't right-click on the domain controller.>

4. Create the new vendor class:
   a. In the DHCP Vendor Classes window, click **Add**.
   b. In the New Class dialog, type the following information:
      - In **Display name** field, type `Pano Logic`.
      - In **Description** field, type `Pano Manager`.
5. In the text box, and underneath **ASCII**, type `Pano Logic`. Even though it is blank you can still click there and type in the field. Click **OK**, then **5**.
6. Click **OK** to close the DHCP Vendor Classes dialog.
7. From the DHCP window, right-click on the Domain Controller and select **Set Predefined Options**.
8. In the Option Class drop-down list, select **Pano Logic**, then click **Add**.
9. In the Option Type dialog, do the following:
   a. Into the Name field, type `Pano Manager`.

b. In the Data type drop-down list, select **IP Address**.

c. In the Code field, type `1`.



d. Press **OK** to close the Option Type dialog.

10. From and Predefined Options and Values window and in the Value area, type the IP address, then click **OK**.

This IP address is the static IP address of the Pano Manager VM.

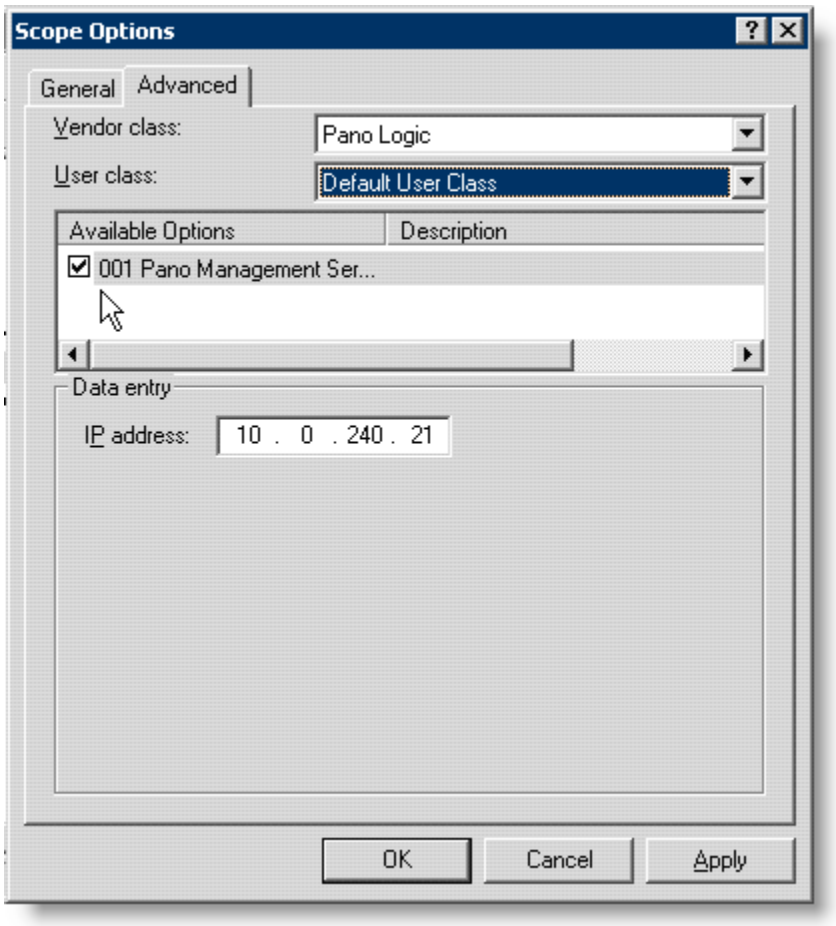
11. Under the Scope folder, right-click **Scope Options**, then select **Configure Options**.

12. In the Scope Options window, select the Advanced tab.

13. From the Vendor class drop-down list, select `Pano Logic`, then select the check box that corresponds to the Pano Manager, then click **OK**.

The Pano Manager now appears in the scope options.

Congratulations! The DHCP Server is properly configured to pass the Pano Manager's address to Pano devices.



14. Install the Pano devices, if you haven't already. Simply connect them to your network using the Pano devices' Ethernet port. To verify that the Pano devices are connected to the network, go to "Pano Button's Light Indicators" on page 15.

15. Locate the new Pano devices that the Pano Manager VM just discovered. From the Pano Manager, click on the Pano devices tab. The default name for Pano devices is `PanoDevice-`*`MACAddress`*.

Next Step(s): If you're in the process of deploying the Pano Manager VM, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

9 Verify Pano VDS Deployment

After you complete all the steps in (Start Here) Deploy Pano VDS, verify that your Pano VDS is working correctly in your environment.

To verify Pano VDS deployment:

1. For each collection type that you have, ensure that you can log on to a DVM.
   - Ensure desktop session is loaded and displayed on video monitor/LCD.
   - Ensure mouse movements and keyboard is functioning as expected.
2. Verify that you can log on to Pano Manager.
3. Ensure that Pano Manager can connect to VirtualCenter and your directory service.
4. Verify that web login works.

10
Prepare Desktop Virtual Machines

(Overview) Prepare Desktop Virtual Machines

Before You Begin: Set up the Pano Manager, as outlined in "(Overview) Integrate Pano Manager into Your Environment" on page 49, before you prepare DVMs.

When you prepare a DVM you might intend to use that single machine directly, or you might intend to use that DVM as the template from which other DVMs are cloned:

- The Perform basic DVM setup section of the following workflow describes how to create a DVM that is suitable for immediate use. The steps in this section are required for a typical trial, or as the basis for building a template.
- The Tune settings section of the following workflow describes how to configure settings for an optimal end user experience. Perform the steps in this section to deploy DVMs to end users.
- The Automate deployment section of the following workflow describes how to take advantage of the Pano VDS's ability to automatically deploy DVMs.

Task	Go to...
Perform basic DVM setup	
1. Prepare to create a DVM.	"Prepare To Create Desktop Virtual Machines" on page 63
2. Create the virtual machine.	"Create Virtual Machines" on page 63
3. Install Windows.	"Install Windows XP or Vista" on page 69
4. Install VMware Tools.	"Install VMware Tools" on page 69
5. (Important) Set hardware acceleration to `Full`.	"Set Hardware Acceleration" on page 71
6. Install the Pano Desktop Service.	"Install Pano DAS" on page 71

Task		Go to...
7.	Make sure that network settings (firewalls, proxies, etc.) are properly configured in the DVM.	"Configure DVM Firewall" on page 73
8.	Make sure that the desktop virtual machine is enabled for Remote Desktop, and that the user(s) of the desktop virtual machine are added to the Remote Desktop Users Group for that computer.	"(RDP Connections Only) Enable Remote Desktop and Set Remote Desktop Users" on page 75
9.	Wait! Let's test DVM connectivity. Don't proceed unless you have DVM connectivity.	"Verify DVM Connectivity" on page 75 "Troubleshoot DVM Login Problems" on page 155 "Verify Newly Created DVMs" on page 115
Tune settings		
10.	(Recommended) Control session timeouts.	"Control Session Timeouts" on page 78
11.	(Optional) For additional security, consider using USB filters to limit USB device use.	"Restrict or Allow Use of Specific USB Devices" on page 100
12.	(Optional) Configure video display for 24-bit color depth. 16-bit provides better user experience for most users. Graphics are much sharper with 24-bit color.	"Configure Pano DAS for 24-bit Color" on page 103
Automate deployment		
13.	Make the necessary changes to optimize DVM performance. You must do so before you create the template. You must do so before you create the DVM template so that all DVMs that you provision from this template receive the performance benefits.	"Optimize DVM Performance" on page 141
14.	If you intend to use automated provisioning (via Permanently Assigned Desktops collection type or Pooled Desktops collection type), create a DVM template.	"Create DVM Templates" on page 79
15.	Install Microsoft Sysprep tools on VirtualCenter Server.	Install Sysprep Tools on VirtualCenter Server
16.	Create the guest specification.	"Create Guest Customization Specification" on page 82
17.	Test deployment.	"Test DVM Deployment" on page 83

Next Step(s): If you're performing this workflow as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

Prepare To Create Desktop Virtual Machines

You must have valid licenses for Microsoft desktop operating systems. If you don't, the virtual machine provisioning will fail, waiting for the correct Windows product license key.

To prepare to create DVMs:

1. Identify the base desktop virtual machine you want to deploy to users. Go to "Supported Operating Systems for Pano Desktop Service" on page 31.
2. Retrieve the operating system installation media (disk) and Windows product license key.

Next Step(s): "Create Virtual Machines" on page 63

Create Virtual Machines

Create the virtual machines by doing one of the following:

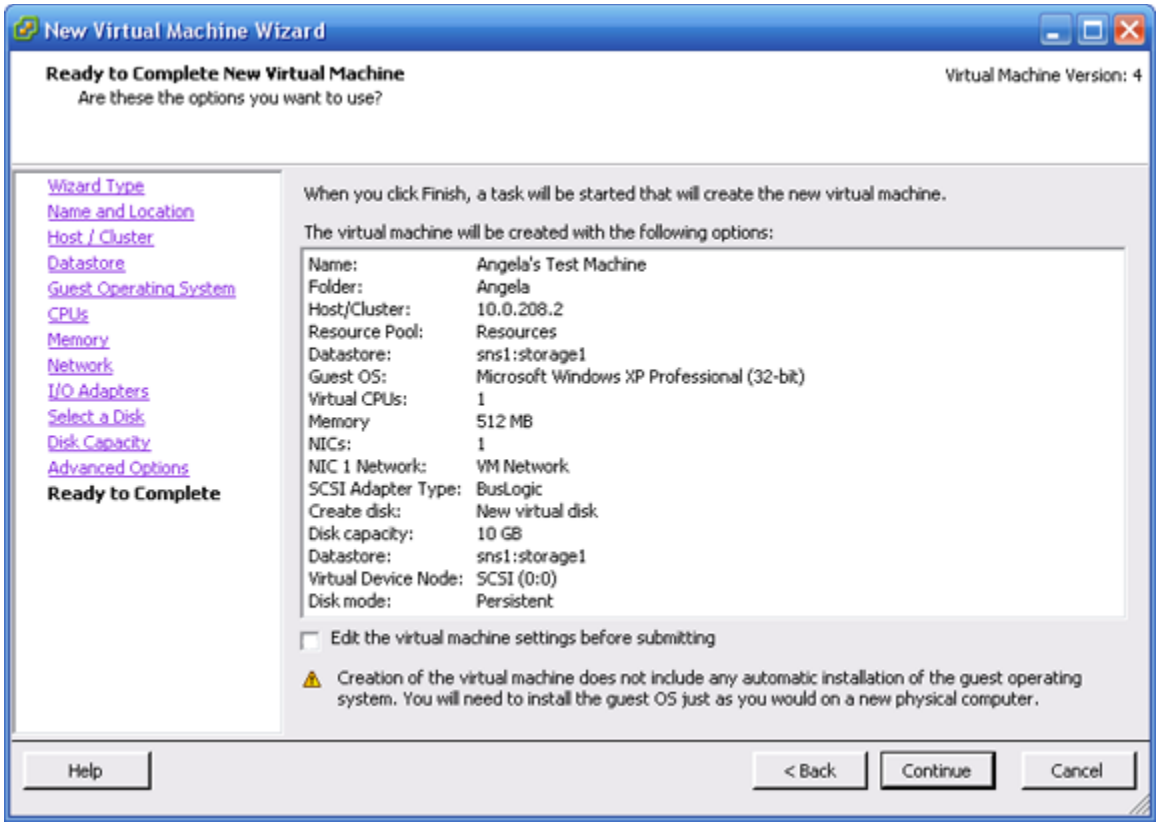
- **(Recommended)** Create from scratch, using the VMware Virtual Infrastructure Client. This approach is outlined below.
- **(Not Recommended)** Create by converting a physical machine to a virtual machine, using either the standalone version of VMware Converter or the version integrated with VirtualCenter. VMware Converter images the target PC and migrates it into VMware VI3. This method is not recommended for production because this method doesn't result in an optimal virtual machine. This method is a "quick and dirty" conversion in the event that you want to try out Pano VDS, or if you have a virtual machine that you can't recreate from scratch.

To create a desktop virtual machine from scratch:

To create a virtual machine from scratch, use the VMware Infrastructure Client (VMware VIC).

1. Using the VMware VIC, connect to VirtualCenter.
2. Launch the New Virtual Machine Wizard (**File** > **New** > **Virtual Machine...**), then select **Custom** as the baseline settings for the virtual machine.

3. Follow the wizard's instructions to create the initial virtual machine, specifying values for the following settings:



Parameter	Description
Name and Location	A descriptive and unique name for your virtual machine template (for example, `xptemplate`). The location of the virtual machine can be any folder in your datacenter inventory. Pano Logic recommends that you name the folder `Templates`.
Host/Cluster	The standalone ESX host or ESX host that is part of a cluster that will be used to run this virtual machine. The location of the initial virtual machine or template does not specify where future virtual machines will reside: you can change this host/cluster at anytime.
Resource Pool	If your ESX server resources are divided into resource pools, you can assign these resource pools to this virtual machine.
Datastore	The location where files associated with the virtual machine should be stored.
Guest Operating System	The operating system that you will install on the virtual machine. It's best practice that the template name include the name of the operating system (for example, `xptemplate`).
CPUs	The number of virtual processors that will be presented to the virtual machine. A single processor is sufficient for most of your users.

Parameter	Description
Memory	The amount of memory to allocate to each virtual machine that you create from the template. 512MB is enough for most users running typical Microsoft Office applications. In rare cases where your users are running memory intensive applications, allocate 1 GB.
Network	The number of virtual network adapters that the virtual machine needs to use. Most virtual desktops need only one network adapter.
I/O Adapters	BusLogic drivers that come pre-installed with Windows XP are sufficient for Pano VDS users. (For VDI-based deployments, VMware recommends the LSI Logic adapter. However, the LSI Logic driver is not included as part of the Windows XP installation. You must download and add it during the OS installation.)
Disk	Because you are creating a new virtual machine, choose **Create a new virtual disk**.
Disk Capacity	The disk space that you assign to the virtual machine. Assign at least 10 GB. It's a best practice to store as much of the user's data on a network share rather than on the virtual machine (locally). When saving locally, ask users to save to My Documents, and back up that data.
Advanced Options	Accept the default Virtual Device Node. Also, there's no need to specify a Mode.

Tip: A few things to consider:

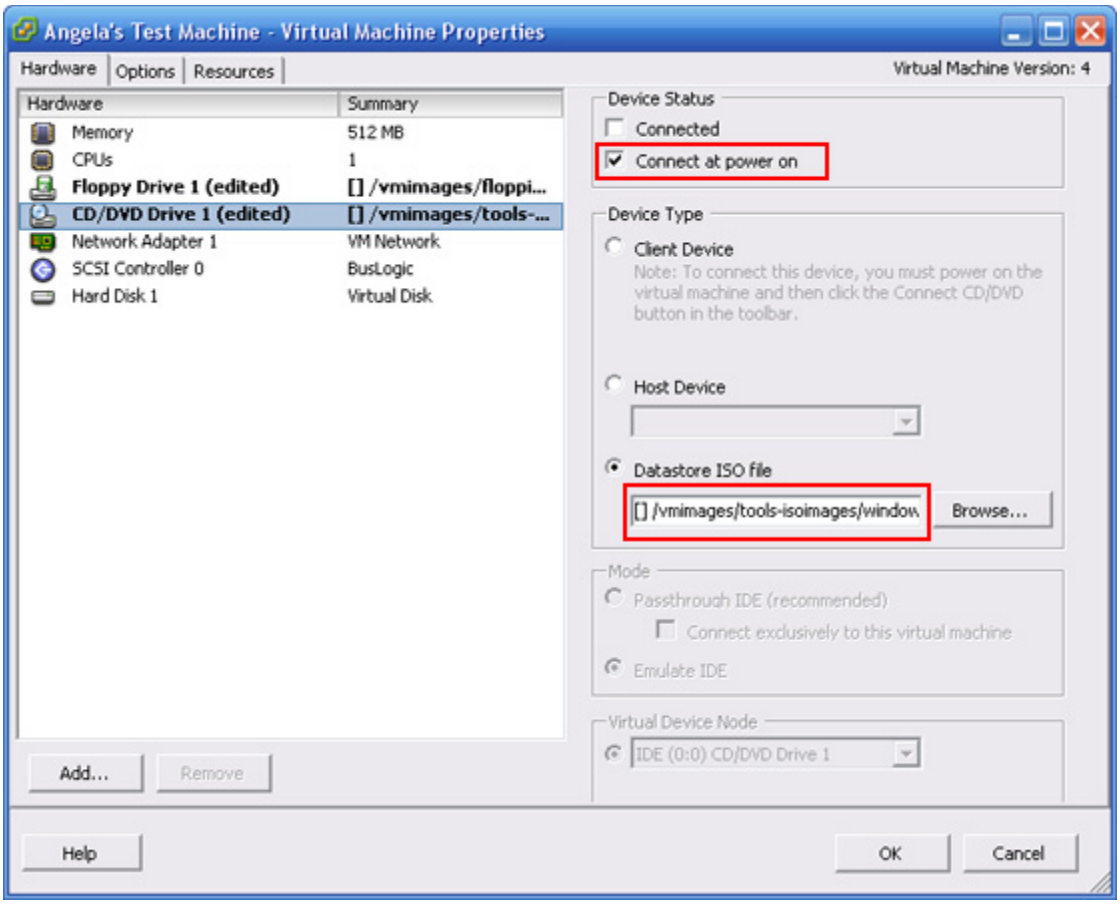
- Physical-to-Virtual (P2V)

Except in select cases Pano Logic does not recommend using a Physical-to-Virtual (P2V) conversion to create a DVM template. A P2V conversion yields large disk image that is difficult to manage in a VDI environment. Other drawbacks associated with a P2V conversion include preservation of any "OS faults" that the physical machine might have had.

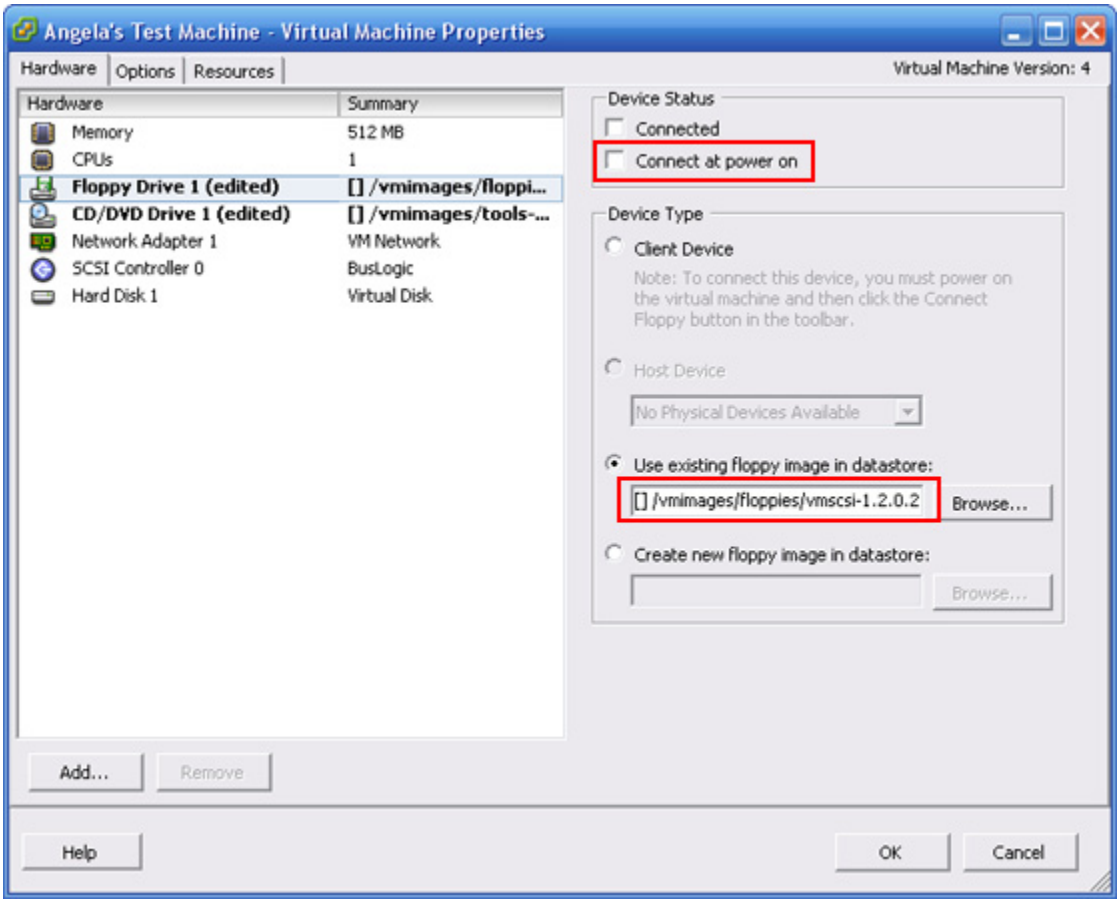
- DVM disk size

The size of the virtual disk of a DVM should be kept to a minimum. Large disks will consume more Storage resources and make it longer to provision new DVMs.

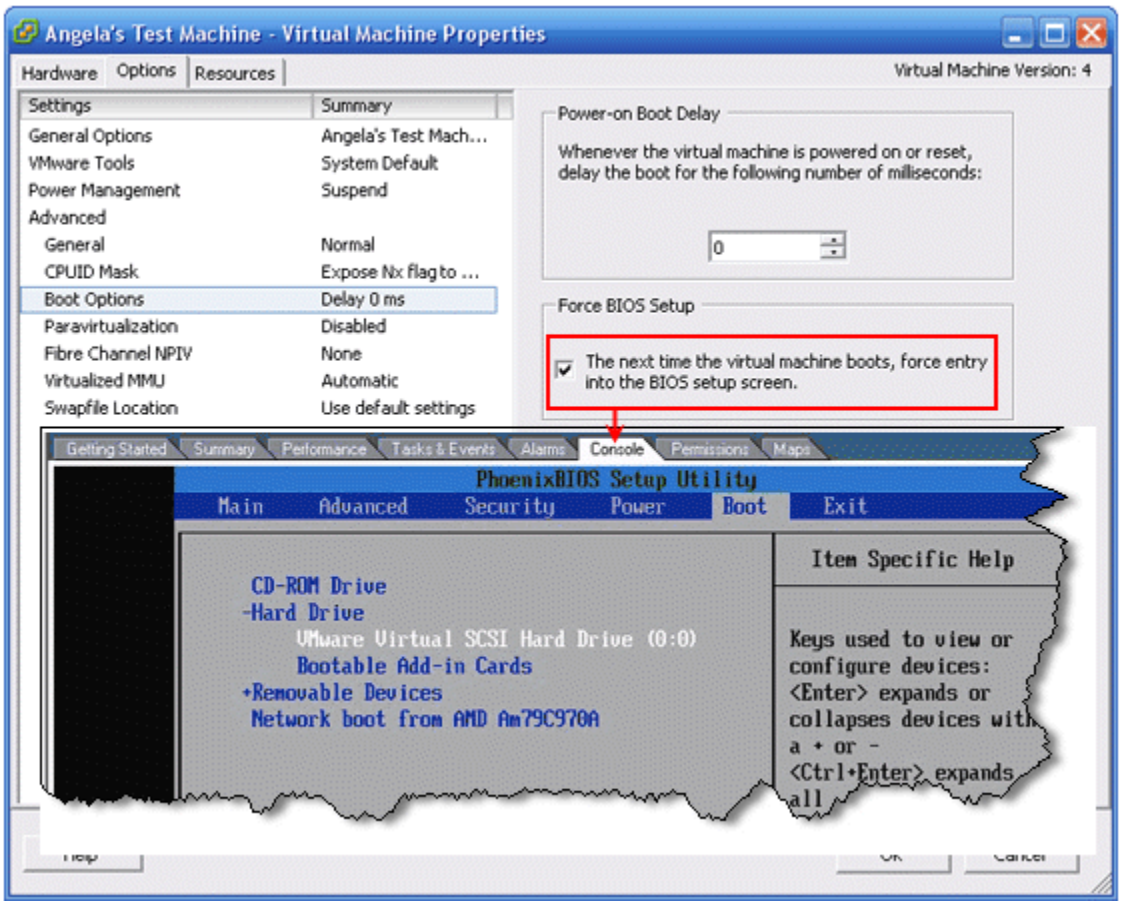
4. Before you start the Windows installation, do the following:
   a. From VirtualCenter, locate the virtual machine that you just created, power on the virtual machine, and select **Edit Settings**.
   b. Edit the following hardware settings:
      - Ensure the CD/DVD drive is present and configured to connect at power on.
      - Ensure the CD/DVD Device Type is configured to point at the Windows CD or ISO image.



- Ensure a Floppy Drive is present and does not connect at power on. The `Connect at power on` option enables the DVM to boot from that device.
- Ensure the Floppy Drive's Device Type is configured to point at the BusLogic image: `/vmimages/floppies/vmscsi-1.2.0.2.flp`. This driver improves SCSI virtual disk performance.



- Launch the BIOS setup screen by selecting the **Force BIOS Setup** option.
- From VirtualCenter, go to the virtual machine, and click the **Console** tab.
- Click the **Boot** tab and change the order of the boot options to (1) CD-ROM drive (2) Hard drive, and (3) Removable Devices.



Next Step(s):

1. (Windows XP) "Install Pano Device USB Support" on page 97
2. "Install Windows XP or Vista" on page 69

Install Windows XP or Vista

After you create the virtual machines as outlined in “Create Virtual Machines” on page 63, you’re ready to install the operating system (Windows XP or Vista) for those virtual machines.

To install Windows XP or Vista:

1. From the VMware Infrastructure Client (VMware VIC), connect to VirtualCenter.
2. Power on the virtual machine that you created in “Create Virtual Machines” on page 63.
3. Use the console in VirtualCenter to view the boot process and to send input to the virtual machine.
4. As the Windows Setup process begins, press **F6** to add an additional SCSI driver to specify the BusLogic driver on the floppy image.
5. Switch over to the VirtualCenter, select **Floppy Drive 1** on the left and select the **Connected** checkbox.
6. When Windows XP setup asks for the floppy with the SCSI driver, press **ENTER** and the system will be able to browse the floppy image that you specified when you created the virtual machine.
7. Complete the Windows XP or Vista setup just as you would for a typical Windows installation.

   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, which you’ll do shortly, go to “Create Guest Customization Specification” on page 82.
8. Apply the most recent Microsoft updates and service pack.

Recommendation: Install the updates recommended in Supported Operating Systems for Pano Desktop Service.

9. Verify that Windows machine boots properly, that you can log on, and that it joined the domain.

Next Step(s): “Install VMware Tools” on page 69

Install VMware Tools

The Pano Manager VM has VMware Tools preinstalled, so you don’t need to install VMware Tools for this component. However, you do need to install VMware Tools for all your DVMs.

VMware bundles the latest VMware Tools with VI3. For detailed instructions, go to “Installing and Upgrading VMware Tools" in the VMware V13 Basic System Administration Guide. The benefits of VMware Tools:

- Better network, virtual-disk, and keyboard performance.
- Time synchronization between the host and guest operating system. The Options tab in VMware Tools provides a Time synchronization check box.

To install VMware Tools:

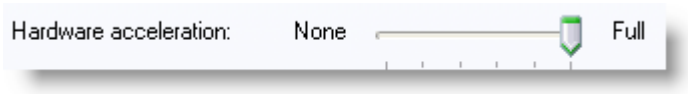
1. Use the VMware Infrastructure Client (VMware VIC) to connect to VirtualCenter.
2. Locate the virtual machine on which you intend to install VMware Tools.
3. Right-click on the virtual machine and select **Install VMware Tools**.

Next Step(s): “Set Hardware Acceleration” on page 71

Set Hardware Acceleration

Pano DAS v2.5.1 uses Console Direct technology (Console Direct). Console Direct requires that you set hardware acceleration to `Full`. This is not a step that you should overlook: without this setting, mouse movements will become very slow.

1. From the Windows Control Panel, go to **Display** > **Settings**.
2. Click the **Advanced** button.
3. Click the **Troubleshoot** tab.
4. Set **Hardware acceleration** to `Full`.



Next Step(s): "Install Pano DAS" on page 71

Install Pano DAS

The Pano Desktop Additions Wizard walks you through the installation of the Pano Desktop Service (Pano DAS). You must install the Pano DAS on all DVMs that you want to access from Pano devices. However, start with one DVM initially because in "Verify DVM Connectivity" on page 75 you need only one DVM to test connectivity. Once you verify connectivity, you can install the Pano DAS on all other DVMs.

To install the Pano DAS:

This version of the Pano DAS—v2.5.1, supports both Console Direct technology (Console Direct) and Pano Classic. By default the install wizard configures Pano DAS for Console Direct. After you complete this installation, you might need to switch between these modes, depending on your environment. For more information, go to "Switch Connection Modes" on page 14.

1. Make sure that your operating system is supported. Go to "Supported Operating Systems for Pano Desktop Service" on page 31.
2. Make sure you have administrative rights to the desktop virtual machine.
3. Copy the Pano DAS installer file (`PanoDAS.msi`) from the Pano media disk, or download the package to the DVM's local drive.
4. Double-click on `PanoDAS.msi`. The Pano Desktop Additions Wizard launches. Follow the on-screen instructions.
5. If prompted, save and close all open applications. The installer waits for you to close all applications. Click **Retry** to continue with the installation.

   The installer prompts you to close all open applications because the installer will automatically restart Windows in order to complete the installation.
6. (Windows XP) If prompted to install a Windows USB driver (`USBD.sys`), do so now. The installer can detect if this file is installed in `C:/Windows/System32/drivers`. Go to "Install Pano Device USB Support" on page 97.

   If you plan to allow redirection of advanced USB devices such as printers, scanners or mass storage, you must first install the Windows USB driver (`USBD.sys`) on your virtual machine or template. Go to "Install Pano Device USB Support" on page 97.

Pano Logic would love to make your life easier by installing this support automatically, but Microsoft doesn't allow this file to be redistributed. Sorry.

7. (Windows XP SP2/SP3) If prompted to install a Windows hotfix (KB952132), do one of the following:
   - If you don't want to install the hotfix, perform the installation through the VMware Infrastructure Client (VMware VIC), or use a software distribution tool such as SMS.
   - If you want to perform the install using RDP, download and install the Windows hotfix.

   Pano Logic would love to make your life easier by installing this hotfix automatically, but Microsoft doesn't allow this file to be redistributed. Sorry.

   If you decide to transfer this file by sending it to your work email account, consider that some Spam firewalls identify `.zip` files and `.exe` files as spam. As such, it's best to email the file to a web mail account, or save the file to a USB key.
8. Follow the steps in the wizard. When prompted to choose the installation type, choose Typical setup or Complete setup.
9. Wait 10 to 30 seconds. The installer tries to install the drivers, and temporarily disappears for about 10-30 seconds in order to enable you to see potential Windows alerts. Windows alerts are notorious for launching in the background.
10. If you receive a Windows alert, do one of the following:
    - If the `Devices: Unsigned driver installation behavior` setting in your GPO is set to **Warn but allow installation**, the wizard asks you to approve the installation of these unsigned drivers. You must approve to continue with the installation. Click **Continue Anyway**.
    - If the `Devices: Unsigned driver installation behavior` setting in your GPO is set to **Do not allow installation**, Windows displays a dialog box (an alert) because the Pano DAS installer wants to install unsigned drivers. Do the following:
      - From the wizard, click **Cancel** to manually exit the installation.
      - Change the **Devices: Unsigned driver installation behavior** setting in your GPO to allow unsigned drivers: Go to **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**, then change it to `Silently succeed`.
      - Uninstall Pano DAS: From the Windows Control Panel, double-click on **Add or Remove Programs**, go to **Pano Desktop Additions** and click **Remove**.
      - Launch the Pano Desktop Additions Wizard again, and continue with the installation.
11. Wait for the system to reboot before you attempt to log on to the desktop virtual machine.
12. (Important!) Log on to the DVM.

    If you don't, your end-users might be prompted to type credentials with Administrator privileges. This behavior is caused by a Windows bug that is currently unresolved. The Administrator credentials are not necessary; users can dismiss the dialog, but the prompt may confuse or concern them.
13. If you have less than 10Mbps end-to-end or the DVM is running Vista, switch to Pano Classic. Go to "Switch Connection Modes" on page 14.
14. Congratulations! You've successfully installed Pano DAS.

Next Step(s): "Configure DVM Firewall" on page 73

Configure DVM Firewall

The Pano DAS communicates with the Pano Manager and Pano devices over certain network ports. If there is a firewall on the DVM, it needs to be configured to allow communication over certain ports for both inbound and outbound traffic. Otherwise, the DVM fails because it cannot communicate with the Pano Manager.

You can configure the DVM's Windows Firewall using one of the following methods:

- Domain policy
- Local policy

Domain policies have higher precedence than local policies. Therefore, you should not expect local policies that are applied to a DVM template to always be used when new DVMs are cloned from the template. The best strategy is to always use the domain level GPOs.

Remember, GPOs can be applied to an organizational unit (OU) so it is possible to narrow the scope of this Firewall policy to just the collections of DVMs that the Pano Manager manages.

To use a local policy or domain policy to open the ports:

1. Become Domain Admin on any Windows Server.
2. Do one of the following:

   For domain policy:

   a. Launch the Group Policy Wizard.

   b. When prompted for the Group Policy Object (GPO), select **Local Computer.**

   For local policy:

   a. Open Microsoft Management Console's (MMC) Group Policy Object Editor snap-in.

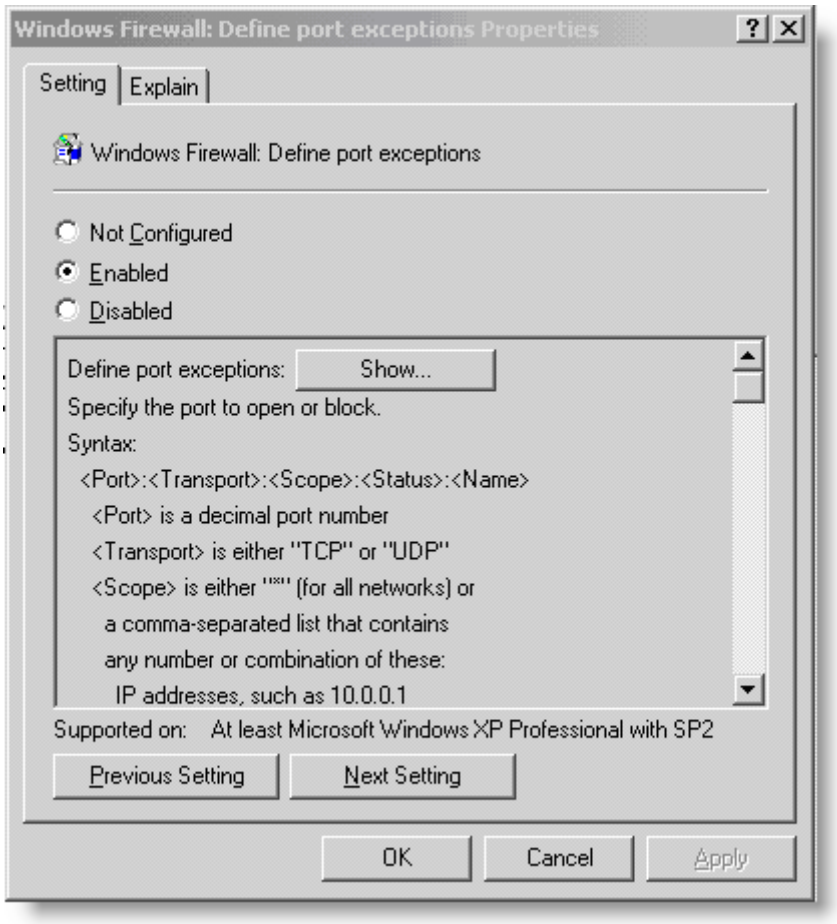
   b. Select the default domain policy.
3. Navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile**.
   - The Domain Profile is where you set the properties that take effect when the machine is running attached to a domain.
   - The Standard Profile is where you specify different firewall settings for times when the computer is disconnected from the domain.
4. Open TCP and UDP ports–both inbound and outbound:

   a. Double-click on **Windows Firewall: Define port exceptions** setting. The Windows Firewall Define port exceptions window appears.

   b. Click **Show**.

   c. Add the following two lines. The syntax is described in the Explain tab of the properties dialog box.

```
8319:TCP:*:Enabled:Pano Manager Connection
8321:UDP:*:Enabled:Pano Device Connection
```



d. Click **OK,** then **OK** again. You're done!

Next Step(s): "(RDP Connections Only) Enable Remote Desktop and Set Remote Desktop Users" on page 75

(RDP Connections Only) Enable Remote Desktop and Set Remote Desktop Users

Console Direct technology does not rely on RDP and does not require that you set the Remote Desktop Users group; however, Pano Logic recommends that you configure this property to enable your users to connect via Windows Remote Desktop Connection and the Pano web access.

To enable remote desktop and set remote desktop users:

1. Log on to the desktop virtual machine.
2. Right-click on **My Computer**, and select **Properties**. The System Properties dialog appears.
3. Select the **Remote** tab.
4. Select the **Allow users to connect remotely to this computer** check box.
5. Click the **Select Remote Users…** button.
6. Click **Add…** to select the desired set of users, then add all users who need to connect to a DVM in this template's collection.
7. Click **OK** to close the Remote Desktop Users dialog, click **Apply**, then **OK**.

Next Step(s): "Verify DVM Connectivity" on page 75

Verify DVM Connectivity

This procedure assumes that you've already installed at least one Pano device, and that it is properly connected to the network. If your Pano devices aren't connecting to the network, go to "Pano Button's Light Indicators" on page 15.

Perform this procedure before adding additional DVMs or enabling automated deployment. Don't proceed with your deployment unless you have verified basic DVM connectivity. This procedure verifies that you can connect to your DVM from a Pano device.

In order to run this test you need to create a DVM collection. The DVM collection associates the authorized user(s) to the specified DVM(s).

To verify DVM connectivity:

1. Connect one existing virtual machine to a single Pano device by simply adding one DVM to the Existing Desktops collection type. For simplicity, you must use the Existing Desktops collection type:
   a. Log on to the Pano Manager.
   b. Click the **DVM Collections** tab.
   c. Click **Add**. The Add DVM Collection window appears.
   d. Specify the following parameters:
      - **Type** - Select `Custom`.
      - **Name** - Enter a name for the DVM collection. Let's call it `Test`.
      - **Users** - Click the browse button (…) to find the directory objects to which you want to give access to the DVM collection. You can select security groups, users and organizational units (OU). Select the object(s), and then click OK.

- **DVMs Folder** - Browse to find the VirtualCenter folder that contains the DVM that you created earlier for this collection. Select the folder, and then click **OK**. If you organized your DVMs as outlined in "Organize DVMs, Templates, Folder in VirtualCenter" on page 107, then the folder name is `DVMs`.
- **Login Enabled** - Select this check box. When checked, users that are entitled to the collection are allowed to log on. Now let's see if you one of the authorized users can log on to the DVM.

2. From the Pano device, log on to the DVM as one of the authorized users.
   - If Windows appears, then you have successfully verified the basic operation of the Pano Virtual Desktop Solution. Wonderful! You're ready to proceed.
   - If you are not successfully connected to the Windows desktop, go to "Troubleshoot DVM Login Problems" on page 155 and "Verify Newly Created DVMs" on page 115.

Next Step(s): "Control Session Timeouts" on page 78

(Optional) Provide Disposable Desktops

For DVMs in a Pooled Desktops collection type, you have the option to make those DVMs disposable by making each DVM's hard drive a *non-persistent disk*. If you intend for most of your users to have a Pooled Desktops collection type and you want the DVMs in that collection to be disposable, make the configuration change as part of your template.

With disposable dekstops, when a user makes any changes to a DVM, then logs off, Windows powers off that DVM. When that DVM is powered on the changes made by the user are gone due to non-persistent disk.

A non-persistent disk adds greater security. If while searching the web users downloaded viruses, the user data associated with that virus would be immediately deleted after the user logs off, and that virus would not spread to future users of that DVM from the pool.

Often users save cookies and passwords as they browse the web; this data would also be deleted. Lastly, any personal files that the users saves would be deleted, so that other users do not have access to this data.

There's no need for users with disposable desktops to understand that their data isn't saved because users of a Kiosk expect their data to be deleted when they log off.

To provide disposable desktops:

1. Download PsShutdown to the DVM's desktop. PsShutdown is part of Windows SysInternals (PsTools).
2. Extract `PsTools.zip` to a `PsTools` folder on the DVM's desktop. `PsTools.zip` includes many tools, but you only need one of them–PsShutdown.
3. Assuming that `psshutdown.exe` is under `C:\\Desktop\PsTools`, add the following line to `SessionLogout.cmd` script under `C:\Program Files\Pano Logic\Pano Desktop Additions\SCRIPTS`:

```
"C:\\Desktop\PsTools\psshutdown.exe" -k -f -t 2
```

1. Copy `psshutdown.exe` from the temporary folder to is part of Windows SysInternals
2. Configure DVM's hard drive as a *non-persistent disk*:
   a. From VirtualCenter, right-click on the DVM and choose **Edit Settings** > **Hard Disk**.
   b. Change to `Non-Persistent disk`.

3. Power off then power on the virtual machine. A reboot won't do the trick. You must power-cycle the DVM.
4. (Recommended) To minimize the amount of time users need to wait for a DVM, when you create the Pooled Desktops collection type set **Extra Powered Off** to `0` and **Extra Powered On** to at least `3`.

Control Session Timeouts

Pano Logic supports session timeout settings that can be used in a Pano VDS environment to help manage users and resources. These Session Timeout settings end two type of sessions:

• Idle Session Timeout

Idle Session Timeout can be used as an alternative to pressing the Pano Button to disconnect a user after a specified period of inactivity.

A timelimit can be specified where if there is no keyboard or mouse movement, Pano VDS does one of the following:

- **Disconnects user from session**. If the specified action is to `disconnect`, the user's Windows session remains active and the Pano device returns to the Pano client login screen.
- **Logs off the user**. If the specified action is to `logoff`, Pano VDS automatically logs off the user, thereby ending the Windows session, and the Pano device returns to the Pano client login screen.

Warning: Forcing a logoff in this manner causes unsaved data in the session to be lost.

To specify the idle session timeout value:

Specify (in seconds) this value in the registry string value: `HKEY_LOCAL_MACHINE\SOFTWARE\Pano Logic, Inc.\Pano Desktop Additions\Native Session\Max Idle Time`. A value of `0` disables the idle session timeout. The Pano Desktop Service (Pano DAS) must be restarted for this change to take effect.

To specify the action when the idle timeout limit is reached:

Specify the action in the registry string value: `HKEY_LOCAL_MACHINE\SOFTWARE\Pano Logic, Inc.\Pano Desktop Additions\Native Session\Logoff On Max Idle Time`. Choose one of two values:

- `True` - causes the user to be logged off when the session timeout limit is reached.
- `False` - causes the user to be disconnected when the session timeout limit is reached.

The Pano Desktop Service (Pano DAS) must be restarted for this change to take effect.

• Disconnected Session Timeouts

Disconnected Session Timeouts are particularly useful for your users as they can use the Pano Button to disconnect the Pano device from their DVM. This feature enables users to secure their desktop when they walk away or roam to another office or conference room to pick up their session on another Pano device.

The problem is that these disconnected but active sessions could be running for hours or days if the user is away from the office. A disconnected timeout can be used to automatically log out the user (end the user's Windows session) after a specified period of time passes and after the user's presses the Pano Button.

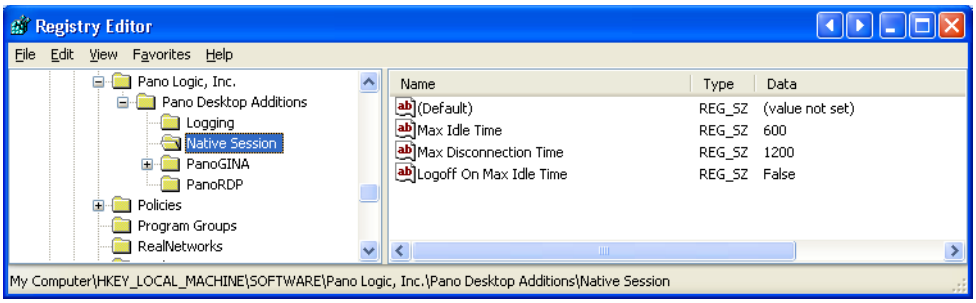
This time can be set long enough to enable fast Pano device mobility around the office without keeping the DVM running for days with no use. When the session limit is reached, Pano VDS automatically logs off the user from Windows.

To specify a disconnected timeout value:

Specify (in seconds) in the registry string value: `HKEY_LOCAL_MACHINE\SOFTWARE\Pano Logic, Inc.\Pano Desktop Additions\Native Session\Max Disconnection Time`. A value of `0` indicates no maximum time. After this timeout limit is reached, the Pano VDS logs off the user and ends the user's session.

You can use `Max Idle Time and Max Disconnection Time` timeouts in a cascading manner, in which Pano VDS disconnects the idle user after a specified period of time, then logs off the user after a separately specified period of time.

The following example instructs Pano VDS to disconnect the user after being idle for 10 minutes; after being disconnected, the user has 20 minutes to reconnect before Pano VDS automatically logs off the user:



The Pano Desktop Service (Pano DAS) must be restarted for this change to take effect.

Next Step(s): Do the following:

1. (Windows XP) "Install Pano DAS" on page 71.
2. "Create DVM Templates" on page 79.

Create DVM Templates

Use templates to create multiple identical desktop virtual machines. You must create a DVM template for User Permanently Assigned Desktops collection type or Pooled Desktops collection type. In VirtualCenter, create a template by doing one of the following:

- Cloning a virtual machine to a template.
- Converting any desktop virtual machine into a template

Templates provide the following benefits:

- They save you time by enabling you to automate desktop provisioning and quickly update (manage) virtual machines.
- They ensure consistency and reduce the risk of human error.

Consider creating a separate template by one of the following:

- Business unit (Finance, Sales, HR, etc); or
- User type. types of users (Administrator, Technical Support Engineer, Software Engineer, Office Administrator, etc) where each user might require; or
- Workgroup.

Each business unit, user type, or workgroup might require unique software or virtual hardware configuration. Choose to create templates based on the method that makes sense for your organization.

To convert a virtual machine into a template:

Any virtual machine can be converted to a template. This conversion is done from VirtualCenter. DVM templates are created within VirtualCenter using the standard VMware procedures. For detailed instructions, go to "Working with Templates and Clones" chapter of the VMware VI3 Basic System Administration Guide.

Note: A virtual machine can also be cloned to a template by simply creating a copy of the virtual machine, leaving the original virtual machine in place. This method is helpful if you update the template and redeploy desktops often, for instance, when deploying Pooled 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.

1. Connect to VirtualCenter.
2. Locate the virtual machine in the inventory**.**
3. Select **Convert to Template**.

To clone a virtual machine to a template:

For detailed instructions, go to “Working with Templates and Clones” chapter of the VMware VI3 Basic System Administration Guide.

Cloning creates a copy of the virtual machine. The original virtual machine remains in tact and unchanged. With cloning you can convert a template to a virtual machine, update the virtual machine, then convert it back to a template at any time. Use this method if you update templates and redeploy often.

Next Step(s): “Install Sysprep Tools on VirtualCenter Server” on page 81.

Install Sysprep Tools on VirtualCenter Server

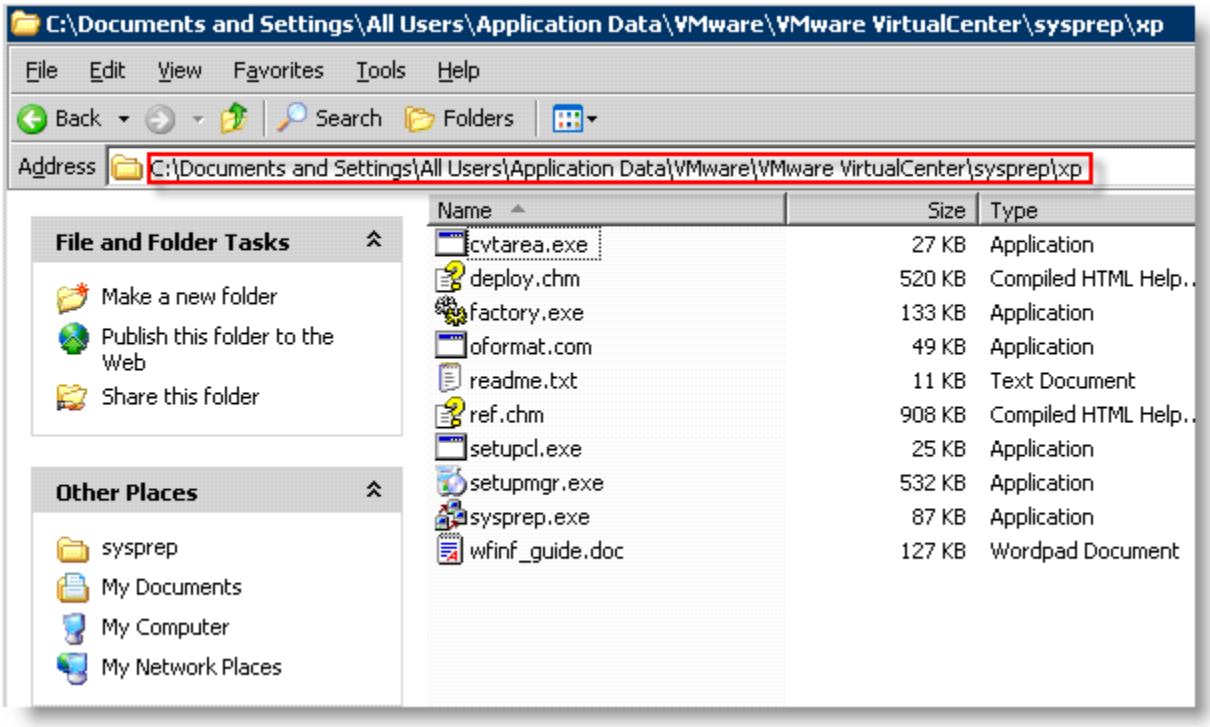
Microsoft Sysprep tools is Microsoft's System Preparation utility for automated Windows deployment. Sysprep needs to be installed on the host on which VirtualCenter is running so that VirtualCenter can automatically create DVMs when required. This procedure assumes that the VirtualCenter server is running Windows XP, so adjust this procedure as necessary.

For detailed instructions, go to VMware's Installing the Microsoft Sysprep Tools procedure

To install Sysprep:

1. Download `deploy.cab` file (shortname for Deployment Tools) from Microsoft's website. Every Windows operating system has a different `deploy.cab` file.
2. On the VirtualCenter server, copy `deploy.cab` to `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\sysprep\xp`.

   That's all!



Next Step(s): "Create Guest Customization Specification" on page 82

Create Guest Customization Specification

A guest Customization Specification enables you to customize virtual desktops as you clone them from a template. You must create a guest Customization Specification from within VMware VirtualCenter.

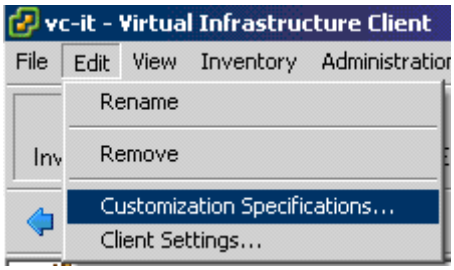
Within your VirtualCenter, simply use the Customization Specification wizard to specify details such as virtual machine name, license key, domain to be joined, etc. This Customization Specification uses the Microsoft Sysprep files from the `deploy.cab` file on your Windows install media, which you place on your VirtualCenter server to give DVMs a unique SID and to prepare them for use in your environment.

Once the sysprep files are on your VirtualCenter server and you have configured your Customization Specification, simply tell your Pano Manager two things: (1) the name of the Customization Specification to use, and (2) number of DVMs you'd like to always have available.

To create a guest customization:

For detailed instructions, go to the “Customizing Guest Operating Systems” chapter of the VMware VI3 Basic Administration Guide.

1. Ensure that you have Microsoft Sysprep Tools installed. You probably installed this earlier in “(Overview) Install and Configure Pano Manager VM” on page 37.
2. Connect to VirtualCenter.
3. Select **Edit** > **Customization Specification**. The Customization Specification wizard launches.



4. Type the name of your organization, then click **Next**.
5. In the **Computer Name** windows, select the **Use the virtual machine name** radio button, then click **Next**.

   The names of DVMs that VirtualCenter creates must match the names of virtual machine names. The name of the DVM is defined in the DVM collection specification in the Pano Manager.

   For example, if the DVMs are for employees in your Technical Support department, in the Pano Manager you can specify `Support` as the name of the DVM collection. Pano Manager works with VirtualCenter to create DVMs named `Support-1`, `Support-2`, `Support-3`, etc.
6. In the **Windows License** window, do the following:
   a. Type the Windows License information for the Windows DVMs. The license can be the volume license number.
   b. Clear the **Include Server License Information** check box, then click **Next**
7. In the **Administrator Password** window, do the following:
   a. Type the local administrator password for the DVM to be created.

b. Clear the **Automatically log on as the administrator** check box, then click **Next**. Typically you don't want users to log on as administrator.

8. In the **Network Interface Settings** window, select the **Typical settings** radio button for network interface so that the DVM will obtain an IP address from DHCP once it is created, then click **Next**.
9. In the **Workgroup or Domain** window, specify the Windows domain that this DVM should join, then click **Next**.

   The DVMs must be part of a domain because the Pano Manager only authenticates the user against a directory (for example, Active Directory).
10. In the **Operating System Options** window, click the **Generate new Security ID (SID)** radio button to specify that the system create the SID, then click **Next**. You're done!

Next Step(s): "Test DVM Deployment" on page 83

Test DVM Deployment

To test DVM deployment:

1. Deploy a DVM from the template. "Deploying Virtual Machines from Templates" chapter of the VMware VI3 Basic Administration Guide.
2. Verify that the DVM joins the domain successfully. This means that the guest Customization Specification is working.
3. Verify that you can connect to the DVM remotely through the Windows Remote Desktop Connection client.

If everything looks good, you're ready to move on.

Next Step(s): If you're performing this task as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

11

Configure and Manage Pano Devices and Desktop Preferences

(Overview) Set User Preferences

Before You Begin: You must set up your collections, as outlined in "(Overview) Create DVM Collections" on page 105, before you can set user preferences.

Task	Go to...
1. Set login image	"Load Custom Pano Login Image" on page 87
2. (Optional) Configure for dual-monitor use	"Configure Pano Devices for Dual-Monitor Use" on page 89
3. (Optional) Add Pano devices	"Manually Add Pano Devices" on page 89
4. Set preferences	"Default User Login Preferences" on page 91

Next Step(s): If you're performing this workflow as part of a deployment, this workflow completes your deployment. Congratulations!

About Pano Devices Tab

Column Name	Description
Name	The name of the Pano device. The Pano Manager automatically generates this name. You can edit the name by clicking on the **Edit...** button.
Secondary	The Pano device associated with the Pano device that shows the secondary monitor for the user.
Dual Monitor	Lists the association between Pano devices.
MAC Address	The unique MAC address for the Pano device's network interface.
IP Address	The IP Address of the Pano device.
Connection	Connection status of the Pano device as known to the Pano Manager. The status can be: • **Unreachable** - The Pano Manager cannot contact the Pano device. • **Discovered** - The Pano Manager has discovered the Pano device on the network. • **Login** - The Pano Manager is running the login screen and is waiting for a user to log on. • **DVM** - The DVM is connected to a Pano Manager.
Rx Packets	Number of packets per second received by the Pano device as observed by the Pano DAS.
Re Rx Packets	Number of identical packets per second received by the Pano device multiple times as observed by the Pano DAS.
Tx Packets	Number of packets per second transmitted by the Pano device as observed by the Pano DAS.
Re Tx Packets	Number of identical packets per second transmitted by the Pano device multiple times as observed by the Pano DAS.
Min RTT	Minimum round-trip time from the Pano device to an agent on the DVM and back. A “normal” range varies from network to network; compare this metric against typical traffic for your specific network.
Avg RTT	Average round-trip time from the Pano device to an agent on the DVM and back. A “normal” range varies from network to network; compare this metric against typical traffic for your specific network.
Max RTT	Maximum round-trip time from the Pano device to an agent on the DVM and back. A “normal” range varies from network to network; compare this metric against typical traffic for your specific network.

Load Custom Pano Login Image

You can replace the image that is presented on the Pano client login screen. The image must meet the following requirements:

- Image format must be PNG
- Image dimensions must be 640 pixels wide by 200 pixels high or smaller
- Image file size must be less than 1MB

To load a custom image:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Click on the **Settings** button, then choose **Login Image…**.
4. Press the **Set Custom Image…** button.
5. Select the desired image from your local disk, then close the window.

Next Step(s): (Optional) “Restart Pano Client Login Screens” on page 88

Reset Pano Login Image To Default Image

To reset the image to the default:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Click on the **Settings** button, then choose **Login Image…**.
4. Click **Restore Default Image**, then close the window.

Next Step(s): (Optional) "Restart Pano Client Login Screens" on page 88

Restart Pano Client Login Screens

After you load or reset the login image, the login image changes the next time the user logs on (that is, when the Pano client login screen restarts). However, you can restart all Pano client login screens to force the change.

To restart all Pano client login screens:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Click on the **Settings** button, then choose **Restart all...**.

Configure Pano Devices for Dual-Monitor Use

Two Pano devices can be configured to work as a team to provide a single Windows desktop that is spanned across two monitors. To configure this option attach two Pano devices to the network as normal. Make sure each Pano device is discovered by the Pano Manager and that you can access the Pano VDS from either device.

The requirements for dual-monitor use are as follows:

- The primary monitor must be placed to the left of the secondary monitor.
- The monitors that make up the pair must support a common vertical resolution.
- Both Pano devices must be attached to the network and functioning. This pair of Pano devices operate as a team. If any member of the team is not available you will not be able to log on.

To configure a pair of Pano devices for dual-monitor use:

1. Arrange the equipment so that the Pano device that is to be primary is connected to the left monitor and the Pano device that is to be the secondary is connected to the right monitor.
2. Log on to the Pano Manager.
3. Click on the Pano devices tab.
4. Select the primary Pano device from the list and click **Edit…**.
5. Type the name of the secondary Pano device.

   You can type in the name of the device, or use the browser to choose from a list of available devices.
6. Click **Update Pano Device**.

To change to a single monitor configuration, simply edit the properties of the primary Pano device and delete the information in the Secondary Monitor field.

Manually Add Pano Devices

If you enabled one of the following automatic discovery methods during setup, Pano Device discovery automatically discovers and adds the Pano devices to your Pano Manager:

- (Broadcast/Probe Method) Set Up Pano Device Discovery
- (DHCP Method) Set Up Pano Device Discovery

If you do not enable one of theses discovery methods, then you need to manually add Pano devices. Pano Logic recommends that you use a discovery method. The only reason to manually add Pano devices is if you have more than one Pano Manager in your environment, and this configuration is very unusual.

To manually add a Pano device:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Click **Add**.
4. Type the name you want to use to identify the Pano device. For example, you can enter a user name or the physical location of the Pano device.
5. Type the MAC address of the Pano device.

6. Type the IP address.
7. Click **Add Pano**.

Edit Pano Device Information

There are no restrictions on the Pano device name other than a length limit of 255 characters.

To edit a Pano device:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Select the Pano device from the list.
4. Modify the name, MAC address, or IP address.
5. Click **Update Pano**.

Remove Pano Devices

Any DVM that is assigned to the Pano device that you remove, will remain in tact. If the Pano device is discovered later by any discovered method, the Pano Manager will add the DVM to the inventory.

To remove a Pano device:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Select the Pano device from the list.
4. Click **Remove**.

Default User Login Preferences

Pano devices have a number of default preferences that you can set. These preferences affect display, audio, keyboard and mouse properties. You can change these defaults; however, users can override these defaults when the user logs in their virtual machine.

Default settings are used by Pano devices when they are displaying the Pano client login screen. Default settings are also used when a user has logged in and has not set their personal preferences, which they can do through the Pano Control Panel running within their desktop virtual machine. The end user does not have control over the color quality (bit depth). If you wish to allow users to connect at millions of colors (24 bits), go to "Configure Pano DAS for 24-bit Color" on page 103.

Note: In a kiosk configuration, if one user changes the preferences, the changes are applied to all users (Automatic Login collection type).

• Display Preferences

The display settings (resolution, colors, refresh rate and power save delay) indicate the preferred settings to be used by a Pano device to drive a video monitor. However, the physical monitor might not support the preferred display settings; in this case, the Pano device queries the monitor for its list of supported settings to get as close as possible to the preferred settings.

Pano device can only query monitors that support EDID. If you use non-EDID monitors, the resolution that the Pano device uses might be lower than expected. As outlined in "Set Screen Resolution Settings for Specific DVMs" on page 96 and "Set Power Save Settings for Specific DVMs" on page 96, end-users can set these preferences through the Pano Control Panel.

• Audio Preferences

The audio preferences can be set by the administrator to control the volume of the internal speaker and the volume of the external audio jack. As outlined in "Set Audio Settings for Specific DVMs" on page 92, end-users can set these values individually to suit their personal preference through the Pano Control Panel running.

• Keyboard Preferences

The keyboard repeat delay indicates how long the user needs to hold down a key before it starts to automatically repeat. The keyboard repeat rate determines how quickly the key repeats when it is held down. As outlined in "Set Keyboard Settings for Specific DVMs" on page 92, end-users can set these preferences through the Pano Control Panel.

• Mouse Preferences

The mouse pointer speed determines how far the screen cursor moves on screen relative to the movement of the physical mouse.

• Locale

You can configure Pano devices to use a specific language for keyboard input. Also, Pano devices use the language preference when they display the Pano client login screen. To specify a language, go to "Set Language Preference for Pano Client Login Screen" on page 94.

Next Step(s): If you're performing this task as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 to determine the next step.

Set Keyboard Settings for Specific DVMs

If you need to configure an individual end-user's keyboard settings, you can do so from the user's DVM, using the Pano Control Panel.

To set keyboard settings:

1. Open the Pano CP by either clicking the icon on your taskbar or navigating to it by selecting **Start** > **Programs** > **Pano Desktop Additions** > **Pano Control Panel**.
2. Change the speed of the keyboard:
   a. Click on the **Keyboard** tab.
   b. Use the Keyboard Settings slider to specify your Repeat delay and Repeat rate settings.
3. Click **Apply**.

Troubleshooting: Go to "Troubleshoot Monitor, Mouse, and Keyboard Problems" on page 157.

Set Audio Settings for Specific DVMs

If you need to configure an individual end-user's audio settings, you can do so from the user's DVM, using the Pano Control Panel.

To set audio settings:

1. Open the Pano CP by either clicking the icon on your taskbar or navigating to it by selecting **Start** > **Programs** > **Pano Desktop Additions** > **Pano Control Panel**.
2. Change the speed of the mouse:
   a. Click on the **Audio** tab.
   a. Use the related sliders to define the following settings:
      - Master. The Master Volume.
      - Internal Speaker. The internal speaker on the Pano device.
      - Audio Output Jack. The overall volume level for output to either headphones or speakers.
3. Click **Apply**.

Troubleshooting: Go to "Troubleshoot Monitor, Mouse, and Keyboard Problems" on page 157.

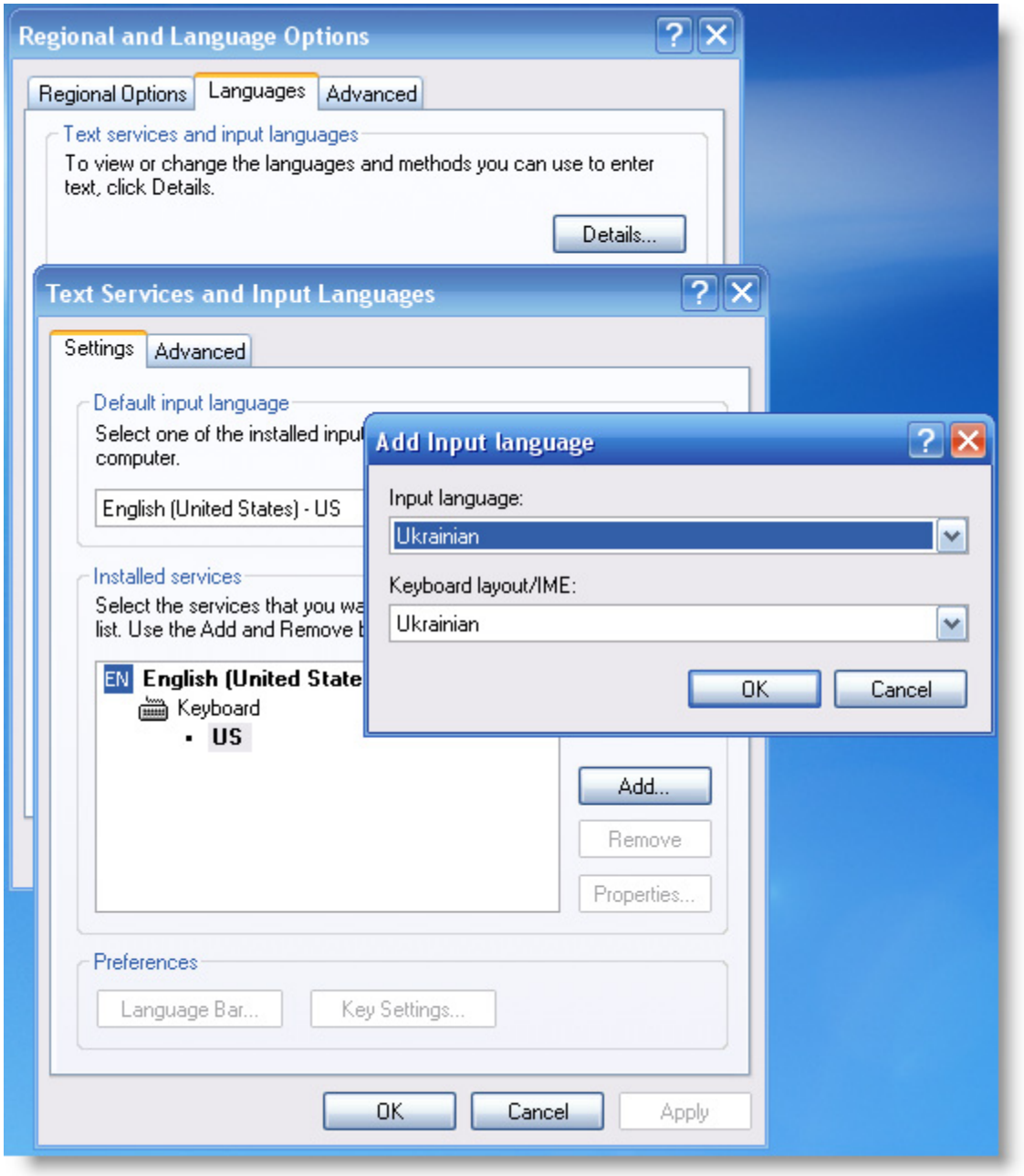
Set Default Keyboard Layout and Input Language for Specific DVMs

If you need to configure an individual end-user's keyboard layout and input language, you can do so from the user's DVM.

To specify a default keyboard layout and input language:

1. Log on to the DVM.
2. Go to **Start** > **Control Panel** > **Regional and Language Options**.
3. Click the **Languages** tab, then the **Details** button.

4. Add your default input language if it has not been added, choose it as the default input language, then click **OK**.



5. In Regional and Language Options, click the **Advanced** tab.
6. In the Default user account settings area, click the **Apply all settings to the current user account and to the default user profile** check box, then click **OK**.
7. Log off the DVM. When the user logs on again, the end-user sees the default language that you specified.

Set Language Preference for Pano Client Login Screen

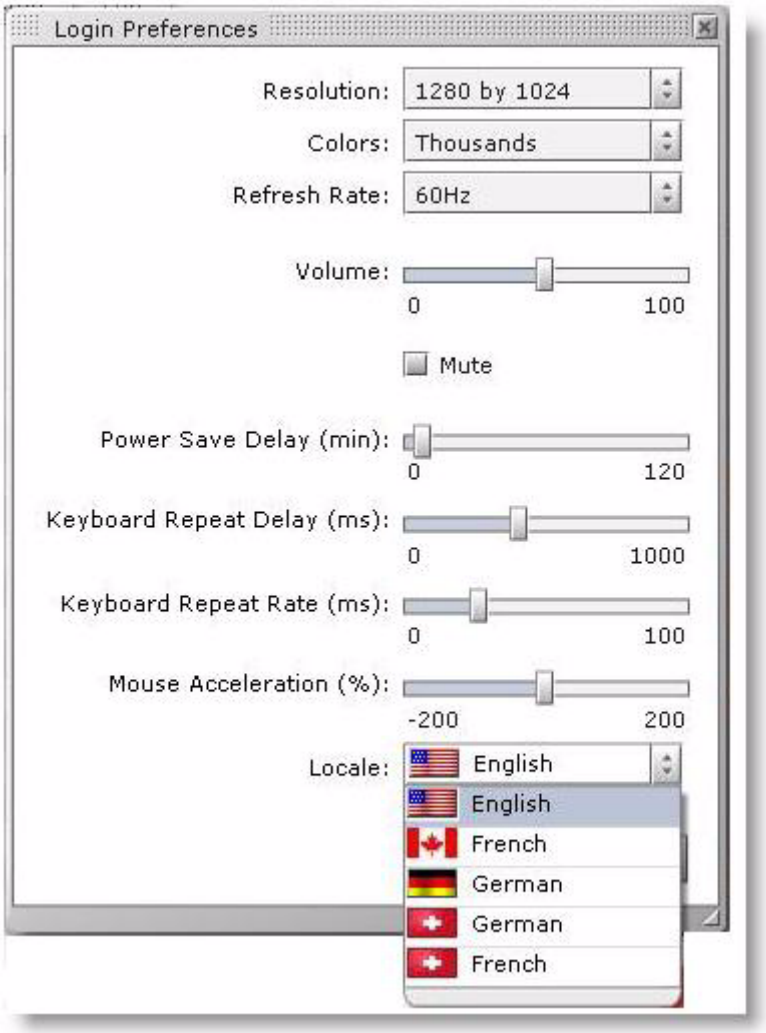
Pano devices use the language preference when they display the Pano client login screen. You can choose one language for all Pano devices. English is the default, but the Pano VDS supports all the following languages.

- English
- UK English
- UK English Extended
- German
- Swiss German
- Swiss French
- Canadian French

To specify a language preference for the Client Login screen:

1. Log on to the Pano Manager.
2. Click on the Pano devices tab.
3. Click on **Settings** button, then choose **Login Preferences…**.

4. In the Locale drop-down list, specify one of the supported languages.



Set Screen Resolution Settings for Specific DVMs

If you need to configure an individual end-user's screen resolution, you can do so from the user's DVM, using the Pano Control Panel.

To change the screen resolution:

1. Open the Pano CP by either clicking the icon on your taskbar or navigating to it by selecting **Start** > **Programs** > **Pano Desktop Additions** > **Pano Control Panel**.
2. Click on the **Display** tab, then change the screen resolution.
3. Click **Apply**.
4. Press the Pano button for the change to take effect. Some changes will not be available until the user's next login/session to the DVM.

Troubleshooting: Go to "Troubleshoot Monitor, Mouse, and Keyboard Problems" on page 157.

Set Power Save Settings for Specific DVMs

If you need to configure an individual end-user's monitor settings, you can do so from the user's DVM, using the Pano Control Panel.

To set the power save option:

1. Open the Pano Control Panel by either clicking the icon on your taskbar or navigating to it by selecting **Start** > **Programs** > **Pano Desktop Additions** > **Pano Control Panel**.
2. Click the **Display** tab.
3. Specify a value for the **Power Save Delay** setting.
4. Click **Apply**.

Troubleshooting: Go to "Troubleshoot Monitor, Mouse, and Keyboard Problems" on page 157.

12
Enable USB Peripheral Support

Install Pano Device USB Support

In general, the decision to enable or disable USB support should be set in the DVM template itself. All DVMs that are created from the template inherit its properties so their USB support will reflect the USB support in the template.

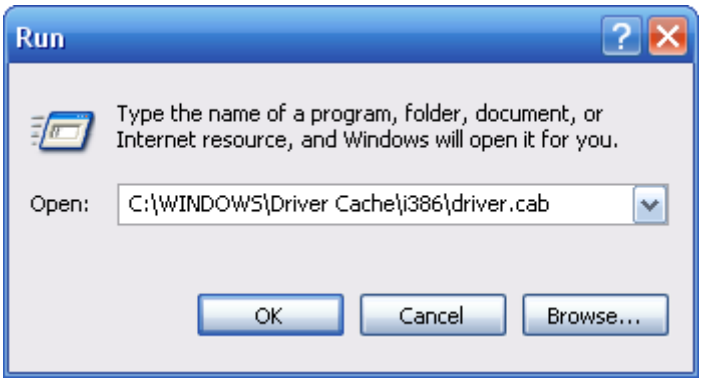
The USBD.SYS file must be present on the DVM template or individual DVMs to enable Pano USB support. This file is part of the Windows XP distribution, but is not installed on virtual machines by default during a Windows XP install. Pano Logic would love to make your life easier by installing this support automatically, but Microsoft doesn't allow this file to be redistributed. Sorry.

(Quick and Easy) To enable support using an existing driver.cab file:

This method is the easiest because it doesn't require that you have your Windows media. However, to use this method, your system must have its driver.cab file.

1. From the Windows Start Menu, select **Run...**.
2. Type the following path to open the Windows cabinet file, then press **Enter**. The driver cabinet file opens.

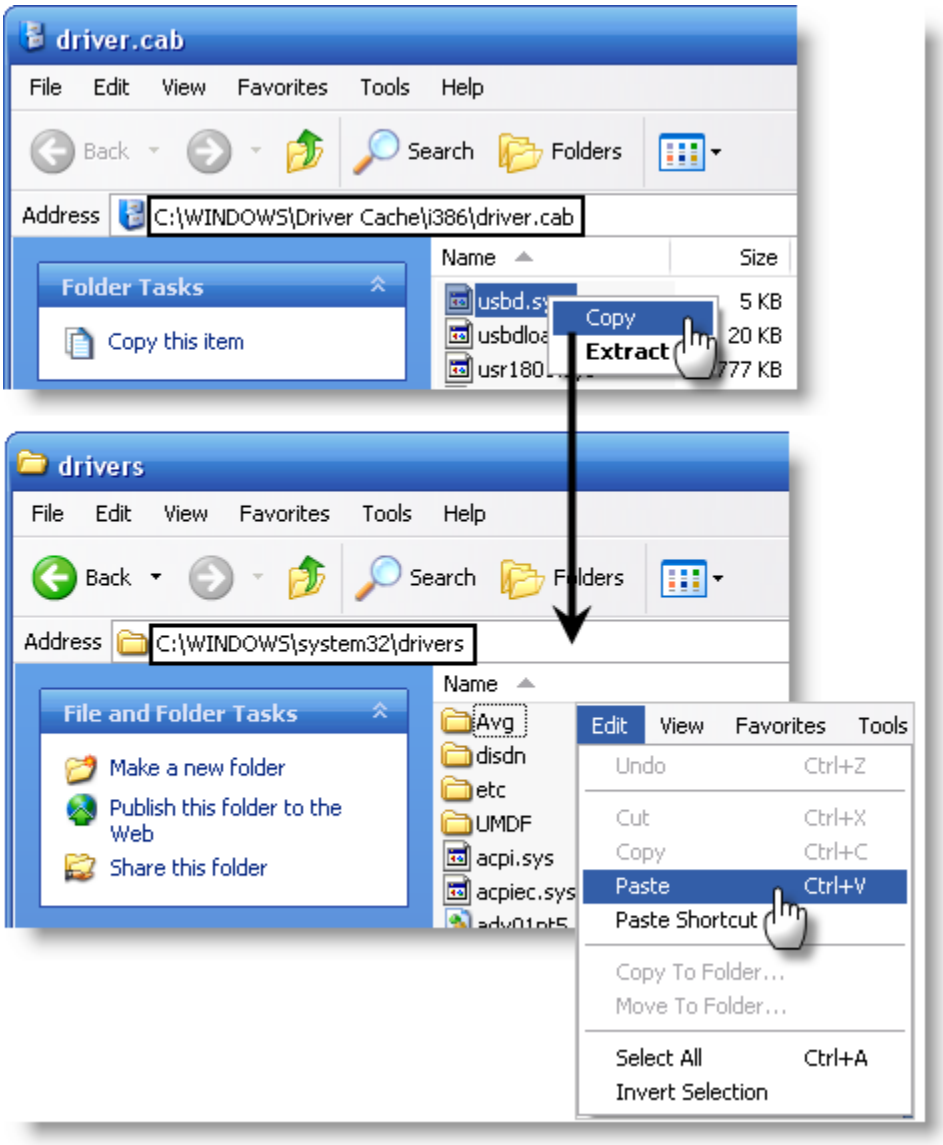
```
C:\WINDOWS\Driver Cache\i386\driver.cab
```



3. Copy the `USBD.SYS` into the your system's `drivers` folder:
   a. Right-click on the `USBD.SYS` file, then choose **Copy**.
   b. In the Windows Explorer address bar, type the following path:

```
C:\WINDOWS\system32\drivers
```

   c. Paste the `USBD.SYS` file into the `drivers` folder.



That's it!

Next Step(s): If you were in the process of installing Pano DAS, return to "Install Pano DAS" on page 71.

To enable USB support using Windows media:

This method requires that you have your Windows media. Perform this procedure on individual DVMs or the template that you use to clone DVMs.

1. Retrieve the USBD.SYS file from the Windows XP disk.
2. Manually copy and expand this file to the proper location on your virtual machine. You only need to perform this step the first time you configure a virtual machine or template to use USB devices.
   a. Connect the Windows XP Service Pack 2 CD (.iso image) to the CD drive by editing the virtual machine settings in VMware VirtualCenter.
   b. From a command prompt and assuming your virtual machine CD drive is on D: and your virtual machine hard drive is on C:, open a command prompt window and type the following commands:

```
C:> cd windows\system32\drivers
C: \windows\system32\drivers> copy d:\i386\usbd.sy_ .
C: \windows\system32\drivers> expand usbd.sy_ usbd.sys
```

That's it!

Next Step(s): If you were in the process of install the Pano DAS, return to "Install Pano DAS" on page 71.

Enable Users To Safely Remove USB Mass Storage Devices

When connecting remotely, Windows XP allows *only administrators* to access the Safely Remove Hardware utility from the system tray. This is the recommended way to remove USB mass storage devices from your Pano device.

To reduce the chance of data corruption, allow your end-users to eject USB drives.

To configure Windows to allow users to eject removable media:

Enabling users to safely remove USB Mass Storage devices is just a matter of assigning the proper permission. Afterward, users can right-click on the USB drive letter icon in Windows Explorer and select **Eject** to gracefully disconnect USB drives.

1. From Windows, click **Start** > **Run**.
2. Type **secpol.msc**, then press **OK**.
3. In the Local Security Settings MMC window, select **Security Settings** > **Local Policies** > **Security Options**.
4. In the right pane, double-click on **Devices: Allowed to format and eject removable media**.
5. On the ensuing dialog box select **Administrators and Interactive Users**, press **OK**, then close the Local Security Settings MMC window.

Next Step(s): (Optional) "Restrict or Allow Use of Specific USB Devices" on page 100.

Restrict or Allow Use of Specific USB Devices

Some companies have departments that work with highly sensitive data (for example, social security numbers). In these types of workplaces, it's important to restrict the use of specific USB devices in order to protect against that data being copied to USB devices. The easier it is for users to copy data to such devices, the harder it is to ensure that the data does not leave the premises.

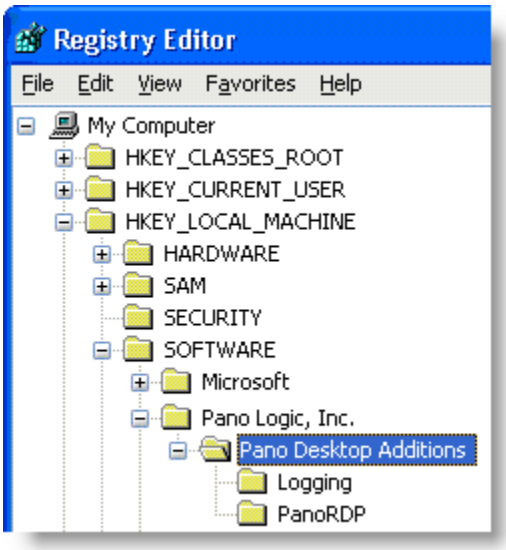
Restricting and allowing the use of USB devices is controlled by USB Filters, which are enabled from the DVM's registry. Simply set the USB Filter String in the DVM's registry settings. The default value for this setting is `255`, which means that all USB devices are allowed. However, you can change the default USB filtering behavior.

Warning: If you use Registry Editor incorrectly, you may cause serious problems that might require you to reinstall your operating system. Neither Pano Logic nor Microsoft can guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To change the default USB filtering behavior:

After you perform this procedure and the next time your users log on to your DVM through a Pano device, they can only use USB peripherals that are specified by the USB filter string value.

1. Launch the Registry Editor.
   a. From Windows, click **Start** > **Run**.
   b. Type **regedit**, then click **OK**.
2. Navigate to `HKEY_LOCAL_MACHINE\Software\Pano Logic, Inc.\Pano Desktop Additions`.



3. If a string value named `USB Filter` does not already exist in the key-value right-hand pane, create it:
   a. In the left-hand pane, right-click on the **Pano Desktop Additions** key, then select **New** > **String Value**.

b. Modify the string value, setting entry in the Value data field to your desired value. The table below lists the possible values and the resulting policy.

If USB Filer value is...	It means...
0	No USB peripherals
1	USB Mass storage only
2	USB Printers only
3	USB Mass storage & Printers only
252	All supported USB peripherals except USB Mass storage & Printers
253	All supported USB peripherals except Printers
254	All supported USB peripherals except USB Mass storage
255	All supported USB peripherals

4. Restart the Pano Desktop Additions service or reboot your DVM.

13 Configure Pano DAS for 24-bit Color

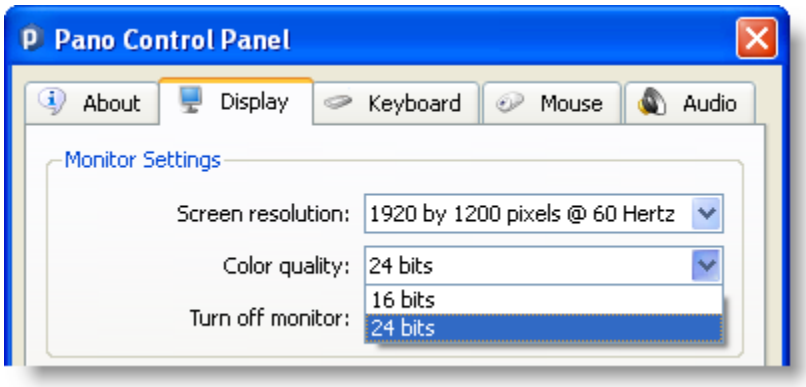
16-bit uses less network bandwidth and gives your users better responsiveness; 24-bit gives richer and smoother color, but is a bit more network intensive.

When connecting to a DVM via Remote Desktop Connection or Pano web access, you must configure the DVM if your users desire 24-bit color depth. To do so, go to "(RDP Connections Only) Configure Pano DAS for 24-bit Color" on page 32.

When connecting via a Pano device to a DVM with Console Direct, your users can select 16-bit or 24-bit color depth through the Pano Control Panel. No other configuration is required.

To select 24-bit color depth from the Pano Control Panel:

1. From the Pano Control Panel, click the **Display** tab.
2. In the **Color quality** drop-down, choose **24 bits**.



14
Create and Manage DVM Collections

(Overview) Create DVM Collections

Before You Begin: "(Overview) Prepare Desktop Virtual Machines" on page 61

After you prepare for automated provisioning, you're ready to create your DVM collections. Perform the following sequence of tasks:

Task		Go to...
1.	Create Security groups in Active Directory that represent the set of users of the desktop virtual machines. You will specify these Security groups when you create the DVM collections.	Create a New Group
2.	Determine the types of DVM collection(s) that you need.	"Provide Access To DVM Collection" on page 109 "DVM Collections" on page 5
3.	Create a folder structure to help you organize your DVMs.	"Organize DVMs, Templates, Folder in VirtualCenter" on page 107 "DVM Collections" on page 5
4.	Determine if you need device restrictions. If so, and to make things easier for you, add these restrictions after you create the collection.	"Use Cases for Device Restrictions" on page 116
5.	Create the DVM collection	"Assign Pano Devices and Users To DVMs" on page 111

Task	Go to...
6. Assign Pano devices to DVMs	"Assign Pano Devices and Users To DVMs" on page 111
7. Verify that the DVM collection is working properly.	"Verify Newly Created DVMs" on page 115
8. Set up collection with device restrictions, if you didn't do so when you created the collection.	"Set Up Collections with Device Restrictions" on page 117

Next Step(s): If you're performing this workflow as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 determine the next step.

Choose DVM Collection Type

• Pooled Desktops

A Pooled Desktops collection type is most appropriate for a set of users that all use the same set of applications. By using Windows roaming profiles and document redirection, you can allow users of a Pooled Desktops collection type to have some degree of personalization. The size of users' profiles should be kept small in order to keep login times short.

An example where this type of collection may be used is a Call Center environment. All users would have the same configuration for their machines, which are not assigned to them permanently.

• Permanently Assigned Desktops

A Permanently Assigned Desktops collection type is most appropriate for users that can benefit from starting with a standard image, but require the ability to customize their computer or save files locally.

This collection is most commonly used collection type for a typical office environment where the user's PCs were being replaced by Pano devices.

• Existing Desktops

A Existing Desktops collection type is most appropriate when you want to create a one-to-one mapping between a user and a DVM that has been created through some other process other than Pano Manager's automated process. A Existing Desktops collection type should normally have only one virtual machine in it; otherwise, the user connects arbitrarily to one virtual machine in the collection.

This collection is most commonly used if you converted a user's physical machine to a virtual machine using VMware Converter, and you want to permanently assign that virtual machine to that user.

• Automatic Login

An Automatic Login collection type allows you to set up Pano devices and their corresponding DVMs to act like kiosks. Rather than displaying the Pano client login screen, the Pano device automatically connects and logs into the associated DVM using a specified account name and password. In an Automatic Login collection type, the account name and password used is the same for all DVMs in the collection. The account name and password are entered as properties of the DVM collection. The account can be a domain account or a local account. This collection type is best when you wish to create a set of kiosks but do not want the administrative burden of managing multiple accounts and passwords.

• Different Accounts w/ Automatic Login

An Different Accounts w/ Automatic Login collection type allows you to set up Pano devices and their corresponding DVMs to act like kiosks. Rather than displaying the Pano client login screen, the Pano device automatically connects and logs into the associated DVM using a specified account name and password. An Different Accounts w/ Automatic Login collection type relies on a user group that has as its members the individual accounts to be used. The user group and the individual accounts must exist in the directory service; local accounts are not supported. This collection type is best when you wish to create a set of kiosks and want to have a unique user name and password for each DVM.

• Windows Login

A Windows Login collection type allows you to set up a Pano device and a corresponding DVM to act like a general purpose Windows computer. Rather than displaying the Pano client login screen, the Pano device automatically connects to the DVM but does not login. The user must authenticate to Windows prior to using the DVM. This sort of collection is useful if you require users to use biometric devices (for example, fingerprint scanner to support fingerprint recognition) for authentication.

Next Step(s): Based on the collections that you chose, create a hierarchy for them. Go to "Organize DVMs, Templates, Folder in VirtualCenter" on page 107.

Organize DVMs, Templates, Folder in VirtualCenter

VirtualCenter provides the Virtual Machines & Templates view to help you organize and manage virtual machines. DVM collections rely on this folder organization. For instance, when you configure a DVM collection, you specify a folder that contains the virtual machines. Pano Manager manages all virtual machines that reside in the specified folder.

To organize DVMs, templates, and folders in VirtualCenter:

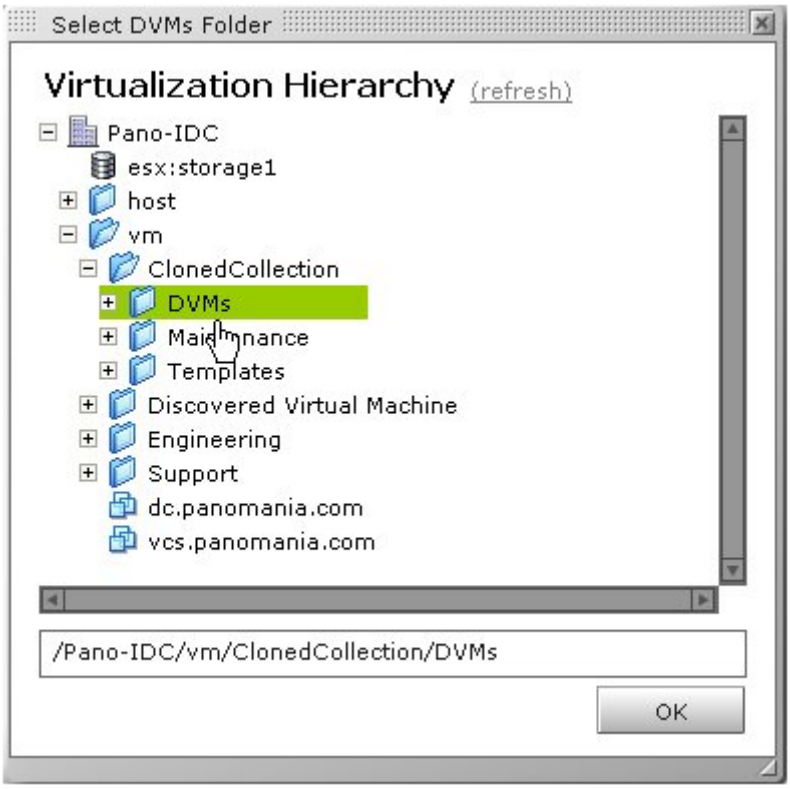
The following example illustrates a best practice.

1. Open your VMware Infrastructure Client and connect to your VirtualCenter Server.
2. Make sure your view in the left hand pane is that of Virtual Machines And Templates by clicking on the Inventory button at the top of the client application window or by pressing Ctrl+Shif+V on your keyboard.
3. Right-click on the Data Center where you want to create your folder hierarchy or alternately select the data center and type Ctrl+F to create the root or base folder for your folder structure.

   You can name the first of these folders Pano Logic or whatever name is logical for your company. Sometimes there is a preference to name them by department, for instance Accounting, Engineering, and so on.
4. Right click the base folder, and do the following:
   a. Create a top level folder with the same name as the DVM collection.
   b. Create a sub-folder called `Templates`. This folder will contain the template (sometimes called Master Copy or Golden Copy) for this DVM collection, the blueprints of the actual instances of the virtual machines from which you can create DVMs.
   c. Create a sub-folder called `DVMs`. This folder will contain all active DVMs, the actual instances of the desktop virtual machines that serve as the virtual user desktops.
   d. Create a sub-folder called `Maintenance`. This folder will contain DVMs that you take out of service while performing maintenance (patching, upgrades, etc) tasks or debugging on them. The Pano Manager does not manage the DVMs in this folder. Once you have

completed any special tasks on the DVM and wish to once again enable it for usage from a Pano device simply drag that DVM back into the DVM folder.

e. Create a sub-folder called `Old DVMs` for use in refreshing a DVM collection (not shown in example).



Next Step(s): "Assign Pano Devices and Users To DVMs" on page 111

Create DVM Collections

To create a DVM collection:

Before You Begin: Determine the DVM types that you want. Go to "DVM Collections" on page 5.

1. Log on to the Pano Manager.
2. Click the DVM Collections tab. If you have never created a DVM Collection, no DVM Collections appear in the table.
3. Click **Add**. The Add DVM Collection window appears.
4. Define collection type.
5. Provide access to DVM collection.
6. Configure for DVM deployment.
7. Configure extra desktops and power state.
8. Configure for user control of desktops.
9. Click **Add DVM Collection**. Pano Manager uses VMware VirtualCenter APIs to create the DVM collection and starts cloning a DVM that belongs to this collection. After a few minutes, the new DVM appears in the table.

Next Step(s): "Assign Pano Devices and Users To DVMs" on page 111

Define Collection Type

1. Log on to the Pano Manager.
2. Click the DVM Collections tab. If you have never created a DVM Collection, no DVM Collections appear in the table.
3. Click **Add**. The Add DVM Collection window appears.
4. Choose the **Type** for the DVM collection. Different collection types are subsequently displayed depending on the type you select.
5. Type a **Name** for the DVM collection.

   For all collections except a Existing Desktops collection type, this name is used to generate the name for DVMs that are automatically provisioned. An alphanumeric ID is appended to the root to generate a unique name for each DVM.
6. Specify the **DVMs Folder**. Browse to find the VirtualCenter folder that contains the DVMs for this collection. Select the folder, and then click **OK**.

   If you organized your DVMs as outlined in "Organize DVMs, Templates, Folder in VirtualCenter" on page 107, then the folder name is `DVMs`.

Provide Access To DVM Collection

You need to select the credentials for automatic logon to the DVMs.

To provide access to the collection:

1. Log on to the Pano Manager.

2. Click the DVM Collections tab. If you have never created a DVM Collection, no DVM Collections appear in the table.
3. Click **Add**. The Add DVM Collection window appears.
4. Specify the **Users**. Click the browse button (…) to find the directory objects to which you want to give access to the DVM collection. You can select security groups, users and organizational units (OU). Select the object(s), and then click **OK**. You may want to type in the name directly in the Users: field, especially if you have a large number of directory objects.
   - If Automatic Login collection type, specify the account to use for automatic logon. If you are using a local account, type the name of the account into the field (for example, `localuser01`). If you are using a domain account, type the name of the account into the field or use the browser to select a user (for example, `kioskuser01@domain.com`).
   - If Different Accounts w/ Automatic Login collection type, specify the user group that contains the accounts to be used for automatic logon. You can type the name of the group (for example, `kioskgroup@domain.com`) or you can use the browser and select the group from the directory hierarchy.
5. Specify the **Password**.

   If you chose Automatic Login collection type, specify the password of the account used to automatically log on to Windows. Otherwise, leave blank.
6. Specify a **Device Restriction**(s).

   This parameter is used with any collection type to specify the set of devices that are allowed to access this collection. For more information, go to "Use Cases for Device Restrictions" on page 116 and "Set Up Collections with Device Restrictions" on page 117.
   - If Automatic Login collection type or Different Accounts w/ Automatic Login collection type, leave this field blank.
   - Otherwise, if you want to allow a user to access the collection from any Pano device, or if you want to restrict access, enter a search string (for example, `PanoFirstFloor`*) that matches the names of the Pano devices that must be used to access this collection.

Configure for DVM Deployment

To configure for DVM deployment:

1. Log on to the Pano Manager.
2. Click the DVM Collections tab. If you have never created a DVM Collection, no DVM Collections appear in the table.
3. Click **Add**. The Add DVM Collection window appears.
4. Specify the following parameters:
   - **DVM Template** - (Pooled Desktops collection type or Permanently Assigned Desktops collection type) Browse to find the DVM template you want to use to configure new DVMs that are added to the collection. Select the template, and then click **OK**. You created this template in "(Overview) Prepare Desktop Virtual Machines" on page 61.
   - **DVM Customization**: (Pooled Desktops collection type or Permanently Assigned Desktops collection type) - Browse to find the DVM customization script you want to use to customize new DVMs that are added to the collection. You created this script in "(Overview) Prepare Desktop Virtual Machines" on page 61.
   - **Resource Pool** - Select the resource pool(s) from which CPU and memory resources should be allocated for new DVMs. For more information, go to "Deploy Resources" on page 116.

- **Datastore** - Select the datastores on which you want DVMs to be created. For more information, go to "Deploy Resources" on page 116.
- **Deploy Enabled** - When checked, automated provisioning of new DVMs is enabled. When unchecked, the Pano Manager does not automatically deploy the new DVMs. For more information, go to "Automated Provisioning" on page 11.

Configure Extra Desktops and Power State

To configure extra desktops and power state:

1. Log on to the Pano Manager.
2. Click the DVM Collections tab. If you have never created a DVM Collection, no DVM Collections appear in the table.
3. Click **Add**. The Add DVM Collection window appears.
4. Specify the following parameters:
   - **Extra Powered On** - Enter the number of unassigned DVMs that should be pre-provisioned and powered on. As DVMs are assigned, the system powers on or creates another to take its place in order to maintain this number of extras. For more information, go to "Automated Deployment" on page 9 and "DVM Power Management" on page 9.
   - **Extra Powered Off** - Enter the number of unassigned DVMs that should be pre-provisioned and powered off. As DVMs are assigned, the system creates another to take its place in order to maintain this number of extras. For more information, go to "Automated Deployment" on page 9 and "DVM Power Management" on page 9.
   - **Power Off Enabled** - When checked, the Pano Manager automatically powers off DVMs that are not needed. For information about how Pano Manager manages power states, go to "DVM Power Management" on page 9.

Configure for User Control of Desktops

To configure for user control of desktops:

1. Log on to the Pano Manager.
2. Click the DVM Collections tab. If you have never created a DVM Collection, no DVM Collections appear in the table.
3. Click **Add**. The Add DVM Collection window appears.
4. Specify the following parameters:
   - **Trash Enabled** - When checked, users are able to have their DVM moved to a trash folder and can then be assigned a new DVM. This feature is only applicable to a Permanently Assigned Desktops collection type.
   - **Login Enabled** - When checked, users that are entitled to the collection are allowed to log on. However, when unchecked, new logins from a Pano device or the Pano web client are not allowed.

Assign Pano Devices and Users To DVMs

You can assign either Pano devices or users to DVMs. The assignment type that you need depends on the DVM collection to which the DVM belongs:

- Assign users to DVMs – DVMs that belong to User Based collections (for example, a Permanently Assigned Desktops collection type) must be assigned to users. After assignment, a lock icon appears in the DVMs tab next to the username. Assignments to DVMs managed by

VMware View cannot be made through the Pano Manager. Such DVMs should be assigned to users through the VMware View product.

- Assign Pano devices to DVMs – DVMs that belong to Device Based collections (for example, an Automatic Login collection type) must be assigned to Pano devices. After assignment, a lock appears in the DVMs tab next to the Pano devices.

User Membership Rules

A user can belong to more than one collection of a User Based collection and/or different User Based collections.

User belongs to more than one collection User Based collection. The Pano Manager provides the DVM from first collection that has the user as a member by searching the collections in the following order:

- Existing Desktops
- Permanently Assigned Desktops
- Pooled Desktops
- VMware VDM

User belongs to more than one collection of the same collection type. When a user logs on to the Pano VDS, the Pano Manager sorts all the collections of the same type that has the user as a member in descending alphabetic order (A-Z). The DVM from the first collection in the order that the list is provided.

Assign Users To DVMs in User Based Collections

Let's discuss a process known as *auto-assignment*. When a user with membership to a collection logs on to the Pano VDS, the Pano Manager auto-assigns the user to an available DVM based on the membership rules. If there are no DVMs, and the collection is configured for deployment, then Pano Manager creates a new DVM and auto-assigns it to the user.

The assigned user displays in the Assigned User column on the same row as the DVM and an padlock icon appears next to the user name.

To assign a user to a DVM from Pano Manager:

Perform the following steps for each DVM.

1. Log on to the Pano Manager.
2. Click the DVMs tab.
3. Select the desired DVM from the list, then click **Assign**.
4. Select the desired user from the list, click **Assign**.
5. Click **OK**.

   The assigned user displays in the Assigned User column on the same row as the DVM, and a padlock icon appears next to the user name.

Next Step(s): "Verify Newly Created DVMs" on page 115

Assign Pano Devices To DVMs

Let's discuss a process known as *auto-assignment*. To auto-assign a Pano device to an available DVM, log on to the Pano VDS. With the account specified in the Device Based collection, the Pano Manager auto-assigns the Pano device to an available DVM. If there are no DVMs, and the collection is configured for deployment, the Pano Manager creates a new DVM and auto-assigns it to the Pano device. Upon assignment a lock icon appears next to the Pano device in the Client column in the Pano Manager.

To assign a Pano device to a DVM from Pano Manager:

Perform the following steps for each DVM.

1. Log on to the Pano Manager.
2. Click the DVMs tab.
3. Select the desired DVM from the list, then click **Assign**.
4. For Windows Login and Automatic Login, select the desired Pano device from the list
5. For Different Accounts w/ Automatic Login, do the following:
   a. In the Pano Device field, select the Pano device.
   b. In the User field, specify the user account to be used for automatic login. The user account must be a member of the user group that was specified when the collection was created.
   c. In the Password field, type the password for the user account.
   d. Select the desired Pano device from the list.
6. Click **OK**.

   The assigned Pano device name displays in the Client column on the same row as the DVM, and a padlock icon appears next to the name of the Pano device.

Next Step(s): "Verify Newly Created DVMs" on page 115

Verify Newly Created DVMs

The key aspects of verifying a newly created DVM includes ensuring that the DVM appears in the Pano Manager, and that the Pano DAS is running.

To verify a newly created DVM:

1. Log on to the Pano Manager.
2. Click the **DVM tab**, verify that everything looks okay.

	Verify...	Field/Value
☐	The DVM appears in the table.	**Virtual Machine Name**
☐	The DMV is powered on.	**DVM State** indicates `PoweredOn`
☐	The DVM has an IP address that was acquired using DHCP	**IP Address** and **DNS Name** have appropriate values
☐	The Pano Desktop Service (Pano DAS) is running and responding to status check messages from Pano Manager.	**DAS Status** indicates `Responding`
☐	The version of Pano DAS appears, and is the expected version.	**DAS Version**
☐	The desktop virtual machine shows a user in the field, if you created User Based Collections. If not, that's because you forgot to add users. You can do so now. Go to Assign Pano Devices and Users To DVMs.	**Assigned User**
☐	The desktop virtual machine shows a user logged on. If not, log on using that user's DVM to ensure that you can connect.	**Logged In User**
☐	The desktop virtual machine shows clients connected, if you created Device Based Collections. If not, no Pano device is connected to this DVM. Connect via a Pano device to make sure it's working.	**Client**

3. Click the **Pano device tab**, and verify that everything looks okay.

	Verify...	Field/Value
☐	The login screen is being displayed on the monitor that is connected to the Pano device.	**Connection** indicates DVM or Pano device is connected to a DVM
☐	The Pano device has a MAC address and IP address	**MAC Address** and **IP Address**
☐	The Pano device is assigned to the DVM.	**Assignment**

Deploy Resources

You can optionally constrain the resource pools and datastores that the Pano Manager can use when it deploys DVMs. These features are only supported when using VirtualCenter 2.x.

If you do not specify a set of resource pools to use, then Pano Manager uses all root resource pools. If you do not specify a set of datastores to use, then Pano Manager uses all datastores.

When there are multiple resource pools, the Pano Manager selects the resource pool with the most unreserved CPU. When there are multiple datastores accessible from the selected resource pool, the Pano Manager selects the datastore with the most free space.

VirtualCenter requires a datastore to be specified even when using a resource pool that is part of a cluster. In that case, you should specify the SAN/NAS datastore that should be used. If you do not, then the Pano Manager chooses the largest datastore in the cluster. If that datastore is local to a single host, then Pano Manager uses only that host within the cluster.

Always specify the correct resource requirements for templates. If you do not, hosts can be over-provisioned and your DVMs will perform poorly.

The Pano Manager keeps at least 512MB of memory free in a resource pool. This avoids problems with VirtualCenter where it may complete deployment, but not have enough memory to power on the DVM.

• Example 1

Single Host Dedicated to Pano - do not specify resource pools or datastores.

• Example 2

Multiple Hosts Dedicated to Pano - do not specify resource pools or datastores. The Pano Manager automatically distributes the DVMs across all hosts.

• Example 3

Multiple Hosts shared with Pano and other applications - create a resource pool within a cluster for Pano use. Specify the Pano resource pool and the appropriate SAN/NAS datastore.

Log Messages for Resource Deployment

When deployment fails due to unavailable resources a message is written to the Pano Manager log, indicating the resources that should be checked for each resource pool. To retrieve these log messages, go to "Work with Log Files" on page 163.

Use Cases for Device Restrictions

Device restrictions can be used with either Device Based Collections or User Based Collections. However, the use cases are slightly different.

• Device Restrictions for User Based Collections

Combining a User Based collection model (i.e. Pooled Desktops collection type, Permanently Assigned Desktops collection type or Existing Desktops collection type) with device restrictions is useful, particularly if you want to allow users to roam only within a subset of your overall environment. A good example of such a use case is within a hospital that must restrict access to patient records based on the physical location of the user (a nurse) and the patient.

In this simple scenario, a hospital may want to implement a policy that allows nurses to access only records from patients on the same floor as the nurse. Within that floor, the nurse should be

free to roam among multiple Pano devices; but if the nurse moves to a different floor, she should no longer access information from the previous floor.

Such a policy can be supported by creating a separate Pooled Desktops collection type for each floor of the hospital. Nurses can be entitled to use some or all of these collections. In addition, the administrator can specify that DVMs in the collection can only be accessed from a specified set of Pano devices.

The result is that a nurse who uses a Pano device on floor 2 will be assigned to a DVM from the collection that corresponds to floor 2. The administrator needs to have configured the DVMs within the collection to access only the authorized data. This is done using a 3rd party access management solution.

A device restriction is a property of the collection, not the device. While device restrictions limit the devices from which a specified collection can be accessed, it does not limit the collections to which the device may potentially connect.

"Set Up Collections with Device Restrictions" on page 117 outlines the steps to follow when setting up a configuration that utilizes a User Based collection with the device restrictions feature.

• Device Restrictions for Device Based Collections

Set device restrictions for Device Based collections if you wanted to prevent a user from inadvertently establishing an assignment between a device and a Device Based collection.

Let's assume you created an Automatic Login collection type. One way to assign a device to such a collection is to log on to an unassigned Pano device using the credentials of the specified user. If you have setup device restrictions as part of the collection properly, you can prevent someone from logging on to the collection and establishing the assignment with an unauthorized device.

Set Up Collections with Device Restrictions

Device Restrictions identify the devices that are allowed to access the collection. You can specify device restrictions for any collection type.

- To learn about these collection types, go to "Assign Pano Devices and Users To DVMs" on page 111
- To understand the use cases for device restrictions, go to "Use Cases for Device Restrictions" on page 116.

To implement device restrictions:

The easiest way to implement device restrictions is to use a naming convention for your Pano devices.

1. Rename your Pano devices so that they use a naming convention that represents how you intend to apply device restrictions. To learn how to edit the name of a Pano device, go to "Edit Pano Device Information" on page 90.

   Example:

   If you want to restrict access from the Pano devices on the 1st floor to a given collection, then rename all such Pano devices that are physically installed on the 1st floor to something like `PanoFirstFloor01`, `PanoFirstFloor02`, `PanoFirstFloor03`, etc.

2. For the collection, specify your naming convention as a search string in the Device Restrictions field. Continuing the same example, enter `PanoFirstFloor*` as the search string.
   - To create a collection, go to "Assign Pano Devices and Users To DVMs" on page 111.
   - To edit an existing collection, go to "Manage DVM Collections" on page 118.

If you add new Pano devices to your network and you want them to access the restricted collection, make sure to edit the name of the Pano device. Similarly, if you change the physical location of the Pano device and no longer want it used to access the restricted collection, change the name of the Pano device.

Next Step(s): If you're performing this task as part of a deployment, return to "(Start Here) Deploy Pano VDS" on page 35 determine the next step.

Manage DVM Collections

To edit an existing DVM collection:

1. Log on to the Pano Manager.
2. Click the **DVM Collections** tab.
3. Select the collection in the list, then click **Edit**.
4. Edit the information you provided when you added the collection.
5. Click **Update DVM Collection**. For details about the parameters, go to "Assign Pano Devices and Users To DVMs" on page 111.

To remove a DVM collection:

Removing a DVM collection does not delete the virtual machines from the virtual infrastructure.

1. Log on to the Pano Manager.
2. Click the **DVM Collections** tab.
3. Select the collection in the list, and then click **Remove**.

15
Monitor and Manage DVMs in Pano Manager

Monitor DVM Utilization and State

You can track and monitor the utilization of DVMs within each collection.

To monitor DVM utilization and state:

1. Log on to the Pano Manager.
2. Click on the **DVM Collections** tab.
3. Select a collection from the list. A stacked-bar chart displays the utilization for that collection.
   - Each bar represents a two-hour period, and the height of the bar reflects the total number of DVMs in the collection.
   - Each section of the bar represents the number of DVMs in a particular state:

Bar Color	DVM State	Description
White	Suspended	The DVM is suspended, not powered on, or the Pano DAS is not reachable.
Green	Ready	The DVM is powered on and the Pano DAS is reachable. The DVM is available to be assigned to a user.
Gray	Assigned/idle	The DVM is assigned to a user, but the user is not logged in.
Red	Waiting	The DVM is unavailable when a user attempts to log on.

Monitor DVM Status

To monitor the status of DVMs:

1. Log on to Pano Manager.
2. Click on the DVM Collections tab.
3. In the DAS status column, observe the current status:
   - Unreachable - DVM cannot be reached.
   - Unresponsive - DVM is reachable, but it is not responding.
   - Connected - DVM is connected.
   - Responding - DVM responds.

About User Assignment

You can assign both users to DVMs and Pano devices to DVMs. To learn about Pano device assignment, go to "About Device Assignment" on page 121.

In Pooled Desktops collection type and Permanently Assigned Desktops collection types, users are assigned to a specific DVM. Assignment happens automatically and works differently for a Pooled Desktops collection type and Permanently Assigned Desktops collection type:

• For a Existing Desktops collection type.

Users cannot be assigned to DVMs that are part of a Existing Desktops collection type.

• For a Pooled Desktops collection type.

User is automatically assigned to a DVM each time a new Windows session starts. The assignment lasts until the user logs out of Windows.

If a user merely disconnects from their session, the assignment remains active so that the user can log back in from the same or different Pano device or software client.

• For a Permanently Assigned Desktops collection type.

User is automatically assigned to a specific DVM the first time they access the collection. The initial assignment lasts indefinitely until an administrator manually removes the assignment or the user moves the DVM to the trash as outlined in "Move DVMs To Trash" on page 122.

To assign in advance, go to "Manually Assign Users To DVMs" on page 120.

To remove assignment, go to "Unassign Users from DVMs" on page 121.

Manually Assign Users To DVMs

In some cases you might want to manually assign a user to a specific DVM prior to the user logging on. For instance, you might want to assign a DVM to a new employee before they start work so that you can perform some special customization for that user ahead of time.

To manually assign a user to a DVM:

1. Learn how long assignments lasts. Go to "About User Assignment" on page 120.
2. Log on to the Pano Manager.
3. Click on the **DVM Collections** tab.

4. Select the DVM from the list, then click **Assign**.
5. Select the desired user object from the directory hierarchy. The DVM is now assigned to that user.

Unassign Users from DVMs

To unassign users from DVMs:

1. Learn how long assignments last.
2. Log on to the Pano Manager.
3. Select the DVM from the list, then click **Unassign**. The DVM is now available to be assigned to another user.

About Device Assignment

In Device Based collections (Automatic Login collection type, Windows Login collection type, Different Accounts w/ Automatic Login collection type), devices are assigned to specific DVMs. Assignment happens automatically the first time a user logs on to the DVM or assignment can be done manually through the DVMs tab on the Management User Interface (MUI).

Manually Assign Pano Device To DVMs

A Pano device can only be assigned to one DVM at a time. However, you can assign the same DVM to more than one Pano device.

To manually assign a Pano device to a DVM:

1. Learn how long assignments lasts. Go to “About Device Assignment” on page 121.
2. Log on to the Pano Manager.
3. Select the DVM from the list, and then click **Assign**.
4. Select the desired Pano device from the list.

   The list does not include Pano devices that have already been assigned to DVMs, so if your desired device is not listed you need to unassign it from another DVM first.

Unassign Pano Devices from DVMs

To unassign a Pano device from a DVM:

1. Select the DVM from the list.
2. Click **Unassign**. The DVM is now available to be assigned to another device.

Move DVMs To Trash

Only a user can move a DVM to the Trash. Use this procedure in the event that you need to show a user how to trash the DVM.

Of course, to move a DVM to the Trash the DVM must be assigned to that user. A user might want to do trash the DVM if it becomes unusable (corrupted operating system, virus/malware, etc.).

This operation causes the DVM assigned to the user to be decommissioned and moved to the Trash folder. The Trash folder will be created is a sub-folder under the collection's folder in VirtualCenter if it does not exist.

This operation is only available to users with DVMs in a Permanently Assigned Desktops collection type. After moving a DVM to trash, the user receive a new DVM (cloned from the collection's template) upon the user's next login.

To move a DVM to Trash:

1. Log on to the desktop virtual machine.

Note: The button changes from Help to Options when the user has typed in a username and password.

2. From the Pano client login screen, click on **Options…**.
3. Click **Move to Trash**.

Set Power Save Option for All Pano Devices

When a user is not logged in to the Pano device or hasn't used the device for a period of time, it's common for a user to want to put the screen in to saver mode so that the image of the current view doesn't get burned into the screen.

There is a power save option in the Pano Manager where you can set the time limit. If you want to change these settings for a specific end-user, go to "Set Power Save Settings for Specific DVMs" on page 96.

To set the power save option from the Pano Manager:

1. Log on to the Pano Manager.
2. Click the **Pano Devices** tab.
3. Click the Settings button, then click **Login Preferences**.
4. Specify a value for the **Power Save Delay** setting.

Display Company Logo on Pano Login Screen

Once you specify a logo for the login screen, all DVMs use this login screen. Pano Virtual Desktop Solution preserves your logo during upgrades.

To display your company's logo on the Pano login screen.

1. Prepare a `.png` image file. You will select this file later.
2. Login to the Pano Manager as Administrator.
3. Click on the **Pano Devices** tab.
4. Click the **Settings** drop-down button, then click **Login Image**.
5. Click the **Set Custom Image...** button, select your `.png` file, then click **Refresh**. Your new login screen appears in the Login Image window.

Replace or Reimage DVMs

You might need to replace a user's DVM if it is simply unusable. To do so, simply re-image it. The process sounds difficult, but it's quite easy.

To re-image a DVM:

1. Unassign the user from the DVM. Go to "Unassign Users from DVMs" on page 121.
2. In VirtualCenter, move the DVM to the `Maintenance` folder. You created this folder in "Organize DVMs, Templates, Folder in VirtualCenter" on page 107.
3. Power off the DVM. Go to "Shut Down DVMs" on page 19.
4. Assign a new, unassigned DVM to the user. Go to Assign Pano Devices and Users To DVMs.

   If a spare DVM does not exist in the collection then it should be created by changing the properties of the DVM collection.

   For example, if you set the **Extra DVMs** value to `1` and select the **Deploy Enabled** checkbox, Pano Manager creates a new DVM in the collection.

The user is ready to login to the "new" DVM.

Expand DVM Hard Drives

There are two methods of expanding a drive, and the method you choose depends on the type of drive. Because a DVM's Windows XP operating system resides on the system (boot) drive, it's a lot easier to expand a data drive.

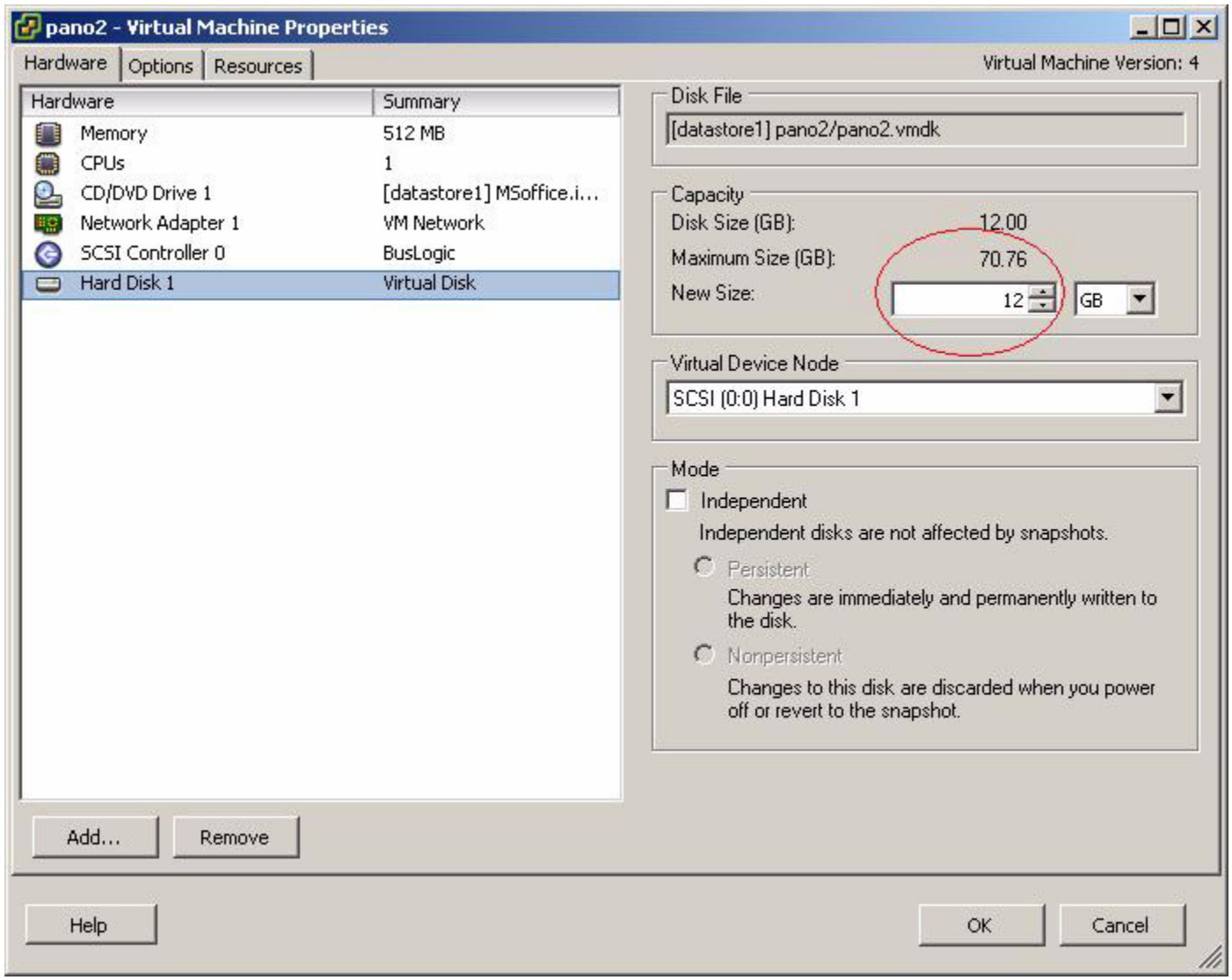
To expand DVM hard drive if the drive is a system drive:

You cannot expand a DVM's system drive from within the DVM while the operating system is running. So, the solution is to add the DVM's system drive to another DVM, then expand it from within that DVM.

Warning: Make sure that you do not have an active snapshot on the DVM. If you expand a virtual disk with a snapshot you *will* cause data corruption.

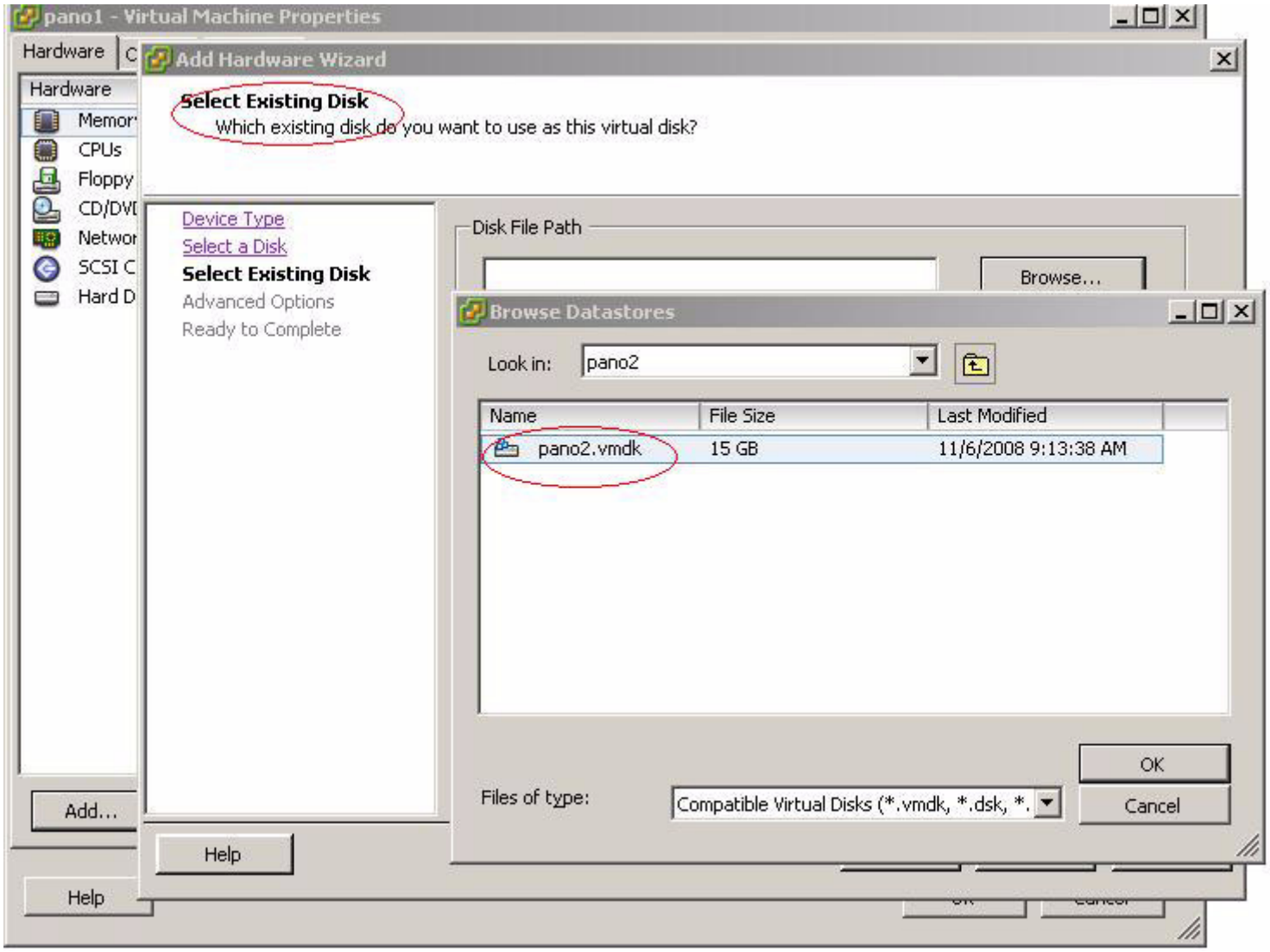
1. Power off the DVM that contains the system drive that you want to expand. Let's call this DVM **Pano2**.
2. Make a backup copy of **Pano2**; after all, this disk contains your user data and things don't always go as planned.
3. Power off **Pano2**.

4. Increase the size of **Pano2**'s virtual disk file. Let's assume 12 GB to 15GB.

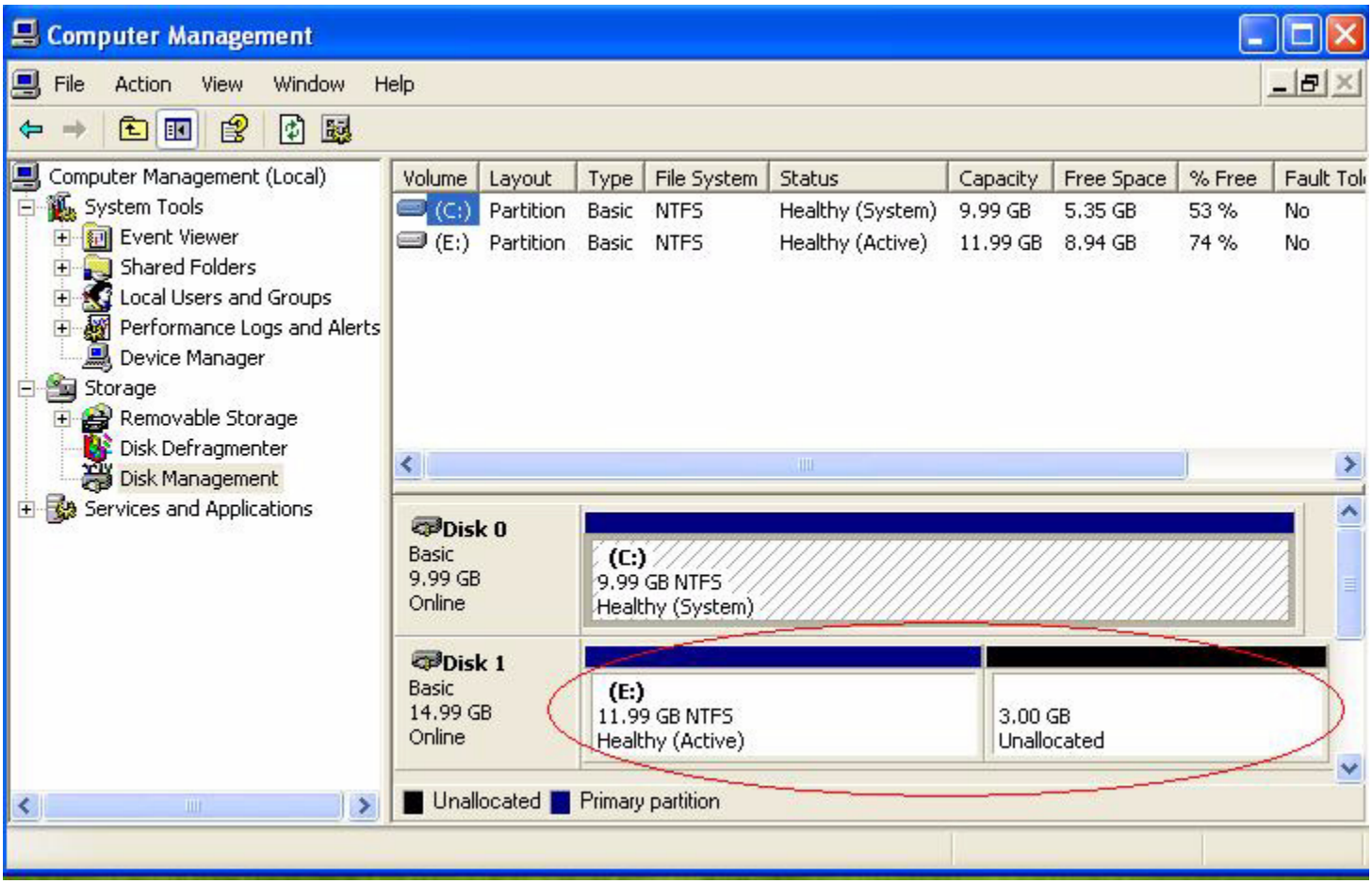


5. Create a temporary Windows XP DVM or use an existing DVM. Let's call this DVM **Pano1**.

6. Power off **Pano1**, then add **Pano2**'s disk to **Pano1**.

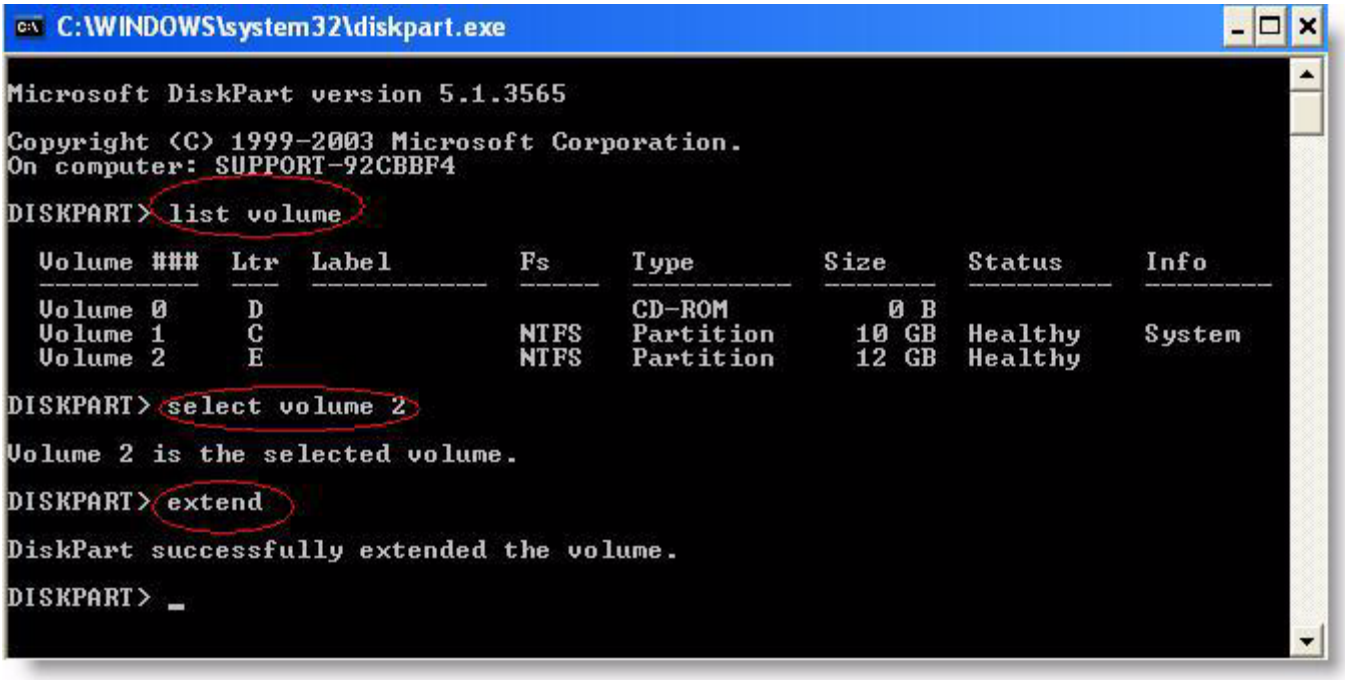


7. Power on **Pano1**, then verify that the imported disk has unallocated space on it.

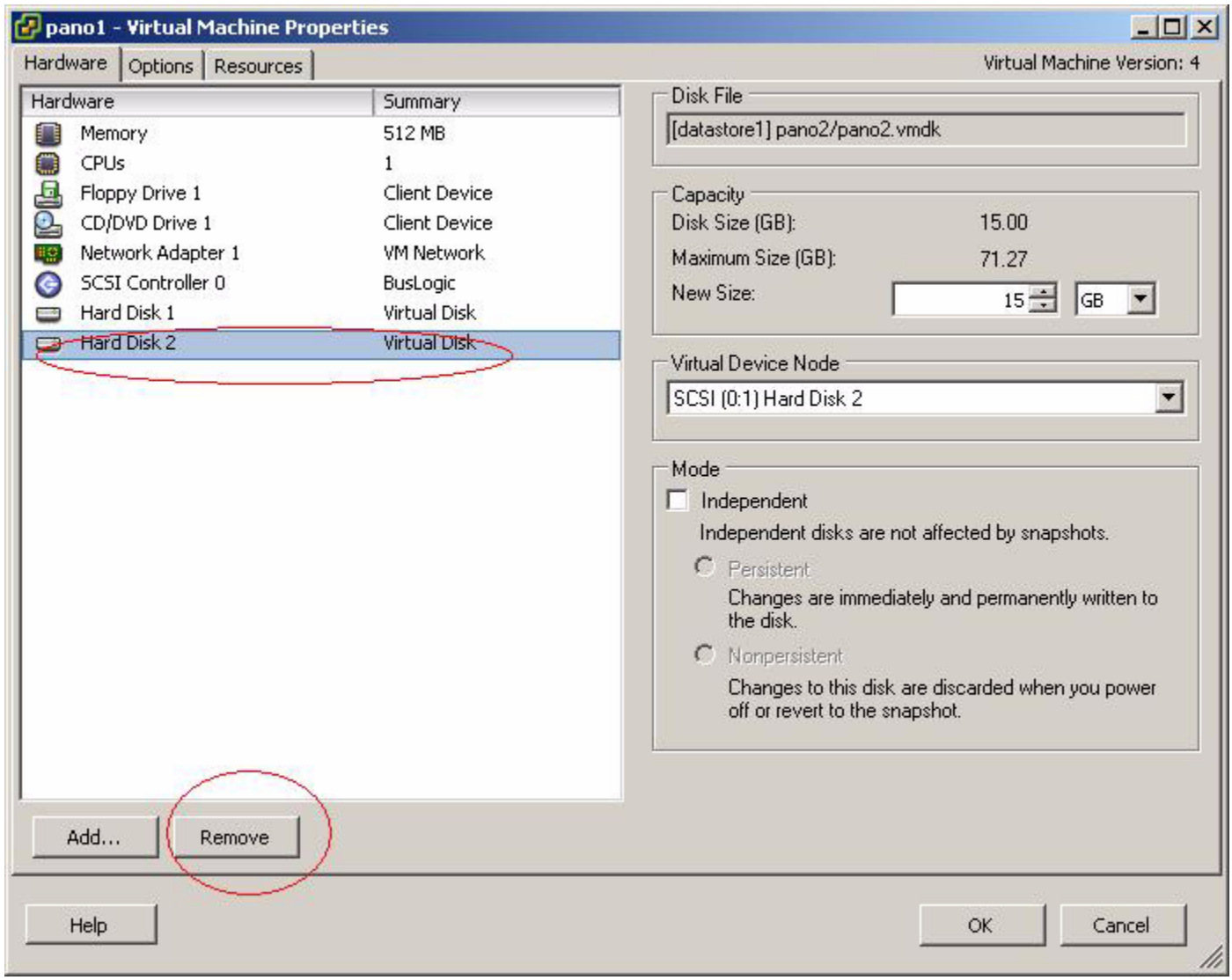


8. From the **Pano1**'s run menu, type **diskpart.exe**, then press Enter. The command line utility that resizes disk partitions launches.

9. From the list of available volumes, select your volume, then run the expand command to expand the volume. Let's assume that you're expanding Drive E, which is volume 2.



10. Power off **Pano1**, then remove the disk from **Pano1**.



11. Power on **Pano2**, and verify your expanded disk drive.

To expand DVM hard drive if the drive is a data drive:

Unlike with a system disk, you can expand a data drive from within the DVM itself. You don't need to use a temporary DVM to expand a data drive.

1. Make a backup copy of the DVM; after all, this disk contains your user data and things don't always go as planned.
2. Power off the DVM.
3. Increase the size of DVM's virtual disk file. Let's assume 12 GB to 15GB.
4. From the DVM's run menu, type **diskpart.exe**, then press Enter. The command line utility that resizes disk partitions launches.
5. From the list of available volumes, select your volume, then run the extend command to expand the volume.
6. Power on the DVM, and verify your expanded disk drive.

16

Refresh Virtual Machines in Pooled Desktops

From time to time, you might may want to update software in the DVMs that belong to a collection. You can use Microsoft Systems Management Server (SMS), Active Directory, or any of the software deployment and management products to do so. For the Pooled Desktops collection type, an easier alternative is also available:

To refresh a Pooled Desktops collection type:

1. Create a new folder in VirtualCenter called `Old DVMs` or similar. (You might already have such a folder if you followed the instructions in "Organize DVMs, Templates, Folder in VirtualCenter" on page 107.)
2. Move all the old DVMs into the `Old DVMs` folder.
3. Update the template used for the Pooled Desktops collection type with the changes. From now on, any new virtual machines that you clone that template will also have these changes.
4. After all users log off the virtual machines that are in the Old DVMs folder, one by one delete the virtual machines in that Old DVMs folder.

17
Integrate Pano VDS with VMware View

Pano Virtual Desktop Solution (Pano VDS) offers a full virtual desktop solution that includes Pano devices and corresponding Pano Desktop Services (Pano DAS), plus the Pano Manager, which acts as a full-featured connection broker.

For customers that choose to use VMware View Manager (formerly known as VMware VDM) or as their connection broker, Pano Logic offers seamless integration. Customers typically choose to run VMware View if they have a very diverse set of client devices such as Pano devices, traditional PCs, and thin clients.

In a mixed device environment, VMware View typically performs connection brokering and automated deployment functions, even though Pano Manager offers these same capabilities. In such a deployment, both the VMware View agent and the Pano DAS run side by side in the same virtual machines. (To learn about Pano Manager's connection broker functionality, go to "Pano Manager" on page 3.)

In this scenario the Pano Manager continues to perform the following functions:

- Discovers and controls Pano devices.
- Collects user credentials and authenticates users through the directory service.
- Queries VMware View for the address of the virtual machine assigned to the user.
- Establishes the connection between the virtual machine and the Pano device.

When Pano Manager is set up with a VMware View, any credentials that users input through the Pano client login screen's are passed to a VMware View. Provisioning of the DVMs is done through VMware View.

In this scenario, the Pano Manager's function is to is to establish the connection between the Pano device and the DVM. Also, the Pano Manager does not communicate with VirtualCenter to start the DVM; rather, VMware View handles these tasks.

In short, Pano devices must be controlled by the Pano Manager, so you can't completely eliminate the Pano Manager.

(Overview) Integrate Pano VDS with VMware View

Before You Begin: Perform all the steps as outlined in "(Start Here) Deploy Pano VDS" on page 35. Integrating Pano VDS with VMware View Manager is simply the last step, and the only step that is different from a Pano device-only environment and a mixed device environment. Everything else is the same, including device discovery and Active Directory integration.

To integrate Pano VDS with VMware View, perform the following sequence of tasks:

Task		Go to...
1.	Install and configure VMware View for use with PCs running the VMware View client.	VMware's Installation and Administration Guide for Virtual Desktop Manager 2.1
2.	Configure the VMware View agent.	"Configure VMware View Agent" on page 134
3.	Enable desktop connections.	"Enable Desktop Connections from Pano Devices" on page 137
4.	Connect the Pano Manager to VMware View.	"Connect Pano Manager To VMware View" on page 137
5.	Create a VMware VDM collection	"Create VMware VDM Collection" on page 137
6.	Validate the configuration	"Validate Pano Manager-VMware View Configuration" on page 139

Configure VMware View Agent

The VMware View agent includes an optional feature called *View Secure Authentication*. If this feature is enabled, the VMware View agent prevents users from accessing the DVM from an RDP client such as Windows Remote Desktop Connection. Enabling this feature also blocks connections from Pano VDS unless you are using Pano DAS v2.5.x with Console Direct™ technology.

• System behavior when View Secure Authentication is enabled

If you choose to enable VDM Secure Authentication you must install the Pano Desktop Service (Pano DAS) before you install the VMware View agent. If you later update the Pano DAS, you must reinstall the VMware View agent. In this mode the VMware View agent must always be installed or updated last.

The following table indicates the methods by which you or your users can access the DVM when View Secure Authentication is enabled:

Client Type	Supported
VMware View client	✓
Remote Desktop Connection	✗
Pano device connecting to Pano DAS v2.5.x–configured for Console Direct technology For information about Console Direct technology, go to Switch Connection Modes.	✓
Pano device connecting to Pano DAS v2.5.1–configured for Pano Classic. For information about Console Direct technology, go to Switch Connection Modes.	✗
Pano device connecting to Pano DAS v2.0.x or earlier	✗
Pano web access	✗
VMware Infrastructure Client (VMware VIC) [1]	✓
SMS Remote Control or Dameware Mini Remote Control	✓

Table 17.1 DVM Access Support: View Secure Authentication–Enabled

1. When View Secure Authentication is enabled and an end user is connected to the DVM via a Pano device using v2.5.1, the VMware VIC displays the Pano lockout screen. In order for an Administrator to access the DVM from the VMware VIC, the user must disconnect from the DVM by pressing the Pano Button. Alternatively, the Administrator can access the DVM via a remote control tool such as SMS Remote Control or Dameware Mini Remote Control.

• System behavior when VDM Secure Authentication is disabled

Note: If you choose to disable View Secure Authentication you can install the Pano DAS and VMware View in any order.

The following table indicates the methods by which you or your users can access the DVM when View Secure Authentication is disabled:

Client Type	Supported
VMware View client	✓
Remote Desktop Connection [1]	✓
Pano device connecting to Pano DAS v2.5.1 [1]	✓
Pano device connecting to Pano DAS v2.0.x or earlier	✓
Pano web access [1]	✓
VMware Infrastructure Client (VMware VIC)	✓
SMS Remote Control or Dameware Mini Remote Control	✓

Table 17.2 DVM Access Support: View Secure Authentication–Disabled

1. When View Secure Authentication is disabled, direct RDP connections are allowed; however, if a user is connected to a DVM via Windows Remote Desktop Connection and attempts to access the same session from a VMware View or a Pano device, the VDM Connection Server does not allow the established connection to be broken and reports that the desktop is unavailable. A user who wishes to roam a session from an RDP-based client must first disconnect before attempting to log on from a different client.

To enable VDM Secure Authentication

View Secure Authentication is selectable when you install the VMware View. In the **Custom Setup Option** step of the VMware View installation wizard, select the View Secure Authentication component.

Next Step(s): Enable Desktop Connections from Pano Devices

To disable VDM Secure Authentication

View Secure Authentication is selectable when you install the VMware View. In the **Custom Setup Option** step of the VMware View installation wizard, deselect the View Secure Authentication component.

Next Step(s): Enable Desktop Connections from Pano Devices

Enable Desktop Connections from Pano Devices

Because of a known issue with VMware View and the new XML API, you must enable a specific VMware View setting to allow desktop connections from a Pano devices.

To enable desktop connections:

Do one of the following:

- (VMware View Manager 3) Select **Direct Connection to desktop** in **View Server Settings**.
- (VMware View Manager 2) Set **Direct Connect to virtual desktop** to `Yes`.

Next Step(s): Connect Pano Manager To VMware View

Connect Pano Manager To VMware View

When connecting a user session from a Pano device to a virtual machine that VMware View manages, the Pano Manager needs to communicate with the VMware View server.

To connect Pano Manager to VMware View:

1. Log on to the Pano Manager.
2. Click the Setup tab.
3. In the **VMware VDM Configuration** area, specify the VMware View server. Type a URL of the following form:

   If the **Require SSL for client connections** setting in **View Server Global Settings** is selected, then you must specify a https URL.

   ```
   https://server_name_or_IP_address
   ```

   Example:

   ```
   https://vdmserver1.panologic.com
   ```

4. Type the user name and password for VMware View account.
5. Click **Configure**.

Next Step(s): “Create VMware VDM Collection” on page 137

Create VMware VDM Collection

The easiest way to configure the system is to create one collection that encompasses all your users; afterward, the Pano Manager relies on VMware View Manager to determine the appropriate mapping of users to DVMs.

To setup a generic collection for all your VMware View users:

1. Log on to the Pano Manager.
2. Click on the **DVM Collections** tab.
3. Click **Add…**.
4. In the Type drop-down list, select **VMWare VDM**.

5. Type a name for the collection.
6. Specify the users. If you specify a group that contains all your users, VMware View determines the specific mapping.
7. Click **Add** DVM Collection.

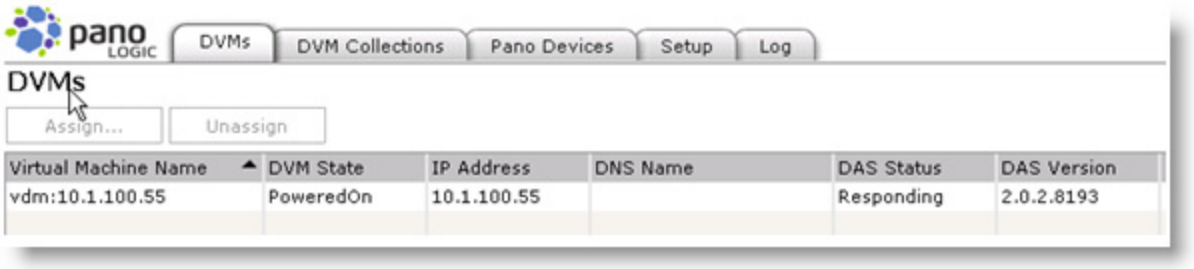
Next Step(s): "Validate Pano Manager-VMware View Configuration" on page 139

Validate Pano Manager-VMware View Configuration

Assuming your VMware View Manager connection broker has DVMs configured, you can validate the configuration.

To validate the configuration:

1. Verify that the Pano Manager shows that the DVMs are powered on and receiving an IP address, and that the Pano DAS is responding.



2. Log on to a DVM from a Pano device.

   After successful authentication, the Pano Manager determines to which collections the user has been assigned. If the user is assigned to multiple collections, the user is mapped according to the following precedence:
   - Existing Desktops collection type
   - Permanently Assigned Desktops collection type
   - Pooled Desktops collection type
   - VMware VDM collection

   Assuming the user has not been assigned to a collection of higher precedence, the Pano Manager queries VMware View to determine the appropriate desktop for the user. Afterward, the Pano Manager connects the Pano device to the desktop specified by VMware View.

18 Optimize DVM Performance

Ways To Optimize DVM Performance

Enabling or disabling specific Windows settings can help you improve DVM performance. The following table provides numerous tips about how to improve performance. If you want more tips, go to Slimming Down Windows XP: The Complete Guide on Bold Fortune Forums.

What	Why	How
Increase ESX Server Service Console memory.	Improves overall DVM performance.	"Increase VMware ESX Server Service Console Memory" on page 145
Limit the amount of memory that PowerPoint consumes.	Improves overall DVM performance.	"Minimize DVM CPU Consumption" on page 146
Configure the behavior of window dragging such that the windows contents doesn't show.	Improves window dragging performance. **Note:** By default, when you move a window the entire contents of the window move.	1. Right-click on the Desktop, then choose **Properties** > **Appearance**. 2. Uncheck **Show windows contents while dragging**.
Disable any unused hardware, such as COM1 and COM2.	Improves overall DVM performance.	Use Microsoft's COMDisable tool.
Turn off theme enhancements.	Improves overall DVM performance.	1. Go to **Start** > **Control Panel** > **Display** > **Themes** tab. 2. Ensure that you're using the Windows XP theme.
Adjust performance settings.	Improves overall DVM performance.	1. From My Computer, click on **View system information**. 2. In the Advanced Tab, go to the Performance section and click **Settings**. 3. Select the **Adjust for best performance** radio button.

What	Why	How
Ensure hardware acceleration is enabled on your video cards.	Improves mouse movement.	For detailed instructions and explanation, go to "Set Hardware Acceleration" on page 71. 1. Right-click the desktop, and then click **Properties**. 2. In the Display Properties dialog box, click the **Settings** tab, and then click the **Advanced** button. 3. Click the **Troubleshoot** tab. 4. Set **Hardware acceleration** to `Full`.
(Vista) Disable mouse scheme.	Improves mouse performance	1. From Vista Control Panel, go to **Mouse** > **Pointers** > **Scheme**. 2. Choose None in the drop-down list.
Delete any hidden update uninstall folders.	Improves overall DVM performance.	Look in `c:\WINDOWS`. Example: $NtUninstallKB893756$.
Disable Indexing Services.	Improves overall DVM performance. **Note:** Indexing improves searches by cataloging files. For users who search a lot, this may be beneficial and should not be disabled.	1. Go to **Start** > **Run**. 2. Type **services.msc** and press Enter. 3. Double-click on Indexing Service icon. 4. If the service status is `Running`, then click the Stop button. 5. In the Startup type: drop-down box, choose **Disabled**.
Disable Indexing of C: drive.	Improves overall DVM performance.	1. Right-click on the C: drive. 2. Click Properties from the context window. 3. Clear the **Allow Indexing Service to index this disk for fast file searching**.
Remove or minimize System Restore points.	Improves overall DVM performance.	1. Go to **Start** > **Control Panel** > **System** > **System Restore**. 2. Turn off System Restore on all drives.

What	Why	How
Disable any unwanted services/drivers	Improves memory and CPU usage. For more tips about additional services that you can disable, go to Black Viper's Service Configuration Guide.	1. (Optional) To get a closer look at the services that are running, try out the AutoRuns utility. 2. Go to **Start** > **Control Panel** > **Administrative Tools** > **Services**. 3. If the unwanted service status is `Started`, double-click on the service, then click the Stop button. 4. In the Startup type: drop-down box, choose **Disabled**. Suggested services that you might want to disable: • Automatic Updates (this can be switched it back on selectively to use Windows Update) • ClipBook • Error Reporting Service • Fast User Switching Compatibility • Help and Support • IMAPI CD Burning Service • NetMeeting Remote Desktop Service • Performance Logs and Alerts • Task Scheduler • Themes • Uninterruptible Power Supply • Windows Audio • Windows Time • Web Client • Wireless Zero Configuration
Run the Disk Cleanup tool.	Improves overall DVM performance.	1. Go to **Start** > **All Programs** > **Accessories** > **System Tools** > **Disk Cleanup**. 2. Select the drive, then click **OK**.
Run the Disk Defragmenter.	Improves overall DVM performance.	1. Go to **Start** > **All Programs** > **Accessories** > **System Tools** > **Disk Defragmenter**. 2. Select the C: drive, then click the Defragmenter button.

What	Why	How
Optimize Startup and Recovery Settings	Improves overall DVM performance.	1. Go to **Advanced** > **Startup and Recovery**. 2. Clear the **Write an event to the system log** check box. 3. Clear the **Send an administrative alert** check box. 4. Clear the **Automatically restart** check box. 5. Clear the **Set Write Debugging Information to None** check box.
Optimize performance settings	Improves overall DVM performance.	Go to Advanced > Performance Settings. • Set Visual effects to a minimum. In Visual Effects tab, select “Adjust for best performance”. • Enable CPU to prioritize programs. In Advanced Tab, select **Adjust for best performance of programs**. • Enable Memory to prioritize programs. In the Advanced tab, select **Adjust for best performance of programs**. • Switch off page file. In the Virtual Memory section of the Advanced Tab, click **Change**. Select **No Paging File** and click **Set**, then **OK**. Restart the virtual machine.
Disable offline files	Improves overall DVM performance.	In the Offline Files tab, clear the **Enable Offline Files** check box.
Disable search from network drives and printers	Improves overall DVM performance.	In the View tab, clear the **Automatically search for network folders and printers** check box.
Turn off power schemes	Improves overall DVM performance.	In the Always On tab, **turn off monitor** and **turn off hard discs** to **Never**.
Turn off hibernation	Improves overall DVM performance.	In the Hibernate tab, clear the Hibernation check box.
Show inactive icons	Improves overall DVM performance.	In the taskbar tab, clear the **Hide Inactive Icons** check box.
Clear the IE cache	Improves overall DVM performance.	In the General tab, click **Delete**, **Delete All**.

What	Why	How
Make a few registry tweaks	Improves overall DVM performance.	• Speed Up Menus. Set HKEY_CURRENT_USER\Control Panel\Desktop\MenuShowDelay to 1. • Disable NTFS Last Access Time Logging (NTFS Only). Add a new DWORD value named NtfsDisableLastAccessUpdate to HKEY_LOCAL_MACHINE\ SYSTEM\ CURRENTCONTROLSET\ CONTROL\FILESYSTEM. Set value to 1. • Disable Balloon tips. Add a new DWORD value, called EnableBalloonTips to HKEY_CURRENT_USER\ Software\Microsoft\Windows\ CurrentVersion\Explorer\Advanced Set it to 0.
Set maximum event log (admin tool) sizes and clear all events	Improves overall DVM performance.	**1.** Right-click on **Application** and click **Properties**. **2.** In the Log Size section, select **Overwrite events as needed**. **3.** In the Log Size section, set the **Maximum Log Size** to 64kb. **4.** Click **Clear Log**, and click **No on the save dialog**. **5.** Repeat for Security, System and Internet Explorer logs.

Increase VMware ESX Server Service Console Memory

Increasing the amount of memory assigned to the ESX host's Service Console greatly improves the performance of virtual machines on that given host. The ideal amount of memory is 800 MB. After assigning more memory, you need to reboot the ESX host.

To increase service console memory:

1. Find out how much memory is already assigned to the Service Console:
   a. From VirtualCenter, click the **Hosts** tab.
   b. Double-click on the VMware ESX Server 3.x.
   c. Click the **Configuration** tab.
   d. In the Hardware area, click the **Memory** link.
2. Increase the memory to 800 MB.
3. Reboot the ESX host.

Minimize DVM CPU Consumption

`rdpclip.exe` of PowerPoint consumes large share of DVM CPU. `Rdpclip.exe` is a component of PowerPoint that provides functionality in a Terminal Services environment, allowing users to copy and paste between the server session and the Terminal Services client.

Pano VDS does not need this functionality at all because there is no copy and paste between server and client. Pano Logic tested running PowerPoint presentations and noticed that the CPU can reach about 100% even while the user is idle. In the Task Manager Pano Logic noticed `rdpclip.exe` consumes more than 60% CPU. As such, Pano Logic recommends that you disable `rdpclip.exe` by using a GPO setting.

To disable `rdpclip.exe`:

1. Go to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Terminal Services** > **Client/Server data redirection**.
2. Enable the **Do not allow clipboard redirection** setting.

User Group Policy Settings Management with Loopback Processing

By default, as users log on to DVMs (the same applies to physical machines) that are in a specific organizational unit (OU), their environment is composed of two portions:

- Computer portion of the GPO associated with the OU that the DVMs are in
- User portion of the GPO associated with the OU that the users are located in

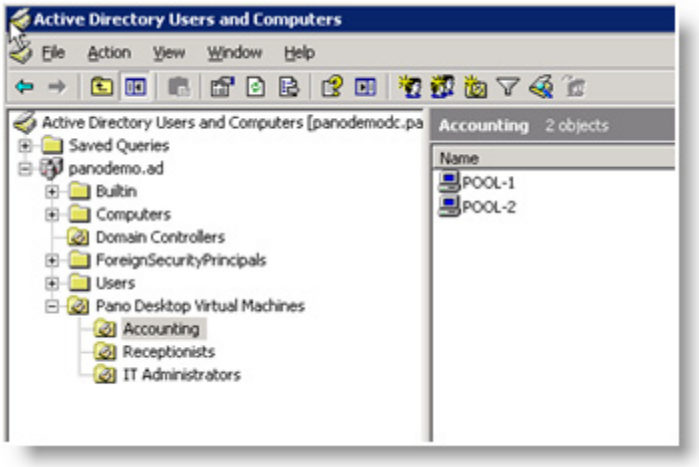
In some cases it may be desirable to use User Group Policy Loopback processing mode to manage user settings in your environment instead.

Loopback processing mode allows an administrator to force the User portion of the GPO associated with the OU that the machines are in to either override or merge with the settings associated with the OU the users are from.

The benefit is that users receive a more uniform environment, because regardless of what OU they come from, they will always get the same User GPO settings from the OU the DVMs are in.

To enable loopback processing:

1. Create an OU that contain the DVMs:



2. Enable the Loopback Processing mode. For each folder under the OU, do the following:
   a. Click on the folder, then click the **Group Policy** tab.
   b. In the table, double-click **DVM policy**. The Group Policy Object Editor launches.
   c. Go to **Computer Configuration** > **Administrative Templates** > **System** > **Group Policy**.
   d. Enable the **User Group Policy loopback processing mode** setting, and set the mode to either Replace or Merge.
      - **Replace** - indicates that the user settings defined in the computer's Group Policy objects replace the user settings normally applied to the user.
      - **Merge** - indicates that the user settings defined in the computer's Group Policy objects and the user settings normally applied to the user are combined. If the settings conflict, the user settings in the computer's Group Policy objects take precedence over the user's normal settings.

19
Pano Manager Network Port Usage

The components of Pano VDS, Pano Manager, Pano Desktop Service and Pano Device, communicate with each other on several ports. In order to function properly, these components require access to these ports. So, you must open these ports and adjust firewall rules accordingly.

Apart from Inbound ports used and Outbound ports used on the Pano Manager, you also need to specify the ports used between Pano devices and the Pano DAS.

For more information, go to “Configure DVM Firewall” on page 73 and “Configure Data Center Firewall” on page 50.

• Inbound Ports Used by Pano Manager

Ports	Protocol	Service	Usage
ICMP		ping	Test connectivity to the server
80	TCP	HTTP	Connections from the UI to control the Pano Manager
443	TCP	HTTPS	Connections from the UI to control the Pano Manager
22	TCP	SSH	Remote terminal access
68	UDP	DHCP	DHCP responses
123	UDP	NTP	Synchronizing of server time
8320	UDP		Communication from the Pano
8321	UDP		Communication from the Pano

• Outbound Ports Used by Pano Manager

Ports	Protocol	Service	Usage
ICMP		ping	Test connectivity to the server
53	TCP	DNS	DNS requests
80	TCP		Communication to VirtualCenter
443	TCP		SSL communication to VirtualCenter
389	TCP	LDAP	Communication to LDAP server
636	TCP	LDAPS	Communication to LDAP server (Secured)
3268	TCP		Communication to the Global Catalog
3269	TCP		Communication to the Global Catalog (Secured)
8319	TCP		Connection brokering to the Pano devices
53	UDP	DNS	DNS requests
67	UDP	DHCP	DHCP
123	UDP	NTP	
389	UDP	LDAP	Communication to LDAP server
636	UDP	LDAPS	Communication to LDAP server (Secured)
8321	UDP		Connection brokering to the Pano devices

• Inbound Ports Used by Pano DAS

Ports	Protocol	Service	Usage
8319	TCP		Communication from the Pano Manager to the Pano DAS
8321	UDP		Communication from the Pano Manager to the Pano devices

• Outbound Ports Used by Pano Devices

Ports	Protocol	Service	Usage
8320	UDP		Communication from a Pano device to the Pano Manager
8321	UDP		Bi-directional communication to/ from the Pano Manager

20 Troubleshooting

If your symptom(s) might be related to performance, not a misconfiguration, user error, or third-party bug, go to "Optimize DVM Performance" on page 141. Otherwise, compare your symptoms against the following common problems:

Troubleshoot Networking Problems

If the color on the Pano Button does not turn blue (go to "Pano Button's Light Indicators" on page 15), the Pano client login screen will not display. Therefore common troubleshooting starts from the color of the Pano Button:

Table 20.1 Pano Button Light Indicators: Fault State

Symptom	What's it mean?	What do I do?
Solid red	Something is wrong with the Power connection of Pano device.	Try connecting another compatible power adapter to the Pano device. If that doesn't work, then the Pano device is defective. This occurrence is rare. Call Pano Logic Technical Support to initiate a replacement.
Blinking red	There is no network cable plugged into a Pano device, or the network cable is damaged (disconnected on the other end)	Try using another network cable to connect the Pano device to the network.

Table 20.1 Pano Button Light Indicators: Fault State

Symptom	What's it mean?	What do I do?
Blinking orange	If the Pano Button does not turn Solid Orange after a minute, the Pano device is not able to get an IP address from the DHCP server. The most common reason for this is that the IP addresses in the DHCP server have been exhausted.	Check the DHCP Server logs to for messages indicating that the server didn't have anymore IP address in its range to assign. Consider the following: • Are there any port filters? • Any relay agents being used? • IP Helper being used? If possible get a wireshark packet capture of the request and response from the Pano device to DHCP server. If that isn't the case, try another Pano device—using the same network cable.
Solid orange	If the Pano Button does not turn solid blue after a minute, the Pano device could not connect to Pano Manager or its Desktop Virtual Machine. The DHCP Server is not configured with the Vendor class to allow communication with Pano Manager.	Set up the Vendor Option in DHCP Server. Go to "(DHCP Method) Set Up Pano Device Discovery" on page 55.

Troubleshoot DVM Login Problems

Normal Login Process

Once a Pano device is connected to a Pano Manager, the Pano client login screen is displayed to the user. After the user enters the username and password and hits the Login button, the Pano Manager displays the user's desktop.

Between the time the user hits the Login button and the desktop is displayed, the screen turns blank and the color on the Pano Button changes to solid orange for a few seconds. This sequence exists because the Pano Manager transfers the connection of the Pano device to the Pano Desktop Service (Pano DAS) running on the DVM.

There is a small interval of time between which the connection of the Pano device to Pano software (Pano software refers to Pano Manager or Pano DAS) is broken. This is normal behavior and the disconnection should only last a couple of seconds.

DVM Login Error Messages

The administration of a DVM includes two management infrastructure components: Pano Manager and the virtual infrastructure (VMware VirtualCenter). If you're like many IT organizations, where one group manages the administration of virtual infrastructure and another group performs desktop management, you might not have access to the virtual infrastructure management tools to troubleshoot DVM login issues. That's okay! You can use the error messages that Pano Manager displays–without accessing the virtual infrastructure.

When the user types the credentials in the Pano client login screen and clicks **Login**, the Pano Manager presents the user's desktop. If the Pano Manager cannot do its job, Pano Manager displays messages to the user. The following messages are the most common:

- **No desktops are available. Please contact your system administrator; No DVMs are configured for you; No DVMs are available for you.**

This means that Pano Manager could not find a desktop that is available and to which the user has access.

If the user is a member of a Permanently Assigned Desktops collection type, a new DVM should be created for this user in the Pano Manager by modifying the settings of the DVM collection, or in VMware VirtualCenter. Ideally, users should not get this error at all because a new DVM should be waiting before they login for the first time.

If a free DVM is not available when the user logs in; a new one will be created. This can take some time and the user will be shown a `waiting for deployment to start` message along with a time indication. Then the `Your desktop is being created. Please wait or click Cancel to return to the login screen` message is displayed along with amount of time remaining.

After the DVM is created the `Your desktop is ready for you to Login` message appears. User can now log on to the DVM.

If the user is a member of a Pooled Desktops collection type, it could mean that other users are not logging off after they are done. Instead of creating a new DVM and encountering DVM sprawl, you can enforce session limits (go to "Control Session Timeouts" on page 78) in the DVMs in the collection using Windows mechanism. Alternatively, as a quick fix, you can log on as

administrator into the DVM that has a user logged on but is disconnected from any Pano device and then logoff. That will free up the DVM and return it to the pool.

- **The connection to your client was lost unexpectedly. Please log on to resume your session.**

The user session is still running in the server. The user will be connected to the same session upon login through Pano client login screen. There is no data loss and the desktop will be displayed as the user had left it.

- **Your desktop is powered off. You can power it on or click Cancel to return to the login screen.**

The DVM has been powered off. This power off is equivalent to a physical machine poweroff. Just as in the case of a physical desktop machine, the user can click **Power On** to power on the virtual machine. Once the user does so, the `Pano Manager` displays a `Your desktop is being powered on. Please wait or click Cancel to return to the login screen` message.

- **Your desktop is powered on but not yet ready. Please wait or click Cancel to return to the login screen**

The Pano Manager is in the process of contacting the user's DVM. This can take some time. After a few seconds the Pano Manager displays a `Your desktop is ready for you to log in` message. The user can click the Login button at this point to get to the desktop.

- **Incorrect Login even though the login id and password are correct.**

The connection to Active Directory server is lost. Refresh the configuration. Log on to Pano Manager, then in the Directory Configuration area, click the Setup tab, then click **Configure**. If it does not connect then there is a problem with connectivity between Pano Manager and Active Directory.

Troubleshoot Monitor, Mouse, and Keyboard Problems

Generally, we support and have certified most USB device classes (go to "Supported USB Devices" on page 32) with the Pano device. Here are some troubleshooting steps related to computer peripherals:

Symptom	What do I do?
Audio is not working with Pano devices	
• There is no sound	Do the following: • Enable sound. "Control Session Timeouts" on page 78. • Apply fix to sound problem. Go to "Control Session Timeouts" on page 78.
Monitor is not working with Pano devices	

• The screen is black
• The monitor displays out of range error message
• The colors are different/the windows screen has a different tint
• The screen has lines on it
	If the screen is black it might be out of range.
	• Unplug and re-plug monitor by unplugging the power cable and plugging it back in.
	• Power re-cycle the Pano device.
	• Hook up monitor to another PC or laptop.
	• Do one of the following:
	  • For global change, Go to Pano Manager and change the screen resolution to 800*600.
	  • For local change, Change the screen resolution to 800*600 through the Pano Control Panel.
	• If those solutions don't work, then collect the log files just like in Mouse/Keyboard malfunction. Go to "Download DVMs' Log Files" on page 164.

• Login screen goes blank and displays a `Desktop VM does not support 24 bit color` error message	Do the following: 1. Log on to DVM using RDP. 2. From the Pano Control Panel, go to **Properties**, and verify that color quality is set to 16-bit. If it is some odd number like 15, it means that there might be a Group Policy that is over-riding the color quality set by Pano Control Panel. 3. Set the local machine's color quality to 16-bit, then log on to the DVM again using RDP. If the setting is still set to 15-bit, then there is a Group Policy in Active Directory that is overwriting the local machine settings.

Symptom	What do I do?
Mouse or keyboard is not working with Pano devices	
• The mouse moves too fast/too slow. • Keyboard types in the same letter multiple times [Repeat rate is very high]. • The mouse/keyboard do not work at all • Mouse moves only in vertical/ horizontal direction.	• If the mouse is not moving at all then re-plug the USB. • Verify that VMware Tools are installed on your DVM(s). VMware Tools improves keyboard input performance. Go to "Install VMware Tools" on page 69. • Verify that the Pano DAS is installed. If the Pano Logic icon appears in your task bar (**Start** > **Programs** > **Pano Desktop Additions** > **Pano Control Panel**), then the Pano DAS is installed. The Pano Control Panel works in coordination with the VMware Tools and the Pano DAS on your DVM to further configure and accelerate your keyboard input response. If not installed, go to "Install Pano DAS" on page 71. • Change the Repeat rate keyboard setting. Go to "Set Keyboard Settings for Specific DVMs" on page 92. • If those solutions don't work, then collect the log files. Go to "Download DVMs' Log Files" on page 164.

Troubleshoot USB Devices Problems

If a user plugs in a USB device and it does not show up in the DVM, it could be for the following reasons:

- USB Support is not enabled. Go to "Install Pano Device USB Support" on page 97.
- The USB device might be overdrawing current. USB standard allows for 500mA of current to be drawn from the source. If the device draws more than that, then the Pano device will not allow the connection. The user should try to connect the USB device to the Pano device via a powered USB hub.
- Sometimes the Pano device might take a long time (2-4 minutes) to recognize that the USB device has been plugged in. This delay can happen with an external storage device; for example; if the size of the storage device is large.

The best practice with USB devices is to plug them into powered USB hubs, then plug the powered USB hub into Pano device.

Troubleshoot RDP Connection Problems

Generally, RDP settings should have been correctly set during DVM Template creation; as such, a user should not experience any problems in logging on to a DVM using RDP. The most common reasons for not being able to RDP to a DVM are as follows:

• RDP not enabled

Enable RDP protocol on the virtual machine as outlined in "(RDP Connections Only) Enable Remote Desktop and Set Remote Desktop Users" on page 75.

• AD groups doesn't have permissions

Select an AD user group that has permissions to connect to this DVM using RDP. Verify that the Group Policy does not disallow RDP. Make sure that the user has a UPN (User@Company.com) in Active Directory.

• Firewall prevents communication

Ensure that there is no Windows firewall rules that prevent the Pano device from communicating with the Pano DAS running on every DVM. Go to "Configure DVM Firewall" on page 73. Some organizations have a policy to enable the Windows firewall and many do not have this policy. You can troubleshooting, by temporarily disabling the firewall.

• RDP not listening on the correct port

Ensure that RDP runs on default port 3889.

• Incomplete UPN

Check to verify that the user has a complete UPN (User@Company.com) defined within Active Directory or your alternate user authentication service. For more information, go to "No Privileges or No UPN Format" on page 161.

• Data encryption error

If you try to connect to a DVM using RDP, you might receive a data encryption error. This problem is caused by a known issue (KB323497) in Windows XP. To fix this problem, do the following:

1. Launch Registry Editor.
2. Locate and click the `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TermService\Parameters` registry subkey.

3. Under this registry subkey, delete the following values:
   - Certificate
   - X509 Certificate
   - X509 Certificate ID
4. Quit Registry Editor, and then restart the virtual machine.

Troubleshoot Authentication and Directory Services Problems

• Missing Fields

If a red error message appears to the right of Directory Configuration area when you click Configure, the information in the fields is incorrect.

• No Global Catalog

If the dialog box is empty (you cannot browse), but a red error message does not appear, the Pano Manager cannot communicate with the Domain Controller. To fix this problem, specify the port of the Global Catalog. For example: ldap://10.1.100.1:3268.

By default the Global Catalog runs on port 3268 in unencrypted mode and on 3269 in encrypted mode. Therefore, the URL is `ldaps://dirserver1.yourdomain.com:3269` for encrypted mode and `ldap://dirserver1.youdomain.com:3268` for unencrypted mode. Consult your Active Directory administrator if the Global Catalog runs on a different server or if it is configured to run on a different port.

If you are convinced that the Active Directory server address is indeed correct, try to enter the Global Catalog server address. [Global Catalog generally runs on port 3286]. If putting in Global Catalog address works, check to see if the Pano Manager is on the same domain as Active Directory domain controller whose address was entered. If not, then change it to same domain.

• No service location record

If you receive a “javax.naming.CommunicationException: localhost:389 [Root exception is java.net.ConnectException: Connection refused]” exception, you might not have a service location record in your DNS Server.

If you have more than one domain controllers, Pano Manager can automatically choose one based on the workload on each domain controllers. However, sometimes this configuration gives this exception if you don’t have a service location record in your DNS server.

To create a service record for your Active Directory:

1. Open your DNS management console, navigate to the domain, then `_tcp`.
2. Right-click your mouse to bring up the menu, then click **Other New Records**.
3. In **Resource Record Type** dialog, pick **Service Location (SRV)**, then click **Create Record**.
4. In **New Resource Record** dialog, choose _ldap in **Service:** drop-down list.
5. Enter the name of the domain controller in **Host offering this service**, then click **Ok**.
6. Try to connect to Active Directory again.

• No Privileges or No UPN Format

In order to properly establish a relationship between a user and a DVM the user must be able to be authenticated using a complete UPN (User Principal Name) that, in the end, gets passed along as something like the form of username@yourdomain.com.

The portion @domain.com is appended to the user name from information defined in the users account within Active Directory (or your alternate directory services database). If a `No UPN` error is encountered, do the following:

- Check to make sure that an account with adequate credentials is being used within the Directory Configuration portion of your Pano Manager to browse your AD tree and do user lookups and authentication.
- Look at the account information in your Active Directory or alternate user database for the username that is being used when you encounter this error. When you (or the system administrator of the Active Directory server) logs in to the directory services to look at this users properties, make sure that a "@yourdomain.com" or "@yourdomain.net" etc is selected for the user so that it can properly be appended to the username during the process of authenticating a user and establishing a session to a DVM. Once this has been done, login via a Pano device using only a username/passwd. There's no need to type in the entire username@domainname.com. Verify that the user is able to log on successfully. To further verify that this completely resolves the issue, log on using alternate users that may have previously failed.

• Other failure reasons

To help troubleshoot configuration issues, the host URL and the following Root DSE attributes are written to the log after connecting. If above checks fail then get information about the exception in Pano Manager via the log file (go to “Work with Log Files” on page 163):

- supportedLDAPVersion
- namingContexts
- defaultNamingContext
- configurationNamingContext
- supportedCapabilities
- supportedControl

Troubleshoot Communication Problems with VirtualCenter

- If you click **Configure** and get a Java exception error, then do the following:
  - Check that the URL of VirtualCenter is correct. Ensure that you have the correct IP address or hostname, and that you specified `/sdk` at the end of the URL string.
  - Verify the username. The username should be of valid user who has permissions on the Folder hierarchy in VirtualCenter as well as customization scripts and other objects. This user should be able to login to VirtualCenter from the VMware Infrastructure Client.
- If you are unable to connect to VirtualCenter, try using the admin user of VirtualCenter and check if Pano Manager can connect to VirtualCenter. If Pano Manager can connect to Virtual Center with the admin user then the original user does not have sufficient privileges.
- If the exception stack shows a xml parser error, check that the Data Center and the Cluster have been created in VirtualCenter. Then, stop the VirtualCenterservices and restart. Log out of Pano Manager, then log on again and try to connect again.

21
Work with Log Files

The Pano Manager provides a list of system messages concerning the activity and performance of the Pano Virtual Desktop Solution.

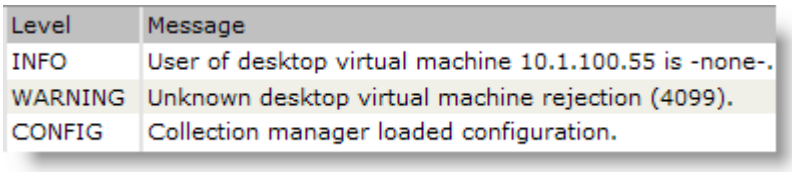
The Pano Manager and the Pano DAS (Pano Desktop Service) generate log files that can help you diagnose problems that affect your users. Occasionally, Pano Logic Technical Support might ask that you send these log files.

Display and Filter Pano Manager's System Messages

To display a Pano Manager's system messages:

1. Log on to the Pano Manager.
2. Click on the **Log** tab.
3. Use the following information to determine the significance of the message.

Column Name	Contents
Time	Time the system message was issued
Level	The security level of the incident
Message	Text of the system message



Level	Message
INFO	User of desktop virtual machine 10.1.100.55 is -none-.
WARNING	Unknown desktop virtual machine rejection (4099).
CONFIG	Collection manager loaded configuration.

4. (Optional) Download these messages. Go to "Download Pano Manager's Log Files" on page 164.

To filter the list of system messages:

1. Log on to the Pano Manager.
2. Click on the Log tab.
3. Select the **Show Most Recent** check box.
4. Enter your filter string in the Message Filter field, and then press **Enter**.

To clear your filter:

1. Log on to the Pano Manager.
2. Click on the **Log** tab.
3. Select the **Show Most Recent** check box.
4. Delete your search string from the Message Filter field, and then press **Enter** on your keyboard.

To see the full details of a message:

1. Log on to the Pano Manager.
2. Click on the **Log** tab.
3. Click on the desired row in the message list. The full message appears in the area below the message list.

Download Pano Manager's Log Files

The log files download as a zip file. These log files contain archived messages.

To download the Pano Manager's log files:

1. Log on to the Pano Manager.
2. Click on the **Log** tab.
3. Click **Download**.
4. When prompted, save the `.zip` file to a specific location.

Download DVMs' Log Files

To download a DVM's log files:

1. Connect to the DVM using a Pano device or RDP. Go to "Log On To DVMs as End User" on page 17.
2. Zip the contents of directory `C:\Program Files\Pano Logic\Pano Desktop Additions\LOG` and copy to your desktop.
3. Unzip the file.
4. Use Wordpad to open the `atto.log`. Neither Notepad nor Excel will not format the text properly.

22
Upgrade Pano VDS

(Overview) Upgrade Pano VDS

Pano Logic recommends that you use your company's existing Software Lifecycle Management tools. Use the same software management practices with virtual machines that you currently use with physical computers.

To upgrade Pano VDS, perform the following sequence of task:

Task		Go To...
1.	Download software.	"Get Pano VDS Software" on page 165
2.	Upgrade Pano Manager.	"Upgrade Pano Manager" on page 166
3.	Verify the version of VMware Tools that you're running.	"Check Status of VMware Tools" on page 167
4.	Update VMware Tools.	"Update Pano Manager VM's VMware Tools" on page 168
5.	If you previously uploaded a certificate from a Certificate Authority, you must upload it again as this information is not saved during an upgrade.	"Add Certificate from Certified Authority" on page 171
6.	Upgrade Pano Desktop Service.	"Upgrade Pano DAS" on page 169

Get Pano VDS Software

To get the software:

1. Go to http://download.panologic.com (contact Pano Logic Technical Support at support@panologic.com to obtain access credentials).
2. Click on the latest download link to download the following files:
   - PanoMan.tar.gz (Installer for the Pano Manager)
   - PanoDAS.msi (Installer for the Pano Desktop Service)

Next Step(s): "Upgrade Pano Manager" on page 166

Upgrade Pano Manager

Use this procedure to upgrade from Pano Manager v2.0.4 or v2.5 to v2.5.1. If you are currently running v2.0.2 or older, you must first upgrade to v2.0.4; if you don't, the kernel upgrade will fail.

This upgrades takes approximately 5 minutes. Updating the Pano Manager entails copying a file from the Pano Logic Technical Support download server to the Pano Manager VM. This file is then used to update the Pano Manager application, and occasionally, the Pano Manager VM's Linux kernel.

While the update process is running, users will not be able to establish *new* connections to their DVMs. Users that have *existing* connections to their DVMs will be able to work without interruption.

To upgrade the Pano Manager:

Before You Begin: "Get Pano VDS Software" on page 165.

1. Using a secure connection, copy `PanoMan.tar.gz` to the Pano Manager Virtual Machine's `/tmp` directory.
2. From VMware VirtualCenter, log on to the Pano Manager console.
3. From the Pano Manager console, Select **4 - Drop to bash shell (Power Users)**.
4. Change directories to `/tmp`, then run the installer:

```
# cd /tmp
# /opt/installbroker_wrapper.sh PanoMan.tar.gz
```

   After the installer completes, the Pano Manager VM restarts automatically if necessary.

Next Step(s): "Check Status of VMware Tools" on page 167

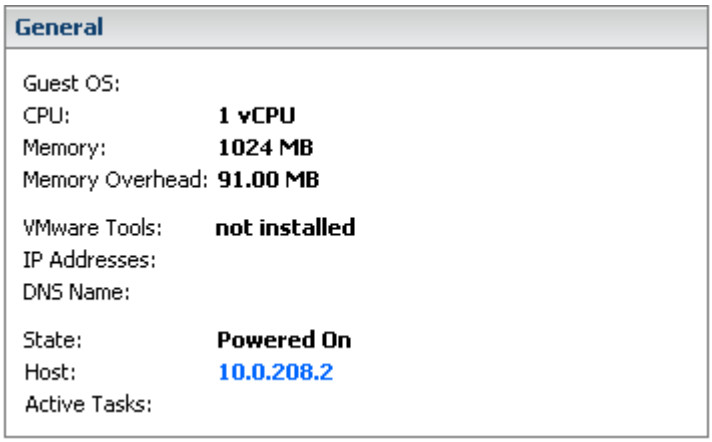
Check Status of VMware Tools

The Pano Manager VM ships with a version of VMware Tools installed. Keep VMware Tools up to date on the Pano Manager VM. VMware Tools on your virtual machines often become out of sync with your ESX server when you upgrade your host. Always use the latest version of VMware Tools.

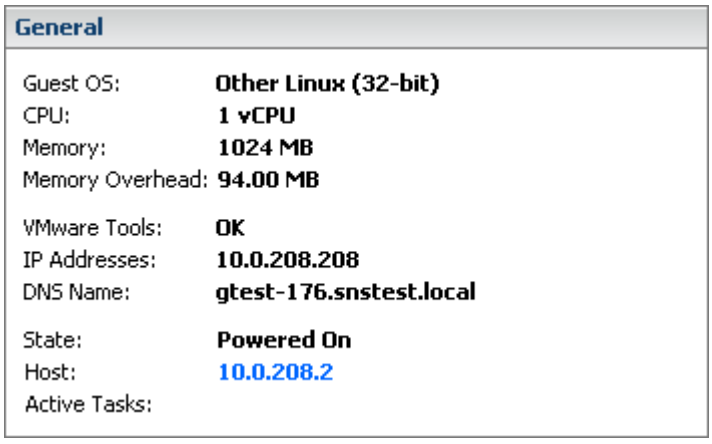
To check the status of VMware Tools:

1. Log on to VirtualCenter.
2. Select **View** > **Inventory** > **Hosts & Clusters**.
3. Click the **Summary** tab. The **General** area displays the current status of VMware Tools, in addition to the version that is installed. If outdated, the VMware Tools field says `out of date` or, if not installed, `not installed`.

Not installed



Installed and updated



Next Step(s): If your Vmware Tools version is outdated, go to "Update Pano Manager VM's VMware Tools" on page 168.

Update Pano Manager VM's VMware Tools

The Pano Manager VM ships with a version of VMware Tools installed. Ensure that you keep VMware Tools up to date on the Pano Manager VM, especially for major versions: in other words, don't use Vmware Tools from ESX 2.5 on a 3.5 server.

To update Pano Manager VM's VMware Tools:

Perform the following series of steps on the Pano Manager VM.

Before You Begin: "Check Status of VMware Tools" on page 167

1. Ensure that the Pano Manager VM has a DVD/CDROM device: power off the Pano Manager VM, right-click on the Pano Manager VM, click **Edit Settings**, then use the Add Hardware wizard.

   For detailed instructions about how to add hardware devices, go to the *Adding Hardware* section of the VMware VI3 Basic System Administration Guide.
2. Using the Virtual Infrastructure Client, connect to VirtualCenter or the ESX host to access the Pano Manager VM.
3. Right-click on the Pano Manager VM and choose **Install VMware tools**.
4. Log on to the Pano Manager VM as `root`.
5. From the Pano Manager console Main Menu, select option **4 - Drop to bash shell (Power Users)**.
6. As root, mount the VMware Tools virtual CD-ROM image and change to a working directory (for example, `/tmp`), as follows.

```
# mount /dev/cdrom /mnt/cdrom
# cd /tmp
```

7. Uncompress the installer and unmount the CD-ROM image, where `xxxx` is the build/revision number of the Workstation release.

Note: If you don't know the version of VMware Tools, press the **Tab** key after you type `VMwareTools-`; the version automatically appends to the command string.

```
# tar -zxf /mnt/cdrom/VMwareTools-5.0.0-<xxxx>.tar.gz
# umount /dev/cdrom
```

8. Run the VMware Tools tar installer for the appropriate version of ESX, answering the on-screen configuration questions. Press Enter to accept the default value.
   - For ESX 3.5 execute:

```
# cd vmware-tools-distrib
# ./vmware-install.pl
```

   - For ESX 3.0.x execute:

```
# cd vmware-tools-distrib
# ./vmware-config-tools.pl
```

9. Log off the root account.

```
# exit
```

Next Step(s): "Upgrade Pano DAS" on page 169

Upgrade Pano DAS

Use this procedure to upgrade directly from Pano Desktop Service (Pano DAS) v2.0.x or Pano DAS v1.5.x to Pano DAS v2.5.1.

The Pano Desktop Service can also be updated using software tools such as Microsoft Systems Management Server (SMS), though this method can be a bit complicated. Pano Logic Technical Support prefers to walk you through this process. Please contact Pano Logic Technical Support.

Don't forget to upgrade both your DVM templates as well as the existing desktop virtual machines in your Pano VDS. It is very important that you upgrade templates because they are used to provision new DVMs.

To upgrade the Pano Desktop Service from v1.5.x or v2.0.x:

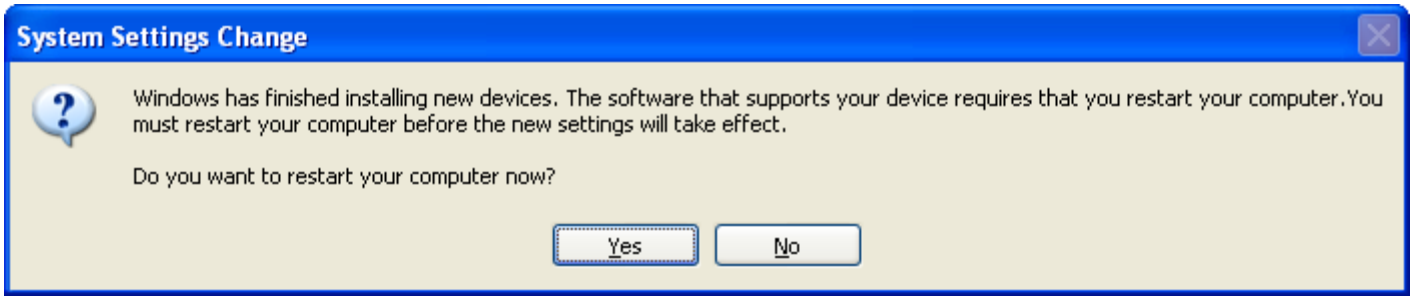
1. Copy `PanoDAS.msi` from your network share to the desktop virtual machine.
2. Double-click on `PanoDAS.msi`.
3. When prompted for the setup type, choose **Complete**, and accept all the other default options.
4. When the installation process completes, click **Finish**.

To upgrade the Pano Desktop Service from v2.5.0:

1. Copy the `PanoDAS.msi` from your network share to the desktop virtual machine.
2. Uninstall the version of Pano DAS that is currently running on the DVM.
   a. From the Windows Control Panel, double-click on **Add or Remove Programs**.
   b. Go to **Pano Desktop Additions** and click **Remove**.

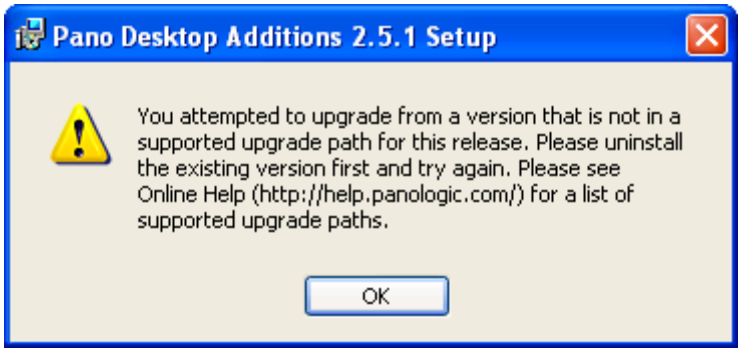
   The DVM loses its connection because Pano DAS is no longer installed.
3. Using the VMware VIC, connect to VirtualCenter.
4. From VirtualCenter, right-click on the DVM, then click **Open Console**. You are prompted to log on.
5. Log on as Administrator and, when prompted, restart the DVM.

6. After the DVM restarts, log on again as Administrator and, when prompted, restart the DVM again. Sorry about the additional restart, but it's required to install all the required files.



7. Double-click on `PanoDAS.msi`.
8. When prompted for the setup type, choose **Complete**, and accept all the other default options.

   If you receive the following message, it's because you need to uninstall the old version of Pano DAS that is running on the DVM.



9. Wait a few seconds, and allow the DVM to restart.
   - The installer tries to install the required files and temporarily disappears in order to enable you to see potential Windows alerts. Windows alerts are notorious for launching in the background. There's no reason to expect that you'll receive any Windows alerts.
   - After installation, the installer restarts the DVM.
10. Restart the DVM again. Sorry about the double-restart, but its required to get the DVM in the correct state.
11. (Important!) Log on to the DVM.

    If you don't, your end-users might be prompted to type credentials with Administrator privileges. This behavior is caused by a Windows bug that is currently unresolved. The Administrator credentials are not necessary; users can dismiss the dialog, but the prompt may confuse or concern them.
12. Congratulations! You've successfully upgraded Pano DAS. In the next release, the upgrade process will be much simpler.

23 Add Certificate from Certified Authority

The Pano Manager uses a self-signed certificate for secure communication over HTTP using SSL (HTTPS). You can replace this self-signed certificate with a more secure solution—a certificate from a Certificate Authority.

(Overview) Replace Pano Manager's Self-Signed Certificate

To replace Pano Manager's self-signed certificate with a certificate from a Certificate Authority, perform the following sequence of tasks:

Before You Begin: After you install and configure the Pano Manager VM as outlined in "(Overview) Install and Configure Pano Manager VM" on page 37, and you confirm that Pano Manager VM is working in your network, you can replace its self-signed certificate. Of course, you can also apply your certificate at any point.

Task	Go to...
1. Upload your certificate	"Upload Your Certificate" on page 172
2. Disable the HTTP port	"(Optional) Redirect HTTP Port To HTTPs Port" on page 173

Upload Your Certificate

Each time you upgrade Pano Manager, you will need to upload your certificate because this information is not saved during an upgrade.

To upload your certificate:

1. Connect to the Pano Manager VM using a secure connection. Go to "Initiate Secure Connections" on page 24.
2. Copy the certificate to the Pano Manager VM. Save the file in the `/opt` directory.
3. Copy the `/opt/hostname/broker/conf/server.xml` file from the Pano Manager VM to your desktop.
4. Open the `server.xml` in an editor (Notepad or vi).
5. Add the following XML tags to the Connector element where `mycert.p12` is the filename of your certificate:
   - keystoreType="PKCS12"
   - keystoreFile="<path to the certificate>"
   - keystorePass="<password for the certificate>"

   Example:

```
<Connector
className="org.apache.coyote.tomcat5.CoyoteConnector"
      port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true" disableUploadTimeout="true"
      acceptCount="100" debug="0" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreType="PKCS12" keystoreFile="/opt/mycert.p12"
      keystorePass="example_password"/>
```

6. Restart the Pano Manager VM:
   a. From the VMware console, log on to the Pano Manager VM using the superuser (root) credentials.
   b. Select option **4: Drop to bash shell**.
   c. Type the following command, then press Enter.

```
service atto restart
```

   Pano Manager can now be accessed via HTTPS using your custom certificate. The Pano Manager continues to accept connections on the HTTP port (port 80) if it has not been disabled.

Next Step(s): "(Optional) Redirect HTTP Port To HTTPs Port" on page 173

(Optional) Redirect HTTP Port To HTTPs Port

To disable the HTTP port:

1. Edit `/opt/atto/broker/bvm/system-conf/iptables.sh`.
2. Comment out (using '#') or remove the following lines:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
REDIRECT --to-port 8084
iptables -A INPUT -p tcp --destination-port 8084 -j ACCEPT
```

3. Update the firewall:

```
bash /opt/atto/broker/bvm/system-conf/iptables.sh
```