Pano System for VDI Administrator’s Guide

Help Version 6.0.6 - 26 September 2012
Software Version 6.0
+1 650-454-8966 or support@panologic.com

Optimize DVM Performance 351

Endpoint Administration 361

Define USB Peripheral Support 367

Configure & Manage Pano Zero Clients & Desktop Preferences 371

Pano System 6.0 Help for Administrators

Other versions: 5.0 | 4.5 | 4.1 | 4.0 | 3.5 | What's New in Pano System for VDI 6.0

Thank you for purchasing the Pano® System! You’re on your way to a simpler and easier way to manage your desktop software applications. With the Pano System you can move all your software off desktops and onto the server. Whether you’re deploying the Pano System for the first time, or you’re maintaining the desktop virtual machines assigned to users, there’s plenty in this online help system for you.

New to Pano Logic and want to learn the basics? Go to Pano System Overview, Understanding Virtual Desktops, and Administering Your Pano System.

Ready to upgrade your existing installation? Go to Upgrading Your Pano System to 6.0.

Haven’t deployed yet? Go to Deployment Planning.

Want to download the complete PDF? PDF   Have a Specific Question? Browse our FAQs

New! We’ve created several short videos to explain some key setup and configuration steps. You can find them all at Pano Logic videos. We’ve also added an icon to indicate where video is available on a particular topic

Owners of iPads will be interested in Using an iPad to connect to Pano Desktops.

Pano System Quick Links

- New! Licensing
- New! Pano Virtual Client
- Deploy Pano Remote - now with RSA SecurID
- Support for USB Devices
- Upgrading Your Pano System to 6.0
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen
- Configure & Manage Pano Zero Clients & Desktop Preferences
- System Requirements
- Troubleshooting
- Optimize DVM Performance

Third-Party Quick Links

- Microsoft Getting Started with Hyper-V
- VMware vSphere
- VMware Basic Administration Guide
- VMware Compatibility Guides
- Microsoft Active Directory Server Portal
- Microsoft Document Downloads
- Microsoft Hyper-V Server Docs
- eDirectory Documentation
- OpenLDAP Documentation

Help Version 6.0.6 - 26 September 2012
Software Version 6.0 Copyright © Pano Logic, Inc.
+1 650-454-8966 or support@panologic.com

2
What's New in Pano System for VDI 6.0

Overview of What's New

- Pano Virtual Client is software that repurposes PCs as Pano endpoints. This lets you use your existing PCs along with new Pano Zero Clients, thus reducing your transition cost.
- RSA SecurID Support in Pano Remote allows the use of SecurID tokens for two-factor authentication of the Pano Remote login process. This improves remote access security and simplifies management.
- WDDM Support for Windows 7 on VMware and Citrix platforms simplifies installation and prepares you for Windows 8 support.
- New Licensing System provides access to new licensing and maintenance entitlements. Provides a unified License Manager UI to check license status and history. This makes it easier to monitor & optimize license use and ensure compliance with license requirements and corporate governance
- Support for New Release of Virtualization Platforms
  - VMware View 5.0.1 and 5.1
  - vSphere 5.0U1
  - vCenter Appliance 5.0 supported
  - 5.5 and 5.6 Citrix XenDesktop
  - 6.0 and 6.0.2 XenServer
  - XenDesktop 5.6 with Hyper-V 2008 R2
  - XenDesktop 5.5
  - XenServer 6.0.2
  - VMware View 4.5, XenDesktop 4.0 SP1 and 5.0 dropped
- Bug Fixes lists items fixed in this release.
- There is no support for dual monitors on the Pano Zero Client G1 device under 6.0.

Pano Virtual Client

This new software client lets you repurpose PCs to function as virtual desktops. It works alongside Pano Zero Clients and Pano Remotes, and runs on Windows XP and 7 PCs and laptops.

Comparison of Pano Virtual Client, Pano Zero Client, and Pano Remote Client

- Pano Virtual Clients provide the same USB support as theG2 Pano Zero Client, except for isochronous devices such as webcams or headsets.
- Pano Virtual Client is not a replacement for Pano Remote. It uses PDP, not RDP. It must be LAN-based, not WAN/Internet. It is installed on the host PC, and does not use or require a USB.
- It runs full-screen only, not windowed, and does not provide shared access to local PC clipboard, etc.

Pano Virtual Client Deployment

Pano Virtual Client deployment is done via Active Directory (AD). This provides simple management even across large numbers of PCs. You can tie it to selected set of users and PCs. Updates and uninstalls are all handled via policies and filters.

It allows users to still login to local Windows OS on PC.

Manual installation is possible, especially for initial evaluation, but is not recommended for deployment.

Pano Virtual Clients are managed just like Pano Zero Clients. You can monitor via Clients and Sessions tabs in the Pano Controller console. It is registered per NIC used - based on MAC address.

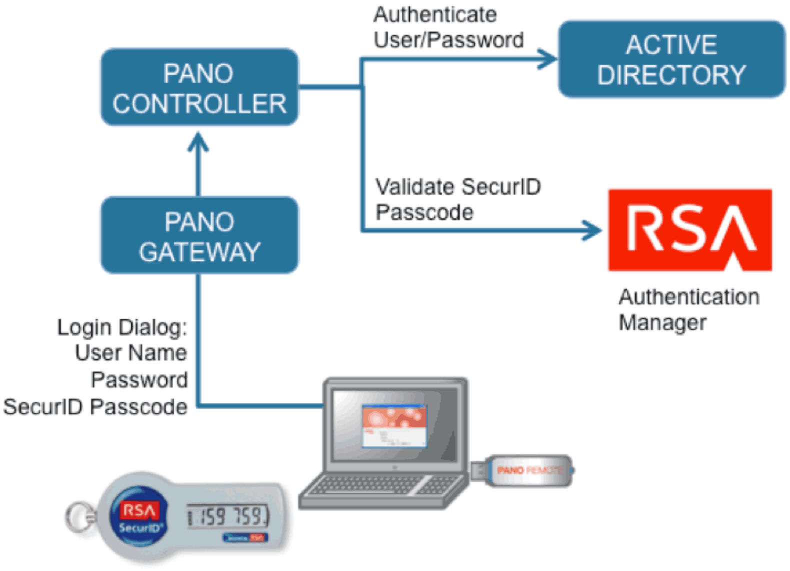
Host PC or Laptop Hardware for Pano Virtual Client

RSA SecurID Support in Pano Remote

Pano now offers new optional two-factor authentication for all remote access users. This adds RSA's SecurID passcode to the Pano Remote login. The user must still enter User name and Password. In addition, the user enters a passcode, create from a User PIN and the RSA SecurID tokens's one-time password.

RSA SecurID is set, or not, per user by the system administrator. Pano Controller integrates with RSA's Authentication Manager software (7.1 SP4).

Learn more at Deploy Pano Remote.



WDDM Support

WDDM can now be used in place of the XPDM display driver in Windows 7 DVMs, but not in XP. It makes DVM installation and updates simpler than prior Pano System versions, and allows use of default (WDDM) drivers when installing both VMware and Citrix client tools in DVMs - there is no need to patch default settings. WDDM under Windows 7 requires 2GB or RAM per DVM.

You can convert existing XPDM DVMs to WDDM if you wish, but this is not required; you can remain on XPDM. Implementing WDDM support does help prepare for Windows 8, which requires it.

Note: You must have the floppy drive controller enabled in the DVMs in order for the WDDM driver to work correctly.

New Licensing System

There is a new license key format that requires only one license key file per customer. License key files are cumulative, holds entire purchase and support/maintenance history

5.0 licenses are not supported with Pano System 6.0. You will need new license key files. These are generated by Pano Logic and updated with each Invoice. They will be emailed to the customer's registered licensing contact, and can be downloaded from Customer Center for existing customers.

Evaluations/trials won't need a license key if run for less than 60 days. You can run UNCONFIGURED for 60 days. By default, all software can be used for 60 days without needing a license with full functionality. Upon expiration, only the installation of a new license key can reset expiration date. Pano Virtual Client will run for 60-day from first connection to Pano Controller.

Learn more at Licensing.

Bug Fixes

Number	Description
6309	Analog driver caused PDS crashed on Win7-32bit when using Logitech webcam(C310) and playing YouTube
6770	DVMs that are part of a device based collection are no longer powering on automatically in Pano System 5.0
6748	Attempting to launch a VM console in Pano Controller v5.0.0.21397 fails with error
6514	RFE: do not display “connection lost unexpectedly” message if Fujitsu ZC monitor is powered off immediately
7083	DVM status fields stop refreshing after ~ 30 minutes
6723	Pano Manager virtualization configuration backup configuration lost when upgrading from 4.5.0 to 4.5.1
6696	Change the default speaker configuration to stereo when connected to G2 devices
5100	Custom login image not transferred to secondary in failover configuration
6293	Screen Artifacts with tile caching engaged
7016	Hyper-V: panonosysprepfixwithprogramfiles.xml for Win7 x64 needed
6807	Pano Manager shows incorrect client status in device-based collection
6777	Catalina error message after configuring passwords and network on Pano Controller
4744	Pano Manager fails to vMotion unless VM has its virtual hardware upgraded
6965	Java Post Hash Collision DoS vulnerability
6962	Access-IS keyboard results in blue-screen crash
6740	Users must attempt multiple logins before being connected to their desktops
7037	Pano Connector for SCVMM installer needs to be updated for new Pano Controller naming
6843	RFE: clone primary monitor video display to second video output
7038	Pano Controller server.xml file should include line for vmm.adapter.scvmm.port
6425	Add ability to send down resolution information via Client Name in PanoMan
7013	Hyper-V: Auto deployment hung in 1%

3

Upgrading Your Pano System to 6.0

This chapter includes the following topics:

Beginning with 6.0, software upgrade is a system-level process. Individual applications do not have to be upgrade one-by-one; the system is upgraded as a whole. To upgrade Pano System, do the following:

Task	Go To...
Obtain a license key. Licensing is different in 6.0;a new key is needed.	Licensing in Pano System 6.0
Get new software.	Get Pano System Upgrade Software
Backup Pano Controller/Manager; then shut down the Controller.	Upgrade a Single Pano Controller (Virtual Appliance Upgrade)
Import new 6.0 Pano Controller VM.	Upgrade a Single Pano Controller (Virtual Appliance Upgrade)
Load License Key in License Manager	Licensing in Pano System 6.0
Restore from backup.	Upgrade a Single Pano Controller (Virtual Appliance Upgrade)

The Pano Manager is now the Pano Controller. Users upgrading from older systems should read 'Pano Controller' as Pano Manager".

Pano Controller is delivered as a virtual appliance and thus includes an operating environment (e.g. operating system, internal database and supporting services) and the Pano Controller application.

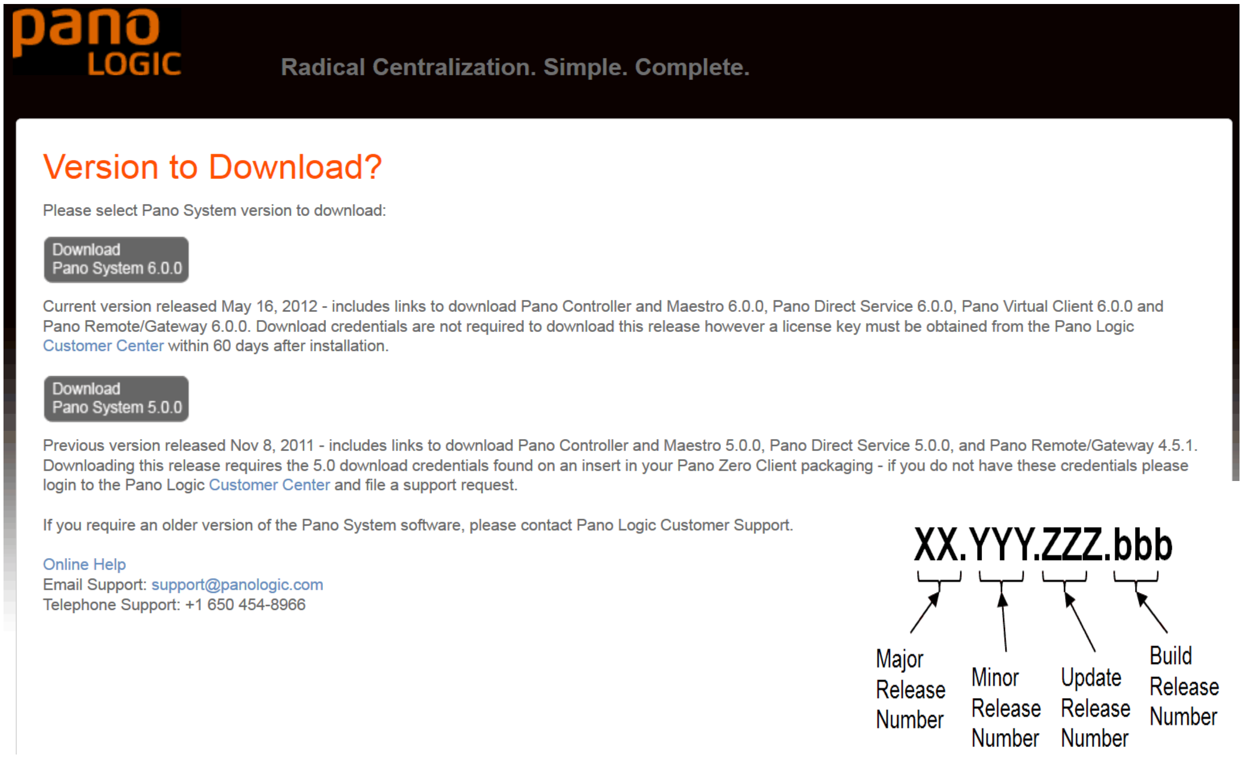
Related Topics

Get Pano System Upgrade Software

Get Pano System Upgrade Software

Begin by either pointing your browser at http://download.panologic.com, or going to the Pano Logic Customer Center at http://customer.panologic.com.

You can select the version you wish to download. Please fill in the download registration form; it will help us contact you if there is a software upgrade, or other critical information.



Version to Download?

Please select Pano System version to download:

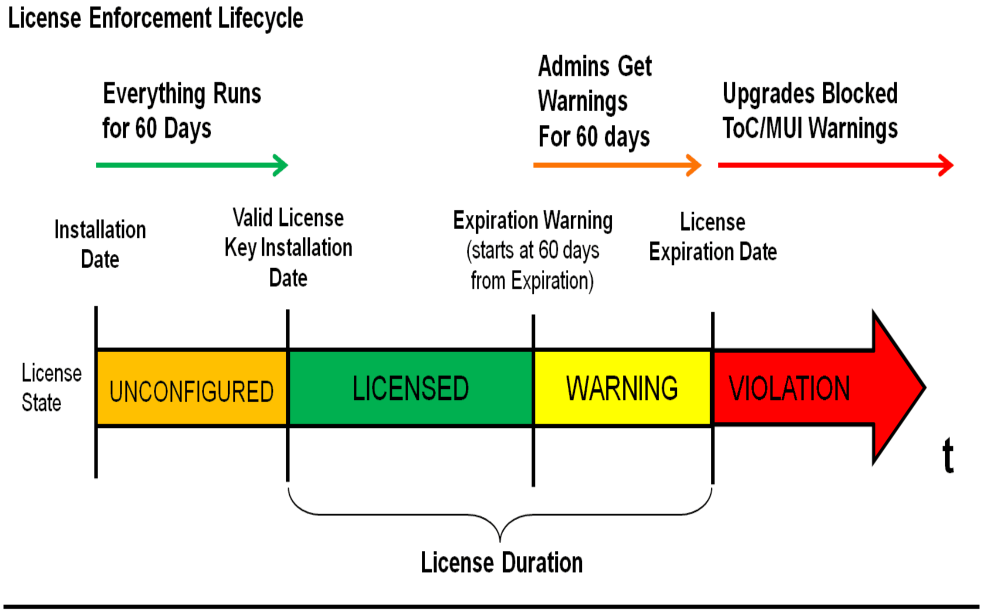
Current version released May 16, 2012 - includes links to download Pano Controller and Maestro 6.0.0, Pano Direct Service 6.0.0, Pano Virtual Client 6.0.0 and Pano Remote/Gateway 6.0.0. Download credentials are not required to download this release however a license key must be obtained from the Pano Logic Customer Center within 60 days after installation.

Previous version released Nov 8, 2011 - includes links to download Pano Controller and Maestro 5.0.0, Pano Direct Service 5.0.0, and Pano Remote/Gateway 4.5.1. Downloading this release requires the 5.0 download credentials found on an insert in your Pano Zero Client packaging - if you do not have these credentials please login to the Pano Logic Customer Center and file a support request.

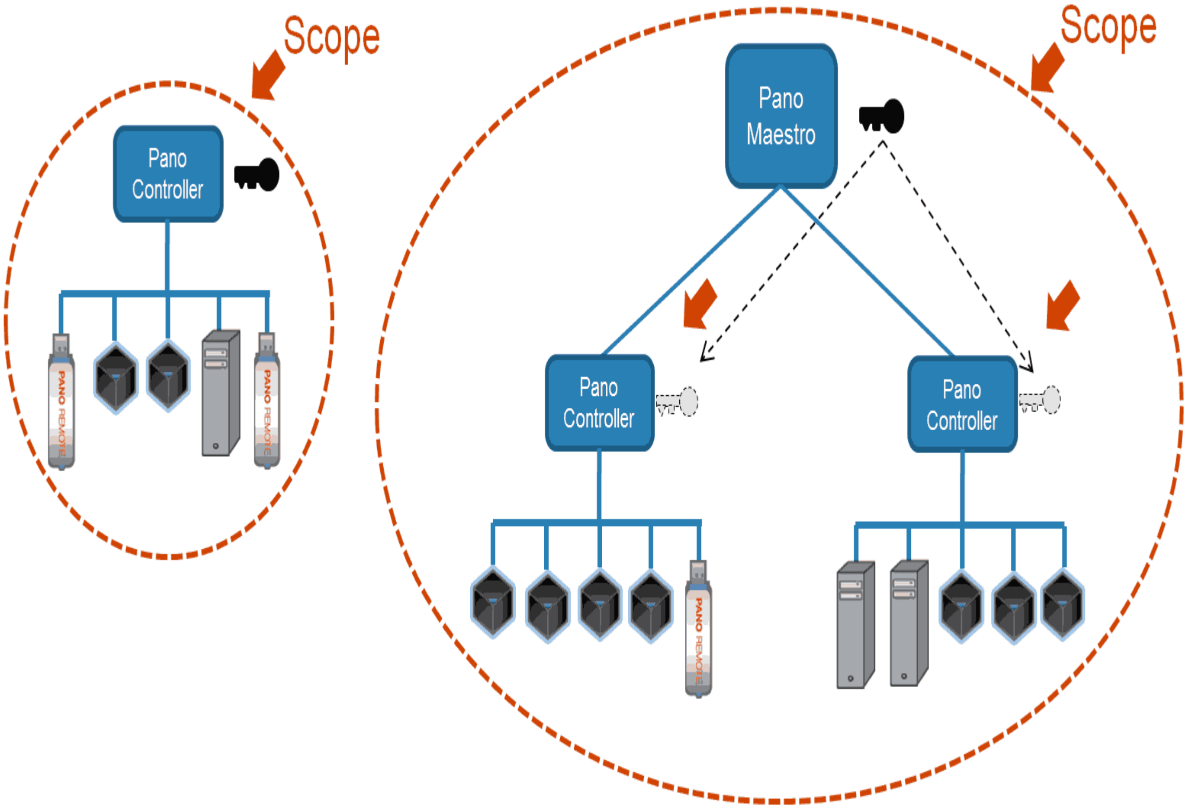
If you require an older version of the Pano System software, please contact Pano Logic Customer Support.

Online Help
Email Support: support@panologic.com
Telephone Support: +1 650 454-8966

The EULA is shown below. Read the EULA and then click on the button to agree. You can also download or print a PDF of our EULA/Warranty booklet. It is included in printed form in your Pano Zero Client shipment. You must agree to the EULA to continue to the download page.

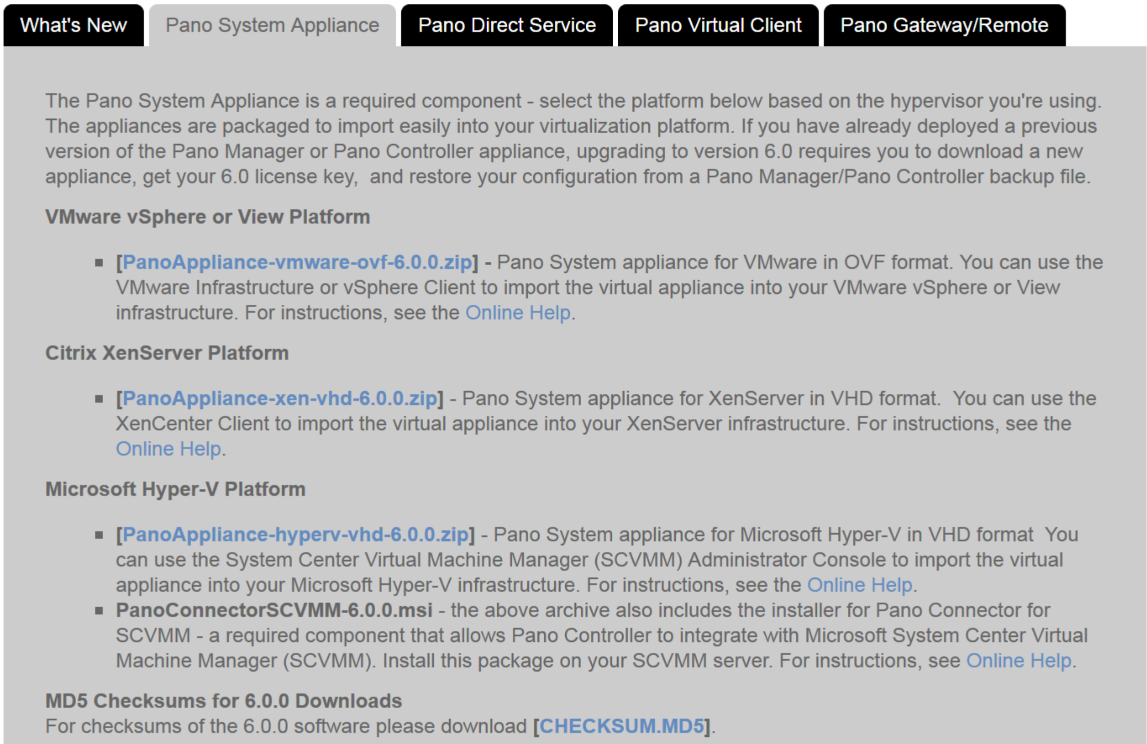

License Enforcement Lifecycle
Everything Runs for 60 Days
Admins Get Warnings For 60 days
Upgrades Blocked ToC/MUI Warnings
Installation Date
Valid License Key Installation Date
Expiration Warning (starts at 60 days from Expiration)
License Expiration Date
License State
UNCONFIGURED
LICENSED
WARNING
VIOLATION
t
License Duration

Next, you'll see the Pano System 6.0 download page. You'll need to download several items from the page. There is a guide to which components are required and under which circumstances to add them, at the top of the page. You'll also find a listing of what's new in the release vs the last major release. On the left you'll find information and links to help you contact our Customer Support team if you need help.



On the other tabs at the bottom of the Download page you'll find sections with links to download each of the following components:

- Pano System Appliance - this is the virtual machine or appliance for Pano Controller and Pano Maestro and is required for all Pano System deployments. A separate zip archive is available for each of three formats for the appliance - you'll need to download the format that matches the hypervisor you're using (see for more details):
  - For VMware vSphere/View the appliance is in OVF format and is imported using the vSphere Client: `PanoAppliance-vmware-ovf-6.0.0.zip`
  - For Citrix XenServer the appliance is in VHD format and is imported using the XenCenter Client: `PanoAppliance-xen-vhd-6.0.0.zip`
  - For Microsoft Hyper-V the appliance is in VHD format and is imported using the System Center Virtual Machine Manager (SCVMM) administration console: `PanoAppliance-hyperv-vhd-6.0.0.zip`. This zip archive also includes the Pano Controller Connector for SCVMM.



The Pano System Appliance is a required component - select the platform below based on the hypervisor you're using. The appliances are packaged to import easily into your virtualization platform. If you have already deployed a previous version of the Pano Manager or Pano Controller appliance, upgrading to version 6.0 requires you to download a new appliance, get your 6.0 license key, and restore your configuration from a Pano Manager/Pano Controller backup file.

VMware vSphere or View Platform

- **[PanoAppliance-vmware-ovf-6.0.0.zip]** - Pano System appliance for VMware in OVF format. You can use the VMware Infrastructure or vSphere Client to import the virtual appliance into your VMware vSphere or View infrastructure. For instructions, see the Online Help.

Citrix XenServer Platform

- **[PanoAppliance-xen-vhd-6.0.0.zip]** - Pano System appliance for XenServer in VHD format. You can use the XenCenter Client to import the virtual appliance into your XenServer infrastructure. For instructions, see the Online Help.

Microsoft Hyper-V Platform

- **[PanoAppliance-hyperv-vhd-6.0.0.zip]** - Pano System appliance for Microsoft Hyper-V in VHD format You can use the System Center Virtual Machine Manager (SCVMM) Administrator Console to import the virtual appliance into your Microsoft Hyper-V infrastructure. For instructions, see the Online Help.
- **PanoConnectorSCVMM-6.0.0.msi** - the above archive also includes the installer for Pano Connector for SCVMM - a required component that allows Pano Controller to integrate with Microsoft System Center Virtual Machine Manager (SCVMM). Install this package on your SCVMM server. For instructions, see Online Help.

MD5 Checksums for 6.0.0 Downloads
For checksums of the 6.0.0 software please download **[CHECKSUM.MD5]**.

- Pano Direct Service - this is installed into the Windows OS in your DVMs and is required for all Pano System deployments. It comes in one zip archive, `PanoDirect-6.0.0.zip`, which contains three separate installer `.msi` files for Windows XP x86, Windows 7 x32 and x64.

  This archive also contains several other files to help with deployments on Windows 7:

  - `PanoLogicAuthCode.zip` contains a certificate called `PanoLogicAuthCode.cer` which is required for manual or silent installations of PDS on 64-bit Windows 7; this same certificate is also required to enable silent installs of 32-bit Windows 7. Pano Direct Service software is digitally signed by Pano Logic using this Authenticode certificate.
  - `panonosysprepfixwithprogramfiles_x32.xml` and `panonosysprepfixwithprogramfiles_x64.xml` are special Sysprep answer files needed if you are running Windows 7 32-bit and 64-bit desktops on Microsoft Hyper-V and you wish to include the Pano Direct Service pre-installed in the template used to clone desktop virtual machines.
- Pano Virtual Client - This is the new software client used to repurpose PCs and laptops as Pano System Endpoints. It is a single zip archive that contains the .msi installers for all three supported desktop OS running on the host PCs for Pano Virtual Client.
- Pano Gateway - this is an optional security gateway for Pano Remote. It is only required if your Pano Remotes will connect from outside networks like the Internet.
- Pano Remote - this download is only required if you have Pano Remote USB keys that are damaged or need to have their software updated.

After you've completed all downloads you'll need a License Key file. New customers will have their License Key file emailed to them as part of the invoice process. Existing customers can download their License Key file from the Customer Center at http://customer.panologic.com (registration required). If you're not yet a Pano Logic customer and just want to try the software, you can download it and use it without a license for up to 60 days.

Next: Upgrade Pano Controller

Upgrade Pano Controller

Use the Pano Controller Console, or, for power users, use the Pano Controller Command Line to upgrade to 6.0.

During this short upgrade process, the Pano Controller copies a file from the Pano Logic Technical Support download server to your local desktop or to the Pano Controller VM directly, depending on your upgrade path. This file updates the Pano Controller application, and occasionally, the Pano Controller VM's Linux kernel.

Note: While the update process is running, users are not able to establish *new* connections to their DVMs. Users that have *existing* connections to their DVMs can work without interruption.

If you previously obtained a certificate from a Certificate Authority, you do not need to upload it again. The installer saves this information during an upgrade.

The upgrade process is different for single instance and multi-instance deployments. Select the appropriate topic for your scenario:

- Upgrade a Single Pano Controller (Virtual Appliance Upgrade)
- Upgrade a Group of Pano Controllers (Virtual Appliance Upgrade)

Upgrade a Single Pano Controller (Virtual Appliance Upgrade)

Follow these steps to upgrade from Pano Controller to Pano Controller a single instance that is not part of a group.

1. Download and import the new Pano Controller virtual appliance

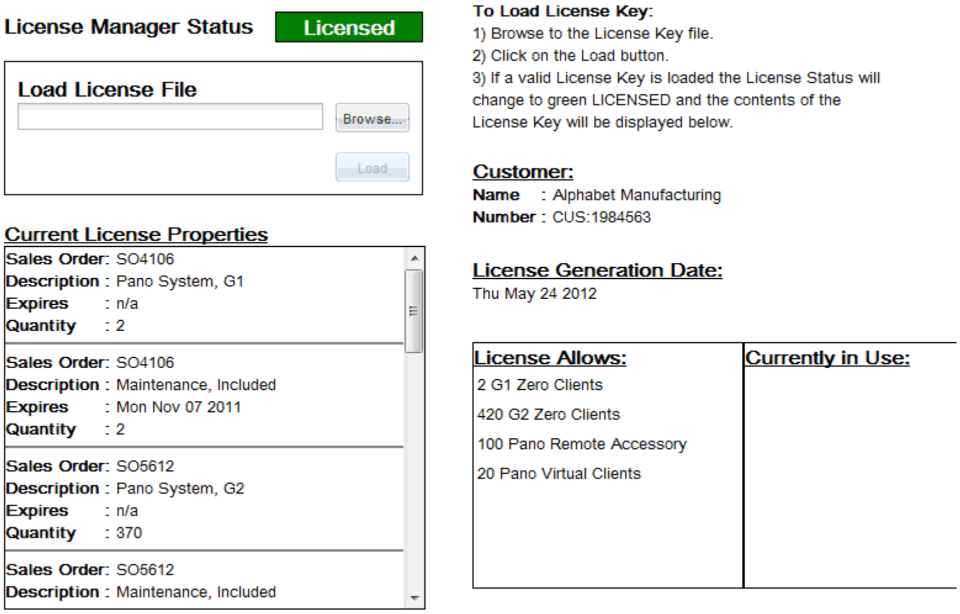
   Do not power on the virtual machine yet
2. Make a backup of your production Pano Controller.
   a. Using a browser, sign into your existing Pano Controller administrative interface
   b. Navigate to the **Setup** tab.
   c. Expand the Backup Configuration section
   d. Click the **Backup & Restore...** button
   e. Press the Backup Now button
   f. Enter a description for the backup
   g. Press the **Backup Now** button
   h. Confirm that the information for the new backup is displayed in Available Backups
   i. Close the Backups dialog
3. Shutdown your existing Pano Controller virtual appliance

   Existing user sessions will not be affected; however, users will not be able to login via until the backup is restored in Step 10 below
4. Power on the new Pano Controller v6.0 virtual appliance
   a. Configure the passwords and IP address for the new virtual appliance
   b. Select option 1 for Pano Controller.
5. Using a browser, sign into the Pano Controller console for the new controller and navigate to the **Setup** tab.
6. Load your License Key file in the Pano Controller License Manager:

a. On the Setup tab move down to the License Configuration section at the bottom of the page and click on the Manage Licenses button.

b. After the License Manager dialog opens, click on the Browse button and then navigate to where you saved your License Key file (previously downloaded from the Customer Center or received in an email from Pano Logic). After you've located your License Key file click on the Load button to load it into the License Manager.

At this point the license status at the top of the dialog should change to green and say “LICENSED” with the details of your purchased products and services shown in the scrolling area in the lower-left corner.



To Load License Key:
1) Browse to the License Key file.
2) Click on the Load button.
3) If a valid License Key is loaded the License Status will change to green LICENSED and the contents of the License Key will be displayed below.

Current License Properties

Sales Order: SO4106
Description : Pano System, G1
Expires : n/a
Quantity : 2

Sales Order: SO4106
Description : Maintenance, Included
Expires : Mon Nov 07 2011
Quantity : 2

Sales Order: SO5612
Description : Pano System, G2
Expires : n/a
Quantity : 370

Sales Order: SO5612
Description : Maintenance, Included

Customer:
Name : Alphabet Manufacturing
Number : CUS:1984563

License Generation Date:
Thu May 24 2012

License Allows:	Currently in Use:
2 G1 Zero Clients	
420 G2 Zero Clients	
100 Pano Remote Accessory	
20 Pano Virtual Clients	

7. Expand the Backup Configuration section

8. Configure the connection to the file server storing your backup files

   a. Enter the URL, username and password

   b. Press **Configure**

9. Restore the latest backup into the new Pano Controller

   a. Press the **Backup& Restore...** button

   b. Select the backup that you created in the step above

   c. Press the **Restore** button

10. Confirm status fields on the **Setup** tab. The relevant fields and expected results are:

    a. Appliance Role: Full Mode

    b. Directory Configuration: Connected

    c. Virtualization Configuration: Connected

    d. Broker Configuration: Configured

    e. License Configuration: Configured

11. Verify that users can login and connect to their desktops.

12. Once the new Pano Controller has run for a number of days and you are confident that your new Pano Controller is working correctly, you may choose to delete the earlier Pano Controller virtual appliance to free up disk space.

Upgrade a Group of Pano Controllers (Virtual Appliance Upgrade)

Here’s how to upgrade multiple Pano Controllers that are part of the same failover group.

Prepare to upgrade Pano Controllers in a failover group:

1. Download and import new Pano Controller virtual appliances
   a. You will need one new virtual appliance for each existing instance of Pano Controller. In some cases it may be faster to import one virtual appliance and clone additional virtual machines from the first.
   b. Do not power on the virtual machines yet.
2. Verify that your primary and secondary Pano Controllers show the following status for Failover Configuration:
   a. The primary is active
   b. The secondary is in Standby mode

Important! Do not continue until the modes are correctly set.

3. Turn off automatic failover
   a. On the primary Pano Controller navigate to the **Setup** tab
   b. Expand the Failover Configuration section
   c. Click the **Edit** button
   d. Clear the **Enable Automatic Switchover** check box
   e. Click **OK** to save changes
4. Make a backup of your primary Pano Controller
   a. Expand the Backup Configuration section
   b. Click the **Backup & Restore...** button
   c. Press the **Backup Now** button
   d. Enter a description for the backup. Make sure your description indicates that this backup is from the primary Pano Controller.
   e. Press the **Backup Now** button
   f. Confirm that information for the new backup is displayed in Available Backups
   g. Close the Backups dialog
5. Shutdown all existing instances of Pano Controller/Pano Manager. The order in which you shut these systems down does not matter

Upgrade the primary Pano Controller virtual appliance

1. Power on the new Pano Controller v6.0 virtual appliance

   Configure the passwords and IP address for the new virtual appliance. Use the same IP address as you did for your original primary Pano Controller.

   Select option 1 for Pano Controller.
2. Using a browser, sign into the Pano Controller console for the new controller and navigate to the **Setup** tab.
3. Expand the License Configuration section
   a. Load your License Key file using the steps listed above b

   b. Your License Status should now be green and LICENSED
   c. Return to the Setup tab- License Configuration should now be Configured
4. Expand the **Backup Configuration** section
5. Configure the connection to the file server storing your backup files
   a. Enter the URL, username and password
   b. Press **Configure**
6. Restore the primary backup into the new Pano Controller
   a. Press the **Backup& Restore...** button
   b. Select the backup that you created in the step above. Verify that the description indicates this backup is from the primary Pano Controller.
   c. Press the **Restore** button
7. Confirm status fields on the Setup tab. The relevant fields and expected results are:
   a. Appliance Role: Full Mode
   b. Directory Configuration: Connected
   c. Virtualization Configuration: Connected
   d. Broker Configuration: Configured
   e. License Configuration: Configured
8. Verify that users can login and connect to their desktops.

Upgrade the secondary Pano Controller virtual appliance

1. Power on another of the new **Pano Controller** v6.0 virtual appliances

   Configure the passwords and IP address for the new virtual appliance. Use the same IP address as you did for your original secondary Pano Controller.

   Select option 1 for Pano Controller.
2. Using a browser, sign into the Pano Controller console for the new controller and navigate to the **Setup** tab.
3. Expand the **Group Configuration** section.
4. Enter the group name and password and press **Configure**.

Both Pano Controllers should appear in the group list.

Enable Automatic Switchover

1. Using a browser, sign into the primary Pano Controller console and navigate to the **Setup** tab.
2. Enable Automatic Switchover
   a. Expand the **Failover Configuration** section
   b. Press the **Edit** button
   c. Select **Enable Automatic Switchover**
   d. Press **OK** to save changes
3. When failover is configured properly, the fields in the **Failover Configuration** section for the primary controller with display the following values:
   a. Virtual IP Address: will display the IP address you entered previously
   b. Primary Controller: will display the IP address assigned to the primary controller

c. Automatic Switchover: will display a check mark

d. Role: will display "Primary"

e. Mode: will display “Active”

f. Availability Status: will display “Active Is Responding”

g. Last Data Change: will indicate the date and time when the primary controller's database last changed

h. .Last Data Sync: will indicate the date and time when the controllers last synchronized their databases. The time difference between Last Data Change and Last Data Sync should be within 30 seconds.

Add auxiliary instances of Pano Controller

If your previous configuration included more than two Pano Controller instances, create new auxiliary instances of Pano Controller and add them to the group.

1. Power on another of the new Pano Controller v6.0 virtual appliances

   Configure the passwords and IP address for the new virtual appliance. Use the same IP address as you did for your original auxiliary Pano Controller (these instances were formerly called slave instances.)

   Select option 1 for Pano Controller.
2. Using a browser, sign into the Pano Controller console for the new controller and navigate to the **Setup** tab.
3. Expand the **Group Configuration** section
4. Enter the name and password for your existing group and press **Configure**.
5. Verify that all members of the group are visible and reporting **OK** status, especially the primary and secondary instances.

Repeat the above steps until you have the desired number of auxiliary instances configured.

Next: Upgrade Pano Direct Service

Upgrade Pano Direct Service

Use the following procedure to upgrade from Pano Direct Service v3.5 or later to v6.0. If you are currently running any other version, perform a fresh install of v6.0.

The Pano Direct 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, so 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 System. Templates are used to provision new DVMs.

Upgrade PDS from v3.0.0 or later, using Pano Controller

Upgrade PDS from v3.0.0 or later, using the installer

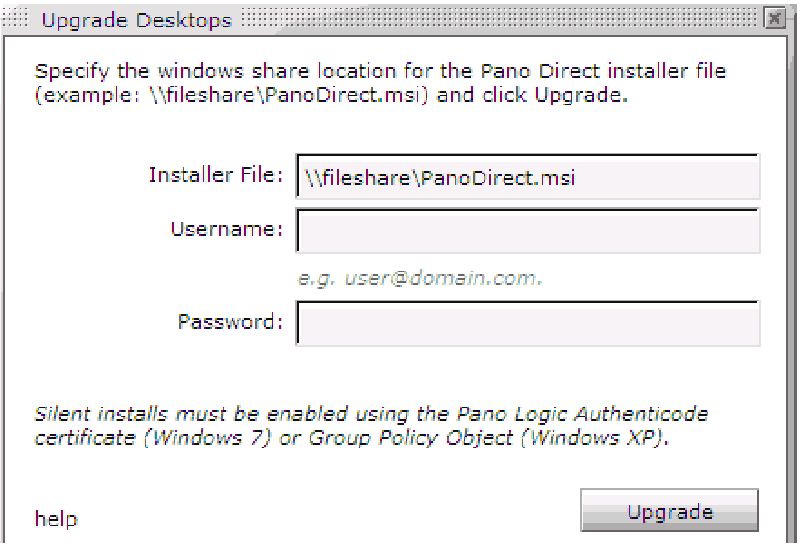
Upgrade PDS from v3.5.x or later, using a GPO

After upgrading, Check Status of Virtualization Tools on DVMs

Upgrade PDS from v3.0.0 or later, using Pano Controller

Before You Begin: Get Pano System Upgrade Software.

1. Enable a silent install:
   - (Windows 7) Use Pano Logic Authenticode certificate.
   - (Windows XP) Group Policy Object. Go to Enable Silent Installation for Windows XP.
2. Copy the `.msi` file to a network share.
3. Log on to the Pano Controller.
4. Click on the **DVMs** tab.
5. Select one or more DVMs, then, from the Desktop drop-down button, choose **Upgrade Desktop...**. The Upgrade Desktops dialog appears.
6. Specify the share location and the credentials, then **Upgrade**.



Specify the windows share location for the Pano Direct installer file (example: \\fileshare\PanoDirect.msi) and click Upgrade.

Installer File: \\fileshare\PanoDirect.msi

Username:

e.g. user@domain.com.

Password:

Silent installs must be enabled using the Pano Logic Authenticode certificate (Windows 7) or Group Policy Object (Windows XP).

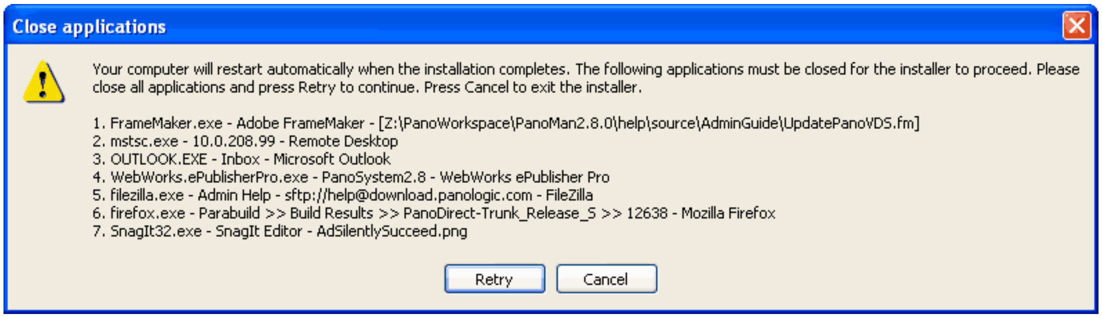
Upgrades will be skipped for any DVM that has an active user session. If you wish to remotely upgrade a DVM, first make sure that no user is logged into Windows.

Upgrade PDS from v3.0.0 or later, using the *installer*

Before You Begin: Get Pano System Upgrade Software.

1. Copy the `.msi` file from your network share to the desktop virtual machine.
2. Double-click on the `.msi` file. The installer launches.
3. Select the **Restart computer when installation finishes (Required)** check box, then click **Next**.
4. Click **Install** to begin the installation.
5. Follow the on-screen instructions. If prompted, save all data 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 automatically restarts Windows in order to complete the installation.



Close applications

Your computer will restart automatically when the installation completes. The following applications must be closed for the installer to proceed. Please close all applications and press Retry to continue. Press Cancel to exit the installer.

1. FrameMaker.exe - Adobe FrameMaker - [Z:\PanoWorkspace\PanoMan2.8.0\help\source\AdminGuide\UpdatePanoVDS.fm]
2. mstsc.exe - 10.0.208.99 - Remote Desktop
3. OUTLOOK.EXE - Inbox - Microsoft Outlook
4. WebWorks.ePublisherPro.exe - PanoSystem2.8 - WebWorks ePublisher Pro
5. filezilla.exe - Admin Help - sftp://help@download.panologic.com - FileZilla
6. firefox.exe - Parabuild >> Build Results >> PanoDirect-Trunk_Release_S >> 12638 - Mozilla Firefox
7. SnagIt32.exe - SnagIt Editor - AdSilentlySucceed.png

6. Wait for the DVM to reboot.

Troubleshooting:

If you have a supported GINA installed, Pano Direct Service fails to upgrade if it determines that the GINA chaining is broken. If the installer returns `broken GINA chain` error, re-establish the GINA chain before you proceed.

Upgrade PDS from v3.5.x or later, using a *GPO*

You should already have a version of Pano Direct Service installed on all the DVMs in your Organizational Unit (OU) and have successfully deployed the software using a GPO. This procedure demonstrates an upgrade using a old version of Pano Direct Service, but the approach is the same.

- Ensure that your Windows Server version is supported. Check Windows Server Support.
- Determine if your users want to use Pano Dual Monitor. If yes, tailor the instructions below to meet the installation requirements outlined in the steps to Configure & Manage Pano Zero Clients & Desktop Preferences.
- Before you perform an upgrade: schedule 5-10 minutes of “downtime”. A GPO upgrade can take several minutes to complete. Also, during the upgrade your end users’ DVMs will disconnect. If your end users attempt to log on they will receive an error message stating that the DVM is not available. Impatient users might choose Power Off or Reset from the Pano Control Panel, resulting is an upgrade failure and DVM lockouts.
- Never manually upgrade Pano Direct Service. Since you’re using a GPO to upgrade you don’t need to upgrade from the DVM directly; however, your end users might not be aware and might try to upgrade on their own, resulting in duplicate entries (also called *phantom program entries*) in **Add or Remove Programs**.

1. Add a new software package and point it to the package(s) that you want to upgrade:

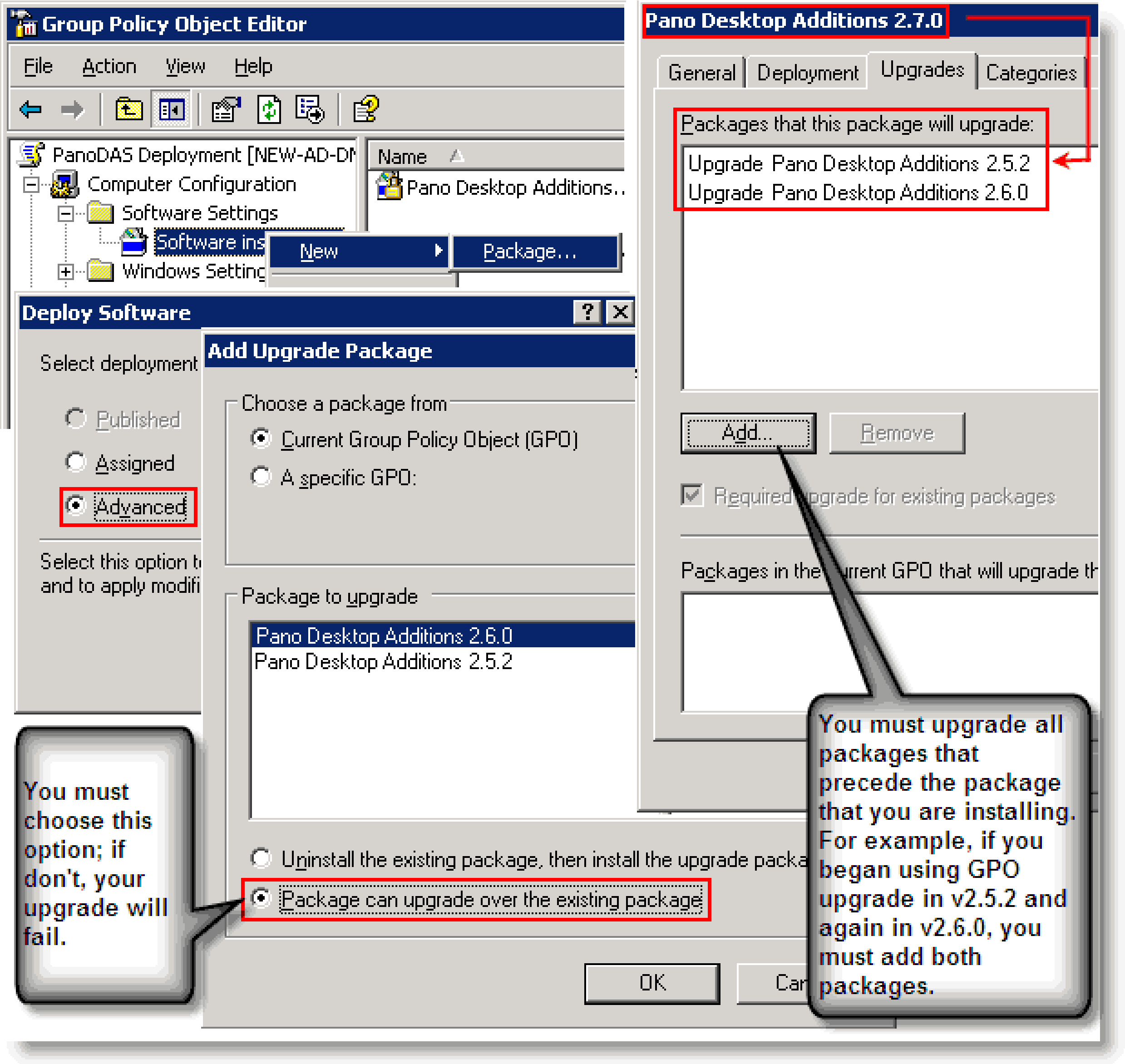
   a. From the Group Policy Editor, choose **Computer Configuration** > **Software Settings** > **Software Installation** > **New** > **Package**, then browse to the new package.

   b. From the Deploy Software dialog, select the **Advanced** radio button.

   c. Do the following:

   - From the Upgrade tab, add all packages that precede the package you want to install. For example, if you began using GPO upgrade in v2.5.2 and again in v2.6.0, you must add both packages.

- From the Add Upgrade Packages dialog, select **Package can upgrade over the existing package**, then click **OK**. You must select this option. If you choose the other option the upgrade will fail.



○ Published
○ Assigned
● Advanced

Choose a package from
● Current Group Policy Object (GPO)
○ A specific GPO:

Package to upgrade
Pano Desktop Additions 2.6.0
Pano Desktop Additions 2.5.2

○ Uninstall the existing package, then install the upgrade packa
● Package can upgrade over the existing package

Packages that this package will upgrade:
Upgrade Pano Desktop Additions 2.5.2
Upgrade Pano Desktop Additions 2.6.0

☑ Required upgrade for existing packages

You must choose this option; if don't, your upgrade will fail.

You must upgrade all packages that precede the package that you are installing. For example, if you began using GPO upgrade in v2.5.2 and again in v2.6.0, you must add both packages.

2. Restart all the DVMs so that the Pano Direct Service on those Pano System Endpoints will be upgraded to the newer version.

   A restart allows your users to save their data and close applications. If you want to force a restart you need to perform a reset instead. Forcing your users to log out will not initiate the GPO upgrade. You must either restart or reset the DVMs.

3. Verify that all the DVMs are running the new version of Pano Direct Service.

   If a DVM is running an older version it's likely that the cause is a restart failure. A restart, as opposed to a reset, is a best practice in initiating an upgrade; but, some users don't save and close their applications as instructed, and the GPO cannot upgrade if the DVM doesn't restart. In this case, you'll need to perform the upgrade again.

Check Status of Virtualization Tools on DVMs

For VMware, as outlined in Install Windows, for best performance, the latest virtualization tools should be running on each DVM. The Pano Controller draws attention to DVMs that should be updated.

1. Log on to the Pano Controller.
2. Click on the **DVMs** tab.
3. Observe the value in the DVM Tools State column. For VMware, Pano Controller reports the status of virtualization tools based on the information in vCenter Server.

Color Bar	DVM Tools State	Description
n/a	OK	Virtualization tools are installed and up to date.
Red	Not Running	Service is not running. For VMware, depending on your ESX version, sometimes vCenter Server reports the status incorrectly. You might need to restart the service. See also ID 4335.
Red	Needs Upgrade	Virtualization tools on the DVM are out of date. If you just upgraded and the Pano Controller still reports that virtualization tools are out of date, restart the DVM.
Red	Not Installed	The user is logged on to the DVM.

If required, Upgrade Virtualization Tools on DVMs

Upgrade Virtualization Tools on DVMs

You do not need to put the DVM into maintenance state prior to an upgrade. Users can be logged in when you perform the upgrade. However, a reboot is required to complete the upgrade. For VMware, this upgrade is equivalent to performing the Automatic Tools Upgrade through the vSphere Client.

1. Log on to the Pano Controller.
2. Click on the **DVMs** tab.
3. Select the DVM, and then, from the Desktop drop-down button, choose **Upgrade Tools**.
4. When prompted to confirm your selection, click **Upgrade Tools**. If the user is logged in, the end user sees an installer flash across the screen. Shortly thereafter, the installer prompts the end user to reboot.

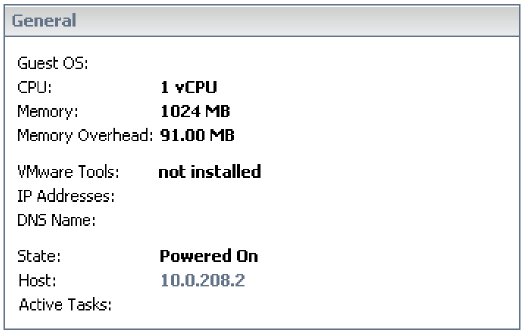
For VMware users: Check Status of Pano Controller VM's VMware Tools

Check Status of Pano Controller VM's VMware Tools

The Pano Controller VM ships with a version of VMware Tools installed; keep it up to date on the Pano Controller VM. VMware Tools often become out of sync with your ESX host when you upgrade your host. Always use the latest version of VMware Tools.

1. Log on to vCenter Server.
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

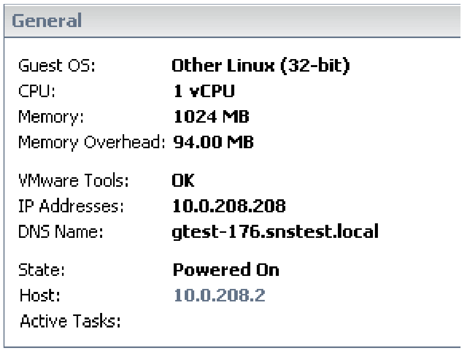


General

Guest OS:
CPU: 1 vCPU
Memory: 1024 MB
Memory Overhead: 91.00 MB

VMware Tools: not installed
IP Addresses:
DNS Name:

State: Powered On
Host: 10.0.208.2
Active Tasks:



General

Guest OS: Other Linux (32-bit)
CPU: 1 vCPU
Memory: 1024 MB
Memory Overhead: 94.00 MB

VMware Tools: OK
IP Addresses: 10.0.208.208
DNS Name: gtest-176.snstest.local

State: Powered On
Host: 10.0.208.2
Active Tasks:

What to do next: If your VMware Tools are outdated, go to Update Pano Controller VM's VMware Tools.

Update Pano Controller VM's VMware Tools

The Pano Controller VM ships with a version of VMware Tools installed. Ensure that you keep VMware Tools up to date on the Pano Controller VM, especially for major versions.

Before You Begin: Upgrade Pano Direct Service

1. Ensure that the Pano Controller VM has a DVD/CDROM device: power off the Pano Controller VM, right-click on the Pano Controller VM, click **Edit Settings**, then use the **Add Hardware** wizard. For detailed instructions about how to add hardware devices, go to the *Adding New Hardware* section of the VMware vSphere 4.0 U1 Basic System Administration Guide.
2. Using the vSphere Client, connect to vCenter Server or the ESX host to access the Pano Controller VM.
3. Right-click on the Pano Controller VM and choose **Install VMware tools**.
4. Log on to the Pano Controller VM as `root`.
5. From the Pano Controller console Main Menu, select option **5 - 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-<xxxx>.tar.gz
# umount /dev/cdrom
```

8.Run the VMware Tools tar installer, answering the on-screen configuration questions. Press Enter to accept the default value.

```
# cd vmware-tools-distrib
# ./vmware-install.pl
```

9.Log off the root account.

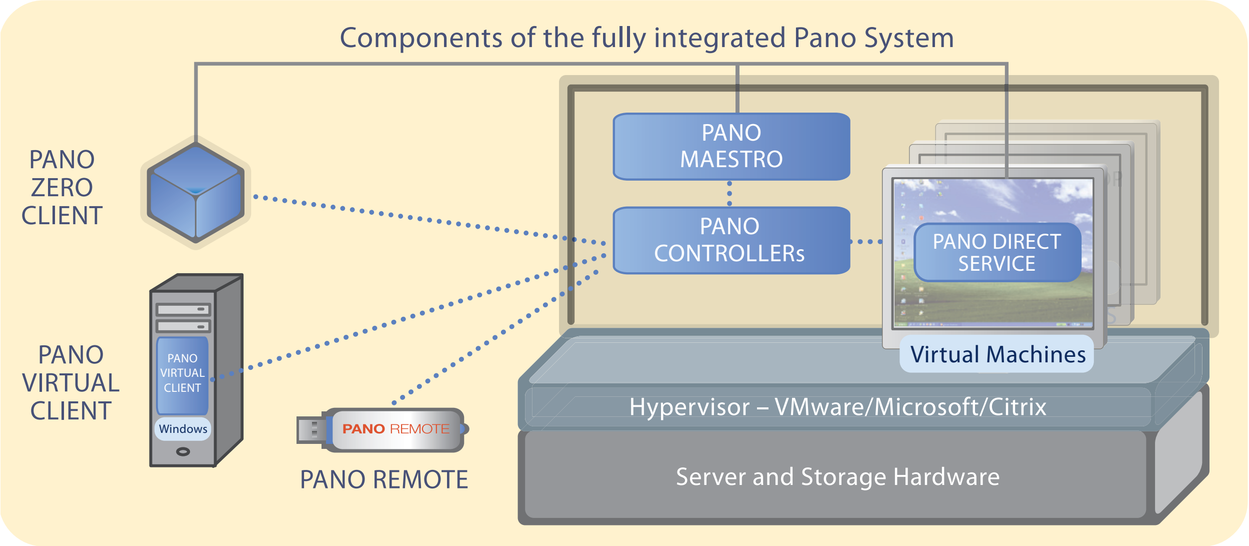
```
# exit
```

4

Pano System Overview

The Pano System consists of hardware zero client endpoints, software endpoints, virtual desktop software services, and centralized management software, all purpose-built for virtual desktops and running atop your server-based virtualization infrastructure.

The Pano System enables organizations to centralize desktop computing inside the data center rather than having it scattered across user's desktops. Rather than having to deploy, support, and secure a copy of Windows on a PC or laptop at every users desk, you can run the same operating systems and applications within desktop virtual machines (DVMs) on servers using the Microsoft, VMware, or Citrix virtualization platforms. This centralization can radically reduce the TCO of delivering desktop computing while also simplifying deployment, reducing the time and effort for support, and substantially cutting energy consumption compared to PCs.



Users connect to their virtual desktops using one of several Pano System endpoints. Pano Direct Service software runs in the OS of each virtual machine, and communicates with the user's endpoint. The Pano Controller manages it all.

- Pano System Endpoints - Pano Logic provides a choice of endpoints from which users can connect to their Windows 7 or XP virtual desktops. Each endpoint has its own set of advantages. You can use one or more of these endpoints in your environment.
- Virtualization Platform - A lightweight Windows service that resides on each desktop virtual machine. This service connects the Windows drivers in the desktop virtual into the Windows drivers and sends the display, keyboard, mouse, audio and USB peripheral data over the network to the Pano System Endpoint. This service links peripherals attached to the Pano System Endpoint to the unmodified Windows drivers on the virtual machine. This design guarantees that all existing Windows drivers work without modification.
- Pano Controller Group Architecture - The Pano Logic Controller provides common management across all endpoints. It offers centralized service and web-based management interface. Pano Controller lets administrators manage the entire virtual desktop installation by integrating with existing directory services and virtualization

platform managers. Pano Controller acts as a connection broker, integrating with your directory service for user authentication. Additionally, Pano Controller supports connecting a Pano System Endpoint to a user's desktop virtual machine with a third-party connection broker such as VMware View and Citrix XenDesktop.

The Pano Controller has been enhanced to a role-based model. Pano Controllers can be grouped for greater scalability and more diverse deployment options. Pano Controller functionality is configured by enabling or disabling either or both of two roles:

- **Full Mode** is the default configuration and provides full functionality. It includes both Zero Client Controller and Virtual Desktop Broker functionality.
- **Zero Client Controller** (ZCC) role provides support for client discovery, authentication, and login services.
- **Virtual Desktop Broker** (VDB) role provides support for Pano connection brokering.

While some customers will run Pano Controller in Full Mode using a single Pano Controller instance, customers requiring advanced scalability and deployment options should choose to take advantage of the Zero Client Controller and Virtual Desktop Broker roles for a highly scalable, highly flexible enterprise architecture enabled by Pano Controller groups.

Differentiated Pano Controller roles and groups enable flexible third-party broker support and enhanced Pano System scalability. Each Pano Controller groups consists of a primary Pano Controller, a secondary Pano Controller and up to four auxiliary Pano Controllers.

- Pano Maestro for Centralized Management - A centralized management access point to manage the configured Pano Controller groups. Centralized management includes collecting inventory data from all the devices managed in the groups, integrating with Directory Services (AD) for access authentication, and providing license configuration and enforcement. Pano Maestro is installed on a separate VM.
- Pano Controller - An optional security server for Pano Remote which is run in the DMZ. It connects your internal LAN and the Internet. Pano Gateway provides for secure Pano Remote connections from external, insecure networks. It runs as a plug-in on Window Server 2008 R2 Remote Desktop Services (formerly called Terminal Services Gateway).
- Next:Pano ControllerVirtualization Platform - The underlying virtualization platform that allows multiple virtual machines to run on shared server resources.
- **Hypervisors** – Software that allows multiple virtual machines (VMs) to run concurrently on a host server. Hypervisors host both DVMs running on desktop servers and host system VMs, like Pano Controller, or platform tools on infrastructure servers.
- **DVM Management and Provisioning Tools** – Various platform-specific tools, often deployed as VMs on infrastructure servers, which are used for automated provisioning, management tasks or optimizing the storage used by DVMs.
- **Client Tools** – Platform-specific software installed into the DVM’s operating system to provide connections to the supporting hypervisor and platform DVM management tools.

Next: Pano System Endpoints for endpoint options; Pano Direct Service for the Windows drivers.

Pano System Endpoints

Pano System endpoints provide several choices for users to connect to their desktop virtual machines and users can freely roam between different endpoints by simply logging into their running Pano virtual desktop:

- Pano Zero Client - Ideal if you want the highest level of security and reliability at the lowest total cost of ownership (TCO). The Pano Zero Client hardware endpoint provides a compact, highly reliable and secure means to connect to Pano virtual desktops over a LAN. Pano Zero Clients effectively extend the pure hardware; they do not run any software of any sort on the endpoint itself.

  Pano Zero Clients have the following characteristics:

  - Hardware only - no operating system, drivers or software on the endpoint.
  - No endpoint processing - do not contain a CPU, memory or storage.
  - Reliable and compact - no moving parts, uses only 6.5 watts and is just 3.5” square.
  - LAN-based - has a 100-Mbit Ethernet port.
  - PDP - uses the Pano Direct Protocol for communications
- Pano Virtual Client - Lets you repurpose a standard PC or laptop as a Pano System endpoint, freeing you to benefit from virtual desktops until you can migrate to a Pano Zero Client. The Pano Virtual Client is software that lets you repurpose PCs or laptops to work as Pano System endpoints, letting you benefit from virtual desktops even if locked into a lease or other obligation that requires PCs.

  The Pano Virtual Client has the following characteristics:

  - software only - software client installed via Active Directory GPO
  - Windows-based - requires a Windows XP or 7 PC or laptop as a host
  - Flexible - allowing a smooth transition from PCs to virtual desktops and zero clients
  - LAN-based - requires an Ethernet connection but will also work over Wi-Fi with limitations
  - PDP - uses the Pano Direct Protocol for communications
- Pano Remote - Ideal if you have users who need access to their virtual desktops when working from home or on the road. Generally, is used as an accessory to a Pano System Endpoint.

  Pano Remote is a software client delivered on a secure serialized USB key and optimized for remote access over low bandwidth, high latency wide area networks (WANs). Pano Remote is commonly used by people who access their virtual desktop in the office, from their home and while on the road. Pano Remote has the following characteristics:

  - software on hardware - software must be run from secure serialized USB key.
  - Windows-based - requires a Windows XP, Vista, or 7 PC or laptop as a host.
  - LAN or WAN-based - can run both over internal LAN and over WANs like the Internet.
  - no install - runs on host PC without any installation, leaves nothing behind
  - secure - uses optional Pano Gateway and RSA SecurID passcodes for added security.
  - RDP - uses the Microsoft Remote Desktop Protocol for communications.

Pano Zero Client

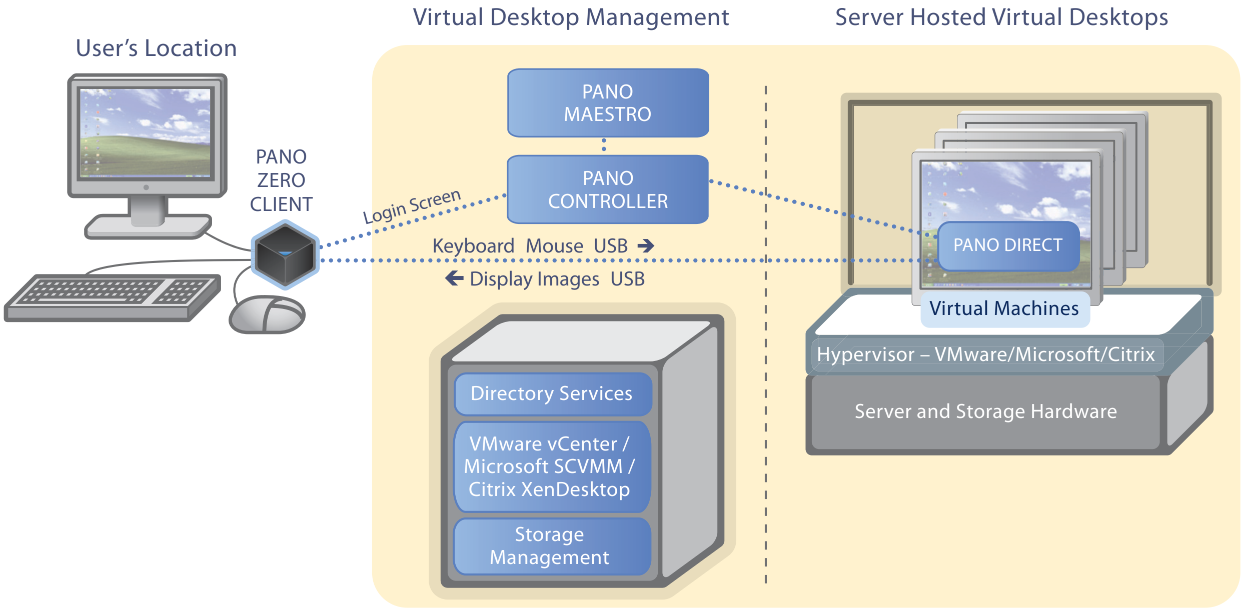
The Pano System Endpoint is specifically designed for server-based desktop virtualization. Because the Pano System Endpoint is 100% hardware, all software can now in the data center, where all your software can be centrally managed and effectively protected.

The Pano System Endpoint 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 Support for USB Devices.

The Pano System Endpoint is stateless — it contains no intelligence or software memory — and is controlled by centralized services such as the Pano Controller and DHCP. The Pano System Endpoint includes a single button — the Pano Button™ — that initiates out-of-band control of a user's virtual desktop. By simply pushing the Pano Button, a user can disconnect from the desktop, instantly securing the work environment, while preserving the state and operation of the virtual desktop.

A Pano System Endpoint consumes only 6.5 watts of power with a monitor connected — around 5% of the energy consumed by a traditional desktop computer — and contains no moving parts or compute resources that would require frequent upgrades or replacement. Also, a Pano System Endpoint has a configurable sleep mode that consumes less than.2 watts of power.

A Pano System Endpoint provides a desktop experience to the user by communicating with Pano Controller Group Architecture 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 Desktop layers are hosted in the data center.)



Pano Virtual Client

Pano Virtual Client is a software client that is installed on a Windows XP or 7 PC or laptop to repurpose it as a Pano System endpoint. The Pano Virtual Client acts as a replacement shell (in place of Windows Explorer) essentially taking over the PC to make it work as a dedicated endpoint. While it is running users will not have access to the local Windows operating system and unlike Pano Remote it will not run in a window on the host PC. The was done both to improve security of the host PC and to provide tighter integration and higher user experience performance.

Pano Virtual Client is typically installed using Active Directory group policy objects (GPOs) but can also be installed manually with some limitations. If desired it can be uninstalled, allowing the host PC to be used as a regular Windows desktop.

Pano Virtual Client is designed to work over a LAN and does not provide the same level of support for WANs and security as Pano Remote and Pano Gateway. If you have users that usually access their virtual desktop using a Pano Virtual Client in the office they can still use Pano Remote when working from home or travelling.

Pano Remote

Pano Remote is a combined hardware/software solution that allows your always-on-the-go end users to conveniently access their desktop virtual machines from any PC and from a remote location. It is delivered as a secure serialized USB key and allows administrators to register and disable keys from Pano Controller.

Pano Remote enables users to reach their Pano desktop virtual machine from a remote location over wide-area networks like the Internet. Pano Remote enables users to easily access their Pano virtual desktops when they are away from the office, whether working in the evening or when travelling.

Pano Remote User Experience

Pano Remote provides access to a DVM either in a window or using the full screen. The user experience within Pano Remote is generally not a capable as that provided by Pano Zero Clients, with limitations in both display updates (such as with full screen video) and USB device support. These limitations are mostly the result of Pano Remote using the general-purpose Microsoft Remote Desktop Protocol rather than the optimized Pano Direct Protocol. Administrators can set policies for Pano Remote in the Pano Controller console to allow or restrict access to local printers and drives along with controlling transfer of data on the clipboard between the virtual desktop and host PC’s operating system.

Pano Remote vs Pano Zero Client

With Pano Remote, your end users can access their DVMs even when they are not sitting in front of a Pano System endpoint like the Pano Zero Client or Pano Virtual Client. A Pano Zero Client is still the primary way of accessing a DVM, but Pano Remote offers a secondary way of gaining access. Because of limitations in both the user experience performance and support for USB devices, Pano Remote is generally not suitable as the sole means for a user to access their virtual desktops.

RSA SecurID for Pano Remote

With Pano System 6.0 we’ve added optional support for using RSA SecurID tokens to provide two-factor authentication for Pano Remote logins. This option is configured on the Setup tab in the Pano Controller console and applies to all Pano Remote logins to that Pano Controller (or group of Pano Controllers linked by Pano Maestro).

When activated, the login dialog for Pano Remote will show an added field labeled “Passcode”. Users would then enter a combination of their RSA PIN and the one-time password generated by their RSA SecurID token. Pano Controller then uses the entered passcode to authenticate the user against the RSA Authentication Manager server in addition authenticating the entered user name and password with your directory service such as Active Directory.

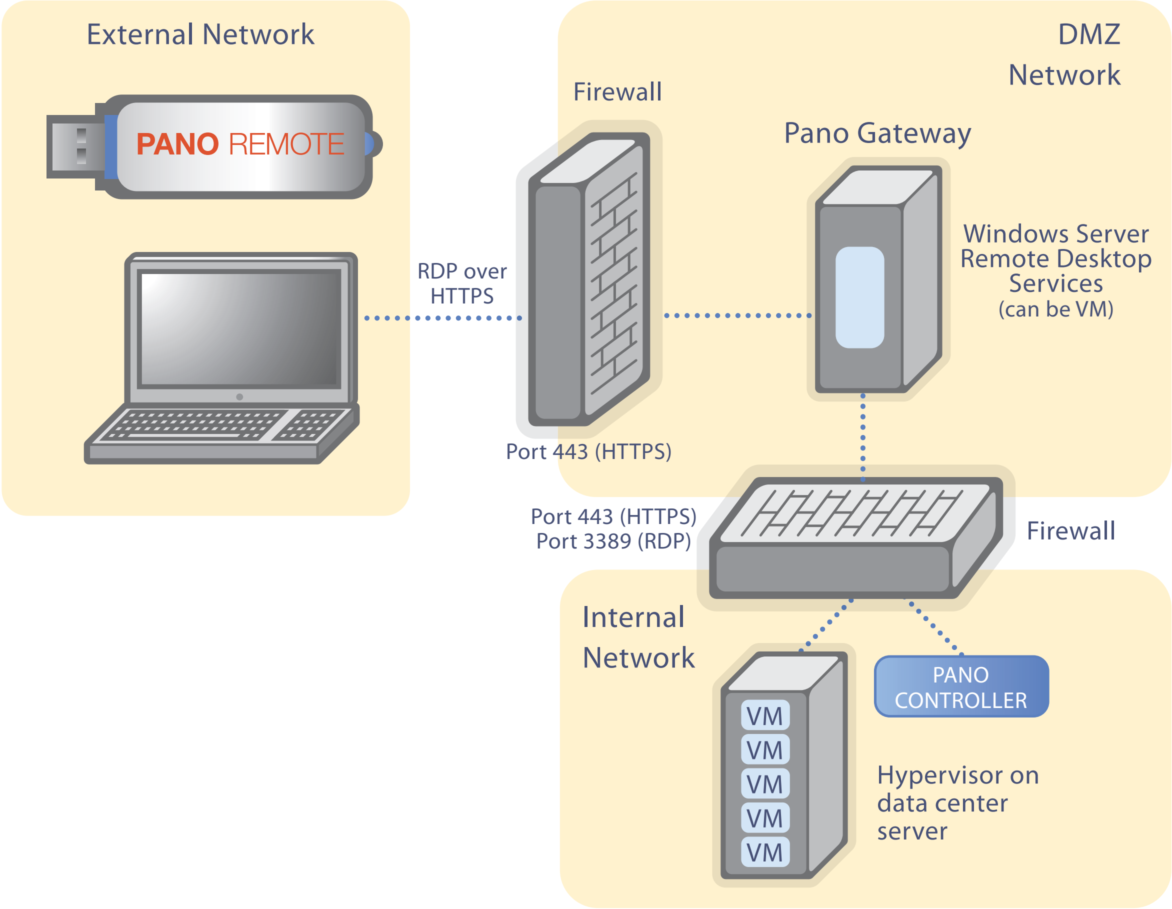
Note that as this new feature is mediated by Pano Controller it will work with any version of Pano Remote (and Pano Gateway) including even the legacy unserialized Pano Remote keys issued prior to Pano Remote 4.5.

Pano Gateway

Pano Gateway is an optional security server bundled with Pano Remote that provides secure connections from external networks using Microsoft Windows Server 2008 Remote Desktop Services (formerly called Terminal Services Gateway) as supporting infrastructure.

Pano Gateway allows your end users to use Pano Remote from outside your firewall without the need for VPN software or hardware. The Gateway uses standard secure protocols (RDP via HTTPS/Secure Sockets Layer) to connect to the Pano Gateway server, and, in turn, to the virtual desktops, simplifying the configuration of firewalls and security policies.

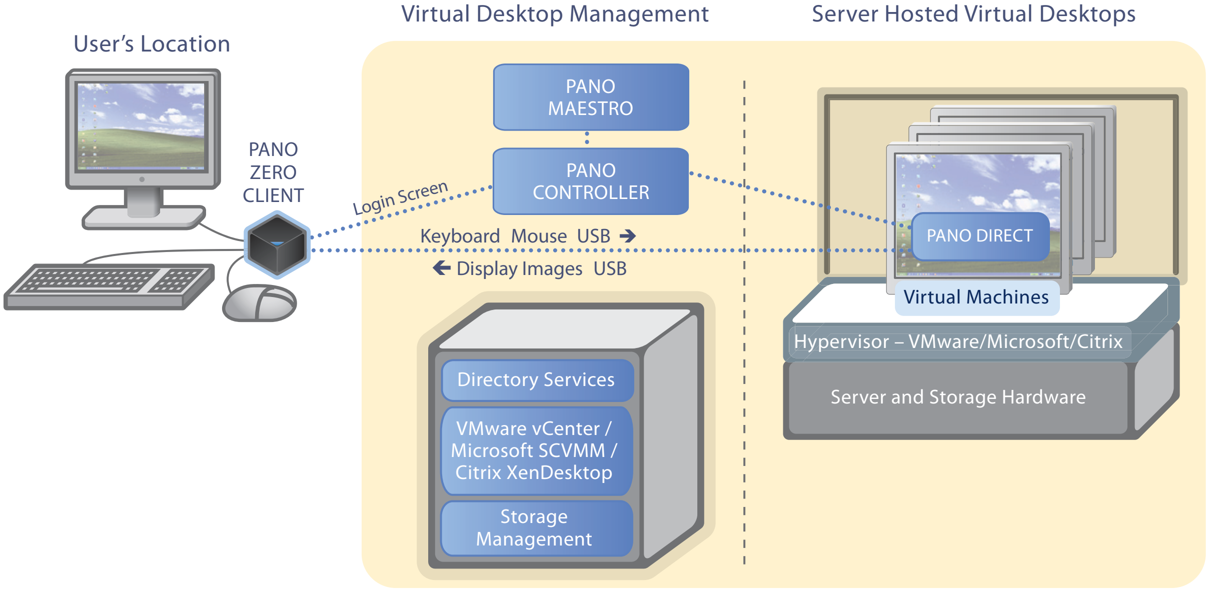
Pano Gateway ensures that users get suitable performance in the remote Windows desktop, even over connections like consumer-level DSL or cable modems. Performance is usually better over higher speed connections, however.



Pano Direct Service

This lightweight Pano Direct Service (PDS) runs on each DVM. The Pano Direct Service 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 Direct Service Service, allows individual users to set their personal preferences for keyboard, mouse, display and audio settings within their DVM.



Next:Pano Controller

Pano Controller

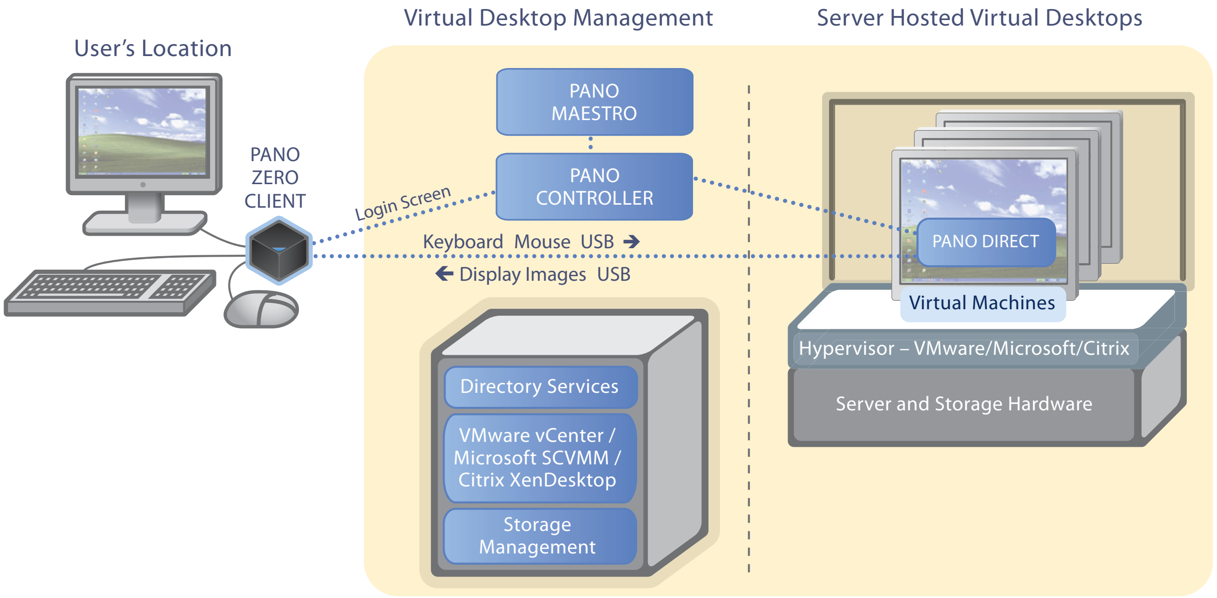
Pano Controller is a centrally-hosted management console that is delivered as a virtual appliance. Typically, Pano Controller runs as a virtual machine located on the same host servers as your desktop virtual machines. You can add multiple Pano Controllers to your configuration to meet your availability and scalability requirements.

Pano Controller provides secure access to virtual desktops by leveraging services such as Microsoft Active Directory and RSA Authentication Manager for user and remote access authentication.

Pano Controller controls and deploys desktop virtual machines by leveraging virtualization management systems such as Microsoft System Center Virtual Machine Manager (SCVMM) and VMware vCenter Server.

Pano Controller connects end users and Pano System endpoints to desktop virtual machines using its internal connection broker service or an external third-party connection broker like Citrix XenDesktop Controller or VMware View Connection Server.

Note: In versions prior to Pano System 5.0 this component was called Pano Manager. It is now called Pano Controller.



Pano Controller has built-in connection broker functionality. As a connection broker, Pano Controller uses your Directory Services (typically Microsoft Active Directory) and the management tools provided by the virtualization provider (such as VMware vCenter Server) to connect a Pano System endpoint to a user's selected DVM. The connection broker is responsible for a couple of important tasks, specifically:

- Receiving the user credentials that users enter in the Pano user login screen, and relaying that information to the directory service for authentication.
- Checking its internal database to see which DVMs are associated with the authenticated user or, for device-based connections, with a specific Pano System endpoint.
- Communicating with Pano Direct Service and platform-specific VM tools installed in the DVMs so that the correct virtual desktop is connected to the correct user.

There must be at least one connection broker for any virtual desktop deployment.

Next: Pano Controller Roles

Pano Controller Roles

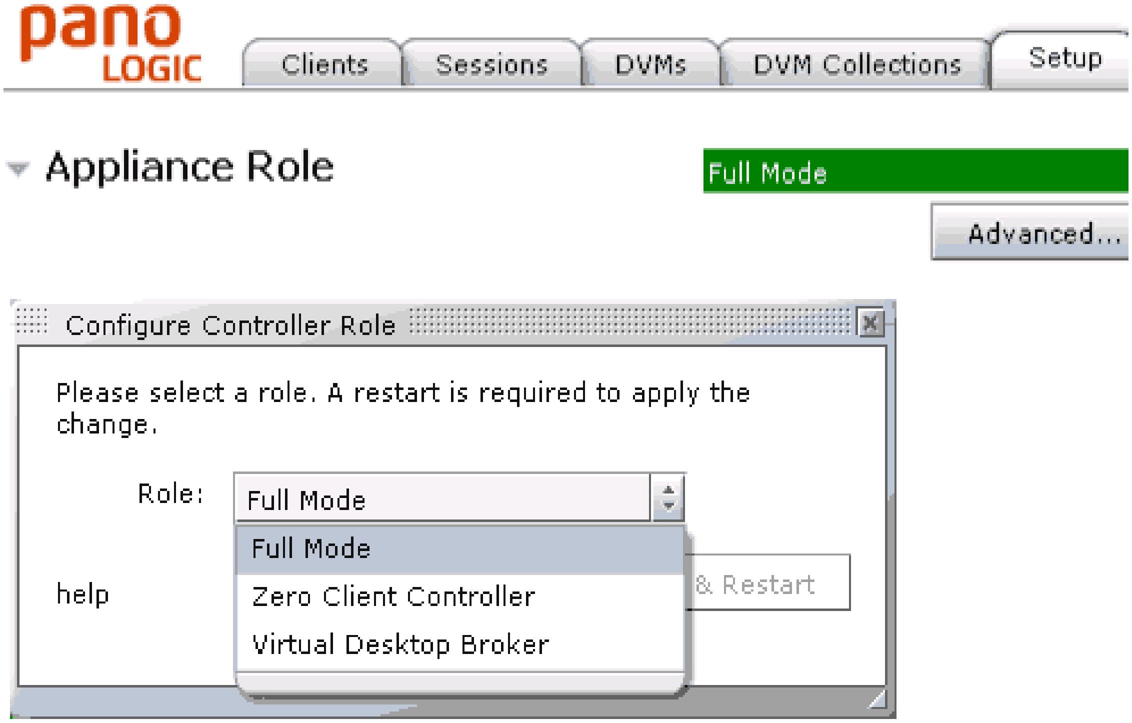
The administrator can enable or disable these roles by selecting the appropriate Appliance Role. The Pano Controller must have at least one of these roles enabled. The possible options for the Appliance Role are:

- **Full Mode** - By default the Pano Controller virtual appliance comes configured in Full Mode. In this configuration, the Pano Controller is able to perform all tasks including discovery and control of Pano clients and brokering and provisioning of desktops. Customers who have deployed earlier versions of Pano Controller will want to run their Pano Controller in Full Mode because it is functionally equivalent to earlier versions of Pano Manager. In general, Full Mode is the configuration best suited to most environments.
- **Zero Client Controller** - As an advanced setting, the administrator may choose to enable only the Zero Client Controller role. In this configuration, the Pano Controller only discovers and controls Pano Zero Clients, Pano Virtual Clients, and Pano Remote clients. A separate connection broker service is required. This separate connection broker service

can be another Pano Controller configured in Virtual Desktop Broker role, XenDesktop or VMware View.

- **Virtual Desktop Broker** - As an advanced configuration, the administrator may choose to enable only the Virtual Desktop Broker role. This is valid when you have configured a separate instance of Pano Controller running as a Zero Client Controller for scalability.

The Appliance Role is configured in the Pano Controller console on the Setup tab:



Appliance Role: Full Mode

Please select a role. A restart is required to apply the change.

Role: Full Mode

Next: Pano Controller Group Architecture

Pano Controller Group Architecture

For scalability with high availability and load balancing, you can add additional Pano Controllers to your configuration to form a Pano Controller group. Each Pano Controller groups consists of a primary Pano Controller, a secondary Pano Controller and up to four auxiliary Pano Controllers to support up to a total of six Pano Controllers.

With third-party connection brokering, Pano Controller groups can be configured to support up to 10,000 DVMs/clients. Users can roam across Pano Controller groups for flexible DVM access.

Note: Scalability and redundancy groups from previous Pano Manager configurations are converted into a Pano Controller group.

See Deployment Planning and Pano Maestro for Centralized Management

Pano Maestro for Centralized Management

Pano Maestro provides a centralized management access point to manage Pano Controller groups. Centralized management includes collecting inventory data from all the devices managed in the groups, integrating with Directory Services (AD) for access authentication, and providing license configuration and enforcement.

Pano Maestro is installed on a separate VM and manages up to five Pano Controller groups. Pano Maestro features include:

- Centralized management, status monitoring, provisioning from single management console.
- High-level view and status of Pano Controller Groups and group members. The Pano Controller Group status shows the cumulative status of all group members. Any changes in member status are propagated to the Group status. For example, when one member enters a Warning state, the Pano Controller Group status changes to Warning.
- Functional interface tabs to manage multiple controllers at the same time.
- Optional drill down to each of member's Pano Controller console management interface.
- Management and enforcement of Pano System licenses across Pano Controller groups throughout the customer network.
- Seamless authentication and access to all the members using Directory Services.
- Flexible Pano Maestro display and management options.

Pano Maestro can be set up on same virtualization stack using the same server hardware that is used for setting up the Pano Controller. However, Pano Maestro must be set up on separate virtual machine.

Next: Virtualization Platform

Virtualization Platform

Hypervisor (virtualization) software allows multiple virtual machines to run concurrently on a host server. Pano Logic’s system leverages the three industry-leading server-based virtualization platforms to abstract processor, memory, storage and networking resources into multiple virtual machines, to give you greater hardware utilization and flexibility. Hypervisors are used both to host desktop virtual machines (DVMs) running on desktop servers and to host system VMs like Pano Controller or XenDesktop Controller on infrastructure servers.

The Pano Controller plays well with hypervisors, such as vSphere ESX/ESXi, Hyper-V, and XenServer. XenServer and vSphere ESX are type 1 or bare metal hypervisors that require no other host operating system (OS). They interact directly with the server hardware rather than relying on the host OS driver stack. Because of this, you need to be sure that your server hardware, including RAID controllers and network interface cards, are on the hardware compatibility list for your selected hypervisor. For a complete list of supported virtualization infrastructure, go to Supported Virtualization Platforms.

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

5

Understanding Virtual Desktops

The Pano System is designed to make it easy for you to deploy large numbers of virtual desktops for users. It offers several types of virtual desktops, and several methods for creating and managing them.

You should understand what Pano means by the following terms:

- DVMs
- DVM Collections
- Types of Collections
- Automated Deployment Concepts
- Templates
- Virtual Desktop Management
- Scalability

DVMs

A desktop virtual machine (DVM) is a virtual machine that runs an operating system such as Windows 7. DVMs run on top of a virtual infrastructure hosted on one or more servers.

From the perspective of a virtual infrastructure, there's no difference between a DVM and a standard virtual machine. The same operations that can be performed on a standard virtual machine can be performed on a DVM.

When inside the enterprise network, users can connect to DVMs through Pano Zero Client or Pano Virtual Client as outlined in Log On To DVMs as End User. When outside the enterprise, users can connect by running the Pano Remote access application on another computer. Pano Remote is described in Deploy Pano Remote.

Next: DVM Collections

DVM Collections

It would be tedious to have to manage hundreds of desktop virtual machines one by one, manually, so Pano created DVM Collections. When you create a collection, you specify the level of user control and personalization. How you create and use collections is essentially the same, regardless of the virtual machine system you are using.

You can create as many collections as you wish; defining each according to the level of user control you want to make available to user.

Keeping Track of DVMs

In order to have a flexible, platform-independent method of tracking hundreds of DVMs, Pano assigns each one a Globally Unique Identifier. The DVM location within your overall storage hierarchy does not matter, because the Globally Unique Identifier is used to track the DVM. This tracking method makes it easy for collections to manage lists of DVMs, instead of tracking DVMs by folder membership.

To associate DVMs with a DVM Collection, you pick the DVM from within a collection view. To view a new DVM in the DVMs view, you simply associate the new DVM with a collection, manually.

When a new DVM is created in a folder that is not managed by a collection, the DVM does not appear in the DVM view. However, when the Pano Controller automatically deploys a new DVM from a managed collection, the relationship to a DVM Collection is automatically updated.

Related Topics

Types of Collections

Create and Manage DVM Collections–VMware & Hyper-V

Types of Collections

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**

User Based Collections are used when you want the user to be able to access “their” computer; in other words, just as if the user had a PC on their desk.

The DVM assignment is based on the identity of 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.

- **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 System Endpoint to always connect to a specific DVM. This is useful for kiosk, Point-of-Sale, and other applications where the role of the machine is the defining element, rather than the identity of the user. Note that you can still require the user to authenticate; so, for example, you can define a Point-of-Sale role and still require individual cashiers to log in.

For more information, go to Device Based Collections.

- **Third-Party Connection Broker Collections**

This special type of collection works in conjunction with VMware View Connection Server (formerly known as VMware VDM) and Citrix XenDesktop. Use of VMware View and Citrix XenDesktop with Pano Controller is optional. For details, go to Set Up Desktop Brokering. and Pano Controller Configuration.

User Based Collections

With User Based Collections, Pano System Endpoints display the Pano user login screen whenever the endpoint is not connected to a DVM. Users simply type their credentials at the Pano user login screen to connect to their assigned DVMs.

There are several User Based Collections from which you can choose. Not all collections are available with all virtual environments. The exceptions are:

- Citrix Xen Desktop is the only DVM that is supported for XenDesktop. It is described in Create DVM Collections–XenDesktop. This collection does not work with VMware or Hyper-V.
- VMware View Connection Server receives user credentials from the Pano Controller (if so configured). VMware View specifies the appropriate desktop virtual machine for the session and the Pano Controller connects the Pano System Endpoint to the appropriate desktop virtual machine. DVM provisioning is managed through VMware View. In this scenario, the Pano Controller establishes the connection between the Pano System Endpoint and the DVM. The Pano Controller does not communicate with vCenter Server to start the DVM; rather, VMware View handles these tasks.

User Based Collection Types

• Pooled Desktops

A Pooled Desktops collection type is most appropriate for a set of users that all use the same set of applications. This collection is commonly used in a call-center environment where there are work shifts and where only a subset of users need a desktop at any given time. The intent of this collection type is to save computing resources by not having each user assigned to a specific desktop.

All users have the same desktop configuration because these desktops are not permanently assigned to these users. However, you can use Windows roaming profiles and document redirection to allow users of a Pooled Desktops collection type to have some degree of personalization. Keep the size of users' profiles small in order to keep login times short.

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 can be created automatically from a specified template and assigned to users by the Pano Controller. The set of users that are entitled to use the collection is specified in the collection properties (see Create DVM Collections).

Assignment of DVMs in a Pooled Desktops collection 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.

• Permanently Assigned Desktops

A Permanently Assigned Desktops collection type is most appropriate for users that require dedicated virtual desktops, with the ability to customize their virtual desktops and save files locally.

This collection type is most commonly used for a typical office environment where users’ PCs are being replaced by Pano System Endpoints.

The desktops are created automatically and permanently assigned to users upon first login. After Pano System assigns a DVM to a user, that user retains the same dedicated desktop until it is unassigned by the Administrator.

The set of users that are entitled to use the collection is specified in the collection properties (see Create DVM Collections). After the Pano System assigns a user to an available DVM, the Pano System gives that user the same dedicated DVM every time the user logs on with the same credentials.

Assignment of the user to the DVM is automatically established the first time the user logs on to the DVM. Alternatively, you can assign a particular DVM to a user through the Management User Interface (MUI).

Permanently Assigned Desktops collection types allow you to leverage automated deployment, while providing users a dedicated DVM that they can customize and personalize.

- **Existing Desktops**

If you are evaluating the Pano System, or are moving existing users' real PCs to a virtual machine with VMware Converter, you will probably want to use the Existing Desktops collection type.It creates a one-to-one mapping between a user and a DVM that has been created through some other process other than Pano Controller's automated process. It also permanently associates that user with the new DVM.

This collection is the least-used collection type in a production environment.

Each Existing Desktops collection type should contain only one DVM; otherwise, the user will connect arbitrarily (and randomly) to one virtual machine in the collection. However, you *can* create multiple Existing Desktops collections.

Pano System temporarily allocates the DVM to a user automatically upon login. You can manually assign users to DVMs, if they are part of the vCenter Server inventory. The set of users that are entitled to use the collection is specified in the collection properties (see Create DVM Collections).

Device Based Collections

Device-Based Collections allow you to assign Pano System Endpoints, 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. You can find kiosks in public places such as libraries, company break rooms or corporate lobbies.

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 user 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.

Creating a Device-Based Collection is similar to creating a User Based Collection. Device-Based Collections take advantage of the automated deployment features of the Pano Controller, 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 Pano Controller administrator interface or by logging on for the first time from a device through the Pano user login screen.

Once assigned, the Pano Controller 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 System Endpoint to automatically log on to the DVMs using the *same* credentials throughout the collection.

DVMs are automatically created from a specified template. Pano System Endpoints are assigned to specific DVMs either through the Management User Interface (MUI) or by logging on through the device for the first time. As soon as the Pano System Endpoint comes up on the network and connects with the Pano Controller, the device automatically connects and logs in to the assigned DVM. The login credentials for the automatic login for 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 System Endpoint to automatically log on to the DVMs using *unique* credentials for each login device.

A Different Accounts w/ Automatic Login collection type allows you to set up Pano System Endpoints and their corresponding DVMs to act like kiosks. 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.

Rather than displaying the Pano user login screen, the Pano System Endpoint automatically connects and logs on to the associated DVM using a specified account name and password.

A 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.

DVMs are automatically created from a specified template. Pano System Endpoints are assigned to specific DVMs either through the Management User Interface (MUI) or by logging on through the device for the first time. As soon as the Pano System Endpoint comes up on the network and connects with the Pano Controller, the device automatically connects and logs on to the assigned DVM. Upon automatically logging on 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 System Endpoint to connect to a DVM, but not log on to the actual DVM (i.e. display the Windows Login screen).

A Windows Login collection type allows you to set up a Pano System Endpoint and a corresponding DVM to act like a general purpose Windows computer. This collection type is useful if:

- You require users to use biometric devices (for example, fingerprint scanner to support fingerprint recognition) for authentication, or
- You have users that will always connect to a DVM from the same Pano System Endpoint and desire the same look-and-feel that they experience from a Windows computer, namely a Windows Login screen as opposed to a Pano user login screen.

The Pano System Endpoint automatically connects to the DVM, but does not log on. The user must authenticate to Windows prior to using the DVM.

You can assign Pano System Endpoints to specific DVMs either through the Management User Interface (MUI) or by logging on through the device for the first time.

As soon as the Pano System Endpoint is discovered on the network and communicates with the Pano Controller, the Pano System Endpoint automatically connects to the assigned DVM. Users must type their credentials at the Windows login prompt (see Supported Third-Party Login Screens).

Automated Deployment Concepts

Automated deployment is the ability to configure Pano Controller to automatically create new desktop virtual machines by:

- Cloning virtual machines using *Templates.*
- Automating Windows Sysprep process using a *Customization Specification.*

You can automatically provision new DVMs by cloning templates. Also, by executing customization specification scripts, you can perform automated sysprep on individual DVMs generated from the template.

Pano Logic designed its solution to run on top of virtualization platforms, such as VMware vSphere, Microsoft Hyper-V, and Xen. Therefore, you must integrate with the virtual management component so that the Pano System can have full control of the DVMs that are available in vCenter Server.

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

All collection types, except Existing Desktop, 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 you create the collection or update the collection. (To turn off automated deployment for a collection, uncheck the **Deploy Enabled** option.)

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 System can automatically deploy extra DVMs but not assign them to users right away. When a new user signs into the collection, the Pano System automatically assigns that user to one of the extra DVMs, then deploys a new DVM to replenish the extra DVMs. This way, future users have quick access to a new DVM.

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 to Keep On** and **Extra Desktops** values in the collection properties dialog determines how many extra DVMs you want the Pano Controller to maintain for the collection, and whether they should be powered on or off. Extra DVMs is the number of additional DVMs that the Pano Controller deploys so that they are quickly available for new users. These extra DVMs are in addition to any assigned or in-use DVMs.

Next: Templates

Templates

The Pano System connects to a client OS (Windows XP or Windows 7) on desktop virtual machines (DVMs) running on virtualization platform. A template is a VMware vCenter Server concept that refers to a base virtual machine from which you provision DVMs. Templates are key to efficient management of DVMs, and they 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.

In a Pano System deployment there can be one or more templates. Typically, a template is associated with a specific user type or business unit. It can be customized with specific virtual hardware configuration and installed software to conform to unique requirements and needs.

Consider creating a separate template based on one of the following. Choose to create templates based on the method that makes sense for your organization.

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

Examples of templates include:

• Nurse Station Template

A Nurse Station template might have 2 GB of RAM and a single CPU. Software installed on this virtual machine template might include 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 might have 1GB of RAM and a single CPU. Software installed on this virtual machine template might include Call Answer Magic software. This template is used as base to provision DVMs for all the Call Center Agents.

• Financial Analyst Template

A Financial Analyst template might have 1024GB of RAM, two CPUs, and a 12GB hard disk. Software installed on this virtual machine can include Microsoft Office and decision support software that requires greater processing and memory resources.

• Help Desk Template

A Help Desk template might have 2 GB of RAM and a dual CPU. Software installed on this virtual machine template can include 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 might have 768 MB of RAM, a single CPU, and a 10GB hard disk. Software installed on this virtual machine template can include 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.

Next: Virtual Desktop Management

Virtual Desktop Management

You can manage your virtual desktops as you would Windows desktops in a non-virtualized environment. In other words, you can continue to use your Windows administration best practices and tools. For example, to deploy the latest Microsoft product updates to virtual desktops running the Windows operating system use your existing Windows management tools such as Microsoft Windows Server Update Services (WSUS) and Microsoft System Center Operations Manager (SCOM). These tools work just as they would on standalone Windows computers.

Next: Scalability

Scalability

The Pano System provides flexible deployment options to scale from small office architectures to highly scalable, highly flexible enterprise architectures.

Pano Controllers can be configured in groups of up to six Pano Controllers for load balancing and client/DVM scalability. A Pano Controller Group can contain from one to six Pano Controllers. Two Pano Controllers can be used to provide Primary and Secondary redundancy. Additional auxiliary Pano Controllers can be added to support up to a total of six Pano Controllers. The Primary/Secondary pair and auxiliary Pano Controllers support up to 2,000 DVMs/clients per group.

With third-party connection brokering, up to five Pano Controller groups can be configured to support up to highly-scalable deployments of DVMs/clients. Users can roam across Pano Controllers for flexible DVM access.

6
System Requirements

The Pano System has specific hardware and software requirements for each supported platform:

- Supported Virtualization Platforms
- Network Addressing Requirements
- Hardware & Resource Requirements
- Trial Requirements

Supported Virtualization Platforms

The Pano System 6.0 supports VMware, Citrix and Microsoft virtualization platforms as follows.

- **VMware**

Vendor	Product	Versions	Notes
VMware	View	4.6, 5.0, 5.0.1	5.0.1, 5.1in Pano System 6.0. Check with Pano support on status.
	vSphere	4.1, 5.0, 5.0 U1	For ESX/ESXi configured with Pano Controller as the primary connection broker
	vCenter Server	4.1 U1, 5.0	VCenter Server 5.0 Appliance (on Linux) supported in 6.0.

- **Citrix**

Vendor	Product	Versions	Notes
Citrix	XenDesktop (XD)	5.5, 5.6	Both added in Pano System 6.0.
	XD on XenServer	5.6, 6.0, 6.0.2	Adding 6.0.2 in Pano System 6.0
	XD on ESX	4.0 U1, 5.0, 5.0 U1	Only XenDesktop 5.5 with ESX 4.0 U1 and 5.0 U1, XenDesktop 5.6 with vSphere 5.0.
	XD on Hyper-V	2008R2	Only on XenDesktop 5.6

- **Microsoft**

Vendor	Product	Versions	Notes
Microsoft	Hyper-V	2008 R2	Both Windows Server 2008 R2 and free Hyper-V Server.
	SCVMM	2008 R2	Required for Hyper-V

Related Topics

Choose Your VMware Virtualization Infrastructure

Limitations of VMware View Connection Server

Network Addressing Requirements

Hardware & Resource Requirements

Trial Requirements

Network Addressing Requirements

The Pano System relies on IPv4 for network addressing. If both IPv4 and IPv6 are enabled on a DVM, the Pano Controller communicates via IPv4 despite IPv6 being active. You do not need to disable IPv6 on the DVM or on the server that's running your virtualization platform as long as IPv4 is enabled; but you may wish to; as doing so increases performance somewhat.

If IPv4 is disabled, the Pano Controller cannot communicate with the DVM. In this case:

- the Pano Direct Status column indicates `Unreachable`.
- the IP Address column shows the IPv6 address.

To ensure that your users do not disable IPv4, set up a GPO policy to enable IPv4.

Next: Hardware & Resource Requirements

Hardware & Resource Requirements

Hardware requirements vary according to the virtualization platform chosen:

Requirements for VMware vSphere

Requirements for Windows Server 2008 R2 Hyper-V

Requirements for XenServer

See also Trial Requirements

For additional tools, browse the following resources:

Resource
Pano Logic Solution Brief: Virtual Desktop Infrastructure Sizing
Deployment Architecture Overview Redbook
Remote Deployment Redbook
Pano on Citrix XenDesktop Redbook
Pano on VMware View Redbook
Pano Logic Total Cost of Ownership Calculator

Requirements for VMware vSphere

The hardware and software resources required to support your environment depend on your workload requirements, operating system to be used (Windows XP or Windows 7), network topology, and of course the total number of virtual desktops that you intend to run in your environment. In addition to provisioning for virtual desktops, consider the resource requirements for VMware vCenter Server and the Pano Controller virtual machine.

Server Hardware for VMware vSphere

Server hardware is required to host the ESX/ESXi hypervisor software, the DVMs, and system VMs, includingPano Controller. To find hardware that is compatible with and capable of running ESX/ESXi, go to VMware's compatibility guides.

DVM CPU, Memory, and Disk Space

To estimate your basic requirements, determine an appropriate amount of CPU and memory to each virtual desktop. Multiply that amount by the number of desktops that you expect to run. For Windows XP, consider giving every user 768MB RAM, 1/4 core processor and 1/4 spindle hard disk. Windows 7 users require at least 2GB of RAM.

For disk space, allocate an appropriate amount of space for each DVM. Keep in mind disk I/O rates; 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 1Gbps links between your server and workgroup switches. From workgroup switches to Pano System Endpoints, 100Mbps links are sufficient.

VMware vCenter Server

vCenter Server is a critical component for the Pano System. The minimum recommended configuration for running vCenter Server with the Pano System is as follows:

- Pentium IV 2.0 GHz processor
- 2GB RAM

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

Pano Controller Virtual Machine

The Pano Controller runs as a virtual machine. You can safely run the Pano Controller on the same host as DVMs; however, you must reserve sufficient resources for the Pano Controller VM so that the Pano Controller can render the Pano user login screens. Pano Logic recommends that you allocate the following resources for each Pano Controller VM based on the number of Pano System Endpoints in your environment.

Note: You don't need to account for Pano Remote clients. They don't consume any memory on the Pano Controller VM because of the way the Pano user login screen is rendered.

The following resources are required for a single Pano Controller VM. If you intend to create a Pano Controller group (refer to Configure Pano Controller Groups), make sure that each Pano Controller in that group meets the following resource requirements.

Deployment (DVMs per Pano Controller)	Reserved vCPU	Available vCPU	# of Allocated vCPUs	Reserved Memory (GBs)
0 - 50	512 MHz	2.0 GHz	1	1
51 - 250	1.0 GHz	4.0 GHz	2	2
251 - 500	1.5 GHz	6.0 GHz	4	4

- To reserve these resources in vCenter Server, go to Reserve Resources for the Pano Controller VM in vCenter Server.
- To learn about the maximum number of Pano System Endpoints that you can deploy, go to Supported Number of DVMs and Pano Zero Clients.

Related Topics

Supported Virtualization Platforms

Requirements for Windows Server 2008 R2 Hyper-V

The hardware and software resources required to support your environment depend on your:

- Workload requirements
- Operating system to be used (Windows XP or Windows 7)
- 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 Hyper-V and the Pano Controller virtual machine.

Server Hardware for Microsoft System Center Virtual Machine Manager (SCVMM)

The Pano System integrates with Microsoft System Center Virtual Machine Manager (SCVMM) to provision, manage, and control desktop virtual machines. You must allocate server hardware to run SCVMM.

- The server hardware must comply with Microsoft's requirements for running Microsoft System Center Virtual Machine Manager.
- The server that runs SCVMM must have the Pano Manager Connector for Microsoft SCVMM (SCVMM Connector) installed on it. This component can be found on the Pano Logic download site.

To find compatible hardware, go to Microsoft TechNet.

Pano Manager Connector for Microsoft SCVMM requirements

The Pano Manager Connector for Microsoft SCVMM (SCVMM Connector) allows the Pano Controller to communicate with the SCVMM server. The following must be installed on the SCVMM server.

- SCVMM Administrator Console
- Windows PowerShell version 2.0 (normally included in Windows Server 2008 R2)
- Microsoft .NET Framework version 3.5 (normally included in Windows Server 2008 R2)

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. For Windows XP, consider giving every user 768MB RAM, 1/4 core processor and 1/4 spindle hard disk. Windows7 users require at least 2GB of RAM.

For each disk, allocate an appropriate amount of space for each DVM. Also, disk I/O rates should be considered when placing virtual desktops on physical drives.

Network Bandwidth

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

Microsoft System Center Virtual Machine Manager

The minimum recommended configuration for running Microsoft System Center Virtual Machine Manager with the Pano System depends on your deployment. General recommendations suggest:

- Highly recommended: 2 CPUs. At a minimum, a Pentium IV 2.0 Ghz processor.

- 2GB RAM

Consult the Microsoft System Center Virtual Machine Manager documentation for complete SCVMM server requirements. If you choose to run your SCVMM as a virtual machine, make sure that you factor SCVMM's resource requirements into that host's overall capabilities.

Pano Controller Virtual Machine

Pano Controller runs as a virtual machine. You can safely run Pano Controller on the same host as DVMs; however, you must reserve sufficient resources for the Pano Controller VM so that Pano Controller can render the Pano user login screens. Pano Logic recommends that you allocate the following resources for each Pano Controller VM based on the number of Pano System Endpoints in your environment.

Note: You don't need to account for Pano Remote clients. They don't consume any memory on the Pano Controller VM because of how the Pano user login screen is rendered.

These resources are required for a single Pano Controller VM. If you intend to create a Pano Controller group (refer to Configure Pano Controller Groups), make sure that each Pano Controller in that group meets the following resource requirements.

Deployment (DVMs per Pano Controller)	Reserved vCPU	Available vCPU	# of Allocated vCPUs	Reserved Memory (GBs)
1 - 50	1.0 Ghz	4.0 Ghz	1	1GB
51 - 200	1.0 Ghz	4.0 Ghz	2	2GB

To learn about the maximum number of Pano System Endpoints that you can deploy, go to Supported Virtualization Platforms.

Requirements for XenServer

The hardware and software resources required to support your environment depend on your:

- Workload requirements
- Operating system to be used (Windows XP or Windows 7)
- 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 XenServer and the Pano Controller virtual machine.

Server Hardware for Citrix XenServer

Server hardware is required to host the Citrix XenServer hypervisor software, the DVMs, and system VMs, including Pano Controller. To find hardware that is compatible with and capable of running Citrix XenServer, refer to Citrix XenServer documentation.

DVM CPU, Memory, and Disk Space

To estimate your basic requirements, allocate an appropriate amount of CPU, memory, and disk to each virtual desktop. For Windows XP, consider giving every user 768MB RAM, 1/4 core processor, and 1/4 spindle hard disk. Windows 7 users require at least 2GB of RAM. For disk space, 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. Multiply that amount by the number of desktops that you expect to run.

Network Bandwidth

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

Citrix Desktop Delivery Controller (DDC)/Citrix XenDesktop Controller

The DDC (under XenDesktop 4) or XenDesktop Controller (under XenDesktop 5) (referred to collectively in this documentation as XenDesktop Controller) functions as the connection broker for the entire system. XenDesktop Controller is a critical component for the Pano System. The minimum recommended configuration for running XenDesktop Controller with the Pano System is as follows:

- Pentium IV 2.0 Ghz processor
- 2GB RAM

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

Pano Controller Virtual Machine

The Pano Controller runs as a virtual machine. You can safely run the Pano Controller on the same host as DVMs; however, you must reserve sufficient resources for the Pano Controller VM so that the Pano Controller can render the Pano user login screens. Pano Logic recommends that you allocate the following resources for each Pano Controller VM based on the number of Pano System Endpoints in your environment.

Note: You don't need to account for Pano Remote clients. They don't consume any memory on the Pano Controller VM because of the way the Pano user login screen is rendered.

The following resources are required for a single Pano Controller VM. If you intend to create a Pano Controller group (refer to Configure Pano Controller Groups), make sure that each Pano Controller in that group meets the following resource requirements.

Deployment (DVMs per Pano Controller)	Reserved vCPU	Available vCPU	# of Allocated vCPUs	Reserved Memory (GBs)
0 - 50	512 MHz	2.0 GHz	1	1
51 - 250	1.0 GHz	4.0 GHz	2	2
251 - 500	1.5 GHz	6.0 GHz	4	4

To learn about the maximum number of Pano System Endpoints that you can deploy, go to Supported Number of DVMs and Pano Zero Clients.

Related Topics

Supported Virtualization Platforms

Network and Infrastructure Requirements

Trial Requirements

Before you begin your Pano System trial, ensure that you meet the basic system requirements:

VMware	Citrix Xen	Microsoft

Supported Virtualization Platforms	Supported Virtualization Platforms	Supported Virtualization Platforms
Server Hardware for VMware vSphere	Server Hardware for Citrix XenServer	Server Hardware for Microsoft System Center Virtual Machine Manager (SCVMM)
VMware vCenter Server	Citrix Desktop Delivery Controller (DDC)/Citrix XenDesktop Controller	Supported Directory Services
Supported Directory Services	Supported Directory Services	Support for USB Devices
Support for USB Devices	Support for USB Devices	Supported Operating Systems for Pano Direct Service Service
Supported Operating Systems for Pano Direct Service Service	Supported Operating Systems for Pano Direct Service Service	Supported Virtualization Platforms

To view detailed system requirements, go to System Requirements.

7 Support

The Pano System works in conjunction with many third-party products and features. Use the following support topics to help you build your Pano System environment. If you desire support for a particular third party product or feature, and it's not listed here, let us know!

- Pano Controller and Pano Direct Versions
- Supported Number of DVMs and Pano Zero Clients
- Supported Operating Systems for Pano Direct Service Service
- Supported Directory Services
- Supported Third Party Connection Brokers
- Support for USB Devices
- Supported Isochronous USB Devices for Pano G2
- Supported Monitor Resolutions
- Supported Wireless Bridges
- Supported Third-Party Login Screens
- Windows Server Support

Related Topics

Limitations

Pano Controller and Pano Direct Versions

Pano Controller must always be the same version or newer than the Pano Direct Service and other components running on the virtual desktops. Always upgrade Pano Controller before you upgrade Pano Direct Service.

Next: Supported Number of DVMs and Pano Zero Clients

Supported Number of DVMs and Pano Zero Clients

The maximum number of DVMs and Pano System Endpoints that you can deploy depends on the Pano Controller configuration that you choose (go to Configure Pano Controller Groups). Depending on the size of your deployment, you might need to deploy multiple Pano Controller Virtual Appliances. Pano System supports the following group configurations.

Note: On Hyper-V, scalability is currently limited due to the function of Linux on Hyper-V.

Pano Controller Configuration	# of Pano Controller VMs	Redundant?	Maximum Clients / DVMs	
			vSphere / Citrix XenDesktop	Hyper-V
Single ("Standalone")	1	No	500	200
Scalability Group	2	No	1000	400
Failover Group	2	Yes	500	200
Failover Group and Scalability Group	3	Yes	1000	400

Maximum Seats	Platforms	Pano Controller Configuration
200	Hyper-V	Single (“Standalone”)
400	Hyper-V	Scalability Group
500	VMware, Citrix	Single (“Standalone”)
1,000	VMware, Citrix	Scalability Group
Over 1,000	VMware View	Scalability Group with View Connection Server configured as the primary connection broker

Next: Supported Operating Systems for Pano Direct Service Service

Supported Operating Systems for Pano Direct Service Service

You must have valid licenses for Microsoft desktop operating systems. The following tables list the editions and distribution channels that the Pano System supports. You can install the Pano Direct Service on any supported operating system.

- **Windows 7 Support**

Version	Supported?
Professional x86 (32-bit)	Yes
Enterprise x86 (32-bit)	Yes
Ultimate x86 (32-bit)	Yes
Professional x64 (64-bit)	Yes
Enterprise x64 (64-bit)	Yes
Ultimate x64 (64-bit)	Yes
Home Premium x86 or x64	No
Home Basic	No
Starter	No

- **Windows XP Support**

Version	Supported?
Windows XP Professional, SP3 (32-bit)	Yes
Windows XP Professional, SP2 (32-bit)	Yes
Windows XP Home	No

Note: Pano Logic recommends the following Windows XP Updates:

KB 952132

KB 959252

KB 886199

Supported Directory Services

The Pano System supports the following directory services:

- Active Directory 2003, 2003 R2, 2008, and 2008 R2.
- Novell eDirectory 8.8
- OpenLDAP 2.4.x

Next: Supported Third Party Connection Brokers

Supported Third Party Connection Brokers

Although Pano Controller acts as a full-featured connection broker, Pano System supports the following third-party connection brokers.

- VMware View 4.5
- VMware View 4.6
- VMware View 5.0
- Citrix XenDesktop 5

Next: Support for USB Devices

Related Topics

Limitations of VMware View Connection Server

Support for USB Devices

Support for USB devices varies by Pano System Endpoint:

- Supported Non-Isochronous USB Devices
- Supported Isochronous USB Devices for Pano G2

Verify Interoperability

Pano's unique approach to desktop virtualization — Pano Zero Client hardware and virtualized system bus — provides support for a wide range of USB devices meeting industry standard specifications. Due to variances in specification implementations, Pano recommends contacting your Pano sales representative at 877.677.PANO to verify specific device support. Pano continually tests and certifies additional USB devices to ensure comprehensive device support.

Pano Logic can offer guidance as to which specific devices have been validated and work best with the Pano System. The best practice regarding peripherals is for your IT organization to verify interoperability before your company deploys Pano System Endpoints with peripherals.

Enable Support

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

Related Topics

Supported Monitor Resolutions

Supported Non-Isochronous USB Devices

Non-isochronous refers to the type data transfer used for discontinuous communication between a host and a device where synchronization is used for error recovery and retry. In addition to support for USB keyboards and mice, the Pano System also includes support for the following non-isochronous USB device *types*, including composite devices (often called, *all-in-one* solutions).

Within each general USB type, there might be specific devices that operate differently; therefore, you must test your devices in a Pano System environment before you use those devices in production.

- 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 touch screen display
- USB smart boards

Related Topics

Supported Isochronous USB Devices for Pano G2

Supported Monitor Resolutions

Supported Isochronous USB Devices for Pano G2

Isochronous USB is a class of USB devices that include peripherals such as speakers, microphones, headsets, and webcams used for periodic, continuous communication between a host and a device, usually for time-sensitive data transfers such as audio or video data streams. Isochronous transfers do not support error detection or retry.

Support for specific USB devices varies by Pano System Endpoint type. Only Pano G2 Zero Clients support isochronous USB peripherals. Pano G1 Zero Clients do not support isochronous USB peripherals.

Audio Playback Use Case

The Pano System with a Pano G2 Zero Client supports playback of audio through external USB speakers and headsets. Audio playback is supported on both Windows XP and Windows 7 virtual desktops. Depending on what additional applications and use cases are to be supported simultaneously along with audio playback, you might need to configure the virtual desktop with 2 virtual CPUs.

At the start of an audio stream, users might notice a momentary glitch in audio which can be perceived as a "pop", lasting a fraction of a second. This known issue is expected to be addressed in a future update of the Pano software.

Supported Apps & Services	Supported Devices
• Windows Media Player 10 • Windows Media Player 12 • VLC Player • QuickTime Player • Apple iTunes • YouTube • Pandora • Live360	Speakers: • Logitech S-150 USB Digital Speaker • Altec Lansing Orbit MP3 iM237 Headsets: • Logitech H330 • Logitech H360 • Logitech H555 • Plantronics Audio 995USB • Plantronics M214i • Microsoft LifeChat LX-1000 • Fujitsu HS710

Bi-Directional Audio / Voice Conversation Use Case

The Pano System with a Pano G2 Zero Client supports voice conversations using isochronous USB devices and a software application or "soft phone." Voice communications are supported on both Windows XP and Windows 7 virtual desktops. Depending on what additional applications and use cases are to be supported simultaneously along with audio recording, the virtual desktop may need to be configured with 2 virtual CPUs.

Note: Windows Live Messenger is not supported at this time.

Supported Apps & Services	Supported Devices
• Skype • GoogleTalk • Cisco Unified Communications	• Logitech H330 • Logitech H360 • Logitech H555 • Plantronics Audio 995USB • Plantronics M214i • Microsoft LifeChat LX-1000 • Fujitsu HS7100U • Logitech USB Desktop Microphone AK5370 (using external analog or USB speakers)

Video Conferencing Use Case

The Pano System with a Pano G2 Zero Client supports video conferencing using USB webcams and video conferencing software. At this time, video conferencing is only supported on Windows XP; support for video conferencing with Windows 7 is expected to be added in a future software release. In order to support video conferencing, configure the virtual desktop with 2 virtual CPUs.

Note: At this time, only the webcams listed are officially supported. Webcams can typically transmit video at different bit rates, and a suitable webcam needs to be able to successfully negotiate and support an appropriate bit rate. For this reason, the webcam that you select must be from Pano Logic's official list of approved devices. Video conferencing is not supported on Windows 7 at this time; support is expected to be added in a future software release.

Supported Apps & Services	Supported Devices
• Skype • GoogleTalk •	• Microsoft LifeCam VX-1000 • Microsoft LifeCam VX-3000

Note: The same set of USB devices will work with Windows 7 64-bit so long as the USB device driver supports Windows 7 64-bit.

Related Topics

Supported Non-Isochronous USB Devices

Supported Monitor Resolutions

Supported Monitor Resolutions

Support for specific monitor resolutions varies by Pano System Endpoint type.l.

Monitor Resolution Support for Pano G2

Pano G2 and G2M Zero Clients support the following resolutions:

Resolution	Frequency
Standard	
800 x 600	60
800 x 600	75
1024 x 768	60
1024 x 768	75
1280 x 1024	60
1600 x 1200	60
Widescreen	
1024 x 600	60
1024 x 600	75
1152 x 768	60
1280 x 800	60
1280 x 800	75
1440 x 900	60
1680 x 1050	60
1920 x 1200	60

In addition to the above resolutions, Pano System Endpoints support a monitor's native resolution.

Widescreen monitors are supported only if the monitor advertises them as their native resolution. Widescreen monitors can only display at their native resolutions or at one of the standard timings listed above. To adjust the resolutions of the monitor, go to Set Screen Resolution Settings for Specific DVMs.

Monitor Resolution Support for Pano G1

Pano G1 Zero Clients support the following resolutions:

Resolution	Frequency
800 x 600	60
800 x 600	75
1024 x 768	60
1024 x 768	75
1152 x 864	75
1280 x 1024	60
1280 x 1024	75
1360 x 768	60
1600 x 1200	60
1920 x 1080	60

In addition to the above resolutions, Pano System Endpoints support a monitor's native resolution.

Widescreen monitors are supported only if the monitor advertises them as their native resolution. Widescreen monitors can only display at their native resolutions or at one of the standard timings listed above. To adjust the resolutions of the monitor, go to Set Screen Resolution Settings for Specific DVMs.

Supported Wireless Bridges

Pano Logic supports the following wireless bridges:

- Linksys, WET54G
- D-Link, DWL-G730AP
- Asus, WL-330gE

To configure these wireless bridges, go to Connect Pano Zero Clients To Your Wireless Network.

Supported Third-Party Login Screens

- **Windows 7** - Pano Logic designed Pano Direct Service according to Microsoft’s specifications for Windows 7. As such, Windows 7 is expected to interoperate with other applications, such as Pano Direct Service, that are complaint with Windows 7 credential provider infrastructure so long as:
  - The associated USB device is supported. Go to Support for USB Devices, if applicable.
  - The collection type supports your SmartCard Reader, if applicable. Go to Choose DVM Collection Type.

  No special installation instructions are required. Simply follow the third-party’s installation instructions, then install Pano Direct Service.

- **Windows XP** - Pano Logic supports the following third-party GINA applications with Pano Direct Service for Windows XP. These applications install their own GINA providers, and Pano Direct Service can integrate with these providers. Pano Direct Service can interoperate with any *one* of these applications, but not a combination of them. Moreover, there are special installation instructions that you must follow to install these applications.

If you’re using a GINA that is not supported, contact Pano Logic Technical Support. Pano Logic continues to test additional providers where there is strong customer interest.

Collection Type	VMware View Agent 4.5	SplitView 2009	Imprivata Single Sign-on Agent 3.5	Ensure Technologies XyLoc 8.5.1	Novell Client 4.91[1]
Permanently Assigned Desktops	Yes	Yes	No	No	Yes
Pooled Desktops	Yes	Yes	No	No	Yes
Existing Desktops	Yes	Yes	No	No	Yes
Windows Login	Yes	Yes	Yes	Yes	Yes
Automatic Login	Yes	Yes	No	No	Yes
Different Accounts w/ Automatic Login	Yes	Yes	No	No	Yes
VMware View	Yes	Yes	No	No	No

[1] Novell is supported, but if you’re using a User Collection your users must log on twice–once through the Pano user login screen and again at the GINA Login screen.

Related Topics

What’s a GINA?

About Pano GINA Provider and Registry Changes

Reestablish Broken GINA Chain

Install Third Party GINA Applications

Upgrade or Uninstall Third Party GINA Applications

Windows Server Support

	2008 R2	2008	2003 R2	2003
Pano Gateway Server	Yes	No	No	No
DCHP/DNS Server	Yes	Yes	Yes	Yes
AD Server (Authentication)	Yes	Yes	Yes	Yes
AD Server (GPO upgrades/deployments)	Yes	Yes	Yes	Yes

8 Limitations

The Pano System has some limitations, in many cases because of third party behavior outside of Pano Logic's control. These include:

- Limitations of Pano Controller without vCenter Server
- Limitations to Windows 7 Support
- Limitations to Fast User Switching
- Limitations to Sleep and Hibernate
- Limitations of Pano Controller without Active Directory
- Limitations to USB Device Support
- Pano G1 Zero Client Limitations of Pano Dual Monitor
- Limitations of VMware View Connection Server
- Limitations of XenDesktop
- Limitations on USB Devices with Pano Virtual Client

Limitations of Pano Controller without vCenter Server

You can run the Pano Controller without the need for vCenter Server (formerly Virtual Center). There are limitations in terms of what you can do relative to having the entire suite; but, even with these limitations, the solution can be practical for small or simplistic deployments.

vCenter Server is needed when managing environments that contain more than one ESX host or when you want to take advantage of automated provisioning. Most want to include this component in their deployment.

When using Pano Controller without vCenter Server, you need to point Pano Controller directly at your ESXi server. Once you do this, you should be able to see the list of virtual machines on the server, but you won't be able to organize them into folders (like you can with vCenter Server), or clone DVMs. This list of virtual machines includes all computers, even servers like the Pano Controller, not just desktops.

In such a deployment, you can probably scale to 10 or 15 virtual machines before you discover that you need vCenter Server to help you automate a few management tasks.

Lastly, VMware restricts the use of the vSphere Remote Command Line Interface and related API when using the free version of ESXi. This restriction prevents end users or services such as Pano Controller from making configuration changes such as powering on a virtual machine. For this reason, the use of the free version of ESXi is typically not suitable except in rare instances. If VMware reverts their policy and re-enables such functionality, deployments of Pano Controller free ESXi might once again be viable for small deployments.

What	ESXi 4.0 or later *without* vCenter Server	ESX/ESXi *with* vCenter Server
Create Folders from Pano Controller or vSphere Client	No	Yes
Create more than one collection in Pano Controller	Yes	Yes
Trash DVM from Pano user login screen	No	Yes
Copy/Clone from vSphere Client	No	Yes
Automatically provision desktops	No	Yes

What	ESXi 4.0 or later *without* vCenter Server	ESX/ESXi *with* vCenter Server
End users can power on DVMs from the client UI	No	Yes
Pano Controller can perform power management tasks on DVMs[1]	No	Yes

[1] Power management tasks include Power On, Power Off, Suspend, Reset, Shut Down Guest, Restart Guest, and Power Off the Surplus.

Related Topics

Supported Virtualization Platforms

Install Pano System with ESXi without vCenter Server

Limitations to Windows 7 Support

Limitations to Windows 7 Support

There are a few limitations to DVMs running Windows 7, depending on your virtualization platform.

- **VMware only**
  - Must be running in a vSphere 4.0 Update 1 (or later) environment. This limitation is a VMware requirement.
  - The VMware SVGA 3D (WDDM) display driver is now supported.
- **VMware, Hyper-V, and Citrix XenServer/XenDesktop**
  - IPv6 is not supported. For more information, go to Network Addressing Requirements.
  - All display (monitor), keyboard, mouse and audio settings must be made from the Pano Control Panel. To learn how to do this, go to About Pano Control Panel.

Related Topics

Limitations to Fast User Switching

Limitations to Sleep and Hibernate

Windows 7 FAQs

Limitations to Fast User Switching

Pano Direct Service does not support Fast User Switching on Windows XP DVMs. However, Pano Direct Service does support fast user switching on Windows 7, but only if the DVM is part of a Windows Login collection type.

Windows 7 - In Windows 7, fast user switching is enabled by default, even after a DVM joins the domain. Therefore, unless the DVM is part of a Windows Login collection type, you must disable this by using a group policy (go to Disable Fast User Switching in Windows 7).

- If a user chooses the switch users from a Windows 7 desktop that has fast user switching enabled and that is in a Windows Login collection type, Pano Direct Service disconnects the user from the DVM, and a different user can log on to that DVM, after the Pano System Endpoint reconnects.
- If a user tries to switch users from a Windows 7 desktop that has fast user switching enabled and that is part of *any other collection type*, the Pano Direct Service disconnects the session.

  - For User Based Collections the standard Pano Login appears.
  - For Automatic Login collection type and Different Accounts w/ Automatic Login collection type the session connects using the user information that you specified in the collection properties.

Windows XP - Fortunately, in Windows XP, fast user switching is disabled when a DVM joins the domain. So, end users of Windows XP DVMs don't typically have access to this feature by default. There is a way (a "hack") to enable this feature, but it's not advisable and is not supported.

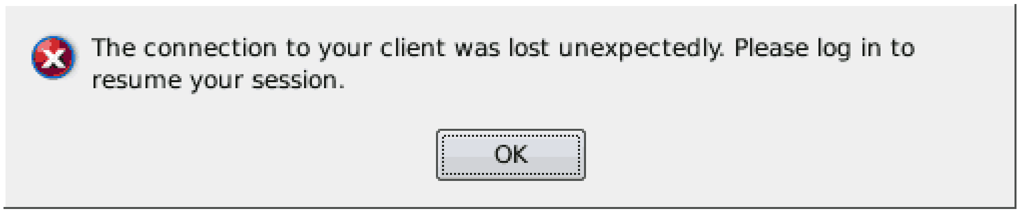
Related Topics

Limitations to Sleep and Hibernate

Limitations to Sleep and Hibernate

Sleep and Hibernate are not supported on DVMs. Pano Direct cannot wake up all saved screens and applications.

- **Windows 7** - In Windows 7, hibernate is enabled by default, even after a DVM joins the domain. Therefore, you must disable this behavior by using a group policy. (go to Disable Sleep and Hibernate in Windows 7). If a user switches to hibernate mode, you or the user must power on the DVM to "wake up" the applications. Pano Direct Service cannot automatically recover its connection to the DVM, and returns the following message when the user attempts to log on: `The connection to your client was lost unexpectedly. Please log in to resume your session.` In this case, you (see Power On DVMs as Administrator) or the user (see Power On DVMs as End User) must power on the DVM to "wake up" the applications.



The connection to your client was lost unexpectedly. Please log in to resume your session.

- **Windows XP** - In Windows XP, hibernate is disabled when a DVM joins the domain. So, end users of Windows XP DVMs don't typically have access to this feature by default.

Related Topics

Limitations to Fast User Switching

Limitations of Pano Controller without Active Directory

You can run the Pano Controller without the need for Active Directory. However, you'd be missing out on some key benefits.

If you are using Pano Controller without Active Directory you can just leave the Directory Configuration section of the Setup tab blank. Without Active Directory, the Pano Controller cannot authenticate users. Hence, you will be limited to a Device-Based Collection, a policy that ties desktop virtual machines to Pano System Endpoints rather than users. In other words, you won't be able to use a User Based Collection.

Limitations to USB Device Support

• Possible data corruption on USB device

If a user inserts a USB storage device into a Pano System Endpoint and then the user's session is improperly terminated, this chain of events can cause data corruption on the USB device. Such corruption is not a problem that is unique to Pano System Endpoints. 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). The common ways to disconnect a session include:

- Select disconnect from the Windows Security dialog.
- Press the Pano Button from a Pano System Endpoint.
- Log on to your original session from another Pano System Endpoint (also known as *session roaming*).
- Log on to your original session from another non-Pano System Endpoint, 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 System Endpoint 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.

• Inability to connect more than one mass storage device to a Pano System Endpoint or transfer data between such devices

Users should not connect more than one mass storage type device (for example, cameras and USB flash drives) to a Pano System Endpoint at any given time.

Furthermore, if you transfer data between two such devices the USB subsystem might freeze; to recover from this issue, press the Pano Button. Keyboards and mice are not affected by this limitation: you can continue using these devices during data transfers.

If you need to transfer data between two such devices, do the following:

1. Connect `device 1`. Do not connect `device 2` yet.
2. Copy the data from `device 1` to the DVM.
3. Disconnect `device 1`.
4. Connect `device 2`.
5. From the DVM, copy the data to `device 2`.

If you need to have two mass storage devices connected at the same time:

Install a USB 1.1 (not USB 2.0) hub, then connect the devices to the Pano System Endpoint through that hub.

Pano G1 Zero Client Limitations of Pano Dual Monitor

Pano Dual Monitor solutions using a Pano G1 Zero Client are not supported in version 6.0.

In versions prior to 6.0, the following restrictions existed:

- Only Windows XP DVMs are supported.
- Only the Pano Logic-branded adapter is supported. The Pano Direct Service will not activate third-party DisplayLink adapters.
- The Pano Dual Monitor USB adapter can have at most one USB hub between it and the Pano System Endpoint. When using a hub, a powered hub is recommended.
- Both displays will be driven at the same resolution, the primary monitor's resolution.
- Pano Dual Monitor might not work reliably when a large amount of information is being transferred to/from a USB device that is connected to a Pano System Endpoint at the same time that a significant amount of display changes are occurring. For example, if you transfer a large file from a USB key to your virtual desktop while you simultaneously watch a YouTube video, you might experience problems. Simultaneous high-traffic use is not supported. If attempted, any of the following *might* occur:
  - secondary monitor fails to refresh.
  - moving the mouse on the secondary monitor results in mouse cursor freezing momentarily.

Limitations of VMware View Connection Server

VMware View Connection Server has the following limitations:

- PC-over-IP:Pano System software and endpoints do not support the Teradici PC-over-IP (PCoIP) protocol included in VMware 4.0 and later. Instead, the Pano Direct protocol is used.
- drivers refer to Install Pano Controller on VMware.
- End users cannot access their DVMs from an RDP client such as Windows Remote Desktop Connection if *View Secure Authentication* is enabled. For more information, go to Configure VMware View Agent.

Limitations of XenDesktop

XenDesktop has the following limitations:

- The Pano system does not use the Citrix HDX protocol. Instead, the Pano Direct Protocol (PDP) is used to connect a Pano Zero Client to a DVM. In order to establish this connection, the Pano Direct Service Service must be installed and running on the DVM. Simply installing the XenDesktop Virtual Desktop Agent is not sufficient. Pano does not support Citrix ICA®, HDX™, or the Citrix Access Gateway™.
- Pano System Endpoints and HDX/ICA clients cannot access the same DVMs.
- You must maintain isolation between desktops that will be accessed using Pano System Endpoints and desktops that will be accessed using HDX clients. You can do this by configuring distinct desktop pools: those for use with Pano and those for use with HDX clients.
- Roaming between Pano System Endpoints and HDX clients is not supported.

- Pano Controller cannot display more than six desktop groups from XenDesktop XD4. If a user has seven or more desktop groups, the user will receive the message: “Cannot login XXX because no desktop virtual machines are configured for you. Please contact your system administrator.”
- On Windows 7, when you install the Pano Direct Service, the Pano Direct Service installer will automatically disable the XenAgent so logins via Citrix ICA or HDX will be disabled. On Windows XP, the XenAgent is not disabled, however, connecting to DVMs via Citrix ICA or HDX is not supported.
- All connection brokering is performed by XenDesktop, with which device-based collections are support if using vCenter Server or SCVMM; you cannot configure anything other than a single, platform-specific, user-based Citrix XenDesktop collection. All Pano DVMs are included in this single type of collection. This means that you will not be able to use device-based collections as part of a Pano System and XenDesktop deployment.
- When integrated with XenDesktop, one and only one DVM collection type (XenDesktop) must be configured in the Pano Controller. No additional DVM collections can be configured.
- End users cannot restart, reset, or trash a DVM from the Options dialog, which is part of the standard Pano Logic login screen. These features are also known as user controls.
- Smart card, biometric, or other USB authentication devices are not supported.

Limitations on USB Devices with Pano Virtual Client

Pano Virtual Client supports most of the same USB devices that are supported by Pano G2 Zero Client. More information can be found at Support for USB Devices and Supported Non-Isochronous USB Devices

9 Deployment Planning

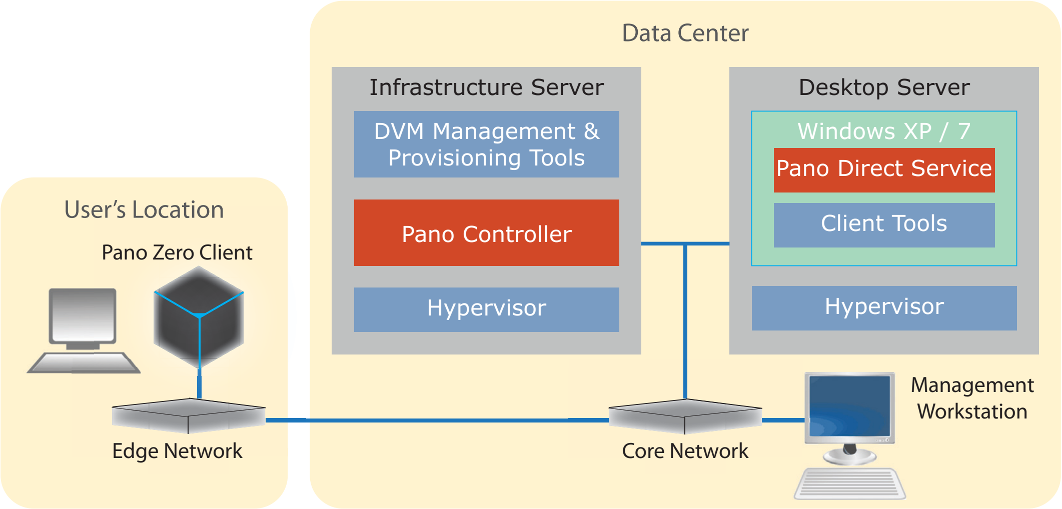
This chapter shows different ways in which the Pano system can be deployed in small, medium, and large enterprises, and the options available for integration with the rest of the IT environment.

It includes the following topics:

- Deployment and Network Terminology, to help you understand how all the require elements interact.
- Planning Your Deployment, which includes advice on integration with existing services and network resources
- Virtualization Platform Options discusses the virtualization platform that will deliver virtual desktops to your clients.
- Pano Controller Resource Requirements explains what's require for the actual controller platform itself
- Sizing Server and Storage Requirements helps you to estimate costs for your deployment.
- Best Practices for Deploying Pano Zero Clients offers suggests to smooth the transition to a virtual desktop environment.

Deployment and Network Terminology

To help understand the terminologies used, below are definitions of several terms used to describe Pano System deployments. The following figure illustrates most of these components and their interconnections.



High-level components in Pano deployment architectures include:

- **Desktop Servers** – shared servers used to host desktop virtual machines (DVMs) and supporting hypervisors. May store DVM images to local direct attached storage or access them over a storage network.

- **Infrastructure Servers** – servers used to host the Pano Controller virtual machine, alternate connection brokers, virtualization platform components for DVM provisioning and management and storage optimization, as well as supporting hypervisors.
- **Management Workstations** – Windows workstations or browser sessions used to connect to management front-ends, including Pano Controller and the hypervisor software. These workstations are used by IT staff to manage and monitor Pano Zero Clients and DVMs. For Pano Controller and most platform management tools, only a web browser session is required. After initial setup, a Pano Zero Client can also be used as the management workstation.
- **Edge Network** – peripheral networks used to connect Pano Zero Clients and other devices, at user locations, back to the central, or core, network. Edge networks, often called local area networks (LANs), typically use 100 Mbps to 1 Gbps Ethernet connections and switches with higher speed backbones connecting multiple switches and the core network.
- **Core Network** – the central network connecting edge networks to the servers supporting a site or organization. Typically, network components in a data center's core network provide higher throughput and additional types of interfaces than edge network components. For example, a core network router or switch could provide connections ranging from 1 Gbps for servers and edge network switches up to 10 or 40 Gbps for campus-wide connections, as well as interfaces to wide area networks (WANs) or the Internet.
- **Storage Area Networks (SANs)** – (not illustrated above) dedicated connections from desktop and other servers to specialized storage controllers and drive arrays. Provide high-speed (4 to 10 Gbps), low latency access to shared storage without creating contention on core networks.
- **Domain Servers** – (also not illustrated above) provide directory services, like Microsoft® AD® from Windows Server®, for user and system authentication. These servers also typically provide network addressing resources, like the dynamic host configuration protocol (DHCP) service, which is important for Pano System Endpoints to be able to connect to the network.

Next: Planning Your Deployment

Planning Your Deployment

Prior to deploying a Pano System, you should make the assessments outlined below to determine the resources you'll need. The general steps for planning your deployment include:

- Perform network infrastructure and site assessments. Got to Network Infrastructure Assessment and Site Assessment for information.
- Conduct a user survey to identify users' resource needs (including server hardware and operating system and applications software). Go to User Workload Assessment.
- Determine your storage requirements: local vs. shared storage. Go to DVM Collections and Storage Choices.

Network Infrastructure Assessment

The first step in the site assessment is to survey your local area network setup and determine if you are prepared for a Pano System deployment.

Pano virtual desktops are typically deployed on a switched Ethernet network, which tends to avoid or minimize network bottlenecks. The edge network links where Pano System Endpoints are located should have 100 Mbps or better switched (rather than shared) Ethernet connections to the core network. Make sure desktop and infrastructure servers are connected via one or more 1 Gbps or better links to the core network. Intervening Ethernet switches or routers are fine, as long as there is a routable connection between Pano System Endpoints and DVMs.

To understand the impact of deploying Pano Zero Clients on your network, you need to evaluate the topology of your network, potential sources of network traffic and bottlenecks and the average and peak bandwidth needs generated by your Pano users' workloads.

Network Traffic Sources

To estimate network traffic, evaluate each potential source of traffic. For example, if you consider a desktop server hosting DVMs, it will generally have up to four distinct sources of network traffic:

- Pano Direct Service Protocol traffic between Pano System Endpoints and servers
- Application and file sharing traffic
- Shared storage traffic, such as iSCSI or NFS traffic from the server to shared storage systems like a network attached storage (NAS) or SAN
- Management tool and other infrastructure traffic, such as DVM migration, fault tolerance, image backup, etc.

Deploying Pano virtual desktops will change your current network traffic characteristics. For example, if you are currently running client/server applications (such as a database) that result in a lot of edge-to-core network traffic between distributed PC clients and application servers, replacing the PCs with Panos will redistribute the traffic. The client-server traffic will now flow between the centralized DVMs (on the desktop server) and application servers over the data center's core network. This will reduce application traffic travelling out to the edge network and may more than offset the Pano Direct Service Protocol traffic that now goes from the DVMs directly to the Pano Zero Clients.

Bandwidth Provisioning

To estimate and provision network bandwidth for Pano System Endpoints, you need to look at two different bandwidth metrics:

- **Average bandwidth** – bandwidth consumed over an extended period (such as 8 hours) and averaged. This number will include periods when the Pano System Endpoint is actively updating the display and periods when it is idle or even disconnected. This figure can be used to estimate the number of users that can be provisioned on a given network link. Each Pano user running typical office application workloads will use an average bandwidth of 500 Kbps.
- **Peak bandwidth** – maximum bandwidth used for short but large intermittent traffic bursts. Typically these result from activities like moving to a new slide in PowerPoint, minimizing a window, etc. Peak bandwidth bursts can use 5 to 10 Mbps of bandwidth and last between 10 and 20 milliseconds (ms).

For Pano Zero Client users with typical office applications workloads, a good rule of thumb would be to provision around 500 Kbps (average bandwidth) per user, which would support about 160 users on a 100 Mbps Ethernet link (after allowing for 20% loss of bandwidth due to Ethernet overhead). However, you also need to allow headroom for peak bandwidth bursts which, depending on your users' behavior patterns, may require that you drop the number of users provisioned per link by up to 30 – 50%. Using 1 Gbps or better links for connections carrying multiple Panos sessions can assure there will be adequate bandwidth even during peak demand periods. Ideally, once your deployment starts, you should measure both average and peak bandwidth usage for a representative sample of your users to adjust provisioning estimates.

Pano Remote™ uses the Remote Desktop Protocol (RDP) rather than the Pano Direct Protocol® used by Pano Zero Clients. Pano Remote's bandwidth usage can vary significantly, as the RDP protocol will try to use as much bandwidth as it needs depending on what the user is doing. A typical average bandwidth usage might be only 128 Kbps per session, provided printing to local printers (which can cause bandwidth usage peaks of several Mbps) is not used.

Network Latency

Latency is another key factor in providing an adequate Pano user experience. Latencies above 10 ms round-trip (from a Pano Zero Client to the desktop server and back) impact the performance of the Pano user interface, causing some display changes to lag on the Pano System Endpoint. Increasing latency will result in a noticeable lag between typing a character and the character showing up on the screen, lag between clicking on a button and seeing the response, and so on. If latency gets too high – above 100 ms – due to server or network congestion, the session between the Pano Zero Client and the DVM will disconnect.

A typical network designed for Pano Zero Client deployments will have no more than 2 ms round-trip latency between the edge networks where the Pano System Endpoints are located and the desktop servers in the data center. Even on a larger multi-facility or campus network with multiple layers of switches and routers, a well-designed network should have no more than 5 ms latency. To achieve this performance, you should provision 1 Gbps or better links between switch layers and servers, cut-through rather than store-and-forward switching/ routing and 10 Gbps links for campus backbones.

Pano Remote, designed to work over WANs like the public Internet, can tolerate round-trip latencies as high as 200 ms and still provide a very usable user experience.

Peak Demand from Login Storms

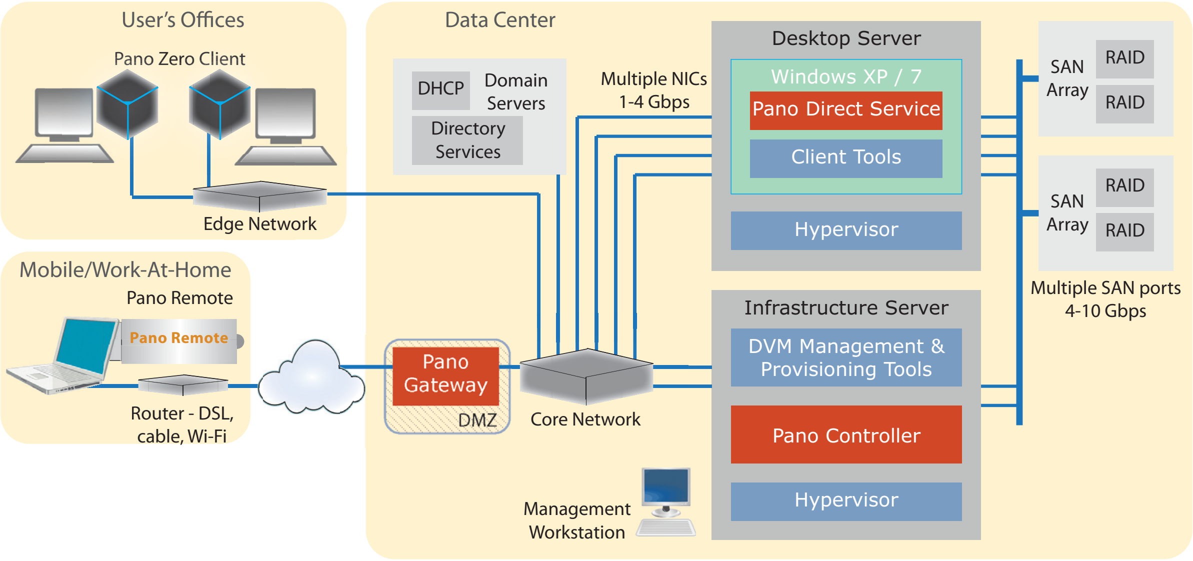
Your network may experience periods of high peak demand when a number of users log in simultaneously, such as when a branch office opens or when a class starts in a training center that uses Pano System Endpoints. These "login storms" take up network bandwidth, as well as CPU cycles and input/output operations per second (IOPS) (go to Storage IOPS Requirements for information about IOPS). This high peak usage can cause delays in Pano user interface responsiveness. To mitigate this potential problem, you can configure your system so the operating systems start up before being requested by a user, stagger periods of high activity or over-provision network and infrastructure resources to accommodate these periods of high, peak demand.

Anticipate Network Bottlenecks

Be sure to identify and characterize any potential bottlenecks between Pano System Endpoints and desktop or infrastructure servers. A typical bottleneck might be due to a large number of DVMs sharing a limited number of physical Ethernet ports on a desktop server.

Ideally, you should provide sufficient physical networking capacity in the servers to handle both sustained average and peak bandwidth needs. Ensure that the anticipated network traffic can be handled by the physical Ethernet network ports installed on the servers. For both performance and redundancy, you should consider installing additional network interface cards (NICs) with multiple network ports. The number of physical network ports should scale with the workload of the server instead of relying on the hypervisor to multiplex numerous virtual network connections from DVMs and system VMs through only one or two physical network ports.

If you are deploying across a multi-facility campus-type environment, there may also be topology constraints, such as at routers or bridges that potentially result in bottlenecks between Pano System Endpoints and associated infrastructure or desktop servers.



Prioritize Network Traffic

Networking equipment, like switches and VPN appliances, may allow you to prioritize traffic on LAN and WAN links based on Quality of Service (QoS) tags. The Pano Direct Service Protocol doesn't directly implement QoS tags, but you may still be able to prioritize Pano traffic based on the ports used or the MAC addresses of the Pano System Endpoints and servers. In general, you should only prioritize Voice over IP (VoIP) traffic (and possibly IP video), over Pano traffic, with all other traffic given a lower priority.

In addition, multicast transmission needs to be enabled within the data center switches to enable Pano Controller group communication. It is not uncommon for multicasting to be disabled by default.

Other Network Infrastructure

You will also need to provide the following network infrastructure:

- **Directory Service:** a directory service (for example, Active Directory, version 2003 or later) is required for most production deployments to provide user authentication and enable additional user-based functionality in Pano Controller. For a list of supported directory services, go to Supported Directory Services. If you choose not to integrate a directory services server, all DVMs will only be able to use device-based DVM collections – for information on DVM collections, go to DVM Collections and Storage Choices.
- **DHCP Server:** Make sure the DHCP network service is available on any network segment that hosts Pano System Endpoints - this is typically provided by either Windows Server or a router. The DHCP server should have a sufficient number of IP addresses for both the Pano System Endpoints and DVMs. Pano System Endpoints and DVMs can be on different network segments and IP subnets as long as they are routable.
- **File Server for User Files:** As a best practice, keep user files on a file server separate from the DVM image. This improves performance by not bogging down the desktop

server's storage capacity and IOPS with user file traffic. It also improves availability by reducing the user's dependence on access to a specific DVM image containing their files. Go to Server/Storage Best Practices for more information.

Site Assessment

Perform a site assessment to check that your location and data center are prepared.

Prepare Server Location

You should review the data center location for the desktop and infrastructure servers. Make sure there is sufficient physical space and cooling for both the infrastructure servers and any other related infrastructure, such as SAN arrays or network infrastructure. Because of the bandwidth requirements for virtual desktops, both for traffic coming in from Panos on an edge network and for connections between servers and your SAN, multiple network drops may be required for each server.

Since both desktop and infrastructure servers can require considerable time to restart and power back on any required virtual machines, be sure to provide adequate backup power for all of the servers to allow operations to continue through power interruptions.

Refer to your server's documentation for your server's power and operating conditions requirements.

Assess Pano Zero Client Deployment Locations

Finally, check on the locations where the Pano Zero Clients will be deployed. For each Pano Zero Client, the following will be required at the location where it is to be installed:

- An AC power outlet for the Pano Zero Client power supply
- A 100 Mbps or better Ethernet connection
- A DVI- or VGA-compatible monitor, with a recommended resolution of at least 1024x768. For information on compatible monitor resolutions, go to Supported Monitor Resolutions.
- A USB keyboard and mouse. For information on compatible USB devices, go to Support for USB Devices.

You can find more information on Pano Zero Client requirements and specifications in the *Pano System Data Sheet* on the Pano Logic web site.

If using Pano Remote clients, a host Windows PC or laptop with a Windows XP SP3 or Windows 7 operating system is required at each user's location. Pano Remote clients also need network connections back to either Pano Controller, if deploying internally, or over the Internet to your Pano Gateway server, if used externally.

User Workload Assessment

An important part of correctly allocating server resources starts with conducting user and application workload assessments to build use cases. These use cases help you estimate the server and storage resources needed for a deployment's specific mix of users. Factors to consider include: the user workload, the operating system being used (Windows XP or Windows 7), the types of applications users will need and the load on the server from other infrastructure or platform software. The following table provides some guidelines for typical workload use cases and corresponding sizings for memory, vCPU and IOPS allocations. These in turn provide general guidelines on the number of DVMs per CPU core and the number of users per server for each workload use case.

Attribute	Light Workloads	Medium Workloads	Heavy Workloads
Application Usage	Task workers running 1 or 2 applications, for example, a web browser or billing app	Knowledge workers running multiple apps simultaneously, including Office	Power users of financial modeling or scientific apps; users viewing full-screen or HD video
Memory per DVM	768MB for Windows XP;2GB for Windows 7	1 GB for Windows XP; 2GB for Windows 7	2 GB for Windows XP; 2+ GB for Windows 7
vCPUs/DVM	1 vCPU	1 – 2 vCPUs	2 vCPUs
IOPS/DVM	Approximately 30 IOPS per DVM	Approximately 40 IOPS per DVM	Approximately 50 or more IOPS per DVM
DVMs per Server CPU Core	Approximately 6 - 7 DVMs per core	Approximately 4 – 5 DVMs per core	Approximately 3 – 4 DVMs per core, but for best performance, allocate as many resources as necessary in the hypervisor.
Average Users/ Server	40 users per server	30 users per server	25 or fewer users per server

DVM Collections and Storage Choices

Pano Controller supports several different forms of DVM collections to simplify provisioning. Collections are used to configure and manage groups of similar DVMs. The types of collections used, along with the level of availability and fault-tolerance required, can determine what storage architecture choices will work best for your Pano deployment.

DVMs can be assigned based on user, device and third-party connection broker collections. 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. Use device-based collections to force a specific Pano System Endpoint to always connect to a specific DVM.

Users can be assigned multiple desktops. For example, a doctor in a clinic might have one permanently-assigned desktop available in their office and a different desktop assigned to an examination room, where each doctor needs to be able to access and update patient records using a certain application.

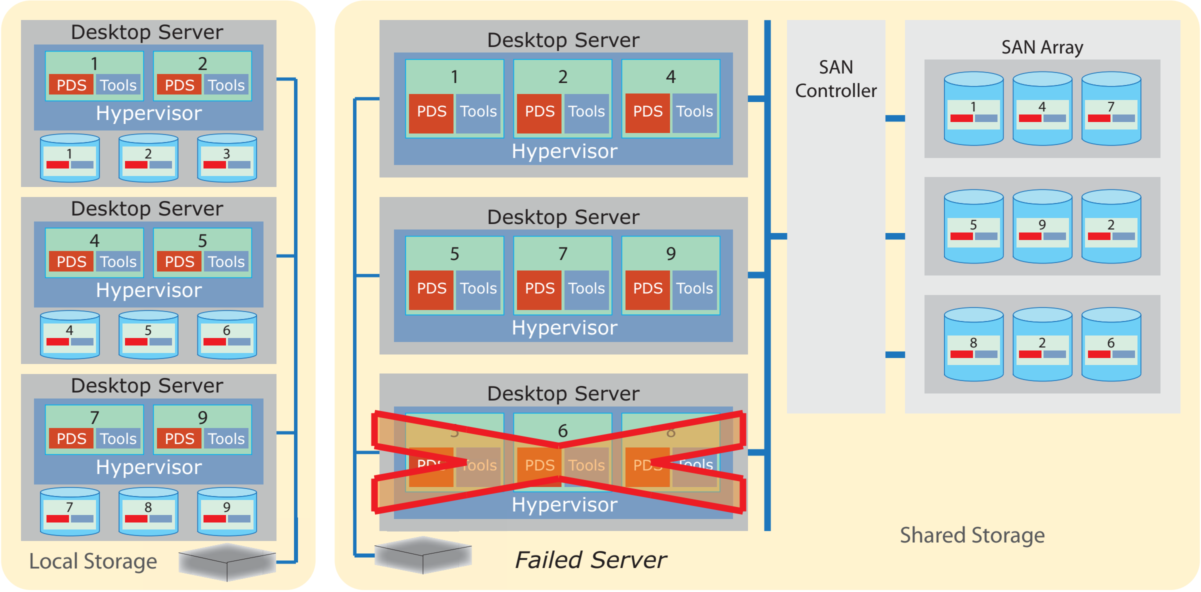
Related Topics

DVM Collections

Local Storage vs. Shared Storage

The decision to use direct attached storage (local storage) vs. a storage area network (shared storage) is largely dependent on the availability requirements for users and the types of DVM collections used. Any DVM stored on local storage is at risk of being unavailable if the server is down due to failure or maintenance. The following figure shows how each server using local storage is only able to run the DVMs it stores.

If this risk is acceptable, or if there are alternate, equivalent DVMs on other servers, then local storage can be used to reduce the cost of storage. However, if DVMs are unique for each user and high availability is required, such as in cases where DVMs have been permanently assigned to users to replace their previous desktop PCs, then shared storage should be used, despite its higher cost. Shared storage, as illustrated in the following figure, allows any desktop server to host any DVM and provides fault tolerance in the event of a server failure, but with the added cost and management complexity of the required storage networks, controllers and arrays.



Pooled Desktops – Local Storage

For this type of DVM collection, local storage can be used to reduce storage costs because users don't need access to a specific DVM, but rather draw DVMs from a shared pool, based on a standard DVM template. Users are assigned the first available DVM from the pool at user login. An example might be standardized desktops used by task workers in a call center or workstations in a training classroom. After the user logs out, the DVM is returned to the pool. If a desktop server fails, a DVM from the same pool or template on another server can be provided to the user. Any sessions that are active on the failed server when the interruption occurs will be terminated. Because users are not guaranteed to be assigned the same DVM on subsequent logins, you may need to leverage folder redirection and/or third-party solutions to ensure persistent user personalization, user-installed applications and so on across different desktops in the pool.

Permanently Assigned – Local Storage

This type of DVM collection can use local storage to reduce storage cost; however, this entails some availability risk. In this type of collection, users are tied to specific DVMs. An example might be where DVMs are replacing a knowledge worker’s previously dedicated PC. If a desktop server becomes unavailable, the sessions for the users with DVMs running on the server will be terminated and the desktops will be unavailable. These users will have to wait for the system administrator to assign alternate desktops or until the server storing their DVMs is back online.

Permanently Assigned – Shared Storage

This type of DVM collection requires shared storage, such as a SAN, if any level of availability after server failures is required. This maintains high availability for users tied to a specific DVM, such as DVMs replacing a knowledge worker’s PC, but involves higher cost. With shared storage, the users’ DVMs may be migrated to other desktop servers in the cluster either manually or automatically.

Next: Virtualization Platform Options

Virtualization Platform Options

Pano System works with the following virtualization platforms: VMware vSphere™ and VMware View™, Microsoft Hyper-V™, and Citrix XenDesktop. Support for all of the platforms is included with Pano System – you select the desired platform during system installation. The platforms provide different management tools, DVM collections and scalability features. Also, the Pano Controller appliance role differs between platforms. Pano Controller in Full Mode can be configured with local VDB connection broker or a third party connection broker. Pano Controller in ZCC role must be configured with a third party broker and supports highly scalable deployments.

Virtualization Platform (Server)	Appliance Role	Connection Broker	Deployment Size
VMware	Full Mode	local VDB	<1000
	Full Mode (with third-party Broker)	VMware View Citrix XD5	<1000
	ZCC	VMware View	<2000
XenServer	ZCC	Citrix XD5	<2000
HyperV	Full Mode	local VDB	<400

Other than noting scalability limits, Pano Logic doesn't recommend specific virtualization platforms, allowing you to make a selection based on how they fit into your current infrastructure and expertise. For example, you might select a platform based on one or more of the following criteria:

- You might select one hypervisor platform over another to leverage your previous experience with it in server or application virtualization, such as with XenApp. Or you might already be using one of the platforms for virtual desktops in some other parts of your organization.
- You might already have existing licenses or volume license agreements with a specific platform vendor that can be used to support Pano deployments with lower or even no new license fees.
- You might prefer one platform's hypervisor architecture or management tools. For example you might have already standardized on Windows Server 2008 R2 on all of your servers, making use of Hyper-V a good fit.
- You might be planning hybrid virtual desktop installations with a mixture of Pano Zero Clients, thin clients and even PCs and laptops as virtual desktop endpoints, making VMware View or XenDesktop better choices.
- The eventual size of your deployment may be a deciding factor – in general, customers planning to eventually deploy over 400 seats select either the Citrix or VMware platforms, and customers deploying fewer than 400 seats might select any of the three platforms.
- If you are deploying over 1,000 seats, support for very large deployments provided by integrating third party connection brokers can also help determine your choice.

Related Topics

Required and Optional Platform Components

Required and Optional Platform Components

For a list of the required components for the supported virtualization platforms and their associated functionality, go to Supported Virtualization Platforms.

VMware Optional Components

VMware View Connection Server – part of VMware View Connection Server and included in both VMware View editions – is recommended as an alternate connection broker for large installations of over 1,000 seats. View Connection Server is also needed for deployments that include heterogeneous populations of virtual desktop clients, such as combinations of Pano Zero Clients, thin clients and repurposed PCs or laptops running the VMware View client software.

View Composer – part of the View Premier Edition – is only recommended for installations over 1,000 seats on the VMware platform. View Composer adds support for linked clones, which can provide storage savings via deduplication of operating system and application images. This helps to reduce duplication of files on the server, thereby reducing the amount of required storage space.

Hyper-V Optional Components

Microsoft provides an option to download a free version of Hyper-V Server 2008 R2, allowing you to configure infrastructure servers as your deployment needs grow without any additional license costs. This can support a very low-cost expansion of deployments up to 400 seats. However, note that this configuration does not provide a graphical user interface (GUI) or support for clustering or Windows high availability. And Microsoft System Center Virtual Machine Manager will still require at least one infrastructure server or VM running Windows Server 2008 as a platform.

Citrix Optional Components

You can optionally deploy Citrix Provisioning Services, which enables you to use a single DVM image template to create multiple DVM images on one or more infrastructure servers. This can greatly reduce the amount of storage required compared to other methods of creating DVM images. This form of storage optimization is typically most useful in deployments of 500 or more seats where the savings in storage space will offset the added costs and complexity.

Pano Controller connects to the XenDesktop Controller connection broker via a single API or interface. If you have a very large and active deployment, the number of connection broker requests might overload a single Controller instance, resulting in unacceptable response times and a degraded user experience. XenDesktop supports deploying multiple Controller instances on one or more servers to provide both scalability and redundancy. However, some form of load balancer is needed to distribute the requests from Pano Controller to the different Controller instances. Citrix NetScaler is recommended as a load balancer that can provide Pano Controller-to-Controller connections.

Next: Pano Controller Resource Requirements

Pano Controller Resource Requirements

The size of the deployment (based on the number of seats) affects the resources required for your Pano Controller group. A Pano Controller group can consist of a single Pano Controller for small-scale deployments to a group of primary and secondary Pano Controllers with up to four additional auxiliary Pano Controllers to the group for scalability.

Make sure that each Pano Controller in you group(s) meets the requirements listed in System Requirements.

Next: Sizing Server and Storage Requirements

Related Topics

Configure Pano Controller Groups

About Pano Controller Scalability and Redundancy

Sizing Server and Storage Requirements

This section describes the server and storage hardware requirements for servers used in virtual desktop deployments. In general, just four server and storage hardware factors will influence the density of users per server that can be supported:

- Processor cores per server and the speed of the cores
- RAM per server, especially on desktop servers
- Available storage system IOPS
- Bandwidth from physical network (NIC) and SAN connections

The following topics are covered:

- Server Architectures
- Allocating Server Resources
- Storage Capacity Requirements
- Storage IOPS Requirements
- Estimating IOPS Requirements per DVM

Server Architectures

Decisions on server architecture need to be driven by a balance between server CPU capabilities, RAM capacity and bandwidth and network connection bandwidth. For Pano deployments of several hundred or more seats, this suggests deploying a large number of 1U or 2U servers equipped with moderate CPUs, such as dual quad-core or six-core Intel® Nehalem or Westmere CPUs (such as E5620 or better), 48 to 72 GB of RAM and multiple NICs and SAN interfaces.

Additional processing capacity can be found by deploying multi-socketed servers with Intel 7500 series Xeon or AMD CPUs, potentially with hundreds of GB of RAM. However, using these larger servers rather than a greater number of smaller dual-socketed servers can both increase per-seat costs and shift the bottleneck from the CPU over to memory capacity, and storage or network bandwidth. Using fewer servers also reduces the level of availability provided by server redundancy. If rack-space requirements are a driving factor, blade-servers can be used in place of 1U servers, although typically at a higher relative cost.

Using servers with earlier, pre-Nehalem processor architectures will reduce the number of seats that can be supported per server CPU core, as the latest microprocessor technology directly incorporates native support for virtualization. Although it might be tempting to employ old servers that might be available after a server consolidation or which might have some unused capacity for virtualization, this approach can result in an unsatisfactory user experience due to slow server performance.

Since any interruption in the servers' operations can at least temporarily suspend the access to virtual desktops, deploying servers with fault-tolerant hardware, such as redundant power supplies, hot-swap drives and fans, and RAID controllers with battery backup for write-caching, may be a useful investment.

Go to User Workload Assessment for information on the typical capacity factors per server based on specific use cases.

Next: Allocating Server Resources

Allocating Server Resources

Virtual CPUs (vCPUs) represent a virtualized CPU core provided to the hosted operating system by the virtualization platform's hypervisor. A single vCPU allocation to a virtual machine would correspond to permission to concurrently share one physical CPU core.

Because of the scheduling done by the hypervisor across all available CPU resources, it is possible to provision more vCPUs than available physical CPU cores. In addition, the frequent pauses in processing loads for desktop virtual machines make their resource needs less strenuous than that of server VMs, which continually process many incoming requests. As a rule of thumb, each physical CPU core provides four vCPUs that can be allocated to DVMs.

This means that a server with dual CPU sockets and two quad-core CPUs, (thus, 8 physical cores) would have up to 32 vCPUs cores available at any time. When a desktop virtual machine with a specific vCPU allocation needs processing time, and sufficient physical cores are available, the hypervisor permits processing to go forward. However, if all vCPUs are allocated, the DVM will be put into a wait state until resources are available. Because of this, and depending on the user workload patterns they support, you should keep the number of vCPUs allocated to concurrently active DVMs close to the actual vCPUs available to ensure predictable performance.

On some virtualization platforms, you can also set MHz reservations (minimums) and limits (maximums) on allocations of vCPU processing resources. By default, vCPUs are assigned the same speed in GHz as the physical CPU core. These reservations and limits can provide finer control over resource allocations, especially for VMs that have fairly consistent loads. However they generally aren't recommended for virtual desktop DVMs, as their loads can have substantial bursts of activity, thus this sort of vCPU restriction can introduce unnecessary wait states and degrade the user experience or over-allocate resources.

Estimating Workloads for Allocations

Beyond the general workload use cases shown in User Workload Assessment, some other factors driving a need for higher vCPU allocations can be included in your assessment of server requirements:

- Applications running in the DVM (e.g. browser, Excel) will consume the same level of CPU resources as on a PC. The more applications you run and the more processing intensive they are, especially on a consistent basis, the more CPU time will be consumed.
- Pano Direct Service needs a certain amount of CPU time in order to process and transfer the desktop experience over the network to the Pano System Endpoint. The amount of CPU time needed is directly proportional to the activity on the display. Active displays (e.g. video playback, graphically rich web sites, rapidly scrolling through documents, resizing or dragging windows, etc.) cause higher vCPU consumption.

It is important to ensure that vCPU allocation (1) does not consume most or all the CPU resources, because if it does, then (2) the system won't have enough resources available to deliver the experience.

Users with dual displays will probably have more applications active, thereby consuming CPU time. They may also generate more display updates as users jump between applications or drag applications between screens. Playing video on one screen while working in Excel on another is supported, but definitely constitutes a heavy workload.

In addition, applications that require low latency (e.g. isochronous USB) will also perform better when there are sufficient CPU resources available. For example, use of web conferencing generally requires two vCPUs, while audio-only VoIP can benefit from two vCPUs. Even so, users running web conferencing and VoIP applications may be fine with one vCPU, depending on whether they are running other applications simultaneously.

You can use the Windows Task Manager inside the DVM (or even on a regular PC) to look at the percentage of CPU time being consumed by specific application or Pano Direct Service processes and workloads.

Simultaneous Peak Resource Demands

With centralized virtual desktops, server resources are shared across all active user sessions. In most cases, you can safely assume that users are performing different activities at any point in time and that periods of high usage (peaks) and periods of low usage (valleys) will tend to cancel each other out. In some cases, such as in a computer lab or training center, all users may be asked to perform the same task at the same time (such as logging in – causing a "login storm"), thus creating a situation in which individual peaks will coincide. In such cases, you will need to allocate sufficient resources to cover needs during these periods of simultaneous peak usage.

Go to Best Practices for Deploying Pano Zero Clients for information about applications and utilities, like anti-virus software, that can consume excessive resources.

Go to Ways To Optimize DVM Performance for information about scaling Pano Systems to accommodate large deployments and About Pano Controller Scalability and Redundancy for information on configuring system redundancy to maximize availability.

Next: Storage Capacity Requirements

Storage Capacity Requirements

This section discusses how to estimate the storage requirements for your deployment.

Estimating DVM Storage Capacity

To estimate storage capacity needed, determine how much virtual disk space is required for the local operating system and installed applications for each DVM, allowing an extra 1 – 2 GB for Windows temporary and page files. The size of the virtual disk for DVMs should be kept to a minimum. Larger DVMs will consume more storage resources and make provisioning of new DVMs take longer. If user files are redirected to a file server and users don't install numerous applications after provisioning, the storage requirements for each DVM should be fairly static.

Multiply this size by the number of DVMs, and add 50 GB overhead for Pano Controller VMs and other platform software. In counting DVMs to estimate required storage capacity, be sure to allow for both active DVMs and inactive or template DVMs. If you're not sure how many template or inactive DVMs will be used, a general rule of thumb would be to allow for

1.5 DVMs per user. This should provide a rough estimate of the capacity needed for the deployment. However, the performance of most storage systems and hard drives drops quickly as they exceed 80% capacity utilization. To avoid these performance problems, add another 25% to the calculated capacity to reserve at least that much unused capacity.

Allowing for RAID Overhead

DVM images are typically stored on RAID arrays that also store redundant parity information to allow the array to continue running after the loss of a drive (with RAID 5 designed to survive the loss of one drive and RAID 6 designed to survive the concurrent loss of two drives). Because of this you also need to add sufficient extra storage capacity overhead for that parity information. The amount of this overhead will vary depending on the number of drives in the array and the RAID level used. A good rule of thumb is to add another 15-25% to your storage capacity requirements to account for this RAID overhead.

DVM Cloning and Deduplication

Some optional platform tools, like VMware View Composer and Citrix Provisioning Services, can reduce the overall storage capacity needed for DVMs via de-duplication techniques like linked clones. This allows a static file (or block within a file), like an operating system component or application DLL, to be stored only once and then be streamed or provisioned to multiple DVMs as they are put into use. Depending on the type and composition of your DVMs, these tools can reduce DVM storage capacity requirements by up to 50%, but at the cost of additional complexity and, in some cases, license fees.

Storage System Deduplication

If the storage subsystem hardware implements data deduplication, it will typically come at a cost in terms of latency and total IOPS supplied by the storage subsystem. Although deduplication can deliver storage capacity reductions of as much as 20 to 1, this sort of storage processing – either done in-line (or on-the-fly) as data is written or post-write after the data is saved – is better suited for large static data like backups rather than smaller, more dynamic data like virtual machine images.

In-line data deduplication is typically much slower than the storage processing needed by virtual machines and can introduce latencies that greatly reduce the DVM user experience. On the other hand, post-write deduplication can be performed by storage systems after the data is initially saved, providing more time to scan for and remove redundant data. While this reduces the real-time load on the storage system it still creates a lot of activity that can reduce the number of IOPS available for real-time processing of virtual machine workloads.

Factor/ Calculation	Value	Description
Number of Seats or Users	# Users	For permanently assigned desktops, number of named users using Panos. For pooled desktops, number of concurrently active users.
Number of DVM Images	DVMs/User	Include active DVMs, template DVMs, inactive DVMs – typically 1.5 DVMs/user.
Average Size of DVMs	DVM Size	Size of virtual disk image for DVMs – typically 15 to 20 GB each, assuming folder redirection used for user files.
% reduction from Deduplication	Varies	Potential percentage reduction in capacity needed due to deduplication or cloning of DVMs.
+ System VM Overhead	+ 50 GB/server	Add 50 GB overhead per server for Pano Controller and platform VMs.
= Net Capacity needed	Net Capacity = (# Users x DVMs/User x DVM Size x (1 – Deduplication %)) + Overhead	
Reserve free space %	25%	Keep 20% free space in storage to avoid performance drops.
Allow for RAID overhead %	15 - 25%	Subtract RAID overhead percentage for parity information storage.
= Raw Capacity Needed	Raw Capacity = Net Capacity x (1- Free Space %) x (1 – RAID overhead %)	

Next: Storage IOPS Requirements

Storage IOPS Requirements

In addition to storage capacity, input/output operations per second (IOPS) is the other critical factor in sizing storage systems to ensure adequate storage performance for DVMs. Inadequate IOPS will cause DVM processing to pause until storage resources becomes available, degrading the interactivity of the user interface. Available IOPS will depend on the IOPS capability of the drives servicing the DVMs, times the number of drives, less any overhead from RAID-array write-processing of parity information, as described below.

Hard drive vendors often provide a raw IOPS number for each drive model. However, these figures may be overstated and they don’t take into account IOPS used inside RAID arrays to write parity information. The total number of raw IOPS from all drives needs to be adjusted for the overhead of RAID arrays. This overhead only applies to write operations – for read operations, RAID drives can perform much like the combined performance of the included drives. DVMs tend to use a much higher proportion of read IOPS than write IOPS, especially if certain optimizations, such as disabling the Windows page file and indexing, are used to limit unnecessary writes.

Factor/Calculation	Value	Description
Number of Drives	# Drives	Add up the number of either direct attached or storage array drives.
Determine IOPS / Drive	IOPS/Drive	Calculate or look up the number of IOPS supplied by the drives you are using – rotation speed (RPM), average disk access latency and seek times. Typical values for 2.5" enterprise-grade SAS drives are 140 raw IOPS per 10K RPM drive and 180 raw IOPS per 15K RPM drive.
= Raw IOPS	Raw IOPS = # Drives x IOPS/Drive	
RAID overhead factor	IOPS/Write	For RAID 5 arrays, this RAID overhead factor can require up to 4 IOPS for each write operation, while RAID 6 arrays can require up to 6 IOPS per write for parity information.
Estimated % Writes	Varies	Estimate the percentage of write operations – typical values for Pano DVMs might be 20-30% if the correct optimizations are performed.
= Total Overhead in IOPS	Total Overhead = Raw IOPS x % Writes x RAID Overhead/Write	
= Available IOPS	Available IOPS = Raw IOPS – Total Overhead	

Provided it delivers adequate bandwidth and low latency (well under 25 ms round-trip for reads and writes) the technology, such as direct Fibre Channel links, iSCSI over teamed gigabit Ethernet, used to interconnect storage systems like SAN arrays and desktop servers won't have any significant impact on the number of IOPS delivered.

Estimating IOPS Requirements per DVM

Storage IOPS available to DVMs on the desktop hypervisor servers will tend to be the gating factor for many virtual desktop deployments. Using servers with more robust CPUs or more RAM can slightly lower the total number of servers required, but the number of available IOPS is critical. To estimate the number of IOPS needed, assume each concurrently active DVM needs about 30-50 IOPS. Go to User Workload Assessment for more information.

One source of unnecessary IOPS consumption is memory paging in VMs. Best practice is to minimize Windows and hypervisor page file access and leverage physical server RAM instead of using the disk system. To accomplish this, allocate sufficient physical server RAM per DVM to support the needs of the operating system and applications, while keeping paging to a minimum. Then set the Windows page file size inside the DVMs to 50% of the allocated RAM.

For DVMs, expect to see a high level of IOPS with a ratio of roughly 90% read and 10% write operations during boot up or powering on of a DVM, and then a reversal of that ratio to a much, much lower level of IOPS, but with only 20% read and 80% write operations once Windows is fully loaded. The first ratio only applies to the initial powering on of a DVM – if it is left running and users simply log in and out via the Pano System Endpoint's dialogs or by using the Pano Button®, only the second ratio will continue, often for many days until the DVM is restarted to apply updates or to correct a temporary problem. This ratio also assumes that network folder redirection is in place and that users aren't working from documents stored locally within their DVMs. Latency between the shared storage and the desktop and infrastructure servers should stay well below 25 ms for both read and write operations.

For Pano Controller, storage IOPS from its VM are minimal, as almost everything gets cached into the infrastructure server's memory. For some platform-specific DVM provisioning and management tools, like vCenter Server, shared storage IOPS can be minimal if the administrator configured them to rely on a separate network-based database server. However, if the supporting database instance is on the same infrastructure server as the platform tool (not recommended for deployments over 200 seats), you may see a significant use of IOPS depending on whether the administrator has enabled non-default reporting settings and or is using the database for additional workload, such as update managers, etc.

Shared storage IOPS for some other platform tools can be significant, depending on whether you are using a SAN that works well them or not. As such, it is difficult to give general IOPS estimation. Check with the virtualization platform vendor for their recommended best practices and be prepared to monitor storage traffic and make adjustments to the storage architecture if problems arise.

Next: Best Practices for Deploying Pano Zero Clients

Best Practices for Deploying Pano Zero Clients

This section contains best practice guidelines for effectively deploying Pano System virtual desktops. The following topics are covered:

- DVM Best Practices
- Network Best Practices
- Server/Storage Best Practices
- Deployment Best Practices

DVM Best Practices

Advise users to close applications and files – because of the persistent access to their Pano desktops, users may tend to leave a broad set of applications running and files open all the time, leading to much higher use of RAM and CPU time and overall poor performance. Either train users to close the applications and files they don’t need in the near term, or force periodic restarts of the DVMs.

Application and utility behavior can cause performance problems – applications and utilities may be written or configured to assume they should have unlimited use of any unused personal computer RAM or processing resources. This behavior is inappropriate in a shared hypervisor server. For example, an anti-virus application initiating scans whenever it detects the DVM is idle can result in a lot of redundant processing and thrashing of disks. To solve this particular problem, use security software that is virtualization-aware. This can be accomplished by using products that work with VMware’s vShield™ Endpoint, which reduces the overhead within each DVM. Or, use an anti-virus application that is intelligent enough to be aware of virtualization and is able to stagger updates and scans between DVMs.

Windows OS optimizations – be sure to apply the Windows OS optimizations listed for Windows XP and 7 in Ways To Optimize DVM Performance to each DVM or template. Windows has a number of behaviors that over-use processing resources on the shared infrastructure server or are inappropriate, such as sleep and hibernate.

Look for hidden user files in DVMs – although you might set up folder redirection to point users’ My Documents folders to a file server, there can be many hidden user files that bloat DVMs and bog down the hypervisors. A prime example would be the email cache maintained by clients like Microsoft Outlook®. Such client applications replicate some portion of the mail, calendar and contacts data store from an Exchange server into a PST file (which can be several gigabytes in size) in the DVM’s hidden Application Data folder.

Network Best Practices

Simplify IP addressing – assign a static IP address to the Pano Controller VM. The default method for assigning an IP address to the Pano Controller VM during network configuration is to use DHCP. However, to avoid additional name-configuration steps related to name resolution, it is recommended that you assign a static IP address to the Pano Controller VM. (If you are configuring a Pano System for redundancy, assign two static IP addresses: one each for the primary and secondary instance of Pano Controller. Go to Set Up and Manage Redundancy for more information.)

Switch multicasting support – if you plan to configure for redundancy, you need to configure a Pano Controller group. If the Pano Controller instances in a group are not all connected to the same Ethernet switch, make sure that the switches connecting the Pano Controller servers for the group support transmission control protocol (TCP) multicasting.

VLANs for Panos – consider putting Pano Zero Clients on their own, private VLAN. VLANs are used to define broadcast domains and control multicast, unicast and broadcast transmissions between Layer 2 devices. This can give you much more freedom in the physical location and intervening network infrastructure for your Pano System, at the slight additional expense of some network management overhead.

Check firewalls ports – the Pano System uses certain TCP and UDP ports for communication (go to Internal Ports Used by Pano Controller for information). Check your network firewalls, gateway devices and servers to make sure that these ports are not disabled.

Optimize networks – minimize packet loss, latency and jitter on the network. Any network latency of more than 10 ms (round trip) will cause problems that can degrade the user experience on Pano Zero Clients. This is much less of an issue when using Pano Remote clients, as it uses RDP, a protocol optimized for use on high-latency WANs.

Pano Remote™ uses the Remote Desktop Protocol (RDP) to connect to Pano Gateway™, usually running on a gateway Windows Server 2008 Terminal Services Gateway or Remote Desktop Services server in a DMZ network. Earlier versions of Pano Gateway required that you provide a connection to your directory services server into the DMZ, opening a potential security hole. Pano Gateway 4.5 closes that hole by using local user accounts on the gateway server rather than requiring a direct connection to your directory services.

Server/Storage Best Practices

Don’t over-commit your servers’ physical memory or CPU cores – if using VMware, the ESX paging or swap (to the DVM’s virtual disk) might be slightly better than the desktop Windows capabilities, but performance is much better if there is close to a 1:1 ratio of physical memory to DVMs and a 1:4 ratio of physical server CPU cores to vCPUs. You may need to allocate two vCPUs per DVM for some power users, particularly for users who watch video on their desktops or use isochronous universal serial bus (USB) data flow.

Keep user files out of the DVM’s virtual file space – to ensure that user files are correctly backed up, you should provide a separate file server to store user files. Often you can use group policies set either inside the DVM's operating system or via AD to use folder redirection to make the My Documents (under Windows XP) or Documents (under Windows 7) folder appear to be a local folder (inside the user's DVM) while actually storing the data on the file server. This improves performance by not bogging down the desktop server’s storage capacity and IOPS with user file traffic. It also improves availability by reducing the user’s dependence on access to a specific DVM image containing their files.

Deployment Best Practices

Don’t overuse user profiles policies – overuse of user-configuration policies in pooled desktops can lead to very poor performance. These policies, which are applied at user login, can cause delays during login.

Review backup policies – you should review your current backup polices and then apply them to the Pano deployment as appropriate. At a minimum, you should leverage the Pano System’s built-in backup features to back up Pano Controller, vCenter Server (if using VMware) and master DVM images. The decision to back up each individual DVM depends on your risk-tolerance level. Ideally, you should design your DVMs to be as replaceable as possible by leveraging the folder-redirection concept noted in Server/Storage Best Practices.

Check license compliance – licenses valid on PCs may not be valid in DVMs for both your standard set of applications and those installed by users. While the hypervisors may hide the fact that the “PC” running Windows and the applications is virtual (so that retail copies of applications can install), their licenses may not be valid in a DVM – especially if that DVM is shared between users and/or the Pano System. For example, Microsoft Office must be licensed under a volume license agreement to be used in a virtual desktop.

Next: Deployment Scenarios

10 Deployment Scenarios

To successfully deploy Pano Logic System Endpoints, you need a balance between CPUs, storage, memory and network components. One or more of these components may allow for less of another. It is strongly recommended that you thoroughly evaluate the anticipated workloads of the DVMs and expect to make some adjustments and perform some fine tuning as your production virtual desktop deployment progresses.

This section provides some guidelines concerning the hardware and software requirements for 25-, 500-, 1,000- and 2,000-seat deployment sizes, along with information about sizing and architecture for servers and storage, Pano System configuration, and virtualization platform options. In most cases, you should be able to extrapolate requirements and sizing for intermediate-sized deployments.

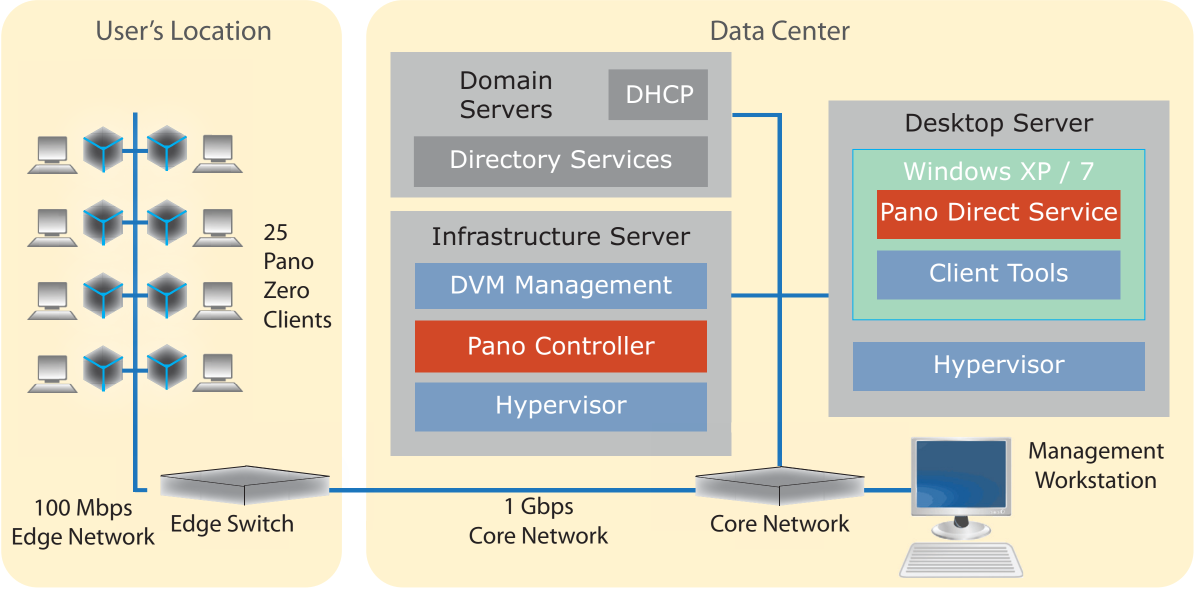
Keep in mind that the recommended hardware and software configurations are based on some assumptions about server performance and user workloads. Specifically, the sample architectures described are based on deploying typical 1U or 2U servers equipped with dual quad-core or six-core Intel® Nehalem or Westmere CPUs (E5620 or better) and 32 to 72 GB of triple-channel, 1333 MHz DDR3 random-access memory (RAM). For additional capacity, multi-socketed servers with Intel 7500 series Xeon® or AMD CPUs can be deployed, potentially with hundreds of GB of RAM. However using these larger high-density servers rather than a greater number of dual-socketed servers can both increase per-seat costs and reduce the level of availability provided by server redundancy.

Finally, these sample architectures assume you are only deploying Pano Zero Clients rather than a mixture of Pano Remote clients, and thin clients or even repurposed PCs used as temporary measures. Most of the same server and storage sizing considerations apply – only network bandwidth and latency needs for the links between the clients and the desktop servers will vary greatly.

- 25-Seat Deployment
- 500-Seat Deployment
- 1,000-Seat Deployment
- 2,000-Seat Deployment

25-Seat Deployment

This provides information on architectures for a basic, 25-seat Pano System deployment.



- Hardware Sizing and Architecture
- Pano System Configuration
- Platform Considerations and Configurations

Hardware Sizing and Architecture

For a 25-seat deployment, typically one desktop server will be needed to host the DVMs, Pano Controller and the hypervisor software. Optionally, a separate infrastructure server can be used to host the Pano Controller virtual machine, platform DVM-management tools, such as vCenter Server (on the VMware hypervisor platform), Microsoft System Center Virtual Machine Manager (SCVMM – on the Microsoft Hyper-V platform) or XenDesktop Controller (on the Citrix platform) and supporting hypervisors.

Given that the storage needs for this deployment size are fairly modest (at 15 - 20 GB per DVM image, including templates and inactive DVMs), direct-attached storage using enterprise-class drives configured as a RAID 5 or RAID 6 volume within the desktop server may be the most cost-effective approach. However, using this sort of internal direct-attached server storage, rather than shared storage like a SAN, means that if a user needs to access a specific DVM image (like a permanently assigned, user-based DVM) and the server containing it is down, the DVM is effectively inaccessible.

In addition to the risks from internal or direct-attached storage, the processing done by a single desktop server also represents a single point of failure – if the server should go offline, access to all of the DVMs would be interrupted. Likewise, the infrastructure server represents another single point of failure – if it were to be offline, user logins would be blocked, although users already connected to their DVMs would be able to continue working until they needed to log in again or connect to another DVM. Both of these availability risks can be mitigated by adding redundant infrastructure and desktop servers, but you will need to assess whether the hardware and software costs involved are feasible for a deployment of this size.

Component	Amount	Description
Desktop Server	1	Dual quad-core Intel Westmere CPU (E5620 or better), and 32-48 GB RAM. Server hosts hypervisor software and Windows DVMs.
Infrastructure Server	1	Server hosts Pano Controller, platform DVM-management tools and supporting hypervisors. Can be hosted on the same desktop server as the DVMs rather than a separate server if user workloads are light.
Storage	Size: 0.6 TB	Allows 15 GB per DVM plus 5 GB overhead for Pano Controller VM, up to 80% capacity utilization and 20% RAID overhead.
	IOPS: 1,040	Requires at least 6 15K RPM drives or 8 10K RPM drives, plus RAID parity drives. Use direct-attached storage internal to servers unless deploying multiple servers for redundancy.
Networking	1	1 Gbps/100 Mbps switch for edge network
	1	1 Gbps segment in the core network
Management Workstation	1	Windows workstation needed to configure and manage the Pano System and platform.

Pano System Configuration

One instance of Pano Controller is sufficient for this deployment size, unless you want to configure the system for future scalability or current redundancy. Pano Controller should be configured for Full Mode and can use the local Pano VDB or a third party connection broker such as VMware View or XenDesktop. Go to Set up Failover Configuration for information.

Pano Controller can run on a separate infrastructure server from the DVMs, which run on a desktop server. While this may be optimum for performance, at this deployment size it is feasible to run Pano Controller on the same server as the DVMs. If you move Pano Controller onto the desktop server, be sure to configure the server with adequate RAM and CPU.

Platform Considerations and Configurations

Required and Optional Software

Go to Supported Virtualization Platforms for a list of the required software for the supported hypervisor platforms. All of the virtualization platforms can support at least 400 concurrent seats.

VMware vSphere/vCenter Server

In this simplest single-server configuration, you can use the free VMware vSphere ESXi hypervisor. vCenter Server is optional, but highly recommended, as it enables significant DVM provisioning capabilities in Pano Controller, including automated provisioning.

Hyper-V

Microsoft provides an option to download a free installation of Hyper-V Server 2008 R2, allowing you to configure infrastructure servers as your deployment needs grow without any additional license costs. This can support a very low-cost expansion of deployments up to 400 seats. However, note that this configuration does not provide a graphical user interface (GUI) or support for clustering or Windows high availability.

If you are not deploying Hyper-V Server on a separate physical server and need more than 32 MB of RAM (a feasible limit if you are supporting only 25 task workers using Windows XP), Windows Server 2008 R2 with Hyper-V Enterprise Edition is recommended for this deployment size.

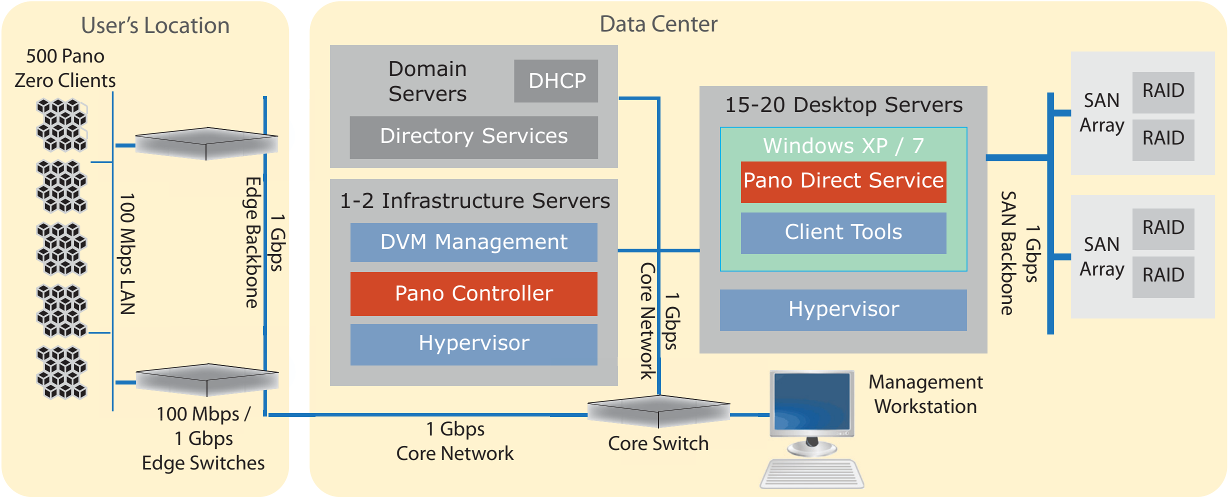
Note that Windows Server is still required as a platform for SCVMM and the Pano Controller SCVMM Connector – if you are using a separate server for SCVMM, you can use the lower-cost Windows Server 2008 R2 with Hyper-V Standard Edition, which is limited to 32 GB of RAM. Even while hosting SCVMM, Windows Server can also provide file sharing, a DHCP server and support for other infrastructure needs. Best practice is to keep SCVMM on its own dedicated instance of Windows, which can be a virtual machine.

Citrix

This configuration requires only a single XenDesktop Controller connected to a single Pano Controller instance. Citrix Provisioning Services may not be required due to the relatively small number of DVMs in this deployment.

500-Seat Deployment

This provides information on architectures for 500-seat Pano System deployments.



- Hardware Sizing and Architecture
- Pano System Configuration
- Platform Considerations and Configurations

Hardware Sizing and Architecture

For a larger, 500-seat deployment, typically at least 15 to 20 desktop servers will be needed to host the DVMs depending on the level of user workloads being supported. One or two infrastructure servers will also be required.

Component	Amount	Description
Desktop Servers	15-20	Each with dual quad-core Intel Westmere CPU (E5620 or better), and 48-72 GB RAM. Server hosts hypervisor software and Windows DVMs.
Infrastructure Servers	1 or 2	Single server unless redundancy or scalability group is used, which requires a second physical server. Servers host Pano Controller, platform management and provisioning tools and supporting hypervisors.
Storage	Size: 11 TB	Allows 15 GB per DVM, plus 5 GB overhead for Pano Controller VM, up to 80% capacity utilization and 20% RAID overhead.
	IOPS: 20,000	Requires SAN with at least 111 15K RPM drives or 143 10K RPM drives, plus RAID parity drives (based on allocation of 40 IOPS/DVM).
Networking	3-4	1 Gbps/100 Mbps switches for edge network
	1-2	1 Gbps segments in the core network
Management Workstation	1	Windows workstation needed to configure and manage the Pano System and platform.

Deployments of this size should use a SAN or NAS for the DVM images. This form of shared storage, along with separate, dedicated high-speed (4 – 10 Gbps) Fibre Channel or Ethernet links between the SAN and the desktop and infrastructure servers, provides the large number of IOPS (20,000) required for adequate performance with 500 concurrently active DVMs. It also improves availability, especially for individually assigned DVMs, as any DVM image can be accessed from any desktop server.

Pano System Configuration

For scalability up to 500 seats, only a single Pano Controller instance is required. However, if you plan to increase the size of your deployment, multiple instances of Pano Controller are required. And if availability is important, you can configure a Pano Controller failover group with two or more Pano Controller instances running on two different physical servers. Pano Controller should be configured in Full Mode and can use the local Pano VDB or a third party connection broker such as VMware View or XenDesktop. Go to Configure Pano Controller Groups for more information.

Platform Considerations and Configurations

Required and Optional Software

Go to Supported Virtualization Platforms for a list of the required software for the supported hypervisor platforms.

VMware vSphere/vCenter Server

VMware ESX or ESXi from VMware View Enterprise Edition or VMware vSphere 4 Standard Edition recommended for up to 1,000 users. vCenter Server is also recommended for anything other than small, single-server deployments; it can be licensed separately on a server basis or per seat as part of VMware View.

VMware View

VMware View Enterprise or Premier Editions can also supply the required vSphere and vCenter Server components along with View Connection Server and, for the Premier Edition, View Composer.

Hyper-V

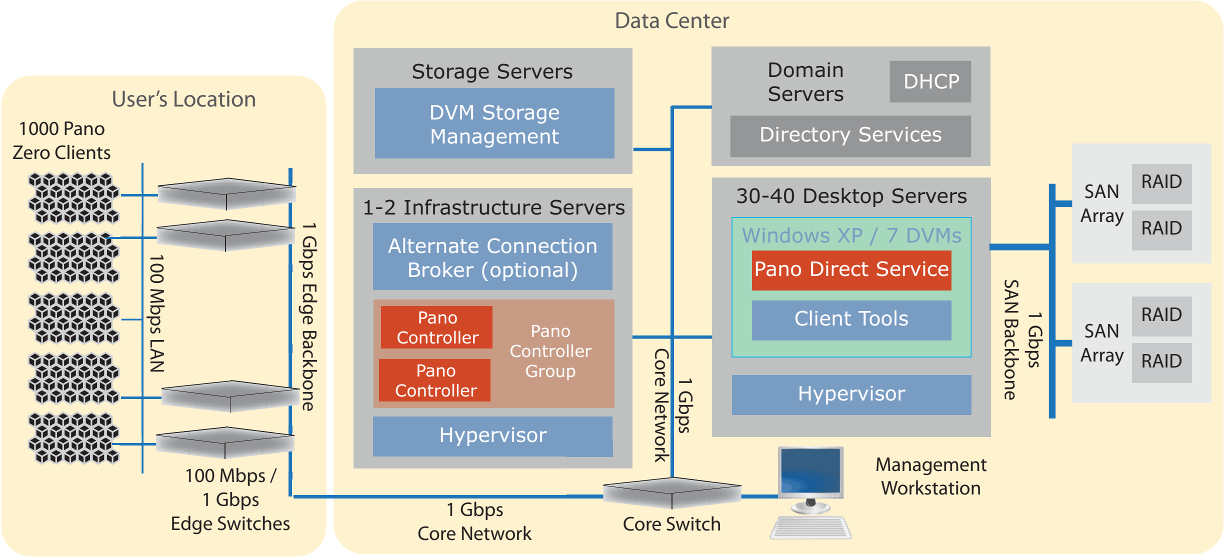
Because scalability is currently limited on Hyper-V to a maximum of 400 seats, this platform is not recommended for this deployment size.

Citrix

More than one XenDesktop Controller connection broker may be required for this deployment size. If so, a load balancer like Citrix NetScaler will also be required. Go to About Load Balancing XenDesktop Controllers for more information.

1,000-Seat Deployment

This provides information on architectures for 1,000-seat Pano System deployments.



- Hardware Sizing and Architecture
- Pano System Configuration
- Platform Considerations and Configurations

Hardware Sizing and Architecture

For a 1,000-seat deployment, typically at least 30 to 40 desktop servers, depending on the level of user workloads, will be needed to host the DVMs. Two to four infrastructure servers are also required.

Shared storage in the form of a SAN or NAS is typically essential for deployments of this size. Shared storage is needed to ensure DVM images remain available in the event of a desktop server failure – something which is much more likely with up to 40 servers. It is also typically required to provide the high level of IOPS (30,000 to 50,000) needed for up to 1,000 active DVMs.

Component	Amount	Description
Desktop Servers	30-40	Each with dual quad-core Intel Westmere CPU (E5620 or better), and 48-72 GB RAM. Server hosts hypervisor software and Windows DVMs.
Infrastructure Servers	2 to 3	Deploy multiple Pano Controller instances in a Pano Controller group for scalability. Servers host Pano Controller, platform management and provisioning tools and supporting hypervisors.
Storage	Size: 22 TB	Allows 15 GB per DVM, up to 80% capacity utilization and 20% RAID overhead.
	IOPS: 40,000	Requires SAN with at least 222 15K RPM drives or 286 10K RPM drives, plus RAID parity drives (based on allocation of 40 IOPS/DVM).
Networking	6-7	1 Gbps/100 Mbps switches for edge network
	4-6	1 Gbps segments in the core network
Management Workstation	1	Windows workstation needed to configure and manage the Pano System and platform.

Pano System Configuration

For a 1,000-seat deployment, to provide sufficient scalability and redundancy (or failover), you should deploy a Pano Controller group with three Pano Controller instances installed on three separate infrastructure servers. Pano Controller can be configured in Full Mode using the local Pano VDB or a third party connection broker such as VMware View or XenDesktop. Pano Controller can also be configured in ZCC role using third party connection brokers such as VMware View or XenDesktop. Go to Configure Pano Controller Groups for more information.

Platform Considerations and Configurations

Required and Optional Software

Go to Supported Virtualization Platforms for a list of the required software for the supported hypervisor platforms.

VMware vSphere/vCenter Server

VMware ESX or ESXi from VMware View Enterprise Edition or VMware vSphere 4 Standard Edition recommended for up to 1,000 users. vCenter Server is also recommended for anything other than small, single-server deployments; it can be licensed separately or as part of VMware View.

VMware View

When using VMware’s View Connection Server as an alternate connection broker, deployments can scale to more than 1,000 users or endpoints. Integrating View Connection Server is also needed if you are deploying heterogeneous endpoint populations that include Pano Zero Client, thin clients and PCs running the VMware View client software.

View Composer, included in the View Premier edition, can let you to take advantage of deduplication of system images via linked clones to optimize storage capacity. Linked clones are particularly useful with pooled populations that can benefit from deduplication via a master image. Using View Composer is only recommended for Pano deployments of 1,000 seats or more due to the added management overhead.

Hyper-V

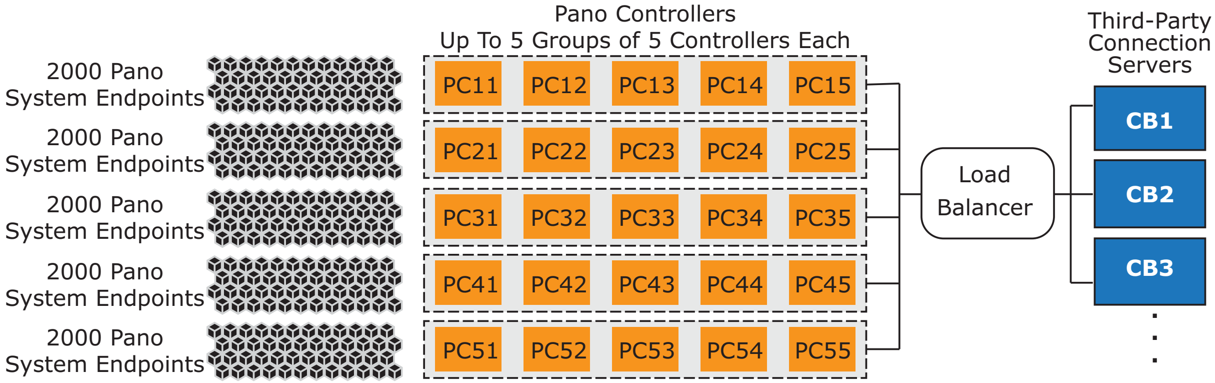
Because scalability is currently limited on Hyper-V to a maximum of 400 seats, this platform is not recommended for this deployment size.

Citrix

For this deployment size, the connection from Pano Controller to the XenDesktop Controller processes used for connection brokering will need to be replicated to several instances to prevent it from becoming a bottleneck. A load balancer like Citrix NetScaler will be needed to connect the Pano Controller instances to the multiple XenDesktop Controller instances. Go to Configure Pano Controller Groups for more information.

2,000-Seat Deployment

This provides information on architectures for 2,000-seat Pano System deployments.


Pano Controllers
Up To 5 Groups of 5 Controllers Each
Third-Party Connection Servers
2000 Pano System Endpoints
2000 Pano System Endpoints
2000 Pano System Endpoints
2000 Pano System Endpoints
2000 Pano System Endpoints
PC11 PC12 PC13 PC14 PC15
PC21 PC22 PC23 PC24 PC25
PC31 PC32 PC33 PC34 PC35
PC41 PC42 PC43 PC44 PC45
PC51 PC52 PC53 PC54 PC55
Load Balancer
CB1
CB2
CB3

Related Topics

- Hardware Sizing and Architecture
- Pano System Configuration
- Platform Considerations and Configurations

Hardware Sizing and Architecture

For a 2,000-seat deployment, typically at least 30 to 40 desktop servers, depending on the level of user workloads, will be needed to host the DVMs. Two to four infrastructure servers are also required.

Shared storage in the form of a SAN or NAS is typically essential for deployments of this size. Shared storage is needed to ensure DVM images remain available in the event of a desktop server failure – something which is much more likely with up to 40 servers. It is also typically required to provide the high level of IOPS (30,000 to 50,000) needed for up to 1,000 active DVMs.

Component	Amount	Description
Desktop Servers	30-40	Each with dual quad-core Intel Westmere CPU (E5620 or better), and 48-72 GB RAM. Server hosts hypervisor software and Windows DVMs.
Infrastructure Servers	2 to 3	Deploy multiple Pano Controller instances in a Pano Controller group for scalability. Servers host Pano Controller, platform management and provisioning tools and supporting hypervisors.
Storage	Size: 22 TB	Allows 15 GB per DVM, up to 80% capacity utilization and 20% RAID overhead.
	IOPS: 40,000	Requires SAN with at least 222 15K RPM drives or 286 10K RPM drives, plus RAID parity drives (based on allocation of 40 IOPS/DVM).
Networking	6-7	1 Gbps/100 Mbps switches for edge network
	4-6	1 Gbps segments in the core network
Management Workstation	1	Windows workstation needed to configure and manage the Pano System and platform.

Pano System Configuration

For a 2,000-seat deployment, to provide sufficient scalability and redundancy (or failover), you should deploy a Pano Controller group with multiple Pano Controller instances installed on separate infrastructure servers. Pano Controller should be configured in ZCC role using a third party connection broker such as VMware View or XenDesktop. Go to About Load Balancing XenDesktop Controllers for more information.

Platform Considerations and Configurations

Required and Optional Software

Go to Supported Virtualization Platformsfor a list of the required software for the supported hypervisor platforms.

VMware vSphere/vCenter Server

VMware ESX or ESXi from VMware View Enterprise Edition or VMware vSphere 4 Standard Edition recommended for up to 2,000 users. vCenter Server is also recommended for anything other than small, single-server deployments; it can be licensed separately or as part of VMware View.

VMware View

When using VMware’s View Connection Server as an alternate connection broker, deployments can scale to more than 2,000 users or endpoints. Integrating View Connection Server is also needed if you are deploying heterogeneous endpoint populations that include Pano Zero Client, thin clients and PCs running the VMware View client software.

View Composer, included in the View Premier edition, can let you to take advantage of deduplication of system images via linked clones to optimize storage capacity. Linked clones are particularly useful with pooled populations that can benefit from deduplication via a master image. Using View Composer is only recommended for Pano deployments of 1,000 seats or more due to the added management overhead.

Citrix

For this deployment size, the connection from Pano Controller to the XenDesktop Controller processes used for connection brokering will need to be replicated to several instances to prevent it from becoming a bottleneck. A load balancer like Citrix NetScaler will be needed to connect the Pano Controller instances to the multiple XenDesktop Controller instances. Go to About Load Balancing XenDesktop Controllers for more information.

Next: Deploying Your Pano System

11
Deploying Your Pano System

This section contains important information on planning your deployment, including flowcharts and decision trees. You should study this section carefully.

The Pano System supports VMware vSphere, Citrix XenServer, and Hyper-V. The Pano System media downloads include software for all supported virtualization platforms. You can decide which platform you want to use when you begin installation. Once installed, a specific Pano Controller instance and all of its managed DVMs are tied to the selected platform. However, you can still run any combination of these installations on the same LAN, provided they are on separate servers.

Don’t worry about installing your Pano System Endpoints just yet. We’ll get to that part later in the deployment, when you configure the Pano Controller for Pano® Client discovery. If you’ve already attached your Pano System Endpoint to the network, it’s normal for the Pano Button light color to be amber until they have been discovered by the Pano Controller.

About Pano Controller

The Pano Controller is the central point of control for all of your Pano System Endpoints and desktop virtual machines; it integrates with your directory service, your virtualization management systems and connection brokers to manage, deploy, and connect virtual desktops to end users.

The Pano Controller is a centrally-hosted server that is delivered as a virtual appliance. Typically, Pano Controller runs as a virtual machine located on the same host servers as your desktop virtual machines. You can add multiple Pano Controllers to your configuration to meet your availability and scalability requirements. In all cases, the Pano Controller:

- Provides secure access to virtual desktops by leveraging services such as Active Directory for user authentication.
- Controls and deploys desktop virtual machines by leveraging virtualization management systems such as Microsoft System Center Virtual Machine Manager (SCVMM) and VMware vCenter Server.
- Connects end users to desktop virtual machines by integrating with its internal connection broker service, XenDesktop or VMware View.

Note: In versions prior to Pano System 5.0 this component was called Pano Manager. It is now called Pano Controller.

The administrator can enable or disable these roles by selecting the appropriate Appliance Role. The Pano Controller must have at least one function enabled.

Next: Deployment Options for Pano Controller

Deployment Options for Pano Controller

The Pano Controller is packaged as a virtual appliance optimized to import seamlessly into your chosen virtualization platform.

Your Pano System can be deployed with a single Pano Controller for your entire environment, or you may deploy groups of Pano Controllers that work together to deliver the redundancy and scalability that you require. If you are starting with a trial or small deployment, you can simply follow the steps below.

If you require redundancy or additional scalability, please consult Pano Controller Deployment Options Decision Tree.

There are three Pano Controller deployment options related to the function of your system.

Standalone Full Mode

By default, the Pano Controller virtual appliance comes configured in Full Mode. In this configuration, the Pano Controller is able to perform all tasks including discovery and control of Pano System Endpoints and brokering and provisioning of desktops. Customers who have deployed earlier versions of Pano System will want to run their Pano Controller in Full Mode because it is functionally equivalent to earlier versions of Pano Manager. This deployment option is the simplest option to configure and provides the full functionality of the Pano System.

If you are planning on using a third-party connection broker, you probably want to use Full Mode with Third-Party Connection Broker.

Full Mode with Third-Party Connection Broker

As an advanced configuration, the administrator may choose to enable only the Virtual Desktop Broker role. This is valid when you have configured a separate instance of Pano Controller running as a Zero Client Controller.

This deployment option allows you to use either XenDesktop or VMware View as the connection broker for user-based assignments. You may also use the Pano Controller's internal connection broker service to support device-based assignments. Choose this option if you want to use a third-party connection broker and you also want to use device-based assignments.

Zero Client Controller with Third-Party Connection Broker

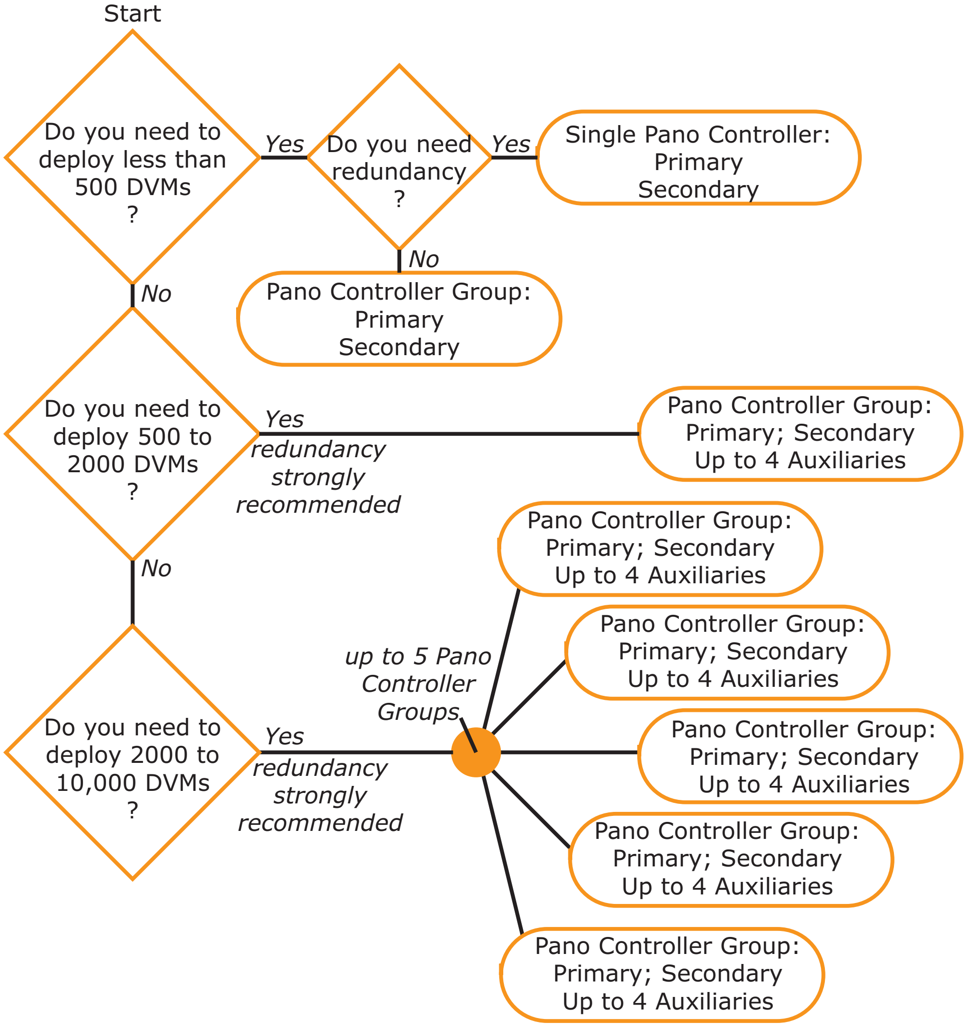
As an advanced setting, the administrator may choose to enable only the Zero Client Controller role. In this configuration, the Pano Controller only discovers and controls Pano Zero Clients and Pano Remote clients. A separate connection broker service is required. This separate connection broker service can be a Pano Virtual Desktop Broker, XenDesktop or VMware View.

This deployment option allows you to use either XenDesktop or VMware View as the exclusive connection broker for your system. With this deployment option you will be limited to user-based assignments only and will not be able to deploy device-based assignments. Choose this option if you want to use a third-party connection broker and you do not want to use device-based assignments.

Note: The new Pano Controller architecture enables a wide range of deployment options. If your needs are not satisfied by any of the options presented above, please contact Pano Logic Professional Services to explore additional options.

Pano Controller Deployment Options Decision Tree

Before deploying, you should use this flowchart to select an option. Make a note of your decision; you will need to know it during deployment. Note that many deployment scenarios require that the controller be set up initially in Full mode, then altered later.


Start
Do you need to deploy less than 500 DVMs ?
Yes
Do you need redundancy ?
Yes
Single Pano Controller: Primary Secondary
No
Pano Controller Group: Primary Secondary
No
Do you need to deploy 500 to 2000 DVMs ?
Yes
redundancy strongly recommended
Pano Controller Group: Primary; Secondary Up to 4 Auxiliaries
No
Do you need to deploy 2000 to 10,000 DVMs ?
Yes
redundancy strongly recommended
up to 5 Pano Controller Groups
Pano Controller Group: Primary; Secondary Up to 4 Auxiliaries
Pano Controller Group: Primary; Secondary Up to 4 Auxiliaries
Pano Controller Group: Primary; Secondary Up to 4 Auxiliaries
Pano Controller Group: Primary; Secondary Up to 4 Auxiliaries
Pano Controller Group: Primary; Secondary Up to 4 Auxiliaries

Next: Scaling

Scaling

Each of the deployment options described above may be deployed using a single instance of the Pano Controller virtual appliance. Each option also allows you to deploy multiple instances of the Pano Controller virtual appliance to gain redundancy and scalability.

Due to the critical nature of virtualized hosted desktops, Pano Logic highly recommends deploying redundant Pano Controller virtual appliances. All of our multi-instance architectures assume a redundant node.

These sections describe how to scale your chosen deployment architecture. The starting point in each case is a single instance of the Pano Controller based on the option you chose to satisfy your functional needs.

Scaling Standalone Full Mode

Scaling Full Mode with Third-Party Connection Broker

Scaling Zero Client Controller with Third-Party Connection Broker

Expanded Scalability

Scaling Standalone Full Mode

If you chose Standalone Full Mode as your desired Pano Controller deployment option, this table will help you determine the appropriate configuration based on your scale requirements. Select the row that satisfies your requirements for number of clients, number of DVMs and redundancy. In all cases, your first step will be to configure a primary instance with Full Mode selected for the Appliance Role; this instance will act as the master node of your Pano Controller group. Next you will configure secondary instance which will add redundancy to your group, but will not increase scalability. Successive instances that are added to the group will be auxiliary instances, which will increase the scale of your system (see Pano Controller Setup Step-by-Step.

Max. End points	Max. DVMs	Redundant	Appliance Role	Primary Instances	Secondary Instances	Auxiliary Instances	Total Instances
500	500	No	Full Mode	1	0	0	1
500	500	Yes	Full Mode	1	1	0	2
1000	750	Yes	Full Mode	1	1	1	3

Scaling Full Mode with Third-Party Connection Broker

If you chose Full Mode with Third-Party Connection Broker as your deployment option, the table below will help you determine the configuration based on your requirements. Select the row that meets your requirements for number of clients, number of DVMs and redundancy. In all cases, your first step will be to configure a primary instance with Full Mode selected for the Appliance Role; this instance will act as the master node of your Pano Controller group. Next, you will configure a secondary instance, which will add redundancy to your group, but will not increase scalability. Successive instances that are added will which will increase the scale of your system.

Max. End points	Max. DVMs	Redundant	Appliance Role	Primary Instances	Secondary Instances	Auxiliary Instances	Total Instances
500	500	No	Full Mode	1	0	0	1
500	500	Yes	Full Mode	1	1	0	2
1000	1000	Yes	Full Mode	1	1	1	3
1500	1500	Yes	Full Mode	1	1	2	4
2000	2000	Yes	Full Mode	1	1	3	5

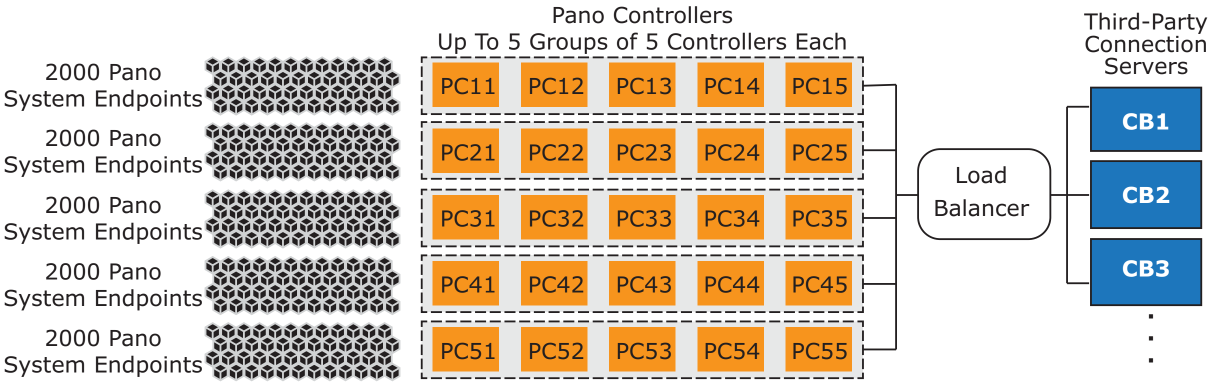
Scaling Zero Client Controller with Third-Party Connection Broker

If you chose Zero Client Controller with Third-Party Connection Broker as your deployment option, this table will help you determine the configuration based on your scale requirements. Select the row that meets your requirements for number of clients, number of DVMs and redundancy. In all cases, your first step will be to configure a primary instance with Zero Client Controller selected for the Appliance Role; this instance will act as the master node of your Pano Controller group. Next you will configure secondary instance, which will add redundancy to your group, but will not increase scalability. Successive instances added to the group will increase the scale of your system.

Max. End points	Max. DVMs	Redundant	Appliance Role	Primary Instances	Secondary Instances	Auxiliary Instances	Total Instances
500	500	No	ZCC	1	0	0	1
500	500	Yes	ZCC	1	1	0	2
1000	1000	Yes	ZCC	1	1	1	3
1500	1500	Yes	ZCC	1	1	2	4
2000	2000	Yes	ZCC	1	1	3	5

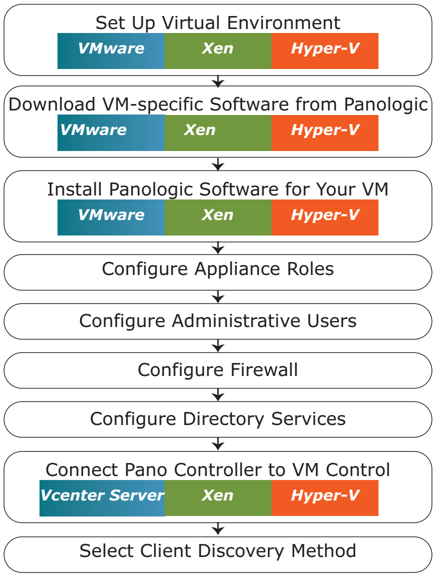
Expanded Scalability

The scalability limits listed above are for a single Pano Controller group. It is possible to scale beyond the above limits when you are using a third-party connection broker. To expand scalability, configure multiple Pano Controller groups and connect them to your third-party connection broker. The diagram below illustrates a 10,000 seat configuration.


Pano Controllers
Up To 5 Groups of 5 Controllers Each
Third-Party Connection Servers
2000 Pano System Endpoints
2000 Pano System Endpoints
2000 Pano System Endpoints
2000 Pano System Endpoints
2000 Pano System Endpoints
PC11 PC12 PC13 PC14 PC15
PC21 PC22 PC23 PC24 PC25
PC31 PC32 PC33 PC34 PC35
PC41 PC42 PC43 PC44 PC45
PC51 PC52 PC53 PC54 PC55
Load Balancer
CB1
CB2
CB3

Next: Pano Controller Setup Step-by-Step

Pano Controller Setup Step-by-Step


Set Up Virtual Environment
VMware
Xen
Hyper-V
Download VM-specific Software from Panologic
VMware
Xen
Hyper-V
Install Panologic Software for Your VM
VMware
Xen
Hyper-V
Configure Appliance Roles
Configure Administrative Users
Configure Firewall
Configure Directory Services
Connect Pano Controller to VM Control
Vcenter Server
Xen
Hyper-V
Select Client Discovery Method

The basic flowchart for Pano Controller installation is shown below. Note that some steps vary slightly according to the virtual platform you are using, but most steps do not.

If you are upgrading an existing installation, see Upgrading Your Pano System to 6.0

.

Task	Go to...
Set up your virtualization environment	For VMware ESX Server and vCenter Server, see VMware Infrastructure documentation. For Citrix XenServer, see Citrix XenServer documentation For SCVMM and Hyper-V, see Microsoft Hyper-V documentation.
Download software	Download your Pano Logic software for the desired platform from the download site, http://download.panologic.com.
Install and configure the Pano Controller VMs	For an overview, start at Pano Controller Setup Step-by-Step. Platform-specific instructions can be found at: Install and Configure Pano Controller on VMware vSphere Install Pano Controller on XenServer Install Pano Controller on Hyper-V

If you are installer multiple Pano Controllers, you should also install Pano Maestro for centralized Pano Controller group management: Deploy Pano Maestro.

You will use the Pano Controller Console to configure options on the Setup tab. Some settings are dependent on your chosen virtualization platform.

Platform	Primary Tools	Instructions
VMware vSphere	Setup tab on Pano Controller Console	Install and Configure Pano Controller on VMware vSphere
Citrix XenServer	Setup tab on Pano Controller Console	Install Pano Controller on XenServer
Microsoft Hyper-V	Setup tab on Pano Controller Console	Pano Controller Configuration

For Pano System configuration, you need to configure for one or more of the following:

Section	Pano System Configuration
Appliance Role	Optional. Default is Full Mode.
Directory Configuration	Required
Virtualization Configuration	Optional. Required for VDB brokering
Broker Configuration	Optional. Required for third-party brokering
Discovery Configuration	Optional
Group Configuration	Optional

Section	Pano System Configuration
Failover Configuration	Optional
Backup Configuration	Recommended
Administrative Roles	Optional
License Configuration	Required
Platform Settings	Optional

Your virtualization configuration requirements depend on your virtualization platform and broker configuration. If you are using Pano VDB connection broker, virtualization configuration is required. If you are using only third-party connection brokering, then virtualization configuration is not required.

If you are using device-based DVMs, Pano VDB brokering is required.

12

Pano Controller Network Port Usage

The components of Pano System, Pano Controller, Pano Direct and Pano Zero Client, communicate with each other on several TCP and UDP network ports. To function properly, these components require access to these ports. You must open these ports and adjust firewall rules accordingly.

Apart from inbound and outbound ports used on the Pano Controller, you also need to specify the ports used between Pano System Endpoints and Pano Direct Service.

For more information, go to Configure DVM Firewall and Configure the Data Center Firewall.

Inbound Ports Used by Pano Controller

Ports	Protocol	Service	Usage
ICMP		ping	Test connectivity to the server
80	TCP	HTTP	Connections from the UI to control the Pano Controller
443	TCP	HTTPS	Secure connections from the UI to control the Pano Controller
22	TCP	SSH	Remote terminal access
68	UDP	DHCP	DHCP responses
123	UDP	NTP	Synchronizing of server time
8318	TCP		Communication between Pano Controllers in a Pano Controller group. The TCP multicast address used by the group is `228.10.10.10`.
8320	UDP		Communication from the Pano System Endpoint to the Pano Controller VM
8321	UDP		Communication from the Pano System Endpoints

Outbound Ports Used by Pano Controller

Ports	Protocol	Service	Usage
ICMP		ping	Test connectivity to the server
53	TCP	DNS	DNS requests
80	TCP		Communication to vCenter Server
443	TCP		SSL communication to vCenter Server
8316	TCP		SSL communication to SCVMM server
8100	TCP		Communication between SCVMM Connector and SCVMM
443	TCP		SSL communication to Citrix XenDesktop Controller
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 System Endpoints
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)
8318	TCP		Communication between Pano Controllers in a Pano Controller group. The TCP multicast address used by the group is `228.10.10.10`.
8321	UDP		Connection brokering to the Pano System Endpoints

Internal Ports Used by Pano Controller

Ports	Protocol	Service	Usage
514	UDP		Log files. The Pano Controller uses this standard port to download syslog messages.
5432	TCP		Postgres database. The database is used by the Pano Controller. The port is used internally (no inbound or outbound). As such, this port cannot be shared with other applications. This port is used on all virtualization platforms.

Inbound Ports Used by Pano Direct Service

Ports	Protocol	Service	Usage
8319	TCP		Communication from the Pano Controller to Pano Direct Service
8321	UDP		Communication from the Pano Controller to the Pano System Endpoints

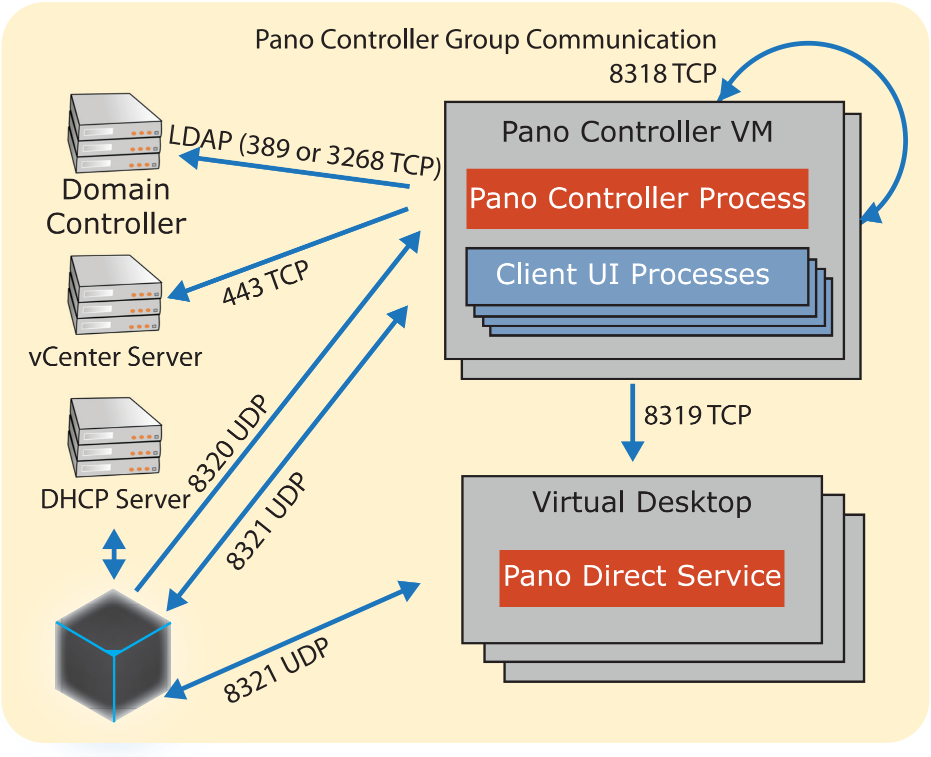
Outbound Ports Used by Pano Devices

Ports	Protocol	Service	Usage
8320	UDP		Communication from a Pano System Endpoint to the Pano Controller
8321	UDP		Bi-directional communication to/from the Pano Controller

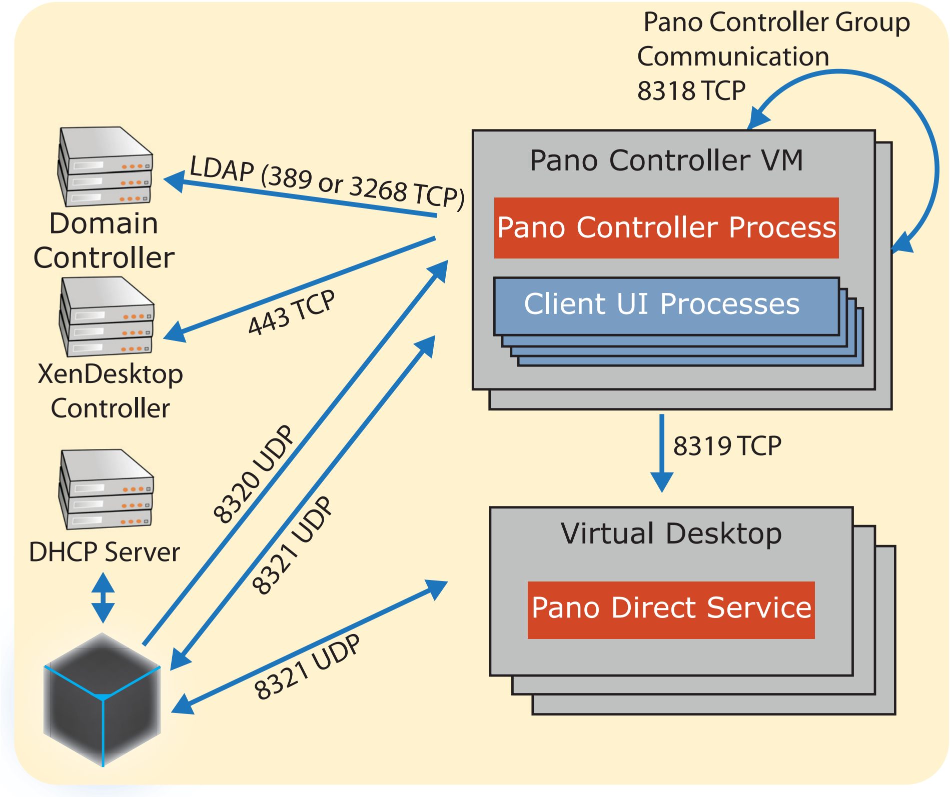
TCP Ports Used by Pano Maestro

TCP Port	Port Usage
80	Web server port for incoming http requests. All the requests to 80 are forwarded to 8080
8080	Maestro port for incoming non secure http requests (for example http://<IPAddress>)
443	Maestro port for incoming secure https requests (for example https://<IPAddress>). Uses default self-signed certificate or customer certificate if configured
8317	Maestro port for incoming secure requests from Pano Controller for license verification or FTS License server for inventory validation

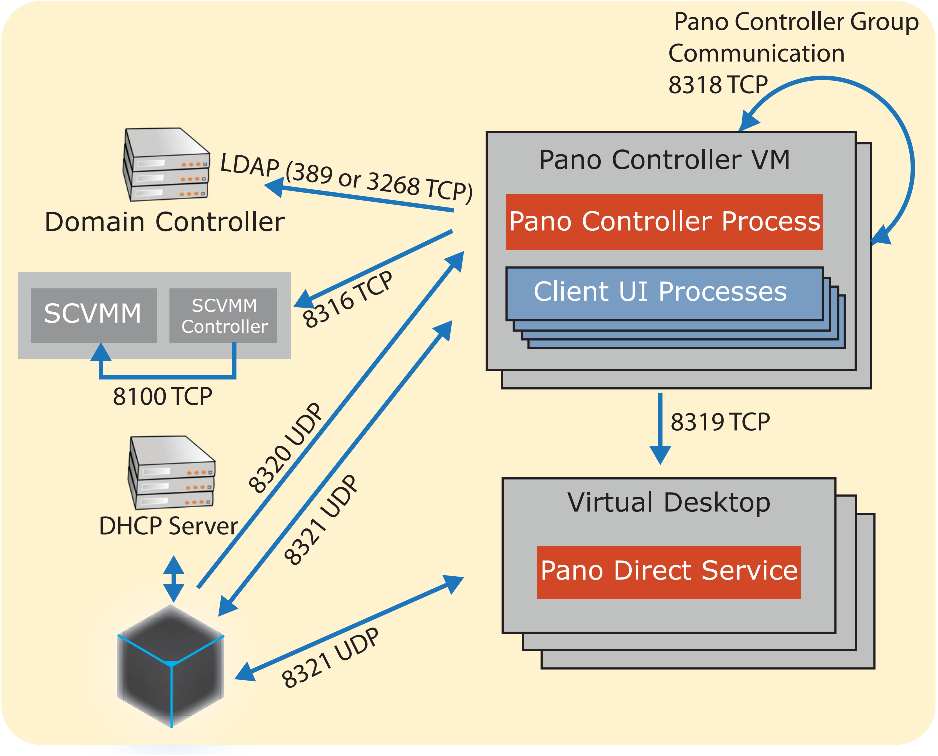
This shows the ports used by Pano with VMware:



This shows the ports used by Pano with XenDesktop



This shows the ports used by Pano with Hyper-V (SCVMM)



13 Install Pano Controller on VMware

This chapter includes the following topics:

- Install and Configure Pano Controller on VMware vSphere System
  - Install and Configure Pano Controller on VMware vSphere
  - Choose Your VMware Virtualization Infrastructure
  - Deploy without vCenter Server and Active Directory
  - Install Pano Controller VM on ESX/ESXi
  - Install Pano Controller VM on ESX/ESXi
  - Change Pano Controller VM's Port Group
  - Reserve Resources for the Pano Controller VM in vCenter Server
  - Install Pano System with ESXi without vCenter Server
  - Protect Against Connection Failures To SAN Devices

Install and Configure Pano Controller on VMware vSphere

Before You Begin: Browse the workflow at Pano Controller Setup Step-by-Step.

To install and configure Pano Controller Virtual Machine on VMware vSphere:

Task	Go to...
Pick the virtualization platform to install, and your Pano Controller configuration.	Choose Your VMware Virtualization Infrastructure Deploy without vCenter Server and Active Directory Deployment Options for Pano Controller
Ensure that IPv4 is enabled.	Network Addressing Requirements
Install Pano Controller VM on vSphere: Install Pano Controller Virtual Appliance. Set passwords. Configure network settings.	Install Pano Controller VM on ESX/ESXi
If necessary, change the Pano Controller VM's port group. By default, Pano Controller VM belongs to the `VM Network` port group.	Change Pano Controller VM's Port Group
Allocate resources to the Pano Controller.	Reserve Resources for the Pano Controller VM in vCenter Server

What to do next: Choose Your VMware Virtualization Infrastructure

Choose Your VMware Virtualization Infrastructure

How you manage DVMs, in some cases, depends on whether you have vCenter Server. You can install Pano System without using vCenter Server; however, there is no folder structure without vCenter Server.

If you haven't already chosen and implemented your preferred virtualization infrastructure solution, consider the following:

- There are differences between ESX host *with* vCenter Server and ESX host *without* vCenter Server.

- There are limitations to managing virtual machines on ESX host *without* vCenter Server, and these limitations are the result of not having a folder structure:

What to do next: Install Pano Controller VM on ESX/ESXi.

Deploy without vCenter Server and Active Directory

You can run Pano Controller without Microsoft Active Directory. However, you'd be missing out on some key benefits. Also, Pano Controller does not require vCenter Server, but there are limitations if you don't use it.

The typical deployment without Active Directory and vCenter Server involves the following steps:

1. Install ESXi on a server, and create 3 desktop virtual machines. In each, install Windows, VMware tools, and Pano Direct Service.
2. Load the Pano Controller onto that ESXi server, and turn on broadcast discovery (Pano Controller’s **Setup** tab). The Pano Controller searches for Pano System Endpoints that are attached to the local network.
3. Plug 3 Pano System Endpoints into the network, and see them discovered by the Pano Controller (Pano Controller’s **Pano System Endpoints** tab).
4. On the **Setup** tab, leave the AD configuration blank, and point the virtualization configuration section directly at the ESXi server.
5. On the **DVM Collections** tab, create a single device based (Windows Login) collection, leaving the Automated Deployment check box disabled.
6. At this point, you should see the three Windows virtual machines listed under the DVMs tab.
7. For each, you can select the virtual machine, then click on the Assign button, and directly associate each virtual machine with a particular Pano System Endpoint.

   The monitor attached to that Pano System Endpoint should now display the Windows login screen for that VM, and you should be able to log on with a local account (such as local admin).

Install Pano Controller VM on ESX/ESXi

The Pano Controller VM can run on any ESX host or ESXi host with or without VMware vCenter Server installed (see Limitations of Pano Controller without vCenter Server and Choose Your VMware Virtualization Infrastructure). vCenter Server is a recommended component needed for installations using more than one ESX host or for automated provisioning.

To install on ESX host or ESXi host with vCenter Server:

You must import the Pano Controller virtual appliance before you can create the Pano Controller VM.

In the following procedure, the `PanoAppliance.ovf` file is the Pano Controller VM itself. The Pano Controller VM has the Pano Controller pre-installed.

The following procedure assumes that you have vSphere Client 2.5 or greater. If you have vSphere Client 2.0, you must import the OVF using VMware Converter as vCenter Server 2.0 does not support OVF format and then apply the workaround outlined in ID 3147.

1. Download the Pano Controller OVF zip file from Pano Logic's download (FTP) site. The password and other details are available from Pano Logic Technical Support.
   - Save the file to a desktop that is accessible from the vSphere Client.
   - Extract the file to its current location, then navigate to the *Pano Controller* folder.

   Warning: Don't use winRAR to extract the file. Customers have reported problems with this tool. Instead, use either Winzip or 7zip.

2. Add the Pano Controller virtual appliance to your ESX/ESXi inventory:

   a. Using the vSphere Client, connect to the ESX/ESXi host as Administrator.

   b. (With vCenter Server Only) Go to the Virtual Machine And Templates view.

   c. Choose **File** > **Virtual Appliance** > **Import**.

   d. Select the **Import from File** radio button, click **Browse** to navigate to the `.ovf` file, select the `PanoAppliance.ovf` file from the unzipped location, then click **Next.**

   The Import Virtual Appliance wizard displays the details of the Pano Controller virtual appliance.

   e. Click **Next** again.

   f. Type a name for the Pano Controller, then click **Next**.

   The default name is `Pano Controller`, but you might want to change the name if you intend to have more than one Pano Controller.

   g. (With vCenter Server Only) Select the ESX host on which you want to install the Pano Controller VM, then click **Next**.

   h. Choose a resource pool, then click **Next**.

   i. Choose a datastore, then click **Finish**. The import takes a few minutes. You know the import completed when:
   - The progress bar indicates `100%`
   - The **Recent Tasks** pane indicates that the **Create Virtual Machine** task `Completed`. Tasks clear after a few minutes.
   - The Pano Controller VM appears in your inventory.

   j. When the progress bar indicates 100%, click **Close**.

3. Power on and configure the Pano Controller VM.

   a. Click the **Console** tab.

   You might see several Linux boot messages, and then the installer prompts you to change your passwords.

   b. Type a new Superuser password, then press **Enter**. As you type the new password, you will not see any characters.

   c. Type a new Web Admin account password, then press **Enter**. As you type the new password, you will not see any characters.

   d. Configure Pano Controller VM network settings. The default is DHCP.

Note: While DHCP is suitable for a trial, a static IP address is recommended for production deployments.

   If you choose to assign an IP address, the installer validates IP format; if the format is correct:
   - The Pano Controller installer initiates a reboot of the Pano Controller VM.
   - The installer returns you to the login prompt.

4. Launch the Pano Controller console. Point your browser to the URL displayed in the Console tab.

5. Log on to the Pano Controller. Log on as `admin` using the password you set earlier.

If you'd like to install more than one Pano Controller virtual appliance to share load (refer to Configure Pano Controller Groups), repeat the following procedure for each Pano Controller. This is not a common configuration.

What to do next: Change Pano Controller VM's Port Group.

Related Topics

Replace Pano Controller's Self-Signed Certificate

Change Pano Controller 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 Controller VM is configured to use the `VM Network` port group. If this port group has been changed or removed, the Pano Controller VM cannot connect to the network. You must edit the Pano Controller 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 vCenter Server using the VMware Infrastructure Client.
2. Right-click on the Pano Controller 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**.

What to do next: Reserve Resources for the Pano Controller VM in vCenter Server. Use VMware resource pools and reservations to allocate the Pano Controller VM sufficient resources based on the Pano Controller's resource requirements.

Reserve Resources for the Pano Controller VM in vCenter Server

The Pano Controller virtual appliance is pre-configured to reserve the recommended resources, but if you changed these defaults, then use this procedure to revert back to the recommended resources.

The Pano Controller 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 Controller VM always has a minimum amount of resources available. For more information, go to Requirements for VMware vSphere.

To reserve resources for Pano Controller VM:

1. Determine the CPU and memory resources that your Pano Controller VM requires based on your deployment size.
2. Reserve CPU and memory resources:
    a. Log on to vCenter Server using the VMware Infrastructure Client.
    b. Power off the Pano Controller 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 Controller to use additional available resources as needed. The amount of resources consumed by the Pano Controller VM usually varies throughout the day based on your usage patterns. The Pano Controller VM consumes the most resources when Pano System Endpoints display the Pano user login screen. Once users have connected to their DVMs, the Pano Controller 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 Controller VM.

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

   a. From vCenter Server, right-click on the Pano Controller VM and select **Edit Settings**.

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

   c. Power on the Pano Controller VM.

   d. Log on to the Pano Controller console.

   e. Select option **5 - Drop to bash shell (Power Users)**.

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

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

You're ready to integrate it into your existing environment. Make sure your Pano Controller is set for Full Mode so that Pano VDB connection broker can be used in your DVM collection configurations. Then, go to Pano Controller Configuration.

Related Topics

Create Virtualization Hierarchy–VMware

Limitations of Pano Controller without Active Directory

What to do next:

- Pano Controller Configuration

Install Pano System with ESXi without vCenter Server

Pano Logic recognizes that users with small deployments might not have the budget for vCenter Server. You can install Pano System without using vCenter Server, but there are some limitations as outlined in Limitations of Pano Controller without vCenter Server.

One limitation of this deployment is that you can only create one collection since there is no folder structure without vCenter Server. Afterward, in Virtualization Configuration, connect to the ESXi host directly instead of using vCenter Server.

To deploy on ESXi without vCenter Server:

1. Determine that your version of ESXi is supported. Go to Supported Virtualization Platforms.
2. Enable ssh access to the ESXi host. Enable Secure Connections.
3. Upload and extract the Pano Controller Virtual Machine:
   a. Connect to the ESXi host through VI client.
   b. Click a datastore and browse it. You can upload the Pano Controller VM to the host by clicking the upload icon. The tar utility inside the ESXi host does not work. You need get another utility from http://download.panologic.com/Tools/.
4. Download the `panotar` file to your desktop, then upload it to the ESXi host the same way you did above.
5. Run the following command on that file to open all permissions:

```
# chmod 777 panotar
```

6. Ssh to the ESXi host:

```
# ssh ESXi_Server_Hostname
```

7. Type the following command:

```
# ./panotar -xzvf PanoManagementServer-xxx.tar.gz
```

8. Continue with the deployment as you would an ESX deployment. Go to How do I prevent the Pano Control Panel from launching after a silent install?.

Related Topics

Limitations of Pano Controller without vCenter Server

Protect Against Connection Failures To SAN Devices

When a cable is pulled, I/O freezes for approximately 30-60 seconds, until the SAN driver determines that the link is down, and failover occurs. During that time, the virtual machines (with their virtual disks installed on a SAN) may appear unresponsive, and any operations on the
`/vmfs` directory may appear to hang. After the failover occurs, I/O should resume normally.

Even though ESX Server's failover feature ensures high availability and prevents connection loss to SAN devices, all connections to SAN devices may be lost due to disastrous events, that include multiple breakages. If all connections to the storage device are not working, then the virtual machines will begin to encounter I/O errors on their virtual SCSI disks. Also, operations in the `/vmfs` directory may eventually fail after reporting an I/O error.

To set up disk timeout:

- For QLogic cards, consider adjusting the `PortDownRetryCount` value in the QLogic BIOS. This value determines how quickly a failover occurs when a link goes down. If the `PortDownRetryCount` value is, then a failover typically takes a little longer than multiplied by 2 seconds. A typical recommended value for is 15, so in this case, failover takes a little longer than 30 seconds. For more information on changing the `PortDownRetryCount` value, refer to your QLogic documentation.
- For the Windows 2000 and Windows Server 2003 guest operating systems, consider increasing the standard disk `TimeOutValue` so that Windows will not be extensively disrupted during failover. For a VMware environment, the Disk `TimeOutValue` must be set to 60 seconds.

1. Select **Start** > **Run**, type **regedit.exe**, and click **OK**.
2. In the left panel hierarchy view, double-click **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk**.
3. Do one of the following:
   - Select **TimeOutValue** if it exists and set the Data value to x03c (hexadecimal) or 60 (decimal). By making this change, Windows waits at least 60 seconds, for delayed disk operations to complete, before generating errors.
   - If **TimeOutValue** does not exist, select **New** from the Edit Menu and then DWORD value. In the Name field, type **TimeOutValue** and then set the Data value to x03c (hexadecimal) or 60 (decimal).
4. Click **OK** and exit the Registry Editor program.

14

Install Pano Controller on Hyper-V

This chapter includes the following topics:

Note: Third party information about SCVMM can be found at Microsoft SCVMM Resources.

Install Pano Controller on Hyper-V

Before You Begin: Browse the workflow at Pano Controller Setup Step-by-Step.

To install and configure Pano Controller Virtual Machine (Pano Controller VM) on Hyper-V perform the following sequence of tasks:

Task	Go to...
1. Pick your Pano Controller configuration.	Install the Pano Manager Connector for Microsoft SCVMM
2. Ensure that IPv4 is enabled.	Network Addressing Requirements
3. Install the Pano Manager Connector for Microsoft SCVMM.	Install the Pano Manager Connector for Microsoft SCVMM
4. Install the virtual appliance.	Install Pano Controller Virtual Appliance on SCVMM
5. Create the virtual machine.	Create the Pano Controller VM
6. Provision the virtual machine.	Provision Pano Controller VM
7. Set up the virtual machine.	Set Up the Pano Controller VM
8. Allocate resources to the Pano Controller.	Requirements for Windows Server 2008 R2 Hyper-V

What to do next: Install the Pano Manager Connector for Microsoft SCVMM.

Install the Pano Manager Connector for Microsoft SCVMM

The Pano Manager Connector for Microsoft SCVMM (SCVMM Connector) provides an interface for Pano Controller to communicate with the SCVMM server. It must be installed on the same machine as the SCVMM server, and before you install the Pano Controller. This component comes with your Pano Controller product package.

Before You Begin:

- Change the port for SCVMM. See ID 5241.
- Make sure the SCVMM Administrator Console is installed on the SCVMM server.

To install the Pano Manager Connector for Microsoft SCVMM:

1. Download the SCVMM Connector file (`PanoConnectorSCVMM.exe`) from Pano Logic's download (FTP) site. The password and other details are available from Pano Logic Technical Support.
2. On the same machine running SCVMM, **double-click** on the file to start installation.
3. Accept the EULA terms and click **Next**.
4. Enter a port value between 1024 and 65535. Default is 8316. Note that some ports may already be allocated. If so, you see a message that asks you to pick another port.
5. Click **install**.
6. When you see the **completed** message, click **done**.

What to do next: Install Pano Controller Virtual Appliance on SCVMM

Install Pano Controller Virtual Appliance on SCVMM

You must import Pano Controller virtual appliance before you can create Pano Controller VM.

Before You Begin:

- Make sure you have a functioning version of Microsoft System Center Virtual Machine Manager (SCVMM) running on your server.
- Make sure the SCVMM Connector is installed.
- Make sure the SCVMM Administrator Console is installed on the SCVMM server.

To import the Pano Controller virtual appliance into SCVMM:

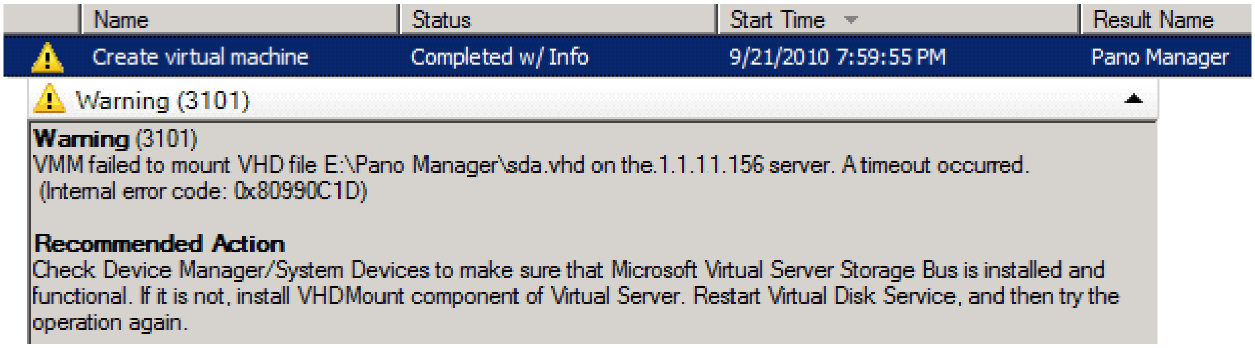
1. Download the Pano Controller VHD zip file from Pano Logic's download (FTP) site. The password and other details are available from Pano Logic Technical Support. Add the file to the SCVMM library.
2. **Unzip** the contents of the zip file. This file unzips to approximately 7.6 GB.
3. Launch the SCVMM Administrator Console and select the **Library** tab in the left panel.
4. **Right-click** on the SCVMM library folder and select **Explore**.
5. In the SCVMM Administrator Console, **right click** on the SCVMM library node and select **Refresh**. To see the Pano Controller VM, **click** on the **VMs and Templates node** in the Resources tree.

What to do next: Provision Pano Controller VM

Create the Pano Controller VM

After you import the Pano Controller virtual appliance, create the Pano Controller VM.

Note: Note: You might see Warning message (3101) at the end of the VM creation process. This is a known issue for Linux guests on Hyper-V. You can safely ignore this message. Your setup is complete and no remedial action is required.



	Name	Status	Start Time	Result Name
⚠	Create virtual machine	Completed w/ Info	9/21/2010 7:59:55 PM	Pano Manager

⚠ Warning (3101)

Warning (3101)
VMM failed to mount VHD file E:\Pano Manager\sda.vhd on the.1.1.11.156 server. A timeout occurred.
(Internal error code: 0x80990C1D)

Recommended Action
Check Device Manager/System Devices to make sure that Microsoft Virtual Server Storage Bus is installed and functional. If it is not, install VHDMount component of Virtual Server. Restart Virtual Disk Service, and then try the operation again.

To create the Pano Controller VM:

1. Select the **Virtual Machines** tab in the left panel.
2. From the **Actions** menu, select **Virtual Machine Manager** > **New virtual machine**. The **New Virtual Machine** wizard launches.
3. In the **Select Source** page of the wizard, select **Use an existing virtual machine, template, or virtual hard disk**.
4. Click **Browse**. The **Select Virtual Machine Source** dialog opens.
5. In the **Select Virtual Machine Source** dialog, select the Pano Controller VM, and click **OK**, then **Next**.

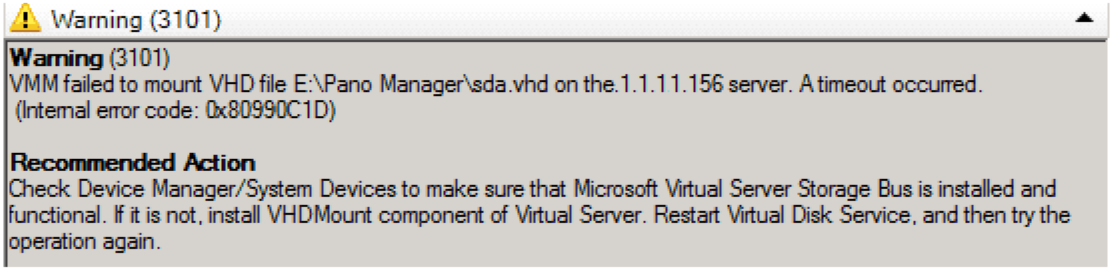
What to do next: Provision Pano Controller VM

Provision Pano Controller VM

1. In the **Virtual Machine Identity** page of the New Virtual Machine wizard:
   a. Enter a name for the Pano Controller virtual machine in the edit field.
   b. Enter the domain and username for this virtual machine's owner in the Owner edit field.
   c. Optionally, enter a description.
   d. Click **Next**.
2. In the **Configure Hardware** page of the New Virtual Machine wizard:
   a. Select the **Network 1** tab within Network Adapters under Hardware Profile.
   b. Under **Connection Requirements**, select your network in the drop-down list for Network location.
   c. No changes are needed for the remaining default settings. Click **Next**.
3. In the **Select Destination** page of the New Virtual Machine wizard, select the **Place the virtual machine on a host** option and click **Next**.
4. In the **Select Host** page of the New Virtual Machine wizard, select the host to use for this virtual machine and click **Next**.
5. In the **Select Path** page of the New Virtual Machine wizard, enter or browse for the storage location on the host for virtual machine files and click **Next**.
6. In the **Select Networks** page of the New Virtual Machine wizard, select the appropriate item from the Virtual Network drop-down menu and click Next.

7. In the **Additional Properties** page of the New Virtual Machine wizard, go to the **Operating system** section, select **Other Linux (32 bit)** from the drop-down menu and click **Next**.
8. In the Summary page, click **Create**.

You may notice this Warning message (3101) at the end of the creation process:



Warning (3101)

Warning (3101)
VMM failed to mount VHD file E:\Pano Manager\sda.vhd on the.1.1.11.156 server. A timeout occurred.
(Internal error code: 0x80990C1D)

Recommended Action
Check Device Manager/System Devices to make sure that Microsoft Virtual Server Storage Bus is installed and functional. If it is not, install VHDMount component of Virtual Server. Restart Virtual Disk Service, and then try the operation again.

This is a known issue for Linux guests on Hyper-V. You can safely ignore this message: your setup is complete and no remedial action is required.

What to do next: Set Up the Pano Controller VM

Set Up the Pano Controller VM

You need to power on your new Pano Controller virtual machine and continue setting it up. Select your new machine and click **Start**.

1. Power on the Pano Controller VM.
2. Right-click the Pano Controller VM to bring up the task selections and select.

   After a few seconds, the setup process prompts you to change your passwords.
3. Type a new Superuser password, then press **Enter**. The screen does not display your entries.
4. Type a new Web Admin account password, then press **Enter**. The screen does not display your entries.
5. Configure Pano Controller VM network settings. The default is DHCP.

Note: While DHCP is suitable for a trial, a static IP address is recommended for production deployments.

If you choose to assign an IP address, the setup process validates IP format. Providing the format is correct:

- The network interface is reset.
- You are returned to the login prompt.

6. Launch the Pano Controller console. Point your browser to the URL displayed in the Console tab.
7. Log on to the Pano Controller Administrator interface. Log on as `admin` using the password you set earlier.

What to do next: Pano Controller Configuration.

Login Access to Pano Controller Connector for SCVMM

To install the Pano Controller SCVMM Connector, the user has to be using the Administrator account. If the Administrator account was disabled for security purposes, the user has to enable it, run the installer, then disable the Administrator account when the installation is complete.

To run the installation from the command line as Administrator, the user has to provide the Administrator password before invoking the `.msi` file from the command prompt.

15
Install Pano Controller on XenServer

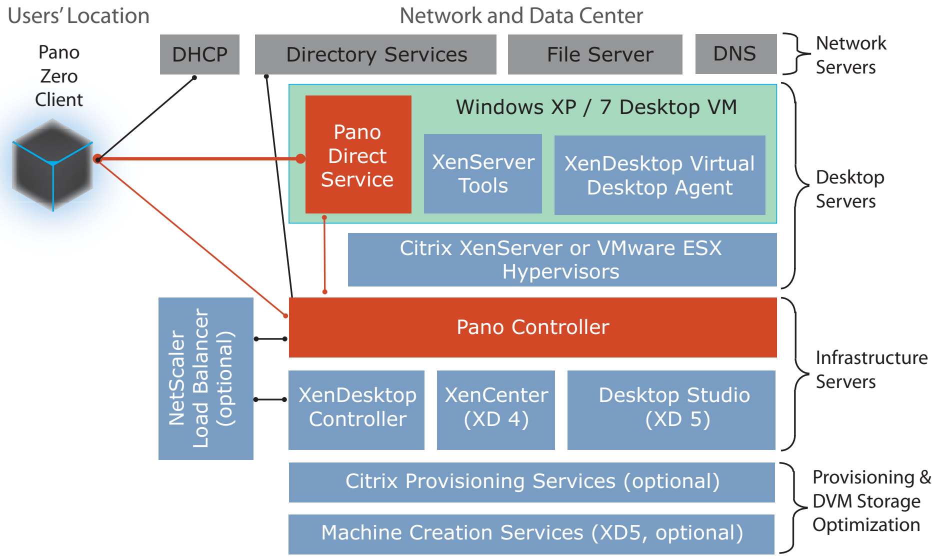
This chapter includes the following topics:

- Install Pano Controller VM on XenServer
- XenDesktop Architecture & Components
- About the Logon Process
- Configure NetScaler to Monitor XenDesktop Controllers

Before You Begin: Browse the workflow at Pano Controller Setup Step-by-Step, and review the following material on Xen and Pano Controller.

XenDesktop Architecture & Components

This shows the system architecture when using Pano System and XenDesktop together.



Users' Location
Network and Data Center
Pano Zero Client
DHCP
Directory Services
File Server
DNS
Network Servers
Windows XP / 7 Desktop VM
Pano Direct Service
XenServer Tools
XenDesktop Virtual Desktop Agent
Desktop Servers
Citrix XenServer or VMware ESX Hypervisors
NetScaler Load Balancer (optional)
Pano Controller
XenDesktop Controller
XenCenter (XD 4)
Desktop Studio (XD 5)
Infrastructure Servers
Citrix Provisioning Services (optional)
Machine Creation Services (XD5, optional)
Provisioning & DVM Storage Optimization

A typical XenDesktop deployment comprises the following components:

- **Hypervisor**: This is the software that allows multiple virtual machines to run concurrently on a host server. For supported hypervisors, go to System Requirements.
- **Citrix Desktop Delivery Controller (DDC) or XenDesktop Controller**: The DDC (under XenDesktop 4) or XenDesktop Controller (under XenDesktop 5) (referred to collectively in this documentation as XenDesktop Controller) functions as the connection broker for the entire system. When using Pano System with XenDesktop, administrators use the same GUI and processes to define desktop pools and user assignments as they normally do when using XenDesktop without Pano System. Each Controller instance connects to Pano Controller via a single API, potentially creating a limit on scalability, even if multiple Pano Controller instances are used. See Managing Scalability for information.
- **DVM**: A DVM is a desktop virtual machine, of which you will typically have many in your environment. Each DVM will need to have both the Pano Direct Service (PDS) software and platform-specific add-ins or tool software installed directly in the Windows® operating system. XenDesktop allows you to create and manage pools of DVMs. Each DVM must

have the Citrix Virtual Desktop Agent and XenServer Tools installed. These tools are required in order for the XenDesktop Controller to manage the state of the DVM. Without these tools installed, the XenDesktop Controller will consider the DVM to be unavailable. If you are using the DVMs on a VMware vSphere ESX hypervisor, you'll need to install VMware Tools into the DVM rather than XenServer Tools.

- **Desktop Studio, XenCenter, Citrix Provisioning Services (PVS)**: When using the Pano System with XenDesktop, Desktop Studio (in XenDesktop 5) or XenCenter (in XenDesktop 4) is used to perform all DVM management and provisioning activities. Pano Controller will not cause any DVMs to be created, nor will it attempt to keep a certain number of DVMs powered on. These provisioning and power-management functions are all performed by these components along with XenDesktop Controller. In addition, Citrix Provisioning Services or Machine Creation Services (in XenDesktop 5 only) can be used to provide automatic provisioning services.Citrix Provisioning Services is optional, but is commonly used to efficiently provision DVMs in a XenDesktop deployment in a XenDesktop 4 deployment. PVS enables you to stream a single desktop image to create multiple virtual desktops on one or more servers in a data center. This can greatly reduce the amount of storage required compared to other methods of creating virtual desktop or DVM images. PVS is only recommended for larger deployments. PVS can also be used for many other image provisioning tasks than just creating hosted virtual desktops like Pano DVMs. If PVS is used, the desktop image managed by PVS must include the following components: XenServer Tools, Citrix Virtual Desktop Agent, and Pano Direct Service. You must install these components in the correct order.
- **Machine Creation Services (MCS)**: MCS is an alternate DVM provisioning service introduced with XenDesktop 5. MCS is required for both Pooled and Dedicated desktop virtual machine types in XenDesktop 5, while PVS is required for Streamed DVMs. Because MCS doesn't offer the same level of RAM-based read caching as PVS does, according to Citrix, it can end up using as much as 50% more IOPS than PVS – however this might not be an issue except for very large deployments. The following table lists the different desktop virtual machine types supported by XenDesktop 5, which provisioning service (PVS or MCS) is required, and how Pano Direct Service (PDS) is installed into the DVMs. The only XenDesktop 5 machine type not supported by the Pano System is Physical, which is used to manage user desktops hosted on dedicated blade PCs rather than in shared VDI servers.

DVM Type	Required Provisioning Service	Supported with Pano?
Pooled	Machine Creation Services	Yes
Dedicated	Machine Creation Services	Yes
Existing	None	Yes
Physical	None	No
Streamed	Citrix Provisioning Services	Yes

- **Load Balancer**: To eliminate single points of failure and ensure scalability, most customers will deploy multiple instances of the XenDesktop Controller. When multiple instances of the XenDesktop Controller are present, you will want to place a load balancer, such as Citrix NetScalerVPX™ or MPX™, in front of multiple instances of the XenDesktop Controller XML server to provide a single, load-balanced interface to which Pano Controller can connect. Go to About Load Balancing XenDesktop Controllers for information. If you do not deploy multiple instances of XenDesktop Controller, you do not need a load balancer.
- **Profile Management tool**: XenDesktop also includes a Profile Management tool that can manage user personalization settings, which can be optionally controlled by AD Group Policy Objects.

About the Logon Process

After deploying the Pano System, the following occurs "behind the scenes" when an end user logs on to a DVM using a Pano System Endpoint:

1. **DHCP** – the Pano Zero Client connects to a DHCP server, receiving an IP address along with the address for the Pano Controller VM (provided the vendor class option has been configured in the DHCP server).
2. **Login Screen** – depending on the selected Pano System Endpoint discovery method, the Pano System Endpoint contacts Pano Controller, which causes the Pano Zero Client to display a login screen. To log in, the end user enters their user name and password into the fields provided on-screen and presses the Login button (or the Enter key.)
3. **Credential Validation** – the user credentials are transmitted by the Pano Zero Client to Pano Controller. Pano Controller submits these credentials to the directory service and receives validation (or rejection) from the directory service.
4. **Query XenDesktop Connection Broker** – upon successful authentication, Pano Controller queries the XenDesktop Controller by passing the user credentials to it.
5. **Credential Validation by XenDesktop** – the XenDesktop Controller also validates the user credentials with the directory service.
6. **DVM Lookup** – all associations between users and DVMs are managed by XenDesktop rather than Pano Controller. Because of this, the XenDesktop Controller checks its database for the list of DVMs to which the user is entitled.
7. **Determine specific DVM** – the XenDesktop Controller returns a list of Desktop Groups to Pano Controller. If the user is entitled to multiple Desktop Groups, Pano Controller will automatically connect the user to the desktop most recently accessed. (If instead of clicking the Login button, the user clicks the Options button in (Step 2), the user will be prompted to select the desired specific desktop from a list of available desktops.)
8. **Transfer of Control** – Pano Controller next checks on the status of the Pano Direct Service running in the target DVM and ensures that it is ready to connect. Once ready, Pano Controller facilitates the connection between the Pano Zero Client and the Pano Direct Service on the appropriate DVM and steps aside – this is called a Transfer of Control.
9. **Session Established** – the user is now connected to their desktop and all session traffic flows directly from the Pano Direct Service to the Pano Zero Client. Pano Controller and the XenDesktop Controller are no longer directly involved in the Pano session.

To install and configure Pano Controller Virtual Machine (Pano Controller VM) on XenServer, follow these steps:

Task	Go to...
Pick your Pano Controller configuration.	Install Pano Controller VM on XenServer
Ensure that IPv4 is enabled.	Network Addressing Requirements
Install the Pano Controller VM on XenServer: Install the Pano Controller virtual appliance. Set passwords. Configure network settings.	Install Pano Controller VM on XenServer
Allocate resources to the Pano Controller.	Requirements for XenServer

What to do next: Install Pano Controller VM on XenServer

Install Pano Controller VM on XenServer

The Pano Controller is delivered as a virtual appliance. This means that the Pano Controller runs within a virtual machine hosted by your virtualization platform.

You must import the Pano Controller virtual appliance before you can create the Pano Controller VM.

Before You Begin: Do the following:

- Make sure you have a functioning version of XenServer running on your server before you install the Pano Controller.
- Make sure you have the Citrix Desktop Delivery Controller (DDC) (under XenDesktop 4) or XenDesktop Controller (under XenDesktop 5) installed on the XenServer.

1. Download the Pano Controller VHD zip file from Pano Logic's download (FTP) site. The password and other details are available from Pano Logic Technical Support.
   - Save the file to a desktop that is accessible from XenCenter.
   - Extract the file to its current location, then navigate to the `PanoController` folder.

   Warning: Don't use winRAR to extract the file. Customers have reported problems with this tool. Instead, use either Winzip or 7zip.

2. Add the Pano Controller virtual appliance to your XenCenter inventory:

   a. Log on to XenCenter, then do one of the following, depending on the version of your XenClient:
      - Select **File** > **Appliance Import...**.
      - Select **Tools** > **Virtual Appliance Tools** > **Import Appliance...**.

   b. In the Select an Appliance for Import page of the wizard, click **Browse** and select the `PanoAppliance.ovf` file from the unzipped location, and then click **Next**.

   c. In the EULA page, click **Next**.

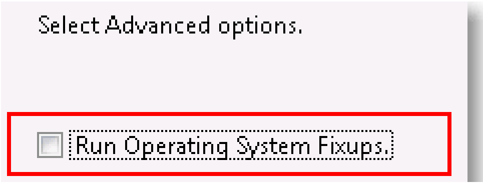
   d. In the Select target XenServers or Pools page, select the target server or pool for hosting the Pano Controller VM, and then click **Next**.

   e. In the Select target SRs page, select the storage for each of the two Pano Controller disks, and then click **Next**.

   f. In the Select Network to connect VM page, select the target virtual network, and then click **Next**.

   g. In the Select your import security settings page, click **Next**.

   h. (Important!) In the Select advanced options for the Appliance import page, clear the **Run Operating System Fixups** checkbox, and then click **Next**. If you don't to this, you will corrupt the Pano Controller virtual appliance, and will need to download and install a new one.



Select Advanced options.

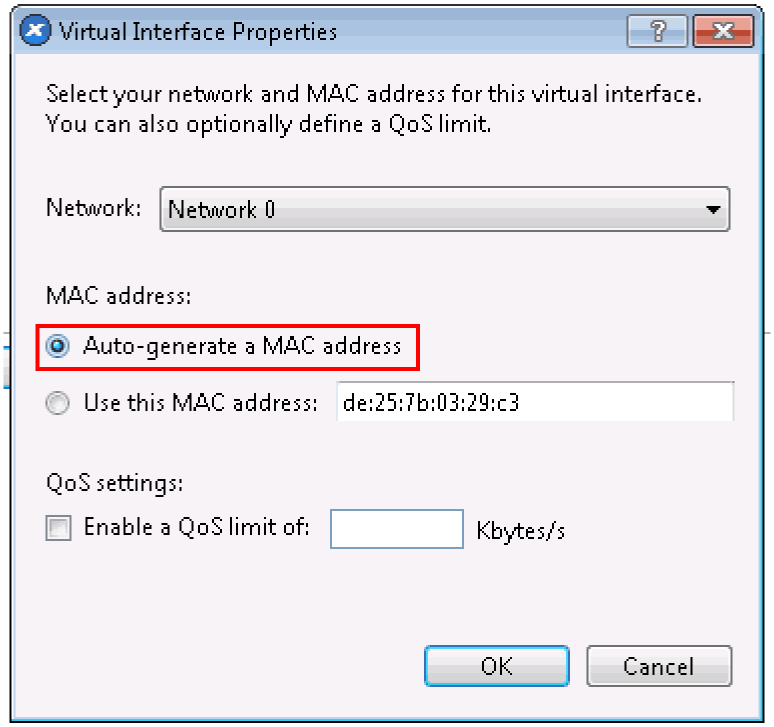
□ Run Operating System Fixups.

   i. In the Ready to import Appliance page, verify the settings, then click **Finish**.
      - The Import Progress page appears. The import process takes about 25 minutes.
      - The Import Progress page indicates the status of the import after it completes.

j. Verify that the message displayed in the Import Progress page indicates that the process was successful, then click **Done**.

3. From the Navigation pane, select the newly created Pano Controller virtual appliance (it will be named `Pano Controller`), go to the **Network** tab > **Properties** dialog and select the **Auto-generate a MAC address** option, and then click **OK**.

   Warning: You must perform this operation before you power on and configure the Pano Controller VM. If you don't, the Pano Controller might have the same MAC address as another virtual machine and cause network addressing problems. In this case, you need to delete the virtual machine and start over: changing the property afterward will not resolve the MAC address problem.



Virtual Interface Properties

Select your network and MAC address for this virtual interface.
You can also optionally define a QoS limit.

Network: Network 0

MAC address:

● Auto-generate a MAC address

○ Use this MAC address: de:25:7b:03:29:c3

QoS settings:

□ Enable a QoS limit of: Kbytes/s

4. (Optional) In XenCenter, change the Pano Controller's name if you intend to have more than one Pano Controller (refer to Monitor Load Balancing Across a Group).The default name is `Pano Controller`.

5. Power on and configure the Pano Controller VM.

   a. Click the **Console** tab.

      You might see several Linux boot messages, and then the installer prompts you to change your passwords.

   b. Type a new Superuser password, then press **Enter**. As you type the new password, you will not see any characters.

   c. Type a new Web Admin account password, then press **Enter**. As you type the new password, you will not see any characters.

   d. Configure Pano Controller VM network settings. The default is DHCP.

Note: While DHCP is suitable for a trial, a static IP address is recommended for production deployments.

If you choose to assign an IP address, the installer validates the IP address format; if the format is correct:

- The Pano Controller installer initiates a reboot of the Pano Controller VM.
- The installer returns you to the login prompt.

6. Launch the Pano Controller console. Point your browser to the URL displayed in the Console tab.
7. Log on to the Pano Controller. Log on as `admin` using the password you set earlier.

If you'd like to install more than one Pano Controller virtual appliance to share load (refer to Managing Scalability), repeat the procedure for each Pano Controller. This is not a common configuration.

Related Topics

Replace Pano Controller's Self-Signed Certificate

What to do next: Pano Controller Configuration

Configure NetScaler to Monitor XenDesktop Controllers

As outlined in Install Pano Controller VM on XenServer, the Pano System supports Citrix NetScaler. However, Citrix NetScaler must be configured to monitor the health of your XenDesktop Controller(s) so that when the broker service is down on the XenDesktop Controller(s), Citrix NetScaler will appropriately flag the server as unavailable. The Pano Controller also needs to know the correct state for *each* XenDesktop Controller, and the Pano System gets this information from Citrix NetScaler.

If your Citrix NetScaler is not properly configured to monitor your XenDesktop Controller(s), your end users might not be able to log on to their DVMs; instead, they will receive the following error message:

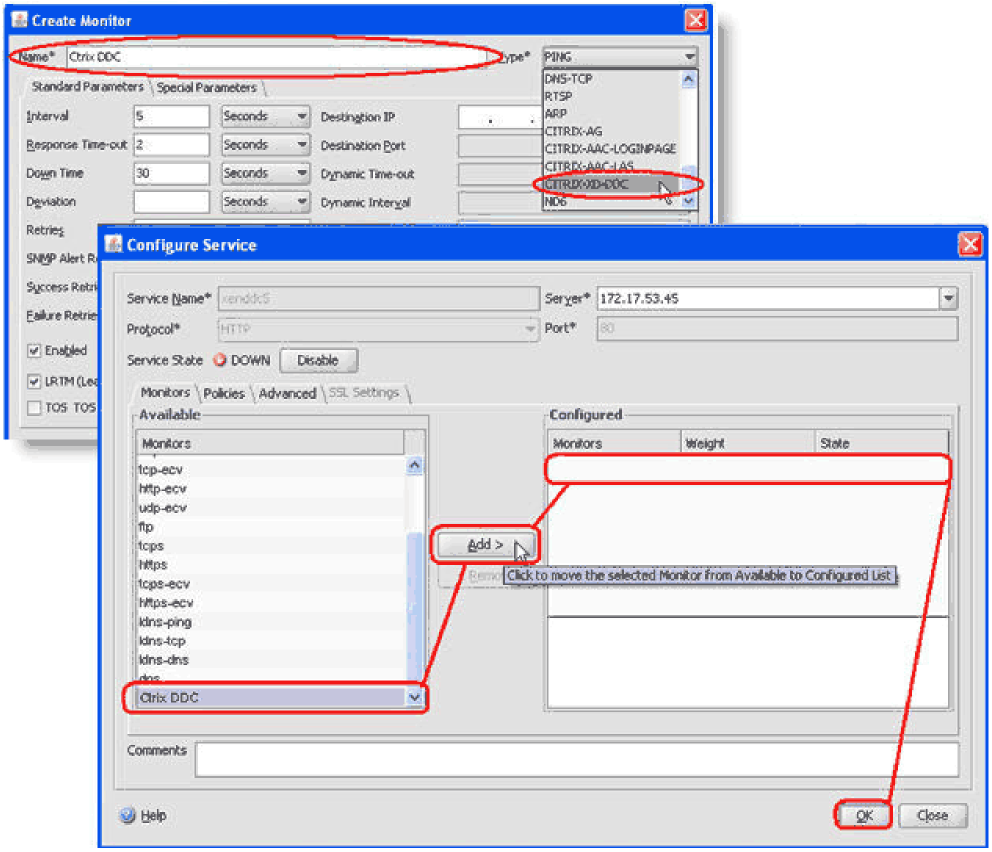
No desktops are available. Please contact your system administrator; No DVMs are configured for you; No DVMs are available for you

In this case, if you have two XenDesktop Controller, and one is up and one is down, the Pano Controller might be incorrectly reporting that the XenDesktop Controller is available.

To properly configure Citrix NetScaler, you must add both the monitor *and* the service for *each* XenDesktop Controller. Perform this procedure for each XenDesktop Controller.

1. Launch the NetScaler VPX UI.
2. Add the Monitor:
   a. Go to **NetScaler VPX *IPAddress*** > **Load Balancing** > **Monitors**.
   b. In the Details pane, click **Add**.
   c. In the Create Monitor dialog, specify the following, then click **Create**, then **Close**.
      - **Name** - Name of the XenDesktop Controller. For example, `Citrix DDC1` or `Citrix DDC2`.
      - **Type** - Choose **CITRIX-XD-DDC**.
3. Configure the Service:
   a. Go to **NetScaler VPX** > **Load Balancing** > **Services**.
   b. Select the **xenddc5** service.
   c. In the Details pane, click **Open**.

d. In the Configure Service dialog and from the Available scroll list, select the monitor that you created in Step 2, click **Add** to add it to the Configured scroll list, then click **OK**.



Create Monitor

Name* Citrix DDC

Type* PING

Interval 5 Seconds

Response Time-out 2 Seconds

Down Time 30 Seconds

Deviation Seconds

Configure Service

Service Name* xenddc5

Server* 172.17.53.45

Protocol* HTTP

Port* 80

Service State DOWN

Click to move the selected Monitor from Available to Configured List

16
Pano Controller Configuration

This chapter includes the following topics:

Configure Pano Controller Appliance Role

Configure the Pano Controller Appliance Role:

1. Identify the Pano Controller role.

By default, the Pano Controller is set to Full Mode. Full Mode is the simplest option to configure and provides the full functionality of the Pano System. This is generally the best option for starting out. If you are planning on using a 3rd party connection broker, Full Mode provides the option to use either Citrix XenDesktop or VMware View as the connection broker for user-based assignments. You may also use the Pano Controller's internal connection broker service to support device-based assignments.

ZCC role enables you to use either Citrix XenDesktop or VMware View as the exclusive connection broker for your system. With this deployment option you will be limited to user-based assignments only and will not be able to deploy device-based assignments. Choose this option if you want to use a 3rd party connection broker and you do not want to use device-based assignments.

All Pano Controller group members of the same group must be configured for the same role.

2. To change from Full Mode to ZCC role, use the Pano Controller console **Setup** -> **Appliance Role** to configure the Pano Controller role.

What to do next: Determine Access Accounts for Integrating Pano Controller

Determine Access Accounts for Integrating Pano Controller

Choose accounts for Pano Controller to use:

1. Identify an account for the Pano Controller 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 System.
2. Identify an account for the Pano Controller to use to integrate with the server that manages the virtualization platform underlying your Pano System.

   This account needs to have Administrator permissions in your virtual machine server.

What to do next: Configure the Data Center Firewall

Configure the Data Center Firewall

The Pano Direct Service communicates with the Pano Controller and Pano System Endpoints over certain network ports. If you have a firewall between your users' Pano System Endpoints and your data center, you must open up these ports for both inbound and outbound traffic. DVMs initiate connections to these clients, so if these ports are closed, Pano Controller cannot discovery your Pano System Endpoints.

What to do next: Connect Pano Controller To Directory Services

Connect Pano Controller To Directory Services

You can run Pano Controller without Active Directory. However, you'd be missing out on some key benefits. The Pano Controller relies on the directory service for user authentication. For a list of supported directory services, go to Supported Directory Services.

To enable user authentication, you need to set up the Pano Controller to read your directory service. Using the standard DNS SRV records (RFC2782), the Pano Controller can automatically determine the best directory servers to contact.

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

To configure Pano Controller without directory services:

1. Log on to the Pano Controller.
2. Ensure that the Directory Configuration section of the **Setup** tab is blank.

Note: XenDesktop Controller users **must** connect the Pano Controller to your directory service before you delegate connection brokering to XenDesktop Controller.

To connect Pano Controller with directory services:

This procedure takes into account the most common configurations. The Pano Controller has a lot of built-in intelligence when it comes to directory services; however, if this procedure doesn’t work for you, go to Alternate Connections for Pano Controller To Directory Services.

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Directory Configuration** area, click the expansion triangle to open the section.
4. In the **URL** field, type your network's domain name (for example, acme.com) or LDAP server URL.

   Only one domain name can be specified.

   One or more space-separated LDAP server URLs can be specified.

   The following characters do not need to be escaped (preceded by a backslash) in the LDAP server URL: ‘%’, ‘a-z’, ‘A-Z’, ‘0-9’, ‘~’, ‘!’, ‘@’, ‘$’, ‘^’, ‘&’, ‘*’, ‘(‘, ‘)’, ‘|’, ‘:’, ‘?’, ‘”, ‘-’, ‘.’, ‘/’.

   If using a distinguished name (DN), the ‘#’ character does not need to be escaped if it occurs within the name. However, it does need to be escaped (\#) if it occurs at the beginning of the name.

   The following characters need to be escaped: ‘+’, ‘”’, ‘<‘, ‘>’, ‘=’, ‘\’, ‘;’, ‘,’.
5. Type the User Principal Name (UPN) and password of the account that you are using to connect to the directory service.
   - The account needs to have read access to all portions of the directory used to authenticate users of the DVMs.
   - When using AD you must use the full User Principal Name (UPN). The UPN is an internet-style login name for the user (for example, readonly@acme.com).
6. Click **Configure**. Pano Controller automatically locates the directory service for your domain.
7. 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 need to use the fully-qualified name of your directory server or you might have a less common environment.
- If that doesn’t work, go to Troubleshoot Authentication and Directory Service Problems.

What to do next: Connecting Pano Controller

Alternate Connections for Pano Controller To Directory Services

The Pano Controller relies on the directory service for user authentication. You need to set up the Pano Controller to read your directory service. (For a list of supported directory services, go to Supported Directory Services.)

If your directory service doesn't work when you configured it as outlined in Connect Pano Controller To Directory Services, then perform the following procedure, which takes into account less common environments such as Active Directory Redundancy.

When connecting to your directory service, you have the ability to specify a specific server or, if you are using Active Directory, you can let DNS determine the domain controller. If your DNS server is configured correctly and the service still doesn't work, try using the fully-qualified name for the server.

You can configure a backup server by providing a space-separated list of the fully-qualified names of the servers. If the first server is not reachable, the Pano Controller attempts to connect to the next server in the list using the same security credentials.

To set up directory service integration for Novell eDirectory/OpenLDAP:

When using Novell eDirectory or OpenLDAP, keep in mind the following:

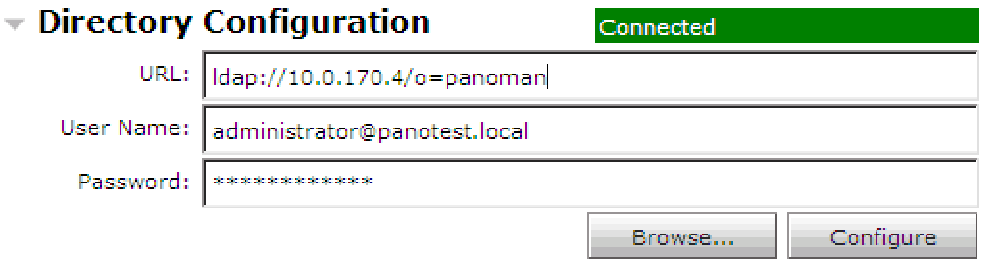
- The Pano Controller tests security group membership using the user's `groupMembership` attribute. If this attribute is not present, the Pano Controller tests group membership using the group's `member` attribute.
- The person's `uid` attribute is used for authentication.

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Directory Configuration** area, type the URL for the LDAP server, type a URL of the following form:

```
ldaps://server_name_or_IP_address
```

Example:

```
ldaps://dirserver1.panologic.com
```



Directory Configuration

Connected

URL: ldap://10.0.170.4/o=panoman

User Name: administrator@panotest.local

Password: **************

4. In the **Directory Configuration** area, type the user principal name (UPN) of the account to be used to connect to the directory server. The user name under Directory Configuration must be in one of the following forms:

```
domain\username
```

or

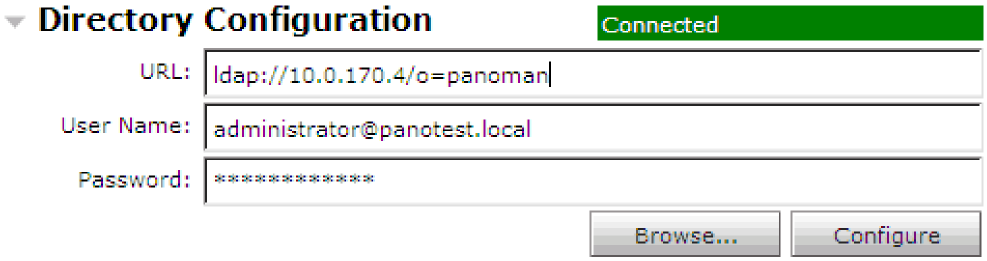
```
username@domain.com
```

The UPN is an internet-style login name for the user. The account needs to have read access to all portions of the directory used to authenticate users of the DVMs.

For user authentication service you can typically use any username that has the privileges or permissions to browse your AD/LDAP tree in order to authenticate users. Many Pano Logic customers simply use a regular account.

Example:

```
panomansvr@yourdomain.com
```



Directory Configuration

Connected

URL: ldap://10.0.170.4/o=panoman

User Name: administrator@panotest.local

Password: *************

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

   If you receive connection errors, details can be found under the **Log** tab or by hovering over the connection status field on the **Setup** tab.

Troubleshooting: Go to Troubleshoot Authentication and Directory Service Problems.

To set up directory service integration for Active Directory:

Before You Begin: Do the following:

- Configure Pano Controller Appliance Role
- Determine Access Accounts for Integrating Pano Controller

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Directory Configuration** area, type the URL for the directory service by doing one of the following:
   - (Option #1) **To have DNS determine the domain controller, type a URL of the following form.**

     ```
     ldaps:///distinguished_name_of_the_domain
     ```

     Example #1:

     ```
     ldaps:///dc=yourdomain,dc=com
     ```

     Example #2:

     ```
     ldaps://dc1.yourdomain.com/dc=yourdomain,dc=com
     ```

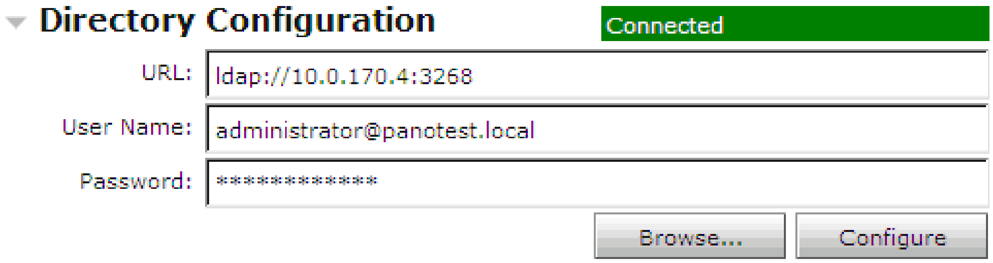
     If you specify the domain name, the Pano Controller queries every domain controller in the domain until one answers.

- (Option #2) **To specify the specific domain controller, type a URL of the following form**:

```
ldaps://server_name_or_IP_address
```

Example:

```
ldaps://dirserver1.panologic.com
```



Directory Configuration

Connected

URL: ldap://10.0.170.4:3268

User Name: administrator@panotest.local

Password: *************

- (Option #3) **For best performance with Active Directory and if you have a multidomain environment, specify a domain controller that is a [Global Catalog Server](#)**. By default the Global Catalog runs on port 3268 in unencrypted mode and on 3269 in encrypted 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.

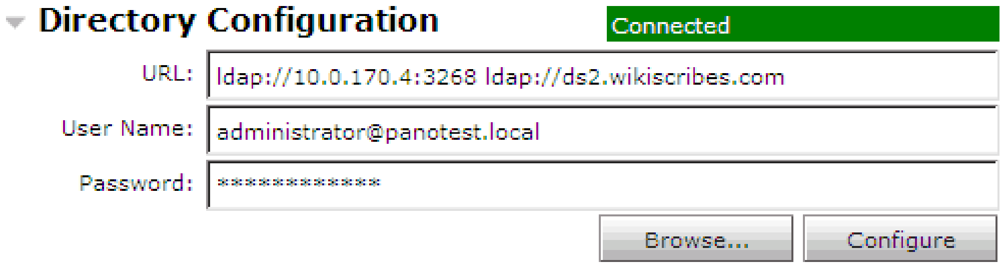
```
ldaps://dirserver1.yourdomain.com:3269
ldap://dirserver1.youdomain.com:3268
```

  The Pano Controller queries the directory server for the default naming context that will be used for queries. If you need to use a different naming context, you can specify it after the host name in the URL.

- (Option #4) For [Active Directory Redundancy](#), type a space-separated list of URLs. The Pano Controller tries the URLs in the order that they appear in the list. The first successful connection will be used.

  Example:

```
ldap://ds1.acme.com ldap://ds2.wikiscribes.com
```



Directory Configuration

Connected

URL: ldap://10.0.170.4:3268 ldap://ds2.wikiscribes.com

User Name: administrator@panotest.local

Password: **************

4. In the **Directory Configuration** area, type the [user principal name](#) (UPN) of the account to be used to connect to the directory server. If you listed more than one domain controller the Pano Controller assumes that these servers are full backups of

each other and so they must use the same credentials. The username under Directory Configuration must be in one of the following forms:

```
domain\username
```

or

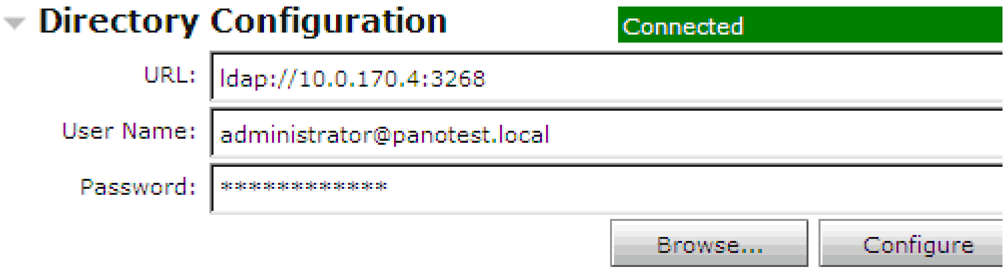
```
username@domain.com
```

The UPN is an internet-style login name for the user. The account needs to have read access to all portions of the directory used to authenticate users of the DVMs.

For user authentication service you can typically use any username that has the privileges or permissions to browse your AD/LDAP tree in order to authenticate users. Many Pano Logic customers simply use a regular account.

Example:

```
panomansvr@yourdomain.com
```



Directory Configuration

Connected

URL: ldap://10.0.170.4:3268

User Name: administrator@panotest.local

Password: ************

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

   If you receive connection errors, details can be found under the **Log** tab or by hovering over the connection status field on the **Setup** tab.

Troubleshooting: Go to Troubleshoot Authentication and Directory Service Problems.

17

Connecting Pano Controller

This chapter includes the following topics:

- Connect Pano Controller To vCenter Server
- Connect Pano Controller to XenDesktop Controller
- Connect Pano Controller to SCVMM

Connect Pano Controller To vCenter Server

Note: If you plan to use VMware View exclusively, you do not need to perform this procedure. For more information, go to Connecting Pano Controller.

Pano Controller does not require vCenter Server, but there are limitations to not using it, including not being able to use Pano Controller's automated deployment.

To configure Pano Controller without vCenter Server:

1. Log on to the Pano Controller.
2. In the Virtualization Configuration section of the **Setup** tab, specify the ESXi server.

To configure Pano Controller with vCenter Server:

Before You Begin:

1. Ensure that vCenter Server web service is installed and running.

   Using the vSphere Client, log on to vCenter Server.
   - If you can't log on, the web service is not functioning.
   - If the service is not running, the Pano Controller can't communicate with vCenter Server.
2. Log on to the Pano Controller.
3. Click the **Setup** tab.
4. In the **Virtualization Configuration** section, type the URL for the vCenter Server 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.

   Note: The URL should end in `/sdk`, which specifies the VMware API.

   For vCenter Server 2.x:

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

   Example:

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

5. Type the user name (for example, `administrator@acme.com`) and password of the account in VMware vCenter Server.

The Pano Controller uses this account to communicate with vCenter Server. Pano Logic recommends that this account be unique–and only used for integration between the Pano Controller and vCenter Server. The username must be a valid user who has permissions on the Folder hierarchy in vCenter Server as well as customization scripts and other objects. You can simplify your evaluation by specifying an account that has administrator privileges.

6. Click **Configure**.
7. When connected, in the **Virtualization Configuration** section, click **Browse**, then browse the virtualization hierarchy to confirm that the account has the proper access privileges.

Troubleshooting: Troubleshoot Communication Problems with vCenter Server

Next: Manage Pano Controller

Connect Pano Controller to XenDesktop Controller

With Pano Controller for XenDesktop, the XenDesktop Controller, not the Pano Controller, performs connection brokering.

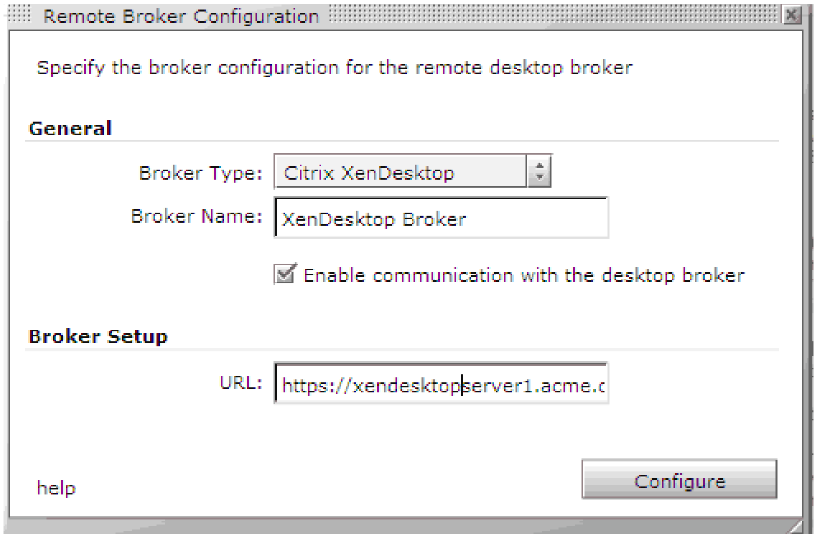
When a user attempts to log on from a Pano System Endpoint, the Pano Controller validates the user's credentials against the directory service and queries the XenDesktop Controller for the list of DVMs to which the user is entitled. Therefore, the Pano Controller must be connected to both the directory service, which you did earlier, and the XenDesktop Controller.

To connect the Pano Controller to the XenDesktop Controller:

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Broker Configuration** area, add the XenDesktop broker.
   a. In the Connection Broker drop-down list, select **Citrix XenDesktop**.
   b. In the **URL** text box, specify the URL or IP address for the XenDesktop Controller(s). For example, https://ddc.acme.com or https://192.168.1.22.

      The connection can be https or http, depending on how XenDesktop was set up.
      - If you have one XenDesktop Controller configured behind a Citrix NetScaler, specify the URL for that XenDesktop Controller.
      - If you have multiple XenDesktop Controllers configured behind a network load balancer, specify the physical IP address or virtual address of the Citrix NetScaler (or other type of load balancer).

      Your Citrix NetScaler must be configured to monitor the health of your XenDesktop Controller(s). For more information, go to Configure NetScaler to Monitor XenDesktop Controllers.



Remote Broker Configuration

Specify the broker configuration for the remote desktop broker

General

Broker Type: Citrix XenDesktop

Broker Name: XenDesktop Broker

☑ Enable communication with the desktop broker

Broker Setup

URL: https://xendesktopserver1.acme.c

4. Click **Configure**.

Next: Manage Pano Controller

Connect Pano Controller to SCVMM

To connect the Pano Controller to SCVMM:

1. Log on to the Pano Controller.
2. Click the **Setup** tab.
3. In the **Virtualization Configuration** section, type the URL for the SCVMM server, appended with the port number of the SCVMM Connector. If no port number is specified, the default, `8316`, is used.

   ```
   https://10.0.32.30:4949
   ```

   The URL can be a FQDN of the computer, IP address, or Netbios name.
4. Type the user name (for example, `administrator@acme.com`) and password of the account with administrator privileges in SCVMM server.
5. Click **Configure**.
6. When connected, in the **Virtualization Configuration** section, click **Browse**, then browse the virtualization hierarchy to confirm that the account has the proper access privileges.

Next: Manage Pano Controller

18
Manage Pano Controller

This chapter includes the following topics:

Change Pano Controller VM Network Settings

You can configure the Pano Controller VM to get its network settings from a DHCP Server or you can assign the Pano Controller VM a static IP Address. Setting a static IP address is generally preferred, and is required if you use DHCP-assisted discovery for Pano System Endpoint as outlined in Set Up Pano Client Discovery Using DHCP

It’s much easier to change the network settings from the Management User Interface (MUI), but you can also do so from the Pano Controller console.

To configure the Pano Controller VM’s network settings from the Pano Controller:

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Platform Settings** section > **Network:**, specify the network settings for the Pano Controller VM, Set to DHCP or provide static IP.
4. Click **Okay**.

To configure the Pano Controller VM’s network settings from the console:

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

Next: Replace Pano Controller’s Self-Signed Certificate

Replace Pano Controller's Self-Signed Certificate

The Pano Controller 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.

The Pano Controller supports public keys that use either pfx file format.

When you install the Pano Controller VM, the Pano Controller VM installer prompts you to upload your own certificate. However, you can apply your certificate at any point after your installation using the Pano Controller's UI.

Note: You don't need to upload your certificate each time you upgrade. The Pano Controller installer preserves this information during an upgrade.

To upload your certificate from the Pano Controller:

Before You Begin: Confirm that Pano Controller VM is working in your network.

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Platform Settings** section > **Web Access:**, do the following:
   a. Clear the **Use Default Certificate** check box.
   b. Browse to and select the certificate.
   c. Type the password.
4. Click **OK**. A confirmation messages appears.
5. Click **OK** to save your changes and restart the Pano Controller VM. If you click **Cancel**, all changes will be lost and you'll need to upload the certificate again.

   Pano Controller can now be accessed via HTTPS using your custom certificate. The Pano Controller continues to accept connections on the HTTP port (port 80) if it has not been disabled.

To upload your certificate from the console:

Before You Begin: Confirm that Pano Controller VM is working in your network.

1. Connect to the Pano Controller VM using a secure connection. Go to Initiate Secure Connections.
2. Copy the certificate to the Pano Controller VM. Save the file in the `/opt` directory.
3. Copy the `/opt/`*`hostname`*`/broker/conf/server.xml` file from the Pano Controller VM to your desktop.
4. Open the `server.xml` in an editor (Notepad or vi).
5. Add the following XML tags to the SCVMM 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 Controller VM. Afterward, you can access the Pano Controller via HTTPS using your custom certificate. The Pano Controller continues to accept connections on the HTTP port (port 80) if it has not been disabled.

Next: Restart Pano Controller VM

See also: Reset To Default Certificate

Restart Pano Controller VM

When working with certificates or when deleting `/tmp` files, you'll need to restart the Pano Controller VM.

1. From the VMware console, log on to the Pano Controller VM using the superuser (root) credentials.
2. Select option **5 - Drop to bash shell (Power Users)**.
3. Type the following command, then press Enter.

```
service atto restart
```

Next: Enable HTTP

Enable HTTP

1. Power on the Pano Controller.
2. Log on to Pano Controller VM.
3. From the Main Menu, select option **4 - Configure HTTPS Settings**.
4. The **Enable HTTP (y/n)?** prompt appears.
5. Type `y`, then press **Enter**. You are asked to reset to the default certificate.
6. Type `n`, then press **Enter**.

Next: Enable HTTP

Reset To Default Certificate

The Pano Controller UI may become inaccessible in some cases after you have disabled HTTP and then configure a certificate file that is a valid PKCS#12 file. If this happens, use the console to reset the certificate to the default self-signed.

1. Power on the Pano Controller.
2. Log on to Pano Controller VM.
3. From the Main Menu, select option **4 - Configure HTTPS Settings**.The **Enable HTTP (y/n)?** prompt appears.
4. Type `y`, then press **Enter**. The **Use default (self-signed) certificate (y/n)?** prompt appears.

5. Type `y`, then press **Enter**. The **Confirm (y/n)?** prompt appears.
6. Type `y`, then press **Enter**.

Next: Change Superuser Password

Change Superuser Password

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

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

Provide Users Administrator Access To Pano Controller

Provide Users Administrator Access To Pano Controller

You can configure network accounts for full access or read-only administrative roles. Local accounts always have full access.

1. Log on to the Pano Controller as `admin`.
2. Click on the **Setup** tab.
3. In the **Administrator Roles** section, specify the network account for the user(s) or group(s) that you want to provide admin access.

   Type the canonical name or browse the tree, then click **Configure**.

   - If you want to provide one user access:

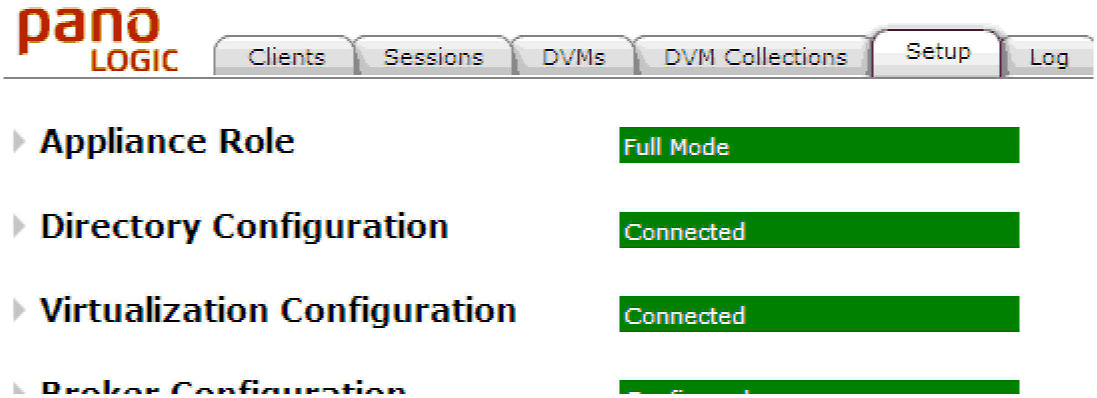
   ```
   acme.com/Departments/IT/John Smith:acme.com/Departments/
   IT/Jane Smith
   ```

   - If you want to add more than one user, provide a colon separated list:

   ```
   acme.com/Departments/IT/John Smith:acme.com/Departments/
   IT/Jane Smith
   ```

   - If you want to provide entire group:

   ```
   acme.com/Departments/IT
   ```



Appliance Role — Full Mode

Directory Configuration — Connected

Virtualization Configuration — Connected

Broker Configuration

Next: Change Web Admin Account 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). There is no default password: the password was set when the Pano Controller was configured as part of deployment.

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

Next: Determine Pano Controller Version

Determine Pano Controller Version

After an upgrade it's important to verify that the Pano Controller reflects the version that you installed.

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. Expand the **Platform Settings** section and observe the value in the **Version** field. This value represents the Pano Controller version that's currently installed.

Next: About Backup Manager

Related Topics

Configure Backup Manager

Backup Retention Policy

Delete Old Backups

Perform Manual Backups

Restore from Backups

Disable Automatic Backups

[Troubleshoot Backup Problems](#)

About Backup Manager

In the event of a catastrophic failure such as database corruption or loss of the Pano Controller VM or an unintentional administrative operation, the Pano Controller enables you to recover by restoring from a backup.

Database backup/recovery protects against data loss due to database corruption. Even failover or clustering does not fully protect against database corruption since the corruption is often transferred to the backup or peer databases.

The restore is fast (about 1 minute) and easy. You can restore to a production Pano Controller, or you can configure a standby Pano Controller that can be activated by restoring from recent database backup file. In the worst case, you can import a new Pano Controller VM and restore a recent backup file. For additional protection, continue to perform routine snapshots or backups of the entire Pano Controller VM.

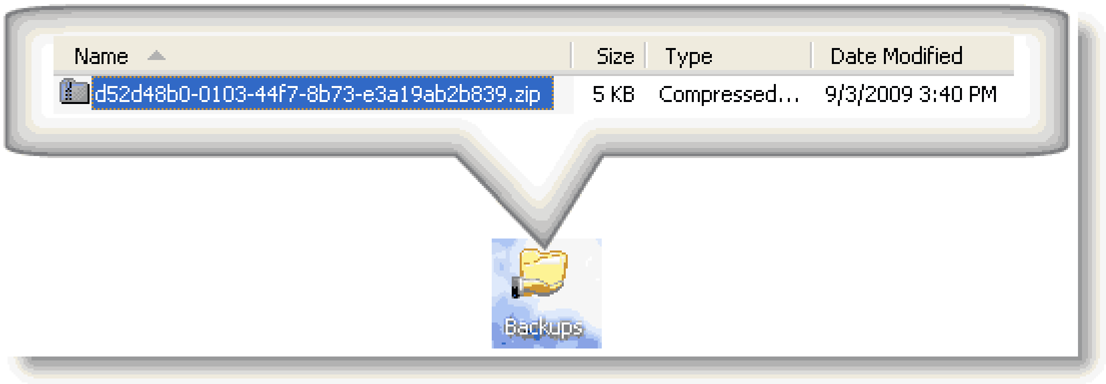
A backup file contains:

- a dump of the database
- virtual machine configuration
- local accounts
- network configuration (e.g. IP address, netmask, default gateway, etc.)
- backup type, description (comment) and data/time

Pano Logic's Backup Manager provides two types of backups:

- **Manual** - a backup triggered by administrator pressing a button on the Setup tab.
- **Scheduled** - a backup automatically initiated by the Pano Controller once per day.

  The backup process starts at 2:00am, when there is a low probability the Pano Controller is handling a lot of requests. For ease of use, this time cannot be changed.



Name	Size	Type	Date Modified
d52d48b0-0103-44f7-8b73-e3a19ab2b839.zip	5 KB	Compressed...	9/3/2009 3:40 PM

Next: [Configure Backup Manager](#)

Related Topics

[Backup Retention Policy](#)

[Delete Old Backups](#)

Perform Manual Backups

Restore from Backups

Disable Automatic Backups

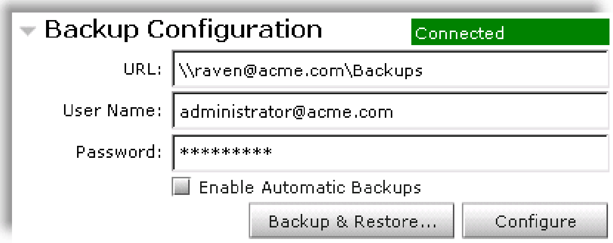
Troubleshoot Backup Problems

Configure Backup Manager

You can specify a Windows or Samba share as the target destination for your backups. The Pano Controller requires at least 10MB of disk space on the target destination. A typical backup file is rather small (100 KB to 1 MB). If you don't define a target destination, the Pano Controller saves the backups locally, though you can access them from the Pano Controller. The Pano Controller VM reserves 10MB of disk space for local backups.

If the share becomes unavailable, the dump file will be copied locally and the Pano Controller generates an error and saves it to the log file. When the share becomes available again, the Pano Controller automatically moves the local files to the target destination.

1. Create a share to contain your backups. If you have two Pano Controllers configured as a group, each Pano Controller must have a designated share.
2. Log on to the Pano Controller as `admin`.
3. From the Setup tab, expand the Backup Configuration section.
4. Type a target destination, a secure share, where the URL is `\\<ServerName>or<IPAddress>\<ShareName>`. For example, `\\raven.acme.com\Backups`.



Backup Configuration — Connected

URL: \\raven@acme.com\Backups

User Name: administrator@acme.com

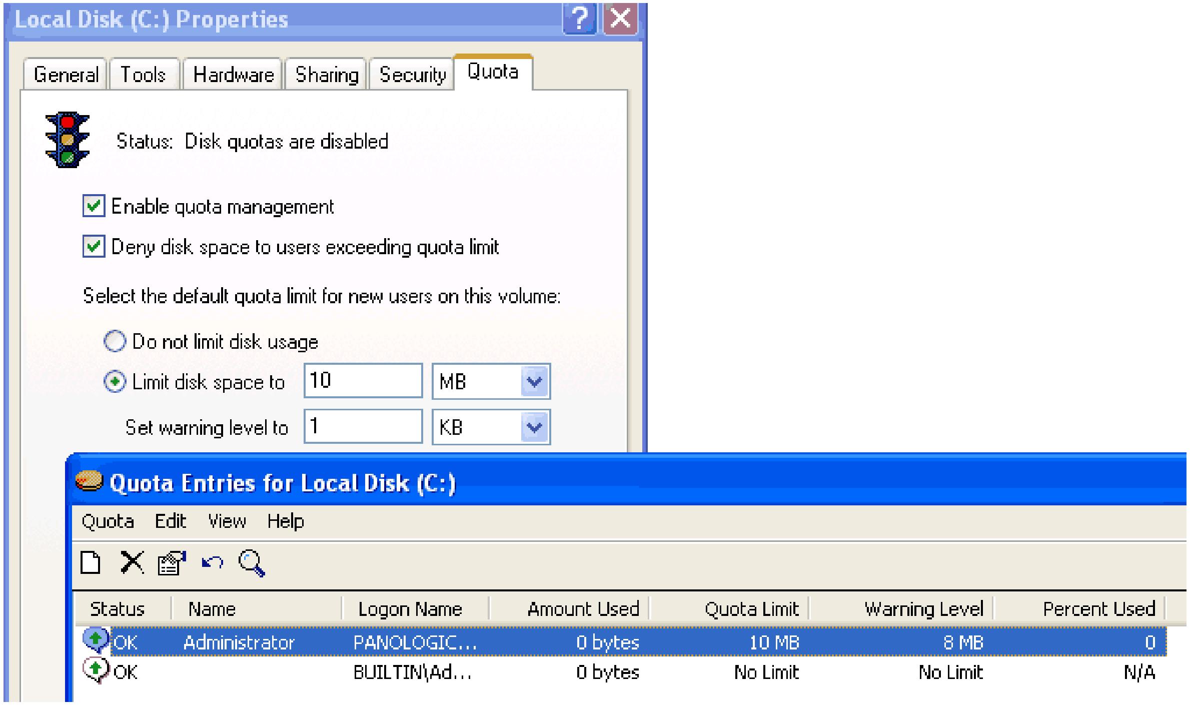
Password: *********

□ Enable Automatic Backups

The Pano Controller requires at least 10MB of disk space on the target destination. If the destination does not meet the minimum disk space requirements the Pano Controller prompts you to choose another destination.

5. Type the credentials for the target destination into the backup configuration, then click **Configure**. The account must have `Full Control`.

6. Ensure that your target destination has at least 10MB of space. If you've implemented user management quotas, make sure the user name that you specified above has a quota limit of no less than 10MB.



Status: Disk quotas are disabled

☑ Enable quota management

☑ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

○ Do not limit disk usage

● Limit disk space to 10 MB

Set warning level to 1 KB

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
OK	Administrator	PANOLOGIC...	0 bytes	10 MB	8 MB	0
OK		BUILTIN\Ad...	0 bytes	No Limit	No Limit	N/A

7. Perform a manual backup to make sure everything is working as expected.

Troubleshooting: If Backup Configuration doesn't indicate `Connected` or for other problems, go to Troubleshoot Backup Problems.

Related Topics

About Backup Manager

Backup Retention Policy

Delete Old Backups

Perform Manual Backups

Restore from Backups

Disable Automatic Backups

Troubleshoot Backup Problems

Backup Retention Policy

When managing your backups, the Pano Controller retains:

- Any manually triggered backup files until you manually delete them.
- 10 days of scheduled backups.

  If there is not enough space to keep 10 scheduled backups the Pano Controller automatically deletes the oldest backup to recover space for the new backup, then logs a warning. The minimum disk space requirement for the destined share is 10MB.

The Pano Controller stores all backups locally. After performing a backup, the Pano Controller moves it to the network destination directory that you specify. This policy makes the system more fault tolerant of network and disk space issues.

For security reasons, never will a backup store the Pano Controller password. Backups themselves are not encrypted, though you can implement a mechanism for encrypting the backup file, or you can store the backup files on secure or encrypted file system.

Related Topics

About Backup Manager

Delete Old Backups

Perform Manual Backups

Restore from Backups

Disable Automatic Backups

Configure Backup Manager

Troubleshoot Backup Problems

Delete Old Backups

There's no need to delete scheduled backups. The Pano Controller automatically makes room for scheduled backups based on its retention policy. However, you can (and should) manually delete unnecessary manual backups just as you would any file on a share.

It's important that you periodically delete old and unnecessary manual backups because your manual backups share the same backup quota. It's important that you always have space for your scheduled backups. Each backup lists its backup size.

Although your backups appear on the share, it's better and easier to delete the backups via the Pano Controller.

1. From the Setup tab, expand the Backup Configuration section.
2. Click the **Backup & Restore** button.
3. In the Available Backups table, select the backup that you want to delete, click **Delete**, then **Delete Backups**. The backup no longer appears in the Available Backups table.

Related Topics

About Backup Manager

Backup Retention Policy

Perform Manual Backups

Restore from Backups

Disable Automatic Backups

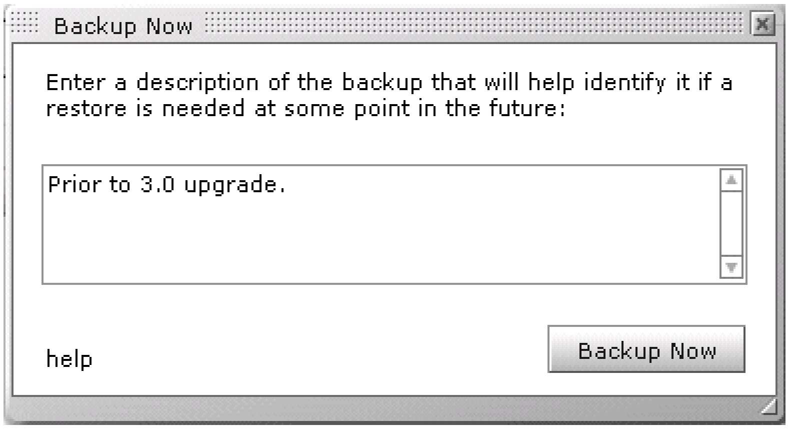
Configure Backup Manager

Troubleshoot Backup Problems

Perform Manual Backups

For reasons outlined in Restore from Backups, there is no need to back up a secondary Pano Controller that is part of a failover configuration. Similarly, there is no need to back up a slave Pano Controller that is part of a Pano Controller group.

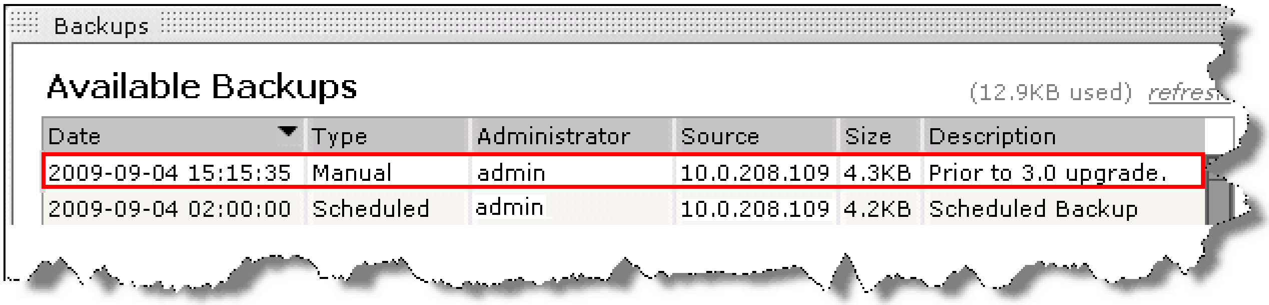
1. From the Setup tab, expand the Backup Configuration section.
2. Click the **Backup & Restore** button.
3. In the Backups dialog box click **Backup Now**.
4. In the Backup Now dialog box, type a description to help you identify the backup in the event that you need to restore, then click **Backup Now**.



Enter a description of the backup that will help identify it if a restore is needed at some point in the future:

Prior to 3.0 upgrade.

5. Verify that the backup appears in the Available Backups table.



Available Backups

Date	Type	Administrator	Source	Size	Description
2009-09-04 15:15:35	Manual	admin	10.0.208.109	4.3KB	Prior to 3.0 upgrade.
2009-09-04 02:00:00	Scheduled	admin	10.0.208.109	4.2KB	Scheduled Backup

Related Topics

About Backup Manager

Backup Retention Policy

Delete Old Backups

Restore from Backups

Disable Automatic Backups

Configure Backup Manager

Troubleshoot Backup Problems

Restore from Backups

If you have a failover configuration, never restore a backup from a primary to a secondary, unless you plan on permanently removing the primary from the failover configuration. Two active nodes in a failover configuration must be avoided to prevent data corruption. In this case, bring down the primary first, then remove it from the failover configuration. You can safely restore a primary backup to the primary. A restore takes no more than a minute.

1. If your Pano Controller has become unusable, build a new Pano Controller VM:
   - from scratch.
   - from same the same Pano Controller VM.
   - from a routine snapshot. If the snapshot is more recent than the most recent backup, then you're done.
   - from a standby Pano Controller VM.
2. On the new Pano Controller, configure the backup settings as they were in your previous Pano Controller.
3. Browse the list of backups. The browser displays the following information for each backup:
   - **Date**. The date that the backup was created.
   - **Type**. The type of backup: manual or scheduled.
   - **Administrator**. The credentials of the admin that initiated the backup.
   - **Source**. The IP address of the Pano Controller that was backed up.
   - **Size**. The size of the backup in KB.
   - **Description**. The description for *scheduled* backups is simply `Scheduled Backup` and you cannot influence the description. The description for *manual* backups will be the description that you defined when you initiated the backup.
4. Select a file from which to restore, then click **Restore**, then Restore Backup.

Related Topics

About Backup Manager

Backup Retention Policy

Delete Old Backups

Perform Manual Backups

Disable Automatic Backups

Configure Backup Manager

Troubleshoot Backup Problems

Disable Automatic Backups

Automatic backups are enabled by default.

1. From the Setup tab, expand the Backup Configuration section.
2. Clear the **Enable Automatic Backups** check box.

Related Topics

About Backup Manager

Backup Retention Policy

Delete Old Backups
Perform Manual Backups
Restore from Backups
Configure Backup Manager
Troubleshoot Backup Problems

19

Choosing a Pano Client Endpoint Discovery Method

After you've installed and configured the Pano Controller VM, you're ready to choose a Pano System Endpoint Discovery Method. We've created a video to help you understand this process: How Pano Discovery Works.

Pano System Endpoints need to be discovered before they can be controlled by the Pano Controller. Once discovered, Pano System Endpoints receive a name of the form:

`PanoDevice-`***PanoDeviceMacAddress***.

For example, PanoDevice-00-1c-02-40-17-95.

As discussed in Set Up Collections with Device Restrictions, you'll eventually decide on a naming convention for your Pano System Endpoints to make discovery easier.

There are two ways that the Pano Controller can discover Pano System Endpoints:

- Broadcast/Probe method
- DHCP method

What to do next: Do one of the following:

Set Up Pano Client Discovery Using Broadcast/Probe

Set Up Pano Client Discovery Using DHCP

Set Up Pano Client Discovery Using Broadcast/Probe

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

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Discovery Configuration** section, click the **Edit** button, specify *any* of the following discovery options, then click **OK**:
   - **Local Broadcast** - Select the check box for this option if your Pano Controller and Pano System Endpoints are located on the same subnet.

     When you enable this option, the Pano Controller periodically broadcasts packets on the local subnet to discover new Pano System Endpoints.

   - **Probe Address** - Use this option to do one of the following:
     - **Specify a range of IP addresses** in which the Pano Controller can probe for Pano System Endpoints. Avoid specifying an overly broad range of addresses as that causes additional unnecessary broadcasts on your network.

     Use this option only when there is a small defined range of IP addresses for Pano System Endpoints as is usually the case during a trial (before you implement Pano System 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.

- **Specify Remote Broadcast Networks** when your Pano System Endpoints are located on multiple subnets of your network. Enter a space-separated list of subnets. For example: 192.168.1.55 191.255.255.255. Subnet IP addresses must end with a value of 255.

4. Set up the Pano System Endpoints, if you haven't already. Connect them to your network using the Pano System Endpoints' Ethernet port. To verify that the Pano System Endpoints are connected to the network, see Pano Zero Client Light Indicators.

5. Locate the new Pano System Endpoints that the Pano Controller VM just discovered. From the Pano Controller, click on the **Pano System Endpoints** tab. The default name for a Pano System Endpoint is `PanoDevice-`***`MACAddress`***.

What to do next: If you're in the process of deploying the Pano Controller VM, return to determine the next step.

Related Topics

Set Up Pano Client Discovery Using DHCP

Set Up Pano Client Discovery Using DHCP

You can configure a DHCP server to provide the address of the Pano Controller to the Pano System Endpoint. 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:

- Linux DHCP server – Add Pano Logic Vendor Class for Linux DHCP Server.
- Netware DHCP server – Add Pano Logic Vendor Class for Netware DHCP Server.
- Cisco DHCP server – Add Pano Logic Vendor Class for Cisco IOS DHCP Server.
- Alcatel/Lucent VitalQIP – Add Pano Logic Vendor Class for Alcatel/Lucent VitalQIP DHCP Server
- Infoblox DHCP server – Add Pano Logic Vendor Class for Infoblox DHCP Server

This example uses 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, use vendor specific option, `Code 1` or `101`, Type IP address, Value: ***`PanoControllerServerIPAddress`*** where `PanoControllerServerIPAddress` is the static IP address of the Pano Controller VM.

1. From the Windows Server running the DHCP Server, launch the Manage Your Server tool (Windows Server 2003) or the Server Manager tool (Windows Server 2008).

2. Right-click on the DHCP Server and click **Define Vendor Classes...**.

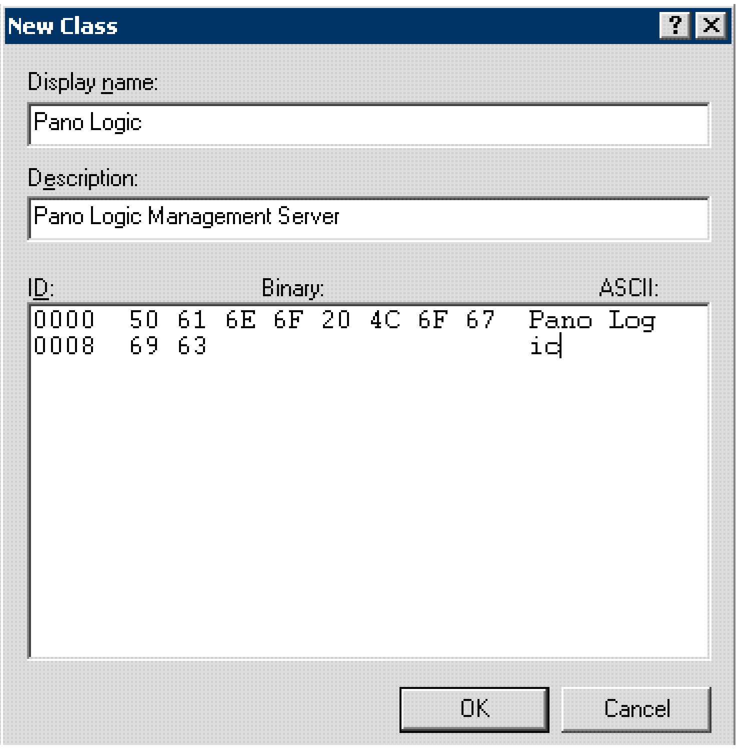
3. Create the new vendor class:

   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 Controller`.
   - In the text box, and underneath **ASCII**, type `Pano Logic`. Even though the text box is blank you can still click in the text box and type in a value.

4. Click **OK**.



Pano Logic

Pano Logic Management Server

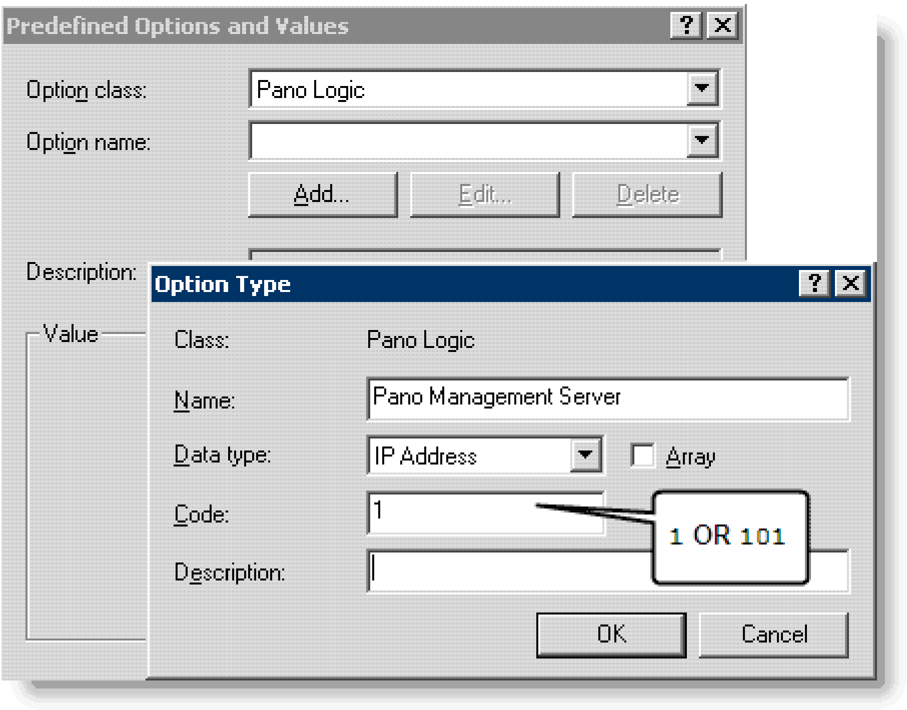
```
0000   50 61 6E 6F 20 4C 6F 67   Pano Log
0008   69 63                     ic
```

5. Close the DHCP Vendor Classes dialog.
6. From the DHCP window, right-click on the Domain Controller and select **Set Predefined Options**.
7. In the Option Class drop-down list, select **Pano Logic**, then click **Add**.
8. In the Option Type dialog, do the following:

   a. Into the Name field, type `Pano Controller`.

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

c. In the Code field, type `1 or 101`.



Option class: Pano Logic

Option name:

Class: Pano Logic

Name: Pano Management Server

Data type: IP Address ☐ Array

Code: 1

Description:

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

9. 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 Controller VM.

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

11. In the Scope Options window, select the **Advanced** tab.

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

The Pano Controller now appears in the scope options.

The DHCP Server is properly configured to pass the Pano Controller's address to Pano System Endpoints.

13. Install the Pano System Endpoints, if you haven’t already. Simply connect them to your network using the Pano System Endpoints’ Ethernet port. To verify that the Pano System Endpoints are connected to the network, go to Pano Zero Client Light Indicators.

14. Locate the new Pano System Endpoints that the Pano Controller VM just discovered. From the Pano Controller, click on the **Pano System Endpoints** tab. The default name for a Pano System Endpoint is `PanoDevice-`***MACAddress***.

What to do next: Get your system licensed. If you’re in the process of deploying the Pano Controller VM, return to determine the next step.

20 Licensing

Licensing in Pano System 6.0

Pano System 6.0 introduces a new form of software licensing in conjunction with the launch of the Pano Virtual Client software.

Please note that license keys issued with Pano System 5.0 are no longer valid in Pano System 6.0 and will need to be replaced by the new format license keys. Since Pano System 5.0 didn’t require a license key except when being upgraded very few customers will have a license key in this older format.

How Licensing Works

Within the new Pano System 6.0 license keys, two kinds of capabilities are listed:

- Enable entitlements that govern your use of a software or hardware endpoint or accessory.
- Upgrade entitlements that govern your ability to upgrade Pano Controller.

The following activities or capabilities are controlled by licensing in Pano System 6.0:

- Upgrading the Pano Controller/Pano Maestro appliance.
- Backup and restore between different versions of the Pano Controller database.
- Running Pano Virtual Client (PVC) software.

The number of Pano Zero Clients and Pano Remote accessories in use is also monitored by the licensing system but no restrictions are applied if your use of these hardware endpoints exceeds the number you are entitled to in your license key. Only the administrator will be notified of this type of license violation.

Some Pano Logic products don't require license keys, such as purely physical hardware like VESA monitor mounts. And some services, such as Advance Warranty Replacement or Per Incident Support, also don't require license keys as they don't impact your maintenance and upgrade rights.

Next: Types of Product Licenses

Types of Product Licenses

Not all Pano Logic products and support services require a separate license. Licenses for endpoints, either Pano Zero Clients or Pano Remote, are included with the purchase of that product (i.e., bundled).

Typically, when you purchase Pano System for VDI, you will also purchase seat licenses for Pano Zero Client, subscription licenses for Pano Virtual Client, or a mix of both. Pano Remote only include a license to use the endpoint as an accessory - you must also purchase a seat license for the Pano System software as part of a Zero Client or Virtual Client bundle.

(The purchase of Pano System for VDI means you are purchasing one of more licenses for Pano Controller and Pano Maestro as well - these are the core control components.)

Device-based licenses, also known as seat licenses, refers to a license that is tied to the use of an endpoint device, such as a Pano Zero Client, although not to a specific serialized endpoint. Concurrent user means the license is for one active concurrent use or session and is not tied to a specific endpoint installation, serialized hardware product, or named user. Both of these types of product licenses are also usually bundled with a period of maintenance rights that allow you to upgrade to new versions of the Pano System software.

Because device-based licenses are not tied to specific hardware devices, you can purchase extra hardware, either to have as spares or to accommodate installation in different areas. For example, you could purchase 60 Pano Zero Clients and 50 licenses, along with your Pano System for VDI. This would let you simultaneously support 50 users, logging in fro any of the 60 endpoints.

Licenses have different terms. The licenses included in the Zero Client bundles and for the Pano Remote accessory are perpetual device-based licenses and never expire while Pano Virtual Client licenses for both the software endpoint and the server software are subscription-based for one concurrent user and typically need to be renewed each year.

This information covers the standard licensing terms for Pano Logic products - variations on these terms including longer license terms are available.

Next: Licenses and Specific Hardware and Installations

Licenses and Specific Hardware and Installations

Licenses, even when device-based, aren't locked to specific Pano hardware. Customers can freely swap out Pano Zero Clients or Pano Remote USB Keys without needing to change or update their license keys.

In the same way Pano Virtual Client licenses are not tied to a specific installation of Pano Virtual Client but rather to the maximum number of concurrently active sessions Pano Controller will allow. You are permitted to install Pano Virtual Client on as many host PCs or laptops as you want as long as the maximum number of concurrent sessions does not exceed the number of licenses.

Next: Evaluation Period for Unlicensed Use

Evaluation Period for Unlicensed Use

To help you try out the Pano System during trials or proof of concept deployments, customers can run in an UNCONFIGURED state without loading a license key file for up to 60 days. During this evaluation period the product will be fully functional but warning messages on the lack of licensing will be displayed to the administrator in the Pano Controller console. An example of these messages is shown below:

```
License Manager Unconfigured: No License Key has been loaded. [X] days remaining
before a License Key must be loaded. Please contact Pano Logic at
licensing@panologic.com to obtain your License Key to prevent any interruption in
access to your virtual desktops.
```

Before the end of this evaluation period a License Key file must be obtained and loaded in the Pano Controller License Manager. If you fail to load a License Key file, the license state will change to VIOLATION, continued use of the software will be restricted, and a warning message like the following will be displayed to the administrator:

```
"License Manager is in Violation state. Evaluation period has expired. Please load
a valid License Key. Please contact Pano Logic at licensing@panologic.com."
```

Please note that this evaluation period doesn't apply to existing Pano System deployments that are being upgraded to Pano System 6.0. Existing customers need to obtain their License Key file from the Customer Center before upgrading to Pano System 6.0.

Pano Virtual Client also has its own grace period of 60 days during which you can run an unlimited number of concurrent user Pano Virtual Client sessions. Even if you have a license key loaded which doesn’t include any licenses for Pano Virtual Client you are still able to try Pano Virtual Client for up to 60 days without a license. However, once you load a license key that includes any Pano Virtual Client licenses you will be limited to just the number of concurrent sessions equal to the number of unexpired Pano Virtual Client subscription licenses.

Next: License States and Transitions

License States and Transitions

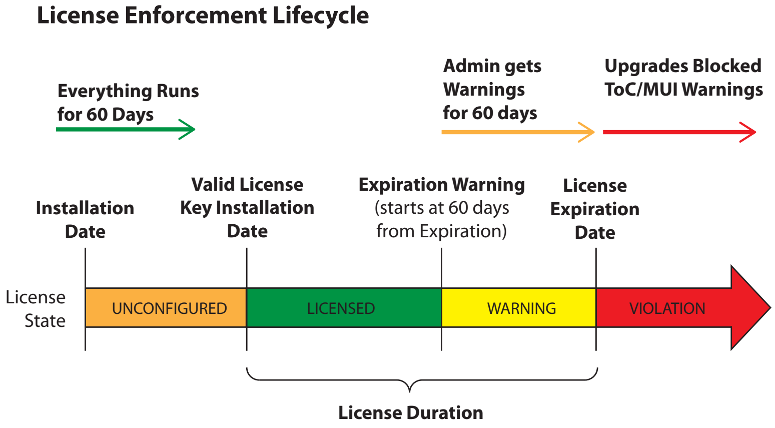
Pano System 6.0 deployments are always in one of several possible license states and each license state has a number of possible transitions to and from the other states:

1. **UNCONFIGURED** - this is the initial state a new deployment will be in until a license key file is loaded in the License Manager. New installations can remain in this state for up to 60 days before either moving to LICENSED (if a valid license is loaded) or VIOLATION (if no license is loaded).
2. **LICENSED** this is the normal state for a license and you are put into this state when:
   - You loading a valid license key after being UNCONFIGURED.
   - You were in WARNING but renewed a subscription license or maintenance right that was about to expire.
   - You were in VIOLATION due to an expired Pano Virtual Client subscription license or a quantity of endpoints in excess of your license.

3. **WARNING** this state is reached from a LICENSED state when:
   - Subscription licenses for Pano Virtual Clients are within 60 days of expiring.
   - Maintenance rights have expired for Pano Zero Client endpoints.
   - Premium Support is within 60 days of expiring.

   Note: Note: no warning is provided if you are about to exceed the number of seats you are licensed to use; only if a subscription license is about to expire.
4. **VIOLATION** this state is reached:
   - If over 60 days passes in an UNCONFIGURED state and no valid license key is loaded.
   - If LICENSED and a larger Quantity of hardware endpoints is in use than is licensed.

This illustrates these different license states but is a simplification as you might not progress from one state to the next in a linear manner. For example, if you have subscription licenses expire and then purchase an extension for these licenses, your license state might change from LICENSED to VIOLATION and then back to LICENSED.


License Enforcement Lifecycle
Everything Runs for 60 Days
Admin gets Warnings for 60 days
Upgrades Blocked ToC/MUI Warnings
Installation Date
Valid License Key Installation Date
Expiration Warning (starts at 60 days from Expiration)
License Expiration Date
License State
UNCONFIGURED
LICENSED
WARNING
VIOLATION
License Duration

You can check on your current license state by going to the License Manager via the License Configuration option at the bottom of the Configuration page of the Pano Controller console. The License Manager can also be accessed from the console via Pano Maestro.

Note that the License Manager might indicate that you are in VIOLATION even though only part of your license rights have been exceeded. For example you might be using fewer Zero Clients than you're licensed for but if you exceed the number of licensed Pano Remotes your license state will change to VIOLATION until this is corrected.

Next: Getting Your License Key

Getting Your License Key

Each customer will be issued a single license key file that covers all of the products and maintenance purchased from Pano Logic. In general a license key file will be generated and emailed to a customer each time an invoice is generated for a licensed product or service. Customers can also go to the Pano Logic Customer Center (at customer.panologic.com; registration required) and manually download their most recent license key file, or contact our Customer Support group via email to licensing@panologic.com to request that your license key be emailed to you.

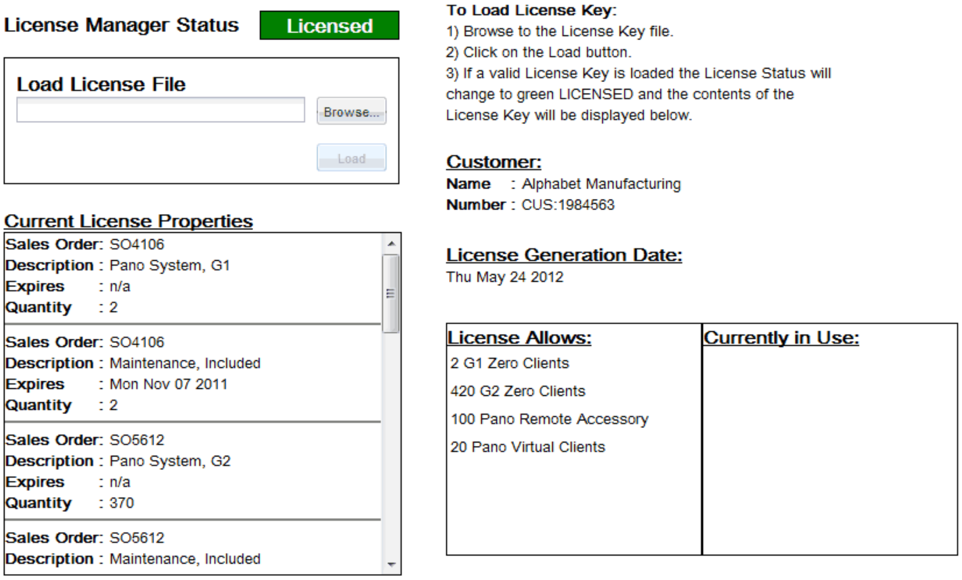
License keys are mailed to the designated “End Customer Sys Admin” contact for the customer. This may be the IT staff member responsible for the Pano deployment or it may be a reseller contact if your reseller provides that type of support service for your Pano deployment. If you wish to change or check on who is designated as the licensing contact for your organization please contact Customer Support.

Next: New License Manager

New License Manager

The new License Manager console in Pano Controller 6.0 is used to load license key files or check the status or state of your licenses. This new console shows both products and services you are licensed for along with the current usage. The License Manager can be reached from the License Configuration option at the bottom of the Configuration tab in Pano Controller.

The License Manager both provides a way for you to load your license key file and to check on license status and contents. The current license status or state (see section below for details on the different license states) is indicated at the top of the License Manager. Details on the contents of the most recent license key loaded are shown in a scrolling list in the lower-left corner. On the right side a summary of the active license rights is listed along with the inventory counts of endpoints that are currently in use.



License Manager Status: Licensed

Load License File

To Load License Key:
1) Browse to the License Key file.
2) Click on the Load button.
3) If a valid License Key is loaded the License Status will change to green LICENSED and the contents of the License Key will be displayed below.

Customer:
Name : Alphabet Manufacturing
Number : CUS:1984563

License Generation Date:
Thu May 24 2012

Current License Properties

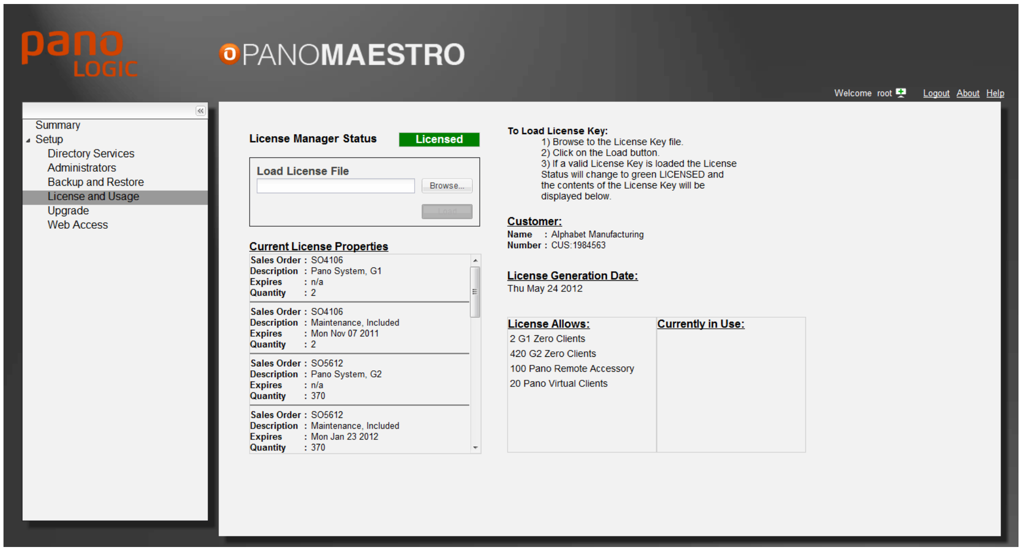
Sales Order: SO4106
Description : Pano System, G1
Expires : n/a
Quantity : 2

Sales Order: SO4106
Description : Maintenance, Included
Expires : Mon Nov 07 2011
Quantity : 2

Sales Order: SO5612
Description : Pano System, G2
Expires : n/a
Quantity : 370

Sales Order: SO5612
Description : Maintenance, Included

License Allows:	Currently in Use:
2 G1 Zero Clients 420 G2 Zero Clients 100 Pano Remote Accessory 20 Pano Virtual Clients	



License Manager Status: Licensed

Load License File

To Load License Key:
1) Browse to the License Key file.
2) Click on the Load button.
3) If a valid License Key is loaded the License Status will change to green LICENSED and the contents of the License Key will be displayed below.

Customer:
Name : Alphabet Manufacturing
Number : CUS:1984563

License Generation Date:
Thu May 24 2012

Current License Properties

Sales Order : SO4106
Description : Pano System, G1
Expires : n/a
Quantity : 2

Sales Order : SO4106
Description : Maintenance, Included
Expires : Mon Nov 07 2011
Quantity : 2

Sales Order : SO5612
Description : Pano System, G2
Expires : n/a
Quantity : 370

Sales Order : SO5612
Description : Maintenance, Included
Expires : Mon Jan 23 2012
Quantity : 370

License Allows:	Currently in Use:
2 G1 Zero Clients 420 G2 Zero Clients 100 Pano Remote Accessory 20 Pano Virtual Clients	

Next: Control of Upgrades by Licensing

Control of Upgrades by Licensing

License keys can control upgrade entitlements, also referred to as Maintenance rights. Maintenance rights can be purchased multiple ways including:

- Bundled with the initial product purchase; for example, 1 year of maintenance is included in the purchase of a Pano System seat with a Pano Zero Client and Pano Virtual Client licenses include maintenance for the entire term of the subscription.
- Maintenance renewals or extensions you purchased either with your product purchase or at a later date.
- As a component of the Premium Maintenance and Support subscription or renewal.

In order to upgrade the Pano Controller and Pano Maestro virtual appliances you must have unexpired maintenance rights for all of your registered endpoints. Prior to allowing the upgrade or even allowing you to restore a backup from an earlier version of the Pano System the License Manager will check your inventory of endpoints against the upgrade rights in your license file.

This check of maintenance rights is done as follows:

- If you are in an UNCONFIGURED license state (see below) due to not having loaded a license you will not be allowed to upgrade or restore from an earlier version.
- If you have at least one unexpired subscription license for Pano Virtual Client, you will be allowed to upgrade.
- If you have only hardware endpoints, you must have an unexpired maintenance right for each hardware endpoint registered in Pano Controller.

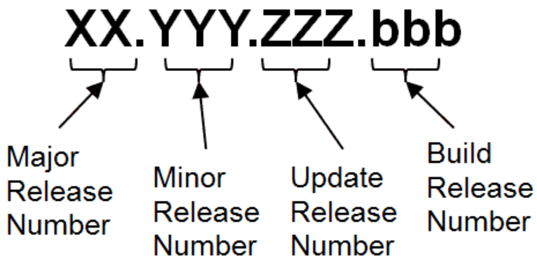
To determine your maintenance rights in your license key, check the License Manager.

Note: The License Manager in Pano Controller may warn you about expiring maintenance, even though you have correctly installed your new license. This is because the License Manager checks all licenses in your system. You should just ignore these messages; they will stop when the expiring maintenance period ends and your renewed maintenance becomes effective. Future software releases will fix this.

Next: Version Numbers and Upgrades

Version Numbers and Upgrades

In deciding whether to check your license key for maintenance rights the License Manager compares the detailed version number of your current Pano System with that of the version into which you are attempting to upgrade. Only upgrades that would change the major or minor version numbers require a license check, while an update that only changes the update or build release numbers do not require any maintenance rights and will not cause your license to be checked.



For example, if you are currently running version 6.0.0 and wish to move to 6.0.2, this is not considered to be an upgrade. No maintenance rights are required and your license is not checked. However, if you were moving from 6.0.0 to 6.1.0 this would be considered an upgrade and you would need to have unexpired maintenance rights for all of your endpoints in your license key.

Next: Enforcement of License Limitations

Enforcement of License Limitations

Warning Alerts for Administrators

When a licensed quantity is exceeded or when a maintenance/support right or a subscription license is within 60 days of expiring the administrator will see license warnings when logging into the Pano Controller console. These warning alerts are only visible to the administrator and will be accompanied by warning notification emails if you have configured email notifications in Pano Controller. Examples of these warning messages are:

```
License Manager is in Warning state:
Maintenance rights for X endpoints will expire in y days.
Licenses for x Pano Virtual Clients will expire in y days.
```

Contact Pano Logic at tlicensing@panologic.com to obtain a new License Key and to prevent any interruption in access to your virtual desktops.

Enforcement for Virtual Desktops

Licenses for endpoints, either Pano Zero Clients or Pano Remote, are included with the purchase of that product (i.e., bundled). Pano System 6.0 uses soft enforcement of licensing for Pano Zero Client and Pano Remote endpoints; even if you've exceeded the licensed number of endpoints and your system is in a VIOLATION state, the system will continue to be fully functional. Pano Zero Client users will see:

```
Licensed quantity of Pano Zero Clients exceeded. Please contact your system
administrator to ensure access to your desktop is not interrupted.
```

Pano Remote users will still be able to log in, but will see a message:

```
Licensed quantity of Pano Remote Accessory exceeded. Please contact your system
administrator to ensure access to your desktop is not interrupted.
```

When this license limitation is exceeded, the administrator will also see warnings on the license status when logging into Pano Controller console, and the license status in the License Manager will change to VIOLATION.

```
"License Manager is in Violation state. Licensed quantity exceeded. Current
<endpoint-type> count exceeds the licensed count by X. Please disconnect unlicensed
additional <endpoint-type>.
```

Enforcement for Pano Virtual Clients

However, for Pano Virtual Clients hard or active enforcement is in place. This means that a user who attempts to start a Pano Virtual Client session that would be in excess of the number of concurrent user sessions you've licensed will be stopped and a license warning dialog will be displayed to the user telling them why they aren't able to use Pano Virtual Client.

```
No valid licenses are currently available for Pano Virtual Clients. Please contact
your system administrator to obtain access.
```

When this happens administrators will receive an email telling them that the license limits were reached provided that email notifications were enabled in the Pano Controller console configuration page.

Enforcement for Pano Controller & Pano Maestro

The only other license constraint that uses hard or active enforcement in Pano System 6.0 is the ability to upgrade the Pano Controller/Pano Maestro virtual appliance. See the section above on Control of Upgrades by Licensing for more details.

```
"License Manager is in Violation state. Licensed quantity exceeded. Current
<endpoint-type> count exceeds the licensed count by X. Please disconnect unlicensed
additional <endpoint-type>.
```

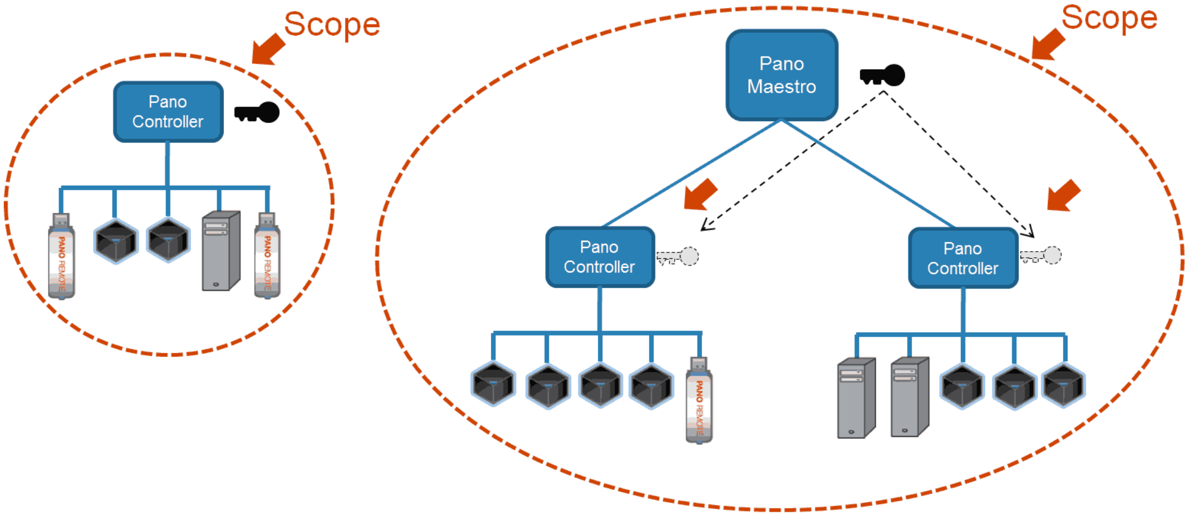
Next: Multiple Sites and License Enforcement

Multiple Sites and License Enforcement

Each Pano Logic customer is issued a single cumulative license that covers all products and services they've purchased. The license may include subscriptions or maintenance & support periods that have expired.

Licenses may also cover products that you have deployed at multiple sites. License can cover multi-site deployments of Pano systems provided there is one "scope" for the license; this means that all licensed endpoints have to be managed by a common Pano Controller instance (or group) and that the sites are linked by a common Pano Maestro instance.

This shows two examples of how license scope can be related to actual deployment sites. In both examples a single license key covers all endpoints in one scope. The example on the left is for a typical multi-site deployment where the sites are linked via a WAN allowing Pano Maestro to be used as the overall License Manager for all of the sites.



If you have multiple sites that are not connected by a secure WAN link to facilitate a common license scope using Pano Maestro or Pano Controller you will need to treat each site as a separate scope. Currently we do not directly support sharing licenses across multiple unlinked sites and the single cumulative license key issued to each customer includes all endpoints across all of your sites.

You can address deployments with multiple license scopes by loading your one license key at each of the sites.

Please note that the Pano Logic end user license agreement still requires that you limit the use of both perpetually licensed and subscription licensed endpoints across all your sites to no more than the number for which you have purchased unexpired licenses.

Next: License Configuration for the Pano System

Enforcement in Mixed Fujitsu and Pano Logic Environments

The licensing in Pano System 6.0 is only enforced for endpoints sold by Pano Logic. One of our OEMs, Fujitsu Technology Solutions (FTS) also sells Pano-powered zero client monitors (the DZ19-2 and DZ22-2) that can be connected to Pano Controller. FTS have implemented their own system of licensing that is not directly comparable to or compatible with the licensing in Pano System 6.0.

When using FTS zero clients in a Pano System 6.0 deployment no licensing check or enforcement will apply to the FTS endpoints; i.e. they will not be included in any checks for license compliance nor will they be counted when checking on maintenance rights prior to an upgrade. You are still legally required to comply with both the terms of your license agreement with FTS and with your Pano Logic end user license agreement.

License Configuration for the Pano System

License configuration for the Pano System involves configuration of the license service and installation of a license key. In this release the configuration of the license service is handled automatically by the system based on other configuration settings such as failover.

Based on your deployment model, the following configuration will be done automatically:

- Single Pano Controller: License service automatically gets set to https://localhost.
- Pano Controller Failover Group: License service automatically gets set to https://localhost on the active Pano Controller. The standby Pano Controller and any auxiliary Pano Controllers will be configured automatically to specify the active controller.
- Pano Controller Group without Failover: Note: This is not a recommended model; consider converting to a Pano Controller Failover Group. In this model, there is no clear?master? so the system automatically sets the license server instance to reside on the node managing the most clients.

When Pano Maestro is utilized, it acts as the license service for the scope of your entire system. Based on your deployment model, the following will occur:

- Single Pano Controller: When your single Pano Controller is first added to Pano Maestro, its license service will be updated to point to Pano Maestro.
- Pano Controller Failover Group: To add a Pano Controller Failover Group to Maestro, add the group from within the Maestro console and specify the virtual IP address of the group. When you do this, the License Configuration on all your Pano Controllers in the group will be automatically updated to point to Pano Maestro.
- Pano Controller Group without Failover: This model is not recommended or supported.

To Configure Licensing for a Pano Controller

1. Log on to the Pano Controller. If this is a Failover Group, log into the active Pano Controller.
2. Click on the Setup tab.
3. In the License Configuration section, make sure the URL points to the desired license service.
   - Single Pano Controller: confirm that the license service is set to https://localhost.
   - Pano Controller Failover Group: confirm that you are logged into the active Pano Controller and that the license service is set to https://localhost.
   - Pano Controller Group without Failover: confirm that you are logged into the Pano Controller that has License Configuration set to https://localhost.
4. Click the Manage Licenses button to check the current license status or import a license file.
5. Enter the path and file name or click the Browse button to locate the license file. License files are named in the format:
   CUS_<customerID>_<time>_<SalesOrderNumber>.xml, e.g.
   CUS_12345_8_35_40_SO1234.xml.
6. Click the Load button to import the license key into the license server.
7. Verify the Current License Properties and License Manager Status fields.

To configure licensing for a Pano Maestro, see Manage Pano Maestro System Licenses and Usage.

21 Configure Pano Controller Groups

This chapter includes the following topics:

About Pano Controller Scalability and Redundancy

A single Pano Controller can manage a small system, but it is not redundant and does not scale to a really useful size. Pano lets you create and group multiple Pano Controllers and configure them to support more users as well as to support each other in case of failure.

Scalability

Pano systems can be configured to support many thousands of users. To estimate the number of users you can support, go to Supported Number of DVMs and Pano Zero Clients. This tells you the approximate number of devices managed by a single Pano Controller instance or group.

Multiple groups can be used to scale this upward. Up to five Pano Controller groups can be centrally managed by Pano Maestro. See Deploy Pano Maestro. For example, you may want to use separate Pano Controller groups for different departments or divisions, or different locations. This also facilitates management by different IT groups.

It is possible to configure scalability without redundancy, but this is not recommended. If you have already set up redundancy, you can begin configuring additional Pano Controllers to support scaling. Go to Managing Scalability.

Redundancy

To ensure Pano system redundancy, the Pano system enables you to configure two Pano Controller instances in an active/standby failover configuration on two different physical servers. In this type of failover configuration, a standby Pano Controller takes the place of a failed primary Pano Controller. The secondary Pano Controller also off loads some client processing from the active primary Pano Controller (servicing client login requests).

When the active Pano Controller fails, the Pano system changes the mode of the standby Pano Controller from **standby** to **active**. The Pano Controller that becomes active assumes the virtual IP address of the failed Pano Controller and begins to handle all processing. You can configure email notifications to be sent in the event of an automatic failover. The failover is transparent to Pano System Endpoints.

The Pano system backs up the active Pano Controller after every configuration change. The configuration change is immediately sent to the standby. When a failover occurs, the standby loads and retains the configuration changes, thereby becoming active. You do not need to have schedule backups enabled.

When a failover occurs, important messages are saved to the log file and, if you have email notifications set up, you will be notified immediately.

If you are deploying a redundant system, you need to configure at least two Pano Controller instances, one primary and one secondary controller. Additional Pano Controllers, called auxiliaries, can be added for scalability.

Pano Controller Groups

A primary, secondary, and zero or more auxiliary Pano Controllers form a Pano Controller group. When you create a Pano Controller group, you will designate one Pano Controller as the primary and one Pano Controller as a secondary. Other Pano Controllers within the group are auxiliary nodes.

In a failover configuration, you have one primary Pano Controller and one secondary Pano Controller. *Primary* and *secondary* are roles. Primary indicates the Pano Controller that you favor as your production Pano Controller.

A primary or secondary Pano Controller can be in either active or standby mode. Normally, the primary is active and the secondary is standby. In a degraded state, the primary is standby and the secondary is active. It's important that you recover from a degraded state as soon as possible.

Active means that the Pano Controller with that role is the broker for the Pano system. The Pano Controller that is in *standby* mode is not a broker; rather, that Pano Controller is simply servicing client UIs login requests.

- **Primary** - The primary contains all the collections and optionally connects to Pano Maestro. The primary Pano Controller is automatically configured to manage all web logins and authentication for Pano user login screens. The primary Pano Controller coordinates the desktop connections and utilizes resources (distributes load) across the other group members as needed.
- **Secondary** - The secondary is configured in the failover configuration as the standby controller. This controller mirrors the primary controller and takes over if a failure occurs on the primary controller.
- **Auxiliary** - Up to four auxiliary Pano Controllers can be added to a group to load balance the Pano Controller functions across additional servers and support additional Pano System Endpoints.

A typical Pano Controller group configured for a high level of scalability consists of a primary Pano Controller, a standby Pano Controller, and additional auxiliary Pano Controllers.

IP Addresses and the Virtual IP Address

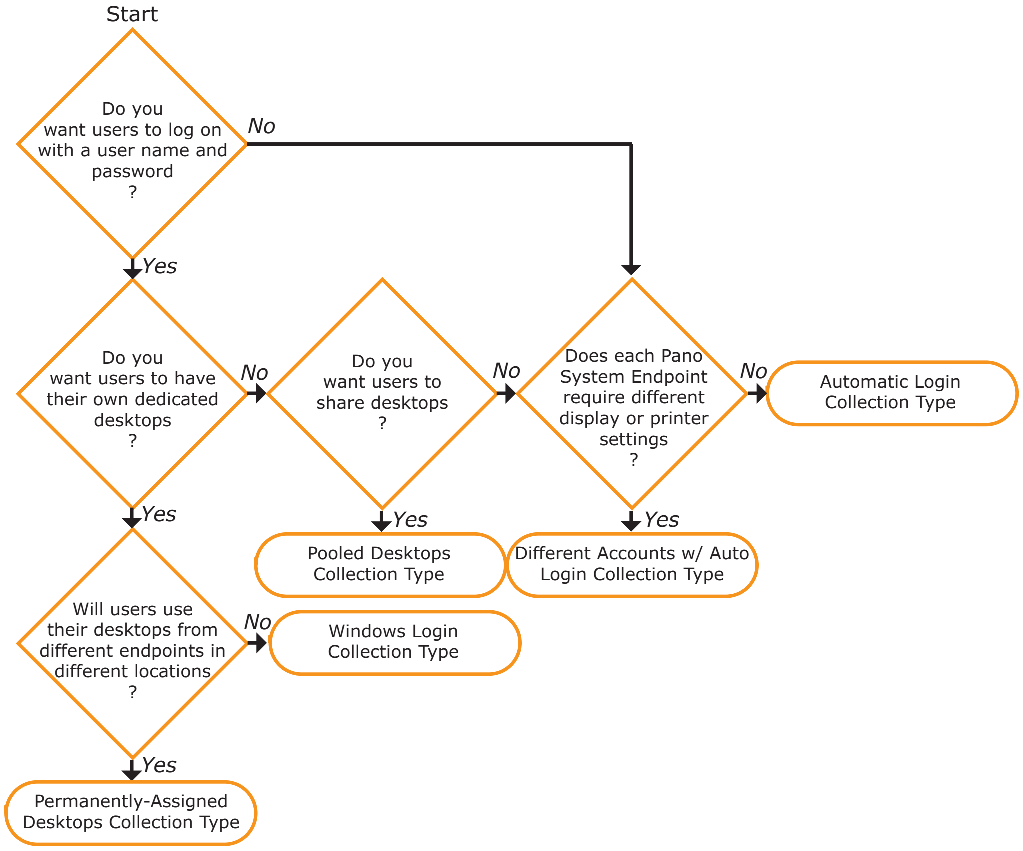
Whether primary, secondary, or auxiliary, each Pano Controller has its own administrative IP address, and this address is used to administer that Pano Controller.

There is also a virtual IP address, and only the active Pano Controller uses it. The virtual IP address is the IP address that clients use to access the active Pano Controller. When a Pano Controller becomes active, it takes ownership of the virtual IP address.

Next: Deciding on a Pano Controller Group Configuration

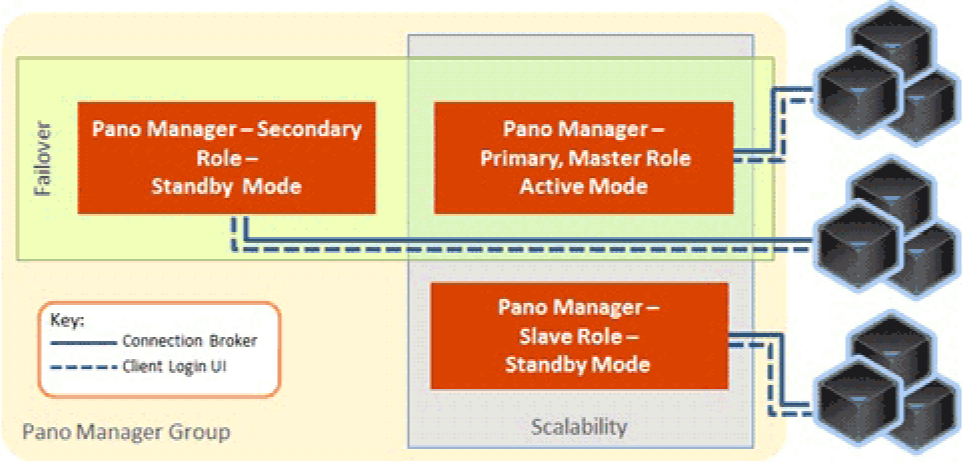
Deciding on a Pano Controller Group Configuration

Use the following diagram to identify the configuration that best meets your needs.


Start
Do you want users to log on with a user name and password ?
No
Yes
Do you want users to have their own dedicated desktops ?
No
Do you want users to share desktops ?
No
Does each Pano System Endpoint require different display or printer settings ?
No
Automatic Login Collection Type
Yes
Yes
Yes
Pooled Desktops Collection Type
Different Accounts w/ Auto Login Collection Type
Will users use their desktops from different endpoints in different locations ?
No
Windows Login Collection Type
Yes
Permanently-Assigned Desktops Collection Type

For example, if you want to deploy 1,000 DVMs, a group of two Pano Controller instances need to be installed on two different physical servers and configured as primary (active) and secondary (passive), and a third Pano Controller instance would also be added and configured as an auxiliary node. See Supported Number of DVMs and Pano Zero Clients for information.

In this configuration, all three instances of Pano Controller belong to the same Pano Controller group; connection brokering logic is made highly available by implementing an active/passive, two-node failover pairing using the two Pano Controller instances. Pano Controller also displays login screens via the Pano System Endpoints to the users. In this configuration, Pano login screens are active across up to three Pano Controller nodes. For Citrix XenDesktop deployments, to complement this multiplication of Pano Controller resources, an equivalent increase in XenDesktop instances, along with a load-balancing front-end, is required See About Load Balancing XenDesktop Controllers for information.


Failover
Pano Manager – Secondary Role – Standby Mode
Pano Manager – Primary, Master Role Active Mode
Pano Manager – Slave Role – Standby Mode
Key:
Connection Broker
Client Login UI
Pano Manager Group
Scalability

Next: Set Up and Manage Redundancy

Related Topics

IP Addresses and the Virtual IP Address

Set Up and Manage Redundancy

You should set up redundancy before configuring for scalability.

- Set up Failover Configuration
- Configure Email Notifications
- Disable Email Notifications
- Determine Status of a Failover Configuration
- Recovering from a Degraded or Inactive Configuration
- Switch Active Modes
- Convert Secondary to Primary
- Remove Failover Configuration

Create Pano Controller Group

Pano Controller groups let you configure redundancy and set up Pano Controllers to share the load of managing Pano System Endpoints. A Pano Controller group consists of a primary Pano Controller, a secondary Pano Controller, and up to four auxiliary Pano Controllers. All Pano Controller group members are configured with the same group name and password.

Pano Logic recommends that you set reservations for both CPU and memory to ensure that the Pano Controller VM always has a minimum amount of resources available. For more information, go to System Requirements.

To create a Pano Controller group:

- If your Pano Controllers are not all connected through the same switch, ensure that each switch has multicast enabled. Many switches have multicast enabled by default. The group communicates using TCP multicast. For details on the multicast addressing, go to Pano Controller Network Port Usage.
- For every member in your configuration, other than the primary, import a new Pano Controller virtual appliance. Configure the virtual machine's networking, but don't configure anything in the Pano Controller console.
- Ensure the virtual IP address and the IP addresses for all the Pano Controllers in the group are on the same subnet.

1. Log on to all the Pano Controllers that you intend to add to the group, and ensure that each member is running the same Pano Controller version.
2. For each member, click on the **Setup** tab. In the Group Configuration area, do the following:
   a. Type a **Name**. The group name must be the same on all members.
   b. Type a **Password** for the group. A password protects unauthorized users from adding members to the group, and this security is particularly important in a failover configuration. The password must be the same on all members.

      Each group member with a matching name and password is displayed in the Group Members table. Group status reflects the aggregate group member status.
   c. Click **Configure** to add the members.
3. Confirm that the newly added Pano Controllers appear in the Group Members table and have the correct status.

Troubleshooting: Go to Troubleshooting Group Membership Problems.

Next: Set up Failover Configuration

Set up Failover Configuration

Whether you migrate from a standalone configuration to a failover configuration or install a failover configuration from scratch–the process is the same: deploy one Pano Controller, then configure another Pano Controller for failover.

This procedure assumes the following:

- You already have already installed and configured an existing Pano Controller. This Pano Controller will be your primary and will become active.
- You want a scalable and redundant Pano Controller group.

To set up a failover configuration:

1. (Important!) As a best practice, back up your primary Pano Controller.

   You must make a backup even if the Pano Controller is a newly imported server with no collection or client data. This protection ensures that you can restore Pano Controller in the event of an unforeseen failure.
2. Prepare to configure:
   a. Reserve two static IP addresses: one for the secondary and one for the virtual IP address. Later you will configure the primary with the virtual IP address.

b. For every member in your configuration, other than the primary, import a Pano Controller virtual appliance. Configure the virtual machine's networking, but don't configure anything in the Management User Interface (MUI).

   After you configure for failover, the secondary automatically receives its Directory Configuration and Virtualization Configuration from the primary.

c. Set up the group, adding all required members to this group. Go to Create Pano Controller Group. A group is required before you can configure a failover configuration. Your primary Pano Controller and secondary Pano Controller must be members of this group. Later you will choose your secondary Pano Controller from the list of group members.

3. Set up the failover configuration:

   a. Log on to the primary Pano Controller.

   b. Go to Setup tab > Failover Configuration area.

   c. Click the **Edit** button.

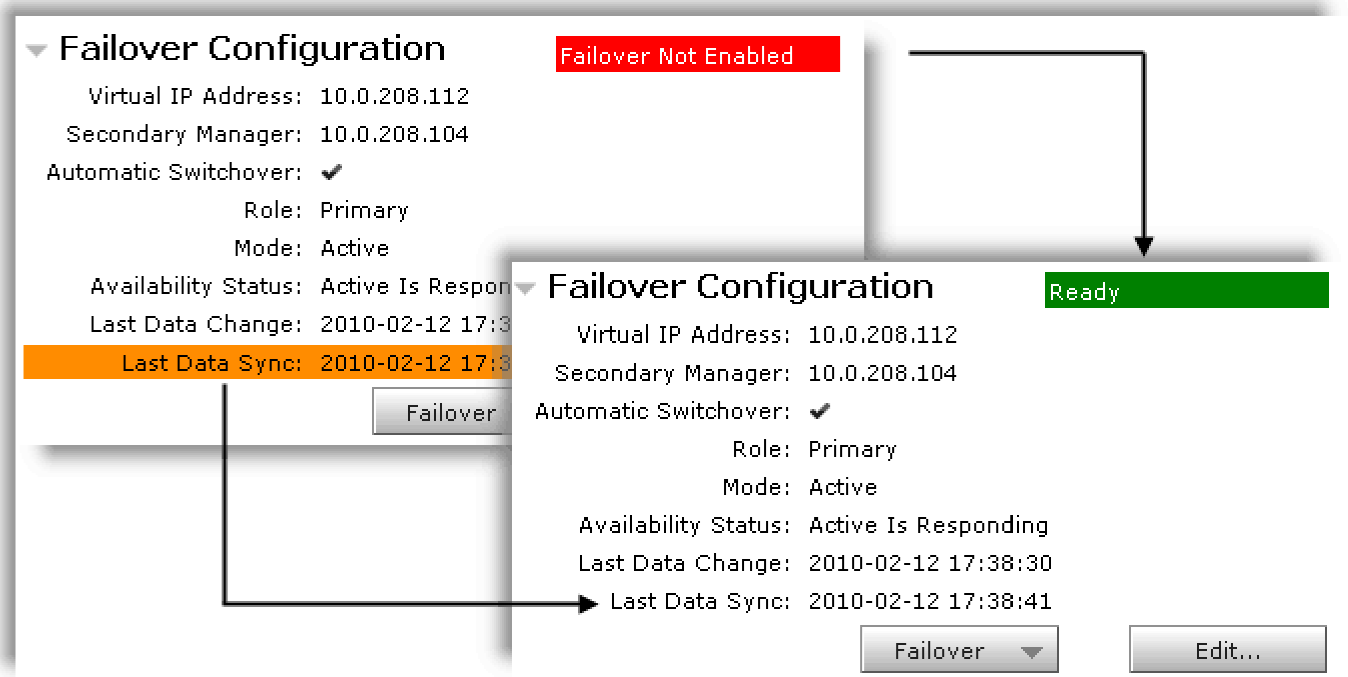
   d. Select the **Enable Automatic Switchover** check box.

   e. In the Secondary field, select the IP address of the secondary Pano Controller from the list of group members.

   f. In the Virtual IP Address field, type the virtual IP address that you reserved in Step a.

   g. Click **OK**.

   h. Wait for the Pano Controllers to synchronize.



Failover Configuration

Failover Not Enabled

Virtual IP Address: 10.0.208.112
Secondary Manager: 10.0.208.104
Automatic Switchover: ✓
Role: Primary
Mode: Active
Availability Status: Active Is Respon
Last Data Change: 2010-02-12 17:3
Last Data Sync: 2010-02-12 17:3

Failover Configuration

Ready

Virtual IP Address: 10.0.208.112
Secondary Manager: 10.0.208.104
Automatic Switchover: ✓
Role: Primary
Mode: Active
Availability Status: Active Is Responding
Last Data Change: 2010-02-12 17:38:30
Last Data Sync: 2010-02-12 17:38:41

4. If you are using the DHCP Method, change the IP address that you added to the vendor class when you configured discovery. The IP address must be the virtual IP address.

   Any previously-discovered Pano System Endpoints and any newly discovered Pano System Endpoint should have no problems communicating with the Pano Controller.

Next: Configure Email Notifications

Configure Email Notifications

Email notifications enable recipients to learn about fault events as soon as they occur. With email notifications you can learn about a failover before your end users, then take corrective action.

To configure email notifications:

Email notification must be configured on the primary.

1. Log on to the primary Pano Controller.
2. Go to Setup tab > Failover Configuration area.
3. In the Failover drop-down button, choose **Configure Email Notifications**.
4. In the SMTP Account for Sending, provide values for the following:
   - **Host**. The name of the mail server.
   - **User Name**. Any username that can authenticate with the mail server. Basically, anyone in your company with a company email account.
   - **Password**. The password for the user account that you specified.
   - **From**. The name ("alias") that you'd like to appear in the from field of the email.
   - (Optional) **Use TLS**. An encryption protocol. TLS replaces SSL.
5. In the **Recipients:** text box, provide a space-separated list of email addresses for the users that you want to receive email notifications.
6. Click OK. The Pano System sends a confirmation email to all recipients.

Next: Disable Email Notifications

Related Topics

Determine Status of a Failover Configuration

Disable Email Notifications

If you intend to perform maintenance on the Pano Controllers in your failover configuration, and you don't want recipients to be alarmed by any fault events, consider disabling email notifications temporarily.

To disable email notifications:

1. Log on to the primary Pano Controller.
2. Go to Setup tab > Failover Configuration area.
3. Select the **Remove Configuration:** check box, then click OK.

Related Topics

Configure Email Notifications

Determine Status of a Failover Configuration

The Pano Controller provides messages to help you understand the state of your failover configuration. Use the following table to determine if your configuration is in a degraded state, and what to do about it.

- **Configuration State** - The color-coded header message that appears in the Failover Configuration area. This message helps you determine the overall health of the failover configuration.

Config on *Pri*	**State on *Sec.***	**Mode on *Pri.***	**Mode on *Sec.***	**What's this mean?**	**What do I do?**
Ready	Ready	Active	Stand-by	The secondary is ready to become active in the event that the secondary detects that the primary is not responding.	There's no need to worry: failover is working as expected.
Failover Not Enabled	Failover Not Enabled	Active	Stand-by	Failover is not enabled. This state is normal and expected–if you do not have the Enable Automatic Switchover check box selected.	If you're of the users who prefer manual switchover to automatic switchover, you don't need to do anything. If you want to enable automatic switchover, select the Enable Automatic Switchover check box as outlined in Set up Failover Configuration.
n/a	Sec. Active	Down	Active	Failover worked. The secondary is servicing client requests. A failover occurred, subsequent to the secondary detecting that the primary is not responding. When the primary comes up, it will be in standby mode, and this state is a single point of failure.	Go to Recovering from a Degraded or Inactive Configuration
Sec. Un-reachable	n/a	Active	Down	The primary detected that the secondary is not responding.	Fix the secondary.
Fault Detected	n/a	Stand-by	Down	Urgent: there is no active Pano Controller to service requests. The secondary stopped responding, subsequent to a failover that had resulted in the secondary being active.	Go to Recovering from a Degraded or Inactive Configuration.
n/a	Fault Detect	Down	Stand-by	Urgent: there is no active Pano Controller to service requests. The primary stopped responding while the secondary was unable to become active due to the Automatic Switchover being disabled.	Automatic switchover prevents such a state. However, if you're of the small subset of users that prefers manual switchover as opposed to automatic switchover, you probably anticipated this scenario. Go to Recovering from a Degraded or Inactive Configuration.
Primary Not Active	Sec. Active	Stand-by	Active	The primary is in standby mode, and this state is a single point of failure. One of two things occurred: Secondary detected that the primary was not responding; later, the primary came online. Administrator triggered a switchover (see Switch Active Modes), causing the secondary to become active; therefore, the primary went into standby mode.	Go to Recovering from a Degraded or Inactive Configuration.

- **Availability Status** - The text message that appears in the **Availability Status:** field of the Failover Configuration area. This message determines if the Pano Controllers are up and able to communicate.

Availability Status On *Primary*	On *Secondary*	What's this mean?
Active Is Responding	n/a	The primary is active and the secondary is down ("Unreachable").
Active Is Responding	Active Is Responding	The primary is active and the secondary is standby. The two Pano Controllers can communicate with each other.
n/a	Active Is Responding	The secondary is active and the primary is down.

Recovering from a Degraded or Inactive Configuration

A degraded state means the primary has failed but the secondary is still running. The system does not support 'failing over' back from the secondary to the primary, so you must repair or replace the primary as soon as possible. You have two choices:

- Repair the primary immediately, then switch modes; or
- Replace the primary immediately with a new Pano Controller that only has the group configured, then convert the secondary to a primary.

An inactive state means all Pano Controllers are down and there is no active Pano Controller to service requests. Therefore, you must fix one of the Pano Controllers. You have two choices:

- Fix the active, then convert the secondary to a primary if applicable.
- Fix the standby, bring it up, and switch modes. Then, convert the secondary to a primary if applicable.

Switch Active Modes

You might need to switch active modes if:

- **You repaired a primary Pano Controller**. After you repair or replace a primary Pano Controller that is in standby mode, switch it to active. Afterward, the secondary becomes the standby.
- **You want to perform a manual switchover**. If you're of the small subset of users that prefers manual switchover as opposed to automatic switchover, you must manually switch over in the event of a failure.

To swap modes:

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Failover Configuration** section, click the **Failover** drop-down button and choose **Switch Active Modes**.

Related Topics

Convert Secondary to Primary

Convert Secondary to Primary

A failover can only take place from an active primary to a standby secondary. An active secondary cannot fail over to a standby primary. Therefore, if you get in a state where the secondary is active and the primary is down, convert the secondary to a primary.

If you intend to upgrade a primary, switch modes so that the secondary becomes active, then convert the secondary to a primary. You can reverse these steps when the upgrade completes.

To convert a secondary to a primary:

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Failover Configuration** section, click the **Failover** drop-down button and choose **Become Primary**.

Related Topics

Switch Active Modes

Remove Failover Configuration

A failover configuration inherently requires more administration than a standalone system. For example, upgrades are more time consuming in a failover configuration. If your company's needs change and you no longer need redundancy, you can easily remove your failover configuration. No downtime is required to migrate from a failover configuration to a standalone Pano Controller.

To remove a failover configuration:

1. Log on to the Pano Controller.
2. Click on the **Setup** tab.
3. In the **Failover Configuration** section, click the **Failover** drop-down button and choose **Remove Failover Configuration**.
4. (Important!) On the Standby Secondary Pano Controller, do one of the following to fix its state:
   - Restore its database from a previous backup. Go to Restore from Backups. Afterward, you can reuse this Pano Controller in any configuration.
   - Delete the virtual appliance. Start from scratch if you'd like to create a failover configuration (or scalable configuration) in the future.
5. If you're using the DHCP Method, change the IP address in the vendor class. This IP address must be the administrative IP address, not the virtual IP address.

Identifying the Primary Pano Controller

When you need to manage or configure DVMs, do so from the primary Pano Controller. Secondary controllers can only manage Pano user login screens.

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

To identify the primary Pano Controller:

1. Log on to one of the Pano Controllers.
2. Click the **DVM Collections** tab.
   - If your collections appear in the list, then this is the primary Pano Controller.
   - If your collections do not appear in the list, then this is a secondary Pano Controller.

Related Topics

Configure Pano Controller Groups

Managing Scalability

- Add an Auxiliary Controller to a Group
- Remove an Auxiliary Controller from a Group

Add an Auxiliary Controller to a Group

Depending on your redundancy and scalability requirements, you may install and configure one or more auxiliary Pano Controller instances. See Pano Controller Deployment Options Decision Tree for help determining whether you require auxiliary Pano Controller instances.

Before you install and configure an auxiliary Pano Controller, make sure that your primary and secondary Pano Controllers are fully configured as described in Set Up and Manage Redundancy.

When you configure an auxiliary Pano Controller instance, you will add your new controller to the same group to which you your primary and secondary Pano Controllers belong. Your primary controller acts as the master of the group, with the secondary taking over in case the primary controller becomes unresponsive. Auxiliary controllers handle requests from the active master and allow the system to scale out.

The basic workflow you will follow is:

1. Snapshot your existing primary Pano Controller virtual appliance
2. Create a new, auxiliary Pano Controller
3. Add your auxiliary Pano Controller to the existing group

To add scalability to your Pano Controller group:

1. Important! Snapshot your primary Pano Controller virtual machine.

   While not strictly necessary, it is good practice to have a recent snapshot or backup of your primary Pano Controller whenever you add new controllers.
2. Import a new Pano Controller virtual appliance
   - **a.** Make sure the version is the same as the primary Pano Controller
   - **b.** Configure the passwords and IP address for the new virtual appliance
3. Using a browser, sign into the Pano Controller console for the new controller and navigate to the Setup tab

4. Select the same options for Appliance Role as you have for your primary Pano Controller Add the secondary controller to the group
   a. Expand the Group Configuration section
   b. Enter the same name and password as you did for the primary Pano Controller
   c. Click the Configure button
   d. You should see at least three members in the Group Members list. Make sure that you see one entry for each Pano Controller that is part of your group.
5. .Log out of the auxiliary Pano Controller console
6. Review Group Member and Failover Status from the primary Pano Controller
   a. Using a browser, sign into the Pano Controller console for the primary controller
   b. Navigate to the Setup tab
   c. Expand the Group Configuration section
   d. Verify that each member of the group appears in the list and that the status for each is OK
   e. Expand the Failover Configuration section
   f. Verify that Failover Configuration indicates Ready
   g. Verify that Role is "Primary" and Mode is "Active"

Remove an Auxiliary Controller from a Group

To remove an auxiliary controller from a group, in the Pano Controller on the auxiliary node, in the Group Configuration section select the auxiliary controller and click the Remove button.

Repeat this procedure on the group's primary Pano Controller.

Set up a Load Balancing Configuration

This procedure assumes:

- You want load balancing (see Install Pano Controller VM on ESX/ESXi). If you want both load balancing *and* failover, go to Set up Failover Configuration.
- You already have an existing Pano Controller. This Pano Controller is your *master*. In this procedure you will add a *slave* to your configuration. For example, if you want to deploy 1,000 DVMs, you need two Pano Controllers: a master and a slave, each servicing approximately 500 client UIs.

To set up load balancing:

1. As a best practice, back up your master Pano Controller.
2. Reserve a static IP address for the slave.
3. For every member in your configuration, other than the master, import a Pano Controller virtual appliance. Configure the virtual machine's networking, but don't configure anything in the Pano Controller administrator interface.

Set up the group, adding all required members to this group.

Next: Monitor Load Balancing Across a Group

Monitor Load Balancing Across a Group

The active Pano Controller maintains the list of all members and their logins..

To monitor Pano Controller Group members' load:

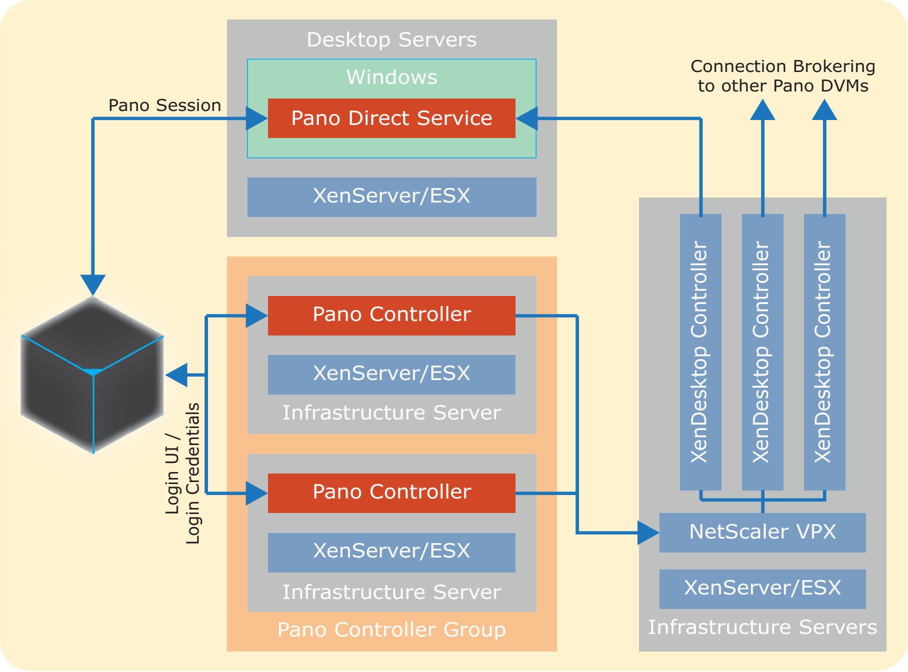
1. Log on to the primary Pano Controller.
2. Click the **Setup** tab.
3. In the Group Configuration section, observe the number in the **Login Screens** column for each member. This number represents the number of client UI login processes that the member is managing.

About Load Balancing XenDesktop Controllers

Pano Controller communicates with XenDesktop via the XML Service that is part of the XenDesktop Controller. In order to provide the redundancy and scale you require, large Pano deployments on XenDesktop need to use multiple instances of the XenDesktop Controller. The XenDesktop Controller connection broker is connected to Pano Controller via a single API and must be capable of servicing the required number of broker requests during user logins.

If you have a very large and active deployment, the number of connection broker requests might overload a single XenDesktop Controller instance, thereby resulting in unacceptable response times and a degraded user experience.

The exact number of users that can be supported by each XenDesktop Controller instance will be dependent on the server hardware used to host the Controllers and the acceptable delays during the login and connection brokering process. These delays only apply up to the point where the user is directly connected to a Pano DVM. Once the user session reaches that point (documented in Connect Pano Controller to XenDesktop Controller), the XenDesktop Controller is no longer involved. The diagram below illustrates load balancing on XenDesktop using Citrix NetScaler.



Running the XenDesktop Controllers as virtual machines on a shared server that is also supporting other infrastructure components – such as Pano Controller or a provisioning tool – will also lower the number of concurrent client logins it can support. To optimize scalability, you can dedicate a physical server to run just one or two XenDesktop Controller instances.

The use of multiple XenDesktop Controller instances is supported with Pano, but some form of load balancer is needed to provide a single interface to which Pano Controller can connect. Citrix NetScaler is recommended as a load balancer to connect a single Pano Controller instance (or group) to multiple Controller instances. Citrix NetScaler can load balance requests to multiple XenDesktop Controller instances installed on the same physical server. But to improve availability in the event of a server failure, as well as to minimize the number of required Citrix NetScaler instances, it is also possible to locate them on physically separate servers.

Citrix NetScaler is available as either a VPX virtual appliance or as an MPX hardware appliance with preinstalled software. Licensing costs are based on the number of Citrix NetScaler servers and bandwidth tiers. The amount of traffic in the form of XML API calls that passes from Pano Controller to the XenDesktop Controller instances is fairly small, making it practical to license Citrix NetScaler in its lowest bandwidth tier to reduce costs. See Connect Pano Controller to XenDesktop Controller for information on connecting Pano Controller to multiple XenDesktop Controllers behind a network load balancer, such as Citrix NetScaler.

Related Topics

Can I use a non-Citrix load balancer?

Can I have multiple instances of Citrix NetScaler?

Connect Pano Controller to XenDesktop Controller

22 Deploy Pano Maestro

After you set up and configure Pano Controller, you can use Pano Maestro for centralized Pano Controller group management.

Pano Maestro is web-based central management console that serves as a centralized access point to manage multiple groups of Pano Controllers. Pano Controller groups are used to scale the management of Pano System Endpoints.

Installing the Pano Maestro Virtual Machine

Pano Maestro is delivered in the same virtual appliance packaging that is used for Pano Controller. After downloading the PanoAppliance.zip file from the Pano Logic download site, expand the zip file and import the appliance into the virtualization stack.

Note: Pano Maestro supports the same virtualization platforms as Pano Controller. As Pano Maestro is packaged in the same appliance as Pano Controller, the same versions and rules apply.

To set up Pano Maestro:

1. Create and prepare the virtual machine. The minimum requirements are 1 vCPU and 1 GB of RAM. After importing and powering on the VM, Pano Maestro can be configured by selecting option 2 (Pano Maestro) from the console window of the VM.
2. Configure Pano Maestro using the web management UI.

   Log into Pano Maestro using a web browser pointing to:
   http://<IP Address> or <Pano Maestro virtual machine hostname>/

   Pano Maestro Summary displays the configured Pano Controller groups and their status. You can now add, edit and remove Pano Controller groups.

   To sort groups, click the **Group Name** heading and select the sort order from the drop-down list.

Pano Maestro provides the following centralized management options:

- Set up system administration access
- Configure directory services
- Back up and restore Pano Maestro configurations
- Manage licenses and usage
- Upgrade Pano VM appliance
- Set up Secure HTTPS Connection for Pano Maestro Web Access

Related Topics

Adding a Pano Controller Group

Editing a Pano Controller Group

Removing a Pano Controller Group

Adding a Pano Controller Group

Up to five Pano Controller groups can be added. When adding a Pano Controller Group, the Virtual IP of the group must be used instead of using the IP Address or Hostname of the active Pano Controller. Without this, Pano Maestro cannot communicate with the group in the event the Primary Controller fails over to the standby Controller.

Because license configuration is hosted on Pano Maestro, the user account (either PAM or LDAP) used for Pano Controller and Administrative roles must be configured on Pano Maestro and specified along with the Pano Controller group name when adding the Pano Controller group. Directory Services on Pano Maestro and Pano Controllers must have the same Directory Services (AD) configuration (i.e., point to same AD server)

1. In the Pano Maestro Console, click the **Summary** tab and click the **Add** button.
2. In the **Add Group** dialog, specify the group settings.
   - Display Name
   - Active Pano Controller Virtual IP Address
   - User Name
   - Password
3. Click **Add.** Pano Controller summary and status are displayed.

Note: The active Controller must be reachable and available when added to the group.

Related Topics

Editing a Pano Controller Group

Removing a Pano Controller Group

Editing a Pano Controller Group

Pano Controller groups can be edited to modify the group information.

1. In the Pano Maestro Console, click the **Summary** tab and click the **Edit** button.
2. In the **Edit Group** dialog, modify the group settings.
   - Group Name
   - Primary Pano Controller
   - User Name

   - Password

3. Click **Okay**.

Related Topics

Adding a Pano Controller Group

Removing a Pano Controller Group

Removing a Pano Controller Group

1. In the Pano Maestro Console, click the **Summary** tab and select the group to be removed.
2. Click the **Remove** button.

   The Pano Controller group is removed from the list.

Related Topics

Adding a Pano Controller Group

Editing a Pano Controller Group

Configuring Directory Services

By default, Pano Maestro can be accessed using default built-in accounts “root” and “admin”, which are set when importing the virtual machine. To provide seamless single sign-on with Pano Controllers, Pano Maestro requires setting up Director Services integration and configuring Administrative accounts.

Note: Without Directory Services integration, Pano Maestro and Pano Controllers need to be set up with same passwords for default built-in accounts.

Directory Services can be configured by going to **Setup -> Directory Services** and providing URL for Active Directory or LDAP server information.

1. In the Pano Maestro Console, click the **Setup** tab and select **Directory Services**.
2. In the **URL** field, type your network's domain name (for example, acme.com) or LDAP server URL.

   Only one domain name can be specified.

   One or more space-separated LDAP server URLs can be specified.

   The following characters do not need to be escaped (preceded by a backslash) in the LDAP server URL: ‘%’, ‘a-z’, ‘A-Z’, ‘0-9’, ‘~’, ‘!’, ‘@’, ‘$’, ‘^’, ‘&’, ‘*’, ‘(‘, ‘)’, ‘|’, ‘:’, ‘?’, ‘”, ‘-’, ‘.’, ‘/’.

   If using a distinguished name (DN), the ‘#’ character does not need to be escaped if it is within the name. It does need to be escaped (\#) if it is at the beginning of the name.

   The following characters need to be escaped: ‘+’, ‘”’, ‘<‘, ‘>’, ‘=’, ‘\’, ‘;’, ‘,’.
3. Type the User Principal Name (UPN) and password of the account that you are using to connect to the directory service.
   - The account needs to have read access to all portions of the directory used to authenticate users of the DVMs.
   - When using AD you must use the full User Principal Name (UPN). The UPN is an internet-style login name for the user (for example, readonly@acme.com).

4. Click **Configure**. Pano Controller locates the directory service for your domain.

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

Troubleshooting: If this procedure didn't work for you, you might need to use the fully-qualified name of your directory server. If that doesn't work, go to Troubleshoot Authentication and Directory Service Problems. Once Directory Services are configured successfully, administrative roles can be added.

Related Topics

Selecting Pano Maestro Administrators

Managing Pano Maestro Administrators

Once Directory Services are configured successfully, administrative roles can be added. Pano Maestro lets administrators set up and control different levels of Pano Maestro use. Administrators can be configured for **Full Access** or **Read Only** access.

1. In the Pano Maestro Console, click the **Setup** tab and select **Administrators**.
2. Click the **Configure** button next to the desired level of access. The Assign Users dialog appears for the selected access level.
3. Add and Remove users. Users can be selected by browsing the network or searching by username.
4. Click **Okay**.

Related Topics

Using the Directory Browser

Selecting Pano Maestro Administrators

Administrators can be selected by browsing directories or searching by username.

1. In the Assign Users dialog, select the desired user(s) and click **Add** and **Remove** to update the Selected Users list.
2. Click **Okay** to assign the selected users.

Related Topics

Managing Pano Maestro Administrators

Using the Directory Browser

Using the Directory Browser

Administrators can be selected by browsing network directories or searching by username.

1. In the Directory Hierarchy dialog, navigate the directory tree to locate the desired user.
2. Click **Okay** to add the selected user.

Related Topics

Adding a Pano Controller Group

Backup and Restore Pano Maestro Configurations

Administrators can back up configuration data manually for Pano Maestro configuration protection and storage in event of a problem.

1. Click **Backup**.

   The current configuration file is backed up to a configuration data file (for example, `PanoMaestro-Backup-Year-Month-Day-HR-Min-Sec-Ms.zip`).

To restore a Pano Maestro configuration:

1. Click **Restore**.

   The Import Pano Maestro DB dialog appears.
2. Browse to the desired backup file.
3. Click **OK** to import the selected file.

Related Topics

Upgrade Pano Maestro

Manage Pano Maestro System Licenses and Usage

Administrators can manage Pano licenses for all Pano Controller groups from the centralized Pano Maestro Console. After a Pano Controller group is added to Pano Maestro, the License Configuration on the Pano Controller group points itself to Pano Maestro for license service.

License key importing is done from under **Setup -> Licenses and Usage**. To activate the Pano System license key, import the Pano System license file.

1. Click **License and Usage**.

   The License and Usage dialog appears and displays current licence properties.
2. Click the **Browse** button to locate the license file.
3. Click the Import button to import and activate the license.

   Verify the license properties to ensure compliance.

Related Topics

Licensing in Pano System 6.0

Upgrade Pano Maestro

Administrators can upgrade Pano Maestro.

1. In the Upgrade screen, click the **Browse** button to navigate to the new software upgrade file.
2. Click **Upgrade**.

The current software is upgraded. The Pano Maestro appliance needs to be restarted to activate the software update.

Related Topics

Backup and Restore Pano Maestro Configurations

Set Up HTTPS Connection for Pano Maestro Web Access

By default, the Pano Maestro uses a self-signed certificate for secure communication over HTTP using SSL (HTTPS).This certificate is installed when you import the VM. You can replace this with a more secure solution—a certificate from a Certificate Authority.

Note: You should replace the default self-signed certificate with your CA certificate to provide a more secure solution.

Pano Maestro supports public keys that use either p12 or pfx file format. When you install the Pano Maestro, the Pano Maestro installer prompts you to upload your own certificate. However, if you do not have your own certificate, you can apply your certificate later.

Note: You don't need to upload your certificate each time you upgrade. The Pano Maestro installer preserves this information during an upgrade.

To upload your certificate from the Pano Maestro:

1. In the Upgrade screen, either use the default certificate or click the **Browse** button to navigate to the SSL certificate file.
2. Enter the password.
3. Click **Configure**.

   The current software is upgraded. The Pano Maestro appliance needs to be restarted to activate the software update.

   Pano Controller can now be accessed via HTTPS using your custom certificate. The Pano Controller continues to accept connections on the HTTP port (port 80) if it has not been disabled.

Related Topics

Installing the Pano Maestro Virtual Machine

23
Desktop Creation - Overview

Now that you have your core Pano system up and running, it's time to create the virtual machines that ordinary users will use. This involves creating a virtual machine and installing the version of Windows you want to run. More importantly, you will also install the Pano Direct Service (PDS), which is the interface between the OS and the user's endpoint.

GINA (Graphical Identification and Authentication, one of the components of interactive logon model on Windows) is optional, but if you want to use it, you should install PanoGINA first. Refer to Integrate Pano GINA.

Creating (and auto-provisioning) DVMs is essentially the same on all three virtual platforms, but there are some differences. These are described in the three platform-specific sections.

After you've created your desktop virtual machines, you will set up one of several brokering systems. These are the entities that map users to virtual machines.

Finally, refer to Verify DVMs & System Deployment to verify that the system is working.

The sequence for each of the three virtualization platforms is shown below. Before you begin, make sure 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.

1. Decide how many Windows XP and how many Windows 7 desktops you want to deploy.
2. Retrieve the OS installation media (disk) and Windows product license key.

Note: If you are going to use the WDDM driver, you must have the floppy driver enabled.

VMware	XenServer / Xen Desktop	Hyper-V
Create Desktop Virtual Machines in vSphere Client	Create Desktops with XenDesktop	Create DVMs in SCVMM
Install Windows	Not required	Install Windows
Set Hardware Acceleration		
Installing Pano Direct Service		
Verify DVM Connectivity		
VMware Disposable Desktops	Not required	Not required
Control Session Timeouts		
Disable Fast User Switching in Windows 7		
Disable Sleep and Hibernate in Windows 7		

VMware Options & Upgrade

VMware offers additional desktop configuration options:

- Create DVM Templates in vSphere
- Install Sysprep Tools on vCenter Server for Windows XP
- Create Guest Customization Specification
- Test vCenter Server DVM Deployment
- Upgrade of Pano Direct Service with View Agent
- Upgrade VMware Tools
- Upgrade VMware View Agent

VMware View Connection Server Integration

The Pano System offers a full virtual desktop solution which includes Pano System Endpoints, Pano Direct Service, plus the Pano Controller, which acts as a full-featured connection broker.

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

Steps for implementing and testing Pano-VMware View integration include:

- Integrate Pano System with VMware View
- Configure VMware View Agent
- Enable Desktop Connections from Pano Devices
- Connect Pano Controller To VMware View
- Create VMware View Collection
- Validate Pano Controller-VMware View Configuration

Hyper-V Options

Hyper-V lets you create DVM templates. Refer to Create DVM Templates in SCVMM for details. You can also Clone with Optional Guest OS Profile if desired.

What to do next: Set Up Desktop Brokering

24
Integrate Pano GINA

What's a GINA?

GINA is one of the components of interactive logon model on Windows. When you initially press Ctrl +Alt +Del on a Windows system, a logon screen appears. This module is called a GINA (Graphical Identification and Authentication). The interactive logon procedure is normally controlled by `Winlogon`, `MSGina.dll`, and network providers.

Microsoft provides a way to customize identification and authentication behavior by replacing `msgina.dll` with a customized GINA DLL. To do so, set the following registry key with the corresponding customized GINA dll. If this value is NOT present, Windows loads standard Windows GINA provider `msgina.dll`.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
CurrentVersion\Winlogon\GinaDLL
```

There are two ways you can customize GINA:

- **GINA filter and passthrough GINA**: Adds some additional capabilities to Windows, but it does not authenticate the user. You can have multiple GINA filters, as long as each GINA filter can chain to the next GINA filter. There are a number of GINA filters. Pano System also installs a GINA filter.
- **GINA authenticator**: Handles the user authentication, and it must be the last GINA called. Most people use one of two GINA authenticators–the Microsoft MSGINA.DLL or the Novell NWGINA.DLL.

Windows also allows multiple GINA providers to coexist. This is called *GINA chaining*. However, Microsoft does not have a standard for where to store the name of the next GINA in the chain. Most third-party chaining GINAs store the next GINA to chain in the registry. This means that if another third-party GINA is installed, they can potentially break the GINA chain.

This chapter on Windows GINA specifically refer to Windows XP.

Related Topics

About Pano GINA Provider and Registry Changes

Install Third Party GINA Applications

Upgrade or Uninstall Third Party GINA Applications

About Pano GINA Provider and Registry Changes

The Pano Direct Service contains a passthrough GINA–`PanoGINA.dll`. When you install Pano Direct Service, this GINA saves to the `\Windows\System32\` folder.

When a user logs on to via a Pano System Endpoint, the user credentials are taken from user and passed to `PanoGINA.dll`. `PanoGINA.dll` validates user info and passes the user credentials to either the standard GINA provider `msgina.dll` or the other GINA provider that is chained to Pano GINA.

The following registry key is set to the other GINA provider to which Pano GINA is chained:

```
HKLM\SOFTWARE\Pano Logic\PanoDirect\PanoGINA\NextGinaDLL
```

The Pano Direct Service installer makes appropriate registry changes to set up Pano GINA correctly, and chains any existing provider to Pano GINA during installation or upgrade. During uninstall, the Pano Direct Service installer removes Pano GINA from the chain if any.

Here are some examples of registry settings after installing Pano Direct Service. These settings could be different depending on your GINA provider.

Scenario	Registry	Points to...
When Pano Direct Service is installed on a DVM with no other GINA providers installed	`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL`	PanoGINA.dll
	`HKLM\SOFTWARE\Pano Logic\PanoDirect\PanoGINA\NextGinaDLL`	Not present or empty
When Pano Direct Service is installed on a DVM with VMware View Agent is already installed	`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL`	PanoGINA.dll
	`HKLM\SOFTWARE\Pano Logic\PanoDirect\PanoGINA\NextGinaDLL`	wsgina.dll. This is VMware GINA provider, and means that Pano GINA is chained to VMware GINA provider.
When VMware View Agent is installed on a DVM with Pano Direct Service already installed	`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL`	wsgina.dll
	`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VdmGinaChainDLL`	PanoGINA.dll
	`HKLM\SOFTWARE\Pano Logic\PanoDirect\PanoGINA\NextGinaDLL`	Not present or empty The VMware GINA provider is chained to PanoGINA.dll.

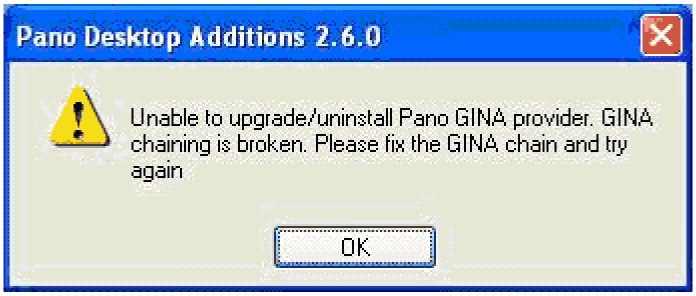
What's a GINA?

Install Third Party GINA Applications

Upgrade or Uninstall Third Party GINA Applications

Reestablish Broken GINA Chain

When you upgrade or uninstall Pano Direct Service, Pano Direct Service fails to upgrade or uninstall if it determines that the GINA chaining is broken. In this case, the installer returns the following error:



Pano Desktop Additions 2.6.0

Unable to upgrade/uninstall Pano GINA provider. GINA chaining is broken. Please fix the GINA chain and try again

A broken GINA chain can occur if other GINA providers are installed after you install Pano Direct Service and do not set up the GINA chain properly. The Pano Direct Service installer doesn’t allow you to uninstall or upgrade Pano Direct Service if there is a broken GINA chain. You must fix the chain.

To reestablish a broken GINA chain:

1. From a command line, run the `PanoDirectCfg` command. `PanoDirectCfg` contains the following options to reestablish GINA chain:

`PanoDirectCfg -ResetGina`	Sets GINA to standard Microsoft GINA provider, removing all other providers.
`PanoDirectCfg -ResetGinaToPano`	Sets GINA to Pano Logic GINA provider chained to Microsoft GINA provider, removing all other providers.

2. Now upgrade or uninstall Pano Direct Service.

Install Third Party GINA Applications

To ensure successful integration, your supported GINA application must be installed *first* before installing Pano Direct Service. This requirement exists whether you perform a “silent install” (refer to Enable Silent Installation for Windows XP) or a normal install using the Pano Direct Service installer. XyLoc Solo is the only exception to this rule. With XyLoc Solo, *Pano Direct Service* must be installed first.

This sequence is necessary because most of the supported GINA applications don't set up the GINA chain properly when other GINA providers are present; however, Pano Logic does support them.

To install Novell Client GINA application:

1. If you have Pano Direct Service installed, uninstall it.
2. Install Novell Client software.
3. Install Pano Direct Service.

To install SplitView GINA application:

1. If you have Pano Direct Service installed, uninstall it.
2. Install SplitView software.
3. Install Pano Direct Service.

To install VMware View Agent GINA application:

1. If you have Pano Direct Service installed, uninstall it.
2. Install VMware View Agent software.
3. Install Pano Direct Service.

To install Imprivata GINA application:

1. If you have Pano Direct Service installed, uninstall it.
2. Install Imprivata software.
3. Install Pano Direct Service.

To install XyLoc Solo GINA application:

Because XyLoc Solo requires a USB port in order to insert the XyLoc USB Lock, you must first install Pano Direct Service. Therefore, you cannot install XyLoc Solo using the vSphere Client or RDP.

1. (Important!) Install Pano Direct Service if it isn’t already installed.
2. From the Pano user login screen, log on to the DVM.
3. Install Xyloc Solo.
4. Run the Xyloc executable to install Xyloc software on to the DVM:
5. Insert the Xyloc Reader into the Pano System Endpoint’s USB port.
6. Turn on the Badge to register the key with the DVM.
7. Using XyLoc Solo logon window, log on to the DVM to verify that the GINA chain is working properly.

Related Topics

About Pano GINA Provider and Registry Changes

Upgrade or Uninstall Third Party GINA Applications

Upgrade or Uninstall Third Party GINA Applications

If you need to upgrade or uninstall a supported GINA application, you must *first* uninstall Pano Direct Service. This sequence is necessary because most of the supported GINA applications don't properly set up GINA chain when other GINA providers are present; however, Pano Logic does support them.

If this requirement is not acceptable or not practical in your environment, contact Pano Logic Technical Support for an existing alternative procedure.

If this requirement is not acceptable or not practical in your environment, use the following manual process:

To upgrade or uninstall a third party GINA if you can't uninstall Pano Direct Service first:

1. From the command line prompt, go to the Pano Direct Service bin folder:

   ```
   cd Program Files\Pano Logic\PanoDirect\Bin
   ```

2. Run the following command to remove Pano GINA from the GINA chain:

   ```
   PanoDirectCfg -RemoveGina
   ```

   Warning: After you upgrade or uninstall the application, do not restart–even if Windows asks you to restart.

3. Upgrade or uninstall the GINA application. Do not restart.
4. Run the following command:

   ```
   PanoDirectCfg -SetGinaChain
   ```

5. Reboot the GINA application.

Related Topics

Install Third Party GINA Applications

Fix Windows GINA State

Reestablish Broken GINA Chain

Fix Windows GINA State

Sometimes after installing, updating, or uninstalling either Pano Direct Service or third-party GINA applications, Windows doesn't allow a user to log on to Windows, displaying the following error message on the DVM's console:

```
The Logon User interface DLL "XXXXX.dll" failed to load. Contact your system
administrator to replace the DLL, or restore the original DLL
```

This error message means that Windows GINA configuration is in a bad state. The possible causes are:

- Improper installation of Pano Direct Service.
- Improper installation of third-party GINA applications.
- Installation of unsupported third-party GINA applications on top Pano Direct Service.

To restore a DVM to a normal state:

1. From vCenter Server, right-click on the DVM, then click **Open Console**. You are prompted to log on.
2. Log on to the DVM.
3. Reboot/reset the DVM, and press **F8** before the Windows boot options screen appears.
4. From the Windows boot options screen, choose safe mode, then press **Enter** to boot Windows into safe mode.
5. Log on to Windows using local administrator account.
6. Open Windows Registry editor (RegEdit) from command line.
7. Go to `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\` and delete the value with name `GinaDLL`.
8. Reboot the DVM. Windows now presents you with a normal login prompt.
9. Log on to the DVM as administrator, then do the following:
   a. Remove any third-party applications that are installed.
   b. Remove Pano Direct Service.
   c. Reboot the DVM again.

Related Topics

Install Third Party GINA Applications

Reestablish Broken GINA Chain

25

Creating Desktops: vSPhere, XenDesktop, SCVMM

This chapter includes the following topics:

Desktop creation often involves installation of the WDDM driver. We’ve created a short video to help explain how to do this: Upgrading Display Drivers from XPDM to WDDM

Create Desktop Virtual Machines in vSphere Client

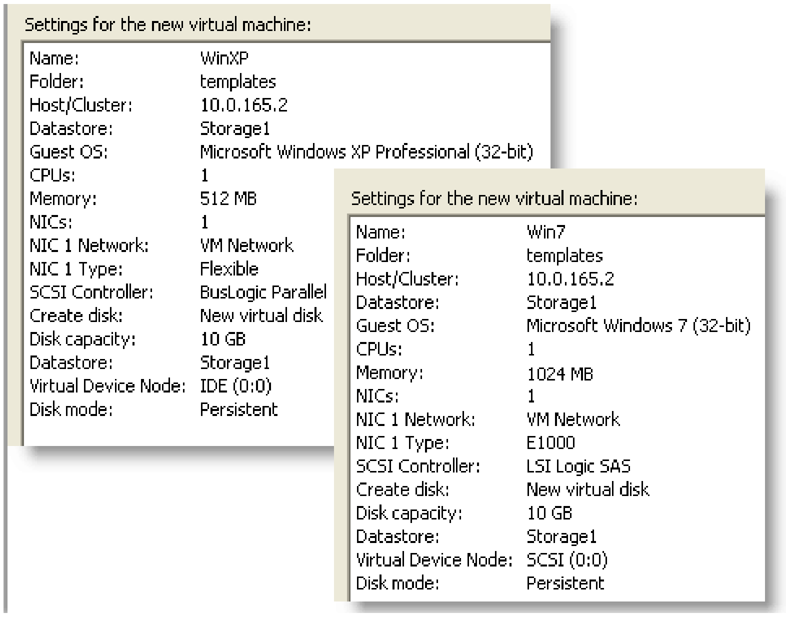
Create the virtual machines. Pano Logic recommends that you create the virtual machines from scratch using the vSphere Client. This approach is outlined below.

Caution: Pano Logic does not recommend that you create the virtual machines by converting a physical machine to a virtual machine (P2V), using either the standalone version of VMware Converter or the version integrated with vCenter Server. VMware Converter images the target PC and migrates it into vSphere. This method is not recommended for production because this method doesn’t result in an optimal virtual machine. 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 possible operating system faults.

To create a desktop virtual machine from scratch:

1. Connect to vCenter Server.
2. Launch the New Virtual Machine Wizard (**File** > **New** > **Virtual Machine...**), then select **Custom** as the baseline settings for the virtual machine.

3. Use the wizard to create the initial virtual machine, specifying values as follows:



Settings for the new virtual machine:

Name:	WinXP
Folder:	templates
Host/Cluster:	10.0.165.2
Datastore:	Storage1
Guest OS:	Microsoft Windows XP Professional (32-bit)
CPUs:	1
Memory:	512 MB
NICs:	1
NIC 1 Network:	VM Network
NIC 1 Type:	Flexible
SCSI Controller:	BusLogic Parallel
Create disk:	New virtual disk
Disk capacity:	10 GB
Datastore:	Storage1
Virtual Device Node:	IDE (0:0)
Disk mode:	Persistent

Settings for the new virtual machine:

Name:	Win7
Folder:	templates
Host/Cluster:	10.0.165.2
Datastore:	Storage1
Guest OS:	Microsoft Windows 7 (32-bit)
CPUs:	1
Memory:	1024 MB
NICs:	1
NIC 1 Network:	VM Network
NIC 1 Type:	E1000
SCSI Controller:	LSI Logic SAS
Create disk:	New virtual disk
Disk capacity:	10 GB
Datastore:	Storage1
Virtual Device Node:	SCSI (0:0)
Disk mode:	Persistent

Parameter	Description
Name and Location	A descriptive and unique name for your virtual machine template (for example, `xptemplate` or, if this is a template specific to a department, `Marketing`). 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 host 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 intend to install on the virtual machine. It's best practice that the template name include the name of the operating system (for example, `win7template` or `xptemplate`).
CPUs	The number of virtual processors (virtual CPUs) that will be presented to the virtual machine. A single processor is sufficient for most of your users.
Memory	The amount to allocate to each virtual machine that you create from the template. **Windows XP** - 768 MB is enough for most users running typical Microsoft Office applications. Where your users are running memory intensive applications, allocate 1 GB. **Windows 7** - 2GB
Network	The number of virtual network adapters that the virtual machine needs to use. Most virtual desktops need only one network adapter. Accept the default network adapter (`Flexible` or `E1000`). Do not choose `vmxnet`, the higher performance network adapter. Change the network adapter later, as outlined in Change Network Adapter Type.
SCSI Controllers	Windows XP - Choose BusLogic. These drivers come pre-installed with Windows XP and are sufficient for Pano System users. Windows 7 - Choose LSI Logic. (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**.

Parameter	Description
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. There's no need to specify a Mode.

Tip: 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. After creating the virtual machine, make sure it resides in a folder by itself. Go to **View** > **Inventory** > **Virtual Machines & Templates**. Create a new folder and move the new virtual machine into that folder.
5. Before you start the Windows installation on the virtual machine you just created, do the following:
   a. From vCenter Server, locate the virtual machine that you just created, power on the virtual machine, right-click on the virtual machine and select **Edit Settings**.
   b. Edit the following hardware settings, and in the following order:
      - Ensure the CD/DVD Device Type is configured to point at the Windows CD or ISO image.
      - Ensure the CD/DVD drive is present and configured to `Connect at power on`.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 BusLogic driver improves SCSI virtual disk performance. Also, note that you must have a virtual floppy configured in order for the Windows WDDM driver to work.
      - Select the **Force BIOS Setup** option to ensure that the BIOS setup screen launches when the virtual machine boots.
      - From the vSphere Client or vSphere Client, power on the virtual machine, then click the **Console** tab. The BIOS Setup utility launches; if not, reset the virtual machine.
      - Click the **Boot** tab and change the order of the boot options to (1) CD-ROM drive (2) Hard drive, and (3) Removable Devices.

What to do next: Install Windows

Create Desktops with XenDesktop

When using Pano System with XenDesktop, the XenDesktop Controller and (optionally) the available provisioning method(s), perform all desktop provisioning services. Pano Controller will not cause any DVMs to be created, nor will it attempt to keep a certain number of powered-on DVMs. These provisioning and power management functions are all performed by XenDesktop. XenDesktop 5 supports several catalog types.

Version	Provisioning Methods Available
XenDesktop 5 or later	Citrix Provisioning Services with XenDesktop 5 and Machine Creation Service (MCS)
XenDesktop 4	Citrix Provisioning Services with XenDesktop 4

Catalog	Supported?	Required Provisioning Method/Service	Install PDS on...	Upgrade PDS via...
Pooled	Yes	Machine Creation Services	Master VM	Master VM
Dedicated	Yes	Machine Creation Services	Master VM	Pano Controller
Existing	Yes	n/a	Manually for each VM	Pano Controller
Physical	No	n/a	n/a	n/a
Streamed	Yes	Citrix Provisioning Services	vDisk	vDisk

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.

Note: The Windows WDDM driver requires that the floppy driver be enabled.

Note: If you intend to use, or are currently using, Citrix Provisioning Services or Machine Creation Service (MCS) to auto-provision virtual desktops, there is no need to perform all the steps outlined in the following table. Instead, simply follow the Citrix documentation to deploy Citrix Provisioning Services. After you verify that auto-provisioning is working as expected, simply update the vdisk to install the Pano Direct Service and apply the Windows settings outlined in the "Tune settings" section. If you are creating your vdisk for the first time, you must install Windows, the XenServer Tools, and then the Citrix Virtual Desktop Agent, in that order, before installing Pano Direct Service.

Create DVMs in SCVMM

Create the virtual machines. This approach is outlined below.

To create a desktop virtual machine:

Use the SCVMM Administrator Console for this process.

1. Connect to SCVMM server.
2. Within SCVMM, create a new virtual machine.

What to do next: Install Windows

Install Windows

After you've created your first VM, you're ready to install the operating system. The process is the same for both Windows XP and Windows 7.

Users of XenServer/XenDesktop can skip this step; Xen has taken care of this for you.

1. Connect to your VM's console.
2. Power on the virtual machine that you created.
3. From the Console, view the boot process. The Install Windows wizard launches.
4. Complete the Windows setup just as you would for a typical Windows installation.

   If you receive any messages indicating that a component has not passed Windows logo testing, simply ignore the messages and click **Yes** to continue with the installation.

   Also, because this image will be used as a template, it's abest practice to make the configuration as generic as possible. You can customize the virtual machines using a Customization Specification; you'll do this task shortly in Create Guest Customization Specification.

5. Apply the most recent Microsoft updates. If you are installing XP, be sure to install the updates recommended in Windows XP Support.
6. Verify that the Windows machine boots properly, that you can log on, and that it joins the domain.

Note: If you are installing under VMware, you should install VMware tools. VMware bundles the latest VMware Tools with VI3. For detailed instructions, go to *Installing and Upgrading VMware Tools* section in VMware vSphere documentation. The benefits of VMware Tools are:

- 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.

What to do next: If you are using VMware,Install VMware Tools on Windows XP or Install VMware Tools on Windows 7

Install VMware Tools on Windows XP

1. Use the vSphere Client to connect to vCenter Server.
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**.
4. Follow the on-screen instructions to install the **Complete** package. Afterward, the VMware Tools installer prompts you to reboot the virtual machine.
5. Verify that the installation worked. Go to Check Status of Virtualization Tools on DVMs.

Install VMware Tools on Windows 7

1. Use the vSphere Client to connect to vCenter Server.
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**.
4. From the virtual machine, click Run `setup.exe`, then allow the `Unknown Publisher` (VMware) to start the installation.
5. Follow the on-screen instructions to install the package.
   a. When prompted, choose **Complete Install**.
   b. In the SVGA Driver drop-down list, choose WDDM.
   c. Make sure you have a virtual floppy configured. WDDM will not work without it.
   d. Click Run setup.exe, then allow the `Verified Publisher` (Microsoft) to complete the installation.

      Afterward, the VMware Tools installer prompts you to reboot the virtual machine.
6. Verify that the installation worked. Go to Check Status of Virtualization Tools on DVMs.
7. Install the VMware View Agent with PCoIP support and reboot Windows.

What to do next: Set Hardware Acceleration

Install Certificate for Pano Direct Service Drivers

Use this procedure to install the certificates on Windows 7 DVMs. You cannot use these certificates on Windows XP DVMs (see Enable Silent Installation for Windows XP).

Note: Earlier versions of Pano Direct Service used different certificates (`PanoCert.cer` and `Thawte.cer`). If you already have these certificates installed, you may leave the existing certificates as is for earlier versions of Pano Direct Service, but you must install the new certificate (`PanoLogicAuthCode.cer`) in order to install Pano Direct Service v4.5 and later.

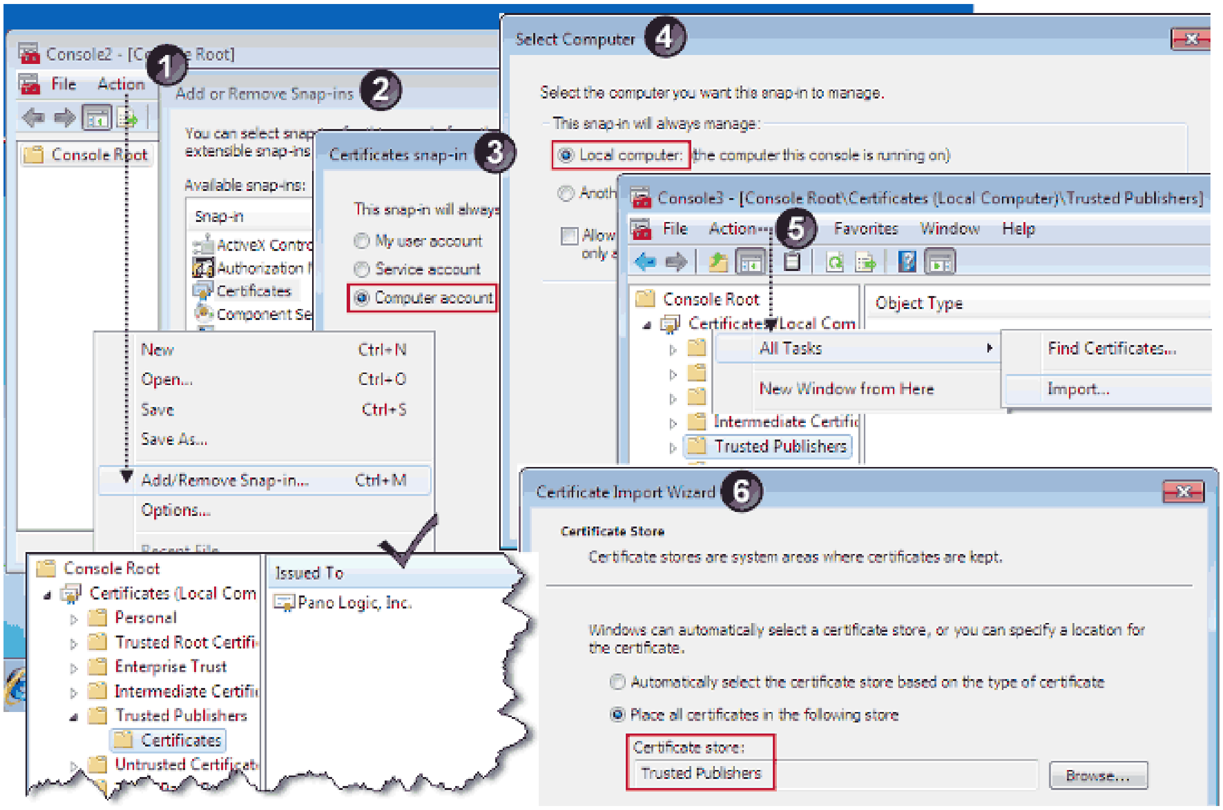
The driver on which Pano Direct depends are digitally signed:

- In the case of a manual deployment of Pano Direct, you need to install the certificates on your DVMs to avoid the annoying unsigned driver alerts.
- In the case of Pano Direct Service installation via GPO, you must install the certificates because Windows 7 does not allow unsigned drivers without user interaction.

To manually install certificates:

Use this procedure to install the certificates on the virtual machine (“gold image”) that you intend to use as your template. Then, when you provision your DVMs, all DVMs will get the certificates.

1. Retrieve the `PanoLogicAuthCode.cer` certificate from Pano Logic’s download site:
2. From mmc (type MMC in the Search box), install the certificates in the `Trusted Publishers` folder on the virtual machine:



This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer

□ Allow ... only ...

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

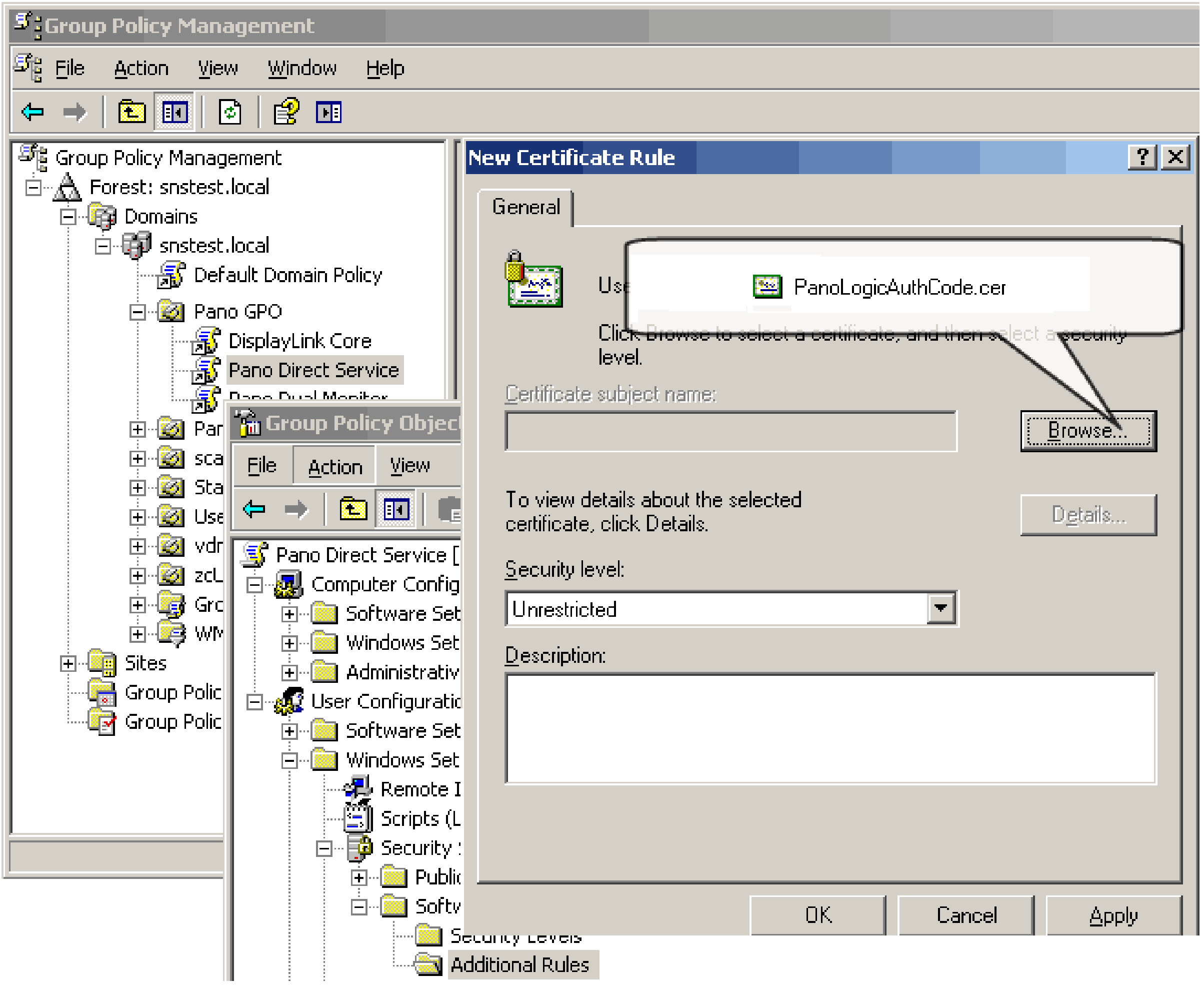
● Place all certificates in the following store

Certificate store:
Trusted Publishers

To install certificates using GPO:

Note: The following example is for Windows Server 2003, but the concept is the same in later versions of Windows Server.

1. Retrieve the `PanoLogicAuthCode.cer` from Pano Logic's download (FTP) site:
2. Open Microsoft Management Console's (MMC) Group Policy Object Editor snap-in, and add the certificates to the software package for your Pano Direct Service deployment. You can install certificates before or after the Pano Direct Service package.
   a. Right-click on the policy for the Pano Direct deployment, and choose Edit.
   b. Go to **User Configuration** > **Windows Settings** > **Security Settings** > **Software Restrictions Policies** > **Additional Rules**.
   c. In the **Security level:** drop-down list, select `Unrestricted`.
   d. Browse to and select the certificates.



PanoLogicAuthCode.cer

Click Browse to select a certificate, and then select a security level.

Certificate subject name:

To view details about the selected certificate, click Details.

Security level: Unrestricted

Description:

Next: Set Hardware Acceleration

Set Hardware Acceleration

Pano 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.

To set hardware acceleration in Windows XP:

1. From the Windows Control Panel, go to **Display** > **Settings**.
2. Click the **Advanced** button.
3. Click the **Troubleshoot** tab.
4. Move the Hardware acceleration slider to `Full`, then apply your changes.
5. Restart Windows.

To set hardware acceleration in Windows 7:

1. From the Control Panel, go to **Appearance and Personalization** > **Display**.
2. In the Navigation pane, click **Adjust resolution**.
3. Click **Advanced Settings**.
4. From the Toubleshoot tab, click on the **Change Settings** button.
5. Move the Hardware acceleration slider to `Full`, then apply your changes.
6. Restart Windows.

What to do next: Installing Pano Direct Service

26 Installing Pano Direct Service

Pano Direct Service (PDS) is the drive package that handles communication between the user's virtual machine and the actual endpoint hardware. There is a version of PDS for Windows XP and a version for Windows 7.

Installation is the same, regardless of the virtualization platform. The Pano Direct Service Wizard walks you through the installation of the Pano Direct Service. You must install the Pano Direct Service on all DVMs that you want to access from a Pano System Endpoint.

It's best to start with a single DVM installation, then test it, before proceeding to mass installation.

This chapter includes the following topics:

- Install Pano Direct Service on Windows 7
- Install Pano Direct Service on Windows XP

Note to Xen users: The Pano Direct Service installer must be run after XenServer Tools and the XenDesktop Virtual Desktop Agent are installed. If you need to upgrade either of these XenDesktop components, you must first uninstall the Pano Direct Service. After upgrading the XenDesktop components, reinstall the Pano Direct Service.

Install Pano Direct Service on Windows 7

Before You Begin: Verify that the DVM is displayed as `available` in the XenDesktop Controller.

Before You Begin: If you intend to Install Third Party GINA Applications, you must do so before you install Pano Direct Service.

1. Make sure that you have a supported hardware and virtualization platform. See System Requirements.
2. Make sure you have administrative rights to the desktop virtual machine.
3. Install the certificates for Pano Direct drivers as outlined in Install Certificate for Pano Direct Service Drivers.
4. Do one of the following to open the ports on which Pano Direct Service depends:
   - (Recommended) Log on to the DVM as a domain administrator, ensuring that the DVM joins the domain. The Pano Direct Service installer automatically opens the necessary ports it needs on the DVM firewall. Installing Pano Direct Service after it joins the domain avoids a GPO policy from potentially overwriting the firewall settings configured by the Pano Direct Service installer.
   - Modify the group policy settings on the domain to allow Pano Direct Service port settings (for more information, go to Configure DVM Firewall):
     - Pano Direct Service to Pano Controller port: Port Number 8319 and Protocol TCP
     - Pano Direct Service to Pano System Endpoint port: Port Number 8321 and Protocol UDP
   - Modify the group policy settings on the domain to allow `local program exceptions`.
5. Copy the Pano Direct Service installer file to the DVM's local drive.

6. If you have open files, save your data. The installer automatically restarts Windows in order to complete the installation. If you do not save now, you will lose all data.
7. Double-click on the `.msi` file.The Pano Direct Service wizard launches, then follow the on-screen instructions.
8. Follow the steps in the wizard.

Note: Before the installer allows you to start the installation, you must agree to restart the virtual machine after the installation:

9. Wait 10 to 30 seconds while the installer installs the drivers.
10. Wait for the system to reboot before you attempt to log on to the desktop virtual machine.

Next: Creating Desktops - Configuration & Tuning

Install Pano Direct Service on Windows XP

Before You Begin: Verify that the DVM is displayed as `Available` in the Citrix XenDesktop Controller.

Before You Begin: If you intend to, you must do so before you install Pano Direct Service. See Install Third Party GINA Applications.

1. Make sure that you follow the support system requirements, See System Requirements.
2. Make sure you have administrative rights to the desktop virtual machine.
3. Do one of the following to open the ports on which Pano Direct Service depends:
   - (Recommended) Log on to the DVM as a domain administrator, ensuring that the DVM joins the domain. The Pano Direct Service installer automatically opens the necessary ports it needs on the DVM firewall. Installing Pano Direct Service after it joins the domain avoids a GPO policy from potentially overwriting the firewall settings configured by the Pano Direct Service installer.
   - Modify the group policy settings on the domain to allow Pano Direct Service port settings:
     - Pano Direct Service to Pano Controller port: Port Number 8319 and Protocol TCP
     - Pano Direct Service to Pano System Endpoint port: Port Number 8321 and Protocol UDP
   - Modify the group policy settings on the domain to allow `local program exceptions`.

   The Pano Direct Service installer opens the necessary ports on the DVM Firewall automatically. Installing Pano Direct Service after joining the domain avoids a GPO policy from potentially overwriting the firewall settings configured by the Pano Direct Service installer.
4. Copy the Pano Direct Service installer file to the DVM's local drive.
5. If you have open files, save your data. The installer automatically restarts Windows in order to complete the installation. If you do not save now, you will lose all data.
6. Double-click on the `.msi` file.The Pano Direct Service wizard launches, then follow the on-screen instructions.

Note: You will receive security warnings (`Unknown Publisher`) during this installation. Such warnings are normal. Simply ignore these warnings by clicking **Run** or **Yes**.

7. If prompted to install a Windows USB driver (`USBD.sys`), you must install USB support manually.

   You are prompted to install a Windows USB driver if the Pano Direct Service installer detected that a `USBD.SYS` file is not installed. The Pano Direct Service installer tried to copy the USBD.SYS file to the correct location to make USB devices work in a Pano System environment. However, if this USBD.SYS file is not present on the DVM, the Pano Direct Service installer cannot enable Pano USB support, so you must enable USB support manually, if you plan to allow redirection of advanced USB devices such as printers, scanners or mass storage.

This USBD.SYS 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 if the file isn't on the DVM, the Pano Direct Service installer cannot provide the file because Microsoft doesn't allow this file to be redistributed. Sorry. You can, however, enable support manually.

8. (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 vSphere Client (vSphere Client), 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.
9. Follow the steps in the wizard.

Note: Before the installer allows you to start the installation, you must agree to restart the virtual machine after the installation:

10. When prompted to choose the installation type, select **Complete** setup.
11. 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.
12. 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 Direct Service 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: For more information, go to Enable Silent Installation for Windows XP.
     - Uninstall Pano Direct Service: From the Windows Control Panel, double-click on **Add or Remove Programs**, go to **PanoDirect** and click **Remove**.
     - Launch the Pano Direct Service wizard again, and continue with the installation.
13. Wait for the system to reboot before you attempt to log on to the desktop virtual machine.

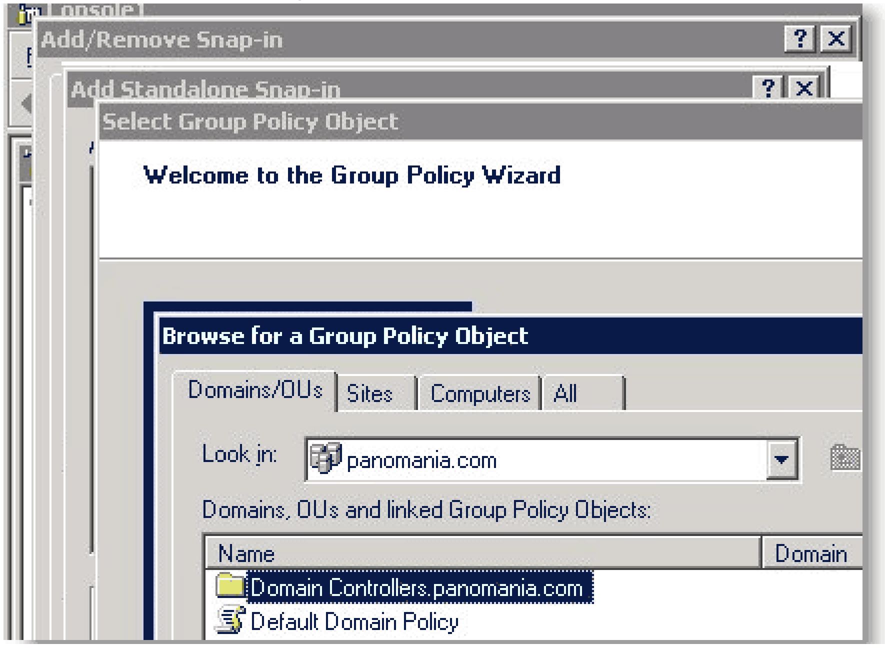
To install Pano Direct Service on multiple DVMs using AD:

Note: The following example is for Windows Server 2003, but the concept is the same in later versions of Windows Server.

If your company deploys a large number of desktop virtual machines (10+), consider updating Pano Direct Service on those desktop virtual machines in an automated manner.

- If your company does not use Active Directory, you can use Microsoft System Management Server (SMS) instead.
- If your company uses Active Directory, perform the following procedure.

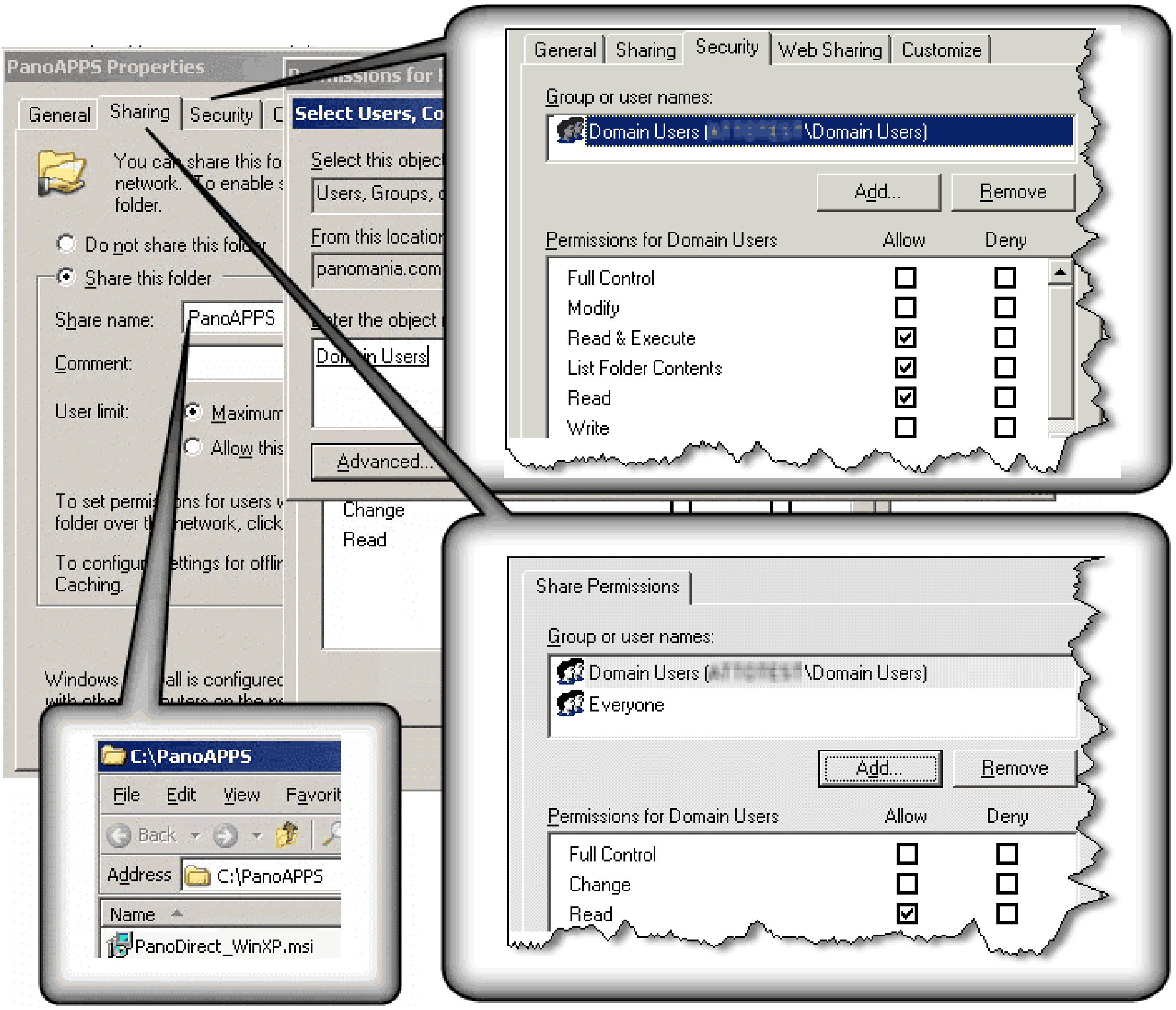
1. Add the Group Policy Editor Snap-in to MMC on the AD Domain Controller. In this example, the domain name is panomania.com.


onsole1
Add/Remove Snap-in
Add Standalone Snap-in
Select Group Policy Object
Welcome to the Group Policy Wizard
Browse for a Group Policy Object
Domains/OUs
Sites
Computers
All
Domains, OUs and linked Group Policy Objects:
Name
Domain
Domain Controllers.panomania.com
Default Domain Policy

Look in: panomania.com

2. Copy the `PanoDirect.msi` file to a folder on the Domain Controller server, then make sure that the folder is shared so that your users have Read access it:
   - **Sharing** tab > **Read**
   - **Security** tab > **Read & Execute**, **List Folder Contents**, and **Read**.

   In this example, the folder is `PanoAPPS`.



PanoAPPS Properties

General | Sharing | Security | C

You can share this fo network. To enable s folder.

○ Do not share this folder
● Share this folder

Share name: PanoAPPS
Comment:
User limit: ● Maximum ○ Allow this

To set permissions for users w folder over the network, click

To configure settings for offlir Caching.

Windows all is configured with other omputers on the ne

Permissions for

Select Users, Co

Select this object
Users, Groups, o
From this location
panomania.com
Enter the object
Domain Users

Advanced...

Change
Read

General | Sharing | Security | Web Sharing | Customize

Group or user names:
Domain Users ([redacted]\Domain Users)

Add... | Remove

Permissions for Domain Users	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□

Share Permissions

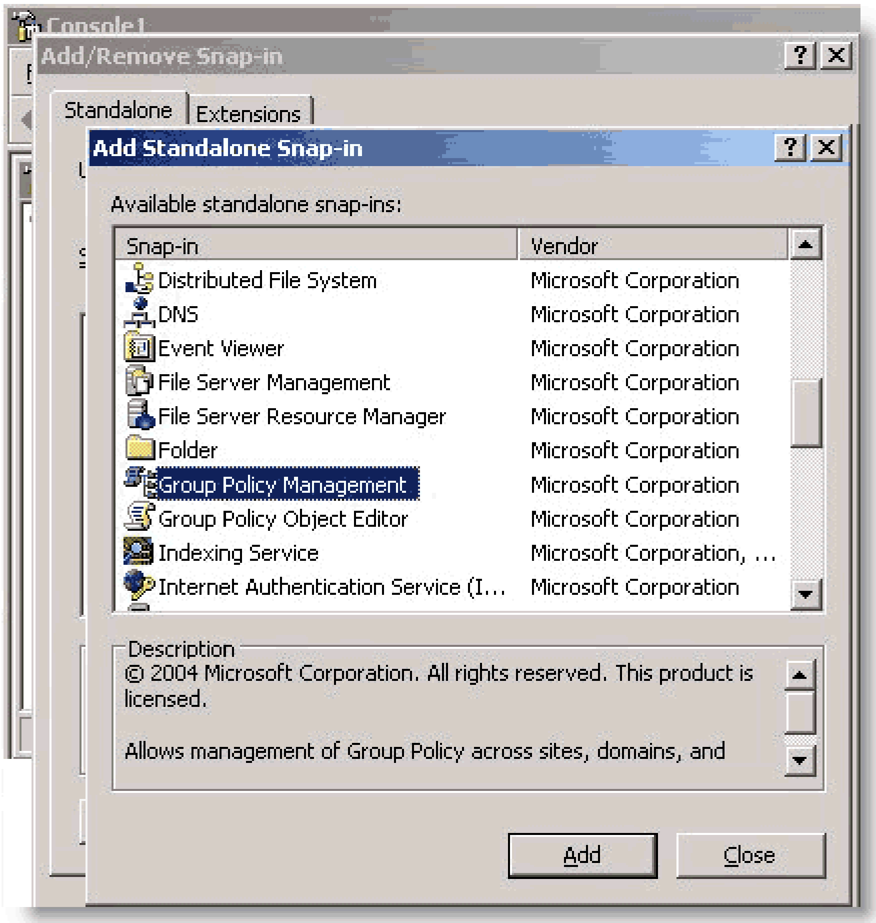
Group or user names:
Domain Users ([redacted]\Domain Users)
Everyone

Add... | Remove

Permissions for Domain Users	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

C:\PanoAPPS
File Edit View Favorit
Back
Address C:\PanoAPPS
Name
PanoDirect_WinXP.msi

3. Download the Pano Direct Service `.msi` file into the folder.
4. (Optional) Prevent the Pano Control Panel from launching after the installer completes. Refer to How do I prevent the Pano Control Panel from launching after a silent install?.
5. Add Group Policy Management Snap-In to MMC.



Console1

Add/Remove Snap-in

Standalone | Extensions

Add Standalone Snap-in

Available standalone snap-ins:

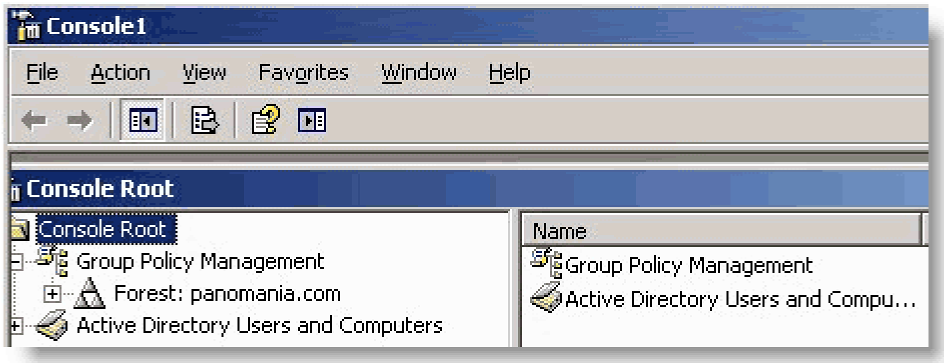
Snap-in	Vendor
Distributed File System	Microsoft Corporation
DNS	Microsoft Corporation
Event Viewer	Microsoft Corporation
File Server Management	Microsoft Corporation
File Server Resource Manager	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy Management	Microsoft Corporation
Group Policy Object Editor	Microsoft Corporation
Indexing Service	Microsoft Corporation, ...
Internet Authentication Service (I...	Microsoft Corporation

Description

© 2004 Microsoft Corporation. All rights reserved. This product is licensed.

Allows management of Group Policy across sites, domains, and

6. Add Active Directory Users and Computers Snap-In.



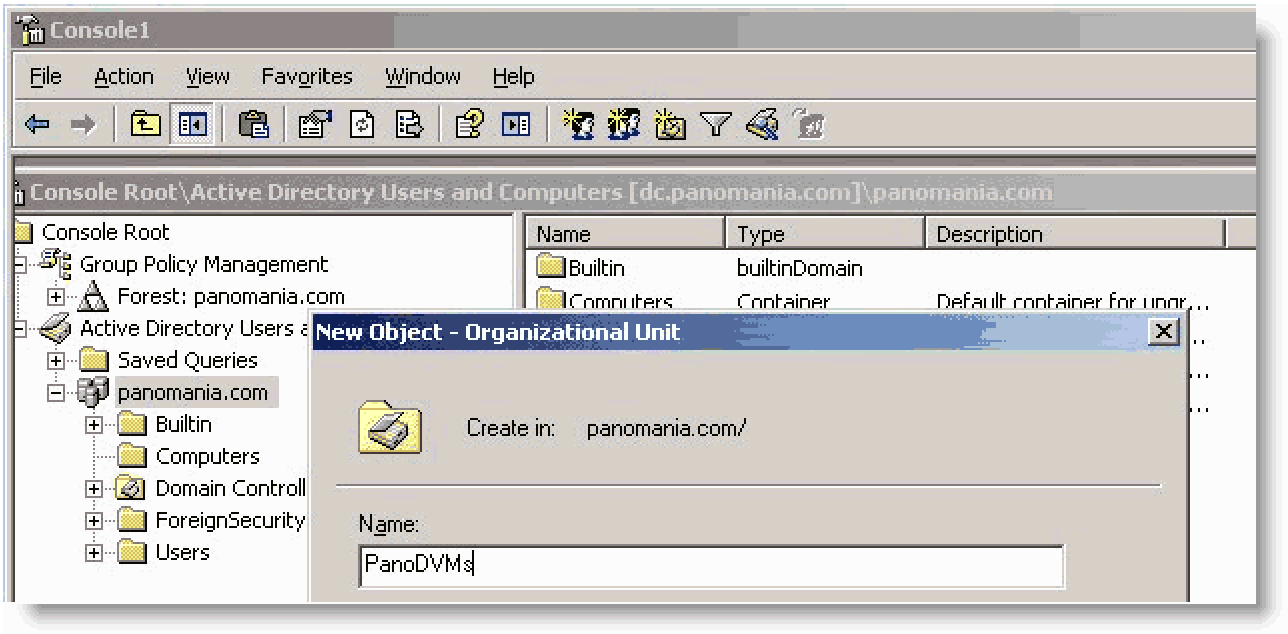
Console1

Console Root

- Console Root
  - Group Policy Management
    - Forest: panomania.com
  - Active Directory Users and Computers

Name
Group Policy Management
Active Directory Users and Compu...

7. Create new OU for DVMs. Put all DVMs in that OU.



Create in: panomania.com/

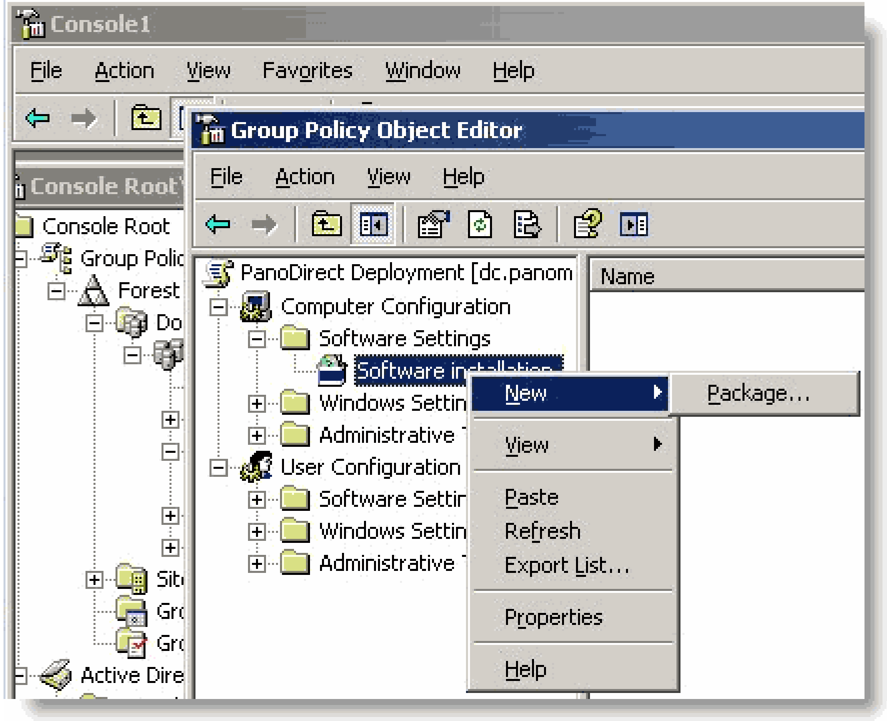
Name: PanoDVMs

8. Right-click on the OU that you just created, choose **Create and link a GPO Here...**, give the New GPO a name, then click **OK**.

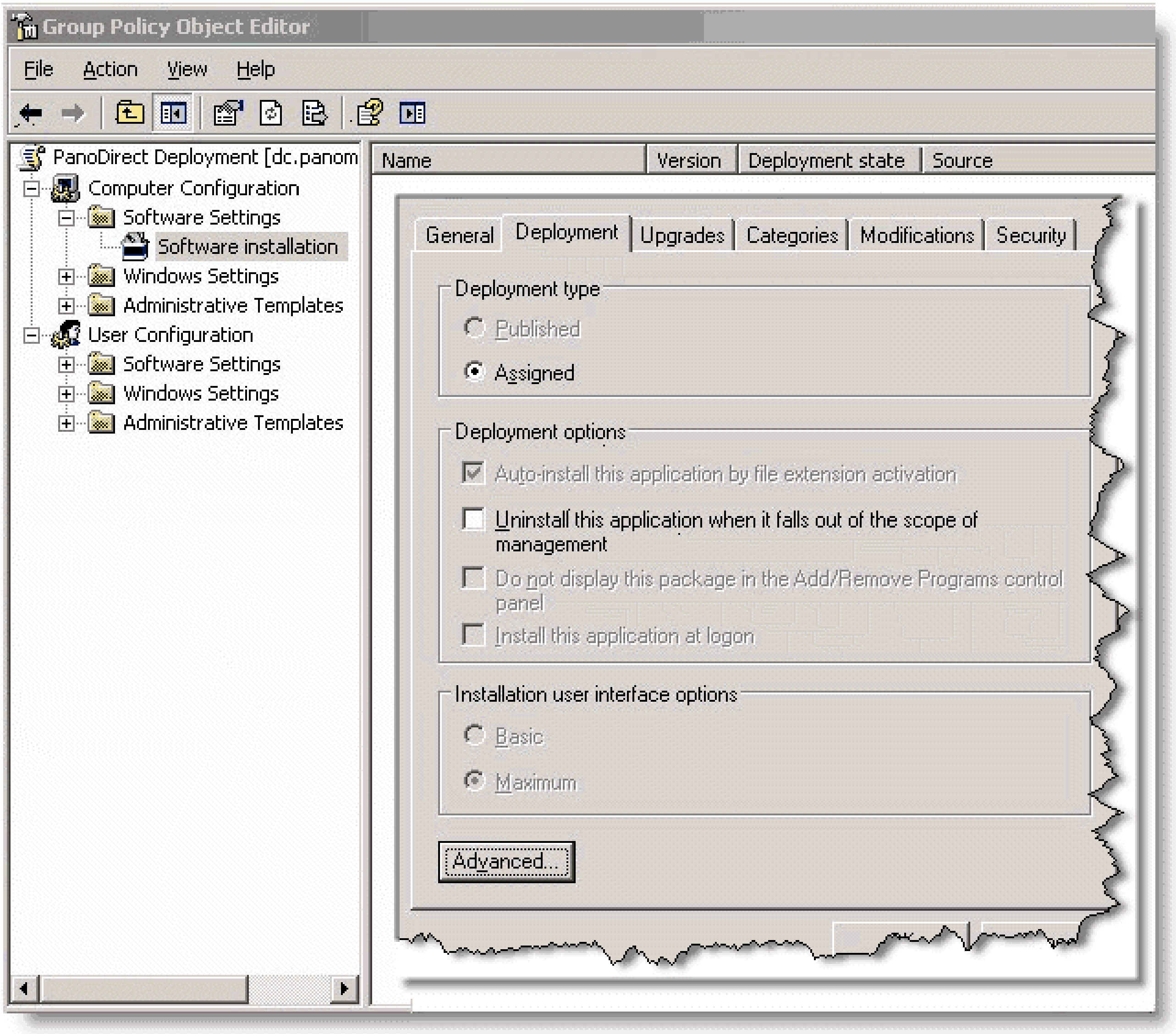
   If you created the GPO in advance, click **Link an existing GPO...**, then link to the objects.

9. Edit Group Policy on the AD Server.

10. Create new software package for Pano Direct Service deployment.



11. Through the network path on the AD Server, select the Pano Direct Service MSI file, then set the properties of the MSI deployment.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

□ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

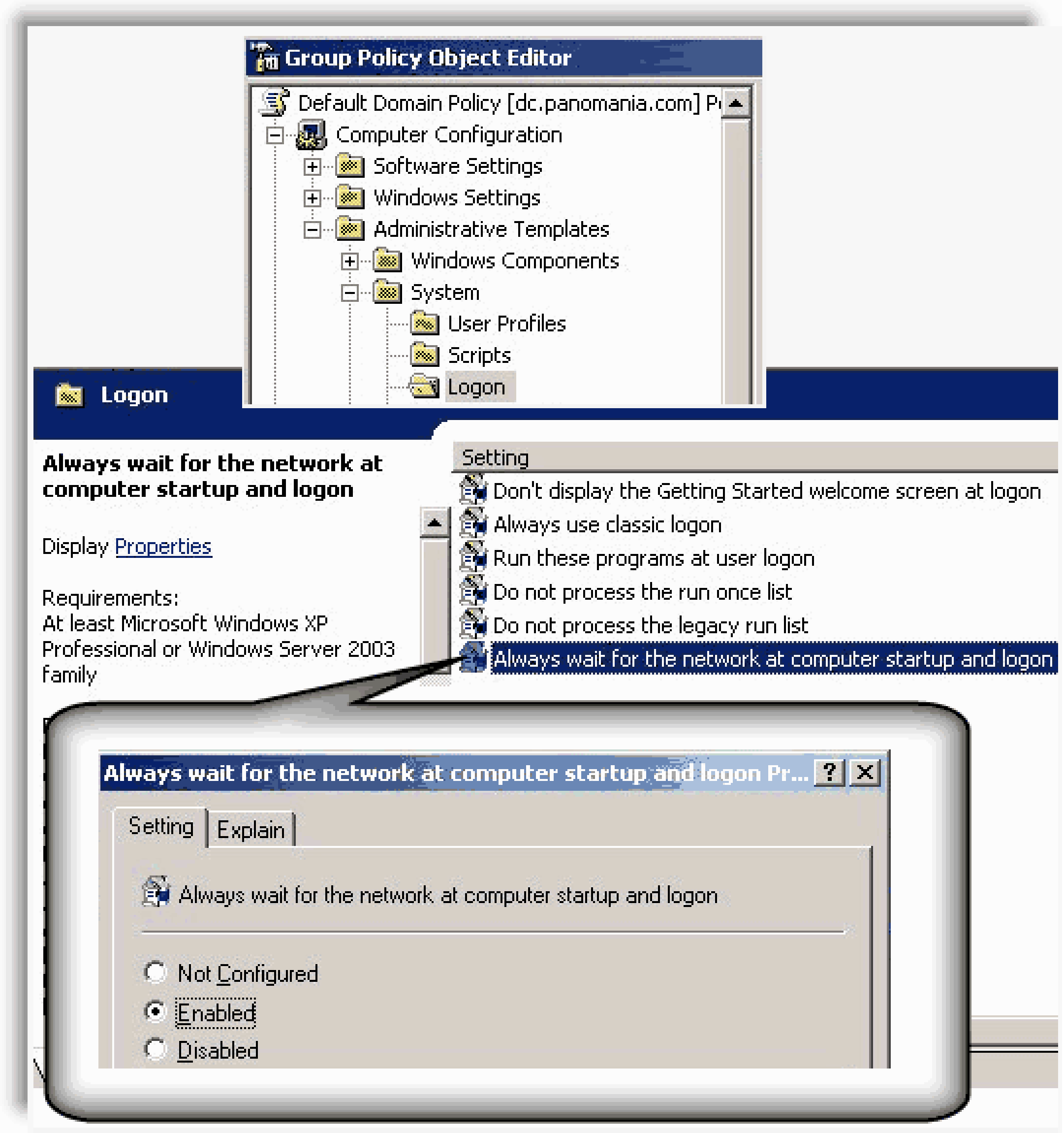
□ Install this application at logon

Installation user interface options

○ Basic

● Maximum

12. Set the **Always wait for the network at computer startup and logon** setting to `Enabled`.


Group Policy Object Editor
Default Domain Policy [dc.panomania.com] P
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Components
System
User Profiles
Scripts
Logon
Logon
Setting
Don't display the Getting Started welcome screen at logon
Always use classic logon
Run these programs at user logon
Do not process the run once list
Do not process the legacy run list
Always wait for the network at computer startup and logon
Always wait for the network at computer startup and logon Pr...
Setting
Explain

Always wait for the network at computer startup and logon

Display Properties

Requirements:
At least Microsoft Windows XP Professional or Windows Server 2003 family

Always wait for the network at computer startup and logon

○ Not Configured
● Enabled
○ Disabled

13. Enable a silent installation:
    - (Windows 7) Go to Install Certificate for Pano Direct Service Drivers.
    - (Windows XP) Go to Enable Silent Installation for Windows XP.

When the DVMs boot, Pano Direct Service is installed during the DVMs' startup process. Afterward, the DVMs automatically reboot. Only after this final reboot will the installation take effect.

Note:

To install Pano Direct Service on all DVMs simultaneously using SMS:

For instructions, email Pano Logic Technical Support at support@panologic.com.

Next: Creating Desktops - Configuration & Tuning

27
Creating Desktops - Configuration & Tuning

This chapter includes the following topics:

- Verify DVM Connectivity
- VMware Disposable Desktops
- Control Session Timeouts
- Disable Fast User Switching in Windows 7
- Disable Sleep and Hibernate in Windows 7

Verify DVM Connectivity

Perform this procedure before adding additional DVMs or enabling automated deployment. See Automated Deployment Concepts. Verify that you can connect to your DVM from a Pano System Endpoint before you proceed with your deployment.

To run this test, you need to create a DVM Collection. The DVM Collection associates the authorized user(s) to the specified DVM(s).

1. :Connect one existing virtual machine to a single Pano System Endpoint by 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 Controller.

b. Click the **DVM Collections** tab.

c. Click **Add**. The Add DVM Collection wizard launches.

d. Specify the following required parameters, and retain all defaults:

- **Type** - Select **Existing Desktops**.
- **Name** - Enter a name for the DVM Collection. Let’s call it `Test`.
- **DVMs Folder** - Browse to find the folder that contains the DVM that you created earlier for this collection. Select the folder, and then click **OK**.
- **Accounts** - 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.

2. From the Pano System Endpoint, log on to the DVM as one of the authorized users.

- If you see a Windows machine, then you’ve successfully verified the basic operation of the Pano System.
- If you are not successfully connected to the Windows desktop, make sure the DVM is configured to join the correct domain. If that doesn’t fix the problem, go to Troubleshoot DVM Login Problems and Deploy Resources.

3. Verify that the Pano Direct Status indicates `Responding` (go to Monitor Pano Direct Service Status).

If Unreachable, it’s likely that you have a GPO policy that’s overwriting the firewall settings that were configured by the Pano Direct Service installer. You have two choices:

    - Uninstall Pano Direct Service, join the domain, then reinstall Pano Direct Service–in that order. Installing Pano Direct Service after joining the domain ensures that all necessary ports are opened.
    - Change your GPO policy to open the necessary ports as outlined in Configure DVM Firewall or disable the firewall locally.
    - Ensure that you do not have IPv4 disabled. The Pano Controller depends on IPv4 as outlined in the appropriate topic for your virtualization infrastructure: Network Addressing Requirements

- If needed, you should create VMware Disposable Desktops. Otherwise, Control Session Timeouts

VMware Disposable Desktops

VMware offers a a *non-persistent disk* option in its Pooled Desktops collection type. These are "disposable" desktops. With disposable desktops, when a user makes 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.

Often users save cookies and passwords as they browse the web, even when they shouldn't; disposable disks deletes this data. Any personal files that the users saves are deleted, so that other users do not have access to this data.

A non-persistent disk adds greater security. If users download 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.

Kiosk and shared-computer users know (or should know) that personal data is note being stored on the local machine. Thus there is not reason to tell users that the DVM is disposable.

If most of your users will use a Pooled Desktops collection type and you want the DVMs in that collection to be disposable, you need to do one of the following:

- Deploy all the needed DVMs from a persistent template, allowing sysprep to complete, then change them to non-persistent. This method increases the administrative overhead work.
- Deploy them from a template with a persistent system disk and a non-persistent user/data disk. This method increases disk usage, unless you use some form of linked clones for the C: drive.

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\PanoDirect\SCRIPTS`:
   ```
   "C:\\Desktop\PsTools\psshutdown.exe" -k -f -t 2
   ```
4. Copy `psshutdown.exe` from the temporary folder to is part of Windows SysInternals
5. Configure DVM's hard drive as a *non-persistent disk*:
   a. From vCenter Server, right-click on the DVM and choose **Edit Settings** > **Hard Disk**.
   b. Change to `Non-Persistent disk`.
6. Power off then power on the virtual machine. A reboot won't do the trick. You must power-cycle the DVM.
7. (Recommended) To minimize the amount of time users need to wait for a DVM, when you create the Pooled Desktops collection type set **Extra Desktops** to `0` and **Extra to Keep On** to at least `3`.

What to do next: Control Session Timeouts

Control Session Timeouts

Pano Logic supports session timeout settings that can be used in a Pano System environment to help manage users and resources. These Session Timeout settings end two types of sessions: (1) Idle and (2) Disconnected.

• 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 time limit can be specified where if there is no keyboard or mouse movement, the Pano System 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 System Endpoint returns to the Pano user login screen.
- **Logs off the user**. If the specified action is to `logoff`, Pano System automatically logs off the user, thereby ending the Windows session, and the Pano System Endpoint returns to the Pano user 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\PanoDirect\Native Session\Max Idle Time`. A value of `0` disables the idle session timeout. The Pano Direct Service 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\PanoDirect\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 Direct Service 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 System Endpoint 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 System Endpoint.

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 System Endpoint mobility around the office without keeping the DVM running for days with no use. When the session limit is reached, Pano System 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\PanoDirect\Native Session\Max Disconnection Time`. A value of `0` indicates no maximum time. After this timeout limit is reached, the Pano System 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 System 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 System to disconnect the user after being idle for 10 minutes; after being disconnected, the user has 20 minutes to reconnect before Pano System automatically logs off the user:

The Pano Direct Service must be restarted for this change to take effect.

What to do next: Disable Fast User Switching in Windows 7

Disable Fast User Switching in Windows 7

There are limitations to fast user switching; in other cases, support isn't appropriate for many collection types. Therefore, apply a domain policy, or apply a local policy on the virtual machine(s) that you intend to convert to a template(s) and for those collection types that do not support fast user switching.

If your users are local Administrators on their desktops, create a domain policy instead of a local policy to ensure that your users don't overwrite your changes.

(Domain Policy) To disable fast user switching on Windows Server 2008:

Enable Computer configuration > Administrative Templates > System > Logon > Hide entry points for Fast User Switching.

(Local Policy) To disable fast user switching for Windows 7 DVMs:

1. Log on as local Administrator.
2. Using the Local Group Policy Editor (type **gpedit.msc** in the Start menu Search box), modify the registry on the DVM.
   a. Go to Local Computer Policy > Administrative Templates > System > Logon.
   b. In the pane to the right, double-click on **Hide entry points for Fast User Switching** option, then set the value to `Enabled`.

What to do next: Disable Sleep and Hibernate in Windows 7

Disable Sleep and Hibernate in Windows 7

Sleep and hibernate are not supported. You must disable this feature.

You can disable sleep by using group or local policies, and you can disable hibernate by running the `powercfg` command on the local computer.

If you plan to manage these settings via Group Policy, you need to use Windows Server 2008. If you have not upgraded to Windows Server 2008 or you plan to manage these policies locally, make sure to configure the local policy of the template used for cloning desktop virtual machines.

(Group Policy 2008) To disable sleep:

1. Enable Computer configuration > Administrative Templates > System > Power Management > Sleep Settings > **Turn Off Hybrid Sleep (Plugged In)**.
2. Disable Computer configuration > Administrative Templates > System > Power Management > Sleep Settings > **Allow Standby States (S1 - S3) When Sleeping (Plugged In)**.

(Local Policy) To disable sleep for Windows 7 DVMs:

1. Log on as local Administrator.
2. Using the Local Group Policy Editor (type **gpedit.msc** in the Start menu Search box), modify the registry on the DVM.
   a. Go to **Local Computer Policy** > **Administrative Templates** > **System** > **Power Management** > **Sleep Settings**.
   b. In the pane to the right, double-click on **Turn Off Hybrid Sleep (Plugged In)** option, then set the value to `Enabled`.
   c. In the pane to the right, double-click on **Allow Standby States (S1 - S3) When Sleeping (Plugged In)** option, then set the value to `Disabled`.

To disable hibernate:

In an elevated command prompt on the local computer, type `powercfg -h off`, then press Enter.

You can use Group Policy to run this command.

28
vSphere-Specific Desktop Options

This chapter includes the following topics:

- Create DVM Templates in vSphere
- Install Sysprep Tools on vCenter Server for Windows XP
- Create Guest Customization Specification
- Test vCenter Server DVM Deployment
- Upgrade of Pano Direct Service with View Agent
- Upgrade VMware Tools
- Upgrade VMware View Agent

We’ve created a video to explain how to configure secure VM View authentication. You should install or update Pano Direct Service first, then configure VM View: Configure Secure Authentication with VMware View

Create DVM Templates in vSphere

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

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

To convert a virtual machine into a template:

Any virtual machine can be converted to a template. This conversion is done from vCenter Server. DVM templates are created within vCenter Server using the standard VMware procedures. For detailed instructions, go to *Working with Templates and Clones* chapter of the VMware vSphere 4.0 U1 Basic System Administration Guide.

A virtual machine can also be cloned to a template which results in creating a copy of the virtual machine and converting that copy into a template, 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. From the vSphere Client, shut down the virtual machine.
2. Select the virtual machine, choose **Inventory** > **Virtual Machine** > **Convert to Template**.

What to do next: Install Sysprep Tools on vCenter Server for Windows XP.

To clone a virtual machine to a template:

For detailed instructions, go to *Working with Templates and Clones* chapter of the VMware vSphere 4.0 U1 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.

1. From the vSphere Client, power off virtual machine.
2. Select the virtual machine, then choose **Inventory** > **Virtual Machine** > **Clone to Template**.

What to do next: Install Sysprep Tools on vCenter Server for Windows XP.

Install Sysprep Tools on vCenter Server for Windows XP

Microsoft Sysprep tools is Microsoft's System Preparation utility for automated Windows XP deployment. Sysprep needs to be installed on the host on which vCenter Server is running so that vCenter Server can automatically create Windows XP DVMs when required; sysprep tools is not needed for automated deployment of Windows 7 DVMs due to that operating system's architecture.

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 vCenter Server server, copy `deploy.cab` to:
   - (Windows Server 2008) `C:\Users\All Users\VMware\VMware VirtualCenter\sysprep\xp`
   - (Windows Server 2003) `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\sysprep\xp`.

What to do next: Create Guest Customization Specification

Create Guest Customization Specification

A guest Customization Specification enables you to customize Windows XP and Windows 7 virtual desktops as you clone them from a template. You must create a guest Customization Specification from within VMware vCenter Server.

Within your vCenter Server, 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 VMware vCenter Server to give DVMs a unique SID and to prepare them for use in your environment.

After the sysprep files are on your vCenter Server server and you have configured your Customization Specification, simply tell your Pano Controller two things when you create the DVM collection:

- the name of the Customization Specification to use
- the 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 vSphere 4.0 U1 Basic System Administration Guide.

1. Ensure that you have Microsoft Sysprep Tools installed. You probably installed this earlier in Install Sysprep Tools on vCenter Server for Windows XP.
2. Connect to vCenter Server.
3. Select **Edit** > **Customization Specification** > **New**. The Customization Specification wizard launches.

4. Type a name for your Customization Specification (for example, `Marketing`), then click **Next**.
5. Type a name for your organization, then click **Next**.
6. In the **Computer Name** window, select the **Use the virtual machine name** radio button, then click **Next**.

   This selection ensures that the names of DVMs that vCenter Server creates match the names of virtual machine names. The name of the DVM is defined when you choose a value for the **Computer Name** in the DVM Collection as outlined in Configure for Concurrent Deployment and Power Operations.
7. In the **Windows License** window, do the following:
   a. Clear the **Include Server License Information** check box.
   b. Type the volume license number for the Windows DVMs, then click **Next**.
8. 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.
9. 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**.
10. In the **Workgroup or Domain** window, specify the Windows domain that this DVM should join, then click **Next**.
11. 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**.
12. Preview your configuration selections, then click **Finish**. You're done!

What to do next: Test vCenter Server DVM Deployment

Test vCenter Server DVM Deployment

The beauty of Pano System is that it can automatically deploy DVMs for you. You no longer need to manually deploy DVMs from within vCenter Server. However, because Pano System uses vCenter Server to deploy DVMs it's a best practice to make sure that your deployment is working within vCenter Server before you begin using the Pano System.

To test DVM deployment:

1. Connect to vCenter Server.
2. From the vSphere Client, deploy a DVM from the template. *Deploying Virtual Machines from Templates* chapter of the VMware vSphere 4.0 U1 Basic System Administration Guide. When prompted, name the DVM
3. Verify that the DVM joins the domain successfully. This means that the guest Customization Specification is working.
4. 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.

What to do next: Create collections as part of a typical production environment.

Upgrade of Pano Direct Service with View Agent

To update the Pano Direct Service with VMware View Agent, follow these steps:

1. If you have not already done so, install VMware tools, eitherInstall VMware Tools on Windows XP or Install VMware Tools on Windows 7.
2. Upgrade Pano Direct Service by installing a new version of Pano Direct Service.
3. Upgrade VMware Tools.
4. Upgrade VMware View Agent.

Upgrade VMware Tools

Follow these steps to upgrade the installed VMware Tools.

To upgrade of VMware Tools

1. Uninstall Pano Direct Service.
2. Uninstall VMware View Agent.
3. Uninstall VMware Tools.
4. Repeat the steps to re-install VMware Tools. Refer to eitherInstall VMware Tools on Windows XP or Install VMware Tools on Windows 7.
5. Re-install a new version of Pano Direct Service.

Upgrade VMware View Agent

Follow these steps to upgrade the installed VMware View Agent.

To upgrade of VMware View Agent

1. Uninstall Pano Direct Service.
2. Uninstall VMware View Agent.
3. Install VMware View Agent.
4. Repeat the steps to re-stall VMware Tools. See Install VMware Tools on Windows XP or Install VMware Tools on Windows 7.
5. Re-install a new version of Pano Direct Service.

Integrate Pano System with VMware View

The Pano System offers a full virtual desktop solution which includes Pano System Endpoints, Pano Direct Service, plus the Pano Controller, which acts as a full-featured connection broker.

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

In a mixed device environment, VMware View typically performs connection brokering and automated deployment functions, even though Pano Controller offers these same capabilities. In such a deployment, both the VMware View Agent and Pano Direct Service run side by side in the same virtual machine. (To learn about Pano Controller's connection broker functionality, go to Pano System Endpoints.)

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

- Discovers and controls Pano System Endpoints.
- 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 System Endpoint.

When Pano Controller is set up with a VMware View, the credentials that users input through the Pano user login screen are passed to VMware View. Provisioning of the DVMs is done through VMware View.

In this scenario, the Pano Controller's function is to establish the connection between the Pano System Endpoint and the DVM. Also, the Pano Controller does not communicate with vCenter Server to start the DVM; rather, VMware View handles these tasks.

In short, Pano System Endpoints must be controlled by the Pano Controller, so you can't completely eliminate the Pano Controller.

- Configure VMware View Agent
- Enable Desktop Connections from Pano Devices
- Connect Pano Controller To VMware View
- Create VMware View Collection
- Validate Pano Controller-VMware View Configuration

Before You Begin: Perform all the steps as outlined in Install Pano Controller on VMware. Integrating Pano System with VMware View Connection Server is simply the last step, and the only step that is different from a Pano System Endpoint-only environment and a mixed device environment. Everything else is the same, including device discovery and Active Directory integration.

Task	Go to...
Learn about VMware View support and limitations.	Supported Third Party Connection Brokers Limitations of VMware View Connection Server
Install and configure VMware View for use with PCs running the VMware View client.	VMware's View Manager Administration Guide
Configure the VMware View Agent.	Configure VMware View Agent
Enable desktop connections.	Enable Desktop Connections from Pano Devices
Connect the Pano Controller to VMware View.	Connect Pano Controller To VMware View
Create a VMware View collection type	Create VMware View Collection
Validate the configuration	Validate Pano Controller-VMware View Configuration

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.

• System behavior when View Secure Authentication is enabled

If you choose to enable VMware View Secure Authentication you must install the Pano Direct Service before you install the VMware View Agent. If you later update Pano Direct Service, 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:

Endpoint	Pano G1 Support	Pano G2 Support
VMware View client	Yes	Yes
Remote Desktop Connection	No	No
Pano System Endpoint connecting to Pano Direct Service v6.0	Yes	Yes
Pano System Endpoint connecting to Pano Direct Service v3.5-v2.6	Yes	No
Pano System Endpoint connecting to Pano Direct Service v2.5.x–configured for Pano Direct™	Yes	No
Pano System Endpoint connecting to Pano Direct Service v2.0.x or earlier	No	No
Pano web access	Yes	Yes
vSphere Client[1]	Yes	Yes
SMS Remote Control or Dameware Mini Remote Control	Yes	Yes

1. When View Secure Authentication is enabled and an end user is connected to the DVM via a Pano System Endpoint using v6.0, the vSphere Client displays the Pano lockout screen. In order for an Administrator to access the DVM from the vSphere Client, 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 VMware View Secure Authentication is disabled**

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

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

Endpoint	Pano G1 Support	Pano G2 Support
VMware View client	Yes	Yes
Remote Desktop Connection[1]	Yes	Yes
Pano System Endpoint connecting to Pano Direct Service v6.0	Yes	Yes
Pano System Endpoint connecting to Pano Direct Service v2.5-v3.5<Superscript>1	Yes	No
Pano System Endpoint connecting to Pano Direct Service v2.0.x or earlier	Yes	No
Pano web access<Superscript>1	Yes	Yes
vSphere Client (vSphere Client)	Yes	Yes
SMS Remote Control or Dameware Mini Remote Control	Yes	Yes

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 System Endpoint, the VMware View 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 VMware View 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.

What to do next: Enable Desktop Connections from Pano Devices

To disable VMware View Secure Authentication:

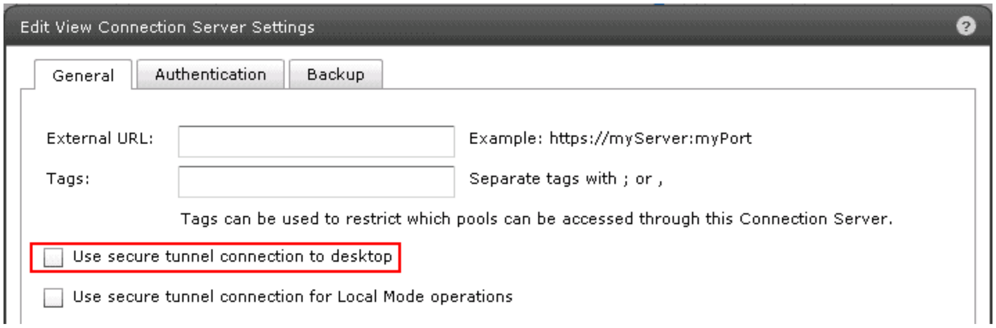
View Secure Authentication is selectable when you install the VMware View. In the **Custom Setup Option** step of the VMware View installation wizard, deselect the View Secure Authentication component.

What to do next: 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 Pano System Endpoints. Otherwise, the VMware View server will only allow tunneled connections.

- (VMware View Connection Server 4.5/4.6) Select **Use secure tunnel connection to desktop** in **Edit View Connection Server Settings**:



Edit View Connection Server Settings

External URL: Example: https://myServer:myPort

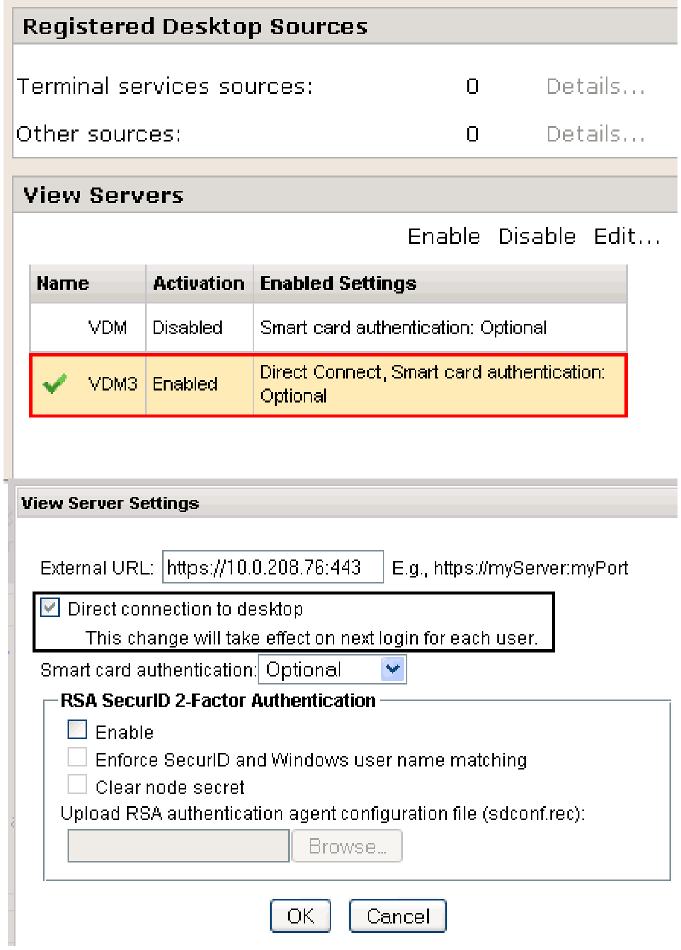
Tags: Separate tags with ; or ,

Tags can be used to restrict which pools can be accessed through this Connection Server.

□ Use secure tunnel connection to desktop

□ Use secure tunnel connection for Local Mode operations

- (VMware View Connection Server 4.0) Select **Direct Connection to desktop** in **View Server Settings**:



Registered Desktop Sources

Terminal services sources:	0	Details...
Other sources:	0	Details...

View Servers

Name	Activation	Enabled Settings
VDM	Disabled	Smart card authentication: Optional
✓ VDM3	Enabled	Direct Connect, Smart card authentication: Optional

View Server Settings

External URL: https://10.0.208.76:443 E.g., https://myServer:myPort

☑ Direct connection to desktop

This change will take effect on next login for each user.

Smart card authentication: Optional

RSA SecurID 2-Factor Authentication

□ Enable

□ Enforce SecurID and Windows user name matching

□ Clear node secret

Upload RSA authentication agent configuration file (sdconf.rec):

What to do next: Connect Pano Controller To VMware View

Connect Pano Controller To VMware View

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

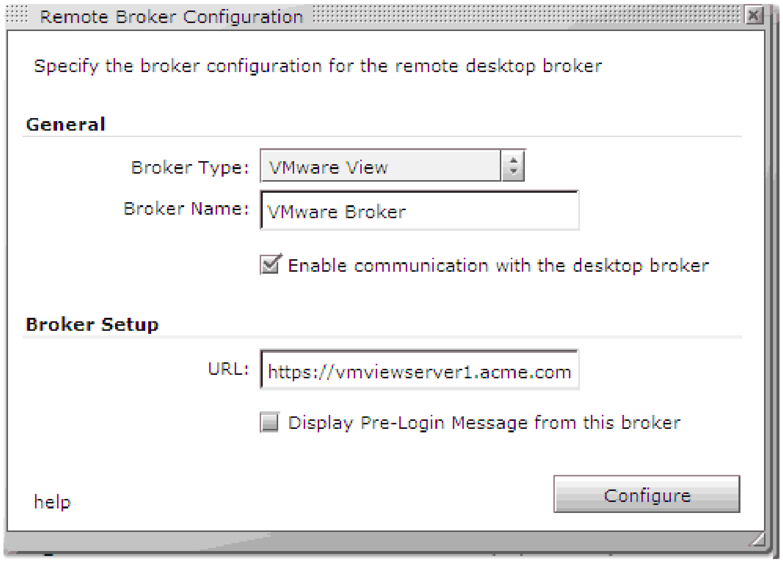
1. Log on to the Pano Controller.
2. Click the **Setup** tab.
3. In the **Broker Configuration** section, click **Add** to enter Broker information
   a. Choose the Broker Type
   b. Specify the Broker Name
   c. Enter the URL for VMware View server and then click **Configure**.

   If you require SSL for client connections, then you must specify a https URL.

```
https://server_name_or_IP_address
```

Example:

```
https://vmviewserver1.acme.com
```


Remote Broker Configuration

Specify the broker configuration for the remote desktop broker

General

Broker Type: VMware View

Broker Name: VMware Broker

☑ Enable communication with the desktop broker

Broker Setup

URL: https://vmviewserver1.acme.com

□ Display Pre-Login Message from this broker

What to do next: Create VMware View Collection

Create VMware View Collection

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

To set up a generic collection for all your VMware View users:

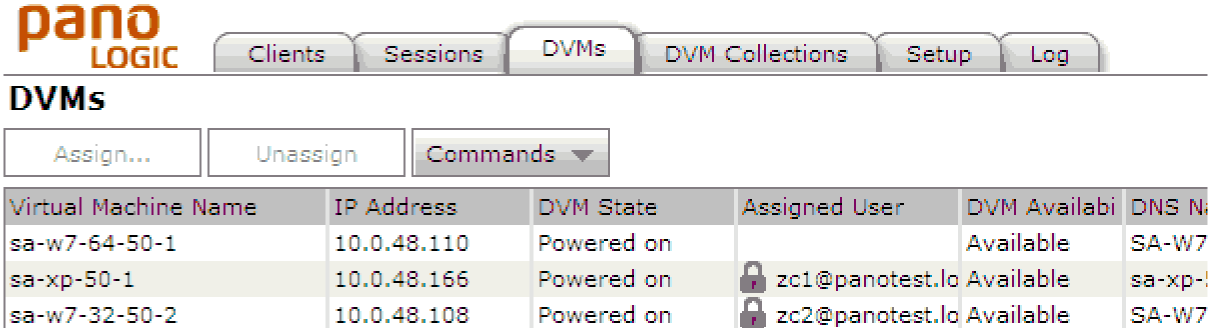
1. Log on to the Pano Controller.
2. Click on the **DVM Collections** tab.
3. Click **Add...**.
4. In the Type drop-down list, select **VMware View**.
5. Type a name for the collection.
6. Specify the users. If you specify a group that contains all your users, VMware View determines the specific mapping.
7. Click **Add** DVM Collection.

What to do next: Validate Pano Controller-VMware View Configuration

Validate Pano Controller-VMware View Configuration

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

1. Verify that the Pano Controller shows that the DVMs are powered on and receiving an IP address, and that Pano Direct Service is responding.



DVMs

Virtual Machine Name	IP Address	DVM State	Assigned User	DVM Availabi	DNS N
sa-w7-64-50-1	10.0.48.110	Powered on		Available	SA-W7
sa-xp-50-1	10.0.48.166	Powered on	🔒 zc1@panotest.lo	Available	sa-xp-
sa-w7-32-50-2	10.0.48.108	Powered on	🔒 zc2@panotest.lo	Available	SA-W7

2. Log on to a DVM from a Pano System Endpoint.

   After successful authentication, the Pano Controller 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 View collection

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

29
Hyper-V Specific Desktop Options

This chapter includes the following topics:

- Create DVM Templates in SCVMM
- Clone with Optional Guest OS Profile

Create DVM Templates in SCVMM

You use templates to create desktop virtual machines. A template serves as a “gold master” image of a DVM containing an OS, applications, policies, software settings and other configurations that have been set for your organization. When you want to create a DVM, you clone from your template.

You can create a new template from an existing virtual machine, but the VM is destroyed in this process. It is always recommended that you clone your “gold master” VM. This ensures that you have a usable copy of your “gold master”, from which you can create new templates.

To clone your source virtual machine:

> **Recommendation:** Before you make a template from your source machine, it is recommended that you clone it.

1. At the **SCVMM Administrators Console**, ensure that all applications are closed in the VM.
2. At the list of **Virtual Machines**, select a machine to use for your new template and stop the machine.
3. Right-click the virtual machine and select Clone.
4. At **Virtual Machine Identity**, specify Name, Owner and Description. Click **Next**.
5. At **Configure Hardware**, select the appropriate Hardware Profile, and Click **Next**.
6. At **Select Destination**, chose whether to store the virtual machine on a host or in the library. Click **Next**.
7. At **Select Path**, type the path for the clone and click **Next**.
8. At **Select Networks**, chose the networks with which to connect and click **Next**.
9. At **Additional Properties**, type any other information as specified and click **Next**.
10. At **Summary**, check the information and then create the clone.
11. When complete, stop the machine. The cloned virtual machine is complete.

To create a template:

1. Right-click the stopped machine and select New template.

   Warning: You see a message about destroying the source virtual machine and user data on it. Make sure that you have already cloned this machine and are prepared to lose the source virtual machine. Click **Yes** to continue.

2. Type a name for the new template and click **Next**.

3. At **Configure Hardware**, go to Bus Configuration and verify that a hard disk or other IDE device is present.

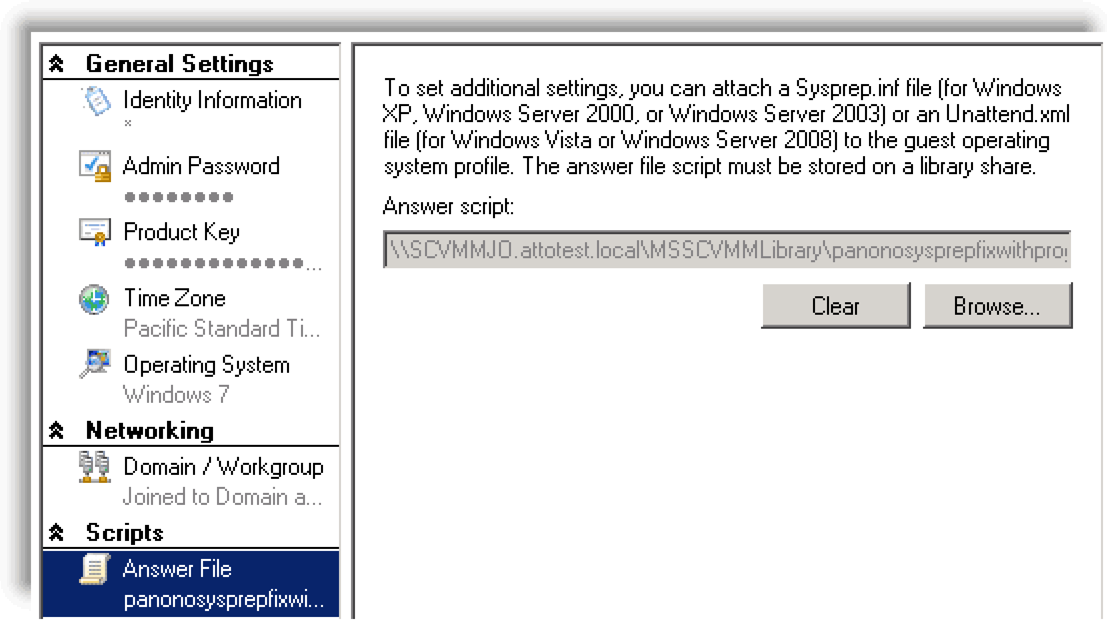
4. At **Network Adapters,** confirm that the Network location is set to the correct domain. Click **Next**.

Note: If you don't see your domain in the drop-down menu, this means that you have a configuration issue. The DNS suffix needs to be set on the SCVMM network adapter.

5. At **Guest Operating System**, do the following:

Go to **General Settings** > **Identify information**. Type the full name of the computer. To have the system randomly select a computer name, use the asterisk (*). During this process, the VM's computer name is replaced with the computer name you specify when you create the DVM collection. See Create DVM Collections.

   a. (Windows 7) Download the `panonosysprepfixwithprogramfiles.xml` from http://download.panologic.com (contact Pano Logic Technical Support at support@panologic.com to obtain access credentials) and save it to a library share. Then, from **Scripts** > **Answer File**, attach the answer file.



General Settings
Identity Information
*
Admin Password
••••••••
Product Key
•••••••••••••...
Time Zone
Pacific Standard Ti...
Operating System
Windows 7
Networking
Domain / Workgroup
Joined to Domain a...
Scripts
Answer File
panonosysprepfixwi...

To set additional settings, you can attach a Sysprep.inf file (for Windows XP, Windows Server 2000, or Windows Server 2003) or an Unattend.xml file (for Windows Vista or Windows Server 2008) to the guest operating system profile. The answer file script must be stored on a library share.

Answer script:
\\SCVMMJO.attotest.local\MSSCVMMLibrary\panonosysprepfixwithpro

Warning: If you don't provide the full computer name, the clone operation will fail.

6. Click **Admin Password**. For Windows 7, provide an account belonging to an Administration group. *Do not use the default Administrator account*.

Warning: If you leave the password field empty, the clone operation will fail.

7. At **Product Key**, enter the key to use for the virtual machine, or check the box indicating that you will use an Answer File for this information.

8. At **Operating System**, select the appropriate OS.

9. Click the radio button for **Workgroup**. Click **Next**.

10. Select the host on which to place the template.

11. Select the location to place the template.

12. Click **Create** to create the new template.

Clone with Optional Guest OS Profile

To clone with Optional Guest OS Profile:

By default, a template already has a copy of the GuestOS profile. Pano Controller lets you replace the embedded GuestOS profile with an external GuestOS profile.

1. Create a new GuestOS Profile using the SCVMM Administrator Console.
2. From Pano Controller, specify the optional GuestOS Profile in the Deployment tab of a collection.

This profile supersedes the Guest OS specified in the Template. Alternately, you can modify the OS Configuration settings in the Template.

To create a clone from a template:

1. At the **SCVMM Administrator Console**, ensure that all apps are closed in the VM.
2. At the list of Virtual Machines, select a machine to use, and stop the virtual machine.
3. Right-click the stopped machine and select Create clone.

   Warning: If you see a message about destroying the source virtual machine and user data on it, you are creating a new template and not a clone. Unless this is your intention, click Cancel and start again.

4. In **Clone Identity**, enter a name for the clone and click **Next**.
5. In **Configure Hardware**, go to Hardware profile, Bus Configuration and verify that a hard disk or other IDE device is present.
6. At **Network Adapters,** confirm that Network Location is set to the correct domain. Click **Next**.

Note: If you don't see your domain in the drop-down menu, this means that you have a configuration issue. The DNS suffix needs to be set on the SCVMM network adapter.

7. At **Guest Operating System**, go to **General Settings**.

Note: The **Operating System Profile**, or **Guest Operating System**, allows you to specify the identity, network settings and scripts, if any, for the new virtual machine.

- At **Identify information**, enter the full name of the computer. To randomly select a computer name, use the asterisk (*).
- During this process, the VM's computer name is replaced with the VM's name you specified in the Deployment tab of collection.

  Warning: If you don't provide the full computer name, the clone operation will fail.

8. At **Admin Password**, for Windows7 OS, provide an account belonging to an Administration group. *Do not use the default Administrator account*.

   Warning: If you leave the password field empty, the clone operation will fail.

9. At **Product Key**, enter the key to use for the virtual machine, or check the box indicating that you will use an Answer File for this information.
10. At **Operating System**, select your OS.
11. At **Domain/Workgroup**, specify the domain in Domain user field.
12. Select the host on which to place the template.
13. Select the location to place the template.
14. Click Create to create the new template clone

30

Pano Direct Service Mass Installation

Pano Direct Service (PDS) is the drive package that handles communication between the user's virtual machine and the actual endpoint hardware. There is a version of PDS for Windows XP and a version for Windows 7.

Installation is the same regardless of the virtualization platform. The Pano Direct Service Wizard walks you through the installation of the Pano Direct Service. You must install the Pano Direct Service on all DVMs that you want to access from a Pano System Endpoint.

It's best to start with a single DVM installation, then test it, before proceeding to mass installation.

This chapter includes the following topics:

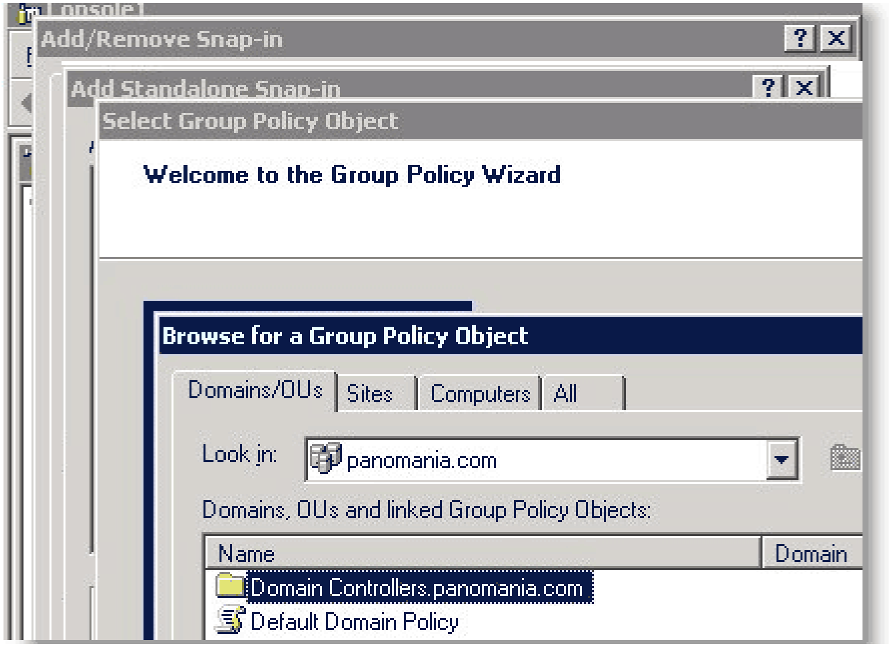
Install Pano Direct Service on multiple DVMs using AD

Note: The following example is for Windows Server 2003, but the concept is the same in later versions of Windows Server.

If your company deploys a large number of desktop virtual machines (10+), consider updating Pano Direct Service on those desktop virtual machines in an automated manner.

- If your company does not use Active Directory, you can use Microsoft System Management Server (SMS) instead.
- If your company uses Active Directory, perform the following procedure.

1. Add the Group Policy Editor Snap-in to MMC on the AD Domain Controller. In this example, the domain name is panomania.com.



Welcome to the Group Policy Wizard

Look in: panomania.com

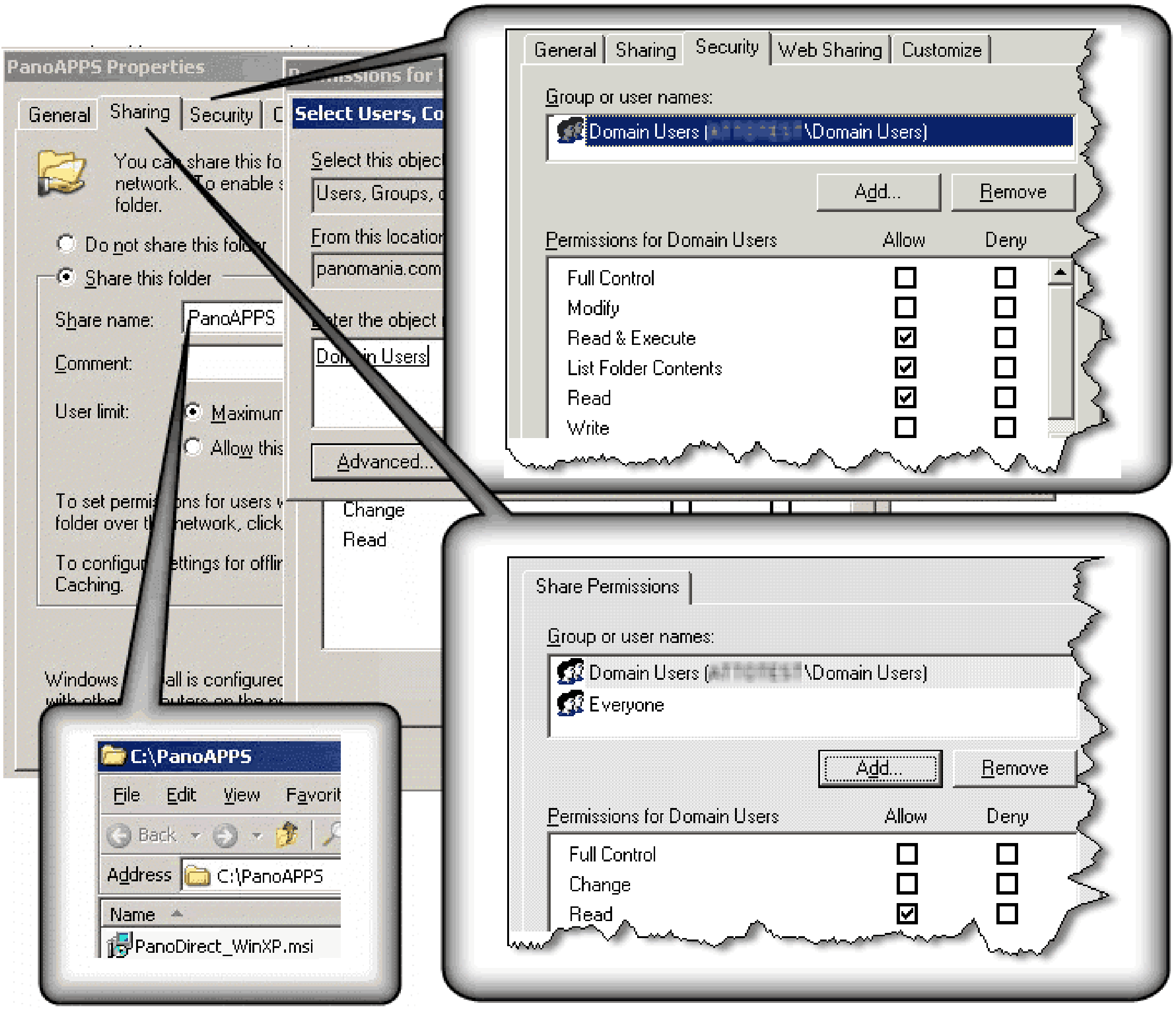
Domains, OUs and linked Group Policy Objects:

Domain Controllers.panomania.com

Default Domain Policy

2. Copy the `PanoDirect.msi` file to a folder on the Domain Controller server, then make sure that the folder is shared so that your users have Read access it:
   - **Sharing** tab > **Read**
   - **Security** tab > **Read & Execute**, **List Folder Contents**, and **Read**.

   In this example, the folder is `PanoAPPS`.



Security, Permissions for Domain Users:

Permissions for Domain Users	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□

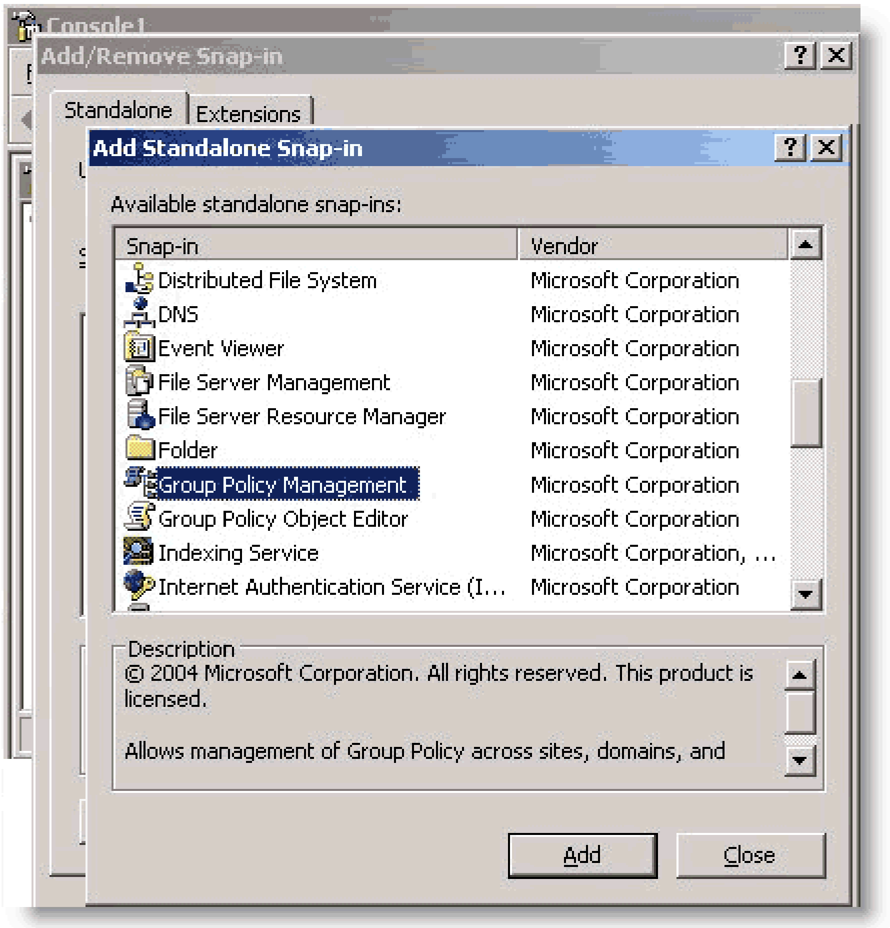
Share Permissions, Permissions for Domain Users:

Permissions for Domain Users	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

3. Download the Pano Direct Service`.msi` file into the folder.

4. (Optional) Prevent the Pano Control Panel from launching after the installer completes. Refer to How do I prevent the Pano Control Panel from launching after a silent install?.

5. Add Group Policy Management Snap-In to MMC.



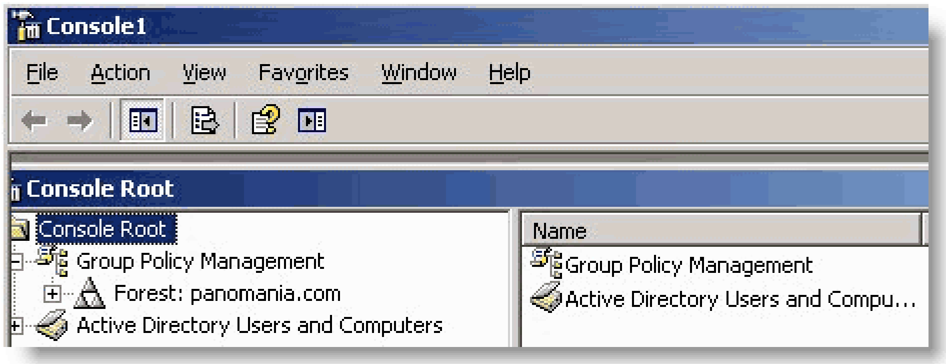
Available standalone snap-ins:

Snap-in	Vendor
Distributed File System	Microsoft Corporation
DNS	Microsoft Corporation
Event Viewer	Microsoft Corporation
File Server Management	Microsoft Corporation
File Server Resource Manager	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy Management	Microsoft Corporation
Group Policy Object Editor	Microsoft Corporation
Indexing Service	Microsoft Corporation, ...
Internet Authentication Service (I...	Microsoft Corporation

Description
© 2004 Microsoft Corporation. All rights reserved. This product is licensed.

Allows management of Group Policy across sites, domains, and

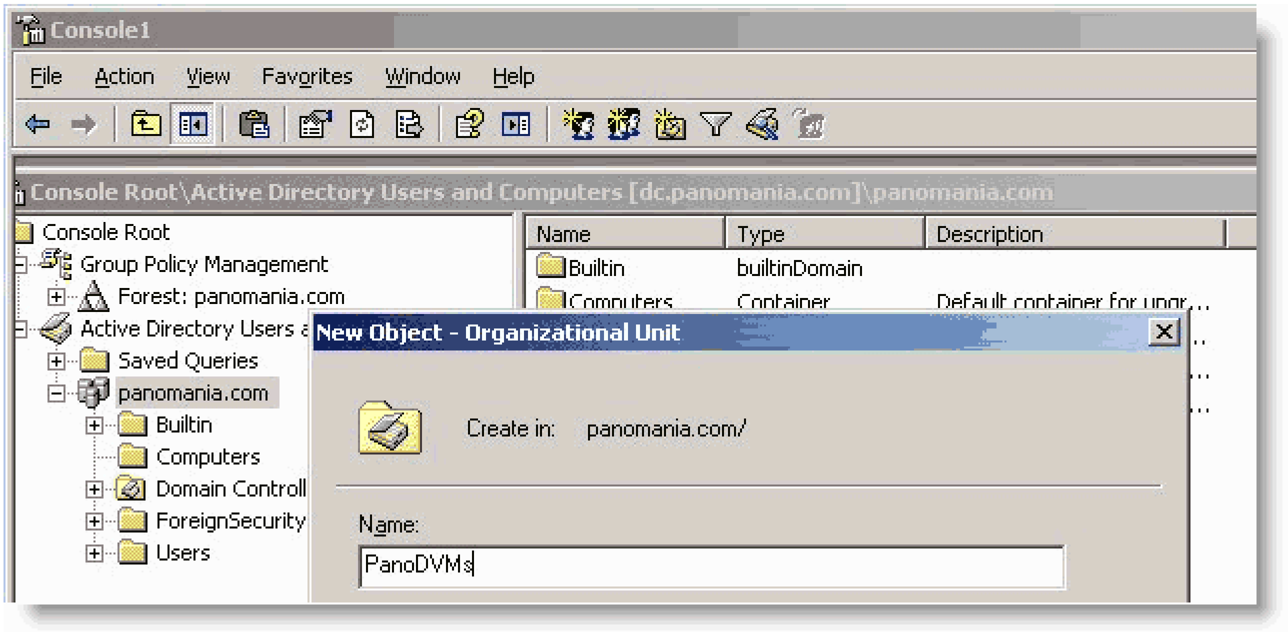
6. Add Active Directory Users and Computers Snap-In.



Console Root
- Group Policy Management
  - Forest: panomania.com
- Active Directory Users and Computers

Name
Group Policy Management
Active Directory Users and Compu...

7. Create new OU for DVMs. Put all DVMs in that OU.



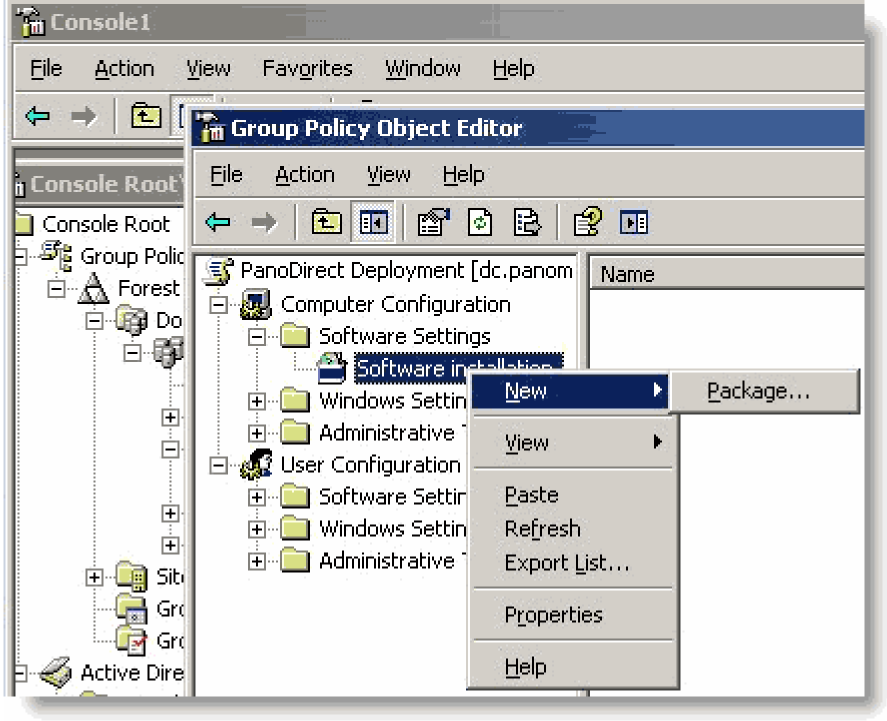
Create in: panomania.com/

Name: PanoDVMs

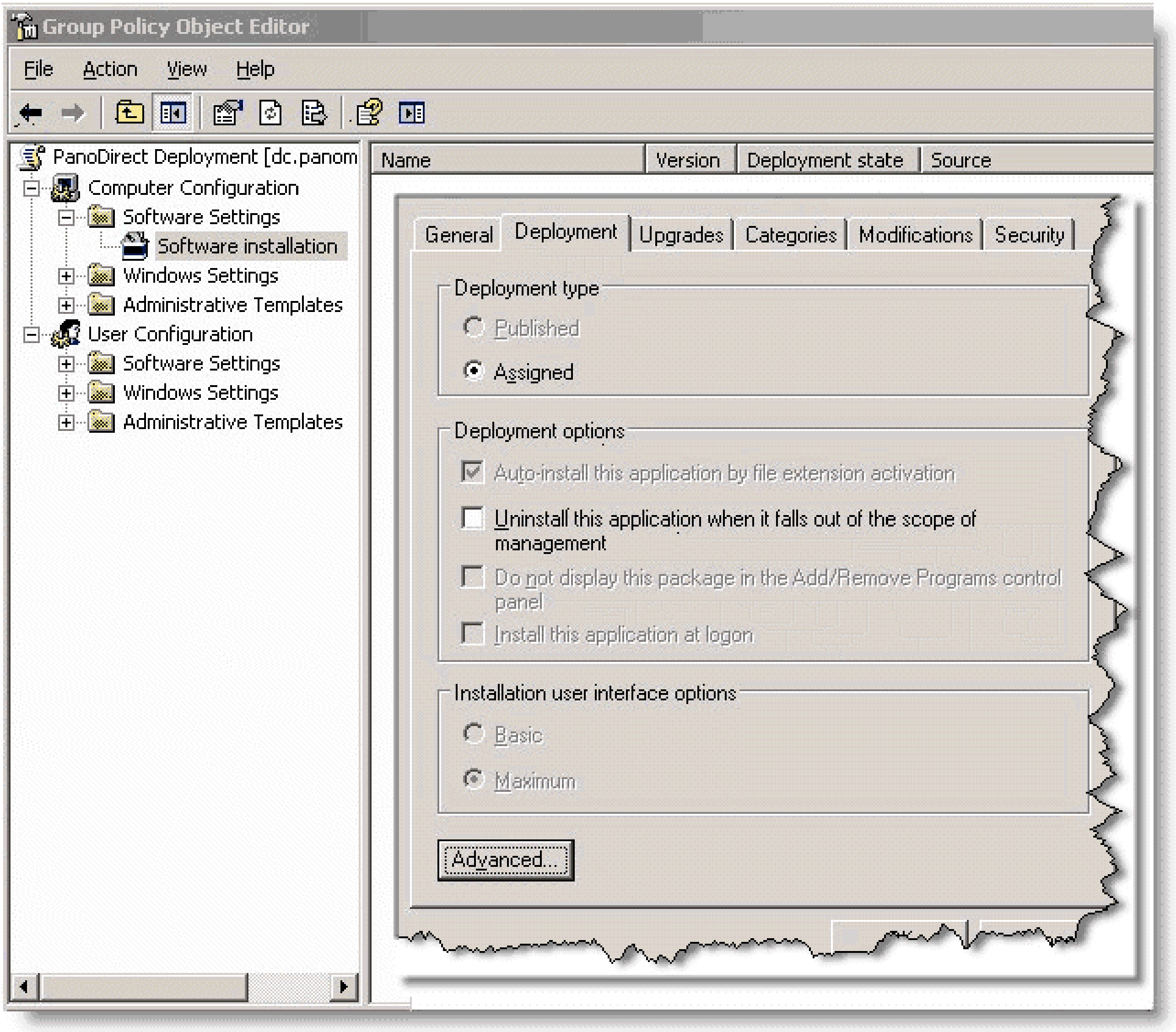
8. Right-click on the OU that you just created, choose **Create and link a GPO Here...**, give the New GPO a name, then click **OK**.

9. Edit Group Policy on the AD Server.

10. Create new software package for Pano Direct Service deployment.



11. Through the network path on the AD Server, select the Pano Direct Service MSI file, then set the properties of the MSI deployment.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

☐ Uninstall this application when it falls out of the scope of management

☐ Do not display this package in the Add/Remove Programs control panel

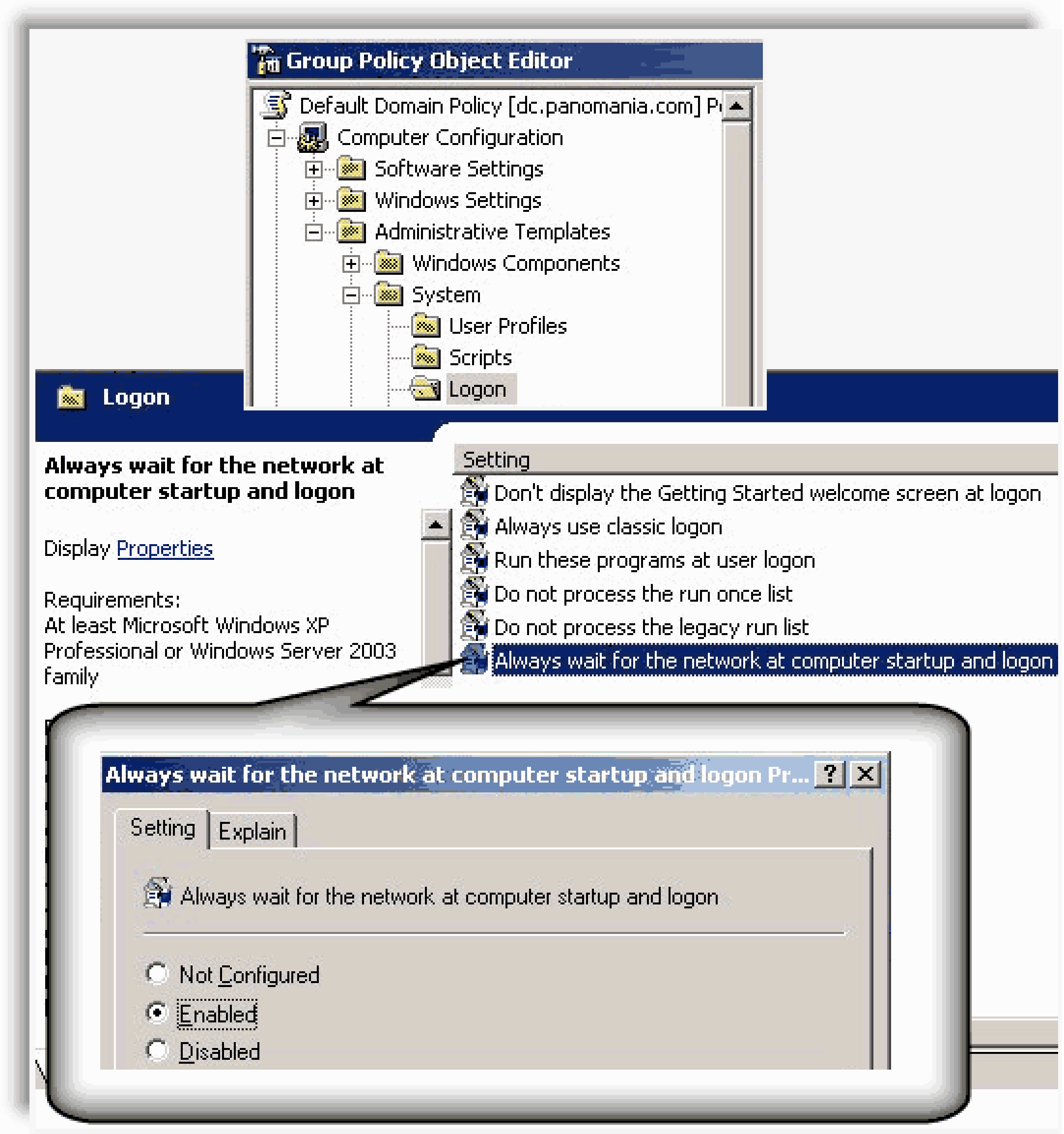
☐ Install this application at logon

Installation user interface options

○ Basic

● Maximum

12. Set the **Always wait for the network at computer startup and logon** setting to `Enabled`.



Always wait for the network at computer startup and logon

Display Properties

Requirements:
At least Microsoft Windows XP Professional or Windows Server 2003 family

Setting
Don't display the Getting Started welcome screen at logon
Always use classic logon
Run these programs at user logon
Do not process the run once list
Do not process the legacy run list
Always wait for the network at computer startup and logon

Always wait for the network at computer startup and logon Pr... ? ✕

Setting | Explain

Always wait for the network at computer startup and logon

○ Not Configured
● Enabled
○ Disabled

13. Enable a silent installation:
    - (Windows 7) Go to Install Certificate for Pano Direct Service Drivers.
    - (Windows XP) Go to Enable Silent Installation for Windows XP.

When the DVMs boot, Pano Direct Service is installed during the DVMs' startup process. Afterward, the DVMs automatically reboot. Only after this final reboot will the installation take effect.

Note:

To install Pano Direct Service on all DVMs simultaneously using SMS:

For instructions, email Pano Logic Technical Support at support@panologic.com.

What to do next:

Deploy Pano Direct Service Using Microsoft System Management Server

If your company deploys a large number of desktop virtual machines, consider updating Pano Direct Service on those virtual desktops in an automated manner.

- If your company does not use SMS, you can use AD instead.
- If your company uses Microsoft System Management Server (SMS), perform the following procedure.

A Pano Direct Service deployment using Microsoft System Management Server (SMS) consists of a few main steps:

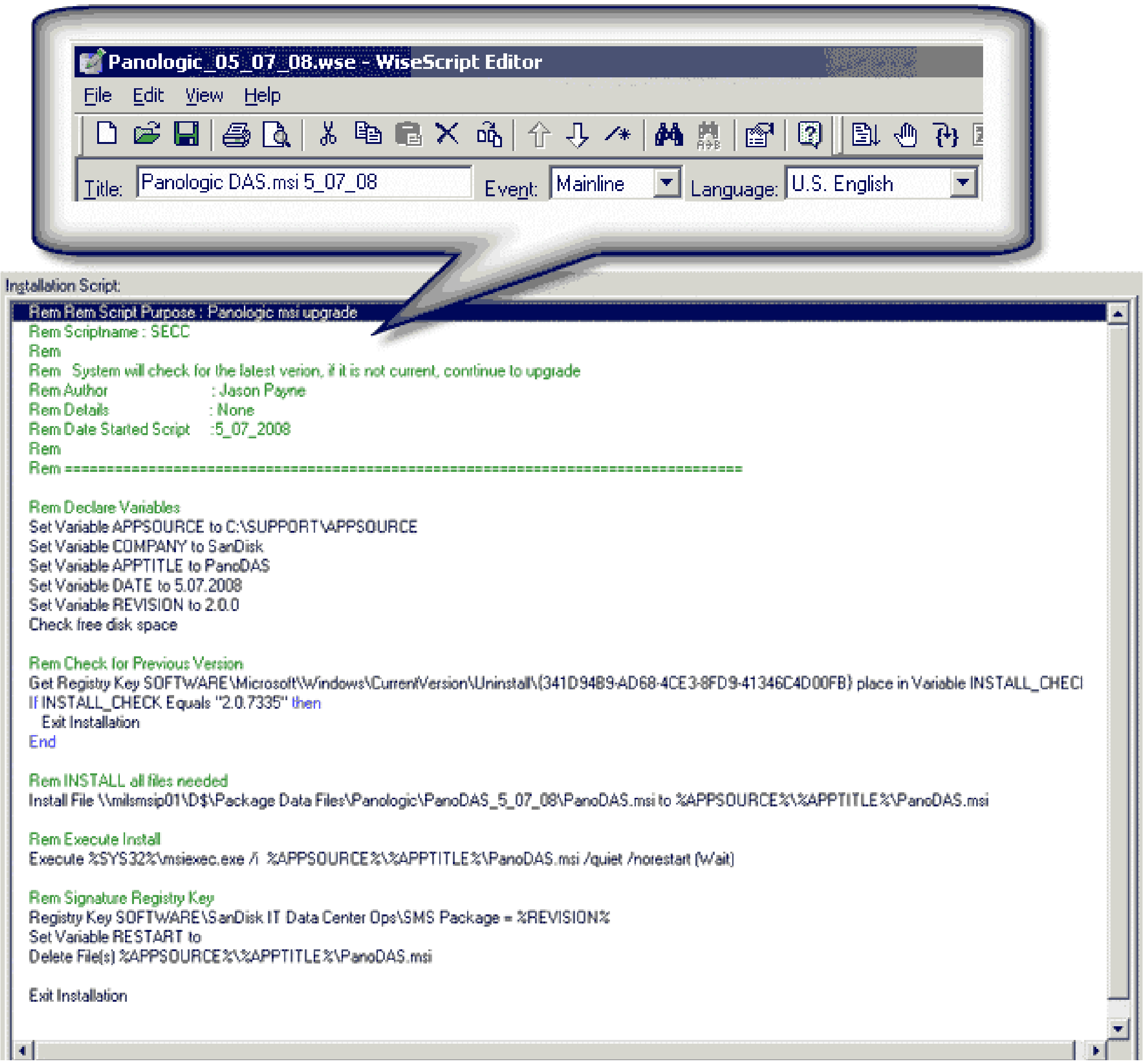
1. Create the deployment package.
2. Create the collection of machines to which the package will be deployed.
3. Create the advertisement so that the machines in the collection discover the package.

To deploy Pano Direct Service using SMS:

1. (Optional) Create the deployment package.

   This step is optional because the `PanoDAS.msi` file can also be deployed directly. The following example uses a third-party packaging tool called Altiris Wise Installation Studio (renamed *Wise Package Studio*).

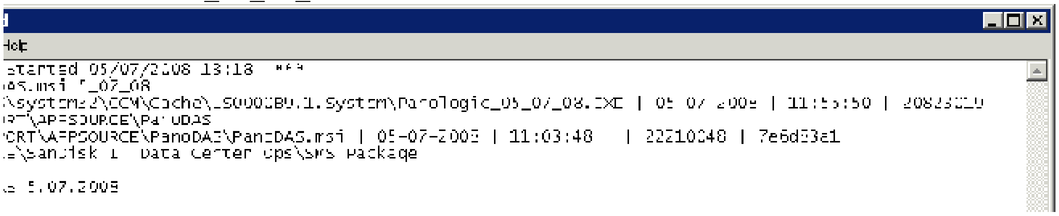
   As the following screen shot shows, the WiseScript Editor script checks in a version that is greater than the version that you want to install. If the version is *not* greater than the version that is already installed, the script does not create the deployment package.



Title: Panologic DAS.msi 5_07_08   Event: Mainline   Language: U.S. English

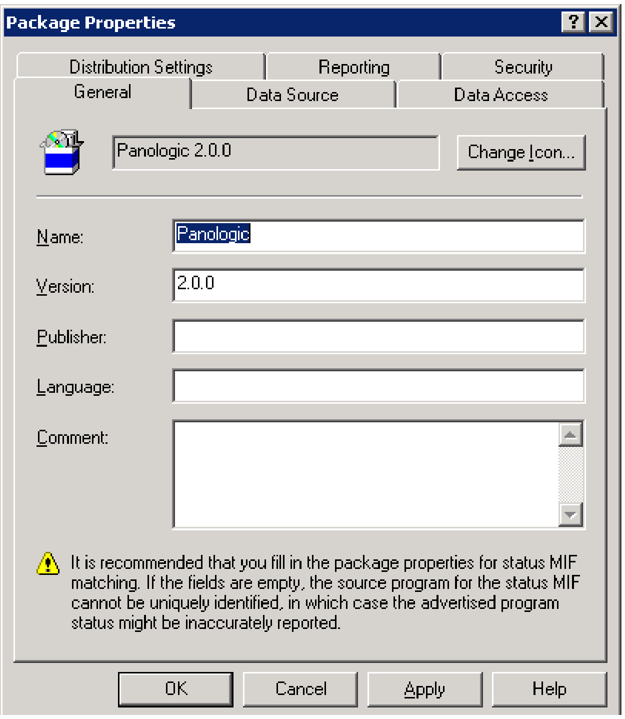
```
Rem Rem Script Purpose : Panologic msi upgrade
Rem Scriptname : SECC
Rem
Rem   System will check for the latest verion, if it is not current, continue to upgrade
Rem Author                    : Jason Payne
Rem Details                   : None
Rem Date Started Script       :5_07_2008
Rem
Rem ==============================================================================

Rem Declare Variables
Set Variable APPSOURCE to C:\SUPPORT\APPSOURCE
Set Variable COMPANY to SanDisk
Set Variable APPTITLE to PanoDAS
Set Variable DATE to 5.07.2008
Set Variable REVISION to 2.0.0
Check free disk space

Rem Check for Previous Version
Get Registry Key SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{341D9489-AD68-4CE3-8FD9-41346C4D00FB} place in Variable INSTALL_CHECI
If INSTALL_CHECK Equals "2.0.7335" then
  Exit Installation
End

Rem INSTALL all files needed
Install File \\milsmsip01\D$\Package Data Files\Panologic\PanoDAS_5_07_08\PanoDAS.msi to %APPSOURCE%\%APPTITLE%\PanoDAS.msi

Rem Execute Install
Execute %SYS32%\msiexec.exe /i  %APPSOURCE%\%APPTITLE%\PanoDAS.msi /quiet /norestart (Wait)

Rem Signature Registry Key
Registry Key SOFTWARE\SanDisk IT Data Center Ops\SMS Package = %REVISION%
Set Variable RESTART to
Delete File(s) %APPSOURCE%\%APPTITLE%\PanoDAS.msi

Exit Installation
```

2. Compile the script into an executable file. In this case the name of the executable is `Panologic_05_07_08.EXE`.



```
started 05/07/2008 13:18  ***
AS.msi 5_07_08
\system32\CCM\Cache\_S000CBU.1.System\Panologic_05_07_08.EXE | 05 07 2008 | 11:55:50 | 2082[illegible]
RT\APPSOURCE\PanoDAS
CRT\APPSOURCE\PanoDAS\PanoDAS.msi | 05-07-2008 | 11:03:48   | 22210048 | 7e6d33a1
e\SanDisk IT Data Center Ops\SMS Package

e 5.07.2008
```

3. Create a new package in SMS. The following screen shot shows the properties of the package in SMS.
   - Specify the name and version.



Panologic 2.0.0

Name: Panologic

Version: 2.0.0

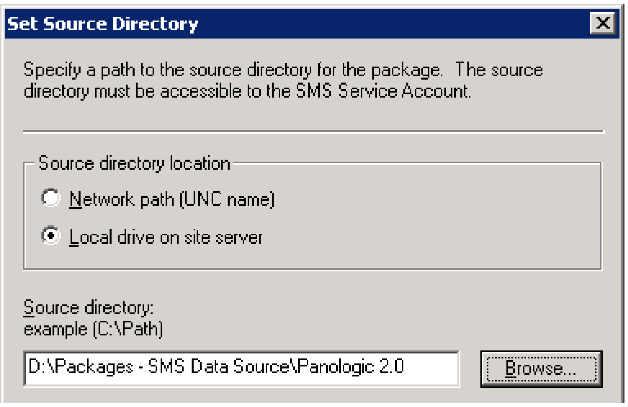
Publisher:

Language:

Comment:

It is recommended that you fill in the package properties for status MIF matching. If the fields are empty, the source program for the status MIF cannot be uniquely identified, in which case the advertised program status might be inaccurately reported.

   - Specify the Source Directory.



Specify a path to the source directory for the package. The source directory must be accessible to the SMS Service Account.

Source directory location

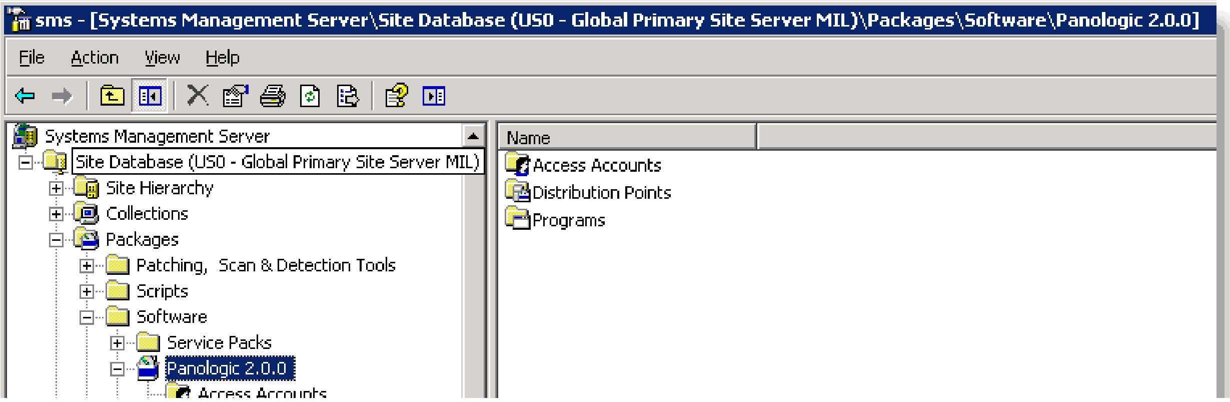
○ Network path (UNC name)

● Local drive on site server

Source directory:
example (C:\Path)

D:\Packages - SMS Data Source\Panologic 2.0

The SMS Console shows the new package.



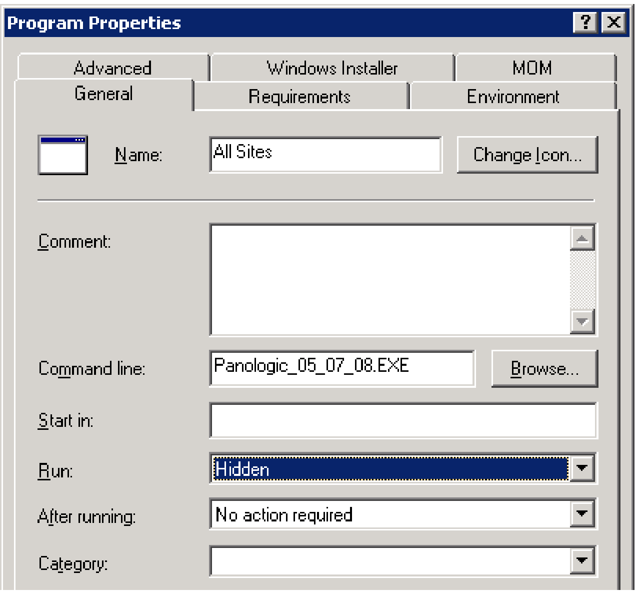
sms - [Systems Management Server\Site Database (US0 - Global Primary Site Server MIL)\Packages\Software\Panologic 2.0.0]

- Systems Management Server
  - Site Database (US0 - Global Primary Site Server MIL)
    - Site Hierarchy
    - Collections
    - Packages
      - Patching, Scan & Detection Tools
      - Scripts
      - Software
        - Service Packs
        - Panologic 2.0.0
          - Access Accounts

Name
Access Accounts
Distribution Points
Programs

4. Define the Package behavior:

   a. Specify the executable, etc.: **Program Properties** > **General**.



Name: All Sites

Comment:

Command line: Panologic_05_07_08.EXE

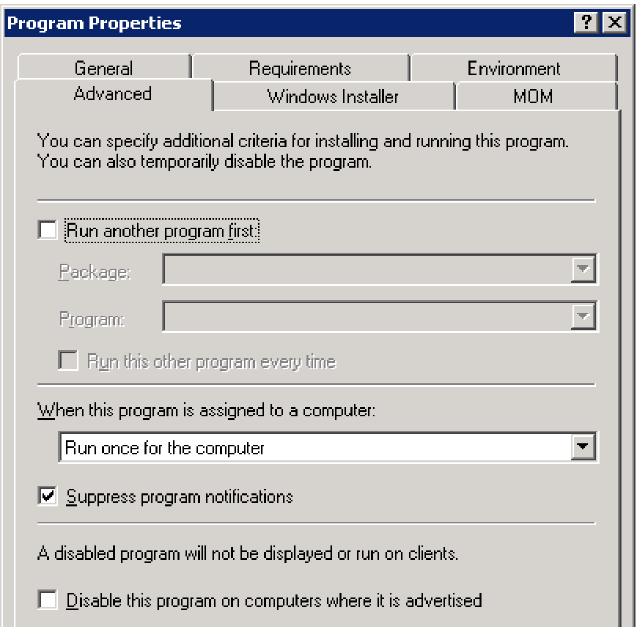
Start in:

Run: Hidden

After running: No action required

Category:

   b. Specify that the program run once: **Program Properties** > **Advanced**.



You can specify additional criteria for installing and running this program. You can also temporarily disable the program.

□ Run another program first

Package:

Program:

□ Run this other program every time

When this program is assigned to a computer:

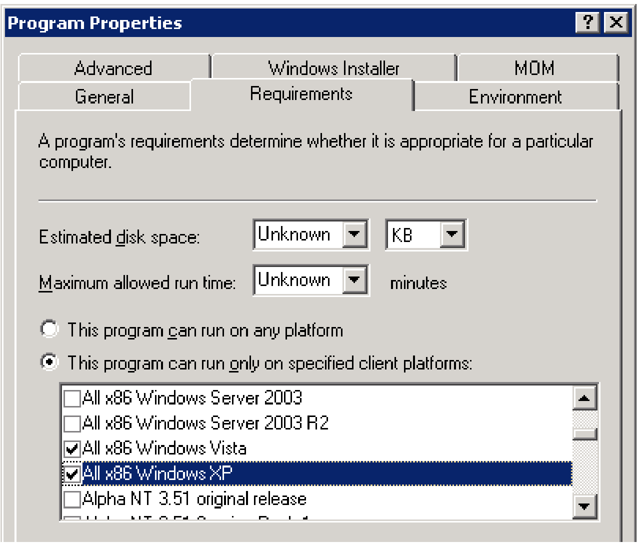
Run once for the computer

☑ Suppress program notifications

A disabled program will not be displayed or run on clients.

□ Disable this program on computers where it is advertised

c. Specify the DVMs on which the Pano Direct Service package can run: **Program Properties** > **Requirements**.



A program's requirements determine whether it is appropriate for a particular computer.

Estimated disk space: Unknown KB

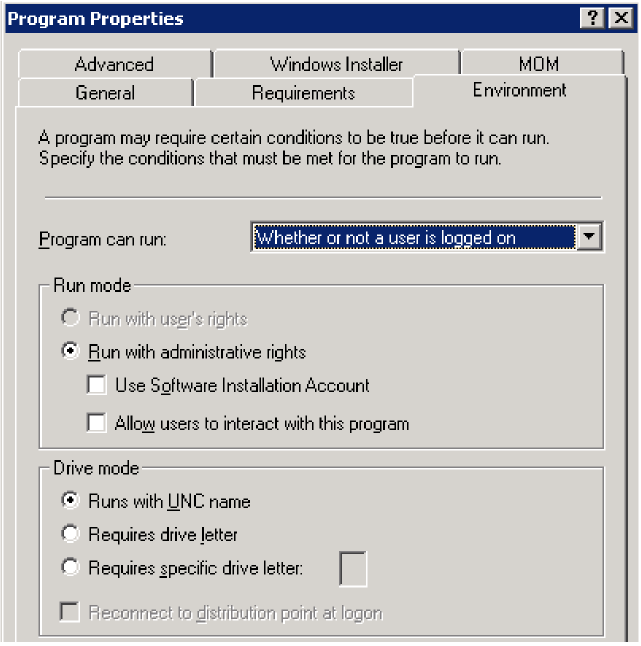
Maximum allowed run time: Unknown minutes

○ This program can run on any platform

● This program can run only on specified client platforms:

- □ All x86 Windows Server 2003
- □ All x86 Windows Server 2003 R2
- ☑ All x86 Windows Vista
- ☑ All x86 Windows XP
- □ Alpha NT 3.51 original release

5. Specify conditions under which the script can run: **Program Properties** > **Environment**.



A program may require certain conditions to be true before it can run. Specify the conditions that must be met for the program to run.

Program can run: Whether or not a user is logged on

Run mode

○ Run with user's rights

● Run with administrative rights

□ Use Software Installation Account

□ Allow users to interact with this program

Drive mode

● Runs with UNC name

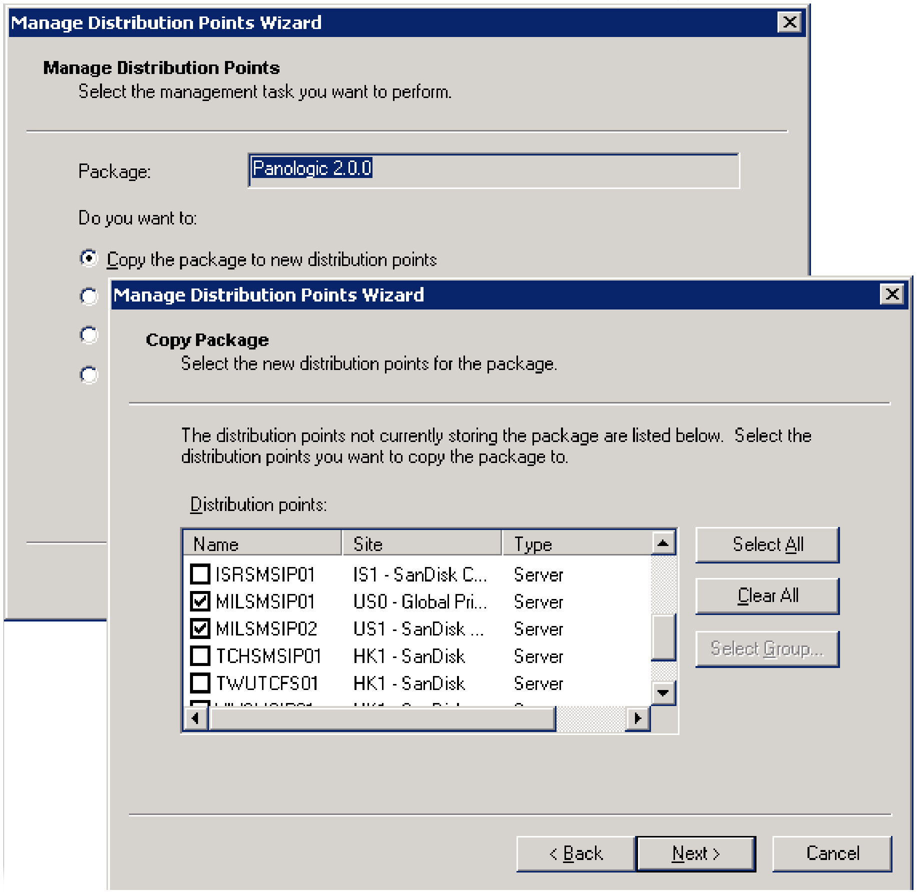
○ Requires drive letter

○ Requires specific drive letter: □

□ Reconnect to distribution point at logon

6. Configure the distribution points: right-click on Distribution, select the **Copy the package to the new distribution points** radio button, then choose the distribution points.

   Go to the Console View to monitor the package status.



Manage Distribution Points Wizard

Manage Distribution Points
Select the management task you want to perform.

Package: Panologic 2.0.0

Do you want to:

● Copy the package to new distribution points
○
○
○

Manage Distribution Points Wizard

Copy Package
Select the new distribution points for the package.

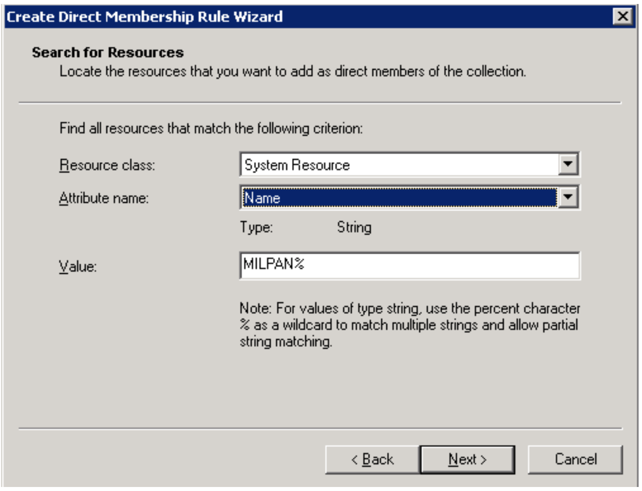
The distribution points not currently storing the package are listed below. Select the distribution points you want to copy the package to.

Distribution points:

Name	Site	Type
□ ISRSMSIP01	IS1 - SanDisk C...	Server
☑ MILSMSIP01	US0 - Global Pri...	Server
☑ MILSMSIP02	US1 - SanDisk ...	Server
□ TCHSMSIP01	HK1 - SanDisk	Server
□ TWUTCFS01	HK1 - SanDisk	Server

7. Create Membership Rule. Using a wildcard, specify a number of Pano Logic systems.

   The following example specifies that the package be distributed to all machines whose names start with MILPAN.



Create Direct Membership Rule Wizard

Search for Resources
Locate the resources that you want to add as direct members of the collection.

Find all resources that match the following criterion:

Resource class: System Resource

Attribute name: Name

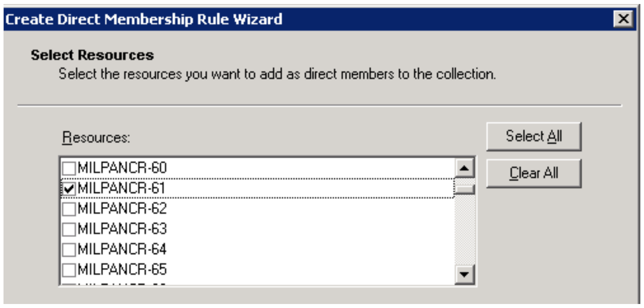
Type: String

Value: MILPAN%

Note: For values of type string, use the percent character % as a wildcard to match multiple strings and allow partial string matching.

8. Select SMS resources. Specify the machines on which you want to install the package within the membership.

   In this following example, MILPANCR-61 and MILPANCR-79 were selected.



Create Direct Membership Rule Wizard

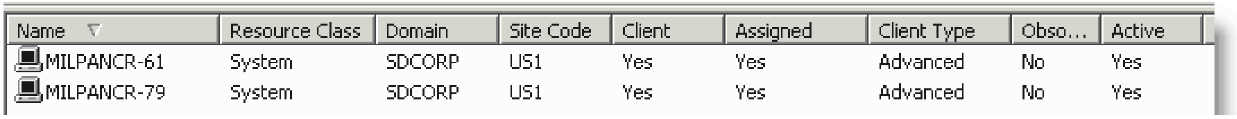
Select Resources

Select the resources you want to add as direct members to the collection.

Resources:

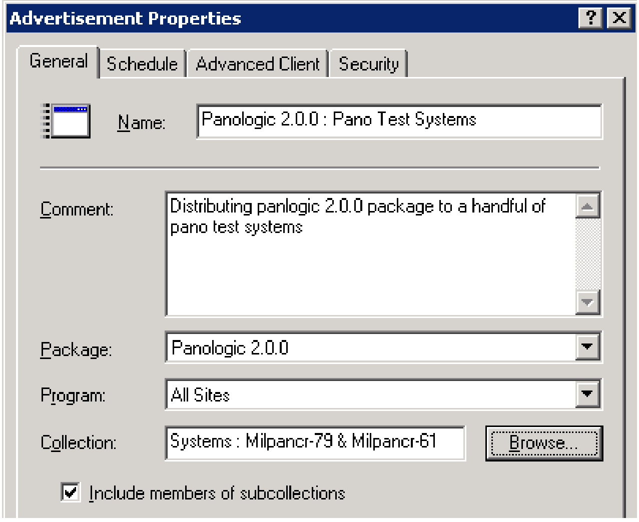
- ☐ MILPANCR-60
- ☑ MILPANCR-61
- ☐ MILPANCR-62
- ☐ MILPANCR-63
- ☐ MILPANCR-64
- ☐ MILPANCR-65

   The SMS console shows current collection.



Name	Resource Class	Domain	Site Code	Client	Assigned	Client Type	Obso...	Active
MILPANCR-61	System	SDCORP	US1	Yes	Yes	Advanced	No	Yes
MILPANCR-79	System	SDCORP	US1	Yes	Yes	Advanced	No	Yes

9. Create the advertisement so that the DVMs in the collection discover the package.



Advertisement Properties

Name: Panologic 2.0.0 : Pano Test Systems

Comment: Distributing panlogic 2.0.0 package to a handful of pano test systems

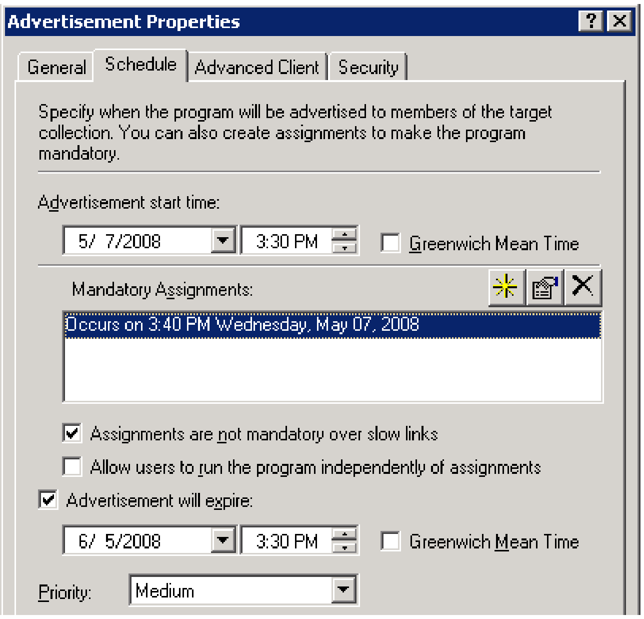
Package: Panologic 2.0.0

Program: All Sites

Collection: Systems : Milpancr-79 & Milpancr-61

☑ Include members of subcollections

10. Schedule the advertisement.



Advertisement Properties

Specify when the program will be advertised to members of the target collection. You can also create assignments to make the program mandatory.

Advertisement start time:

5/ 7/2008 3:30 PM □ Greenwich Mean Time

Mandatory Assignments:

Occurs on 3:40 PM Wednesday, May 07, 2008

☑ Assignments are not mandatory over slow links

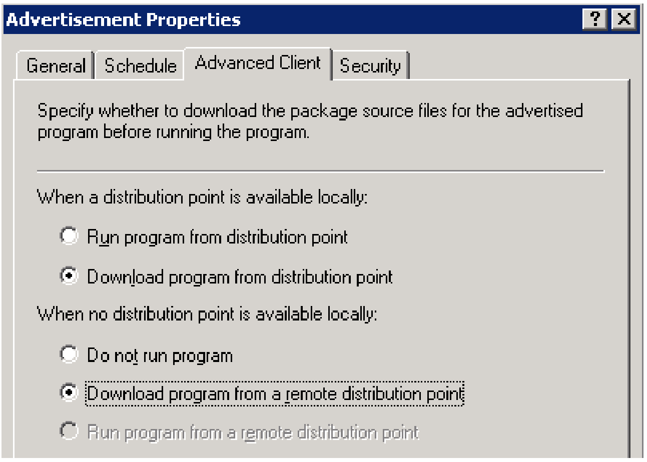
□ Allow users to run the program independently of assignments

☑ Advertisement will expire:

6/ 5/2008 3:30 PM □ Greenwich Mean Time

Priority: Medium

11. Download the program from the distribution point.



Advertisement Properties

Specify whether to download the package source files for the advertised program before running the program.

When a distribution point is available locally:

○ Run program from distribution point

● Download program from distribution point

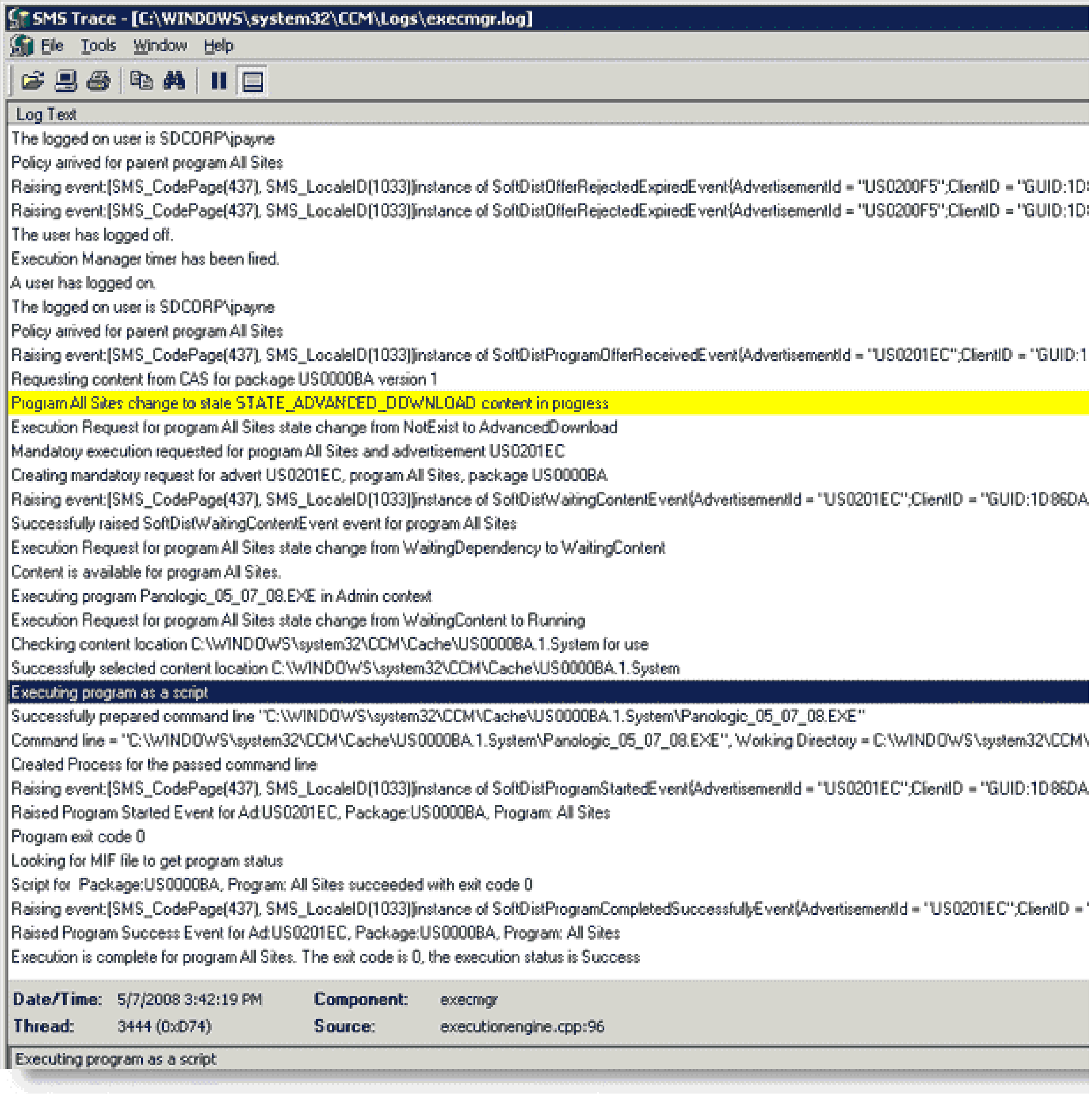
When no distribution point is available locally:

○ Do not run program

● Download program from a remote distribution point

○ Run program from a remote distribution point

After you run the Pano Direct Service package, view the MS Log File, execmgr.log, on the DVM.



```
The logged on user is SDCORP\jpayne
Policy arrived for parent program All Sites
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistOfferRejectedExpiredEvent{AdvertisementId = "US0200F5";ClientID = "GUID:1D
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistOfferRejectedExpiredEvent{AdvertisementId = "US0200F5";ClientID = "GUID:1D
The user has logged off.
Execution Manager timer has been fired.
A user has logged on.
The logged on user is SDCORP\jpayne
Policy arrived for parent program All Sites
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramOfferReceivedEvent{AdvertisementId = "US0201EC";ClientID = "GUID:1
Requesting content from CAS for package US0000BA version 1
Program All Sites change to state STATE_ADVANCED_DOWNLOAD content in progress
Execution Request for program All Sites state change from NotExist to AdvancedDownload
Mandatory execution requested for program All Sites and advertisement US0201EC
Creating mandatory request for advert US0201EC, program All Sites, package US0000BA
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistWaitingContentEvent{AdvertisementId = "US0201EC";ClientID = "GUID:1D86DA
Successfully raised SoftDistWaitingContentEvent event for program All Sites
Execution Request for program All Sites state change from WaitingDependency to WaitingContent
Content is available for program All Sites.
Executing program Panologic_05_07_08.EXE in Admin context
Execution Request for program All Sites state change from WaitingContent to Running
Checking content location C:\WINDOWS\system32\CCM\Cache\US0000BA.1.System for use
Successfully selected content location C:\WINDOWS\system32\CCM\Cache\US0000BA.1.System
Executing program as a script
Successfully prepared command line "C:\WINDOWS\system32\CCM\Cache\US0000BA.1.System\Panologic_05_07_08.EXE"
Command line = "C:\WINDOWS\system32\CCM\Cache\US0000BA.1.System\Panologic_05_07_08.EXE", Working Directory = C:\WINDOWS\system32\CCM\
Created Process for the passed command line
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramStartedEvent{AdvertisementId = "US0201EC";ClientID = "GUID:1D86DA
Raised Program Started Event for Ad:US0201EC, Package:US0000BA, Program: All Sites
Program exit code 0
Looking for MIF file to get program status
Script for  Package:US0000BA, Program: All Sites succeeded with exit code 0
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramCompletedSuccessfullyEvent{AdvertisementId = "US0201EC";ClientID = "
Raised Program Success Event for Ad:US0201EC, Package:US0000BA, Program: All Sites
Execution is complete for program All Sites. The exit code is 0, the execution status is Success
```

Date/Time: 5/7/2008 3:42:19 PM **Component:** execmgr
Thread: 3444 (0xD74) **Source:** executionengine.cpp:96

Executing program as a script

Enable Silent Installation for Windows XP

A silent installation (such as a *GPO install*) makes the Pano Direct Service installation transparent to your users. It does not require user interaction. Pano Direct Service contains three drivers which are signed in XP (display, keyboard/mouse, and audio). Therefore, you need to perform the following procedure before you can deploy via GPO.

Note: There is no need to enable a silent install for Windows 7 because the Pano Direct Service software includes digitally signed drivers; simply install the certificates.

To enable a silent installation:

This summarizes what’s in Microsoft KB 945250; The same steps work on Vista or Server.

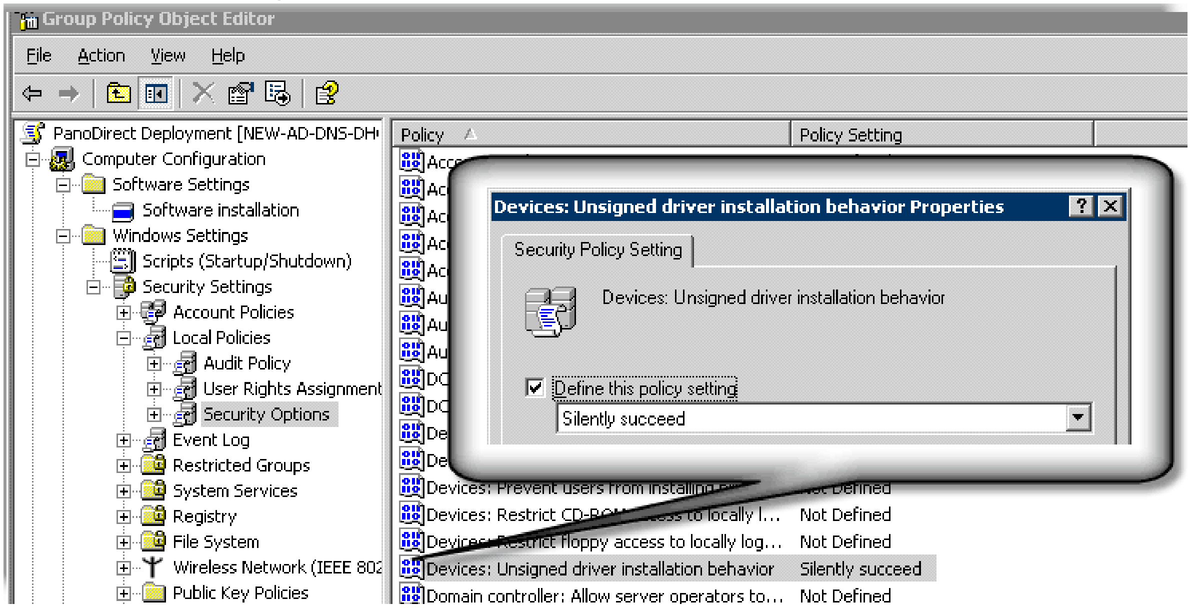
Before You Begin: Ensure that your Windows Server version is supported. Go to Windows Server Support.

1. As admin, take ownership of `Sceregvl.inf`. This file is usually in `c:\windows\inf`.
2. Modify the `Sceregvl.inf` file, then re-register the `Scecli.dll` file:
3. Back up the `Sceregvl.inf` file.
4. Open the `Sceregvl.inf` file, and add to the [Register Registry Values] section:

```
MACHINE\Software\Microsoft\Driver Signing\Policy,3, "Devices: Unsigned driver
installation behavior",3,0| DriverSigning0="Silently succeed ",1|"Warn but allow
installation",2|"Do not allow installation"
```

5. From a command prompt, type **`regsvr32 scecli.dll`**

To enable silent installation in Windows Server 2003, modify unsigned device driver installation to silently succeed:


Group Policy Object Editor
File
Action
View
Help
PanoDirect Deployment [NEW-AD-DNS-DH
Computer Configuration
Software Settings
Software installation
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wireless Network (IEEE 802
Public Key Policies
Policy
Policy Setting
Devices: Prevent users from installing p...
Devices: Restrict CD-ROM access to locally l...
Devices: Restrict floppy access to locally log...
Domain controller: Allow server operators to...

Policy	Policy Setting
Devices: Restrict CD-ROM access to locally l...	Not Defined
Devices: Restrict floppy access to locally log...	Not Defined
Devices: Unsigned driver installation behavior	Silently succeed
Domain controller: Allow server operators to...	Not Defined

Devices: Unsigned driver installation behavior Properties

Security Policy Setting

Devices: Unsigned driver installation behavior

☑ Define this policy setting

Silently succeed

Related Topics

How do I prevent the Pano Control Panel from launching after a silent install?

VMware Disposable Desktops

Upgrade Pano Direct Service

31
Set Up Desktop Brokering

The desktop broker is the part of the system that associates users and devices with the assigned desktop virtual machines. Desktop brokering may also deal with provisioning, starting up and shutting down desktops based on policies defined by the administrator.

With the Pano System you have the choice of which brokers to use. The Pano System supports the Pano Controller's built-in connection broker, called the Pano Virtual Desktop Broker (VDB). You can also use XenDesktop or VMware View for brokering.

The Pano System uses a DVM Collection to store the policies related to desktop brokering. You can set up and manage DVM Collections from the DVM Collections tab in the Pano Controller console. The settings available to you within a DVM Collection vary depending on which connection broker you use. Select the appropriate topic below based on your chosen connection broker.

- DVM Collections for Pano Virtual Desktop Broker
- DVM Collections for XenDesktop
- XenDesktop VMware ESX Server Setup Issues
- DVM Collections for VMware View

DVM Collections for Pano Virtual Desktop Broker

Before you configure DVM collections for use with the Pano Virtual Desktop Broker, please review DVM Collections and Types of Collections.

The Pano Virtual Desktop Broker is used when your Pano Controller runs in Full Mode or with the Virtual Desktop Broker role selected. Additionally, the Virtualization Configuration section on the Pano Controller Setup tab must be configured and connected to VMware vCenter Server or Microsoft System Center Virtual Machine Manager.

Create DVM Collections–VMware and Hyper-V

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

Task	Go to...
Create Security groups in AD that represent the set of users of the desktop virtual machines. You specify these Security groups when you create the DVM Collections.	Create a New Group
Determine the types of DVM Collection(s) that you need.	Choose DVM Collection Type DVM Collections
Create a folder structure to help you organize your DVMs.	Create Virtualization Hierarchy–VMware DVM Collections
Determine if you need device restrictions. You can add these restrictions after you create the DVM Collection.	Use Cases for Device Restrictions
Create the DVM Collection	Create DVM Collections
Assign Pano System Endpoints to DVMs	Assign Pano Zero Clients and Users To DVMs
Verify that the DVM Collection is working properly.	Deploy Resources
Set up the DVM Collection with device restrictions, if you didn’t do so when you created the DVM Collection.	Set Up Collections with Device Restrictions

DVM Collections for XenDesktop

When you use XenDesktop as your connection broker, the Pano Controller delegates connection brokering functionality to the XenDesktop Controller. Assignments that are brokered through XenDesktop are user-based assignments; if you want to support device-based assignments, too, you will need to configure a Pano.

When a user types their network credentials into the Pano login screen of a Pano Zero Client the credentials are first routed to the Pano Controller, which authenticates the user credentials against the directory service. Upon successful authentication, the Pano Controller queries the XenDesktop Controller for the user's desktop assignments. The Pano Controller will next establish the connection directly from the Pano Zero Client to the target desktop.

In order to use XenDesktop as your connection broker, you must enter the address of the XenDesktop Controller on the Setup tab of the Pano Controller console. When Pano Controller connects to the designated Desktop Controller for the first time, it automatically creates a DVM collection of the appropriate type (Citrix XenDesktop.)

By default the built-in "Domain Users" account is automatically added to this collection. Generally it is best to leave the Accounts field on the Access tab configured for all domain users and allow XenDesktop to handle the account specific brokering. If desirable, you can modify this group and specify a more restrictive set of users who can access virtual desktops from the Pano System.

You can also modify the Pano Remote settings of the collection if you are using Pano Remote for remote access.

XenDesktop VMware ESX Server Setup Issues

The following setup issues may occur when setting up XenDesktop on VMware ESX Server.

- The message "The hypervisor was not contactable" is generated.
- Quick Deploy fails with the message "Exception has been thrown by the target of the invocation".
- Catalog creation fails with the message "There are no master images associated with this catalog".
- Prepare the master image.

The message "The hypervisor was not contactable" is generated.

- VCenter4 (Windows): Install the VCenter 's certificate. For details, see http://jariangibson.com/2010/12/21/using-xendesktop-5-with-vmware/.
- VCenter5 (Linux): Replace the certificate on the VMware vCenter Appliance. By default when VCenter5 linux appliance is deployed, the default certificate for the host name is `localhost.localdom`. Installing the certificate on your DDC server, causes a *MisMatched Address in the Certificate Error Reports* error.

Quick Deploy fails with the message "*Exception has been thrown by the target of the invocation*".

Manually delete file `CitrixXenDesktopDB.mdf` and `CitrixXenDesktopDB_log.LDF` in C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS\MSSQLDATA.

For details, please see http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-known-issues-rho.html.

Catalog creation fails with the message "*There are no master images associated with this catalog*".

The user account (administrator@panotest.local) who is installing and configuring the hypervisor needs to be granted permissions on VMware vCenter. For details, please see http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-vmware-rho.html.

Prepare the master image.

1. Perform a full Windows OS update.
2. Install VMware tools.
3. Install Xen Agent5.5 and click the Advanced Install option. Use the FQDN of theXenDesktop and then click Resolve.
4. Install Pano Direct Service.
5. Add the your domain group to the Remote User Group.
6. Add the your domain group to the Direct RDP Access Administrators.
7. With WinXP, we need to install Microsoft Windows Management Core, which has WRM2.0 and Powershell2.0).

Make sure that the master image and the configuration network in Desktop Studio Configuration are in the same subnet.

DVM Collections for VMware View

When you use VMware View as your connection broker, the Pano Controller delegates connection brokering functionality to the View Connection Server. Assignments that are brokered through View are user-based assignments; if you want to support device-based assignments, too, you will need to configure a Pano Virtual Desktop Broker.

When a user types their network credentials into the Pano login screen of a Pano Zero Client, the credentials are first routed to the Pano Controller, which authenticates the user credentials against the directory service. Upon successful authentication, the Pano Controller queries the View Connection Server for the user's desktop assignments.The Pano Controller will next establish the connection directly from the Pano Zero Client to the target desktop.

In order to use View as your connection broker, you must enter the address of the View Connection Server on the Setup tab of the Pano Controller console. When Pano Controller connects to the designated View Connection Server for the first time, it automatically creates a DVM collection of the appropriate type (VMware View.)

By default the built-in "Domain Users" account is automatically added to this collection. Generally it is best to leave the Accounts field on the Access tab configured for all domain users and allow View to handle the account specific brokering. If desirable, you can modify this group and specify a more restrictive set of users who can access virtual desktops from the Pano System.

You can also modify the Pano Remote settings of the collection if you are using Pano Remote for remote access.

32
Verify DVMs & System Deployment

You'll want to verify DVM connectivity and overall system functionality before putting users on the system. This section explains how. We assume you've already installed at least one Pano System Endpoint, and that it is properly connected to the network. If you're not sure if your Pano System Endpoints are connecting to the network, go to Pano Zero Client Light Indicators.

Verify Additional Newly-Created DVMs

Verifying Overall System Deployment

Verify Additional Newly-Created DVMs

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

1. Log on to the Pano Controller.
2. Click the **DVMs** tab; verify that everything looks okay.

Verify...	Field/Value
The state of the DVM–either **Powered On** or **Powered Off**. The state is derived from information provided by the hypervisor. For XenDesktop, the **DVM State** column is not **applicable**.	**DVM State**
The DMV is powered on. For XenDesktop, **DVM Availability** column is not applicable. If the state is **Powered Off** something might be wrong with the DVM. Log on to the DVM from the console. With an initial deployment, the problem is often the result of an incorrect Windows product key.	**DVM Availability** indicates **PoweredOn**
The DVM has an IP address that was acquired using DHCP. For XenDesktop, **DNS Name** column is not applicable.	**IP Address** and **DNS Name** have appropriate values
The Pano Direct Service is running and responding to status check messages from Pano Controller. See Monitor Pano Direct Service Status.	**Pano Direct Status** indicates **Responding**
The version of Pano Direct Service appears, and is the expected version.	**Pano Direct Version**
The desktop virtual machine shows a user in the field, if you created Types of Collections. If not, that's because you forgot to add users.	**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 endpoints connected, if you created Device Based Collections. If not, no Pano System Endpoint is connected to this DVM. Connect via a Pano System Endpoint to make sure it's working.	**Client**

3. Click the **Pano System Endpoints 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 System Endpoint.	**Connection** indicates DVM or Pano System Endpoint is connected to a DVM
The Pano System Endpoint has a MAC address and IP address	**MAC Address** and **IP Address**
DVM assigned to endpoint in case of device collections. Applies to VDB only	Assignment
Name of Broker that is brokering DVM assigned to the client	Assignment Broker

Related Topics

Troubleshoot DVM Login Problems

Verifying Overall System Deployment

After you complete all the steps in Deploying Your Pano System, verify that your Pano Controller is working correctly in your environment.

To verify Pano Controller 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 are functioning as expected.
2. Verify that you can log on to Pano Controller.
3. Ensure that Pano Controller can connect to the virtualization manager and your directory service.
4. Verify that web login works.

33
Connect Pano Zero Clients

After you configure the connection brokers in the Pano Controller, ensure that the Pano Zero Clients are physically connected and powered on.

Connect your Pano Zero Clients to the network, monitor, USB, and power connectors. Press the Pano Zero Client button to power on the device. After power on, the Pano Zero Client button follows the sequence:

- blinking red > blinking orange > solid orange > solid blue.

This process should not last more than 15 seconds.Under normal operation, the Pano Button should have a solid blue color within a few seconds of powering on. Once the Pano Button is solid blue, it should remain in this state until the Pano Zero Client is powered off.

Secure Pano Devices

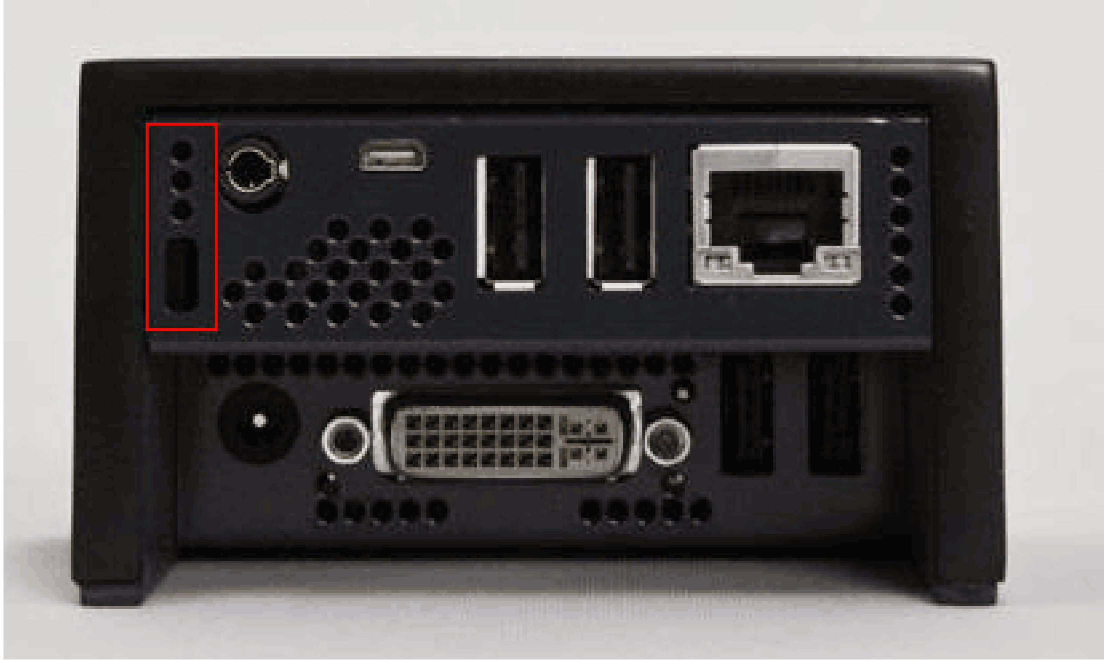
All Pano Zero Clients have a security slot that you can use to secure (lock down) your Pano Zero Clients to an immovable object. The security slot is on the rear of the Pano Zero Client on the left-hand side. The slot itself is a small rectangular hole with rounded corners. The Pano Zero Client is compliant with several well-known clips:

Micro Clip

Kensington ClickSafe

Kensington Desktop and Peripherals Locking Kit

Simply insert the security clip into the security slot, then insert a cable or padlock through the clip holes to prevent the clip from opening.



Related Topics

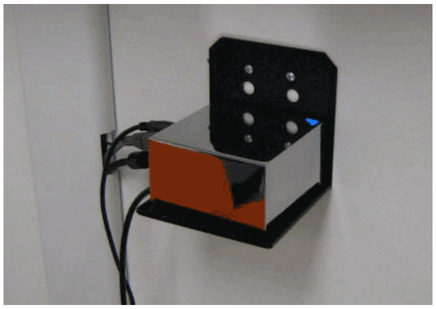
Install Pano Device Mounting Brackets

Install Pano Device Mounting Brackets

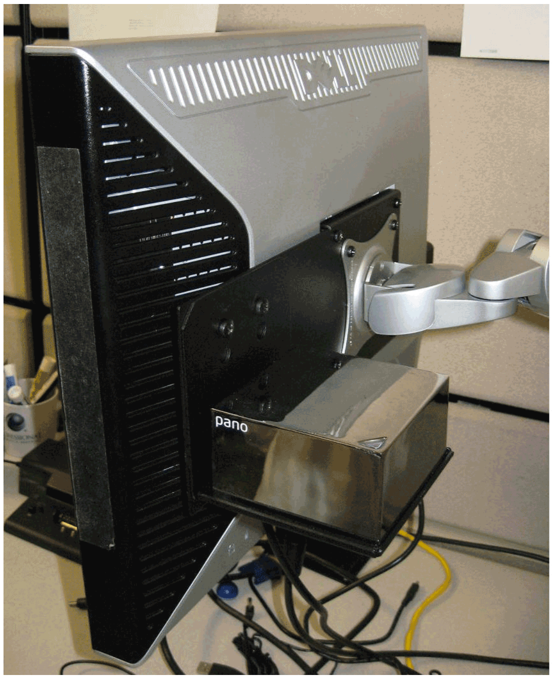
If you'd like to mount a Pano System Endpoint to a monitor in order to free up a little bit of space on your user's desk or because you'd like to secure the user's Pano System Endpoint, you can purchase optional mounting brackets with your Pano System Endpoints.

You can order the wall mount or both the wall mount and monitor mount. This topic assumes that you ordered the Vesa Mounting Kit.

- **Wall Mounting Kit** - includes wall mount only.



- **Vesa Mounting Kit** - includes both wall mount and monitor mount.



If you've already purchased the Pano System Endpoint mounting brackets, go here for installation instructions.

The Pano System Endpoint mounting brackets are VESA-compliant, meaning your Pano System Endpoint is guaranteed to mount on any monitor that adheres to the VESA standards so long as the monitor stand is also VESA-compliant.

Before you purchase Pano System Endpoint mounting brackets make sure that both your monitor and monitor stand are VESA-complaint. It's not uncommon for a company (for example, Dell) to sell a VESA-compliant monitor with a non-VESA-compliant monitor stand. You can also replace a monitor stand with a VESA-complaint stand.

The Pano System Endpoint mounting brackets ship with everything you need to mount the Pano System Endpoint, including screws to fasten the Pano System Endpoint to the mounting brackets and screws to mount the brackets to the monitor and stand. VESA standards dictate the distance between the mount points and the size of the screw holes. VESA does not, however, require that the monitor stand be of a certain thickness; given the variety in monitor stands on the market it's possible that you might need to purchase screws to accommodate the thickness of the monitor stand.

Optionally, one of the mounting brackets can be used as a wall mount if you prefer to mount the Pano System Endpoint on the wall. Pano Logic does not recommend using any adhesives (for example, *Loctite*) on the screws to secure the Pano System Endpoint because you can damage the Pano System Endpoint; doing so will void your Pano System Endpoint hardware warranty. Instead, use a lock washer or self-locking nut, such as a Nylock.

Related Topics

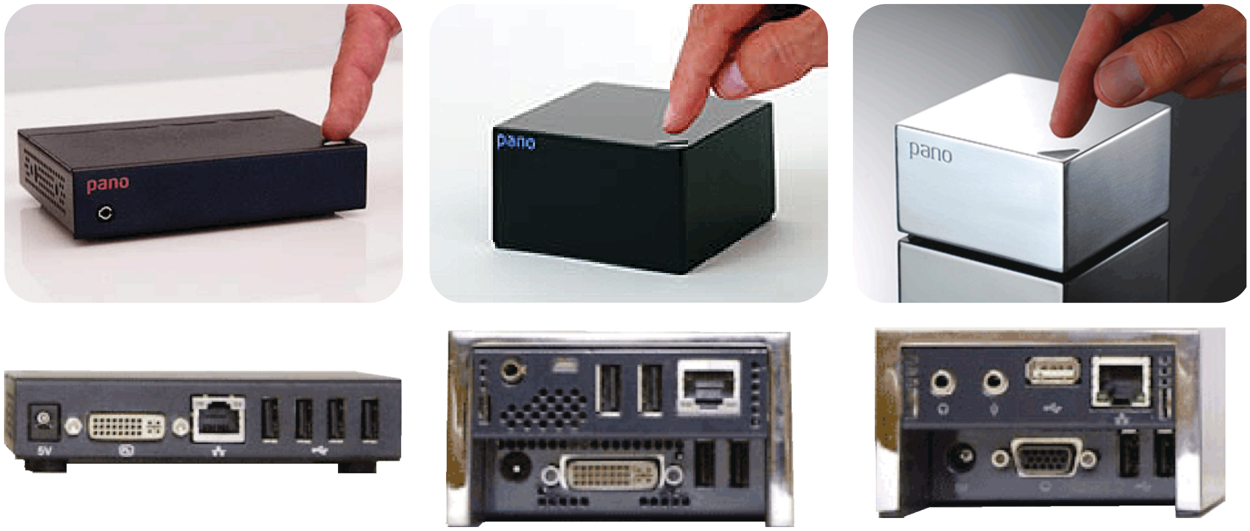
Secure Pano Devices

34

Pano Zero Client Technical Specification

This chapter describes Pano Logic's hardware endpoint, the Pano Zero Client.

There are three members of the Pano Zero Client family. They are, from left to right, the Pano G2M, the Pano G2, and the Pano G1. The Pano G2M is the newest model; Pano G2 has essentially identical function but a different form factor. Pano G1 is non-current, but offers similar functions as well. They key difference is that Pano G2M and Pano G2 have DVI outputs; Pano G1 has a VGA output. Any or all will work.



- Pano Zero Client Hardware Specifications

Related Topics

Connect Pano Zero Clients

Pano Zero Client Hardware Specifications

There are three Pano Zero Client models. The models are easy to distinguish at a glance:

- Pano G2M is a small, rectangular box with a DVI video connector.
- Pano G2 is a slightly larger square box, also with a DVI video connector.
- Pano G1 is very similar to Pano G2, but it has a VGA connector.

Item	Pano G2M	Pano G2	Pano G1
Status	New	Current	Non-current, but supported
I/O:	Four USB 2.0 ports		Three USB 2.0 ports
Primary Video Display:	One DVI-I port capable of driving one DVI-D display, or one VGA display using the DVI-to-VGA adapter supplied.	Pano G2 has DVI-I, plus a mini-port that can drive a compatible monitor when a Pano adapter cable is used.	VGA-type video output.
Networking:	10/100 Base-T Fast Ethernet twisted pair (RJ-45)		

Audio:	Internal speaker for audio output. Single 1/8 inch mini-jack supports audio in and out. Works with iPhone-compatible 4-ring connector / 3.5mm TRRS (tip-ring-ring-sleeve) plug. Using a 4-ring splitter such as KM-IPHONE-2TRS , you can provide a separate jack for speakers and microphone. Audio input is transmitted as 16-bit samples. Tip: Left audio outSleeve: Mic Ring 1: Right audio outRing 2: Gnd	Output: Internal speaker; 1/8-inch mini jack Input: 1/8-inch mini microphone jack
Physical Characteristics:	Height: 0.75" /19 mm Width: 4.50" / 113 mm Depth: 3.50" / 89 mm	Height: 2.00 inches / 51.0 mm Width: 3.50 inches / 88.8 mm Depth: 3.50 inches / 88.8 mm
Power:	Worldwide auto-sensing 100-240 VAC, 50/60 Hz. Average power use with keyboard, mouse and display connected: 6.5 watts. Pano G2M and Pano G2 each have 4 USB ports; Pano G1 has 3. The combined power draw from all ports cannot exceed 1400 mA; no individual port should draw more than 500mA. Power over Ethernet (PoE) cannot be used directly to power the Pano System Endpoint; however, you can use a PoE adapter such as D-Link DWL-P50. This device takes a PoE input and outputs separate Ethernet and power channels which can be connected directly to the Pano System Endpoint. Using such an adapter eliminates the need for the wall socket power adaptor that comes standard with the Pano System Endpoint. Also, you can connect PoE to the network connector on the Pano System Endpoint and still use the wall socket power adaptor that comes standard with the Pano System Endpoint.	
Temperature Range:	50° to 104°F, (10° to 40°C)	
Humidity:	20% to 80% non-condensing	
Weight:	1.1 lbs / 500 grams	
Regulatory Compliance	RF Interference: FCC Class A, CE	
Warranty	Three-year limited warranty	

35
Deploy Pano Remote

Pano Remote lets mobile users use a laptop to connect to their Pano Virtual Desktop, just as though they were using a Pano Zero Client. Pano Remote supports RSA SecurID for user login security, and has the dedicated Pano Gateway in the data center to reduce the computer burden on the virtual desktops themselves.

The software that you need to install to deploy Pano Remote depends on how you want your users to connect to their DVMs:

- When inside the firewall, all you need is Pano Remote.
- When outside the firewall, you need both Pano Remote and Pano Gateway.

Before you can install Pano Remote, you must deploy the Pano System.

To install Pano Remote or both Pano Remote and Pano Gateway, perform the following tasks:

Task	Go to...
(XenDesktop Only) Add domain user accounts to `Direct RDP Access Administrators` group for each DVM. You must do this to enable users to log on remotely to their DVMs without a XenDesktop session.	Citrix KB Article CTX121657.
Set up your Pano Gateway. If you are inside your company's firewall, skip this step. Pano Remote works directly in this case. If you are outside your company's firewall, you must set up your Pano Gateway.	Set Up Pano Gateway
If you intend to use Pano Remote with Pano Gateway, make sure you have hotfix KB952155 installed.	Prepare To Test Pano Remote
On all network PCs, add the desktop icon.	Install Pano Remote
Test the connection.	Test Pano Remote Connectivity
For ease of use, add a Pano Remote server string to the executable.	Recommended: Add Server String to Executable
Secure your Pano Remote USB keys.	Configure Pano Remote Access

Set Up Pano Gateway

Pano Gateway is required if your end users want to use Pano Remote outside your company's firewall. Inside the firewall, Pano Remote works directly.

There is a video, Installing Pano Gateway, which will help you understand how to install Pano Gateway.

1. Set up a Windows Server 2008 R2 server.
2. Install Microsoft .NET Framework 4.0.
3. On the Terminal Services Gateway server, create a local security group called `PanoGatewayGroup`.
4. Add the Remote Desktop Service Gateway Role (formerly called Terminal Services Gateway Role). Follow the step-by-step procedures in Microsoft's TS Gateway Step-by-Step Guide for the core scenario: Configuring the TS Gateway Core Scenario.
   a. When you create the RD CAP Policies, allow access to the PanoGatewayGroup you created earlier.
   b. If the Pano Controller is not connected to the same domain as the Pano Controller, ensure that the certificate used matches that of the <ComputerName>.<DNS_Domain> (which is the same server string to which the Pano Remote key connects).
   c. Ensure that DNS server has a record of the machine that matches the SSL certificate.
5. Go to http://download.panologic.com (contact Pano Logic Technical Support at support@panologic.com to obtain access credentials) and download the Pano Gateway software.
6. Run the `PanoGateway.msi` installer.
7. Modify the `c:\inetpub\PanoGateway\web.config` file.
   a. Specify the fully qualified domain name for the Pano Gateway. This name must match the name under which you issued the SSL certificate.
   b. Specify the IP address of the Pano Controller.

Next Step(s): Login Access to Pano Gateway, Prepare To Test Pano Remote

Related Topics

Upgrade Pano Gateway

Windows Server Support

Login Access to Pano Gateway

To install the Pano Gateway, you must use the Administrator account. If the Administrator account was disabled for security purposes, you must enable it, run the installer, then disable the Administrator account when the installation is complete.

To run the installation from the command line as Administrator, you must provide the Administrator password before invoking the `.msi` file from the command prompt.

Next: Prepare To Test Pano Remote

Prepare To Test Pano Remote

There are two requirements for which you should prepare:

- **PC's RDP client version must be 6.1 or 7.0**. If your company intends to use Pano Remote with Pano Gateway to enable end users to access a desktop virtual machine from a PC outside your company's firewall, that PC's RDP client version must be 6.1 or 7.0. If your company does not intend to use Pano Gateway, any version will work.
- **Printer drivers for local machine must be installed**. If you intend to enable your users to print to their home (local) printers as discussed in Set Access Options for Pano Remote Users, the print drivers for the local printer must be installed on the user's DVM.

In Pano Online Help for End Users, your users are informed of these requirements, but it can't hurt to remind them, or even provide them a pointer to this requirements.

To check your RDP version:

1. Go `C:\WINDOWS\system32` and locate the `mstsc` file.
2. Right-click on `mstsc` and choose **Properties**.
3. Click on the **Version** tab. In the **Item Name:** area, click on **File Version**. The version appears in the **Value:** area.

What to do next: Test Pano Remote Connectivity

To update your RDP client on Windows XP to version 6.1 or 7.0:

Do one of the following:

- Install the hotfix for KB952155. 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.
- Upgrade to Windows XP SP3. This upgrade includes the hotfix for KB952155.

What to do next: Install Pano Remote

Install Pano Remote

Perform this procedure on all network PCs that will connect to a desktop virtual machine. Share this procedure with your end users so that they too can install Pano Remote.

To install Pano Remote:

1. Click on the `PanoRemote.exe` file.
2. Save the file to the PC's desktop.

What to do next: Test Pano Remote Connectivity

Test Pano Remote Connectivity

Before you distribute the Pano Remote USB thumb drives to enable your users to begin using Pano Remote, make sure that you can connect to a desktop virtual machine from a PC.

To test Pano Remote connectivity:

1. Insert the Pano Remote USB thumb drive into a USB port on a PC.

2. Double-click on the **PanoRemote.exe** icon.
3. From the Pano Remote login screen, type the name of your IIS server that you installed on Pano Gateway, then click **Connect**.
4. Log on with your normal Log on information.

   If you have a workplace with both permanent and temporary employees, try credentials for both groups; this verification can catch AD/domain issues.

Troubleshooting: Don’t forget that the collection must provide access to Pano Remote users. Go to Set Access Options for Pano Remote Users.

What to do next: Recommended: Add Server String to Executable

Related Topics

Troubleshoot Pano Remote Problems

Recommended: Add Server String to Executable

Before you distribute the executable to your users, append the web server's name directly to the executable itself. This way, the web server's name is passed automatically to Pano Remote, saving users the time and hassle of having to type the web server’s name from the login screen.

To add Pano Remote server string to the executable:

1. Insert a Pano Remote USB into your computer.
2. Open the command prompt and navigate to the directory where `PanoRemote.exe` resides.

```
> E:
> DIR
03/17/2009 02:06 PM   1,200,128 PanoRemote.exe
03/12/2009 09:52 PM     194 autorun.inf
```

3. Recommended: Make a backup copy of `PanoRemote.exe` before you change the server string.

```
> copy PanoRemote.exe c:
```

4. Run one of the following commands:

   For http:

```
> E:
> echo server:gateway.mydomain.com>> PanoRemote.exe
```

Where `gateway.domain.com` is the FQDN of your Terminal Services Gateway server.

For https:

```
> E:
> echo server:https://gateway.mydomain.com>>PanoRemote.exe
```

PanoRemote.exe uses https when communicating with Pano Gateway and the Pano Controller. Even if you configure PanoRemote.exe with a server name that doesn't use https, the Pano System forces https by redirecting the http connection to an https connection, ensuring that all communication is secure between Pano Remote and Pano Gateway, Pano Controller and DVMs.

5. Replace the .exe file that resides on all your Pano Remote USB thumb drives with the file that you just modified.

What to do next: Configure Pano Remote Access

Related Topics

Troubleshoot Pano Remote Problems

Remove Server String from Executable

If your gateway changes, you'll need to remove server string in the executable, then add it again as outlined in Recommended: Add Server String to Executable.

To remove the server string to the executable:

1. Open the command prompt and navigate to the directory where PanoRemote.exe resides.
2. Type the following:

```
> echo server:>> PanoRemote.exe
```

Add SSL Certificate To Pano Gateway

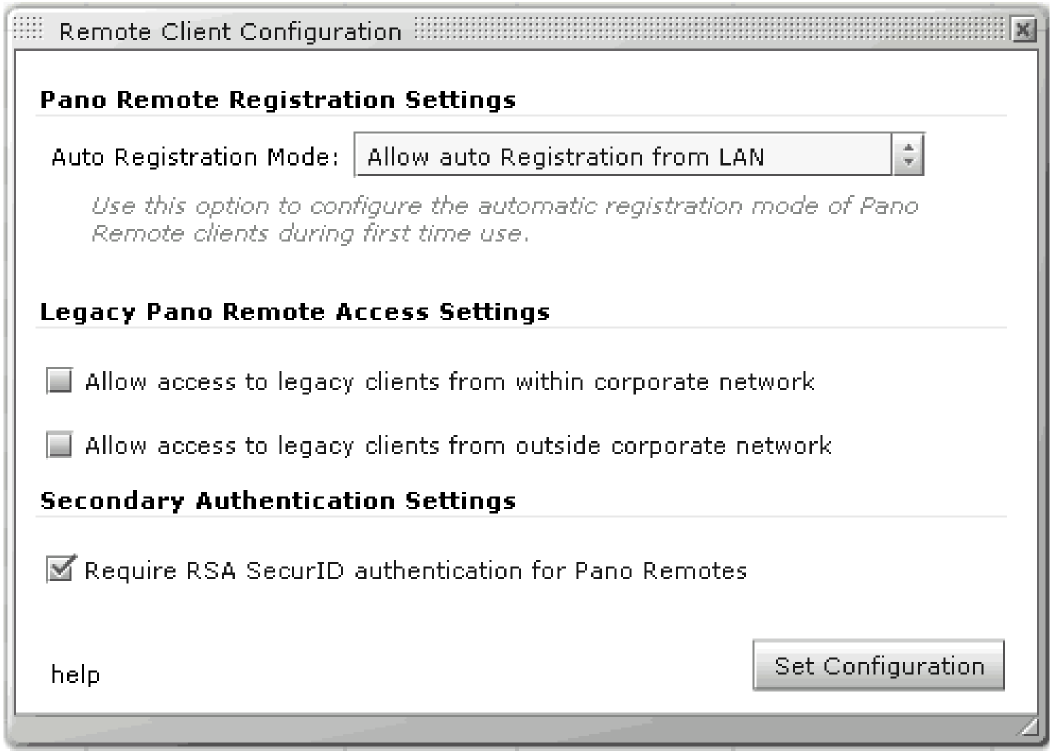
If you're receiving a Server Certificate error from the IIS Manager or your browser when you connect to the gateway, you don't have a certificate installed.

To add the certificate:

1. From the IIS Manager, select the Terminal Services Gateway server, double-click the Server Certificates icon, then use the Server Certificates wizard to create your certificate.
2. Select the Default Web Site, click **Bindings** in the Action pane, then bind port 443 to the certificate that you just created.

Configure Pano Remote for RSA SecurID

This shows the setup screen for configuring RSA login requirements and a user login screen.



Remote Client Configuration

Pano Remote Registration Settings

Auto Registration Mode: Allow auto Registration from LAN

Use this option to configure the automatic registration mode of Pano Remote clients during first time use.

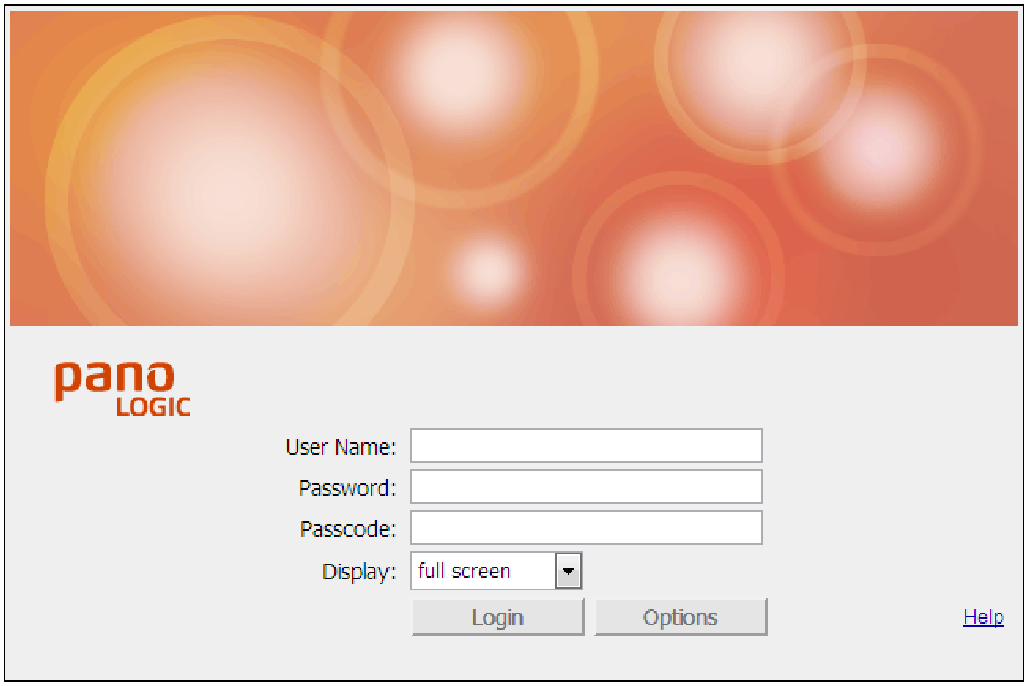
Legacy Pano Remote Access Settings

□ Allow access to legacy clients from within corporate network

□ Allow access to legacy clients from outside corporate network

Secondary Authentication Settings

☑ Require RSA SecurID authentication for Pano Remotes



User Name:	
Password:	
Passcode:	
Display:	full screen

Upgrade Pano Gateway

To upgrade Pano Gateway:

1. On the Terminal Services Gateway server, create a local security group named `PanoGatewayGroup`.
2. Add the local security group `PanoGatewayGroup` to Remote Desktop Services Connection Authorization Policies (CAP) and Resource Authorization Policies (RAP):
   a. Open Server Manager.
   b. Expand **Roles** > **Remote Gateway Manager** > **(Computer Name)** > **Policies**.
   c. Click on **Connection Authorization Policies**, then:
      - Double-click on the policy shown in the main screen.
      - Select the **Requirements** tab.
      - Add the local group `PanoGatewayGroup`.
      - Click OK.

   d. Click on **Resource Authorization Policies**, then:
      - Double-click on the policy shown in the main screen.
      - Select the **User Groups** tab.
      - Add the local group `PanoGatewayGroup`.
      - Click OK.
3. Go to http://download.panologic.com (contact Pano Logic Technical Support at support@panologic.com to obtain access credentials) and download the Pano Gateway software.
4. Run the `PanoGateway.msi` installer.
5. Modify the `c:\inetpub\PanoGateway\web.config` file.
   a. Specify the fully qualified domain name for the Pano Gateway. This name must match the name under which you issued the SSL certificate.
   b. Specify the IP address of the Pano Controller.

Upgrade Pano Remote

New Pano Remote USB thumb drives always include the latest Pano Remote executable preinstalled. However, you might want to upgrade existing Pano Remote USB thumb drives to make use of new fixes or enhancements. If you have a large volume of thumb drives consider using a third-party software program to upgrade all thumb drives simultaneously.

To upgrade a Pano Remote USB thumb drive:

1. Go to http://download.panologic.com (contact Pano Logic Technical Support at support@panologic.com to obtain access credentials).
2. Download the new Pano Remote executable to a PC.
3. If applicable, reconfigure the new executable with the appropriate server name as outlined in Recommended: Add Server String to Executable.
4. Replace the old Pano Remote executable on the Pano Remote USB thumb drive with the new executable.

Configure Pano Remote Access

The Pano System provides security capabilities for both Serialized Pano Remote USB keys and Legacy Pano Remote USB keys. However, the capabilities available are different for each type.

Serialized Pano Remote USB keys have unique serial numbers. Serial numbers enable you to track usage per key and disable (block) access for specific keys. As outlined in the procedure below, you must register such keys before end users can use them.

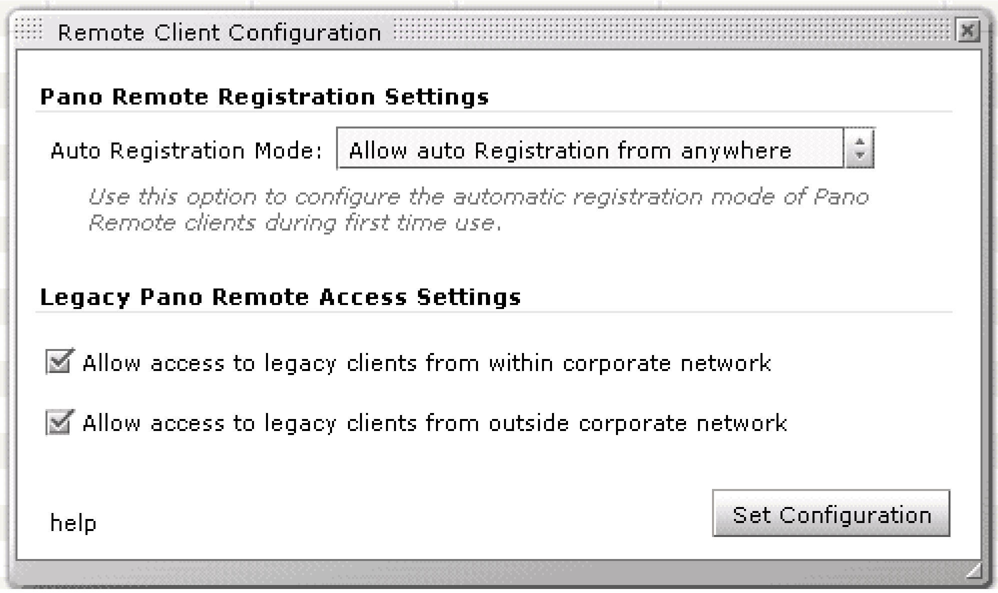
Legacy (non-serialized) Pano Remote USB keys, those produced prior to Pano System 4.5, do not/cannot have serial numbers. Upgrading Pano Remote does not create a serial number for such keys. However, as outlined in the procedure below, there are security policies that you can apply to help manage the security of these devices. Note that these policies apply to any and all non-serialized keys because individual keys cannot be distinguished.

To configure Pano Remote access:

1. Log on to the Pano Controller.
2. Click on the **Clients** tab.
3. Click the **Settings** drop-down list, then choose **Remote Client Configuration**. The Remote Client Configuration dialog appears.
4. Do the following:
   a. (Serialized Pano Remote USB keys) Specify **Pano Remote Registration Settings** (**Auto Registration Mode**):
      - **Allow auto Registration from anywhere** – First time a key is used, it is automatically registered.
      - **Allow auto Registration from LAN** – Key must be used for the first time on a LAN, at which point it is registered. Subsequent use can be from anywhere.
      - **Disallow auto Registration** – New keys are added to the Pano Controller the first time they are used on the LAN, but are automatically disabled. You must enable such keys before end users can use them. See Enable Pano System Endpoints.

   b. For Legacy Pano Remote USB keys: Specify **Legacy Pano Remote Access Settings**:
      - **Allowed within the corporate network** – selecting this checkbox enables this security policy.
      - **Allowed outside the corporate network** – selecting this checkbox enables this security policy.
      - **Not allowed** – clearing all checkboxes enables this security policy.

   c. For RSA SecureID tokens: Specify **Require RSA SecureID for authentication**
      - If Pano Remote is checked, will require check of user ID, password, and RSA SecureID OTP (One Time Password).
      - Pano Zero Clients will only require check of user ID and password.
      - Pano Virtual Clients operate under the same policy as Pano Remote users.


Remote Client Configuration

Pano Remote Registration Settings

Auto Registration Mode: Allow auto Registration from anywhere

Use this option to configure the automatic registration mode of Pano Remote clients during first time use.

Legacy Pano Remote Access Settings

☑ Allow access to legacy clients from within corporate network

☑ Allow access to legacy clients from outside corporate network

5. Click **Set Configuration**.

Related Topics

Identify Pano Zero Client Serial Numbers

Enable Pano System Endpoints

Configure DVMs for 24-bit Color

Sixteen-bit color depth uses less network bandwidth and provides better responsiveness; 24-bit gives richer and smoother color, but is a bit more network intensive.

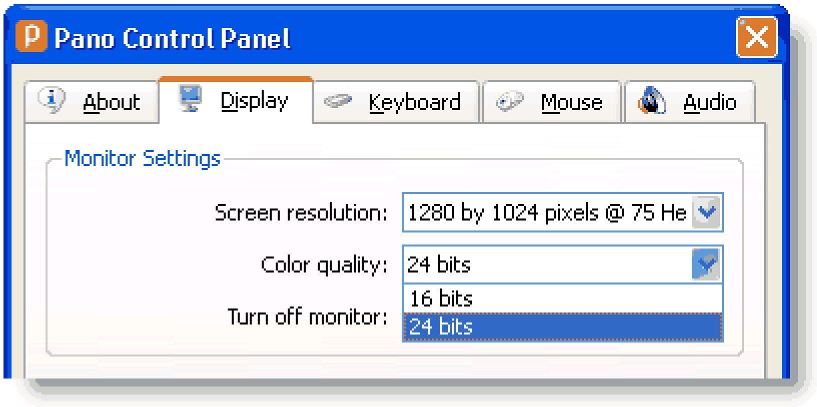
When connecting to a DVM via a Remote Desktop connection or Pano web access, you must configure the DVM if your users desire 24-bit color depth. To do so, go to Configure Pano Direct Service for 24-bit Color This is not the case for Pano System Endpoint connections.

When connecting via a Pano System Endpoint to a DVM with Pano 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**.



Screen resolution: 1280 by 1024 pixels @ 75 He

Color quality: 24 bits

Turn off monitor:

Setting Up RSA SecurID

RSA SecurID login authentication is available in Release 6.0. You can implement RSA SecurID by obtaining licenses and keys from EMC, the vendor.

RSA has designed their system around the secure token, a hardware device, and two 'secret' files. You will work with RSA to create these files, then you will install the files on certain machines within your overall system. The two files are:

```
sdconf.rec
nodesecret.rec
```

You will have one instance of sdconf.rec for your entire enterprise. Each Pano Controller will have its own unique copy of nodesecret.rec.

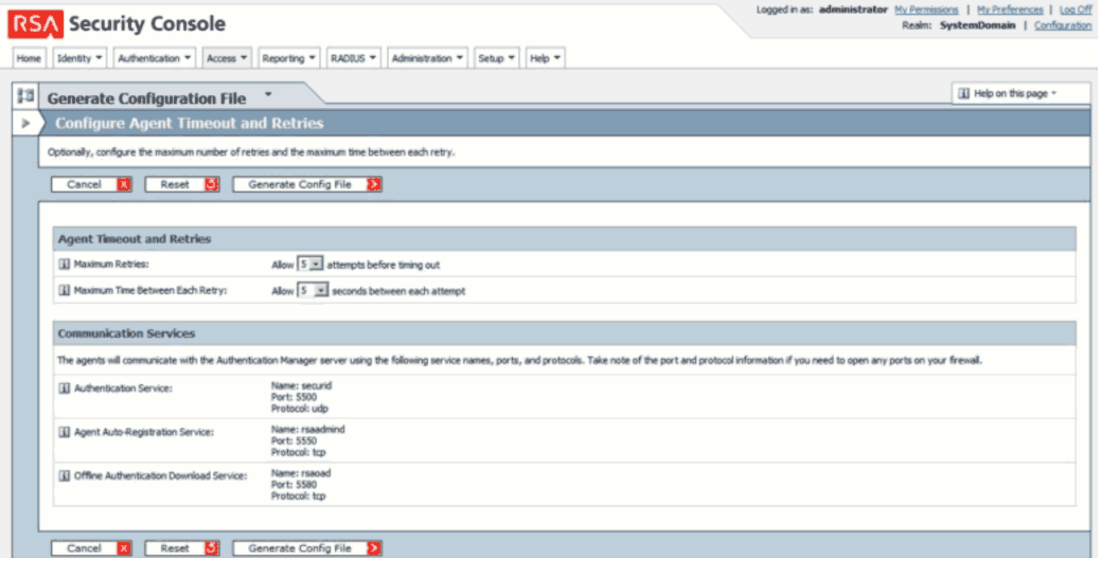
Configuring Pano Controller to talk to the RSA Authentication Manager

These steps are required to configure Pano Controller to talk to the RSA Authentication Manager. We'd make it simpler if we could, but this process is defined by RSA, not Pano.

Note: This requires the administrator password for the RSA Authentication Manager.

1. Create the Authentication Manager configuration file (`sdconf.rec`):

   In the Authentication Manager UI, **Access > Authentication Agents > Generate Configuration File**. Download and save the .zip file.



RSA Security Console
Logged in as: administrator | My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home | Identity | Authentication | Access | Reporting | RADIUS | Administration | Setup | Help
Generate Configuration File
Help on this page
Configure Agent Timeout and Retries

Optionally, configure the maximum number of retries and the maximum time between each retry.

Cancel | Reset | Generate Config File

Agent Timeout and Retries

Maximum Retries:	Allow 5 attempts before timing out
Maximum Time Between Each Retry:	Allow 5 seconds between each attempt

Communication Services

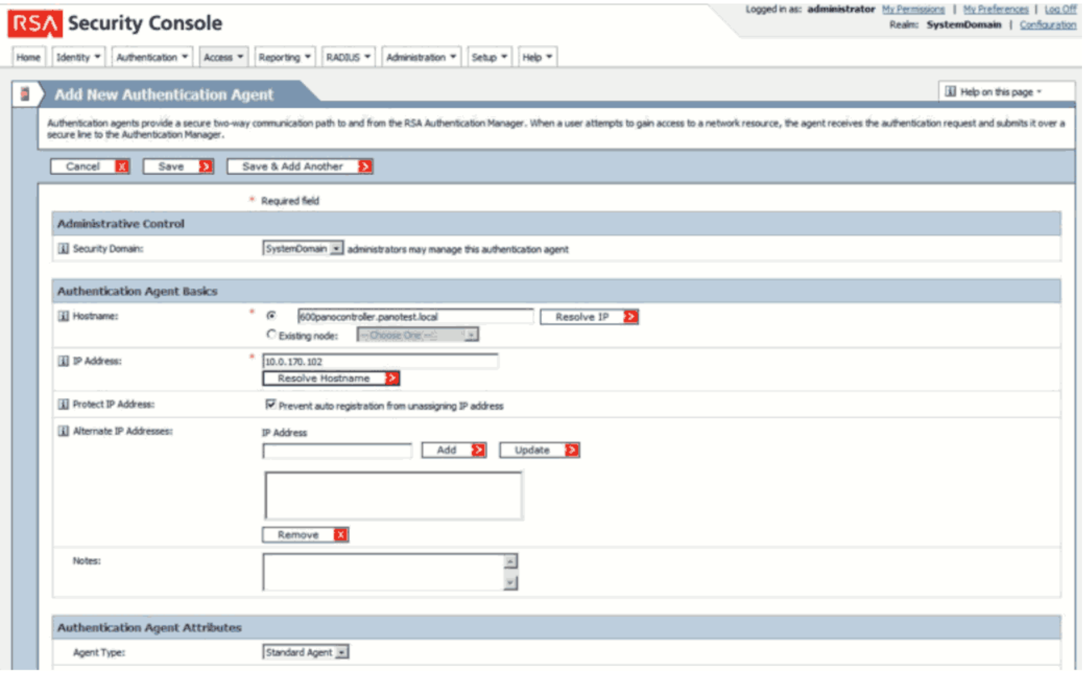
The agents will communicate with the Authentication Manager server using the following service names, ports, and protocols. Take note of the port and protocol information if you need to open any ports on your firewall.

Authentication Service:	Name: securid Port: 5500 Protocol: udp
Agent Auto-Registration Service:	Name: rsaadmind Port: 5550 Protocol: tcp
Offline Authentication Download Service:	Name: rsaoad Port: 5580 Protocol: tcp

2. Register the Pano Controller as an Authentication Agent:

   Security Console > Access > Authentication Agents > Add New

   Note: Use the fully-qualified domain name of the Pano Controller for the Host Name.



RSA Security Console
Logged in as: administrator | My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home | Identity | Authentication | Access | Reporting | RADIUS | Administration | Setup | Help
Add New Authentication Agent
Help on this page

Authentication agents provide a secure two-way communication path to and from the RSA Authentication Manager. When a user attempts to gain access to a network resource, the agent receives the authentication request and submits it over a secure line to the Authentication Manager.

Cancel | Save | Save & Add Another

* Required field

Administrative Control

Security Domain:	SystemDomain administrators may manage this authentication agent

Authentication Agent Basics

Hostname: *	● 600panocontroller.panotest.local [Resolve IP] ○ Existing node: -- Choose One --
IP Address: *	10.0.170.102 [Resolve Hostname]
Protect IP Address:	☑ Prevent auto registration from unassigning IP address
Alternate IP Addresses:	IP Address [Add] [Update] [Remove]
Notes:	

Authentication Agent Attributes

Agent Type:	Standard Agent

3. Create the node secret file, **nodesecret.rec**:

   Security Console > Access > Authentication Agents > Manage Existing > (Select required PanoMan auth agent from list) > Manage Node secret.

   You will be prompted to enter and confirm a password.

Note: This password as it will be required for step 5. Download and save the .zip file.

4. Extract and copy the `sdconf.rec` and `nodesecret.rec` files created in steps 1 and 3 to a working directory on a system that has the RSA utility **agent_nsload** installed.

   Here is an example of running agent_nsload.exe to extract the node secret file on a Win7 32bit machine:

   i. Copy `agent_nsload.exe` and `sdmsg.dll` to the <windir>\system32 folder

   ii. Copy `nodesecret.rec` and `sdconf.rec` to the <windir>\system32 folder

   iii. Launch **Command Prompt** with **Run as administrator**

   iv. On the prompt, run `Agent_nsload.exe -f nodesecret.rec`, and you will be prompted to enter the password.

   ```
   C:\Windows\system32>agent_nsload.exe -f nodesecret.rec
   Enter PASSWORD:
   Loading Node Secret....
   The Node Secret is successfully loaded
   ```

Note: If you are on another OS, please see the RSA Authentication Manager documentation for the details.

5. Copy the `sdconf.rec` and `securid` files to the `/opt/atto/rsa` directory on the Pano Controller VM.

If you are running multiple Pano Controller instances for HA or scalability, you will need to repeat steps 2 - 6 for each Standby Pano Controller VM.

36
Pano Virtual Client

Pano Virtual Client is software that lets you re-purpose a PC to function like a Pano Zero Client. This lets you continue to use PCs you have while gaining the management capabilities and features of the Pano System. Pano Virtual Client also extends the life of older PCs, since the virtual client software does not require an extremely powerful platform.

The PC remains useful as a PC; it can be used locally by logging into the local Windows desktop rather than using Pano Virtual Client to connect to a Pano virtual desktop. However, Pano Virtual Client maintains strict isolation between the OS running on the host PC and the OS in your desktop virtual machines.

Two versions of PVC are available:

- Shell, a full-screen, dedicated app.
- Application, where PVC runs as a Windows application.

Each version has its own installer.

You cannot have both versions installed on a single host PC. If it is necessary, one version must be uninstalled and the other installed. Chose the appropriate installer .msi to achieve the desired mode. See Download Pano Virtual Client Software for details on where to get the files.

Deployment of Pano Virtual Client is usually done via Microsoft Active Directory. Deploying Pano Virtual Client this way provides control over which users and which host PCs are used for Pano Virtual Client. It also allows you to quickly deploy and upgrade across your LAN without requiring a visit to each host PC. In general, while there are some differences in the deployment processes of Pano Virtual Client and Pano Zero Client endpoints, management of them using the Pano Controller console is virtually identical.

To understand requirements, see Requirements for Implementing Pano Virtual Client.

Shell

Deployment of Pano Virtual Client is done via Microsoft Active Directory. Deploying Pano Virtual Client this way provides centralized control over which users and which host PCs use Pano Virtual Client. It also allows you to quickly deploy and upgrade across your LAN without requiring a visit to each host PC.

In general, while there are some differences in the deployment processes of Pano Virtual Client-Shell and Pano Zero Client endpoints, management of them using the Pano Controller for Cloud console is virtually identical.

Restrictions

When the shell version of Pano Virtual Client is installed on a PC, a Pano Logic driver gets installed to provide remote USB access to the DVM. For security, it blocks all local USB access to the PC, except for keyboard and mouse. This prevents infection via USB drive and other issues. Simply rebooting the PC will not restore USB access. You must remove (uninstall) Pano Virtual Client.

Automated Deployment to Repurpose PCs as Virtual Desktop Devices

You are welcome to use any third-part tool you are familiar with to push the .msi installer to windows clients. We've provided a sample configuration for doing this with Active Directory group polices as noted at Deploy Pano Virtual Clients

To create an alt shell to launch Pano Virtual Client automatically for specific users: Configure Windows PC to Launch Pano Virtual Client Alternative Shell.

Next: Application

Application

Deploy by running .msi installer while logged into Windows. Users still need to login to Windows, then manually launch via a program icon or auto launch via a Start Menu entry. To become a Start Menu entry the application needs to be added to the Startup folder in the Program menu as auto-launch. USB support is limited to a keyboard and mouse. The PVC window is either full screen or minimized to task bar -- there is no option to run as a resizable window.

Restrictions

When the application version of Pano Virtual Client is installed on a PC, the Pano Logic USB driver restricts USB device access from PVC, to prevent infection via USB drive and other issues.

Quick Trial Installation

If you want to install PVC on one PC for a quick trial:

1. Run the appropriate installer on the PC that will host Pano Virtual Client.
2. Enable discovery of Pano Virtual Client via a DNS SRV record.

Browse to c:\Program Files\Pano Logic\Pano Virtual Client\BIN\ and the double-click on PanoVirtualClient.EXE. This will cause Pano Virtual Client to launch for the currently logged in session. To exit out of Pano Virtual Client, click the “X” button in the bar at the top of the session. This will close the virtual client and logout the local windows session.

Pano Virtual Client Deployment Options

To install a quick trial of Pano Virtual Client

1. Run the appropriate installer (win7/winxp) on the PC that will host Pano Virtual Client
2. Enable discovery of Pano Virtual Client either via a DNS SRV record or by enabling Probe based discovery in Pano Controller
3. Browse to c:\Program Files\Pano Logic\Pano Virtual Client\BIN\ and the double-click on PanoVirtualClient.EXE
   - This will cause Pano Virtual Client to launch for the currently logged in session. To exit out of Pano Virtual Client, click the "X" button in the bar at the top of the session. This will close the virtual client and logout the local windows session.

Automated Deployment to Repurpose PCs as Virtual Desktop Devices

You are welcome to use any third-part tool you are familiar with to push the msi installer to windows clients. We've provided a sample configuration for doing this with Active Directory group polices as noted at Deploy Pano Virtual Clients

To create an alt shell to launch Pano Virtual Client automatically for specific users: Configure Windows PC to Launch Pano Virtual Client Alternative Shell

Requirements for Implementing Pano Virtual Client

Pano Virtual Client host PC requirements are shown in Host PC or Laptop Hardware for Pano Virtual Client.

Network requirements are shown in Network and Infrastructure Requirements.

We recommend that you first deploy Pano System with any Pano Zero Client you are using before moving on to deploy Pano Virtual Client. This will help isolate any deployment issues that are tied to Pano Virtual Client or Active Directory by ensuring you have functioning back-end servers and desktop virtual machines.

Host PC or Laptop Hardware for Pano Virtual Client

Hardware Requirements

- **CPU:** Pentium-class dual-core CPU or better.
- **RAM:** 1 GB for both Windows XP and Windows 7 as the host OS.
- **Hard Drive:** minimum of 1 GB of free hard disk space.
- **Peripheral Support:** Most non-isochronous USB devices compatible with a G2 Pano are supported. However, isochronous USB audio/video devices, such as USB web cams and headsets, are not.
- **Video monitor support:** at least equivalent to a G2 Pano Zero Client; and include:
   - Support for a single monitor from a single graphics card or integrated GPU in the host PC. Use of more than one monitor is not supported.
   - Output via DVI, VGA, HDMI, or DisplayPort as supported by the host PC's GPU hardware – inclusion of digital audio out as part of HDMI and Display port output is not supported.

  - Color depths of 16-bit or 24-bit.
  - Video resolution support as listed below even if less than those supported by the host PC’s graphics hardware and Windows drivers:
    - Same set of standard and widescreen resolutions supported by G2 Pano Zero Client along with the monitor’s native resolution, provided that it is 1920x1200 or less. Resolutions must also be supported by the underlying host PC’s GPU hardware and Windows graphics drivers.
    - Landscape monitor orientations – portrait monitor rotation is not supported.
  - **Wired Network Port:** a single wired Ethernet network port, at 100 Mbps to 1 Gbps. Wireless 802.11 or Wi-Fi networking does work but requires added preparation and has some limitations and cautions. Any network interfaces you are not planning to use should be disabled in WIndows prior to installing Pano Virtual Client.

Software Requirements

- **Host PC OS** – any of:
  - Windows XP Professional, 32-bit, SP3
  - Windows 7, all editions, 32-bit and 64-bit
- **Driver software** should already be installed for graphics, audio and networking in the PC. Drivers for other supported USB peripherals will be installed in the desktop.
- **Ideally, no other software** should be installed beyond the base Windows operating system and required drivers. Application and utility software isn’t needed as users will not be able to access the local Windows desktop once the Pano Virtual Client is installed. Other application and utility software may cause conflicts and using a new clean install of Windows may be necessary to optimally repurpose some PCs to run Pano Virtual Client.

Network and Infrastructure Requirements

In general Pano Virtual Client requires the same network infrastructure as Pano Zero Client.

- **Administrative access** to your network infrastructure, including the DNS server and Active Directory domain controller.
- **VDI servers** installed with virtualization platform software and running Pano Controller 6.0.
- **DNS Server:** DNS SRV records, the same mechanism that Windows computers use to find their AD Domain Controller, LDAP service, etc., need to be created for discovery of Pano Virtual Clients by Pano Controller. The DNS server and the Active Directory domain controller must be the same machine.
- **DHCP Server:** a DHCP server is needed to provide dynamically-assigned IP addresses.
- **Active Directory for Pano Virtual Clients:** you must have Microsoft Active Directory deployed and have administrative access to your Active Directory domain controller to deploy Pano Virtual Client.The DNS server and the Active Directory domain controller must be the same machine or the Pano Virtual Client hosts may not be able to discover their Pano Controller.
- **Active Directory Organizational Units**: The Pano Virtual Client host PCs must not be in the same Active Directory Organizational Unit (OU) as the DVMs. There is a potential conflict between certificates in the Pano Virtual Client installer, which get distributed via Active Directory, and certificates that can optionally be used in Windows 7 installation of Pano Direct Service. Using separate Active Directory OUs for the Pano Virtual Client hosts

and the Pano DVMs ensure that you won't have a certificate conflict that could cause Pano Virtual Client installation to fail.

Download Pano Virtual Client Software

You'll need to download one or more Pano Virtual Client installers. Use a web browser to go to http://download.panologic.com and select the versions to download.

Filenames for the installer .msi files differ by platform, OS bits (x86 vs. x64), and Shell vs. Application.

Complete the download registration page, and read and accept the End User License Agreement to get to the software download page.

- Windows 7 (32 bit)
  - Shell Mode installer: **PanoVirtualClientShell_Win7_x86-6.1.0.msi**
  - Application mode installer: **PanoVirtualClientApp_Win7_x86-6.1.0.msi**
- Windows 7 (64 bit)
  - Shell Mode installer: **PanoVirtualClientShell_Win7_x64-6.1.0.msi**
  - Application mode installer: **PanoVirtualClientApp_Win7_x64-6.1.0.msi**
- Windows XP (32 bit) - **PanoVirtualClient_WinXP_x86-6.0.0.msi**
  - Shell Mode installer: **PanoVirtualClientShell_WinXP_x86-6.1.0.msi**
  - Application mode installer: **PanoVirtualClientApp_WinXP_x86-6.1.0.msi**

Copy all of the installer .msi files you'll need for the Windows operating systems you plan to use on your host PCs. For the shell version they will need to be in a location that is accessible to your Active Directory server.

Next: Prepare Network Infrastructure

Prepare Network Infrastructure

Check Active Directory and Workgroup Configuration

Windows machines which are within a Workgroup cannot use the DNS Service Record to locate the Pano Controller. The machines that will host Pano Virtual Client should either:

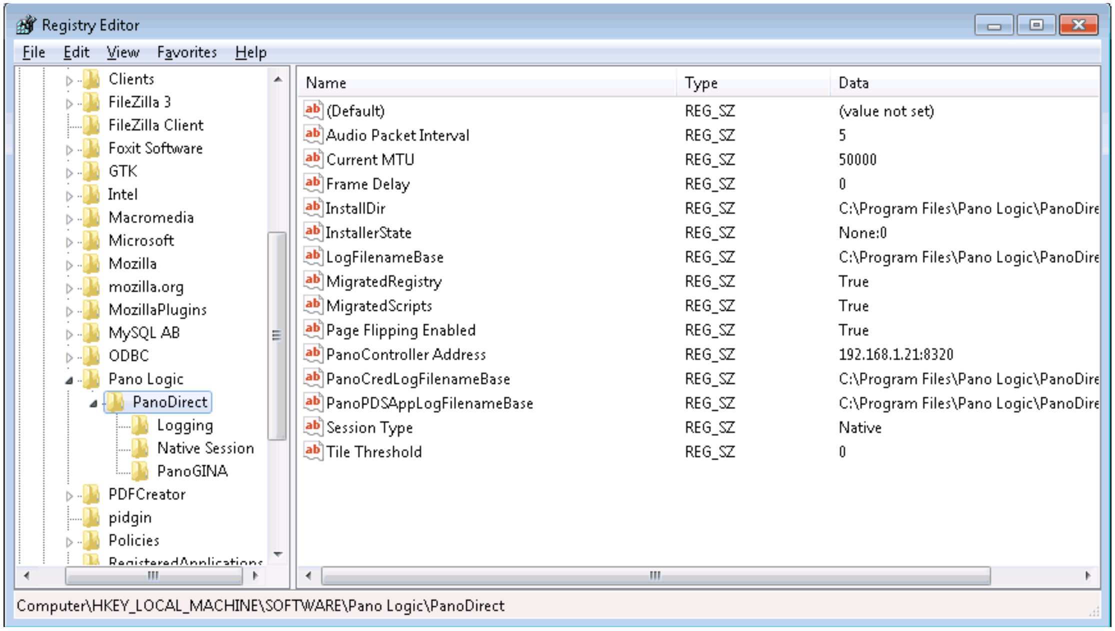
- Be added to your Active Directory domain.
- Have a Registry Key loaded which will tell the PC where the Pano Controller is.

  You will need to manually add a registry key that holds the IP address of Pano Controller in the Windows registry on each host PC. For convenience this registry key can be saved as a .reg file using the regedit.exe tool included with Windows. This `.rteg` file can then distributed and run on each host PC to add the registry key.

  The registry key needed is called "PanoController Address"- the complete registry path to the key is: "`HKEY_LOCAL_MACHINE\SOFTWARE\Pano Logic\Pano\Direct\PanoController Address`"

  If the key isn't already present create it as a String Value type - the value of the key is the IP address of your Pano Controller plus a colon and the port number used by the Pano Direct Protocol, 8320 - for example: `192.168.10.21:8320`.

Figure 36.1 Manual Registry-Edit Example



Name	Type	Data
(Default)	REG_SZ	(value not set)
Audio Packet Interval	REG_SZ	5
Current MTU	REG_SZ	50000
Frame Delay	REG_SZ	0
InstallDir	REG_SZ	C:\Program Files\Pano Logic\PanoDire
InstallerState	REG_SZ	None:0
LogFilenameBase	REG_SZ	C:\Program Files\Pano Logic\PanoDire
MigratedRegistry	REG_SZ	True
MigratedScripts	REG_SZ	True
Page Flipping Enabled	REG_SZ	True
PanoController Address	REG_SZ	192.168.1.21:8320
PanoCredLogFilenameBase	REG_SZ	C:\Program Files\Pano Logic\PanoDire
PanoPDSAppLogFilenameBase	REG_SZ	C:\Program Files\Pano Logic\PanoDire
Session Type	REG_SZ	Native
Tile Threshold	REG_SZ	0

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Pano Logic\PanoDirect

If neither of these option is desirable, you must configure your Pano Controller to use the probe method of client discovery.

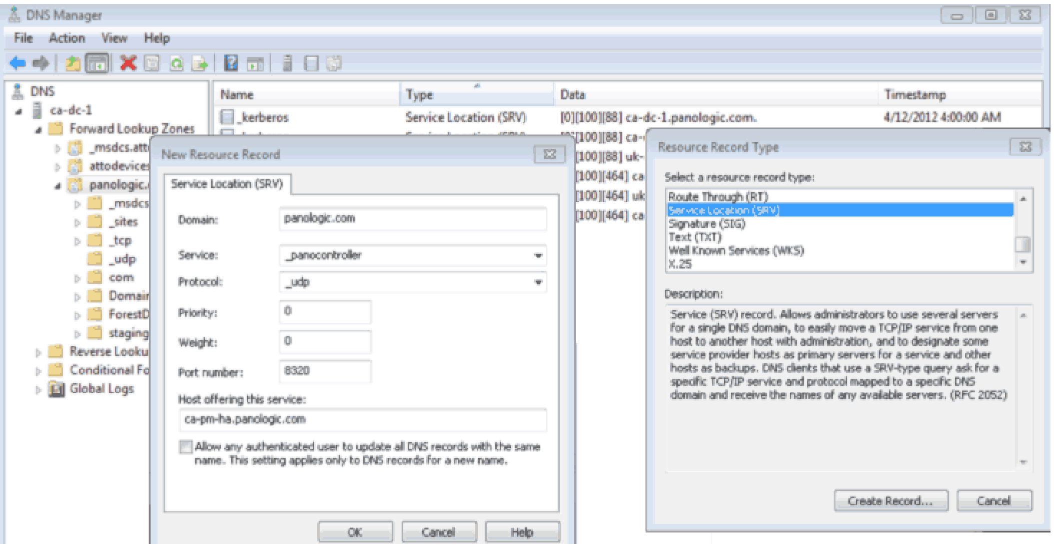
Check DHCP Server Setup

Ensure that your DHCP server is able to provide sufficient dynamically-assigned IP addresses to your Pano Virtual Client PCs. Static IP addresses and DHCP reservations can also be used for the PC’s IP addresses.

Add a Service Record for Pano Controller to the DNS Server

1. Go to your DNS server and select the zone for your domain. We strongly recommend that you use your Active Directory domain controller as your DNS server; using other types of DNS servers may not work with Pano Virtual Client.
2. Right click; select “New Other Records”->”Service Location(SRV)” and click “Create Record”
3. In the service field type “_panocontroller.”
4. In the protocol field type “_udp”
5. In the Port number field type “8320”

6. In the Host offering this service field, type the IP or hostname of your Pano Controller. If you have an HA Pano Controller environment, this should be the HA IP/Hostname.



Domain: panologic.com

Service: _panocontroller

Protocol: _udp

Priority: 0

Weight: 0

Port number: 8320

Host offering this service:
ca-pm-ha.panologic.com

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Select a resource record type:
Route Through (RT)
Service Location (SRV)
Signature (SIG)
Text (TXT)
Well Known Services (WKS)
X.25

Description:
Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)

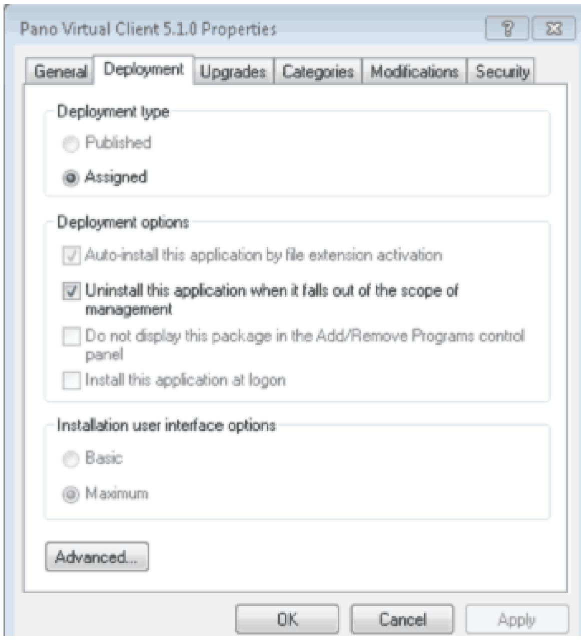
Note: Optionally, you can use a registry key to point to the Pano Controller that is managing the Pano Virtual Clients. The path is `/hkm/software/pano_logic/panodirect` and the key is `reg_sz`, of type ‘string’.

Note: Next: Deploy Pano Virtual Clients

Deploy Pano Virtual Clients

Follow these steps to do an automated deployment via Active Directory:

1. Create an Active Directory group policy that will distribute Pano Virtual Client to PCs under this OU. If you plan to support Pano Virtual Clients running Windows 7 and Windows XP, you'll need to create two separate deployment GPOs
   - Each policy should be restricted via WMI filter to either Windows 7 or Windows XP, depending on which OS you intend to use on the PCs.
   - Each policy should be set to remove software if the PC falls out of the group policy scope.
   - Set the Windows 7 policy to not allow the 32-bit version to run on 64-bit Windows.



Pano Virtual Client 5.1.0 Properties

Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

☑ Uninstall this application when it falls out of the scope of management

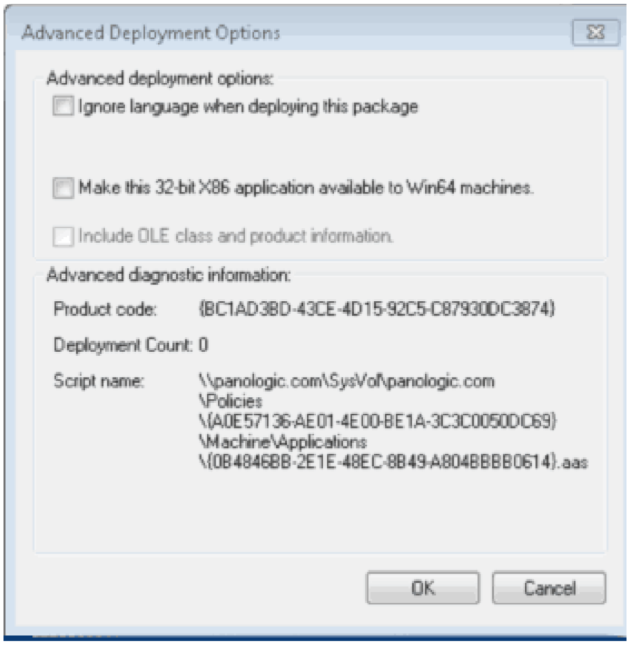
□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

Installation user interface options

○ Basic

● Maximum



Advanced Deployment Options

Advanced deployment options:

□ Ignore language when deploying this package

□ Make this 32-bit X86 application available to Win64 machines.

□ Include OLE class and product information.

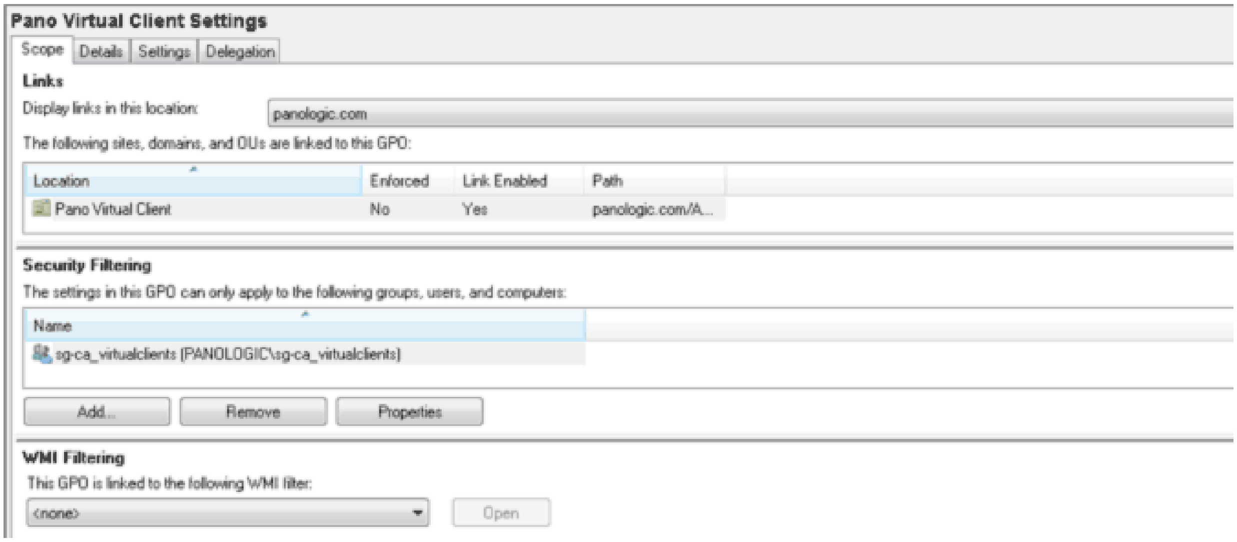
Advanced diagnostic information:

Product code: {BC1AD3BD-43CE-4D15-92C5-C87930DC3874}

Deployment Count: 0

Script name: \\panologic.com\SysVol\panologic.com\Policies\{A0E57136-AE01-4E00-BE1A-3C3C0050DC69}\Machine\Applications\{0B4846BB-2E1E-48EC-8B49-A804BBBB0614}.aas

The resulting Active Directory group policy is shown below:



Pano Virtual Client Settings

Links

Display links in this location: panologic.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Pano Virtual Client	No	Yes	panologic.com/A...

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

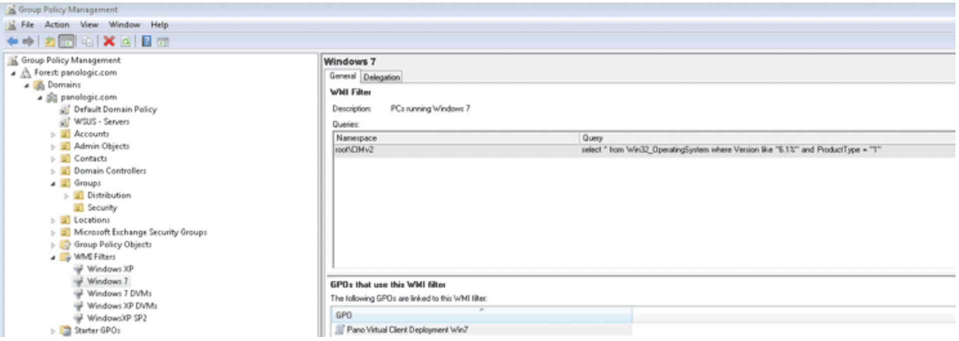
Name
sg-ca_virtualclients (PANOLOGIC\sg-ca_virtualclients)

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

2. Add a WMI filter to restrict GPO to Windows 7, as illustrated below:



Windows 7

WMI Filter

Description: PCs running Windows 7

Queries:

Namespace	Query
root\CIMv2	select * from Win32_OperatingSystem where Version like "6.1%" and ProductType = "1"

GPOs that use this WMI filter

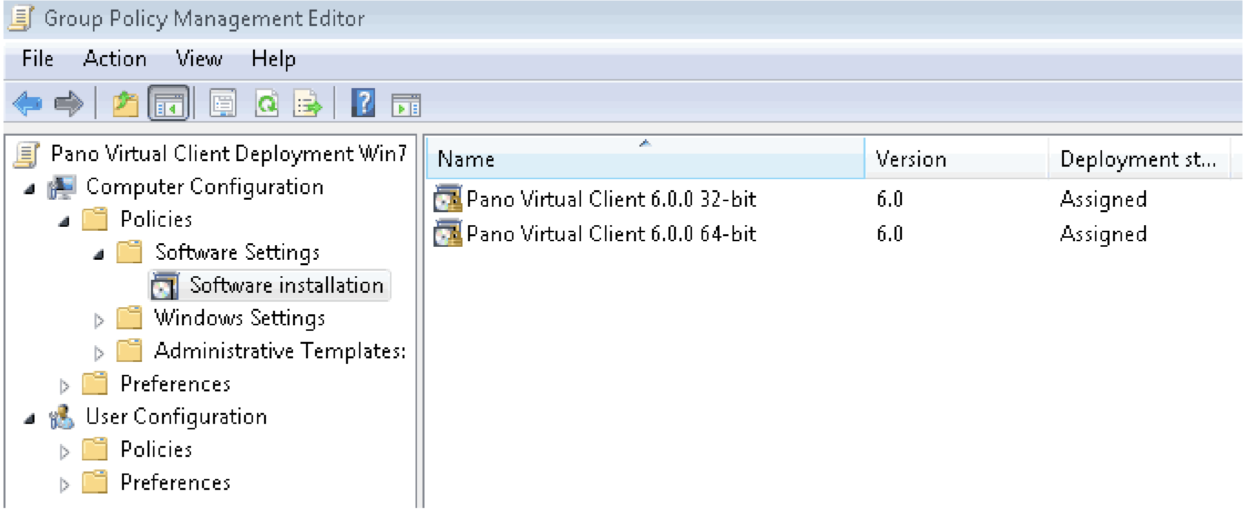
The following GPOs are linked to this WMI filter:

GPO
Pano Virtual Client Deployment Win7

Edit the newly created WMI filter for Windows 7 and use the WMI Query:

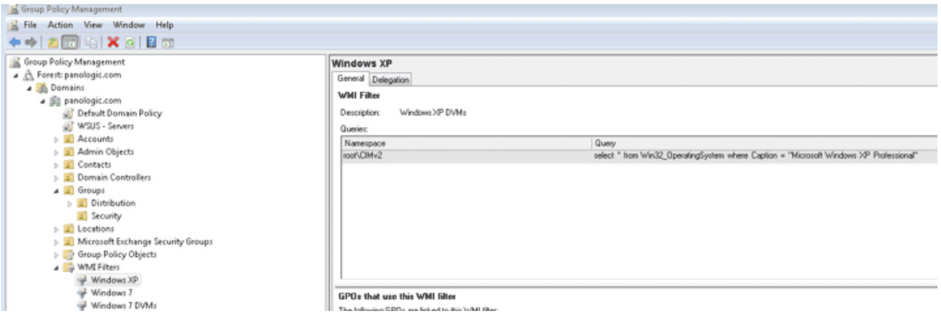
- Select * from Win32_OperatingSystem where Version like "6.1%" and ProductType = "1"
- Add a Windows 7 Pano Virtual Client Deployment GPO which uses this WMI filter.

  This screen shows a Group Policy for Windows 7, with images for both 32-bit and 64-bit Windows. A GPO screen for XP will be similar.



Name	Version	Deployment st...
Pano Virtual Client 6.0.0 32-bit	6.0	Assigned
Pano Virtual Client 6.0.0 64-bit	6.0	Assigned

3. Add a WMI filter to restrict GPO to Windows XP as shown below:



Description: Windows XP DVMs

Queries:

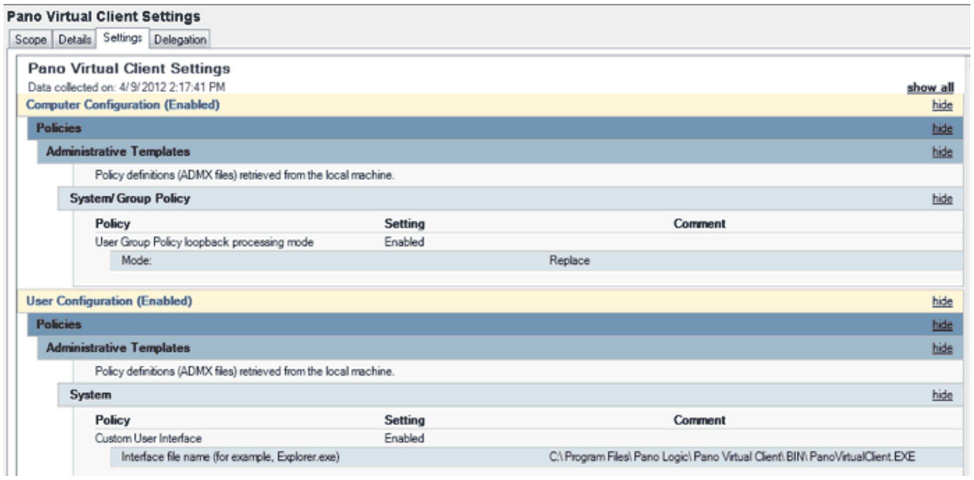
Namespace	Query
root\CIMv2	select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP Professional"

Edit the newly created WMI filter for Windows XP. Use the WMI Query by selecting * from Win32_OperatingSystem, where Caption = "Microsoft Windows XP Professional". Then add a Windows XP Pano Virtual Client GPO which uses this WMI filter

Configure Windows PC to Launch Pano Virtual Client Alternative Shell

1. Define a security group in Active Directory. Add the users and computer objects that will use the Pano Virtual Client to the security group. The users in this group do not need any special privileges beyond that of existing in the local users group on each PC – i.e. being a member of “Domain Users” in Active Directoryis sufficient.
2. Create a new group policy, called Pano Virtual Client Settings, with the settings listed below. Apply the group policy to the OU created to hold Pano Virtual Clients, and then restrict the GPO to this group (remove authenticated users).

3. Edit this Group Policy with the settings defined below:



Pano Virtual Client Settings

Data collected on: 4/9/2012 2:17:41 PM

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local machine.

System/ Group Policy

Policy	Setting	Comment
User Group Policy loopback processing mode	Enabled	
Mode:	Replace	

User Configuration (Enabled)

Policies

Administrative Templates

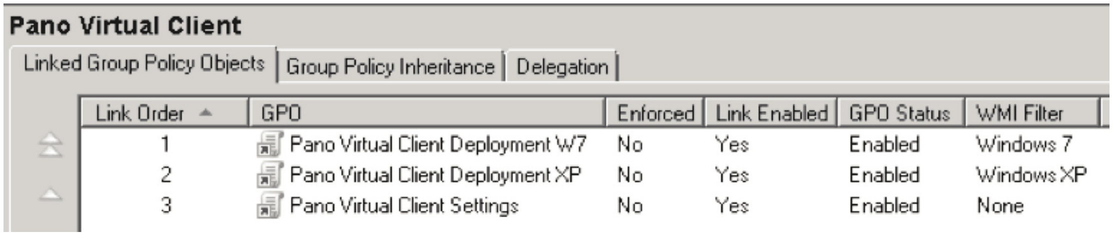
Policy definitions (ADMX files) retrieved from the local machine.

System

Policy	Setting	Comment
Custom User Interface	Enabled	
Interface file name (for example, Explorer.exe)	C:\ Program Files\ Pano Logic\ Pano Virtual Client\ BIN\ PanoVirtualClient.EXE	

Order of GPOs on Pano Virtual Client OU

The order of GPOs is important as it ensures that polices are only applied after the software installed. Please follow the order as illustrated below. If deploying to both Windows XP and Windows 7 PCs, you should see a total of three different GPOs applied to the same OU.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Pano Virtual Client Deployment W7	No	Yes	Enabled	Windows 7
2	Pano Virtual Client Deployment XP	No	Yes	Enabled	Windows XP
3	Pano Virtual Client Settings	No	Yes	Enabled	None

Check PCs

To ensure your host PCs are ready, please follow the steps below

1. Anti-virus software may inhibit the automatic installation of Pano Virtual Client by Active Directory. You may need to temporarily disable any AV software when rolling out Pano Virtual Client. It can then be re-enabled.
2. If you do not plan to use the PC as a local machine, you may wish to erase the drive and re-install the OS. This eliminates any chance of software conflict between Pano Virtual Client and the host.
3. Some peripherals (e.g. a biometric scanner or a bluetooth device) may attempt to load drivers into Pano Virtual Client. If these peripherals are not needed in Pano Virtual Client, remove them before installing Pano Virtual Client. If they are needed, make sure you have drivers for the version of Windows 7 that your Pano Virtual Client will run,
4. Please make sure the data and time on the PCs is correct once they are joined to your Active Directory domain.
5. Host PCs which have not been rebooted in a long time may have aged out of the current Group Policy. Consider rebooting each host PC before deploying Pano Virtual Client.
6. Allow some time for the Group Policy to be applied and the Pano Virtual Client to be deployment to the selected host PCs.

7. To turn on secondary display on Pano Virtual Client you need to enable the settings from host PC's Windows. To do that, boot up the Pano Virtual Client, then select the Logoff button from the Connection Bar (see below) and login as a user with administrative rights in the host PC's Windows. Once you've logged in, right-click anywhere on the desktop and select Screen Resolution, in the Screen Resolution control panel select the secondary display (at "Display:") and choose "Extend desktop to this display" (at "Multiple displays:").

Prepare DVMs

Before logging into a DVM, you must configure it to work with the Pano Virtual Client. For each DVM, be sure to update the Pano Direct Service to version 6.0.0 or later. Once you've done that the DVMs can be used with both Pano Virtual Client endpoints and with Pano Zero Clients and Pano Remote.

Using Pano Virtual Client

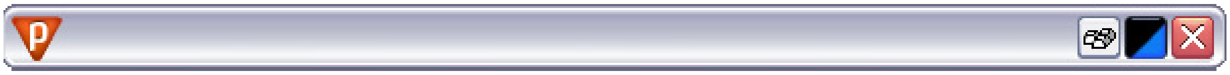
Login and Options Dialogs

When using thePano Virtual Client you'll initially be presented with a login dialog just like on a Pano Zero Client. You can enter a valid user name and password and then select one of two buttons at the bottom of the login dialog:

1. Login – will take you to the last DVM accessed by your user name.
2. Options – takes you to the options dialog letting you select a different Desktop (DVM) from your list of authorized DVMs.

Connection Bar

To control or end a Pano Virtual Client session move the mouse pointer to the top center of the screen and the Connection Bar will appear:



The buttons on the Connection Bar have the following functions:

- **Ctrl-Alt-Del** - sends a Ctrl+Alt+Del keypress to your Pano DVM. Pressing this button may let you regain control of your DVM if it becomes unresponsive but will have no impact on your local Windows operating system on the test PC. If you need to send a Ctrl-Alt-Del keypress to the local Windows operating system on your PC, press the actual Ctrl, Alt, and Del keys on your keyboard instead
- **Status/Disconnect** - displays both the connection status (like the hardware Pano Button on Pano Zero Clients) and when connected, end your Pano DVM session and return to the Pano Virtual Client login dialog equivalent to pressing the Pano Button on a Pano Zero Client to end your Pano session. Doing this will not shutdown or reboot your Pano DVM or the host PC's Windows operating system, nor will it exit the Pano Virtual Client shell.

  Status indications are by color:

- Red: no IP address (from DHCP) or no network connection found.
- Amber: Awaiting connection fromPano Controller or DVM.
- Blue: Connected to Pano Controller or DVM - can press to Disconnect session.
- ☒ **Logoff** - pressing this button will both disconnect your Pano session and temporarily stop the Pano Virtual Client software or shell, returning you to the local Windows login and allowing you to login under a different user account to use the local Windows operating system on your PC, or to shut-down or restart the host PC's Windows operating system

Windows Keys and Pano Virtual Client

Some special keys used by Windows can cause confusion when working inside Pano Virtual Client sessions:

- If running Windows 7 on the host PC or in the DVM hitting the Windows (logo) Key + L will lock both Windows 7 on the host PC and the DVM. To unlock, first unlock the host PC (no password is needed), then unlock your DVM by entering the same password you used when logging in.
- Pressing Ctrl + Alt + Del directly will be sent only to the host PC's Windows. To send Ctrl+Alt+Del to your DVM use the button on the Connection Bar, described above.

Using Pano Virtual Client on Wireless Networks

Officially, Pano Virtual Client is not supported over wireless or Wi-Fi networks but with preplanning and certain cautions it can be run over these types of wireless networks. In most cases we recommend Pano Remote for connections over wireless networks because the protocol Pano Remote uses, Microsoft RDP, is more resistant to the network congestion and latency issues common to wireless networks. If you do wish to use Pano Virtual Client over a wireless network there are a number of guidelines you should follow to help ensure good performance.

Planning for Pano Virtual Client Use on Wireless Networks

Size the network to provide generous bandwidth and coverage. 802.11n Wi-Fi connections are preferred over the lower bandwidth 802.11b/g. Pano Virtual Client generates much more traffic that normal connections from laptops or other mobile devices. This is because Pano Virtual Client transfers the entire display image as well as all USB traffic over the wireless connection, not just files and web pages.

The bandwidth used by Pano Virtual Client is highly dependent on the frequency of display updates; it isn't possible to give a fixed value. If users are just sitting at the Windows desktop, very little bandwidth is used. However, if they are viewing full-screen video or scrolling through large spreadsheets or presentation decks a large amount of bandwidth will be used. This will not only slow down the active user but may impact other uses of the WLAN. With only one or two Pano Virtual Client users this impact is not likely to be noticeable but larger numbers might periodically swamp even robust wireless networks.

High-bandwidth USB devices, such as USB mass storage devices, scanners, and printers are not recommended for wireless connections as they can generate large amounts of traffic. For example, even just mounting a flash drive and having it show up in Windows Explorer can cause significant delays in operations.

Prepare Pano Virtual Client Hosts for Use over Wireless Networks
Users must first connect to the local wireless network before launching Pano Virtual Client, because once Pano Virtual Client is running the local Windows desktop and task bar are hidden.

During a Pano Virtual Client session users can't to monitor possible drops in the strength of their connection because the local Windows task bar won't be visible.

If a user running Pano Virtual Client on a laptop moves out of range the network connection will be temporarily severed and the Pano session will disconnect. The Pano session will still be running on the DVM server, so as soon as the user regains a network connection, a login window will appears and they can resume using the DVM.

Using Pano Virtual Client on Laptops

Pano Virtual Client works on many laptops provided that they meet the hardware and OS requirements for host PCs. However, laptops usually have tight integration between hardware and the local Windows OS; use of Pano Virtual Client entails a few added considerations.

Laptop Hardware Settings
Laptops often use sets of vendor-specific drivers to work with the hardware power management capabilities. These settings will remain active even while running Pano Virtual Client but the settings will not be accessible unless you log out of Pano Virtual Client and log in to the local Windows desktop. Be sure to set any power management policies as needed in the local Windows desktop on the host laptop before starting a Pano Virtual Client session.

Dual Active Network Interfaces
Laptops often have both a wireless Network Interface Card (NIC) and a wired Ethernet NIC, each with their own unique MAC address. Pano Controller identifies Pano Virtual Client installations by the MAC address of the active NIC - if both of these network connections are used the laptop may be listed twice in the Pano Controller Clients tab. Please note that this has no impact on Pano Virtual Client licensing as that is tied to concurrent connections, not to the number of installations or client MAC addresses.

Battery Status Monitoring
Laptops often have software indicators of when the battery is running low. Software warnings will not be visible while in a Pano Virtual Client session. However, hardware warnings, such as audible beeps (often set up in the laptop's BIOS settings) and battery indicator lights should still function while Pano Virtual Client is running. If you are using Pano Virtual Client on a laptop that is running on battery be sure to watch for any indicators that your battery power is depleted. If you laptop does shutdown from lack of power you will be

disconnected from your Pano session but it will continue running on the DVM server. You will just need to reconnect to it from the recharged laptop or from another endpoint like a Pano Zero Client to continue your use of the DVM.

Specialized Input Devices

Laptops typically have specialized pointing devices such as trackpads or trackpoints which support enhanced input options like tap to click, scrolling, and multi-touch gestures. These are enabled and controlled by vendor-specific drivers and control panel extensions loaded into the local Windows OS. When used as a platform for Pano Virtual Client, some of these special functions will not work and the laptop pointing devices will be treated as a standard input device. Disabling settings in the local Windows control panel, such as disabling tap to click, may also be ignored while running Pano Virtual Client.

Specialized Buttons/Keys

Laptops often have dedicated hardware buttons such as audio volume up/down/mute. Generally speaking, pressing these hardware buttons will have no effect during a Pano Virtual Client session. However, function key combinations (such as Fn-F4 to sleep) will often still work while in Pano Virtual Client, provided you have loaded vendor-supplied drivers and software in the local Windows OS and the function-key combinations were working before Pano Virtual Client was installed. No drivers need to be loaded into the virtual Windows system to which you connect. On-screen confirmation and control dialogs tied to these function keys may or may not be displayed while in the Pano Virtual Client session.

37
Pano Controller Administration

This section provides information on a number of basic system administration functions. Additional administrative functions can be found in:

- Setting Up DHCP
- DVM Administration
- Optimize DVM Performance
- Endpoint Administration
- Define USB Peripheral Support
- Configure & Manage Pano Zero Clients & Desktop Preferences
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen

Pano Controller Tasks

- Power On Pano Controller
- Power Off Pano Controller
- Log On To Pano Controller
- Log Off from Pano Controller
- Log On to Pano Controller VM
- Log Off from Pano Controller VM
- Filter and Sort in Pano Controller
- Reorder and Resize Columns in Pano Controller
- Retrieve IP Address of Pano Controller
- Enable Secure Connections
- Enable Secure Connections
- Initiate Secure Connections

Power On Pano Controller

1. From Hosts and Clusters in vCenter Server or XenCenter, right-click on the Pano Controller VM.
2. Select **Power On**.

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

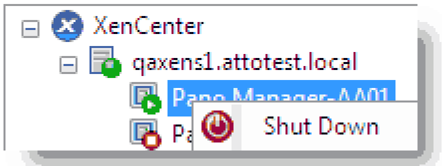
Power Off Pano Controller

To power off the Pano Controller on *VMware*:

1. From Hosts and Clusters in vCenter Server, right-click on the Pano Controller VM.
2. Select **Power Off**.

To power off the Pano Controller on Citrix:

1. From XenCenter, right-click on the Pano Controller VM in the navigation pane.
2. Select **Shut Down**.



Log On To Pano Controller

To administer your deployment, use the Pano Controller administrator interface.

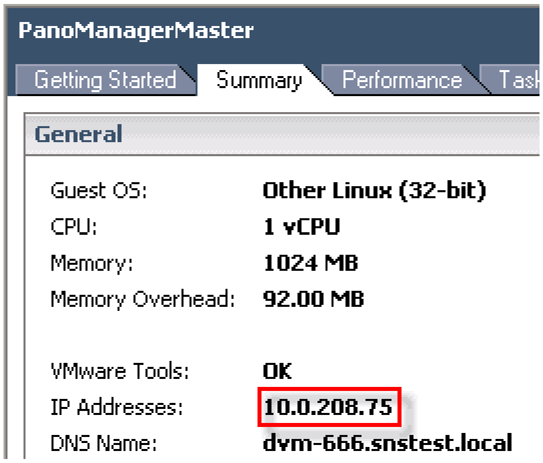
Refrain from logging on to the Pano Controller administrator interface with the `root` account; rather, you should use the `admin` account.

1. Retrieve the Pano Controller's IP address.
2. Go to `http://`***`hostname`***`/admin.jsp` or `http://`***`ipaddress`***`/admin.jsp`, where `hostname` or `ipaddress` is the hostname or IP address of the Pano Controller virtual machine.
3. Log on using one of the following accounts:
   - **Administrator** (Recommended). There is no default password: the password was set when the Pano Controller was configured as part of deployment.
   - **Superuser**. There is no default password: the password was set when the Pano Controller was configured as part of deployment.

Log Off from Pano Controller

To administer your deployment, use the Pano Controller administrator interface. To log off the Pano Controller administrator interface, from the Pano Controller, click **logout**.

Retrieve IP Address of Pano Controller



General

Guest OS: Other Linux (32-bit)
CPU: 1 vCPU
Memory: 1024 MB
Memory Overhead: 92.00 MB

VMware Tools: OK
IP Addresses: 10.0.208.75
DNS Name: dvm-666.snstest.local

1. Power on the Pano Controller, if it isn't already.
2. From the vSphere Client, click the **Summary** tab.
3. In the **General** section, record the IP address in the IP Addresses field.

Log On to Pano Controller VM

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

- Reset To Default Certificate
- Change Web Admin Account Password
- Change Pano Controller VM Network Settings

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

1. Power on the Pano Controller, if it isn't already.
2. From vCenter Server, right-click on the Pano Controller 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 Controller console displays.

Log Off from Pano Controller VM

Do one of the following:

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

Enable Secure Connections

To enable secure connections to any host, you must enable `ssh`. Occasionally you need to connect to the Pano Controller 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. 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. From the ESXi host's console, 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.
   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 a new vi user, let's walk through how to delete the `#`: simply move the cursor to the line that begins with `#ssh`, then press the **Insert** key. Using the arrow key, move the cursor over one space, then press the **Backspace** key to delete the `#`. Now for the easy part.
2. Save the changes: press **ESC** then type **:wq!**. If you make a mistake, press the **ESC** key and then type it **:q!** to quit vi without saving the file.
3. Do the following:
   - Run the following command to determine the process ID for the `inetd` process:

```
# ps | grep inetd
```

   The output of the `inetd` command has a number, a process ID, associated with it. You must kill this process, then restart the `inetd` process:

```
# kill -HUP process_id
# inetd
```

   You should now be able to access the host via SSH. If you can't, browse the comments on this VMware help topic.

Initiate Secure Connections

Occasionally you need to connect to the Pano Controller VM using a secure connection (for example, `scp` or `sftp`). There are many tools such as Filezilla or WinSCP that enable you to connect without having to use a command line; some users find Filezilla easier to use and more reliable. For security reasons, the Pano Controller 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 Controller 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 Controller 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).

Verify vCenter Server Licenses

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

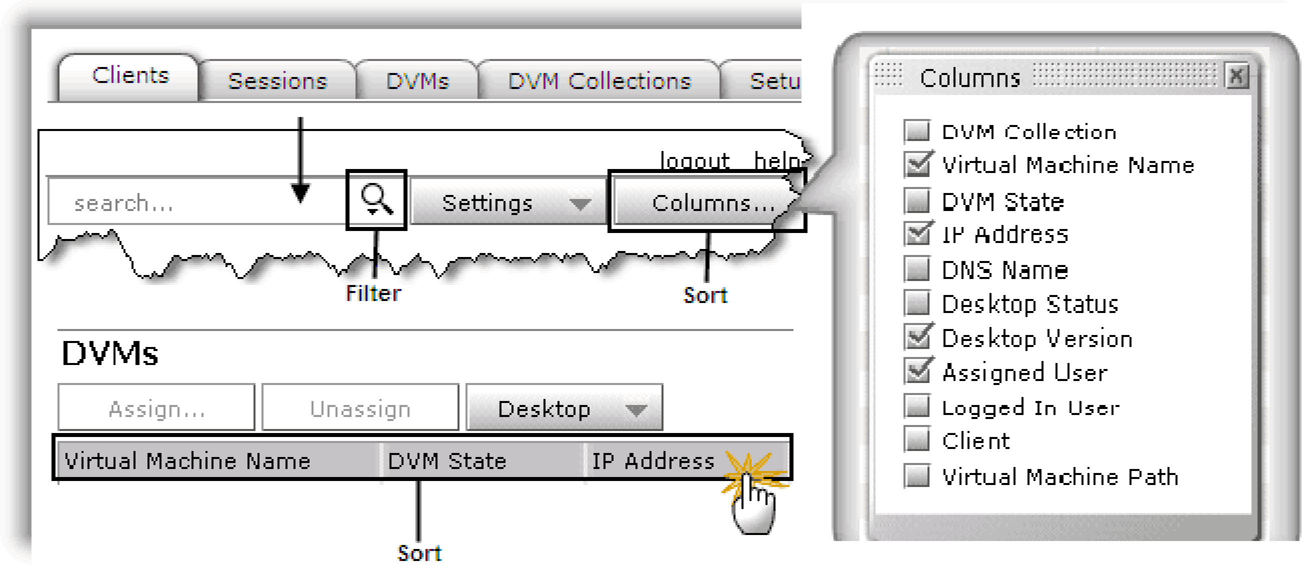
To verify vCenter Server license:

1. Using the vSphere Client, log on to vCenter Server.
2. Go to **Configuration** tab > **Licensed Features** link > **License Sources** link > **Edit**.

Filter and Sort in Pano Controller

As you provision more and more virtual desktops you'll begin to appreciate Pano Controller's filter and sort capabilities. For example, you might want to search for virtual desktops running a specific version of Pano Direct Service or search for a specific DVM. As a matter of fact, you can search based on any string, and the Pano Controller will remember your most recent queries.

You can filter and sort from three tabs within the Pano Controller: **DVMs** tab, **DVM Collections** tab, and **Pano System Endpoints** tab.



Columns

☐ DVM Collection
☑ Virtual Machine Name
☐ DVM State
☑ IP Address
☐ DNS Name
☐ Desktop Status
☑ Desktop Version
☑ Assigned User
☐ Logged In User
☐ Client
☐ Virtual Machine Path

To filter information:

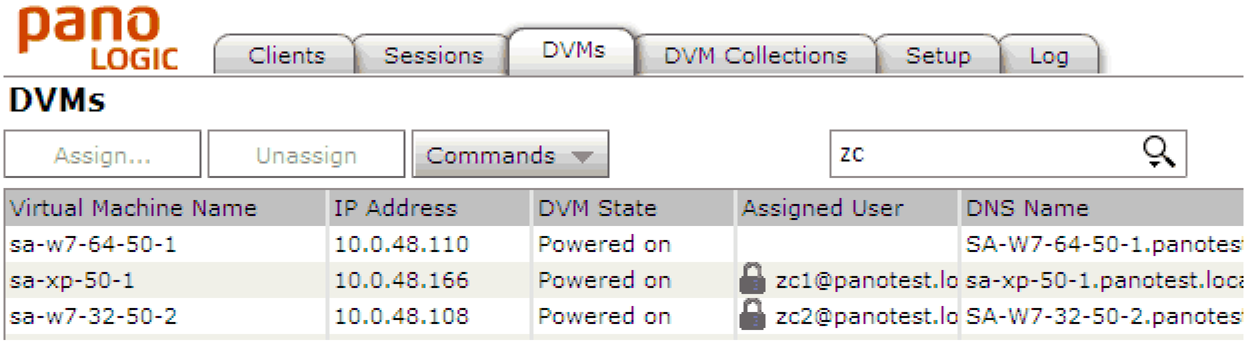
1. Ensure that the columns on which you want to filter appear in the table.

   You cannot filter on columns that are not displayed.
2. From either the DVMs tab, DVM Collections tab, or the Assigned Clients tab, type a value in the search box. This value can appear in any column.

   The search box filters out any rows that do not contain a matching string.

Example: Filter

Let’s search for John’s DVM. Type part of that user’s user name. Notice that the search returns fewer table rows, leaving two matching strings in the following example. This is a good way to search for information about a particular user’s DVM.



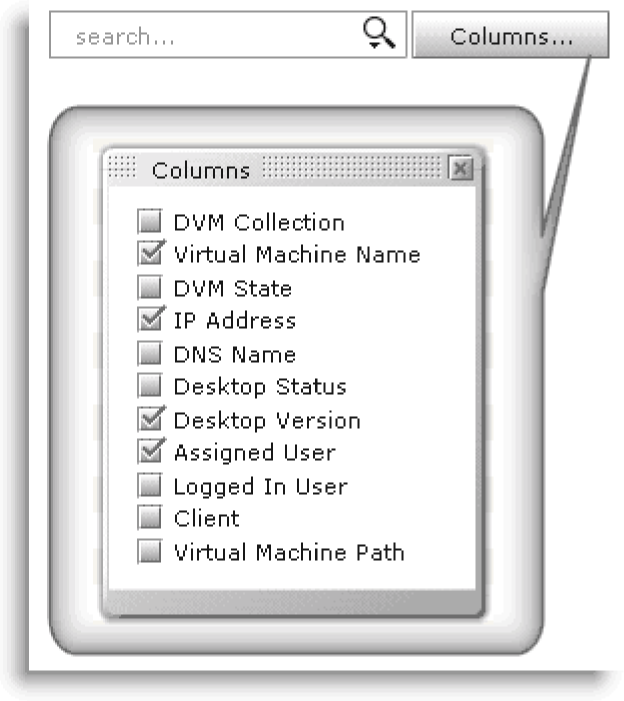
DVMs

zc

Virtual Machine Name	IP Address	DVM State	Assigned User	DNS Name
sa-w7-64-50-1	10.0.48.110	Powered on		SA-W7-64-50-1.panotes
sa-xp-50-1	10.0.48.166	Powered on	zc1@panotest.lo	sa-xp-50-1.panotest.loca
sa-w7-32-50-2	10.0.48.108	Powered on	zc2@panotest.lo	SA-W7-32-50-2.panotes

To sort information:

1. Click on any column header to sort the information in ascending or descending order.
2. (Optional) Click on the **Columns** button, then select or clear any of the column check boxes to include or exclude specific columns.



Columns

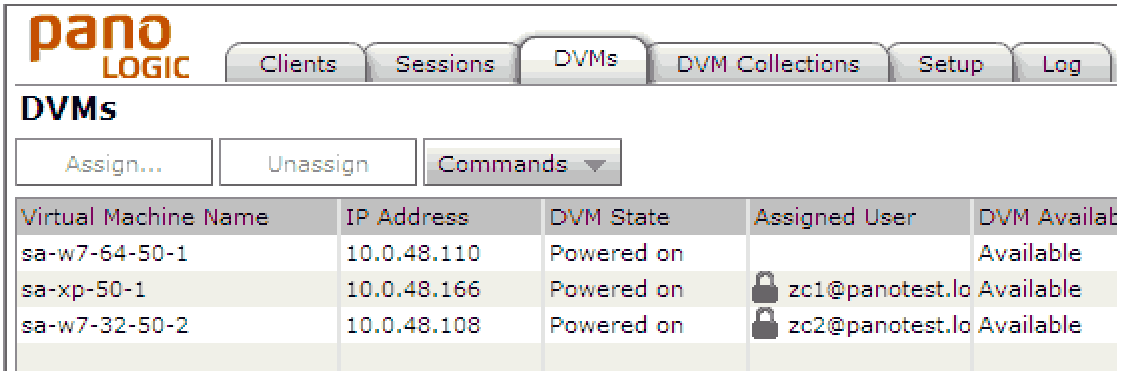
☐ DVM Collection
☑ Virtual Machine Name
☐ DVM State
☑ IP Address
☐ DNS Name
☐ Desktop Status
☑ Desktop Version
☑ Assigned User
☐ Logged In User
☐ Client
☐ Virtual Machine Path

3. (Optional) Perform a filter to display a subset of the information.

Example: Sort by Pano Direct Version

Let’s sort for all virtual desktops that are not running `Pano Direct Service 2.8`. This search is good if you just performed an upgrade of Pano Direct Service and want to verify that there are no virtual desktops running an older version of Pano Direct Service.

The following example shows that there are many virtual desktops still running an older version. If you want to display a subset of the information, you can perform a filter in conjunction with the sort. For example, you can isolate all virtual desktops running `Pano Direct Version 3.5`.

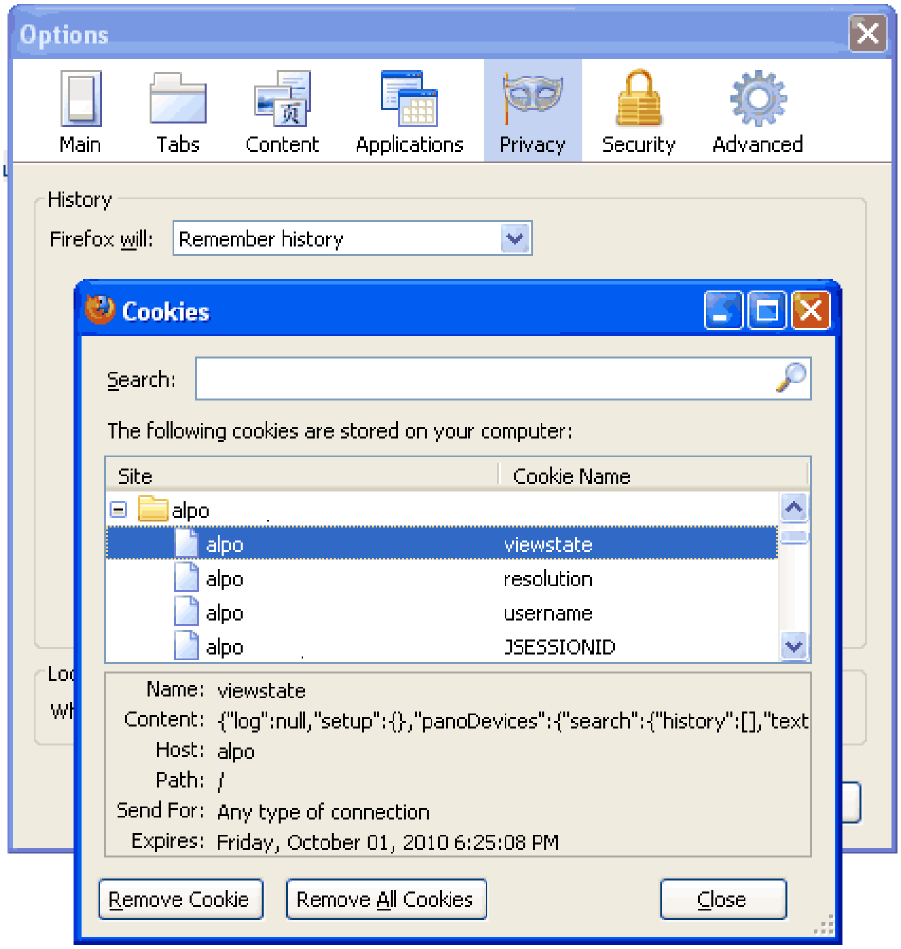


Virtual Machine Name	IP Address	DVM State	Assigned User	DVM Availab
sa-w7-64-50-1	10.0.48.110	Powered on		Available
sa-xp-50-1	10.0.48.166	Powered on	🔒 zc1@panotest.lo	Available
sa-w7-32-50-2	10.0.48.108	Powered on	🔒 zc2@panotest.lo	Available

Reorder and Resize Columns in Pano Controller

You can reorder or resize any column in the Pano Controller. These customizations persist until you change them (you cannot "undo"); in other words, each time you log on to the Pano Controller you will see your preferred table layout. This feature enables each administrator to have a unique table view.

If you want to return to the Pano Controller's default column ordering you can manually reorder; however, if you've changed the order and size of many columns a faster way to return to the Pano Controller's default ordering is to delete the **view state** cookie for your Pano Controller.



Firefox will: Remember history

Search:

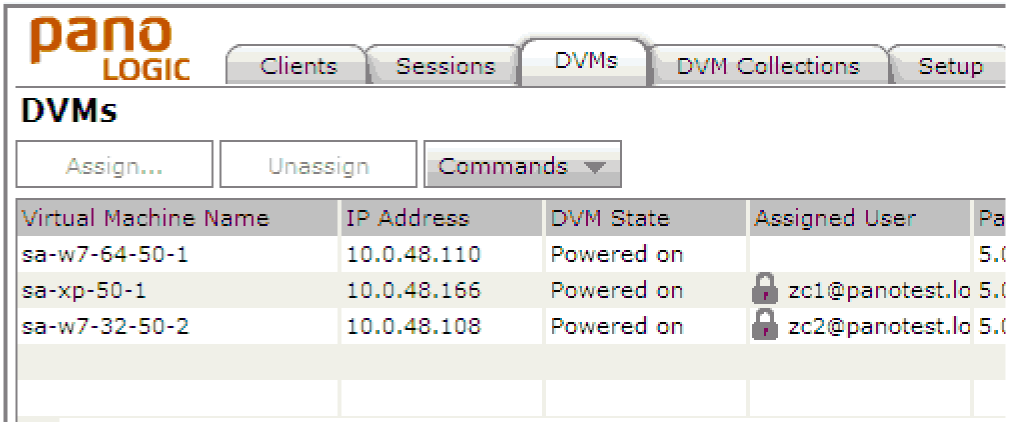
The following cookies are stored on your computer:

Site	Cookie Name
alpo	
alpo	viewstate
alpo	resolution
alpo	username
alpo	JSESSIONID

Name: viewstate
Content: {"log":null,"setup":{},"panoDevices":{"search":{"history":[],"text
Host: alpo
Path: /
Send For: Any type of connection
Expires: Friday, October 01, 2010 6:25:08 PM

To reorder columns:

Simply select any column, then drag and drop it before or after any column. A green divider indicates where the column will be placed.



Virtual Machine Name	IP Address	DVM State	Assigned User	Pa
sa-w7-64-50-1	10.0.48.110	Powered on		5.(
sa-xp-50-1	10.0.48.166	Powered on	zc1@panotest.lo	5.(
sa-w7-32-50-2	10.0.48.108	Powered on	zc2@panotest.lo	5.(

To resize columns:

You can change the width of any column. Simply place the pointer over the right edge of the column and drag the column's vertical slider to increase or decrease the width of the column.

38
Setting Up DHCP

Many installations will use DHCP configuration options to support Pano Logic endpoint discovery. This section provides examples of DHCP configuration for several types of DHCP servers.

- Add Pano Logic Vendor Class for Linux DHCP Server
- Add Pano Logic Vendor Class for Netware DHCP Server
- Add Pano Logic Vendor Class for Cisco IOS DHCP Server
- Add Pano Logic Vendor Class for Alcatel/Lucent VitalQIP DHCP Server
- Add Pano Logic Vendor Class for Infoblox DHCP Server
- Add Pano Logic Vendor Class for Windows 2008 R2 DHCP Server

Add Pano Logic Vendor Class for Linux DHCP Server

Here is an example of `dhcpd.conf` for a Linux DHCP server:

```
option space ATTO;
option ATTO.broker-server-address code 1 = ip-address;
option ATTO.tnp-port code 2 = integer 16;
option ATTO.tnp-client-discovery-port code 3 = integer 16;
option ATTO.broker2-server-address code 4 = ip-address;
option ATTO.broker-server-address-alias code 101 = ip-address;
option ATTO.tnp-port-alias code 102 = integer 16;
option ATTO.tnp-client-discovery-port-alias code 103 = integer 16;
option ATTO.broker2-server-address-alias code 104 = ip-address;

class "vendor-classes" {
 match option vendor-class-identifier;
}
subclass "vendor-classes" "Pano Logic" {
 vendor-option-space ATTO;
 option ATTO.broker-server-address 192.168.1.55;
 #option ATTO.tnp-port 8321;
 #option ATTO.tnp-client-discovery-port 8320;
 #option ATTO.broker2-server-address 192.168.1.54;
 option ATTO.broker-server-address-alias 192.168.1.155;
 #option ATTO.tnp-port-alias 8311;
 #option ATTO.tnp-client-discovery-port-alias 8310;
 option ATTO.broker2-server-address-alias 192.168.1.154;
}
# private network
subnet 192.168.100.0 netmask 255.255.255.0 {
 # Atto clients should be identified as such
```

```
group atto_client {
subnet 192.168.100.0 netmask 255.255.255.0 {
 # --- default gateway
 option routers 192.168.100.55;
 option subnet-mask 255.255.255.0;
 option time-offset -18000;
 range dynamic-bootp 192.168.100.224 192.168.100.254;
 # default-lease-time 21600;
 default-lease-time 120;
 max-lease-time 43200;
}
}
```

Add Pano Logic Vendor Class for Netware DHCP Server

Here is an example of a configuration for a Netware DHCP server:

```
Option: (t=53, l=1) DHCP Message Type = DHCP ACK
Option: (t=58, l=4) Renewal Time Value = 5 minutes
Option: (t=59, l=4) Rebinding Time Value = 8 minutes, 45 seconds
Option: (t=51, l=4) IP Address Lease Time = 10 minutes
Option: (t=54, l=4) Server Identifier = 10.220.9.1
Option: (t=1, l=4) Subnet Mask = 255.255.255.0
Option: (t=3, l=4) Router = 10.220.9.1
Option: (t=43, l=6) Vendor-Specific Information
        Option: (43) Vendor-Specific Information
        Length: 6
        Value: 01040ADC641D
   End Option
   Padding
```

Where the value of option 43 must be in hex format (for example, `01040ADC641D`):

- The first byte (`01`) is the code.
- The second byte (`04`) is the length.
- The remaining bytes comprise the IP address of the Pano Controller after it has been converted to hex format (for example, `182.21.5709` converts to `0ADC641D`). Use this tool to convert the IP address to hex.

For more information, go to Using DHCP option 43 (Vendor Extensions).

Add Pano Logic Vendor Class for Cisco IOS DHCP Server

From your Cisco IOS CLI you need to specify the configuration mode, create a pool, and set a pool name for your Pano System Endpoints. You also need to set proper options.

Here is an example of a configuration for a Cisco IOS DHCP server.

```
ip dhcp pool PoolName
option 66 ascii “Pano Logic”
option 60 ascii “PXEClient”
option 43 hex 01:04:AC:13:35:17
```

Where the value of option 43 must be in hex format (for example, `01:04:AC:13:35:17`):

- The first byte (`01`) is the code.
- The second byte (`04`) is the length.
- The remaining bytes comprise the IP address of the Pano Controller after it has been converted to hex format (for example, `172.19.53.23` converts to `AC:13:35:17`). Use this tool to convert the IP address to hex.

Add Pano Logic Vendor Class for Alcatel/Lucent VitalQIP DHCP Server

In VitalQIP you must create a Client Class based on Vendor Class, so that DHCP hands out a particular DHCP Option 43 value to Pano System Endpoints that include the Vendor Class value of `Pano Logic` in addition to the normal options associated with the IP address.

To add a Pano Logic vendor class for Alcatel/Lucent VitalQIP:

1. Convert the IP address of the Pano Controller to hexadecimal by using this tool to find the hex value of each octet. For example, `10.220.100.29` converts to `0a-DC-64-1D`.
2. Set up a new DHCP Template for that Vendor Class:
   a. Choose **Options** > **DHCP/Bootp Templates** > **Option Template** > **Add**.
   b. From Available Classes/Values, find and expand Application and Services Parameters, select **Vendor Specific Information (43,vs)**, then click **Add**.
   c. Type the hex value in square brackets (for example, `[01040ADC641D]`). click **OK**.
      - The first byte (`01`) is the code.
      - The second byte (`04`) is the length.
      - The remaining bytes comprise the IP address of the Pano Controller after it has been converted to hex format (for example, `10.220.100.29` converts to `0a-DC-64-1D`.). Use this tool to convert the IP address to hex.
   d. Give this DHCP Option Template a name, such as `Pano Logic`–without quotes.
3. Add a Client Class:
   a. Choose **Policies** > **Client Class** > **Add**.
   b. Type a text value such as `Pano Logic`–without quotes–for the Client Class name, and type the correct value for Vendor Class.

      The Client Class must match Option 60 in the template and the value sent by the clients in their DHCP Discover.
   c. From the Option Template drop-down list, assign the appropriate DHCP Template that these Pano System Endpoints should use, then click **OK** to save.
4. Assign this Client class–`Pano Logic`–to the DHCP server:
   a. Choose **Infrastructure** > **Server** > **Modify**.
   b. In the Server Profile, click on the parameter **Client Class**. The Available Value shows the Client Class that you defined above.
   c. Add Available Value to this server's Active Values.

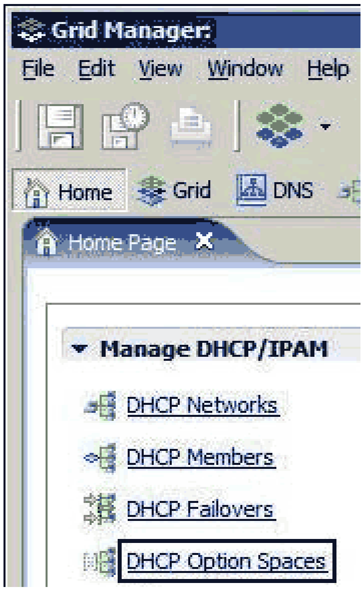
      You can have several Client Classes active on one server: one for Pano System Endpoint and perhaps others for other types of devices.
5. Be sure that the Server Profile does NOT have the policy `ForceClass=Vendor` set.
6. Perform a DHCP Generation (push).

   Afterward, the `dhcpd.conf` file shows a `vendor-class` definition at the end as well as the subnet definitions.

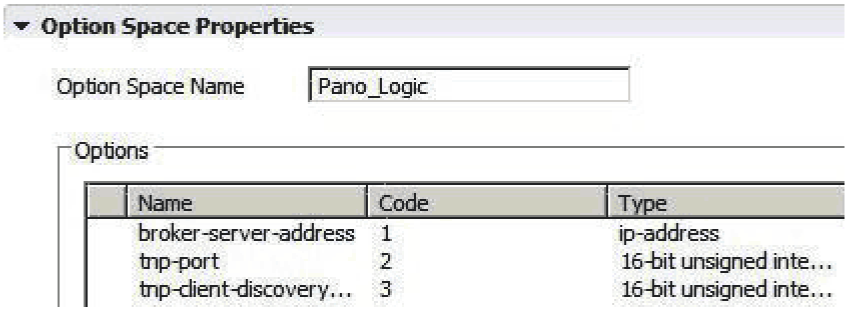
   When the DHCP server receives a DHCP-Discover from a certain subnet with a certain Vendor class, it will give out a lease from that subnet with the DHCP Template options defined for that subnet, plus the DHCP options which are defined for that vendor class. The DHCP options associated with the Vendor class will override those associated with the IP object or its subnet.

Add Pano Logic Vendor Class for Infoblox DHCP Server

1. From the Infoblox Grid Manager, go to the **Home Page** view > **Manage DHCP/IPAM** section, then click the **DHCP Option Spaces** link.



2. Create an Option Space Name called `Pano_Logic`.



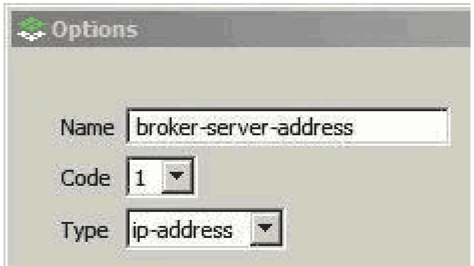
Option Space Name: Pano_Logic

Options

Name	Code	Type
broker-server-address	1	ip-address
tnp-port	2	16-bit unsigned inte...
tnp-client-discovery...	3	16-bit unsigned inte...

3. Add the Option Space options, then Save.

   a. Create the `broker-server-address` option, with values: name: broker-server-address; Code: 1: Type: ip-address

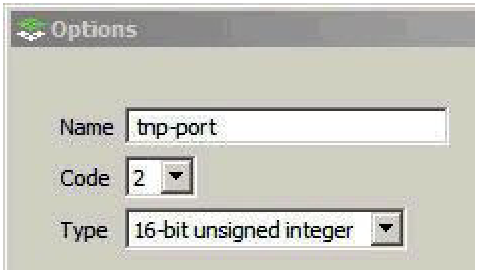


Name: broker-server-address

Code: 1

Type: ip-address

b. Create the `tnp-port` option, with values: name: tnp-port; Code: 2; Type: 16-bit unsigned integer



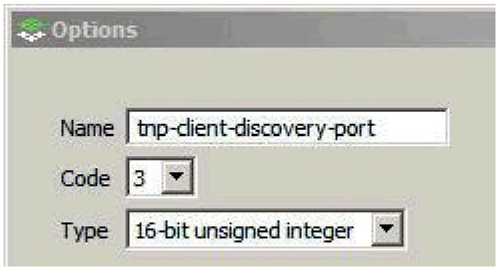
Options

Name: tnp-port

Code: 2

Type: 16-bit unsigned integer

c. Create the `tnp-discovery-port` option, with values: name: tnp-discovery-port; Code: 3; Type: 16-bit unsigned integer



Options

Name: tnp-client-discovery-port

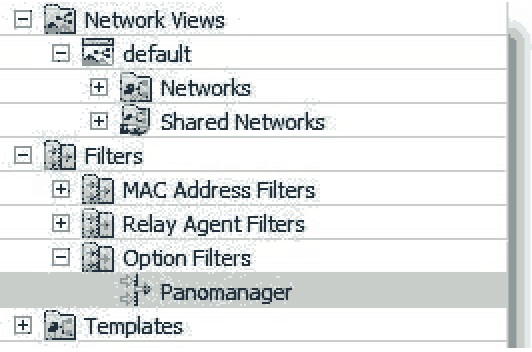
Code: 3

Type: 16-bit unsigned integer

4. Restart the grid services.

5. From the DHCP-IPAM view, select Option Spaces, then verify that the `Pano_Logic` option space with a value of `Pano_Logic` appears in the list.

6. From the DHCP-IPAM view, click on the Networks tab, expand Filters, right-click on the Option Filters to create a new Option Filter named `PanoController`:

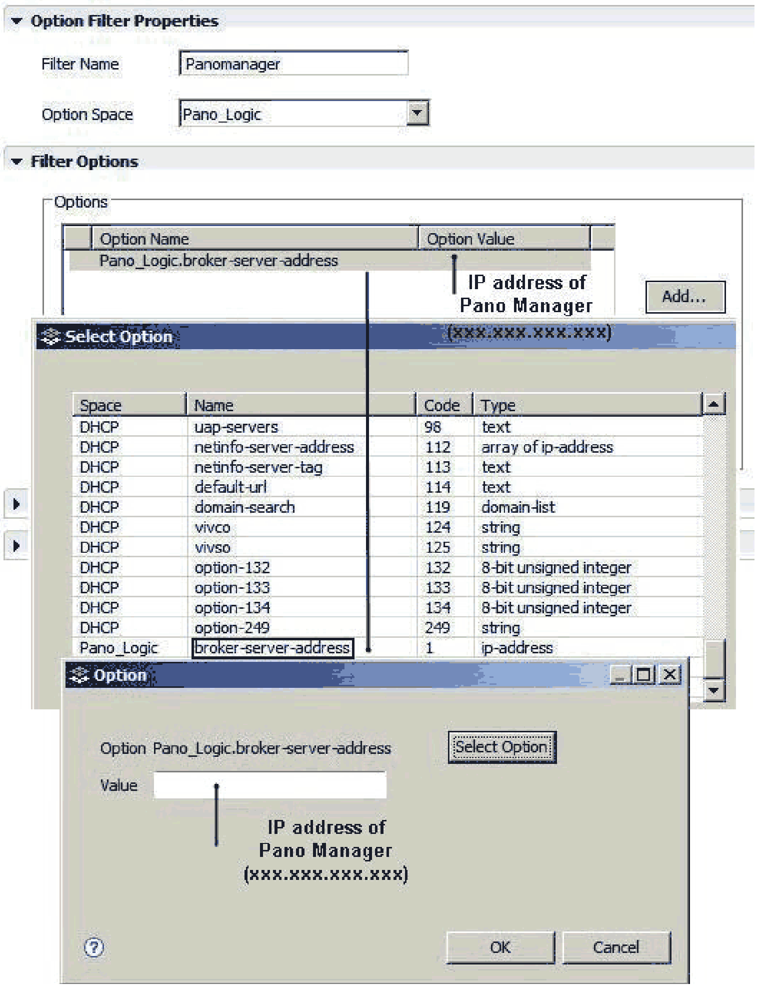


7. Edit the filter's properties:

a. In the Option Space drop-down list, choose `Pano_Logic`.

b. Select and add the `broker-service-address` option that you created in Step a.

c. Edit the IP Option Value to be the Pano Controller’s IP address, then **Save**.



Filter Name: Panomanager

Option Space: Pano_Logic

Option Name	Option Value
Pano_Logic.broker-server-address	

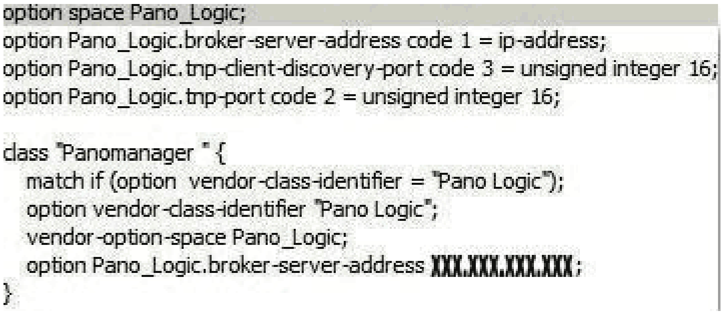
Space	Name	Code	Type
DHCP	uap-servers	98	text
DHCP	netinfo-server-address	112	array of ip-address
DHCP	netinfo-server-tag	113	text
DHCP	default-url	114	text
DHCP	domain-search	119	domain-list
DHCP	vivco	124	string
DHCP	vivso	125	string
DHCP	option-132	132	8-bit unsigned integer
DHCP	option-133	133	8-bit unsigned integer
DHCP	option-134	134	8-bit unsigned integer
DHCP	option-249	249	string
Pano_Logic	broker-server-address	1	ip-address

Option Pano_Logic.broker-server-address

Value

8. Restart the grid services again.

9. Go to the `dhcpd.conf` file and verify that the configuration looks identical to the following file. The IP must be the Pano Controller’s IP address.

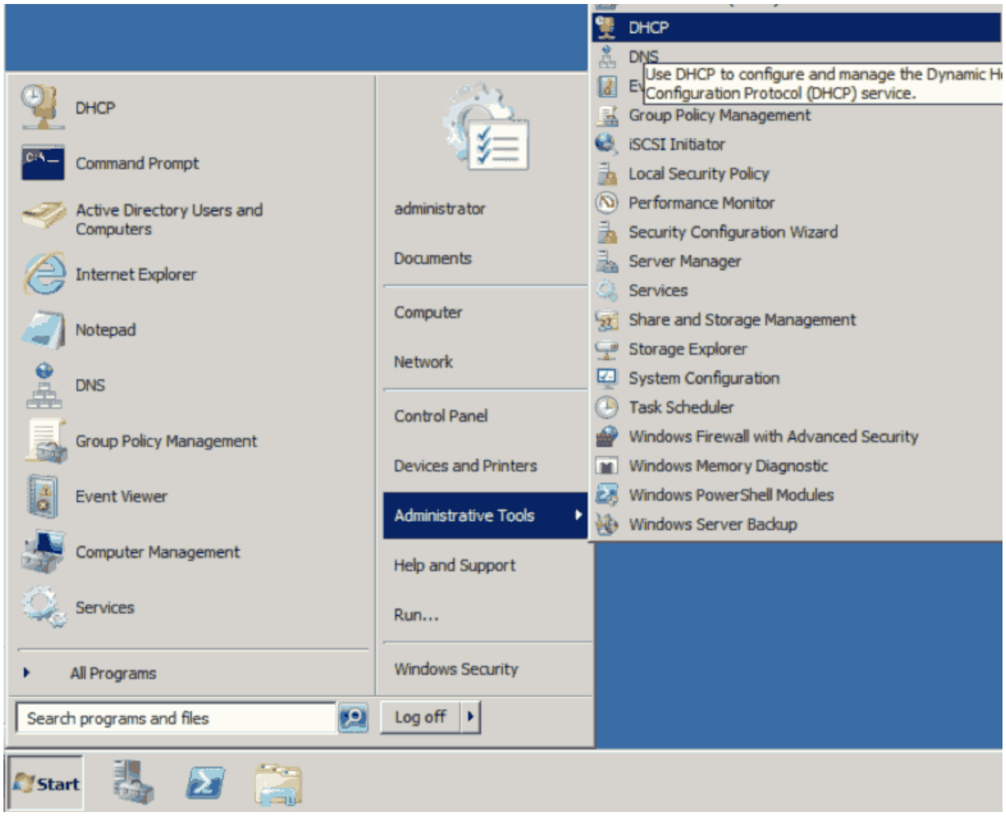


```
option space Pano_Logic;
option Pano_Logic.broker-server-address code 1 = ip-address;
option Pano_Logic.tnp-client-discovery-port code 3 = unsigned integer 16;
option Pano_Logic.tnp-port code 2 = unsigned integer 16;

class "Panomanager " {
   match if (option  vendor-class-identifier = "Pano Logic");
   option vendor-class-identifier "Pano Logic";
   vendor-option-space Pano_Logic;
   option Pano_Logic.broker-server-address XXX.XXX.XXX.XXX;
}
```

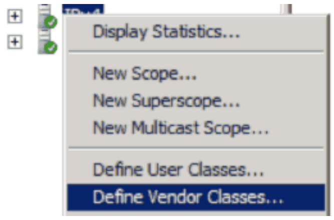
Add Pano Logic Vendor Class for Windows 2008 R2 DHCP Server

This section explains one of several ways to create a DHCP vendor class for Pano discovery on a Windows 2008 R2 DHCP server. Regardless of the exact method you choose, the details shown herein reference the fundamentals needed for managing a Pano deployment.

1. Log into a Windows 2008 R2 server running DHCP services and open the DHCP snap-in

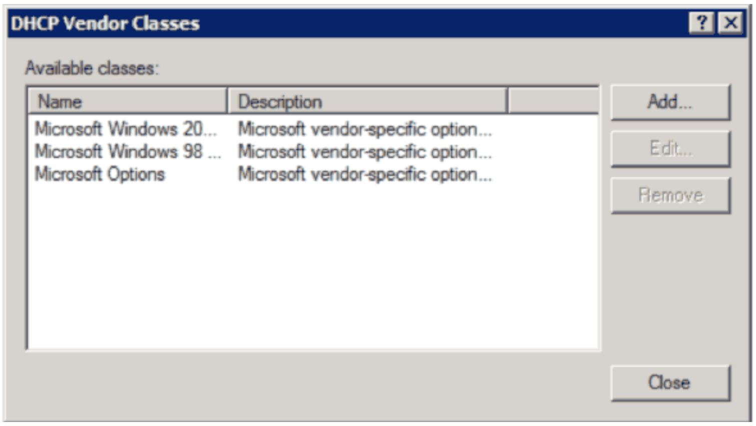


Use DHCP to configure and manage the Dynamic H Configuration Protocol (DHCP) service.



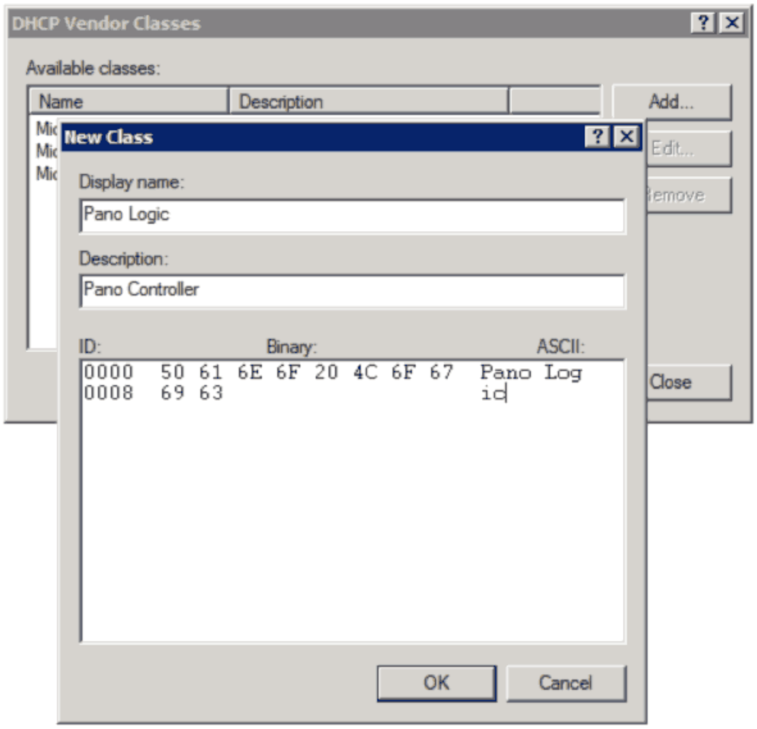
2.In the DHCP snap-in window, right-click on the IPv4 node and select Define Vendor Classes.

Note: Pano devices do not support IPv6 as of the time this KB article was written.



Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

3.A DHCP Vendor Classes window will open. Select the Add button to add a DHCP Vendor Class that will be used for Pano zero client discovery.



Display name: Pano Logic

Description: Pano Controller

```
ID:       Binary:                    ASCII:
0000   50 61 6E 6F 20 4C 6F 67    Pano Log
0008   69 63                      ic
```

4.In the New Class window, enter the following values:

Display Name: Pano Logic

Description: Pano Controller.

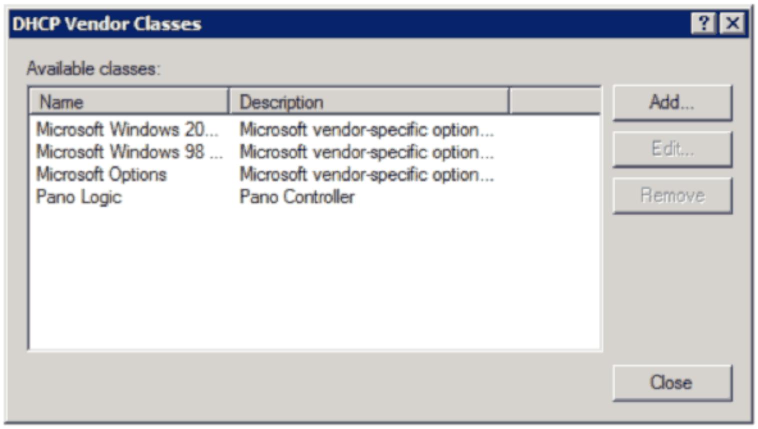
Note: This value just identifies the Pano Controller DHCP vendor class on your DHCP server.

Note: For those using Pano version 4.5.1 or earlier, the Description text can be ‘Pano Manager’ rather than ‘Pano Controller’. Pano Manager was renamed to Pano Controller starting with version 5.0.

Place the mouse cursor under the ASCII field and enter Pano Logic.

The Binary field will automatically update with a value based on the user input in the ASCII field.

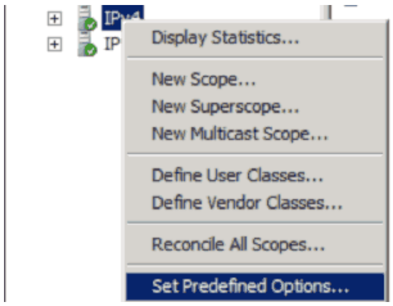
Confirm the settings, and then select the OK button to save these settings and proceed.



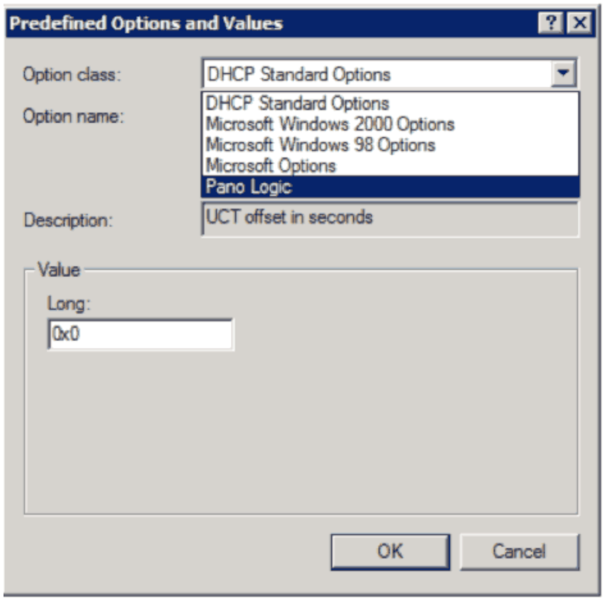
Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...
Pano Logic	Pano Controller

5.Verify that there is a newly created Pano Logic DHCP vendor class referenced in the DHCP Vendor Classes window. Once confirmed, select the Close button to exit the DHCP Vendor Classes window.

6.In the DHCP snap-in window, right click on the IPv4 node and select Set Predefined Options.



7.In the Predefined Options and Values window, select the Option Class dropdown box, then select Pano Logic.


Predefined Options and Values
?
X
DHCP Standard Options
Microsoft Windows 2000 Options
Microsoft Windows 98 Options
Microsoft Options
Pano Logic
Value
OK
Cancel

Option class: DHCP Standard Options

Option name:

Description: UCT offset in seconds

Long: 0x0

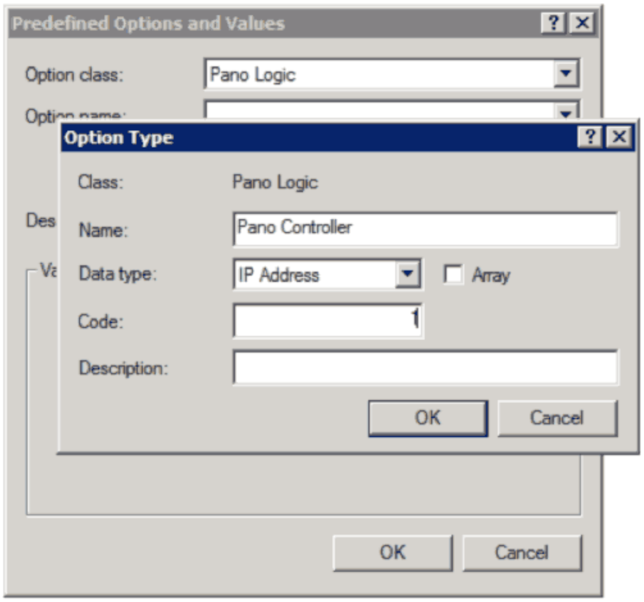
8.Select the Add button in the Predefined Options and Values window to enter the values that will be used for the Pano Logic DHCP vendor class.

In the Option Type window, verify that the Class is referenced as Pano Logic to match the DHCP vendor class that was created. Enter the following values in the Option Type window:

- Enter Pano Controller in the Name field
- Change the Data Type box to IP Address
- Enter either 1 or 101 in the Code text box

Verify the settings, and then select the OK button in the Option Type window to close this window.

Note: For environments that use option code 1 for another DHCP option, an error will be generated. Modify these settings to use option code 101 as an alternative.



Option class: Pano Logic

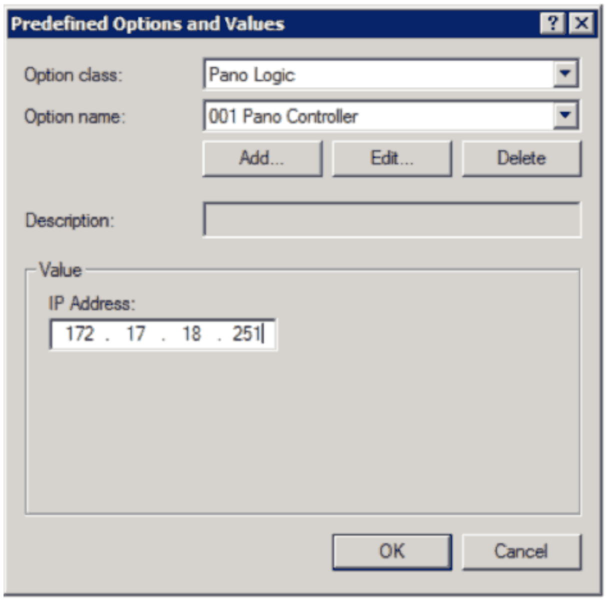
Class: Pano Logic

Name: Pano Controller

Data type: IP Address □ Array

Code: 1

Description:



Option class: Pano Logic

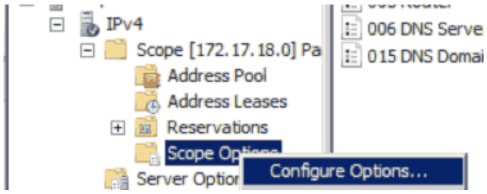
Option name: 001 Pano Controller

IP Address: 172 . 17 . 18 . 251

9.In the Predefined Options and Values window, enter the IP address of your Pano Controller that will be used to discover Pano devices in the Value>IP Address field.

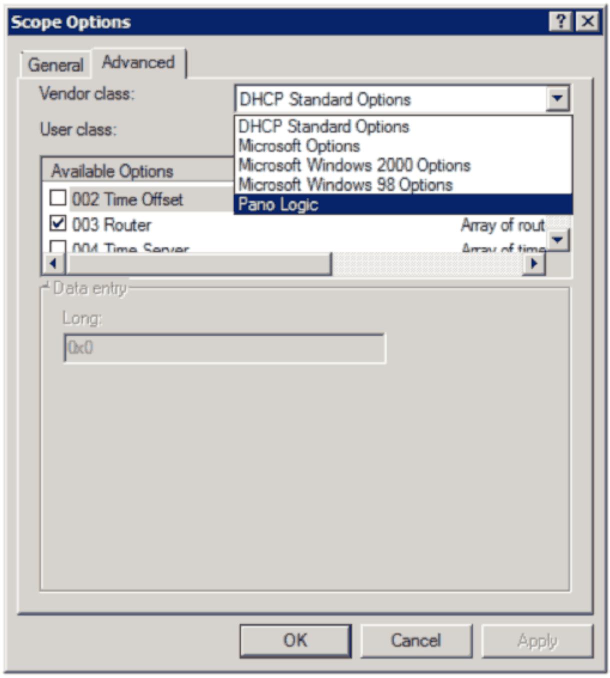
Note: If multiple Pano Controllers are deployed in a group/failover configuration, be sure that the IP address entered is the virtual IP address. This will allow Pano discovery to function as expected, should there be a failover.

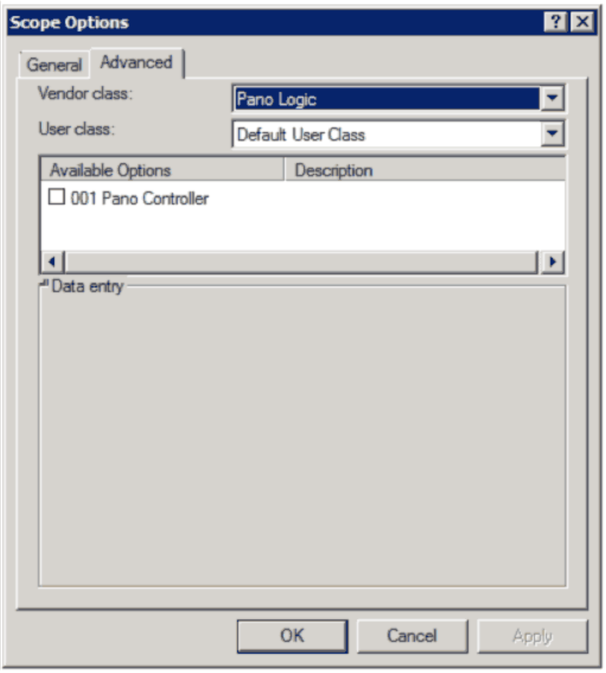
Confirm the IP address entered, and then select the OK button to close the Predefined Options and Values window.



10. In the DHCP snap-in window for any scopes in which Pano devices will be deployed to, expand the IPv4 node>Scope folder node. Select then right click on the Scope Options folder, then select Configure Options.

11. In the Scope Options window, select the Advanced tab>Pano Logic option from the Vendor Class dropdown box.

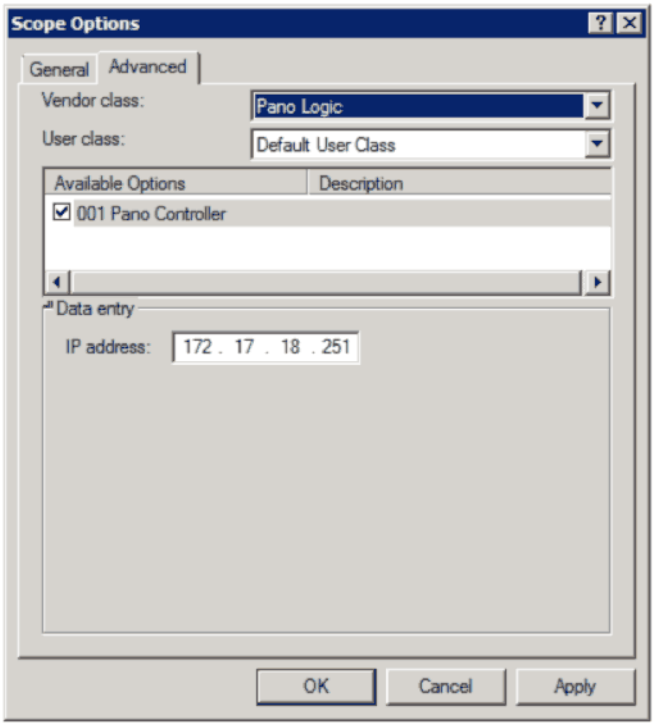




Vendor class: Pano Logic

User class: Default User Class

□ 001 Pano Controller



Vendor class: Pano Logic

User class: Default User Class

Available Options	Description
☑ 001 Pano Controller	

Data entry

IP address: 172 . 17 . 18 . 251

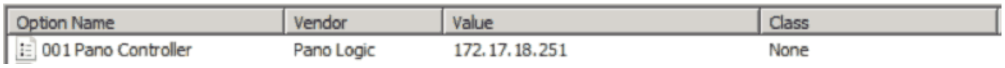
12. Verify that the Pano Controller vendor class is displayed under the Available Options field with the correct options code value previously configured in step 8 above.

Select the checkbox for the Pano Controller vendor class to activate the vendor class for that specific scope.

Verify that the Data Entry section shows the IP address of your Pano Controller or virtual IP address for your Pano Controller group nodes.

Note: If you are troubleshooting Windows 2008 R2 DHCP vendor class issues for Pano discovery, verify that the checkbox is enabled for Pano Controller on the Pano Logic DHCP vendor class on the applicable Scope Options folder.

The Scope Options folder for that specific scope in which the Pano Logic DHCP vendor class was enabled on should show the vendor class option code, name, vendor and IP address.

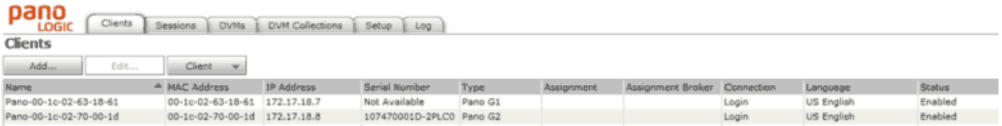


Option Name	Vendor	Value	Class
001 Pano Controller	Pano Logic	172.17.18.251	None

13. Select the Apply button to save the settings, then repeat steps 10 to 12 above for any additional Scopes where Panos will be deployed.

If multiple DHCP servers are deployed, verify that DHCP information is replicated or applied respectively where applicable.

Pano devices go through a standard DHCP process and show up in a Scope's Address Leases folder once the device has acquired an IP address. Pano devices do not have any values populated in the name field of the Address Leases, but they can be referenced in the Unique ID column. All Pano devices can be identified by the starting three bytes of the MAC address in the Unique ID column: 001c02.



Clients

Name	MAC Address	IP Address	Serial Number	Type	Assignment	Assignment Broker	Connection	Language	Status
Pano-00-1c-02-63-18-61	00-1c-02-63-18-61	172.17.18.7	Not Available	Pano G1			Login	US English	Enabled
Pano-00-1c-02-70-00-1d	00-1c-02-70-00-1d	172.17.18.8	107470001D-2PLC0	Pano G2			Login	US English	Enabled

The IP address should match what is displayed for the client in Pano Controller's Clients tab. If they do not, the device may be disconnected from the network. The exception to this is when the client is in the process of a lease renewal. Lease times vary depending on the Scope properties. Default lease times for Windows 2008 R2 DHCP servers are 8 days, although can be changed.

Pano devices and virtual client instances will not have any video output until they have been discovered by Pano Controller. This is expected and functionally correct behavior.

Note: Pano Virtual Clients will use a different discovery process.

39 DVM Administration

This section provides information on a number of basic system administration functions. Additional administrative functions can be found in:

- Pano Controller Administration
- Setting Up DHCP
- Optimize DVM Performance
- Endpoint Administration
- Define USB Peripheral Support
- Configure & Manage Pano Zero Clients & Desktop Preferences
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen

Pano DVM Tasks

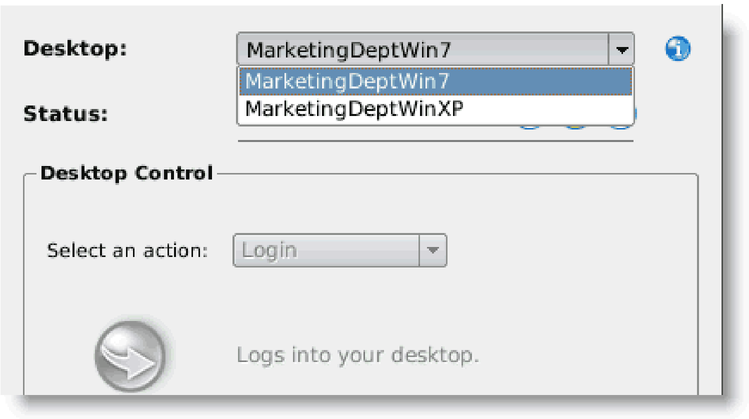
- Launch DVM Console
- Configure DVM Firewall
- Log On To DVMs as End User
- Log On To DVMs as Administrator
- Log Off from DVMs as Administrator
- Log Off from DVMs as End User
- Reset DVMs as End User
- Reset DVMs as Administrator
- Restart DVMs as Administrator
- Shut Down DVMs as Administrator
- Suspend DVMs as Administrator
- Power Off DVMs as End User
- Power On DVMs as Administrator
- Power Off DVMs as Administrator
- Retrieve DVM Information
- Monitor DVM Utilization and State
- Retrieve DVM Information
- Perform Maintenance on DVMs
- Monitor Pano Direct Service Status
- Determine Pano Direct Service Version
- Uninstall Pano Direct Service
- Monitor DVM Events with Pano Direct Service Scripts
- Configure Pano Direct Service for 24-bit Color
- Create Device-Based DVM Assignments
- Determine the User Assigned to a DVM
- View Users' DVM Login Status and DVM Assignment
- Determine Who's Logged on To DVMs
- About User Assignment
- About Device Assignment
- Unassign Users from DVMs
- Move DVMs to Trash
- Remove DVM from Trash
- Delete DVMs from Disk
- Replace or Re-image DVMs
- Expand DVM Hard Drives
- Rename DVMs
- Reuse DVM Names
- Refresh Pooled Desktops Collection Virtual Machines
- Migrate Outlook Nickname & Auto-completion Cache To DVM
- Migrate Browser Bookmarks & Cookies To DVM
- Monitor and Manage DVM Sessions

Log On To DVMs as End User

If you want to log on as an Administrator in order to troubleshoot a DVM, go to Log On To DVMs as End User. If you are experiencing session timeout issues, go to Control Session Timeouts. You can log on to a DVM from a Pano System Endpoint or from Pano Remote.

To log on to a DVM from a Pano System Endpoint:

1. Ensure that the Pano Button on your Pano System Endpoint is solid blue. The Pano user login screen appears on the screen.
2. Do one of the following:
   - If you want to connect to the desktop you used most recently, or you have only one desktop virtual machine:
     - From the Pano user login screen, type your user name and password
     - Click **Login.**
   - If you have more than one desktop virtual machine, and want to log on to a different desktop:
     - Select your desktop in the **Desktop:** drop-down list.
     - In the Select an action drop-down list, choose **Login**, then **Apply**.



Desktop: MarketingDeptWin7

MarketingDeptWin7
MarketingDeptWinXP

Status:

Desktop Control

Select an action: Login

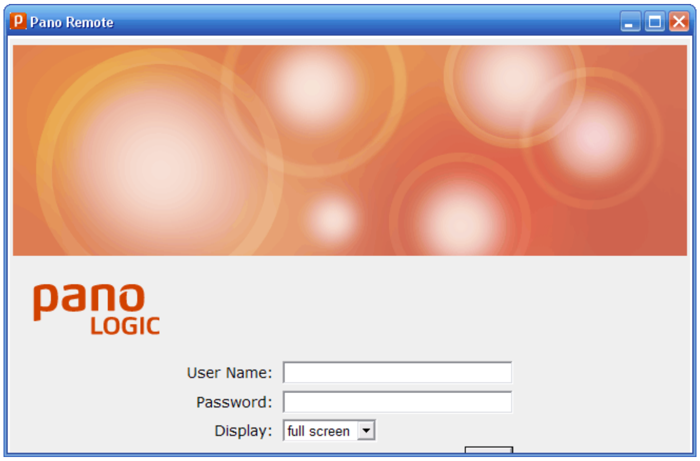
Logs into your desktop.

To log on to a DVM from Pano Remote:

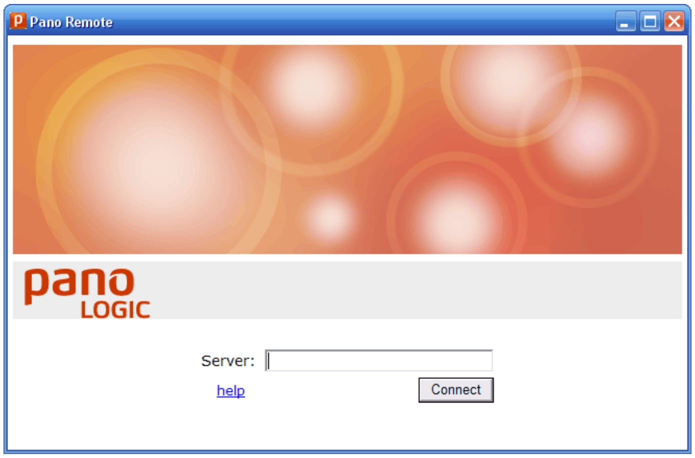
Note: If you are using a web proxy for public access, the web proxy must support RPC over HTTPS protocol or Pano Remote will fail. You must add support for RPC over HTTPS to the web proxy.

After you insert the Pano Remote USB into your computer's USB port and double-click on the `.exe` file, a Pano Remote login screen appears. It will prompt you to type in either a username and password or a server. Do one of the following:

- *If prompted for a username and password*, type in your username and password, then click **Login**. This username and password is the same username and password that you always use to access your virtual desktop.



- *If prompted for a server*, type in the name of the server that you Administrator provided you, then click **Connect**. The name looks something like ***myserver.mycompany*.com**. All users have the same server name.



3. When prompted, type in your username and password, then click **Login**. This username and password is the same username and password that you always use to access your virtual desktop.

To log on to a DVM through a VPN connection using a non-Pano System Endpoint:

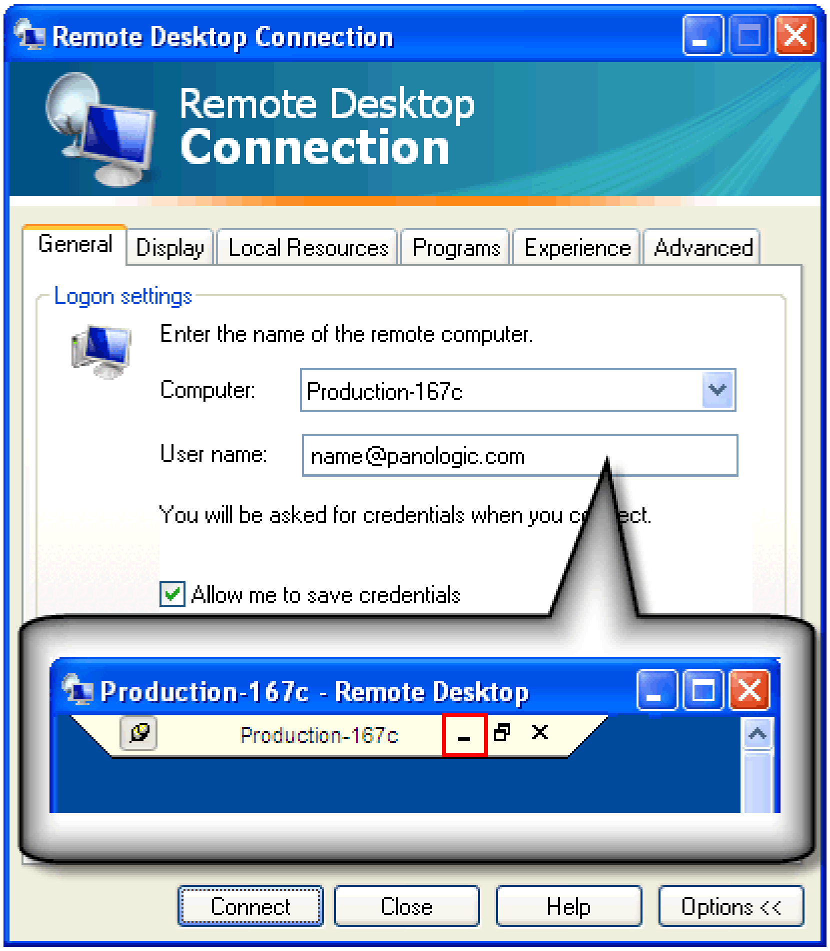
If you need to VPN into a DVM from a remote location, use the Pano web access. This client connects to the DVM using RDP.

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

To log on to two DVMs simultaneously:

If you need to toggle between two DVMs regularly you can log on to the first DVM as you would ordinarily then log on to the second using Pano Remote. However, if your company doesn't use Pano Remote, use the Remote Desktop Connection client.

1. Log on to the first DVM as you would ordinarily.
2. Launch the Windows Remote Desktop Connection client, then connect to the second DVM.
3. Use the minimize and maximize (+/-) icons to toggle between the two DVMs.



Enter the name of the remote computer.

Computer: Production-167c

User name: name@panologic.com

You will be asked for credentials when you connect.

☑ Allow me to save credentials

Related Topics

Log On To DVMs as Administrator

Log Off from DVMs as Administrator

Log Off from DVMs as End User

Log On To DVMs as Administrator

You can log on to a user's DVM using your virtual platform's administrative interface. However, if you need an alternate access, use RDP.

If you encounter RDP problems while logging on to the DVM, try the solutions suggested in Troubleshoot RDP Connection Problems.

You disconnect the user from the DVM when you log on to the DVM as Administrator. While you are logged on, the user receives the following message:

```
The user Domain\Administrator is currently logged on to this computer. Only the
current user or administrator can log on to this computer
```

When you're done, make sure you log off the DVM so the user can log on and resume work.

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!

Related Topics

Log On To DVMs as End User

Log Off from DVMs as Administrator

Log Off from DVMs as End User

Log Off from DVMs as Administrator

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. If the user forgets to log off, you can log off that user from the Pano Controller administrator interface. Alternatively, you can implement session timeouts by using an AD group policy.

A log off forces all open programs to close, so it's a best practice to notify your users in advance because any unsaved data will be lost.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM, then, from the **Desktop** drop-down button, choose **Force Logout**.
4. When prompted to confirm your selection, click **Force Logout**.

Related Topics

Log On To DVMs as End User

Log On To DVMs as Administrator

Log Off from DVMs as End User

Log Off from DVMs as End User

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 the Pano System Endpoint 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, you can implement session timeouts by using an AD group policy (go to Control Session Timeouts). Otherwise, users can simply log off as they would normally in Windows.

Related Topics

Log On To DVMs as End User

Log On To DVMs as Administrator

Log Off from DVMs as Administrator

Reset DVMs as End User

Administrators can reset DVMs from either the Pano Client Login Screen, the Pano Controller or vCenter Server. However, end users can only do so from the Pano user login screen. A shutdown (or power-off) gracefully closes all running programs and powers off the machine. A reset (also called *hard-reset*) simply powers off and on, the DVM. A reset might have some undesired effects on some running programs. Perform a reset only if the DVM is unresponsive.

1. From the Pano user login screen, type in username and password. The **Options...** button is no longer greyed out.
2. Click the **Options...** button.
3. In the pop-up window, click the **Reset Power** button.

Related Topics

Restart DVMs as Administrator

Power Off DVMs as End User

Reset DVMs as Administrator

Administrators can reset DVMs from either the Pano user login screen, the Pano Controller, vCenter Server or SCVMM. A reset might have some undesired effects on some running programs. Perform a reset only if the DVM is unresponsive. To identify the DVM's state, go to Monitor Pano Direct Service Status.

A restart (go to Restart DVMs as Administrator) gracefully closes all running programs. A reset (also called *hard-reset*) simply powers off and on, the DVM.

Note: For XenDesktop, the Reset option is not available.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.

3. Select the DVM that you want to reset, then, from the **Desktop** drop-down button, choose **Reset**.
4. When prompted to confirm your selection, click **Reset**.

Related Topics

Reset DVMs as End User

Power Off DVMs as End User

Restart DVMs as End User

If end users have unsaved user data the restart prompts them to save their changes and close any open applications.

1. From the Pano user login screen, type in username and password. The **Options...** button is no longer greyed out.
2. Click the **Options...** button.
3. In the pop-up window, click the **Restart Guest** button.

Related Topics

Restart DVMs as Administrator

Restart DVMs as Administrator

If end users have unsaved user data the restart prompts them to save their changes and close any open applications.

Note: For XenDesktop, the Restart Guest option is not available.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to reset, then, from the **Desktop** drop-down button, choose **Restart Guest**.
4. When prompted to confirm your selection, click **Restart Guest**.

Related Topics

Restart DVMs as End User

Shut Down DVMs as Administrator

Note: For XenDesktop, the Shut down Guest option is not available.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to reset, then, from the **Desktop** drop-down button, choose **Shut down Guest**.
4. When prompted to confirm your selection, click **Shut down Guest**.

Related Topics

Power On DVMs as End User

Suspend DVMs as Administrator

Note: For XenDesktop, the Suspend option is not available.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to reset, then, from the **Desktop** drop-down button, choose **Suspend**.
4. When prompted to confirm your selection, click **Suspend**.

Power On DVMs as End User

If the DVM is currently powered off, users can power on the DVM quite easily from the Pano user login screen. Unlike with the options outlined in Configure for User Control of Desktops, you do not need to provide users access to this option as they have access by default.

1. From the Pano user login screen, type in username and password. The **Options...** button is no longer greyed out.
2. Click the **Options...** button.
3. In the pop-up window, click the **Power On** button. This option does not appear if the DVM is already powered on.

Related Topics

Power Off DVMs as End User

Power Off DVMs as End User

If the DVM is currently powered off, users can power on the DVM quite easily from the Pano user login screen. Unlike with the options outlined in Configure for User Control of Desktops, you do not need to provide users access to this option as they have access by default.

1. From the Pano user login screen, type in username and password. The **Options...** button is no longer greyed out.
2. Click the **Options...** button.
3. In the pop-up window, click the **Power On** button.

   This option does not appear if the DVM is already powered on.

Related Topics

Power Off DVMs as Administrator

Power On DVMs as Administrator

Note: For XenDesktop, the Power On option is not available.

1. Log on to the Pano Controller.

2. Click the **DVMs** tab.
3. Select the DVM that you want to power on, then, from the **Desktop** drop-down button, choose **Power On**.
4. When prompted to confirm your selection, click **Power On**.

Power Off DVMs as Administrator

If you have more DVMs than you have users, consider powering off those unused DVMs. A DVM that is powered on, though not being used, can consume about 250 MB of memory.

Administrators can power off (shut down) DVMs from either the Pano user login screen (go to Power Off DVMs as End User), the Pano Controller or vCenter Server.

Note: For XenDesktop, the Power Off option is not available.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to power off, then, from the **Desktop** drop-down button, choose **Power Off**.
4. When prompted to confirm your selection, click **Power Off** in the dialog box.

Create Device-Based DVM Assignments

You are able create device-based DVM assignments to assign a Pano System Endpoint to a specific DVM.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the desired client.
4. Click **Clients** > **Assign**.

   The Select DVM dialog appears.
5. Filter DVMs by Broker selection and Show option.
6. Select the desired DVM and click **Ok**.

   The device-based DVM assignment is created.

Related Topics

Manually Add Pano Zero Clients

Determine the User Assigned to a DVM

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

View Users' DVM Login Status and DVM Assignment

To view users' information:

1. Log on to the Pano Controller.
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 type, this field will not be populated. Only the Logged in User field will be populated.

Related Topics

Manually Assign Users in User Based Collections

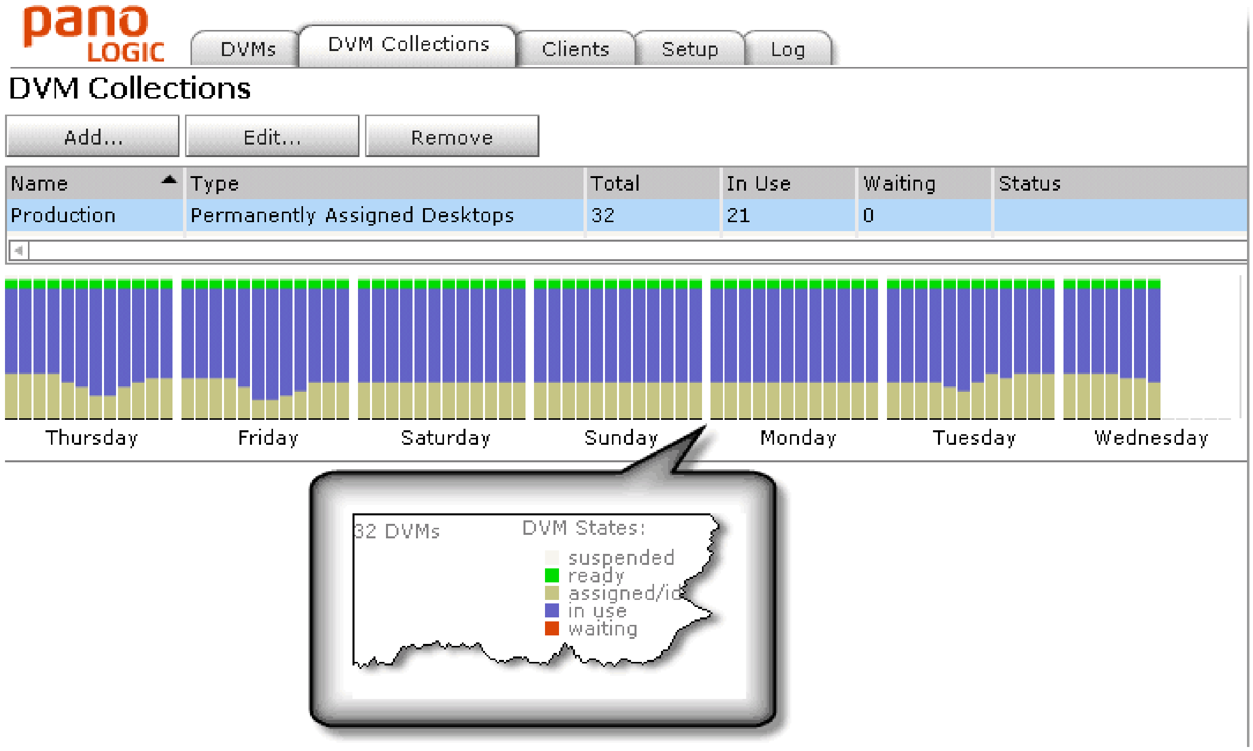
Monitor DVM Utilization and State

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

Note: For XenDesktop, DVM State is not applicable; no data appears in this column.

1. Log on to the Pano Controller.
2. Click on the **DVM Collections** tab.
3. Select a single collection from the table to highlight the row.
4. Scroll down to the bottom and observe the **DVM States** legend. A stacked-bar chart displays the utilization for that collection.
   - Each bar is a two-hour period. The height is the number of DVMs in the collection.
   - Each section of the bar represents the number of DVMs in a particular state:

Color Bar	DVM State	Description
White	suspended	DVM is suspended, not powered on, or Pano Direct Service is not reachable.
Green	ready	DVM is powered on and Pano Direct Service is reachable. The DVM is available to be assigned to a user.
Gray	assigned/idle	DVM is assigned to a user, but the user is not logged in.
Red	waiting	DVM is unavailable when a user attempts to log on.
Blue	in use	The user is logged on to the DVM.



DVM Collections

Name	Type	Total	In Use	Waiting	Status
Production	Permanently Assigned Desktops	32	21	0	

Retrieve DVM Information

From the **DVMs** tab, you can retrieve the following information for all DVMs in all collections.

Column Name	Description
Virtual Machine Name	The name of the DVM. You chose this name pattern when you configured for deployment. For XenDesktop, Virtual Machine field displays the string "xd:" with the IP address of the DVM appended (e.g. "xd: 192.168.1.123).
DVM State	The state of the DVM–either `Powered On` or `Powered Off`. The state is derived from information provided by the hypervisor. **Note:** For XenDesktop, the **DVM State** column is not **applicable**.
DVM Tools State	**Note:** For XenDesktop, the **DVM Tools State** column is not **applicable**. This column only applies to VMware (See Upgrade Virtualization Tools on DVMs) and Hyper-V.
DVM Availability	If the state is `Powered Off` something might be wrong with the DVM, so log on to the DVM from the console. With an initial deployment, the problem is usually the result of an incorrect Windows product key. **Note:** For XenDesktop, the **DVM Availability** column is not applicable.
IP Address	The IP address of the DVM. This IP address is different from the IP address of the Pano System Endpoint.
DNS Name	The Windows computer name. **Note:** For XenDesktop, the **DNS Name** column is not applicable.
Pano Direct Status	The status of the Pano Direct Service that is running on the DVM.
Pano Direct Version	The version of the Pano Direct Service that is running on the DVM.

Column Name	Description
Assigned User	The DVM to which this DVM is assigned.
Logged In User	The user that is currently logged on to this DVM. If you want to log off the user, go to Log Off from DVMs as Administrator.
Client	The device name of the Pano System Endpoint that is connected to the DVM. If you want to disconnect the Pano System Endpoint, go to Disconnect Pano Zero Clients from DVMs.

Monitor Pano Direct Service Status

If a DVM is not working as expected, knowing a Pano Direct Service's status can help you determine where the communication breakdown exists.

1. Log on to Pano Controller.
2. Click on the **DVMs** tab.
3. In the Pano Direct Status column, observe the current Pano Direct Service status.

Pano Direct Status	What's this mean?	What do I do?
Unreachable	DVM cannot be reached.	The DVM might have a firewall, which needs to be configured to allow communication over certain ports for both inbound and outbound traffic (go to Configure DVM Firewall or the DVM might have IPv4 disabled. Go to:Trial Requirements
Unresponsive	DVM is reachable, but Pano Direct Service is not responding.	Make sure you are running the latest Pano Direct Service version (go to Determine Pano Direct Service Version)
Connecting	Pano Controller is attempting to connect to the DVM.	This is normal.
Responding	DVM is responding to Pano Direct Service.	This is normal.
n/a	There is no status to report.	The DVM is probably not powered on: see the DVM Availability column, or you're observing the known issue: ID 4335.

Perform Maintenance on DVMs

Before you do any work on a DVM, place the DVM into maintenance state. You know a DVM is in maintenance state when the DVM Availability column indicates `Maintenance`.

The Pano Controller prevents users from establishing new connections to DVMs under maintenance. If a user tries to log on to a DVM that is in maintenance state, the user will receive an error message directing users to contact their system administrator.

Users already logged on to the DVM will be able to continue working; however, Pano Controller does not allow new connections.

To place a DVM into maintenance state:

1. Log on to the Pano Controller.
2. Click on the **DVMs** tab.
3. Select the DVM (if you need to work on multiple DVMs, highlight all of them), then, from the Desktop drop-down button, choose **Maintenance On**.
4. Confirm your selection, then click the Maintenance On button. The DVM is now in maintenance state, and the Pano Controller will not allow new connections to that DVM.
5. Wait for the user to log off, or ask the user to log off, then proceed with maintenance tasks.

To remove DVM from maintenance state:

1. Log on to the Pano Controller.
2. Click on the **DVMs** tab.
3. Select the DVM, then, from the Desktop drop-down button, choose **Maintenance Off**.
4. Confirm your selection, then click the Maintenance Off button. Users can now log on to this DVM.

Determine Pano Direct Service Version

It's not uncommon for a Pano Controller to communicate with DVMs that have different Pano Direct Service versions installed; however, Pano Logic recommends that all DVMs run the same version–and the latest version.

If you notice that the DVM is not working as expected, verify that it has the latest Pano Direct Service version as indicated at www.panologic.com.

Also, in order for Pano Dual Monitor to work, your virtual desktop must be running Pano Direct Service v2.8.0 or later.

Note: If the Pano Direct Version column is blank, refer to ID 4335 and Trial Requirements.

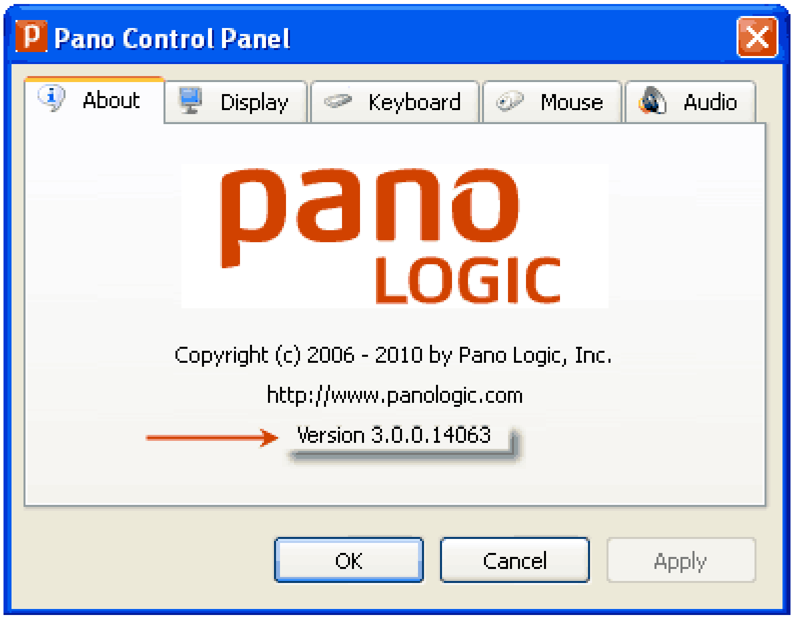
To determine a DVM's Pano Direct Service version from the Pano Controller:

1. Log on to Pano Controller.
2. Click on the **DVMs** tab.
3. If you have many DVMs to verify, apply a filter.
4. In the Pano Direct Version column, observe the Pano Direct Service version for the DVM(s).

   If the version is not the latest, update.

To determine your DVM's Pano Direct Service version from the Pano Control Panel:

1. Open the Pano Control Panel by either double-clicking the icon in the system tray or navigating to it by selecting **Start** > **All Programs** > **PanoDirect** > **Pano Control Panel**.
2. Note the version in the **About** tab.



Copyright (c) 2006 - 2010 by Pano Logic, Inc.

http://www.panologic.com

Version 3.0.0.14063

Determine Who's Logged on To DVMs

For security reasons, you can browse the list of DVMs to see who is logged on to your company's DVMs. You can troubleshoot logon as well. If a user cannot log on to a DVM, another user might be logged on it, indicating an potential collection assignment problem.

1. Log on to Pano Controller.
2. Click on the **DVMs** tab.
3. In the **Logged In User** column, observe the user that is logged on to that DVM.

About User Assignment

You can assign both users and Pano System Endpoints to DVMs. To learn about Pano System Endpoint assignment, go to About Device Assignment.

In the 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 System Endpoint 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.

To assign in advance, go to Unassign Users from DVMs.

To remove assignment, go to Unassign Users from DVMs.

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 it can be done manually through the **DVMs** tab on the Management User Interface (MUI).

Unassign Users from DVMs

If you want to give an assigned DVM to another user, you must first unassign the existing designated user.

4. Log on to the Pano Controller.

5. Click the **DVMs** tab.
6. Select the DVM from the list, then click **Unassign**. The DVM is now available to be assigned to another user.

Related Topics

Manually Assign Users in User Based Collections

Unassign Pano Zero Clients from DVMs

Move DVMs to Trash

An end user might want to trash a DVM if it becomes unusable (corrupted operating system, virus/malware, etc.). Only an end user can move a DVM to the Trash, assuming you enable this option for the Permanently Assigned Desktops collection type (refer to Configure for User Control of Desktops). This operation is only available to users if:

- DVMs is in a Permanently Assigned Desktops collection type.
- DVM is assigned to that user.

If a user trashes a DVM, the DVM's DVM Availability indicates `Trash`, and the DVM is no longer made available to that user. The user receives a new DVM (cloned from the collection's template) upon the user's next login. If you have folder redirection configured, the user can access the user data from the new DVM; otherwise, the user data can only be accessed by removing the DVM from trash.

An administrator can delete the trashed DVM or return it to circulation. Pano Logic recommends that you periodically purge trashed DVMs to recuperate the system resources. To do so, you must delete the DVM from disk.

To move a DVM to Trash (as an end user):

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

1. Log on to the desktop virtual machine that you want to trash.

   Note: The button changes from Help to Options after you type a valid username and password.
2. From the Pano user login screen, click on **Options...**.
3. In the Select an action drop-down list, choose **Trash Desktop**, then click **Apply**.
4. To confirm your selection, click **Trash your desktop**.

Remove DVM from Trash

Only an administrator can remove a DVM from Trash. If you determine that the DVM is okay and you want to recycle the DVM, you'll need to remove the user data. To persuade users to think twice before trashing a DVM, the Pano Controller informs users that a trashed DVM results in data loss. The truth is, the user data remains on the DVM.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM, then, from the Desktop drop-down button, choose **Maintenance Off**.

4. To confirm your selection, then click the Maintenance Off button. You can now recycle this DVM.

Delete DVMs from Disk

Pano Logic recommends that you periodically purge trashed DVMs to recuperate system resources. Keep in mind though, you cannot recover DVMs that you delete from disk.

1. Log on to the Pano Controller.

2. Click the **DVMs** tab.

3. Select the DVM that you want to power on, then, from the **Desktop** drop-down button, choose **Delete from Disk**.

4. When prompted to confirm your selection, click **Delete**.

Replace or Re-image DVMs

You might need to replace a user's DVM if it is simply unusable. To do so, simply re-image it.

1. Unassign the user from the DVM.

2. Place the DVM into Maintenance state.

3. Power off the DVM.

4. Assign a new, unassigned DVM to the user.

5. Create a spare DVM if one does not exist in the collection.

For example, if you set the **Extra DVMs** value to `1` and select the **Deploy Enabled** check box, Pano Controller 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.

Tip: If you're a savvy command-line user, you can use the GNOME Partition Editor instead of the following procedure.

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.

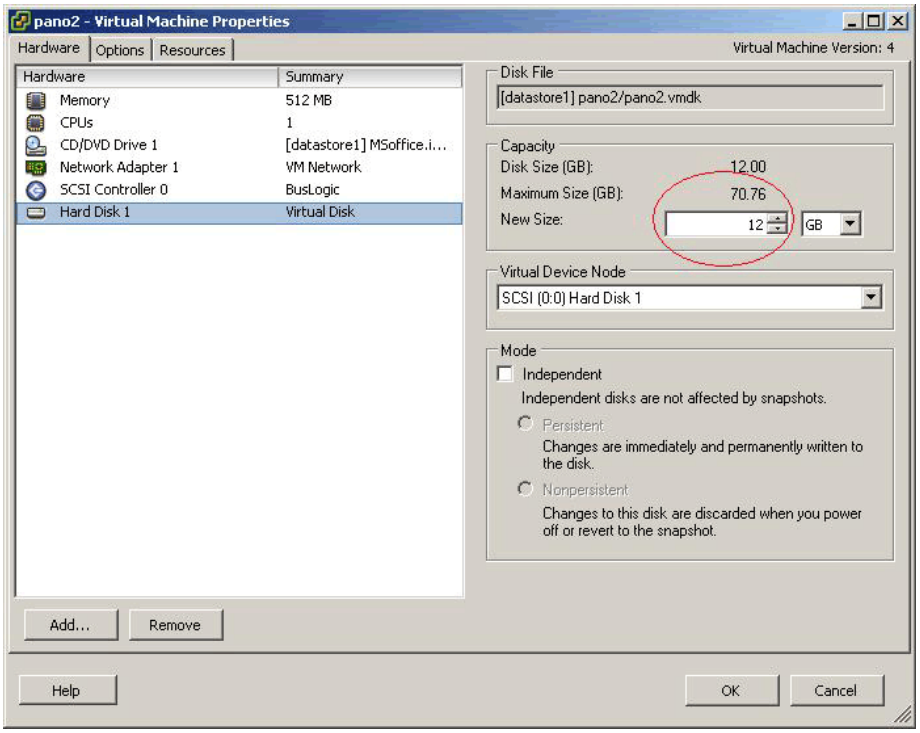
> **Warning:** Make sure that you do not have an active snapshot on the DVM. If you expand a virtual disk with a snapshot you *will* cause data corruption.

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.



Virtual Machine Version: 4

Hardware	Summary
Memory	512 MB
CPUs	1
CD/DVD Drive 1	[datastore1] MSoffice.i...
Network Adapter 1	VM Network
SCSI Controller 0	BusLogic
Hard Disk 1	Virtual Disk

Disk File

[datastore1] pano2/pano2.vmdk

Capacity

Disk Size (GB): 12.00

Maximum Size (GB): 70.76

New Size: 12 GB

Virtual Device Node

SCSI (0:0) Hard Disk 1

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

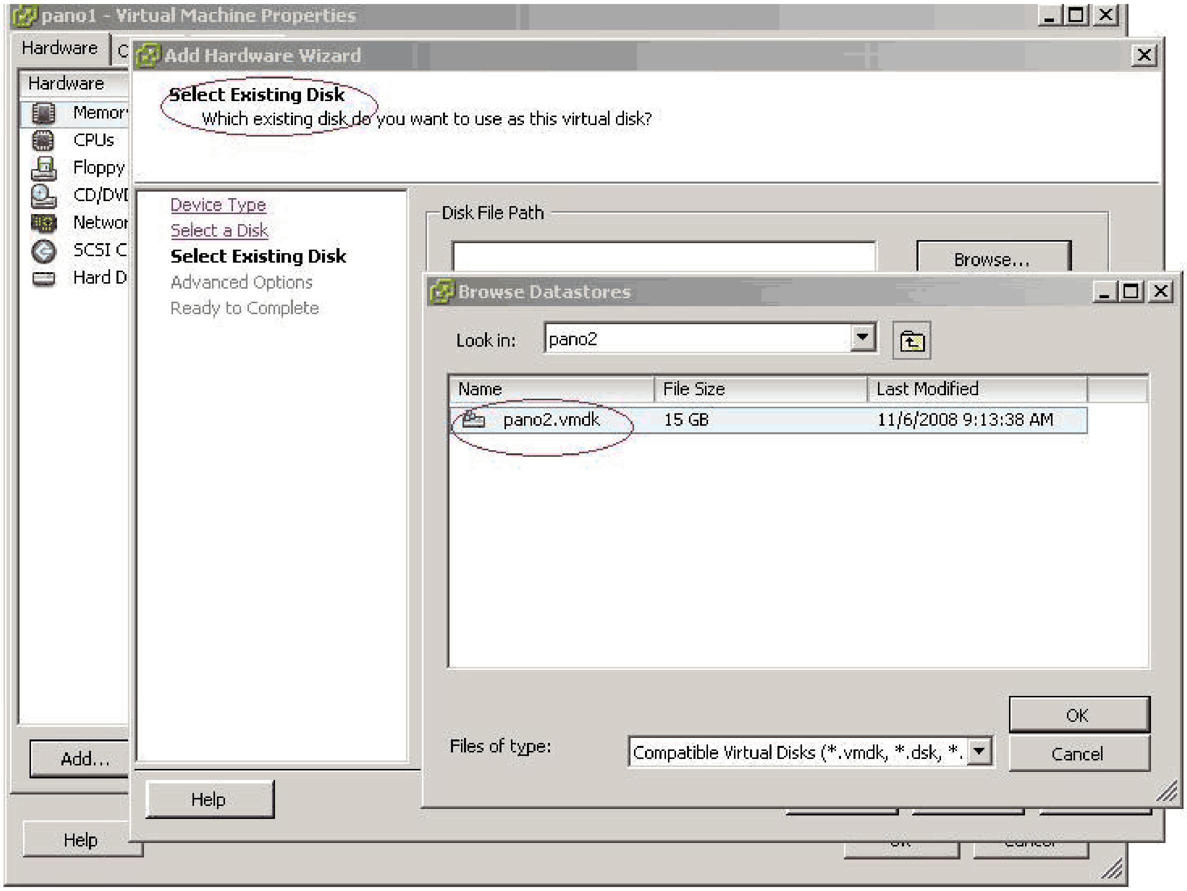
Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

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**.



pano1 - Virtual Machine Properties

Add Hardware Wizard

Select Existing Disk

Which existing disk do you want to use as this virtual disk?

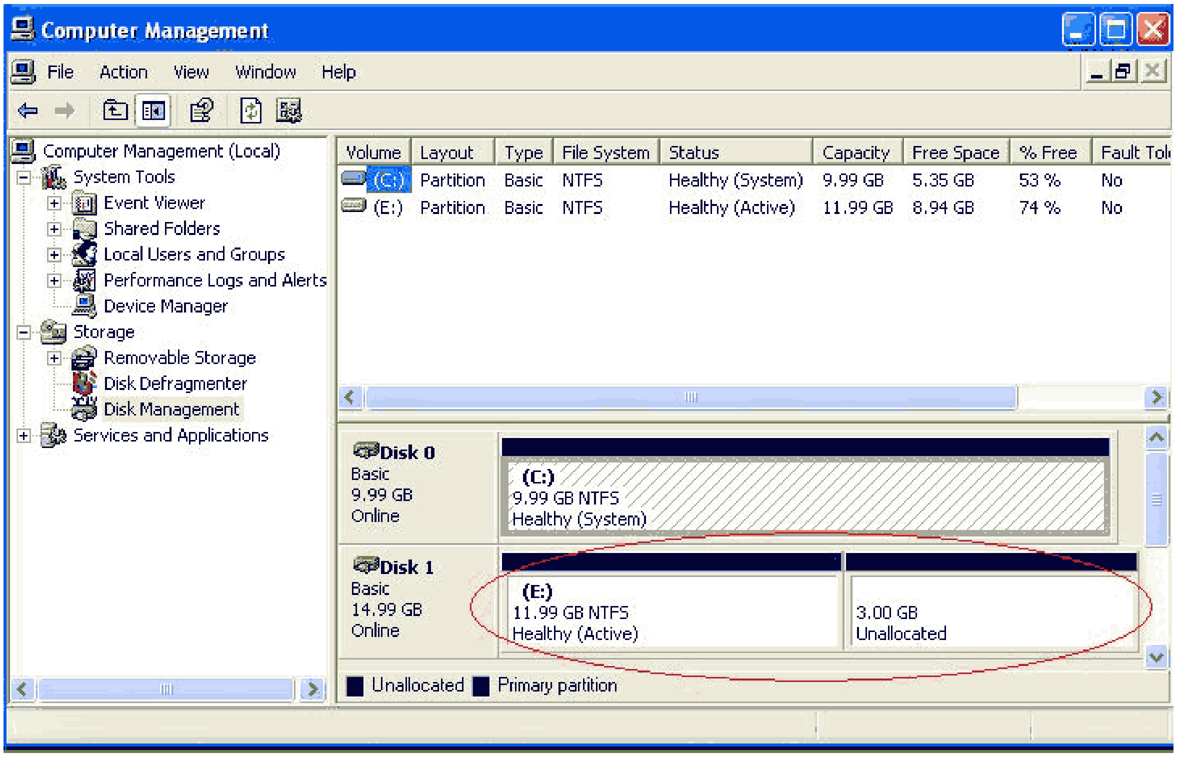
Browse Datastores

Look in: pano2

Name	File Size	Last Modified
pano2.vmdk	15 GB	11/6/2008 9:13:38 AM

Files of type: Compatible Virtual Disks (*.vmdk, *.dsk, *.

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



Computer Management

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tol
(C:)	Partition	Basic	NTFS	Healthy (System)	9.99 GB	5.35 GB	53 %	No
(E:)	Partition	Basic	NTFS	Healthy (Active)	11.99 GB	8.94 GB	74 %	No

Disk 0
Basic
9.99 GB
Online

(C:)
9.99 GB NTFS
Healthy (System)

Disk 1
Basic
14.99 GB
Online

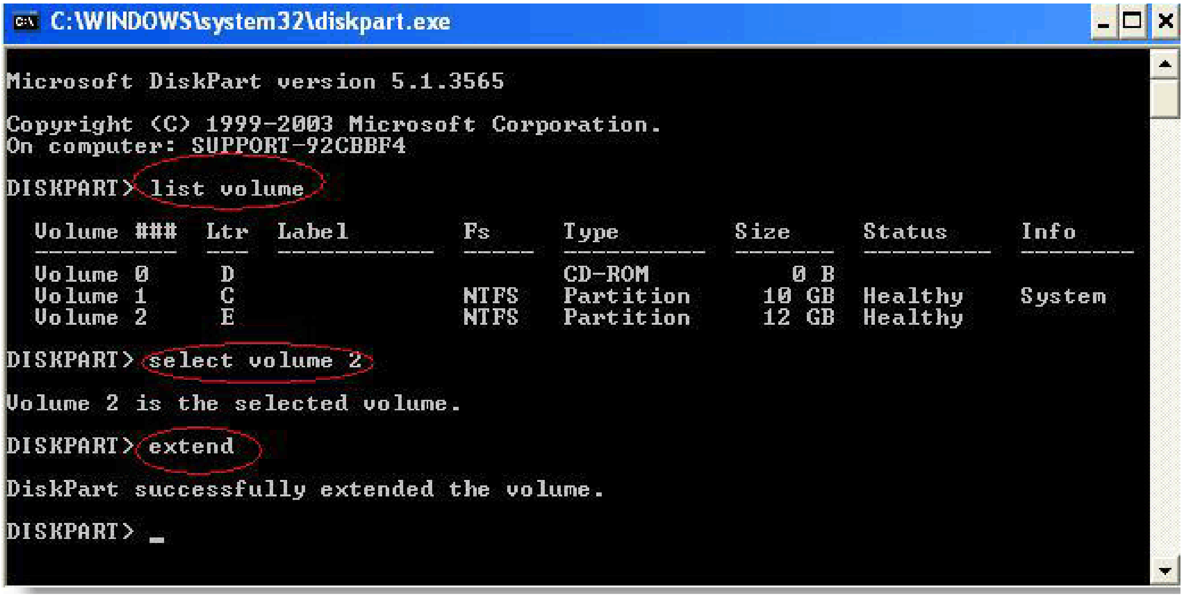
(E:)
11.99 GB NTFS
Healthy (Active)

3.00 GB
Unallocated

■ Unallocated ■ Primary partition

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

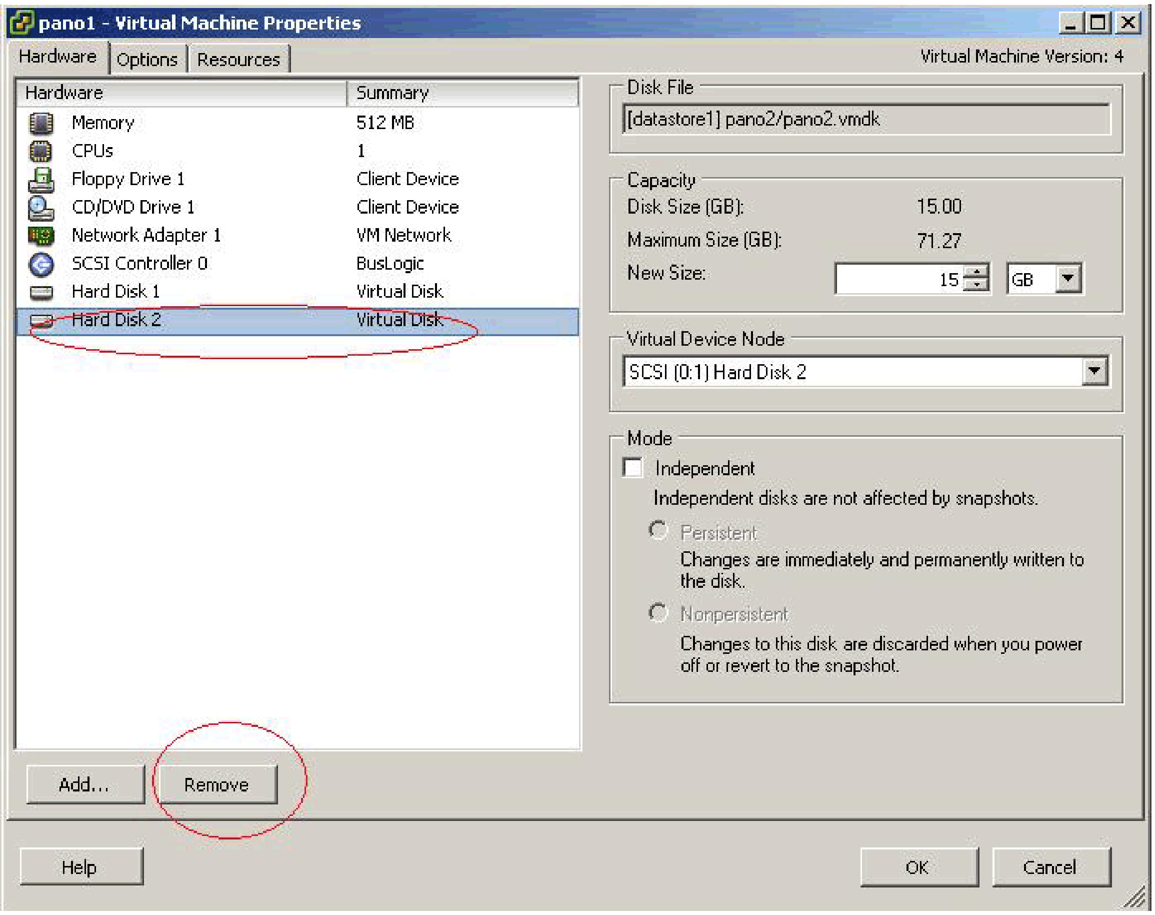
9. From the list of available volumes, select your volume, then run the expand command to expand the volume. Let’s assume that you’re expanding Drive E, which is volume 2.



C:\WINDOWS\system32\diskpart.exe

```
Microsoft DiskPart version 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
On computer: SUPPORT-92CBBF4

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D                       CD-ROM         0 B
  Volume 1     C                NTFS   Partition     10 GB  Healthy    System
  Volume 2     E                NTFS   Partition     12 GB  Healthy

DISKPART> select volume 2

Volume 2 is the selected volume.

DISKPART> extend

DiskPart successfully extended the volume.

DISKPART> _
```

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



pano1 - Virtual Machine Properties

Virtual Machine Version: 4

Hardware	Summary
Memory	512 MB
CPUs	1
Floppy Drive 1	Client Device
CD/DVD Drive 1	Client Device
Network Adapter 1	VM Network
SCSI Controller 0	BusLogic
Hard Disk 1	Virtual Disk
Hard Disk 2	Virtual Disk

Disk File

[datastore1] pano2/pano2.vmdk

Capacity

Disk Size (GB): 15.00

Maximum Size (GB): 71.27

New Size: 15 GB

Virtual Device Node

SCSI (0:1) Hard Disk 2

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

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.

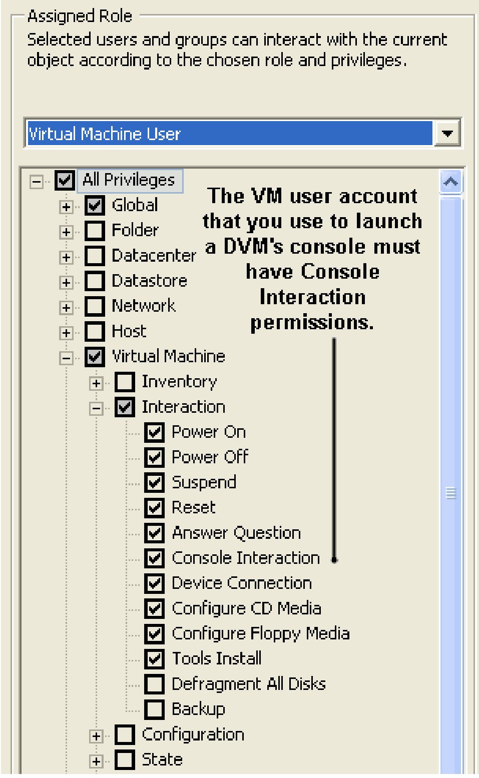
1. Make a backup copy of the DVM; after all, this disk contains your user data and things don't always go as planned.
2. Power off the DVM.
3. Increase the size of DVM's virtual disk file. Let's assume 12 GB to 15GB.
4. From the DVM's run menu, type **diskpart.exe**, then press Enter. The command line 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.

Rename DVMs

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to rename, then, from the **Desktop** drop-down button, choose **Rename**.
4. When prompted to confirm your selection, click **Rename** in the dialog box.

Launch DVM Console

In order to launch a DVM's console, you must have vSphere Client 4.0 or later. Also, the virtual machine user account that you use must have Console Interaction permissions:



Assigned Role

Selected users and groups can interact with the current object according to the chosen role and privileges.

Virtual Machine User

- ☑ All Privileges
  - ☑ Global
  - ☐ Folder
  - ☐ Datacenter
  - ☐ Datastore
  - ☐ Network
  - ☐ Host
  - ☑ Virtual Machine
    - ☐ Inventory
    - ☑ Interaction
      - ☑ Power On
      - ☑ Power Off
      - ☑ Suspend
      - ☑ Reset
      - ☑ Answer Question
      - ☑ Console Interaction
      - ☑ Device Connection
      - ☑ Configure CD Media
      - ☑ Configure Floppy Media
      - ☑ Tools Install
      - ☐ Defragment All Disks
      - ☐ Backup
    - ☐ Configuration
    - ☐ State

The VM user account that you use to launch a DVM's console must have Console Interaction permissions.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to launch, then from the **Desktop** drop-down button, choose **Launch Console**.
4. From the vSphere Client, type your login credentials, then click **Log In**.

Configure DVM Firewall

Pano Direct Service communicates with the Pano Controller and Pano System Endpoints 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 Controller.

The good news is that the Pano Direct Service installer automatically does all this work for you during a Pano Direct Service installation or upgrade. However, if you change your DVMs' firewall, you can configure the DVM's Windows Firewall using one of the following methods. (Alternatively, you can simply upgrade Pano Direct Service):

- 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 that you can narrow the scope of this Firewall policy to just the collections of DVMs that the Pano Controller manages.

(Recommended) 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.

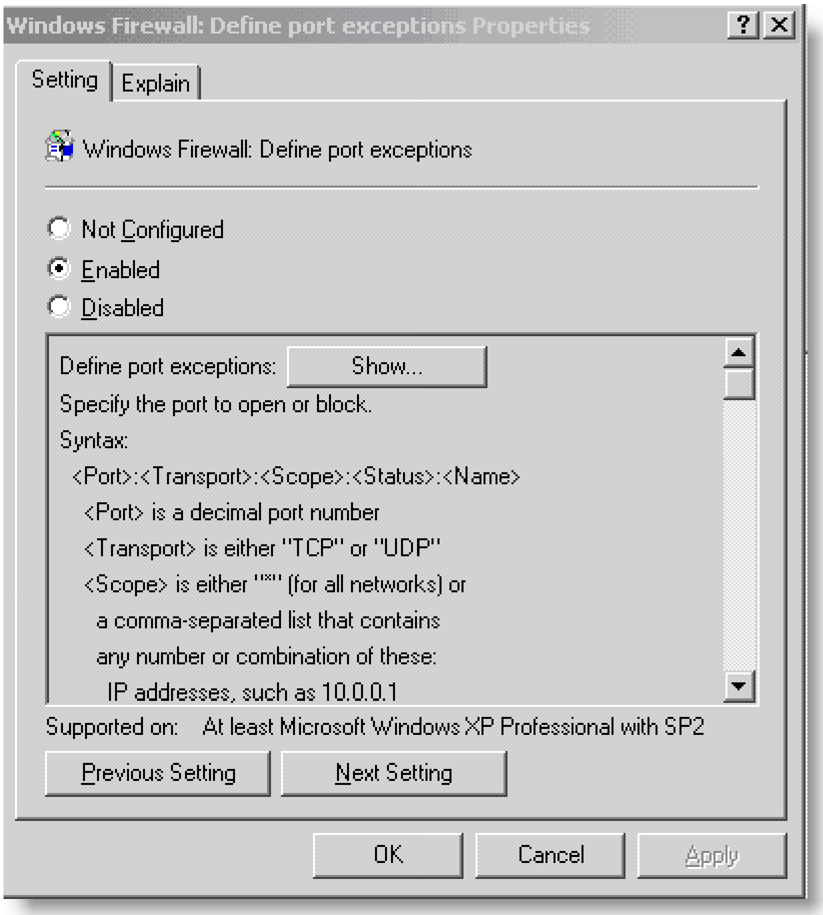
   b. Select the default domain policy.
3. Navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile**.
   - The Domain Profile is where you set the properties that take effect when the machine is running attached 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 Controller Connection
8321:UDP:*:Enabled:Pano System Endpoint Connection
```



Windows Firewall: Define port exceptions

○ Not Configured
● Enabled
○ Disabled

Define port exceptions:

Specify the port to open or block.

Syntax:

```
 <Port>:<Transport>:<Scope>:<Status>:<Name>
   <Port> is a decimal port number
   <Transport> is either "TCP" or "UDP"
   <Scope> is either "*" (for all networks) or
     a comma-separated list that contains
     any number or combination of these:
       IP addresses, such as 10.0.0.1
```

Supported on: At least Microsoft Windows XP Professional with SP2

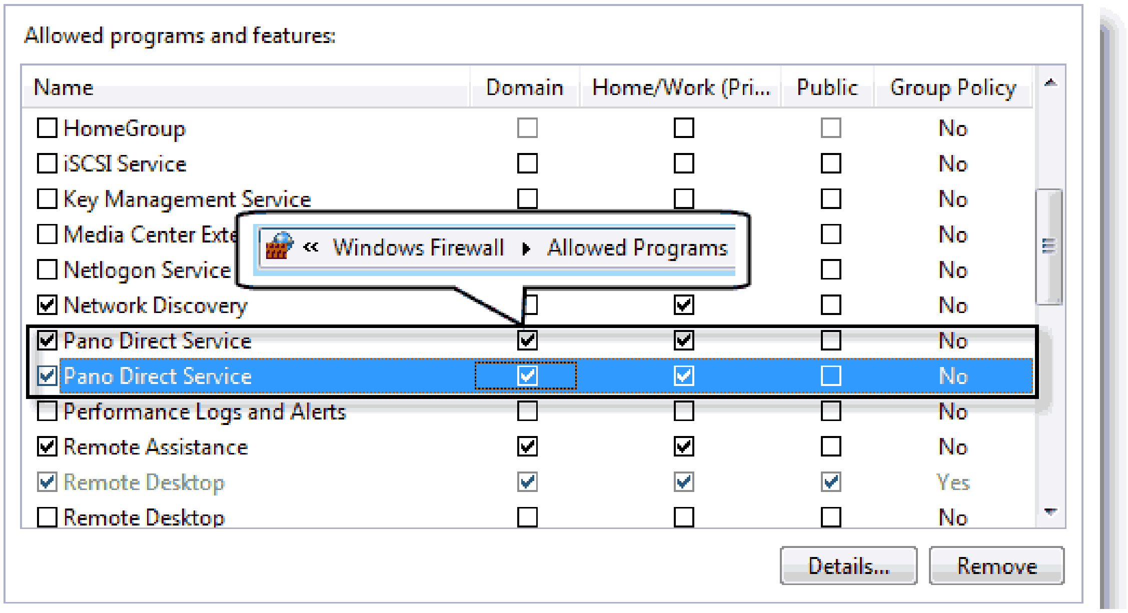
d. Click **OK,** then **OK** again. You're done!

To open the ports from the DVM:

This procedure assumes that you've already installed Pano Direct Service and your DVM is unreachable. Although this procedure uses Windows 7 as an example, the same principle applies on Windows XP.

1. Go to **Control Panel** > **System and Security** > **Windows Firewall** > **Allow a program or feature through Windows Firewall**.
2. Click **Change Settings**.

3. Select Domain checkboxes for the Pano Direct Service:



Allowed programs and features:

Name	Domain	Home/Work (Pri...	Public	Group Policy
□ HomeGroup	□	□	□	No
□ iSCSI Service	□	□	□	No
□ Key Management Service	□	□	□	No
□ Media Center Exte			□	No
□ Netlogon Service			□	No
☑ Network Discovery	□	☑	□	No
☑ Pano Direct Service	☑	☑	□	No
☑ Pano Direct Service	☑	☑	□	No
□ Performance Logs and Alerts	□	□	□	No
☑ Remote Assistance	☑	☑	□	No
☑ Remote Desktop	☑	☑	☑	Yes
□ Remote Desktop	□	□	□	No

Uninstall Pano Direct Service

Note: Do not mix manual installs and uninstalls with GPO deployments. Manually uninstalling Pano Direct in a GPO deployment environment can create a “ghost” Pano Direct folder in Add/Remove Programs. You cannot uninstall this ghost; if you try to, you'll receive a `fatal error during installation` error message. The problem resides in Microsoft’s dll runtime package on which Pano Direct Service depends. If you’re using GPO deployments, do not perform the following procedure.

When you uninstall Pano Direct Service on Windows XP DVMs, Pano Direct Service fails to uninstall if it determines that the GINA chaining is broken. If the installer returns the following error, re-establish the GINA chain before you proceed:

```
Unable to upgrade/uninstall Pano GINA provider. GINA chaining is
broken. Please fix the GINA chain and try again.
```

1. From the Windows Control Panel, double-click on **Add or Remove Programs**.
2. Go to **PanoDirect** and click **Remove**.

   The DVM loses its connection because Pano Direct Service is no longer installed.

Reuse DVM Names

As part of automated provisioning, the Pano Controller assigns a unique name to the new DVM based on the computer name pattern that you defined in the Computer Name option. The Pano Controller assigns the computer names incrementally.

If, for example, you have a computer name pattern of `DVM-{01}`, and you deployed 7 DVMs and 2 are no longer present due to a provisioning failure or deletion, you will have a gap in your sequence: `DVM-01`, `DVM-02`, `DVM-03`, `DVM-05`, `DVM-07`. The good news is that the Pano Controller enables you to reuse unused computer names. In this case, the Pano Controller names newly provisioned DVMs `DVM-04` and `DVM-06` before picking up the sequence again with `DVM-08`.

Note: When you want to rename a virtual machine, rename the DNS name so that it matches the new computer name. Because you configured the Customization Specification to **Use the virtual machine name** as required by Pano System, the Windows computer name is also the DNS name. When you rename a virtual machine in either the Pano Controller or vCenter Server, the computer name changes, but the DNS name stays the same. Two DVMs with the same DNS name will cause problems.

To eliminate the gap in computer name sequence:

1. From the collection, click on the Deployment tab.
2. Select the Reuse Names check box.
3. After the Pano Controller deploys enough DVMs to close the gap, clear the Reuse Names check box.

   It might take days or months before the gap closes, depending on the size of your organization.

Monitor and Manage DVM Sessions

You can monitor and manage active DVMs for a single Sessions display page.

To monitor and manage active DVM sessions:

1. Log on to the Pano Controller.
2. Click on the **Sessions** tab.

   A list of the currently active sessions appears for Pano VDB and the configured third-party brokers.
3. Click a column heading to sort the session display.
4. To manage a session, select the session and choose **Commands > Force Logout** to log the user out of the current DVM sessions or choose **Commands > Disconnect Client** to terminate the client DVM connection.
5. To navigate to additional session data, select the session and choose **Commands > GoTo DVM** to log the user out of the current DVM sessions or choose **Commands > GoTo Client**.

Column Name	Description
Client	The name of the client accessing the active DVM session.
Desktop IP Address	IP address of the DVM used by the session.
Pano Direct Version	Version of Pano Direct used by the session.
Logged In User	Username of user logged in to session.
Broker	The connection broker used by the connection.

Configure & Manage Pano Zero Clients & Desktop Preferences

Refresh Pooled Desktops Collection Virtual Machines

From time to time, you might may want to refresh (update) software in the DVMs that belong to a collection. You can use Microsoft Systems Management Server (SMS), Active Directory, or any of several available third-party software deployment and management products to do so.

For the Pooled Desktops collection type, an easier alternative is also available. This method is very easy for Pooled Desktops, but is not a best practice for DVMs that are not part of a Pooled Desktops collection type, because refreshing this way deletes registry changes.

To refresh a Pooled Desktops collection type:

1. Create a new folder in vCenter Server called `Old DVMs` or similar. (You might already have such a folder if you followed the instructions in Create Virtualization Hierarchy–VMware.)
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. Create new DVMs to replace the old DVMS.

   The same name can be used for the new DVMs as Pano Controller tracks DVMs by an internal global unique identifier (GUID), not the DVM name.
5. 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.

Configure Pano Direct Service for 24-bit Color

When connecting to a DVM via Remote Desktop Connection or the Pano web access, you must configure the DVM if your users desire 24-bit color depth. You do not need to configure for 24-bit color depth for Pano System Endpoint connections, only for Remote Desktop Connections and Pano web access as outlined in Configure DVMs for 24-bit Color.

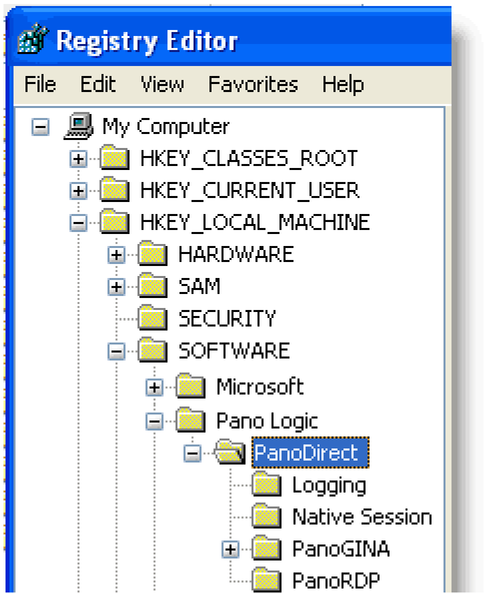
> **Warning:** If you use Registry Editor incorrectly, you can cause serious problems that can require you to reinstall your operating system. Neither Pano Logic nor Microsoft can guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own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

To configure for 24-bit color depth:

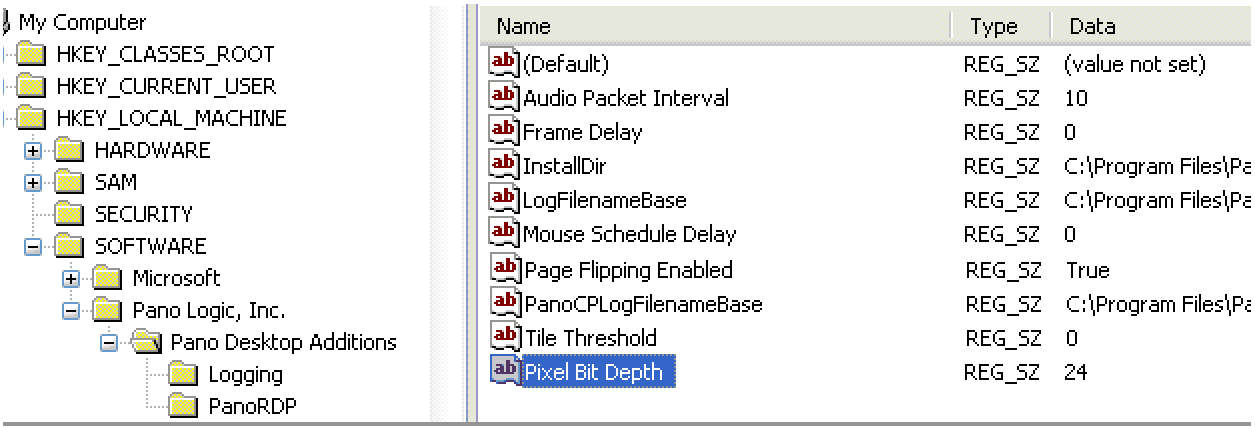
After you perform this procedure and the next time you log on to the DVM via Remote Desktop Connection or the Pano web access, you get 24-bit color depth. If you choose to use 16-bit color depth in the future, you can simply change the value of the registry to `16`.

Before You Begin: if you haven't already.

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\PanoDirect`.



3. Add a string entry Pixel Bit Depth, and set its value to 24.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Audio Packet Interval	REG_SZ	10
Frame Delay	REG_SZ	0
InstallDir	REG_SZ	C:\Program Files\Pa
LogFilenameBase	REG_SZ	C:\Program Files\Pa
Mouse Schedule Delay	REG_SZ	0
Page Flipping Enabled	REG_SZ	True
PanoCPLogFilenameBase	REG_SZ	C:\Program Files\Pa
Tile Threshold	REG_SZ	0
Pixel Bit Depth	REG_SZ	24

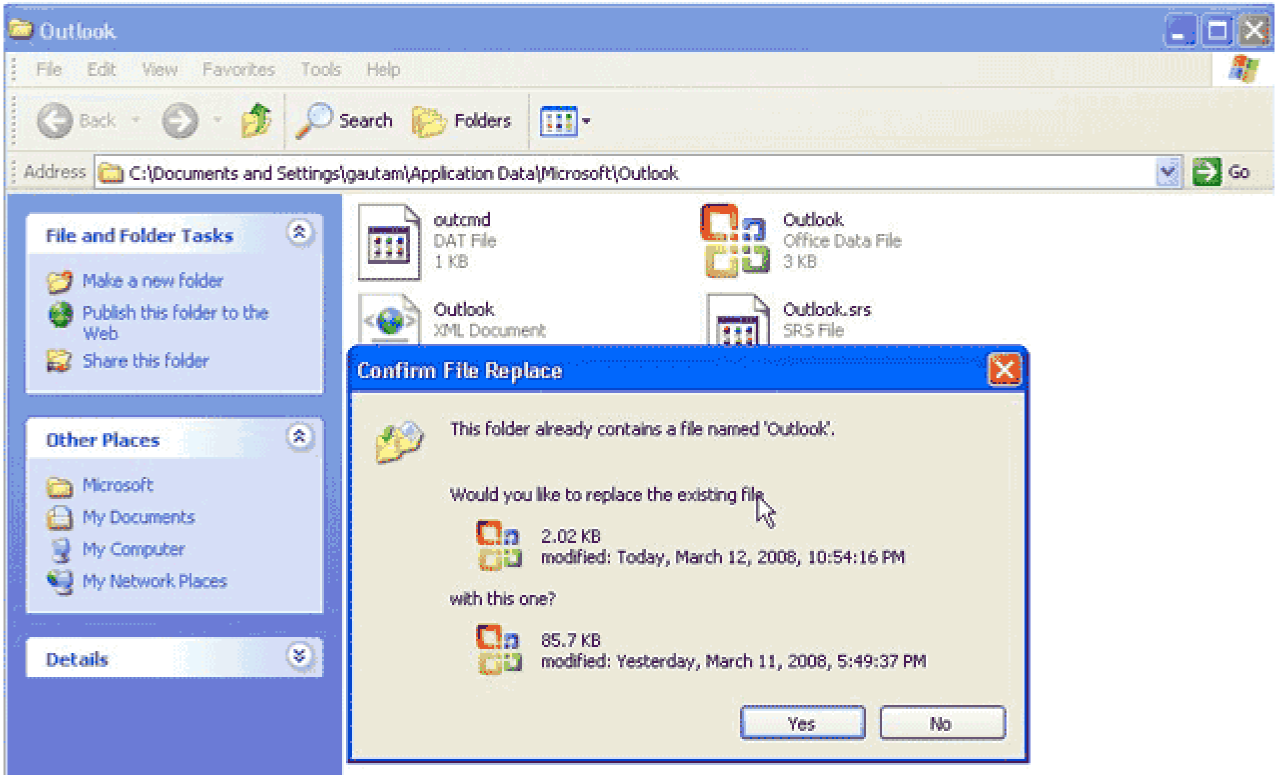
4. Restart the Pano Direct Service or reboot the desktop virtual machine.

Migrate Outlook Nickname & Auto-completion Cache To DVM

Microsoft Outlook attempts to auto-complete email addresses that users are typing in. This feature is very helpful, and many of your users might want to preserve this information stored in the auto-completion cache. It's quite easy to migrate this information to a new DVM.

To migrate nickname and auto-completion cache:

1. Exporting Outlook Nickname and Auto-completion Cache from the current desktop.
2. On the physical desktop, close Microsoft Outlook.
3. Make sure that folder options are set to show hidden files.
4. Go to the `C:\Documents and Settings\username\Application Data\Microsoft\Outlook` folder, the default location for the nickname and auto-completion cache.
5. Copy the file in that folder to a network drive. The file type is an Office Data File.
6. Go to the new DVM, open the `C:\Documents and Settings\username\Application Data\Microsoft\Outlook` folder, then do one of the following.
   - If there is no existing `Outlook` file, Microsoft Outlook has not been used on the new DVM. That's okay. Copy the `Outlook` file from the network share to this location.
   - If the `Outlook` file already exists in the new desktop virtual machine, the user has already sent some emails from the new DVM. That data will be lost. Copy the `Outlook` file from the network share to this location, overwriting the file.



This folder already contains a file named 'Outlook'.

Would you like to replace the existing file

2.02 KB
modified: Today, March 12, 2008, 10:54:16 PM

with this one?

85.7 KB
modified: Yesterday, March 11, 2008, 5:49:37 PM

Migrate Browser Bookmarks & Cookies To DVM

To help your users migrate from a physical desktop to their desktop virtual machines, consider exporting their browser bookmarks and cookies. Such tools help users adapt to their new DVM.

There’s no need to show you how to do this import/export as you can do so “in your sleep”; but, if you want to empower your users to import/export their own bookmarks and cookies, send them the following instructions, and provide them a network share on which they can temporarily store their bookmark/cookie file.

To migrate favorites and cookies in IE:

From the physical desktop, export the bookmarks and cookies to the network share, then log on to the desktop virtual machine, and import the bookmarks and cookies. To learn how to import and export, go to http://support.microsoft.com/kb/211089.

Exporting cookies from one desktop machine and importing them into another desktop machine is identical to exporting and importing Favorites. The only difference is that the option that you must select in the Export and Import Wizard is Export Cookies and Import Cookies respectively.

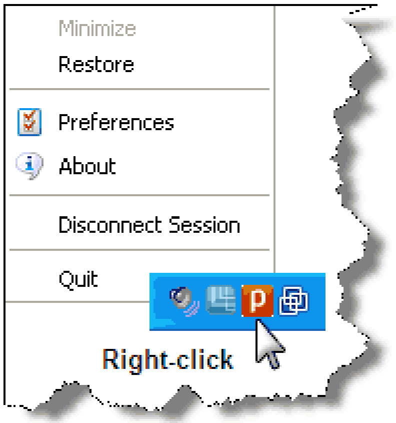
To migrate bookmarks and cookies in Firefox:

From the physical desktop, export the bookmarks to the network share, then log on to the desktop virtual machine, and import the bookmarks. To learn how to import and export, go to http://mozilla.gunnars.net/firefox_bookmarks_tutorial.html#importing_and_exporting_bookmarks.

Tip: A much easier way is to install foxmarks add-on for Firefox on both the physical desktop and the desktop virtual machine. You can then access the same bookmarks and cookies no matter what desktop you use.

Monitor DVM Events with Pano Direct Service Scripts

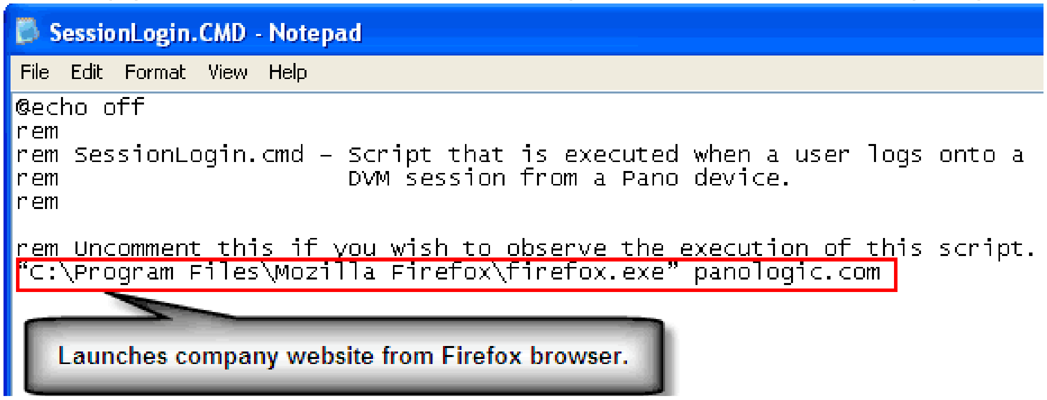
Using Pano Direct Service scripts that the Pano Installer installs by default in `C:\Program Files\Pano Logic\PanoDirect\Scripts`, you can monitor specific events. There are four events that you can monitor, and Pano Logic provides a starting script for each:

Script	Event
`SessionLogin.CMD`	Runs whenever a user logs on to a Windows virtual machine using any supported client (Pano System Endpoint, RDP, or VMware Console).
`SessionLogout.CMD`	Runs whenever a user logs off from a Windows virtual machine using any supported client (Pano System Endpoint, RDP, or VMware Console).
`SessionConnected.CMD`	Pano System Endpoint establishes a connection with Pano Direct Service
`SessionDisconnected.CMD`	Pano System Endpoint loses its connection to Pano Direct Service. User disconnects via one of the following ways: Pano Button DVM: Pano Control Panel:  Minimize Restore Preferences About Disconnect Session Quit Right-click DVM: Start > All Programs > PanoDirect > Disconnect Session:

You can automate tasks based on these events. Let’s explore a couple examples.

Example #1

Perhaps you have a kiosk and want your company’s website to launch as soon as a user logs on. Simply edit the `SessionLogin.CMD` script to launch Firefox and specify the URL.



SessionLogin.CMD - Notepad

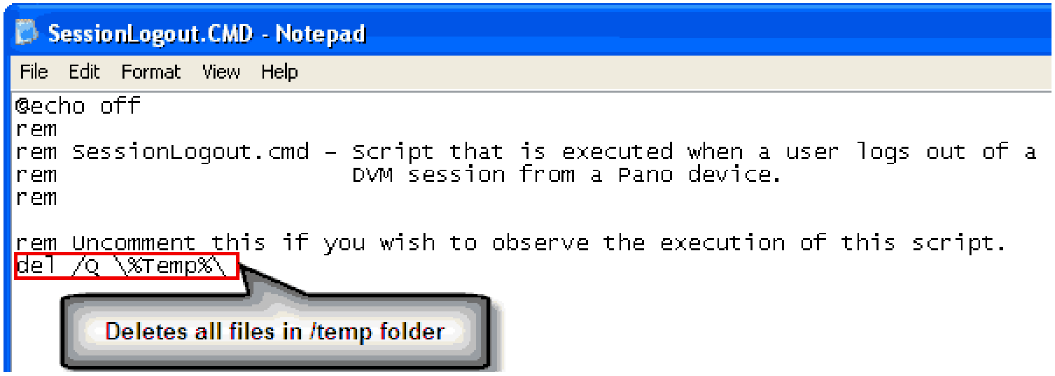
```
@echo off
rem
rem SessionLogin.cmd - Script that is executed when a user logs onto a
rem                    DVM session from a Pano device.
rem

rem Uncomment this if you wish to observe the execution of this script.
“C:\Program Files\Mozilla Firefox\firefox.exe” panologic.com
```

Launches company website from Firefox browser.

In addition, you can add a line that would automatically map a network share so that it is available to a user when that user logs on.

Example #2

After a user logs off the DVM your `SessionLogout.CMD` script executes, then deletes all the files in the `/tmp` folder thereby freeing up disk space and keeping the virtual desktop tidy:



```
@echo off
rem
rem SessionLogout.cmd - Script that is executed when a user logs out of a
rem                     DVM session from a Pano device.
rem

rem Uncomment this if you wish to observe the execution of this script.
del /Q \%Temp%\
```

Deletes all files in /temp folder

The following environment variables are *only* available to the `SessionConnected.cmd` and `SessionDisconnected.cmd` scripts. The environment variables are set in the context of the process running the script. After the script is executed, these environment variables are not available anymore. Therefore, if you want to store these variables, modify the script so that it copies the values either to a file or registry so that they are accessible after the script is executed.

Note: In the case of Pano System Endpoints in a multi-monitor configuration, the environment variables are set with information for the primary Pano System Endpoint. At present there is no way to get the information for the secondary Pano System Endpoint in this configuration.

Environment Variable	Description
`PANO_DEVICE_NAME`	The name used to identify this Pano System Endpoint on the Pano Controller. If no name has been defined on the Pano Controller then this will be a prefix plus the mac address of the device.
`PANO_DEVICE_REVISION`	The hardware (board and chip) version information for the Pano System Endpoint.
`PANO_MAC_ADDRESS`	The MAC address of the Pano System Endpoint.
`PANO_IP_ADDRESS`	The IP address of the Pano System Endpoint.
`PANO_SUBNET_MASK`	The subnet mask for the Pano System Endpoint.
`PANO_GATEWAY_ADDRESS`	The gateway IP address for the Pano System Endpoint.

In addition to environment variables, Pano Direct Service can also set registry variables that provide device information. These registry values are set when a Pano System Endpoint is connected to a virtual machine and remain as long as the Pano System Endpoint is connected to virtual machine and only cleared when the Pano System Endpoint is disconnected from virtual machine. Any application that has registry access can read these values and use them. The registry values are of `REG_SZ` type.

VMware View Client Registry Variables

If VMware View client is installed, the following registry variables are present at `HKEY_CURRENT_USER\Volatile Environment\`:

Registry Variables	Description
`ViewClient_IP_Address`	The IP address of Pano System Endpoint.
`ViewClient_MAC_Address`	The MAC address of Pano System Endpoint.

Registry Variables	Description
`ViewClient_Machine_Name`	The name used to identify this Pano System Endpoint on Pano Controller. If no name has been defined on the Pano Controller then the value will be a prefix plus the mac address of the device.
`ViewClient_Type`	The type of Pano System Endpoint.
`ViewClient_LoggedOnUsername`	The username of the user that is currently logged on to the virtual machine.

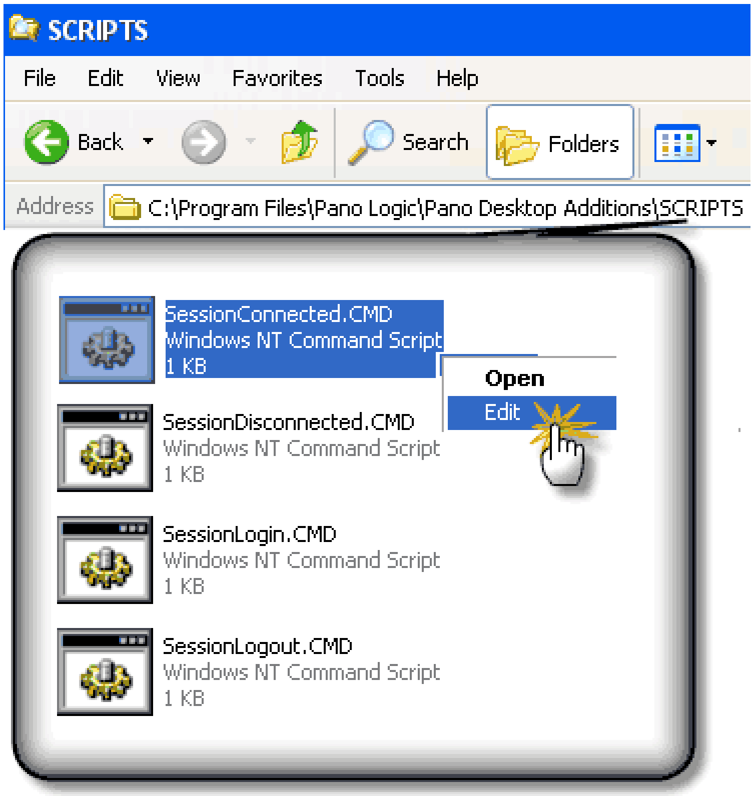
Pano System Endpoint Registry Variables

If VMware View client is not installed, the following registry variables are present at `HKEY_CURRENT_USER\Volatile Environment\`:

Registry Variables	Description
`PanoClient_IP_Address`	The IP address of Pano System Endpoint.
`PanoClient_MAC_Address`	The MAC address of Pano System Endpoint.
`PanoClient_Machine_Name`	The name used to identify this Pano System Endpoint on Pano Controller. If no name has been defined on the Pano Controller then the value will be a prefix plus the mac address of the device.
`PanoClient_Type`	The type of Pano System Endpoint.
`PanoClient_LoggedOnUsername`	The username of the user that is currently logged on to the virtual machine.

To modify existing Pano Direct Service scripts:

1. Locate the script that you want to use.

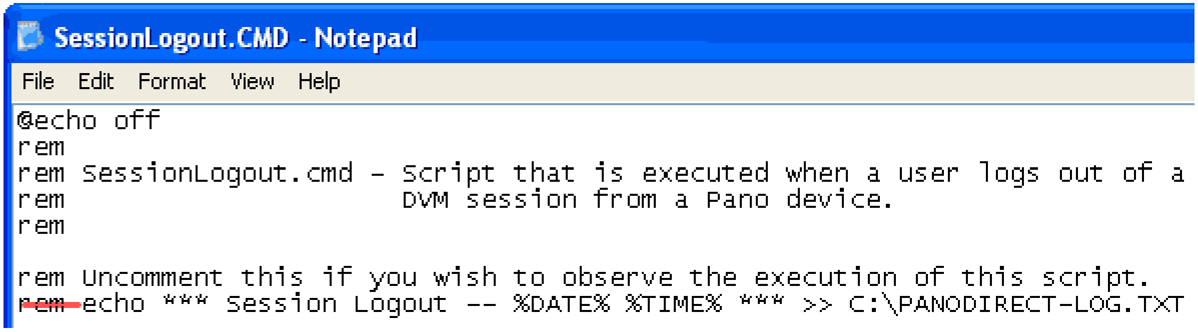


Address C:\Program Files\Pano Logic\Pano Desktop Additions\SCRIPTS

2. Before you edit the script, validate that the script works in its current form.

   Each script includes one or more simple actions. For example, `SessionLogout.CMD` writes a timestamp to the Pano Direct Service log file after a user logs off the DVM.

a. Simply uncomment the echo statements by deleting `rem` from each line of code, then save the file. Don’t change the name of the script’s filename.



```
@echo off
rem
rem SessionLogout.cmd - Script that is executed when a user logs out of a
rem                     DVM session from a Pano device.
rem

rem Uncomment this if you wish to observe the execution of this script.
~~rem~~echo *** Session Logout -- %DATE% %TIME% *** >> C:\PANODIRECT-LOG.TXT
```

b. Trigger the event.

c. Check the log file to verify that the expected data was written to the log file.

3. Edit, save, then test your script.

40
Optimize DVM Performance

This section provides information on a number of basic system administration functions. Additional administrative functions can be found in:

- Pano Controller Administration
- Setting Up DHCP
- DVM Administration
- Endpoint Administration
- Define USB Peripheral Support
- Configure & Manage Pano Zero Clients & Desktop Preferences
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen

This chapter includes the following topics:

- Ways To Optimize DVM Performance
- Increase VMware ESX Server Service Console Memory
- Minimize DVM CPU Consumption
- User Group Policy Settings Management with Loopback Processing

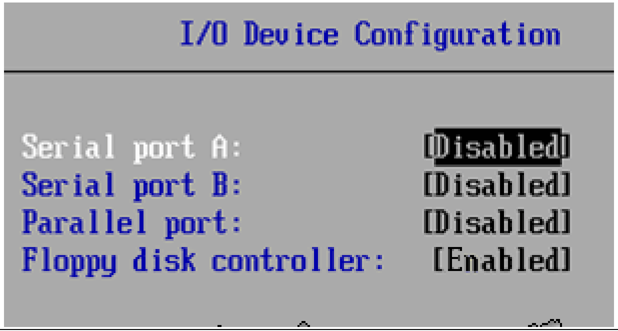
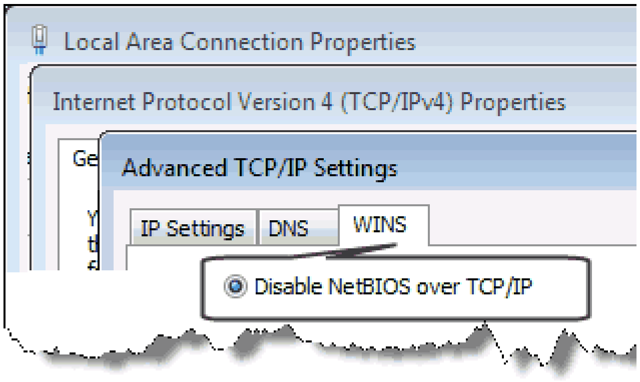
Ways To Optimize DVM Performance

Enabling or disabling specific Windows settings can help you improve DVM performance. The following table provides numerous tips about how to improve performance.

- Windows 7 Optimizations
- Windows XP Optimizations

Windows 7 Optimizations

If you want more tips, go to Microsoft's Optimize Windows 7 for better performance web page.

What	Why	How
Use vmxnet network adapter type.	Improves overall DVM performance.	Change Network Adapter Type
Disable serial COM and LPT ports on the DVM.	Improves overall DVM performance.	From the DVM's BIOS, go to the I/O Device Configuration section and choose Disable for the serial (COM) ports and parallel (LPT) ports.  I/O Device Configuration Serial port A: [Disabled] Serial port B: [Disabled] Parallel port: [Disabled] Floppy disk controller: [Enabled]
Turn off Screen Saver.	Improves overall DVM performance.	Go to Start > Control Panel > Appearance and Personalization > Change screen saver. Choose **(None)** from the Screen saver drop-down list.
Uninstall Tablet PC Components.		Go to Start > Control Panel > Programs and Features > Turn Windows features on or off. Clear the **Table PC Components** check box.
Disable NetBIOS over TCP/IP, if your environment does not rely on WINS (computers that are running operating systems other than Windows 2000 or Windows).	Improves overall DVM performance, slightly.	Go to Start > Control Panel > Network and Internet. Right-click on the network adapter. Select **IP v4** from the list, click Properties, then Advanced. In Advanced TCP/IP settings, click the WINS tab. Select the **Disable NetBIOS over TCP/IP** radio button.  Local Area Connection Properties Internet Protocol Version 4 (TCP/IPv4) Properties Advanced TCP/IP Settings IP Settings DNS WINS ● Disable NetBIOS over TCP/IP
Disable IPv6.	Improves overall DVM performance.	For instructions, see Microsoft's KB 929852. See also Network Addressing Requirements.
Use Windows Media Player's default settings.	Improves overall DVM performance.	For instructions, refer to the Microsoft's Media Player help.
Turn Automatic Computer Maintenance off	Improves overall DVM performance.	Go to Start > Control Panel > System and Security > Windows Update > Change settings > Never check for updates.
Disable Suggested Sites in IE.	Improves overall DVM performance.	Go to Tools button > Suggested sites.

What	Why	How
Disable troubleshooting	Improves overall DVM performance.	Go to Start > Control Panel > System and Security > All Control Panel Items > Troubleshooting > Change settings. Clear the following check boxes: **Allow users to browse for troubleshooters** **Allow troubleshooting to begin immediately when started**
Run the Disk Cleanup tool.	Improves overall DVM performance.	Go to Start > All Programs > Accessories > System Tools > Disk Cleanup. Select the drive, then click **OK**.
Disable power management	Improves overall DVM performance.	Control Panel > Hardware and Sound > Power Options > Show Additional plans. Choose High Performance.
Increase ESX host Service Console memory.	Improves overall DVM performance.	Increase VMware ESX Server Service Console Memory
Ensure hardware acceleration is enabled on your video cards.	Improves mouse movement.	For detailed instructions and explanation, go to Set Hardware Acceleration.
Disable the Disk Defragmenter schedule	Improves overall DVM performance.	Type `dfrgui` in the Start menu Search box, then press Enter. Select the drive, then click **Configure schedule** button. In the Disk Defragmenter Modify Schedule dialog box, clear the **Run on a schedule** check box, then click OK.
Disable network discovery (UPNP)	Improves overall DVM performance.	Go to Start > Control Panel > Network and Internet > Network and Sharing Center. Click on the **Change advanced sharing setting** link. Select the **Turn off network discovery** radio button.
Disable Windows Media Center	Improves overall DVM performance.	Go to Start > Control Panel > Programs > Programs and Features. Click on the **Turn Windows Features on or off** link. Scroll down to **Media Features** folder and expand it. Clear the **Windows Media Center** check box, then click OK.
Disable unneeded scheduled tasks	Improves overall DVM performance.	Use the Task Scheduler tool: Type `taskschd.msc` in the Start menu Search box, then press Enter.
Disable Remote Assistance	Improves overall DVM performance.	Go to Start > Control Panel > System and Security > System. Click on the **Remote Settings** link. In the Remote Assistance pane of the System Properties dialog box, clear the **Allow Remote Assistance connections to this computer** check box, then click OK.
Set virtual memory to hardcoded value of .5x the memory in the system with minidump enabled.		Go to Start > Control Panel > System and Security > System. In the left pane, click Advanced system settings. In the Performance pane of the Advanced tab, click on the **Settings** button. In the Virtual Memory pane of the Advanced tab, click on the **Change** button. Specify the Custom size for the virtual desktop’s virtual memory.
Disable NTFS Last Access Time Logging (NTFS Only).	Improves overall DVM performance. Windows operating systems update the last-accessed time of a file when applications open, read, or write to the file. This increases disk I/O and thereby increases the CPU overhead.	Add a new DWORD value named `NtfsDisableLastAccessUpdate` to `HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\FILESYSTEM`. Set the value to `1`.

Windows XP Optimizations

If you want more tips, go to Slimming Down Windows XP: The Complete Guide on Bold Fortune Forums.

What	Why	How
Use vmxnet network adapter type.	Improves overall DVM performance.	Set Hardware Acceleration
Increase ESX host Service Console memory.	Improves overall DVM performance.	Increase VMware ESX Server Service Console Memory
Limit the amount of memory that PowerPoint consumes.	Improves overall DVM performance.	Minimize DVM CPU Consumption
Configure the behavior of window dragging such that the windows contents doesn't show.	Improves window dragging performance. By default, when you move a window the entire contents of the window move.	Right-click on the Desktop, then choose **Properties Appearance**. Clear the **Show windows contents while dragging** check box.
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.	Go to Start > Control Panel > Display > Themes tab. Ensure that you're using the Windows XP theme.
Adjust performance settings.	Improves overall DVM performance.	From My Computer, click on **View system information**. In the Advanced Tab, go to the Performance section and click **Settings**. Select the **Adjust for best performance** radio button.
Ensure hardware acceleration is enabled on your video cards.	Improves mouse movement.	For detailed instructions and explanation, go to Set Hardware Acceleration. Right-click the desktop, and then click **Properties**. In the Display Properties dialog box, click the **Settings** tab > **Advanced** button > **Troubleshoot** tab. Set **Hardware acceleration** to Full.
Delete any hidden update uninstall folders.	Improves overall DVM performance.	Look in c:\WINDOWS. Example: $NtUninstallKB893756$.
Disable Indexing Services.	Improves overall DVM performance. Indexing improves searches by cataloging files. For users who search a lot, this may be beneficial and should not be disabled.	Go to Start > Run. Type **services.msc** and press Enter. Double-click on Indexing Service icon. If the service status is Running, then click the Stop button. In the Startup type: drop-down box, choose **Disabled**.
Disable Indexing of C: drive.	Improves overall DVM performance.	Right-click on the C: drive. Click Properties from the context window. Clear the **Allow Indexing Service to index this disk for fast file searching**.
Remove or minimize System Restore points.	Improves overall DVM performance.	Go to Start > Control Panel > System > System Restore. 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.	(Optional) To get a closer look at the services that are running, try out the AutoRuns utility. Go to Start > Control Panel > Administrative Tools > Services. If the unwanted service status is `Started`, double-click on the service, then click the Stop button. 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 Help and Support IMAPI CD Burning Service NetMeeting Remote Desktop Service Performance Logs and Alerts Task Scheduler Themes Uninterruptible Power Supply Windows Time Web Client Wireless Zero Configuration
Run the Disk Cleanup tool.	Improves overall DVM performance.	Go to Start > All Programs > Accessories > System Tools > Disk Cleanup. Select the drive, then click **OK**.
Run the Disk Defragmenter.	Improves overall DVM performance.	Go to Start > All Programs > Accessories > System Tools > Disk Defragmenter. Select the C: drive, then click the Defragmenter button.
Optimize Startup and Recovery Settings	Improves overall DVM performance.	Go to Advanced > Startup and Recovery. Clear the **Write an event to the system log** check box. Clear the **Send an administrative alert** check box. Clear the **Automatically restart** check box. 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**.

What	Why	How
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**.
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 the value to `1`. Disable Balloon tips. Add a new DWORD value named `EnableBalloonTips` to `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`. Set the value to `0`.
Set maximum event log (admin tool) sizes and clear all events	Improves overall DVM performance.	Right-click on **Application** and click **Properties**. In the Log Size section, select **Overwrite events as needed**. In the Log Size section, set the **Maximum Log Size** to 64kb. Click **Clear Log**, and click **No on the save dialog**. Repeat for Security, System and Internet Explorer logs.
Apply hotfix to Outlook.	Improves performance when opening/sending emails with Outlook, especially when using Outlook in cache mode.	Download this hotfix.

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:

Use the vSphere Client or the vSphere Client to increase service console memory on the ESX host.

1. Find out how much memory is already assigned to the Service Console:
   a. From the Hosts and Clusters view, click the **Hosts** tab.
   b. Double-click on the VMware ESX Server.
   c. Click the **Configuration** tab.
   d. In the Hardware area, click the **Memory** link.
2. Click the **Properties...** link.
3. In the **Service Console:** text box, increase the memory to 800 MB, then click OK.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 System 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

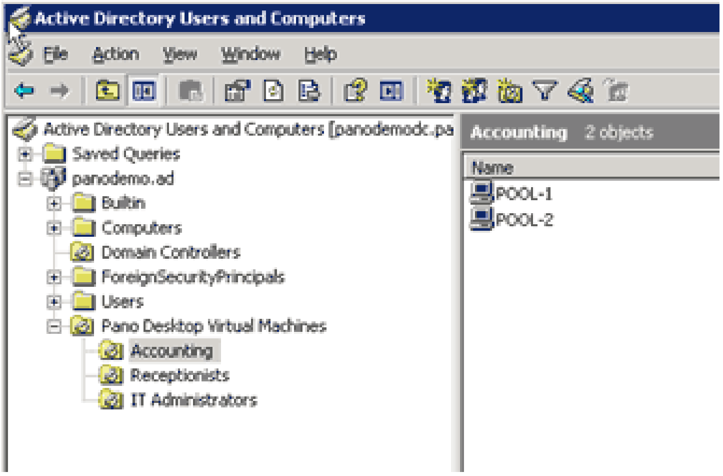
In some cases it may be desirable to use User Group Policy Loopback processing mode to manage user settings in your environment instead.

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.

Change Network Adapter Type

Caution: On Windows XP, the VMware network adapter (`vmxnet)` may appear as an ejectable device. See ID 4359.

Previously, you configured your virtual machine to use the default (`E1000` or `Flexible`) network adapter type. For better performance, you can use VMware's next generation network adapter type: `vmxnet3`.

Before You Begin: Installing VMware Tools (see Install Windows) provides the driver that the `vmxnet3` adapter type needs.

1. Use the vSphere Client to connect to vCenter Server.
2. From the Virtual Machine Properties dialog box, select the Network Adapter that you want to configure.
3. Click the **Change Type** button. Changes to the Adapter Type settings require Add/ Remove Device privileges.
4. Change VMware Network Adapter to `vmxnet`.

What to do next: Disable Network Adapter as Ejectable Device in Windows XP

Disable Network Adapter as Ejectable Device in Windows XP

On Windows XP, the VMware network adapter (`vmxnet)` may appear as an ejectable device, causing users to mistakenly eject the network adapter when they actually intend to eject their flash drive. Ejecting the network adapter causes the DVM to be inaccessible and requires you to add the network adapter back to the DVM through the vSphere Client.

You should modify your virtual machines so the network adapter is not displayed as an ejectable device by disabling the hotplug functionality. Disabling hot-plugability only affects virtual hardware. Users can still eject USB devices connected to the Pano System Endpoint.

Note: This is also discussed in ID 4359.

To remove hotplug functionality using the vSphere Client:

1. Log into the vSphere Client.
2. Select the virtual machine or template and make sure it is powered off.
3. Select Edit Settings, then select the Options tab.
4. Click on General, then Configuration Parameters.
5. Click on Add Row.
6. In the Name field, enter “devices.hotplug”.
7. In the Value field, enter “false”.
8. Click OK, and then click OK again.

To remove hotplug functionality using the command line:

From the virtual machine (that you intend to convert to a template), add the following line to the `vmx` file:

```
devices.hotplug = “false”
```

41

Endpoint Administration

This section provides information on a number of basic system administration functions. Additional administrative functions can be found in:

- Pano Controller Administration
- Setting Up DHCP
- DVM Administration
- Optimize DVM Performance
- Endpoint Administration
- Define USB Peripheral Support
- Configure & Manage Pano Zero Clients & Desktop Preferences
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen

Pano Zero Client and Pano Endpoint Tasks

- Pano Zero Client Light Indicators
- Pano System Endpoint Login Status Indicators
- Wake Pano Zero Client as End User
- Put Pano Zero Client into Sleep State as End User
- View Pano System Endpoint Information as End User
- View Users’ DVM Login Status and DVM Assignment
- Set Power Save Option for All Pano Zero Clients

Pano Zero Client Light Indicators

Under normal operation, the Pano Button should have a solid blue color within a few seconds of powering on. Once the Pano Button is solid blue, it should remain in this state until the Pano System Endpoint is powered off. The sequence is blinking red > blinking orange > solid orange > solid blue. This process should not last more than 15 seconds. If the process exceeds 15 seconds, go to Troubleshoot Networking Problems.

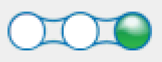
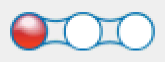
The Pano System Endpoint has the following states which are indicated by the light on the Pano Button.

Operation	Color	What's this mean?
Powered on	Blinking red	The Pano Zero Client is receiving power.
Connected to Network cable	Blinking orange	There is a 'live' Ethernet connection, in other words, the other end of the wire is plugged into something. This does not mean there is a valid IP address.
Connected to the Network	Solid orange	There is aa valid IP address, the color on the Pano Button changes to solid orange
Connected to the Pano Controller or a DVM	Solid blue	Communication has been established with the Pano Controller or a DVM.
(Pano G2) Connected, but in a sleep state	Solid green	When a Pano G2 Zero Client is in a sleep state, it consumes the least amount of power. To wake the device, press the Pano button. For more information, go to Configure Pano Device Sleep State

Pano System Endpoint Login Status Indicators

Although the Pano System delivers existing desktops instantly, sometimes the Pano System requires a few minutes to deploy new desktops. Use the following Status lights and messages to help you understand the login stages.

Table 41.1 **Pano Zero Client Login Status**

Status	Color	What's this mean?
	Yellow	The desktop is being deployed. If no desktop is available, the Pano System deploys (creates) a new desktop and the Options dialog shows a series of Status messages. **Deploy Pending...** - the deployment has not yet begun. The Pano System might be busy deploying new desktops to other users. Wait a few minutes. **Deploying...** - the deployment has begun. Wait a few minutes for the Pano System to deploy the desktop. **Logging on**... - the Pano System is logging you into the desktop. Wait a few minutes.
	Green	The desktop is **Ready**. You can now click Apply to access your desktop.
	Red	The desktop is **Not Ready**. In some cases you might also receive an **Operation Timed Out** message. You cannot log on because the Pano Direct Service is not running on the DVM.

Wake Pano Zero Client as End User

A Pano Zero Client device consumes less than 0.2 watts in low power "sleep" state. Notice the Pano G2 Zero Client's LED color is green. Simply press the Pano button to wake the device. Upon wake, the device goes through standard network IP and discovery routine.

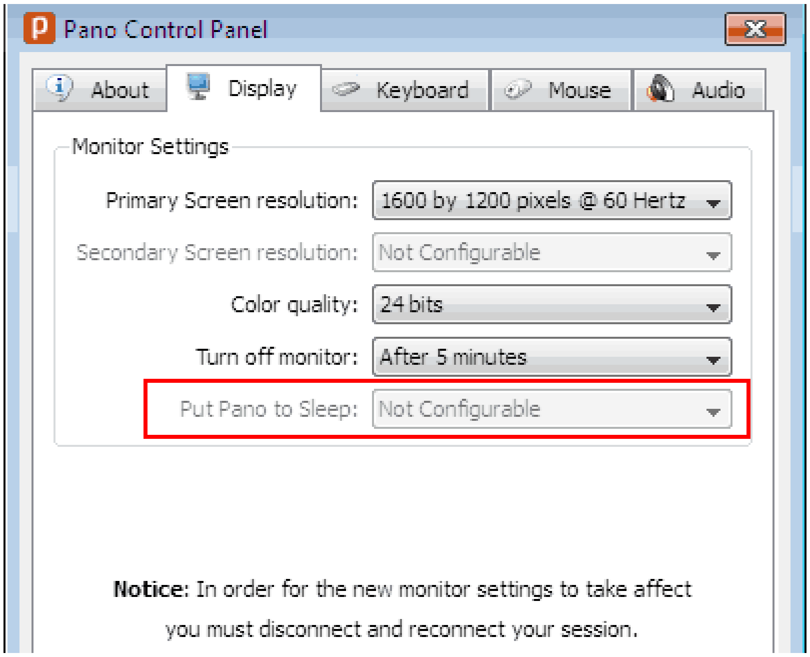
Related Topics

Put Pano Zero Client into Sleep State as End User

Configure Pano Device Sleep State

Put Pano Zero Client into Sleep State as End User

A Pano Zero Client device consumes less than 0.2 watts in low power "sleep" state. If you didn't enable end users to override the default sleep setting as outlined in Configure Pano Device Sleep State, the **Put Pano to Sleep** drop-down list indicates `Not Configurable`.



Monitor Settings

Primary Screen resolution: 1600 by 1200 pixels @ 60 Hertz

Secondary Screen resolution: Not Configurable

Color quality: 24 bits

Turn off monitor: After 5 minutes

Put Pano to Sleep: Not Configurable

Notice: In order for the new monitor settings to take affect you must disconnect and reconnect your session.

1. Open the Pano CP by either double-clicking the icon in your system tray or navigating to it by selecting **Start** > **Programs** > **PanoDirect** > **Pano Control**
2. Click on the **Display** tab, then choose a value from the **Put Pano to Sleep** drop-down list.
3. Click **OK**.

Related Topics

Wake Pano Zero Client as End User

Configure Pano Device Sleep State

View Pano System Endpoint Information as End User

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

Specific information includes:

- MAC address. Note: The MAC address of the Pano System Endpoint can also be obtained from Pano Controller.
- Screen Resolution
- Network Connection Information

To obtain information about a user’s Pano System Endpoint:

1. From the Pano System Endpoint that you want to troubleshoot, go to the Pano user login screen. You don’t need to log on.
2. In the Pano user login screen, click **Help**.

Set Power Save Option for All Pano Zero Clients

When a user is not logged in to the Pano System Endpoint 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 Controller 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 as End User.

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

Related Topics

Limitations to Sleep and Hibernate

Power On DVMs as End User

Power Off DVMs as End User

Power On DVMs as Administrator

Power Off DVMs as Administrator

42
Define USB Peripheral Support

USB support on endpoints can be enabled or disabled. This allows you to implement high-security systems by restricting access to removable media. This section explains the USB configuration options. Other management information can be found in:

- Pano Controller Administration
- Setting Up DHCP
- DVM Administration
- Optimize DVM Performance
- Endpoint Administration
- Configure & Manage Pano Zero Clients & Desktop Preferences
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen

You can install USB support, or not, and you can configure the degree of user control. Note that USB mouse and keyboard is always active.

- Install Pano Device USB Support
- Enable Users To Safely Remove USB Mass Storage Devices
- Restrict or Allow Use of Specific USB Devices

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. You must make sure, manually, that the `USBD.SYS` is installed in the DVM template. the Pano Direct Service installer cannot provide the file because Microsoft doesn’t allow this file to be redistributed.

During Pano Direct Service installation, USB support is enabled by default, but it will not work if the `USBD.SYS` file is not present. If this `USBD.SYS` file is not present on the DVM, the Pano Direct Service installer cannot enable Pano USB support, so you must do so manually.

To manually enable support using an existing driver.cab file:

This method 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.

What to do next: If you were in the process of installing Pano Direct Service, return to VMware Disposable Desktops.

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 vCenter Server.
   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
```

What to do next: If you were in the process of install Pano Direct Service, return to VMware Disposable Desktops.

Related Topics

Restrict or Allow Use of Specific USB Devices

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 Pano System Endpoints.

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

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.

What to do next: (Optional) Restrict or Allow Use of Specific USB Devices.

Restrict or Allow Use of Specific USB Devices

In general, the decision to 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.

Some companies have departments that work with highly sensitive data (for example, social security numbers), and this data cannot leave the premises. In these types of workplaces, restrict the use of specific USB devices in order to help protect against that data being copied to USB devices.

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 a DVM through a Pano System Endpoint, 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\PanoDirect`.
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 **PanoDirect** folder, 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 Direct Service or reboot your DVM.

43 Configure & Manage Pano Zero Clients & Desktop Preferences

This section provides information on a number of basic system administration functions. Additional administrative functions can be found in:

- Pano Controller Administration
- Setting Up DHCP
- DVM Administration
- Optimize DVM Performance
- Endpoint Administration
- Define USB Peripheral Support
- Create and Manage DVM Collections–VMware & Hyper-V
- Create and Manage DVM Collections–Xen

You can pre-configure many aspects of your user’s desktop settings and preferences, and you can decide which settings they will have control over, and which will be restricted.

End User Options

- About Pano Control Panel
- Set User Preferences
- Set Keyboard Settings for Specific DVMs
- Set Audio Settings for Specific DVMs
- Set Default Keyboard Layout and Input Language for Specific DVMs
- Enable Language Preference for Pano Client Login Screen
- Set Screen Resolution Settings for Specific DVMs
- Set Power Save Settings for Specific DVMs as End User

Pano Zero Client

- Retrieve Pano Zero Client Information
- Determine Pano Device Model
- Manually Add Pano Zero Clients
- Rename Pano Zero Clients
- Change Pano Zero Client MAC Address or IP Address
- Remove Pano Zero Clients
- Identify Pano Zero Client Serial Numbers
- Configure Pano Device Sleep State
- Disconnect Pano Zero Clients from DVMs
- Unassign Pano Zero Clients from DVMs

Other EndPoints

- Disable Pano System Endpoint
- Enable Pano System Endpoints

- Enable Remote Desktop & Set RDP Users

Login Options

- Default User Login Preferences
- Use a Custom Login Image
- Reset Pano Client Login Screen Image To Default Image
- Restart Pano Client Login Screens
- About Password Changes via Pano Client Login Screen
- Create Device-Based DVM Assignments

USB

- Install Pano Device USB Support
- Enable Users To Safely Remove USB Mass Storage Devices
- Restrict or Allow Use of Specific USB Devices

Set User Preferences

Before You Begin: You must set up your collections, as outlined in Create DVM Collections, before you can set user preferences.

Task	Go to...
Set login image.	Use a Custom Login Image
(Optional) Add Pano System Endpoints.	Manually Add Pano Zero Clients
Set preferences.	Default User Login Preferences

What to do next: If you're performing this workflow as part of a deployment, this workflow completes your deployment. Congratulations!

Pano Zero Client Light Indicators

Under normal operation, the Pano Button should have a solid blue color within a few seconds of powering on. Once the Pano Button is solid blue, it should remain in this state until the Pano System Endpoint is powered off. The sequence is blinking red > blinking orange > solid orange > solid blue. This process should not last more than 15 seconds. If the process exceeds 15 seconds, go to Troubleshoot Networking Problems.

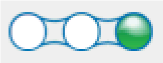
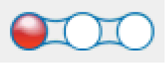
The Pano System Endpoint has the following states which are indicated by the light on the Pano Button.

Operation	Color	What's this mean?
Powered on	Blinking red	The Pano Zero Client is receiving power.
Connected to Network cable	Blinking orange	There is a 'live' Ethernet connection, in other words, the other end of the wire is plugged into something. This does not mean there is a valid IP address.
Connected to the Network	Solid orange	There is aa valid IP address, the color on the Pano Button changes to solid orange
Connected to the Pano Controller or a DVM	Solid blue	Communication has been established with the Pano Controller or a DVM.
(Pano G2) Connected, but in a sleep state	Solid green	When a Pano G2 Zero Client is in a sleep state, it consumes the least amount of power. To wake the device, press the Pano button. For more information, go to Configure Pano Device Sleep State

Pano System Endpoint Login Status Indicators

Although the Pano System delivers existing desktops instantly, sometimes the Pano System requires a few minutes to deploy new desktops. Use the following Status lights and messages to help you understand the login stages.

Table 43.2 **Pano Zero Client Login Status**

Status	Color	What's this mean?
	Yellow	The desktop is being deployed. If no desktop is available, the Pano System deploys (creates) a new desktop and the Options dialog shows a series of Status messages. **Deploy Pending...** - the deployment has not yet begun. The Pano System might be busy deploying new desktops to other users. Wait a few minutes. **Deploying...** - the deployment has begun. Wait a few minutes for the Pano System to deploy the desktop. **Logging on**... - the Pano System is logging you into the desktop. Wait a few minutes.
	Green	The desktop is **Ready**. You can now click Apply to access your desktop.
	Red	The desktop is **Not Ready**. In some cases you might also receive an **Operation Timed Out** message. You cannot log on because the Pano Direct Service is not running on the DVM.

Wake Pano Zero Client as End User

A Pano Zero Client device consumes less than 0.2 watts in low power "sleep" state. Notice the Pano G2 Zero Client's LED color is green. Simply press the Pano button to wake the device. Upon wake, the device goes through standard network IP and discovery routine.

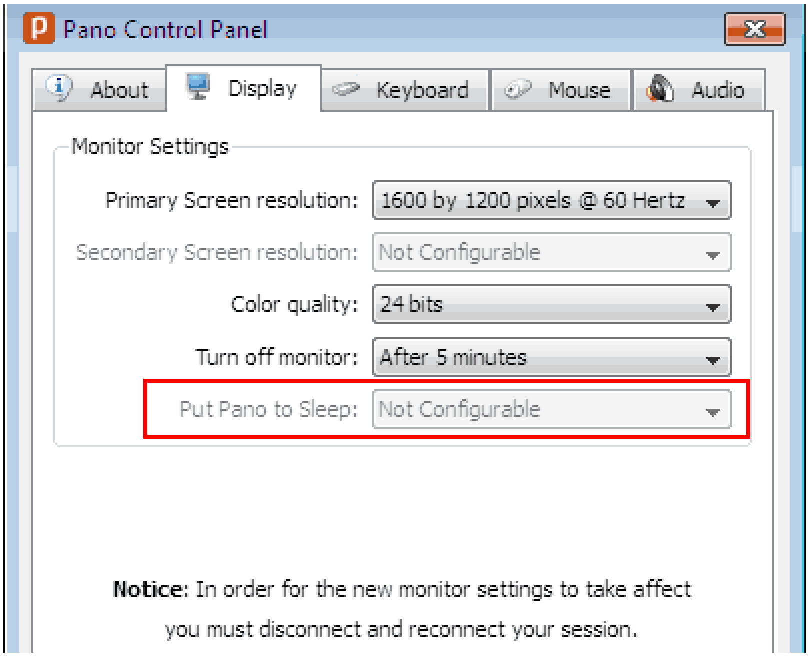
Related Topics

Put Pano Zero Client into Sleep State as End User

Configure Pano Device Sleep State

Put Pano Zero Client into Sleep State as End User

A Pano Zero Client device consumes less than 0.2 watts in low power "sleep" state. If you didn't enable end users to override the default sleep setting as outlined in Configure Pano Device Sleep State, the **Put Pano to Sleep** drop-down list indicates `Not Configurable`.



Monitor Settings

Primary Screen resolution: 1600 by 1200 pixels @ 60 Hertz

Secondary Screen resolution: Not Configurable

Color quality: 24 bits

Turn off monitor: After 5 minutes

Put Pano to Sleep: Not Configurable

Notice: In order for the new monitor settings to take affect you must disconnect and reconnect your session.

1. Open the Pano CP by either double-clicking the icon in your system tray or navigating to it by selecting **Start** > **Programs** > **PanoDirect** > **Pano Control**
2. Click on the **Display** tab, then choose a value from the **Put Pano to Sleep** drop-down list.
3. Click **OK**.

Related Topics

Wake Pano Zero Client as End User

Configure Pano Device Sleep State

View Pano System Endpoint Information as End User

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

Specific information includes:

- MAC address. Note: The MAC address of the Pano System Endpoint can also be obtained from Pano Controller.
- Screen Resolution
- Network Connection Information

To obtain information about a user's Pano System Endpoint:

1. From the Pano System Endpoint that you want to troubleshoot, go to the Pano user login screen. You don't need to log on.
2. In the Pano user login screen, click **Help**.

Set Power Save Option for All Pano Zero Clients

When a user is not logged in to the Pano System Endpoint 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 Controller 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 as End User.

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

Related Topics

Limitations to Sleep and Hibernate

Power On DVMs as End User

Power Off DVMs as End User

Power On DVMs as Administrator

Power Off DVMs as Administrator

Determine Type of Pano Zero Client

To determine the type of Pano System Endpoint used, login to the Pano Controller and select the device in the **Clients** tab.

To determine by looking at the physical device, refer to Pano Zero Client Technical Specification.

Retrieve Pano Zero Client Information

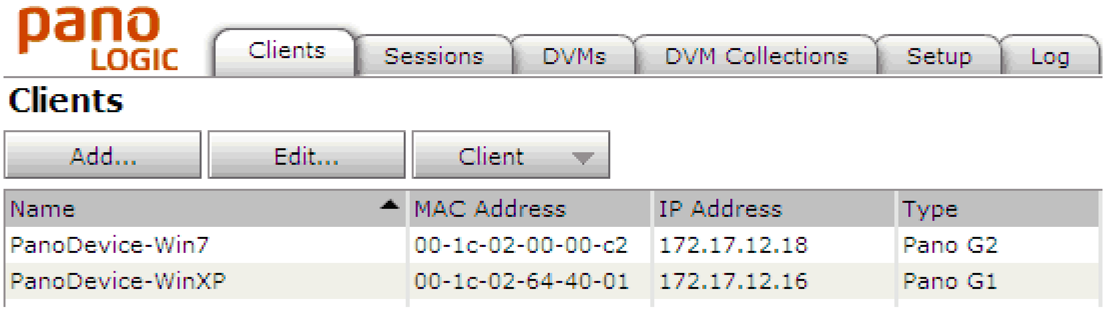
From the **Pano System Endpoints** tab, you can retrieve the following information for all Pano System Endpoints that were either automatically discovered or manually added.

Column Name	Description
Name	The name of the Pano System Endpoint. The Pano Controller automatically generates this name. You can edit the name.
MAC Address	The unique MAC address for the Pano System Endpoint's network interface.
IP Address	The IP Address of the Pano System Endpoint.
Assignment	DVM assigned to client in case of device collections. Applies to VDB only
Assignment Broker	Name of Broker that is brokering DVM assigned to the clientAssignment Broker.

Column Name	Description
Connection	Status of the Pano System Endpoint as known to the Pano Controller. **Unreachable** - Pano Controller cannot contact the Pano System Endpoint. **Discovered** - Pano Controller has discovered the Pano System Endpoint on the network. **Login** - Pano Controller initiated the login screen. This does not mean that the login screen is being displayed on the Pano System Endpoint. The login could have trouble connecting to the Pano System Endpoint. **DVM** - The DVM is connected to the Pano System Endpoint. **Ready** - A secondary monitor is ready to be used. **Sleeping** - The DVM is in sleep state (see Configure Pano Device Sleep State).
Rx Packets	Number of packets per second received by the Pano System Endpoint as observed by Pano Direct Service.
Re Rx Packets	Number of identical packets per second received by the Pano System Endpoint multiple times as observed by Pano Direct Service.
Tx Packets	Number of packets per second transmitted by the Pano System Endpoint as observed by Pano Direct Service.
Re Tx Packets	Number of identical packets per second transmitted by the Pano System Endpoint multiple times as observed by Pano Direct Service.
Min RTT	Minimum round-trip time from the Pano System Endpoint 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 System Endpoint 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 System Endpoint 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.

Determine Pano Device Model

Device type refers to the model of a Pano System Endpoint. The device type can be Pano G2 or Pano G1. You can easily identify a Pano G1 from a Pano G2 by comparing the video display ports. Pano G2 has a DVI port; Pano G1 has a VGA port. To determine the Pano System Endpoint model, Log on to the Pano Controller, and click on the **Pano System Endpoints** tab. The device type appears in the **Type** column.



Name	MAC Address	IP Address	Type
PanoDevice-Win7	00-1c-02-00-00-c2	172.17.12.18	Pano G2
PanoDevice-WinXP	00-1c-02-64-40-01	172.17.12.16	Pano G1

Related Topics

Pano Zero Client Hardware Specifications

Connect Pano Zero Clients To Your Wireless Network

If you want to connect your Pano System Endpoints to your company's existing wireless network, you can connect a Wireless bridge (sometimes called AP client mode) to each Pano System Endpoint. For a list of supported Wireless bridges, go to Supported Wireless Bridges.

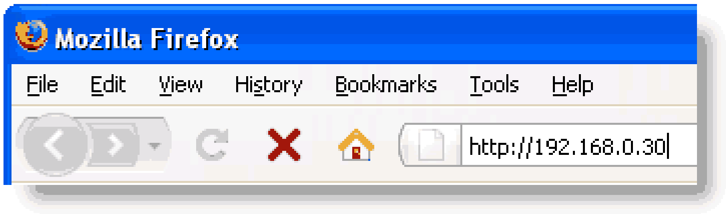
A few details before we begin:

- The Wireless bridge will be an AP client–not a DHCP server. In other words, it will not be assigning IP addresses.
- The Wireless bridge will not be an Wireless access point. In other words, no Pano System Endpoints–other than the Pano System Endpoint to which the Wireless bridge is directly connected–will connect to the network via this Wireless device.

To connect Pano System Endpoints to your wireless network:

1. Retrieve the SSID for your wireless network.
2. Power on the Wireless bridge. You can provide power using either the USB cable or the Power cable.
3. Connect the Wireless bridge's Ethernet cable to an Ethernet port on any PC running Windows XP. This PC is a temporary means for configuring the Wireless bridge.
4. Using the mode switch on the Wireless bridge, set the device to AC Client mode, assuming your device can be either an Access Point, AC Client, or Router.
5. Configure the Wireless bridge.
   - **a.** From a web browser, launch the Wireless bridge's "Setup Wizard".

     Type `http://`*`WirelessAPIPAddress`*, where WirelessAPIPAddress is the designated IP address for your Wireless bridge's UI, to launch the wizard. Usually, such a device can be accessed by 192.168.1.1, though the D-Link DWL-G730AP uses 192.168.0.30.

     http://192.168.0.30

   - **b.** If prompted, go to the vendor's site and download the latest firmware and install the new firmware version on to the Wireless bridge.
   - **c.** When prompted by the wizard, choose the SSID for your network. The wizard should automatically provide you a list of the wireless networks that it finds.
   - **d.** If prompted for a username and password, you must type the default username and password for your Wireless bridge. Each product is different. The D-Link DWL-G730A, for example, has a user name of `admin` and no password is required.
6. Specify your network configuration information.
7. (Recommended) Set the admin password to be the same on all Wireless bridges.
8. Verify that the Wireless bridge is sending and receiving packets. Usually a Wireless bridge's Setup Wizard has a Status tab that shows packet data.

Use a Custom Login Image

You can replace the image that is presented on the Pano user login screen with a custom image such as your company logo. You can also use this screen for a login message with a disclaimer about company policies or security measures.

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

When you upload a login image to any Pano Controller that is a member of a Pano Controller group, the Pano System automatically uploads the image to all the Pano Controllers in that group. (See Create Pano Controller Group) Similarly, if the Pano Controllers are in a failover configuration, then the Pano System automatically applies the new image to the active Pano Controller followed by the standby Pano Controller.

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

1. Prepare a `.png` image file. You will select this file later.
2. Log on to the Pano Controller.
3. Click on the **Pano System Endpoints** tab.
4. Click on the **Settings** button, then choose **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.

Related Topics

Restart Pano Client Login Screens

Reset Pano Client Login Screen Image To Default Image

Reset Pano Client Login Screen Image To Default Image

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

Related Topics

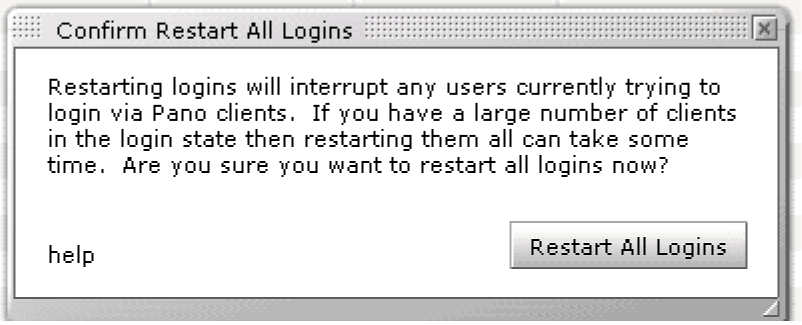
Restart Pano Client Login Screens

Use a Custom Login Image

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 user login screen restarts). However, you can restart all Pano user login screens to force the change.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Click the **Settings** drop-down list, then choose **Restart All Logins**. The Confirm Restart All Logins dialog appears.
4. Click the **Restart All Logins** button.



Restarting logins will interrupt any users currently trying to login via Pano clients. If you have a large number of clients in the login state then restarting them all can take some time. Are you sure you want to restart all logins now?

Related Topics

Reset Pano Client Login Screen Image To Default Image

Use a Custom Login Image

About Password Changes via Pano Client Login Screen

About Password Changes via Pano Client Login Screen

Whenever end users are required by the directory service to change their password, the Pano user login screen prompts the users to make the change and forwards the change to the directory service. After the end user successfully changes the password, the Pano system returns the user to the Pano user login screen, where the user can log on to the DVM using the new credentials.

This feature requires that you configure LDAP communication between the Pano Controller and the directory service for SSL. An out-of-the-box installation of Windows Active Directory does not automatically enable LDAP over SSL. To do so, refer to the following Microsoft Knowledge Base articles:

- Enable LDAP over SSL for Windows Server 2008
- Enable LDAP over SSL for Windows Server 2003

A password change handles all scenarios:

- new accounts that require the end user to change their password on next login;
- time expired passwords;
- integrations with VMware View or XenDesktop;
- Windows XP or Windows 7; and connections via Pano System Endpoints and Pano Remote

Related Topics

Reset Pano Client Login Screen Image To Default Image

Use a Custom Login Image

Restart Pano Client Login Screens

Manually Add Pano Zero Clients

If you enabled one of the following automatic discovery methods during setup, Pano Client Discovery automatically discovers and adds the Pano System Endpoints to your Pano Controller:

- Set Up Pano Client Discovery Using Broadcast/Probe
- Set Up Pano Client Discovery Using DHCP

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

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Click **Add**.
4. Type the name you want to use to identify the Pano System Endpoint. For example, you can enter a user name or the physical location of the Pano System Endpoint.
5. Type the MAC address of the Pano System Endpoint.
6. Type the IP address.
7. Click **Add Pano**.

Related Topics

Set Up Pano Client Discovery Using DHCP

Rename Pano Zero Clients

Pano System Endpoints need to be discovered before they can be controlled by the Pano Controller. Once discovered, the Pano System Endpoints receive a name automatically:

`PanoDevice-`*`PanoDeviceMacAddress`* (For example, PanoDevice-00-1c-02-40-17-95)

However, you can rename Pano System Endpoints. There are no restrictions on the name other than a length limit of 255 characters.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint from the list.
4. Modify the name.
5. Click **Update Pano System Endpoint**.

Related Topics

Set Up Collections with Device Restrictions

Change Pano Zero Client MAC Address or IP Address

Never change the MAC address or IP address of a Pano System Endpoint that has been automatically discovered. The only reason why you'd change a Pano System Endpoint's MAC address or IP address is if you manually added a Pano System Endpoint, and you want to fix a typo in the address.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint from the list.
4. Modify MAC address or IP address.
5. Click **Update Pano System Endpoint**.

Remove Pano Zero Clients

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

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint from the list.
4. Click **Remove**.

Identify Pano Zero Client Serial Numbers

Pano Remote USB keys purchased after April 20, 2011 have unique serial numbers. Serial numbers enable you to track usage per key and disable (block) access for specific or unregistered keys.

Note: Pano System Endpoints also have serial numbers, but these serial numbers are not currently displayed in the Clients tab.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Locate the Pano System Endpoint in the table. The unique serial number for the Pano System Endpoint appears in the Serial Number column.

Related Topics

Configure Pano Remote Access

Enable Pano System Endpoints

Disable Pano System Endpoint

If a Pano Remote USB key or a Pano System Endpoint is lost or stolen, for security purposes it's best practice to disable that Pano System Endpoint.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint, then, from the Clients button, choose **Disable Client**.
4. Click the **Disable** button. The Status column indicates `Disabled`.

Related Topics

Enable Pano System Endpoints

Identify Pano Zero Client Serial Numbers

Enable Pano System Endpoints

If you formerly disabled a Pano Remote USB key or a Pano System Endpoint that was lost or stolen, but it has since been recovered, you can enable it so that your user can continue using it.

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint, then, from the Clients button, choose **Enable Client**.
4. Click the **Enable** button. The Status column indicates `Enabled`.

Related Topics

Identify Pano Zero Client Serial Numbers

Default User Login Preferences

Pano System Endpoints 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 they log on to their DVMs.

Default settings are used by Pano System Endpoints when they are displaying the Pano user login screen. Default settings are also used when users have logged on and have not set their personal preferences, which they can do from the Pano Control Panel.

- **Display Preferences**

The display settings (**Resolution**, **Colors**, **Refresh Rate**, and **Power Save Delay**) indicate the preferred settings to be used by a Pano System Endpoint to drive a video monitor. However, the physical monitor might not support the preferred display settings; in this case, the Pano System Endpoint queries the monitor for its list of supported settings to get as close as possible to the preferred settings.

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

When connecting to a DVM via a Remote Desktop connection or Pano web access, you must configure the DVM if your users desire 24-bit color depth. When connecting via a Pano System Endpoint to a DVM with Pano Direct, your users can select 16-bit or 24-bit color depth through the Pano Control Panel. No other configuration is required.

- **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, end users can set these values individually to suit their personal preference through the Pano Control Panel.

- **Sleep Preferences**

The **Power Sleep Delay** and **User Power Sleep Override** can be set by the administrator to control when Pano System Endpoints go into sleep mode. For more information, go to Configure Pano Device Sleep State.

- **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, 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. End-users can set these values individually to suit their personal preference through the Pano Control Panel.

- **User Logon Languages**

Administrators can provide end users with a variety of language choices for native-language keyboard input. Administrators enable specific keyboard support and end users select their language choice at login.

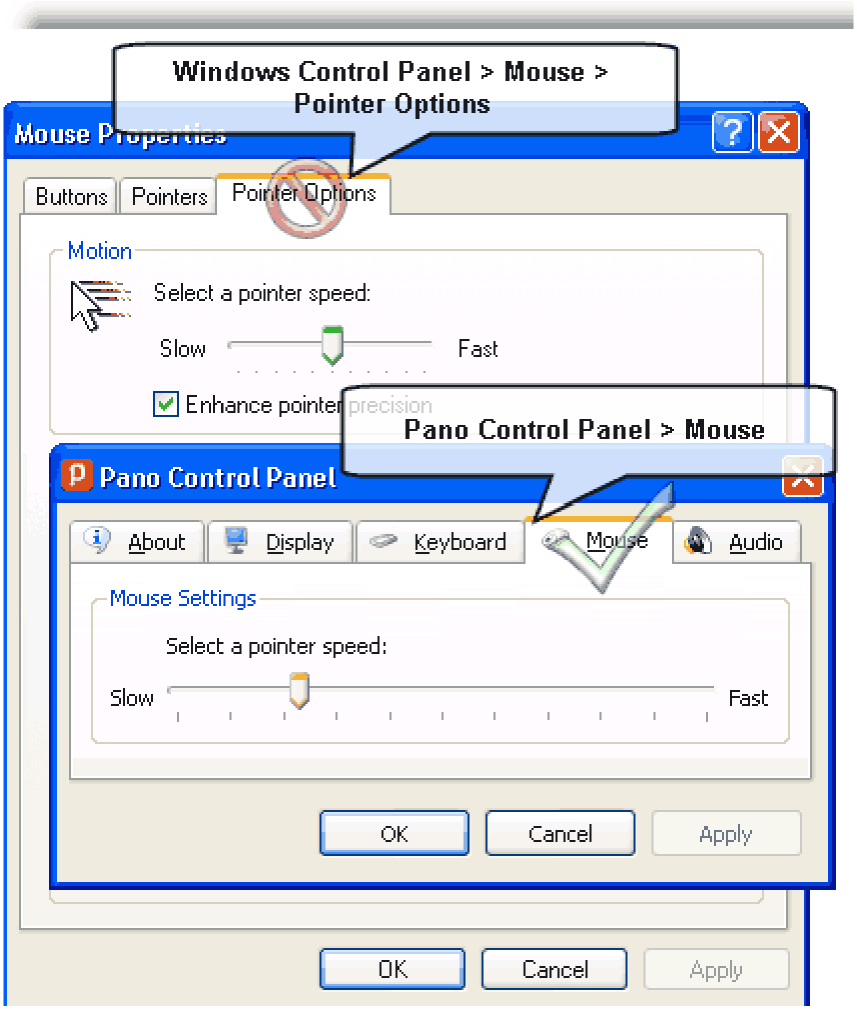
To specify a language, go to Enable Language Preference for Pano Client Login Screen.

About Pano Control Panel

Your users are used to changing their display (monitor), keyboard, mouse and audio settings from Windows Control Panel’s **Display Properties** dialog and **Mouse Properties** dialog. However, now that they have a virtual desktop, and even if they use Pano Dual Monitor, they must make such changes from the Pano Control Panel. All other typical desktop customizations can be done using Windows.

If they try to change monitor, keyboard, mouse and audio settings from within the Windows Control Panel, they’ll notice that the Windows dialogs are “locked down” where appropriate.

You’ll need to introduce your users to this tool, and you can do so by refer your users to the end-user help at http://help.panouser.com, if you haven’t already.



Windows Control Panel > Mouse > Pointer Options

Pano Control Panel > Mouse

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 an end user's login language preference, see Enable Language Preference for Pano Client Login Screen.

To set keyboard settings from the Pano Control Panel:

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

To set keyboard settings from the Pano Controller:

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint.
4. Click the **Settings** drop-down list, then choose **Login Preferences...**.
5. Use the Keyboard Settings slider to specify Repeat delay and Repeat rate settings, then click **Set Preferences**.

Troubleshooting: Go to Troubleshoot Monitor, Mouse, and Keyboard Problems.

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 from the Pano Control Panel:

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

To set audio settings from the Pano Controller:

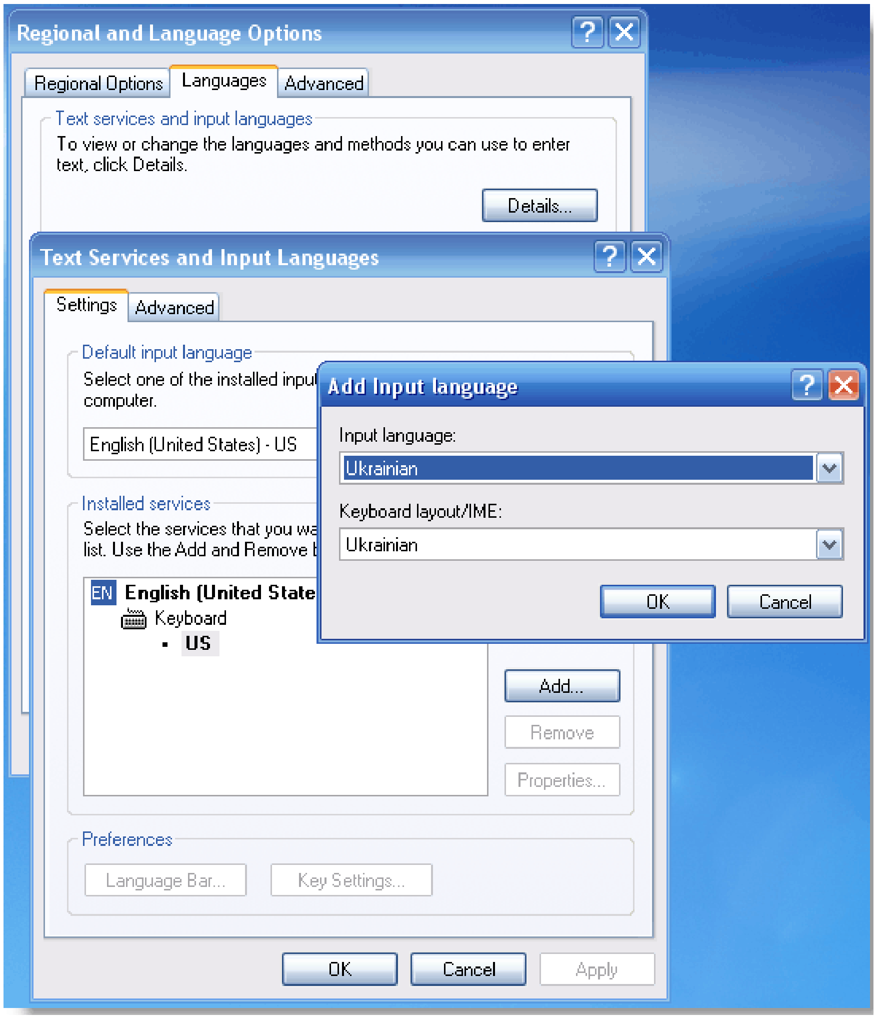
1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint.

4. Click the **Settings** drop-down list, then choose **Login Preferences...**.
5. Use the Volume slider to define the overall volume level for output, then click **Set Preferences**.

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, using the Windows Control Panel.

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 needed. choose it as the default input. Click **OK**.

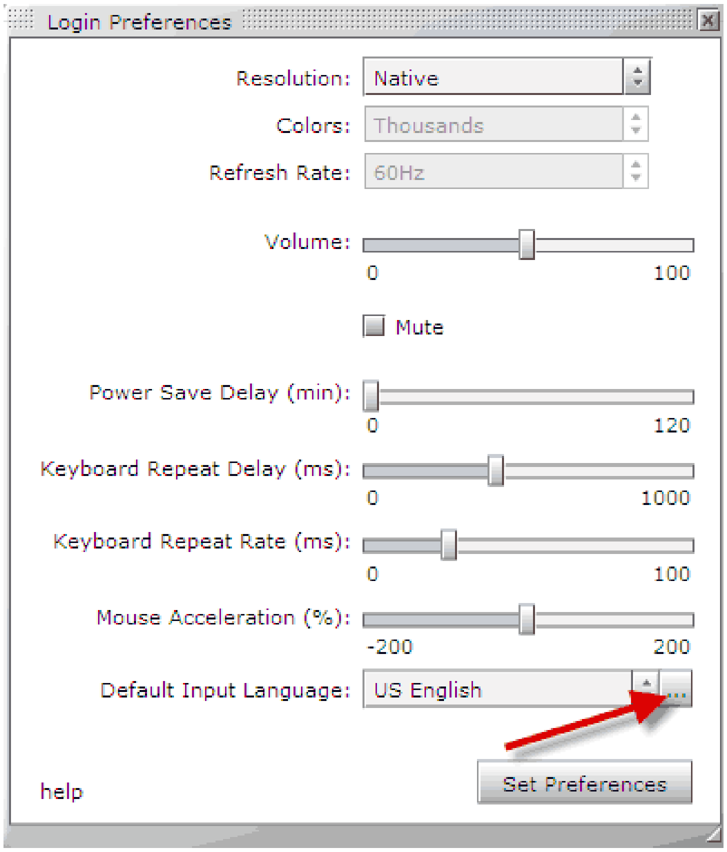

Regional and Language Options
Regional Options
Languages
Advanced
Text services and input languages
To view or change the languages and methods you can use to enter text, click Details.
Details...
Text Services and Input Languages
Settings
Advanced
Default input language
Select one of the installed input
computer.
English (United States) - US
Installed services
Select the services that you wa
list. Use the Add and Remove b
EN English (United State
Keyboard
US
Add...
Remove
Properties...
Preferences
Language Bar...
Key Settings...
OK
Cancel
Apply
Add Input language
Input language:
Ukrainian
Keyboard layout/IME:
Ukrainian
OK
Cancel

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, the specified default language is seen.

Enable Language Preference for Pano Client Login Screen

A Pano System environment supports multiple language keyboard layouts. Administrators can enable any or all supported keyboards; end users can select their preferred language.

1. Log on to the Pano Controller Administration and click on the **Clients** tab.
2. Click on the **Settings** drop-down menu and select **Login Preferences**
3. In the Login Preferences menu, click on **Default Input Language**, then click on the **ellipsis (...)** to bring up the Modify Input Languages menu.
4. Select the languages you want to make available for end users, add them to the selected list box and click **OK**.



Login Preferences

Resolution: Native

Colors: Thousands

Refresh Rate: 60Hz

Volume: 0 100

□ Mute

Power Save Delay (min): 0 120

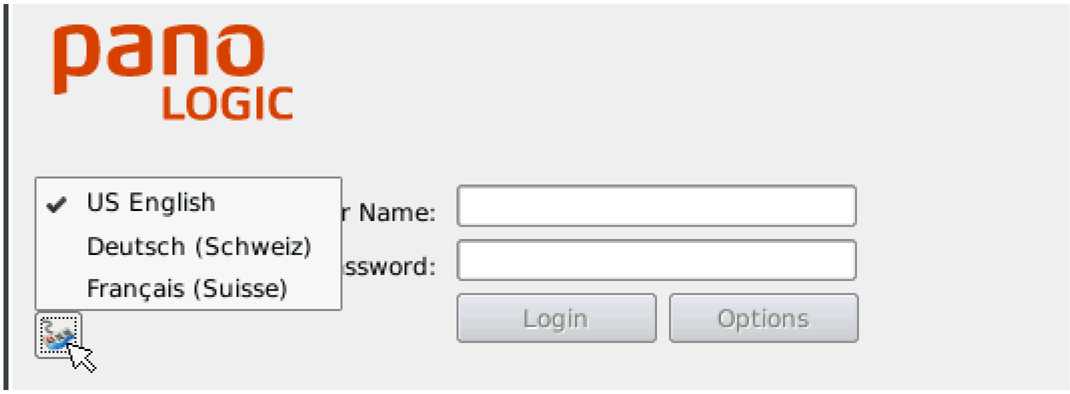
Keyboard Repeat Delay (ms): 0 1000

Keyboard Repeat Rate (ms): 0 100

Mouse Acceleration (%): -200 200

Default Input Language: US English ...

5. To verify, go to a Pano System Endpoint and click on the **Keyboard Language Chooser** button that appears on the login screen, displaying the login languages that you selected.



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 from the Pano Control Panel:

1. Open the Pano CP by either double-clicking the icon in your system tray or navigating to it by selecting **Start** > **Programs** > **PanoDirect** > **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.

To change the screen resolution from the Pano Controller:

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint.
4. Click the **Settings** drop-down list, then choose **Login Preferences...**.
5. Use the **Resolution**, **Colors**, and **Refresh Rate** drop-down lists to specify your screen resolution settings, then click **Set Preferences**.

Set Power Save Settings for Specific DVMs as End User

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.

1. Open the Pano Control Panel by either double-clicking the icon in your system or navigating to it by selecting **Start** > **Programs** > **PanoDirect** > **Pano Control Panel**.
2. Click the **Display** tab.
3. Specify a value for the **Turn off monitor** setting.
4. Click **Apply**.

Related Topics

Limitations to Sleep and Hibernate

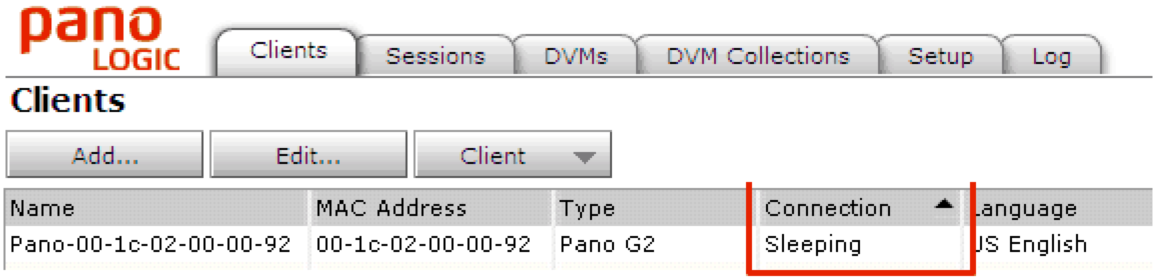
Set Power Save Option for All Pano Zero Clients

Configure Pano Device Sleep State

Configure Pano Device Sleep State

A Pano G2 Zero Client consumes less than 0.2 watts when in low power sleep state. Pano Zero Clients go into sleep state based on configurable time limits, which you can specify from the Pano Controller administrator interface. Alternatively, you can disable this feature altogether. When the Pano Zero Client is in sleep state, end users can simply press the Pano button to wake the device. Upon waking, the Pano System Endpoint goes through the standard network IP and discovery routine.

The Pano Controller reports whether or not a Pano System Endpoint is in sleep state in the Pano Controller administrator interface.

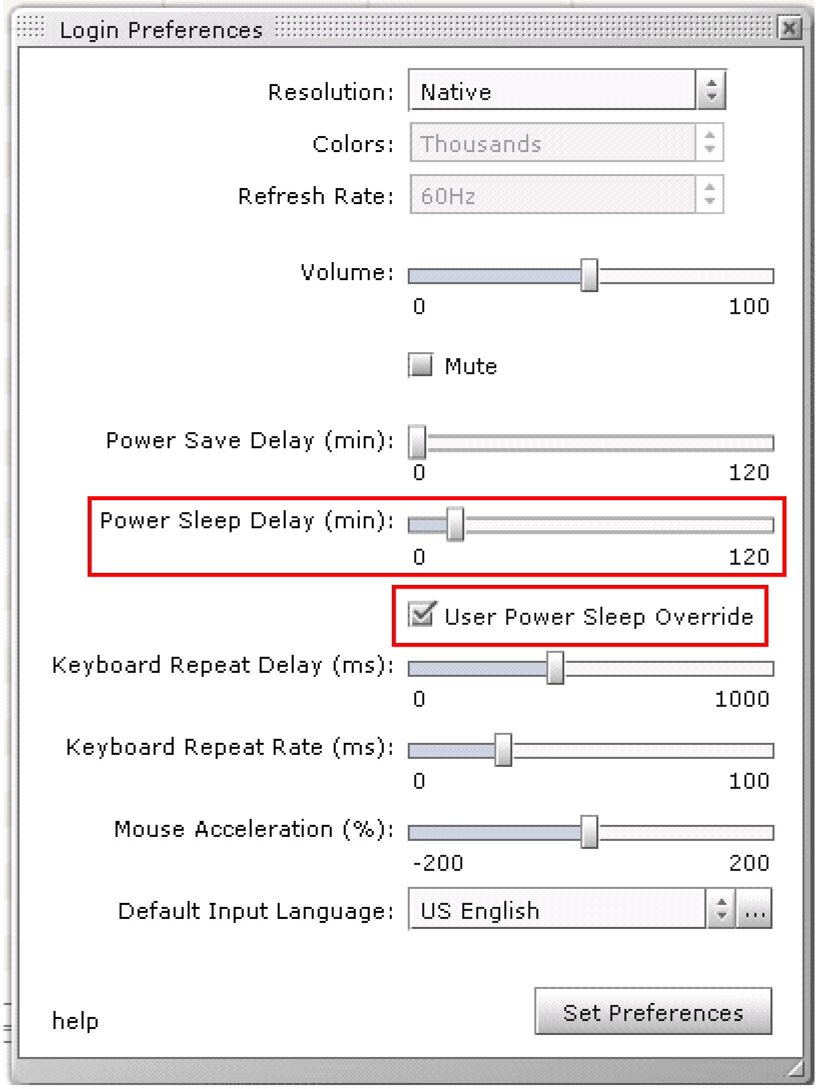


Name	MAC Address	Type	Connection	Language
Pano-00-1c-02-00-00-92	00-1c-02-00-00-92	Pano G2	Sleeping	US English

To configure sleep state:

1. Log on to the Pano Controller.
2. Click on the **Pano System Endpoints** tab.
3. Select the Pano System Endpoint.
4. Click the **Settings** drop-down list, then choose **Login Preferences...**.
5. Use the **Power Sleep Delay** slider bar to set the default value (in minutes) for sleep delay. After idleness exceeds the value you specify, the Pano System Endpoint goes to

sleep. If you'd like to enable end users to change this value, select the **User Power Sleep Override** checkbox.



Login Preferences

Resolution: Native

Colors: Thousands

Refresh Rate: 60Hz

Volume: 0 100

□ Mute

Power Save Delay (min): 0 120

Power Sleep Delay (min): 0 120

☑ User Power Sleep Override

Keyboard Repeat Delay (ms): 0 1000

Keyboard Repeat Rate (ms): 0 100

Mouse Acceleration (%): -200 200

Default Input Language: US English

To disable sleep state:

If you don't want Pano System Endpoint to go into a sleep state, simply set the **Power Sleep Delay** to a value of zero.

Related Topics

Wake Pano Zero Client as End User

Put Pano Zero Client into Sleep State as End User

Limitations to Sleep and Hibernate

Set Power Save Settings for Specific DVMs as End User

Disconnect Pano Zero Clients from DVMs

End users can simply set the screen saver or press the Pano Button to disconnect the Pano System Endpoint from the DVM. However, end users can forget to disconnect and call you in a panic.

Although a rare event, consider this scenario: a “roaming” end user, John Smith, logs on to a DVM from a conference room to give a confidential presentation. John forgets to disconnect and leaves the office. If other visitors to that conference room attempt to log on to a DVM using the same Pano System Endpoint, they will see the confidential information; as such, John calls you in a panic as soon as he remembers that he forgot to disconnect. If you’re at remote location, you can initiate the disconnect from the Management User Interface (MUI); in this case, John will be quite relieved.

1. Log on to the Pano Controller.
2. Click the **DVMs** tab.
3. Select the DVM that you want to reset, then, from the **Desktop** drop-down button, choose **Disconnect Client**.
4. When prompted to confirm your selection, click **Disconnect Client**.

Related Topics

Control Session Timeouts

VMware Disposable Desktops

Unassign Pano Zero Clients from DVMs

In the case of a Device-Based Collection, after a Pano System Endpoint has been assigned to a DVM the Pano Controller allows a device to connect to that designated DVM only. If you later want to use that Pano System Endpoint with a User Based Collection, you must first unassign the Pano System Endpoint from the designated DVM.

To unassign a Pano System Endpoint from a DVM:

1. Log on to the Pano Controller.
2. Click the **Clients** tab.
3. Select the DVM from the list.
4. From the **Client** drop-down list, choose **Unassign**. The DVM is now available to be assigned to another Pano System Endpoint.

Related Topics

Manually Assign Pano Zero Client in Device-Based Collections

Unassign Users from DVMs

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. You must make sure, manually, that the

USBD.SYS is installed in the DVM template. the Pano Direct Service installer cannot provide the file because Microsoft doesn't allow this file to be redistributed.

During Pano Direct Service installation, USB support is enabled by default, but it will not work if the USBD.SYS file is not present. If this USBD.SYS file is not present on the DVM, the Pano Direct Service installer cannot enable Pano USB support, so you must do so manually.

To manually enable support using an existing driver.cab file:

This method 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.

What to do next: If you were in the process of installing Pano Direct Service, return to VMware Disposable Desktops.

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 vCenter Server.
   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
      ```

What to do next: If you were in the process of install Pano Direct Service, return to VMware Disposable Desktops.

Related Topics

Restrict or Allow Use of Specific USB Devices

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 Pano System Endpoints.

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

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.

What to do next: (Optional) Restrict or Allow Use of Specific USB Devices.

Restrict or Allow Use of Specific USB Devices

In general, the decision to 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.

Some companies have departments that work with highly sensitive data (for example, social security numbers), and this data cannot leave the premises. In these types of workplaces, restrict the use of specific USB devices in order to help protect against that data being copied to USB devices.

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 a DVM through a Pano System Endpoint, 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\PanoDirect`.

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 **PanoDirect** folder, 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 Direct Service or reboot your DVM.

Force Users To Log Off

Out of habit, it's not uncommon for an end user to:

- Lock shared Windows desktops
- Disconnect from shared Windows desktops
- Press the Pano button before stepping away from a shared Windows desktop

For all collections, these actions represent disconnects and don't terminate the user's session. Only after the session terminates can other users use the DVM.

In a Pooled Desktops collection type, for example, users must log off in order for the DVM to return to the pool. If, instead, the user presses the Pano Button, for example, when the next user tries to use the DVM, the user cannot log on to that DVM because it has not been returned to the pool, and that’s not good for workplace productivity. Pano Logic has a solution for you, and this solution can apply to any collection.

To force users to log off:

This procedure does exactly what’s outlined in Control Session Timeouts, except that you don’t need to edit the registry manually. The executable outlined in this procedure does it all for you.

Perform the following steps on each DVM, or just one DVM if you are using that DVM as your template.

1. From a Windows prompt, go to the BIN directory:

```
> cd C:\Program Files\Pano Logic\PanoDirect\BIN\
```

2. Run the `panodirectcfg.exe` file with the `DisconnectedTimeout` option set to `2`.

```
> panodirectcfg.exe -DisconnectedTimeout 2
```

3. Reboot the Windows virtual machine.

When the user disconnects, 2 seconds later this script logs off the user and makes the Pano System Endpoint available for the next user automatically.

Related Topics

Log Off from DVMs as Administrator

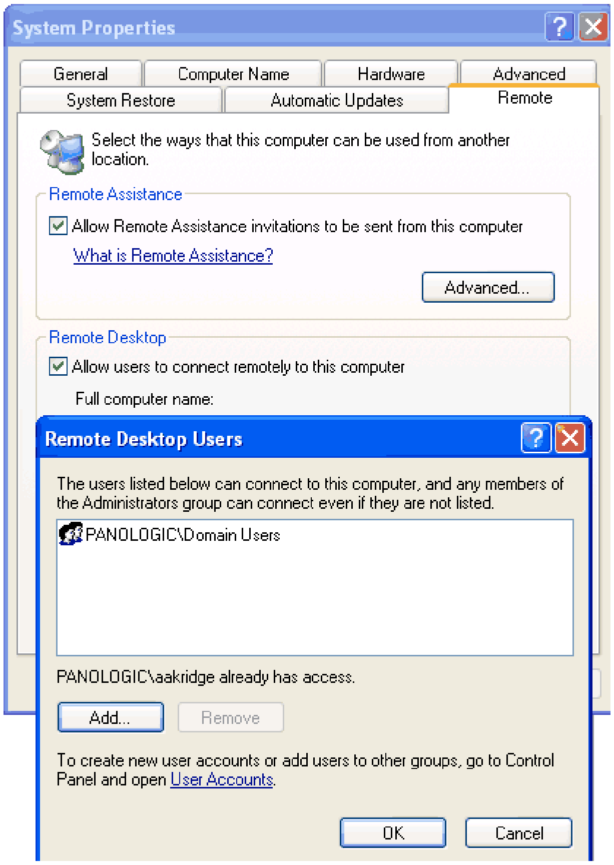
Enable Remote Desktop & Set RDP Users

Pano Direct does not rely on RDP; you don’t have to set a Remote Desktop Users group. If you want users to be able to connect via Windows RDC and the Pano web access:

- Make sure that the desktop virtual machine is enabled for Remote Desktop.
- Add user(s) of the DVM to the Remote Desktop Users Group for that DVM.

The Pano Direct Service installer automatically does this for you during a Pano Direct Service installation or upgrade. If users trying to connect to the DVM have Administrator access, they are able to RDP to the DVM by default. However, if you want to enable users who do not have Administrator access, or for some reason RDP isn't enabled, use the following procedure:

1. Log on to the desktop virtual machine.
2. Right-click on **My Computer**; 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.
7. Click **OK** to close the Remote Desktop Users dialog, click **Apply**, then **OK**.



Select the ways that this computer can be used from another location.

Remote Assistance

☑ Allow Remote Assistance invitations to be sent from this computer

What is Remote Assistance?

Remote Desktop

☑ Allow users to connect remotely to this computer

Full computer name:

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

PANOLOGIC\Domain Users

PANOLOGIC\aakridge already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

44

Create and Manage DVM Collections–VMware & Hyper-V

This section provides information on creating collections of DVM for users of VMware or Hyper-V. We’ve created a short video to help you understand Collections: Understanding DVM Collection Types

Additional administrative functions can be found in:

- Pano Controller Administration
- Setting Up DHCP
- DVM Administration
- Optimize DVM Performance
- Endpoint Administration
- Define USB Peripheral Support
- Create and Manage DVM Collections–Xen

This chapter includes the following topics:

- Choose DVM Collection Type
- Create DVM Collections
- Assign Pano Zero Clients and Users To DVMs
- User Membership Rules
- Manually Assign Users in User Based Collections
- Manually Assign Pano Zero Client in Device-Based Collections
- Deploy Resources
- Log Messages for Resource Deployment
- Use Cases for Device Restrictions
- Set Up Collections with Device Restrictions
- Update DVM Collections
- Delete DVM Collections
- Create Virtualization Hierarchy–VMware
- Configure for Concurrent Deployment and Power Operations

Before You Begin: Create Desktop Virtual Machines in vSphere Client

After you prepare for automated provisioning, you’re ready to create your DVM Collections.

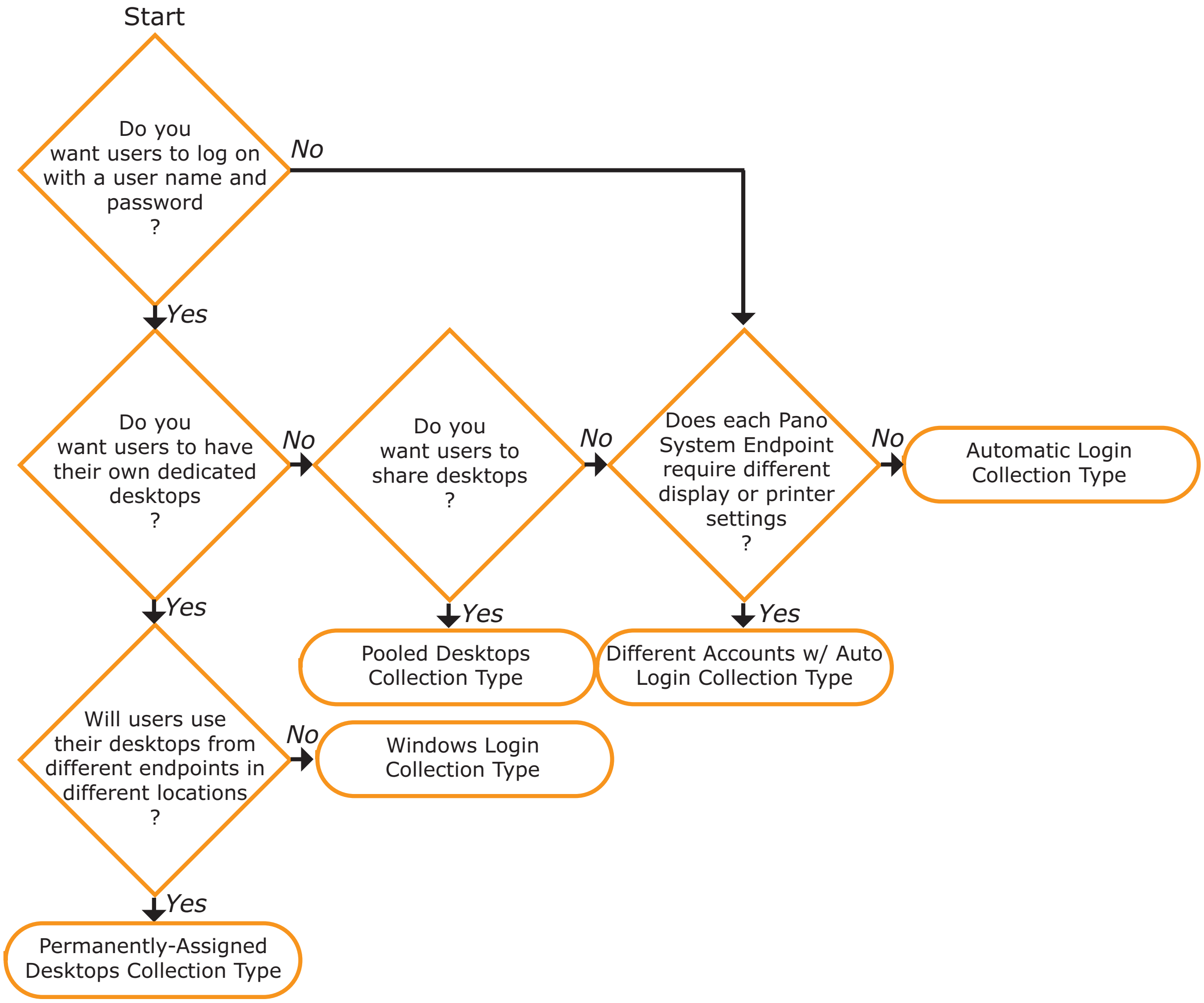
Task	Go to...
Create Security groups in AD that represent the set of users of the desktop virtual machines. You specify these Security groups when you create the DVM Collections.	Create a New Group
Determine types of DVM Collections needed.	Choose DVM Collection Type
(vSphere only) Create a folder structure to help you organize your DVMs.	Create Virtualization Hierarchy–VMware
Determine if you need device restrictions. You can add these restrictions after you create the DVM Collection.	Use Cases for Device Restrictions

Task	Go to...
Create the DVM Collection	Create DVM Collections
Assign Pano System Endpoints to DVMs	Assign Pano Zero Clients and Users To DVMs
Verify that the DVM Collection is working properly.	Verify DVMs & System Deployment
Set up the DVM Collection with device restrictions, if you didn't do so when you created the DVM Collection.	Set Up Collections with Device Restrictions

Choose DVM Collection Type

Use one of the following tools to determine which collection type(s) to choose:

- **Collection Type Flowchart** - a simple series of questions to match the ideal collection type to your needs.


Start
Do you want users to log on with a user name and password ?
No
Yes
Do you want users to have their own dedicated desktops ?
No
Do you want users to share desktops ?
No
Does each Pano System Endpoint require different display or printer settings ?
No
Automatic Login Collection Type
Yes
Yes
Pooled Desktops Collection Type
Yes
Different Accounts w/ Auto Login Collection Type
Will users use their desktops from different endpoints in different locations ?
No
Windows Login Collection Type
Yes
Permanently-Assigned Desktops Collection Type

- **Collection Type Matrix** - a "deep dive" into the differences between all collection types.

	Primary Need	**Pooled Desktops**	**Permanently Assigned Desktops**	**Existing Desktops**	**Automatic Login**	**Different Accounts w/ Automatic Login**	**Windows Login**
End User needs	Use a SmartCard Reader for *OS authentication*.	No	No	No	No	No	Yes
	Use a SmartCard Reader for *application authentication*.	Yes	Yes	Yes	Yes	Yes	Yes
	Use dedicated virtual desktops.	No	Yes	Yes	No	No	No
	Roam from one device to another.[1]	Yes	Yes	Yes	No	No	No
	Log on to DVMs via a dedicated device (also known as a *kiosk*).	No	No	No	Yes	Yes	Yes
	Exact same login experience as a physical PC.[2]	No	No	No	No	No	Yes
Admin needs	Ensure user authentication.	Yes	Yes	Yes	No	No	Yes
	Preserve/minimize computing resources when only a subset of users need a virtual desktop at any given time.[3]		No	No	No	No	No
	Implement Windows roaming profiles and folder redirection to provide users desktop personalization.	Yes	Yes	Yes	No	No	Yes
	Manage identical kiosks.	No	No	No	Yes	No	No
	Manage kiosks with variations in user policies[4].	No	No	No	No	Yes	No
	Automatically deploy virtual desktops.	Yes	Yes	No	Yes	Yes	Yes

1. Roaming is allowed between non-kiosk Pano System Endpoints. If a Pano System Endpoint displays a Pano user login screen then it's not a kiosk.
2. Displays Windows Login screen, no Pano user login screen.
3. Ideal when users have work shifts. Users must also use the same set of software applications for this collection to be feasible.
4. Settings include printer settings for a kiosk that's designed to send print jobs to a specific printer, or display settings geared toward a kiosk that resides in a conference room with a projector. There is some initial overhead as you need to map each DVM to an account.

What to do next: For VMware deployments and based on the collections that you chose, create a hierarchy for them. Go to Create Virtualization Hierarchy–VMware. Otherwise, go to Create DVM Collections.

Related Topics

DVM Collections

User Based Collections

Device Based Collections

Create DVM Collections

Before You Begin: Do the following:

- Determine the DVM types that you want. Go to DVM Collections.
- Create a security group in Active Directory that represents the set of users of the desktop virtual machines for the collection that you intend to create. You will specify this security group when you create the DVM collection.

To create a DVM Collection:

1. Log on to the Pano Controller.
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 wizard launches.
4. In the **General** tab, define collection type, then click **Next**.
5. In the **Access** tab, provide access to DVM collection, then click **Next**.
6. In the **Deployment** tab, configure for DVM deployment, then click **Next**.
7. In the **DVMs** tab, add the desktops that you want to associate with this collection.
8. In the **Capacity** tab, configure extra desktops and power state, then click **Next**.
9. In the **User Control** tab, configure for user control of desktops, then click **Next**.
10. In the **Pano Remote** tab, set options for Pano Remote users, then click **Next**.
11. In the **Overview** tab, verify your selection, then click **Add DVM Collection**.
    - The Pano Controller starts cloning a DVM that belongs to this collection.:
    - After a few minutes, the new DVM appears in the table.

What to do next: Assign Pano Zero Clients and Users To DVMs

Related Topics

Create DVM Collections–XenDesktop

Define Collection Type–VMware and Hyper-V

From the **General** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, provide the following:

- **Type:**

  Choose among the different collection types.

- **Name:**

  Choose a short collection name that represents how you are going to use this collection. For example, if the DVMs in this collection will be used by the Marketing Department, name the folder `MarketingDept`. A user can have more than one DVM, but each must reside in a separate collection. If you intend to enable multi-DVM support, consider naming the collections `MarketingDeptXP`, `MarketingDeptWin7`, etc.

Related Topics

Define Collection Type–XenDesktop

Choose DVM Collection Type

Create DVM Collections

Create Virtualization Hierarchy–VMware

Provide Access To DVM Collection

You can control who can access the collection’s desktops and, optionally, configure auto-assignment to associate devices/users to DVMs. From the **Access** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, enable Auto-assignment of users or Pano devices to DVMs:

- **Auto-Assignment and Auto-Assignment Name**

  Auto-assignment saves you time by automatically assigning users/Pano System Endpoints to DVMs, though not all collections are eligible for this feature. To learn how to manually assign users Pano System Endpoints, go to Assign Pano Zero Clients and Users To DVMs. To learn about how long assignment lasts, go to About User Assignment or About Device Assignment.

DVM Collection	Auto-Assignment	Auto-Assignment Name
Automatic Login	Access is determined by assigning a Pano System Endpoint to a desktop virtual machine. The Pano Controller will automatically connect the specified Pano System Endpoint to the specified desktop virtual machine and log on to Windows using the credentials specified. After you add the collection you can create these assignments manually using the **Assign...** button on the DVMs tabs. Optionally, Auto-Assignment allows an administrator to set the assignment by logging on through the Pano System Endpoint.	n/a
Different Accounts w/ Automatic Login		
Windows Login	Allow administrators to set the assignment between a Pano System Endpoint and a desktop by logging on to a device using the Auto-Assignment name. Access is determine by assigning a Pano System Endpoint to a desktop virtual machine so that Windows can handle user authentication directly. After you add the collection you can create these assignments manually using the **Assign...** button on the DVMs tabs. Optionally, Auto-Assignment allows you to set the assignment by logging on through the Pano System Endpoint.	Type a name to be used to automatically assign a Pano System Endpoint to the desktop. The name is a character string that is used solely for establishing the assignment. The string should not match a Windows account name and should be unique to the DVM collection.
Pooled Desktops	n/a	n/a
Permanently Assigned Desktops	When a new user logs on to the collection they will be assigned an available desktop. The assignment persists until manually unassigned by the administrator.	n/a
Existing Desktops	n/a	n/a
VMware View	n/a Auto-Assignment must be done through the VMware View.	n/a

- **Account Type and Accounts**

  If applicable, click the browse button (…) to find the directory objects to which you want to give access to the DVM Collection.

DVM Collection	Account Type	Account(s)
Automatic Login	Choose one of the following: - Network account - Local account Choose local account if you want to use an account that is local to the desktop. Choose network account if you want to use a domain account.	Type or browse to the network account or local account for automatic login to the desktop. The credentials will not be checked until an automatic login is attempted, so check the Pano Controller log to aid troubleshooting. The account is required.
Different Accounts w/ Automatic Login	n/a	Type the accounts for automatic login to the desktop. The account is required. Specify the user group that contains the accounts to be used for automatic login. 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.
Windows Login	n/a	n/a
Pooled Desktops	n/a	Select the accounts that are entitled to access the desktops in the collection. Groups, and/or individual user accounts can be specified. The accounts are required.
Permanently Assigned Desktops		
Existing Desktops		
VMware View		

- **Password:**

DVM Collection	Password
Automatic Login	Type the account password for automatic login to the desktop. The credentials will not be checked until an automatic login is attempted, so check the Pano Controller log to aid troubleshooting. The account is required.
Different Accounts w/ Automatic Login	n/a
Windows Login	Type a password that will correspond to the Auto-Assignment Name. The password is required.
Pooled Desktops	n/a
Permanently Assigned Desktops	n/a
Existing Desktops	n/a

- **Device Restrictions**

DVM Collection	Device Restrictions
Automatic Login	If you want to restrict access to a specific set of Pano System Endpoints, type a string that matches the names of those Pano System Endpoints. For example, if you're a hospital and you want to restrict access to all Pano System Endpoints on the 1st floor, type `PanoFirstFloor*` as the string, then rename all such Pano System Endpoints that are physically installed on the 1st floor to something like `PanoFirstFloor01`, `PanoFirstFloor02`, `PanoFirstFloor03`, etc.
Different Accounts w/ Automatic Login	
Windows Login	
Pooled Desktops	
Permanently Assigned Desktops	
Existing Desktops	
VMware View	

- **Login Enabled**

DVM Collection	Login Enabled
Automatic Login	n/a
Different Accounts w/ Automatic Login	
Windows Login	
Pooled Desktops	When login is disabled users will not be allowed to log on from any Pano managed endpoint. This option does not restrict users from logging on from the console or Remote Desktop Connection endpoint.
Permanently Assigned Desktops	
Existing Desktops	
VMware View	

Provide Access To DVM Collection–XenDesktop

Choose DVM Collection Type

Create DVM Collections

Log On To DVMs as End User

Configure for DVM Deployment

From the **Deployment** tab of the Add Collection wizard or the Update Collection wizard, provide the following:

- **Deploy Enabled:**

  If you disable this option, the Pano Controller will not automatically deploy desktops, even if users need more desktops. You might want to disable deployment if you want to perform maintenance on the template or if your collection size is static.

- **Computer Name:**

  A pattern (naming convention) used to generate unique computer names for the DVMs that you deploy. The computer name is required. The computer name has no relationship to Pano System Endpoint names.

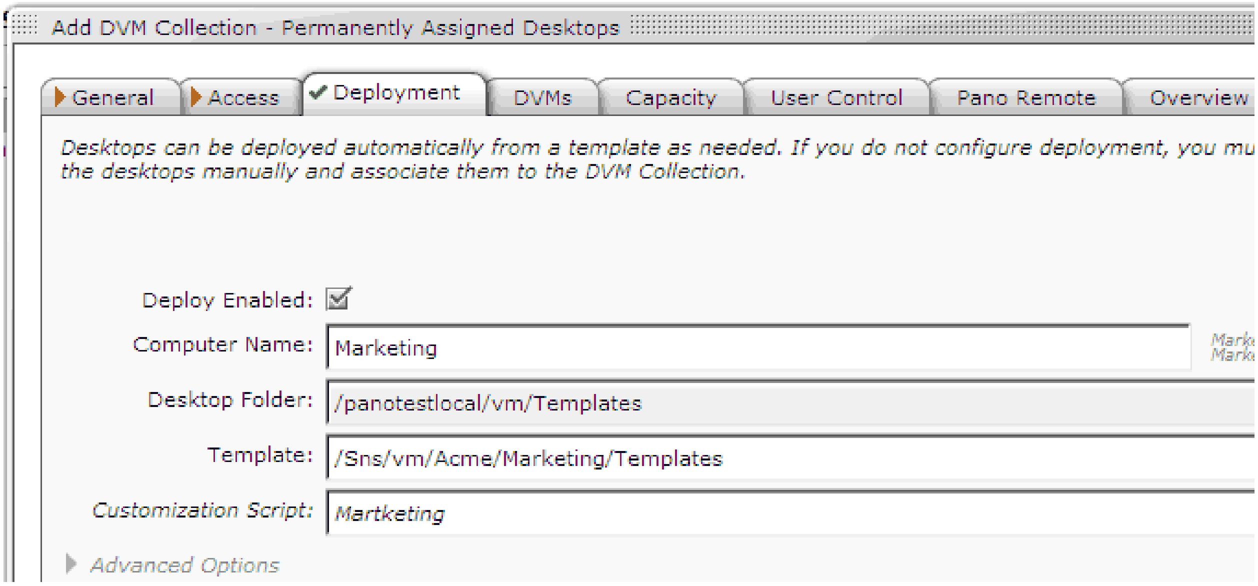
  The computer name pattern is always used to create both the virtual machine names (the names that display via the vSphere Client) and, because you configured the Customization Specification to **Use the virtual machine name** as required by Pano System, the Windows computer name (appears as DNS Name in the Pano Controller). After deployment, you can rename the virtual machine names via the vSphere Client, but there's no need to and it's not recommended if you use the Reuse Names option.

  The pattern comprises a description name and a system generated number. The full computer name is limited by the rules for Windows computer names and DNS names, mainly a maximum of 15 alphanumeric characters including an optional hyphen.

  Use curly braces ({}) to explicitly specify the location of the system generated number in the name: the system generated number can be a prefix or a suffix. In the curly braces, provide a one digit number to specify the maximum number of digits and leading zeros you want for your system generated numbers.

  If all system generated numbers (1 to 999 is one possible range in the following example) are used, deployment fails and an error message appears in the Pano Controller's log file. Use a range that takes into account the number of DVMs that the department might use. For most small departments, 99 is more than sufficient.

Type	Gets you...
{1}-Marketing	1-Marketing thru 9-Marketing
{2}-Marketing	1-Marketing thru 99-Marketing
{3}-Marketing	1-Marketing thru 999-Marketing
Marketing-{1}	Marketing-1 thru Marketing-9
Marketing-{2}	Marketing-1 thru Marketing-99
Marketing-{3}	Marketing-1 thru Marketing-999
Marketing-{01}	Marketing-1 thru Marketing-9
Marketing-{02}	Marketing-01 thru Marketing-99
Marketing-{03}	Marketing-001 thru Marketing-999



Desktops can be deployed automatically from a template as needed. If you do not configure deployment, you mu
the desktops manually and associate them to the DVM Collection.

Deploy Enabled: ☑

Computer Name: Marketing

Desktop Folder: /panotestlocal/vm/Templates

Template: /Sns/vm/Acme/Marketing/Templates

Customization Script: Martketing

- **Template:**

  Browse to find template in vCenter Server to be used to clone new DVMs for this collection. If you created your Virtualization Hierarchy out outlined in Create Virtualization Hierarchy–VMware, then choose among the templates in the `Templates` folder. A template is required. To create a template, go to Create DVM Templates in vSphere.

- **Customization Script:**

  Browse to find the DVM customization script you want to use to customize new DVMs for this collection.

- **Resource Pools:**

  Select a set of resource pools from which CPU and memory resources should be allocated for new DVMs.

- **Datastores:**

  Select a set of datastores on which you want to store the files for the desktop virtual machines.

- **Organizational Unit:**

  Specify an organizational unit (OU) for the new DVM. After the DVM has been cloned, the Pano Controller automatically moves the DVM's computer object within AD into the specified OU, thereby enabling you to apply group policies to the DVMs that are part of that OU.

- **Reuse Names:**

An opportune feature for a case where you have a gap in sequence of DVMs’ computer names that have been deployed. If you don’t currently have such a gap, consider keeping this option disabled. To remove this gap, go to Reuse DVM Names.

Related Topics

Automated Deployment Concepts

VMware Disposable Desktops

Add Desktops

From the **DVMs** tab of the Add DVM Collection wizard, or the Update DVM Collection wizard, provide the following:

1. Click on the **Add** button.
2. In the Select DVMs dialog, highlight (select) the desktops that you want to associate with this collection.

   You can choose any DVM, regardless of its location in the folder hierarchy as outlined in DVM Collections.
3. Click on the **Check Selection** button.

Configure Extra Desktops and Power State

From the **Access** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, provide the following:

- **Extra Desktops**

  Specify how many of the extra desktops should be kept powered on and ready instantly. Any remaining extra-or surplus-desktops will be powered off to conserve server resources. To avoid unnecessary operations, desktops will only be powered off after Pano Desktop Service has been responding for 2 minutes.

- **Extra to Keep On**

  Type 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.

- **Power Off the Surplus**

  Enable/disable powering off the surplus of extra desktops. When this item is selected, surplus desktops beyond the extras to keep on will be powered off.

  The Pano Controller has the ability to power DVMs on and off based on policies. By default, the Pano Controller enforces only the policies that turn DVMs on. If you want the Pano Controller to also enforce the policies that turn DVMs off, select the **Power Off the Surplus** option. When selected, the Pano Controller automatically powers off surplus DVMs that are not needed. The Pano Controller never powers off extras.

  DVMs can be configured for either of the following power management states:

  - **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 Controller 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 the Surplus** 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 to Keep On** and **Extra Desktops** 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 Controller. The power state of a DVM is controlled by the end user and/or by vCenter Server. The user of the DVM has the ability to control the power state of the DVM through the Pano Control Panel's Options screen and when logging on to the DVM via the Pano System Endpoint. 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 vCenter Server.
  - **Extra** - automatically managed based on the values specified in **Extra to Keep On** and **Extra Desktops** values.
- **For Existing Desktops collection type**

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

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

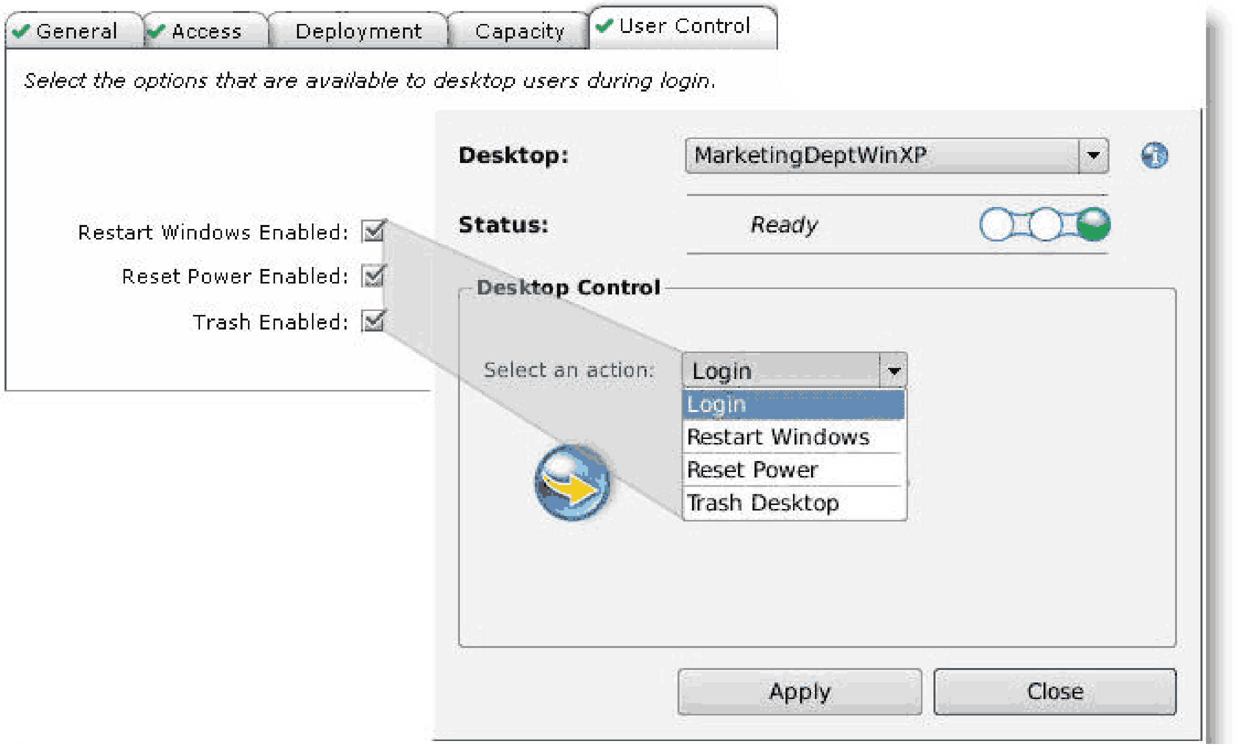
Related Topics

Automated Deployment Concepts

Configure for User Control of Desktops

Note: If you are using VMware ESXi, go to Limitations of Pano Controller without vCenter Server.

User control options provide end users control over their virtual desktops. These options are under administrator control and can be set on a collection-by-collection basis:



Select the options that are available to desktop users during login.

Restart Windows Enabled: ☑

Reset Power Enabled: ☑

Trash Enabled: ☑

Desktop: MarketingDeptWinXP

Status: *Ready*

Select an action: Login

From the **User Control** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, provide the following:

- **Restart Windows Enabled**

  When selected, users are able to log on to their DVMs and, if necessary, restart their DVMs' operating systems. By default, these operations are enabled.

- **Reset Power Enabled**

  When selected, users are able to reset their DVMs.

- **Trash Enabled**

  When selected, users with permanently assigned desktops are able to "trash" their DVMs in order to be assigned a new, working DVM. This feature is only applicable to a Permanently Assigned Desktops collection type.

Related Topics

Move DVMs to Trash

Delete DVMs from Disk

Set Access Options for Pano Remote Users

From the **Pano Remote** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, provide the following:

- **Allow external access**

  External access refers to a connection via the WAN.

- **Allow internal access**

  Internal access refers to a connection via the LAN.

- **Redirect clipboard**

  It's a best practice to enable users to copy paste between the local desktop and the DVM by enabling a shared clipboard between the local Windows system and the remote DVM. For this reason, this option is enabled by default.

- **Redirect printer**

  Your users might want to print to their local printer. If you enable printer redirection, users' local printer appear in the list of printers attached to the DVM. However, the DVM must have the printer driver for the local printer installed on the DVM.

- **Redirect drives**

  For security reasons, you might not want local drives accessible from the DVM. For this reason, this option is disabled by default.

- **Color quality**

  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.

  From the Pano Control Panel, your users can set color quality as outlined in Configure DVMs for 24-bit Color.

Related Topics

Set Access Options for Pano Remote Users–XenDesktop

Assign Pano Zero Clients and Users To DVMs

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

- Manually 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 Controller. Such DVMs should be assigned to users through the VMware View product.
- Manually assign Pano devices to DVMs – DVMs that belong to Device-Based Collections (for example, an Automatic Login collection type) must be assigned to Pano System Endpoints. After assignment, a lock appears in the **DVMs** tab next to the Pano System Endpoints.

To ensure assignment, you must do one of the following, keeping in mind that Auto-Assignment overrides manual assignment.

- Manually assign users to DVMs or manually assign Pano devices to DVMs – after you create the collection.
- Enable Auto-Assignment – at the time that you create the collection (refer to Provide Access To DVM Collection). Auto-assignment saves you time. You don't need to manually assign one user or Pano System Endpoint at a time. With a Permanently Assigned Desktops, you would most likely want to enable Auto-Assignment; for this reason, this feature is enabled by default. Some collections (Pooled Desktops and Existing Desktops) don't have the concept of assignment and so aren't eligible for Auto-Assignment.
    - **For User Based Collections**: When a user with membership to a collection logs on to the Pano System, the Pano Controller 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 Controller creates a new DVM and auto-assigns it to the user.
    - **For Device-Based Collections**: To auto-assign a Pano System Endpoint to a DVM, log on to the Pano System. With the account specified in the Device-Based Collection, the Pano Controller auto-assigns the Pano System Endpoint to an available DVM. If no DVMs are available and the collection is configured for deployment, the Pano Controller creates a new DVM and auto-assigns it to the Pano System Endpoint.

Collection	Assignment	Auto-Assignment Default
Device-Based Collection		
Automatic Login	Yes	Off
Different Accounts w/ Automatic Login	Yes	Off
Windows Login	Yes	Off
User Based Collection		
Pooled Desktops	No	n/a
Permanently Assigned Desktops	Yes	On
Existing Desktops	No	n/a

Related Topics

Assign Pano Zero Clients and Users To DVMs–XenDesktop

View Users' DVM Login Status and DVM Assignment

Manually Assign Users in User Based Collections

Manually Assign Pano Zero Client in Device-Based Collections

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 User Based Collection. The Pano Controller 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 View

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

Manually Assign Users in User Based Collections

Manual assignment is an alternative to Auto-Assignment. Auto-Assignment overrides manual assignment. 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.

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

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

Troubleshooting: If you receive a `not entitled to access the desktop collection` error message, you attempted to assign the DVM to a user that is not a member of the group that is defined in the collection.

What to do next: Deploy Resources

Related Topics

Manually Assign Users To DVMs in User Based Collections–XenDesktop

User Membership Rules

Choose DVM Collection Type

Manually Assign Pano Zero Client in Device-Based Collections

Unassign Users from DVMs

Determine Pano Direct Service Version

Manually Assign Pano Zero Client in Device-Based Collections

Manual assignment is an alternative to Auto-Assignment. Auto-Assignment overrides manual assignment.

1. Log on to the Pano Controller.
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 System Endpoint from the list
5. For Different Accounts w/ Automatic Login, do the following:
   a. In the Pano Zero Client field, select the Pano System Endpoint.
   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 System Endpoint from the list.
6. Click **OK**.

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

What to do next: Deploy Resources

Related Topics

Assign Pano Zero Clients and Users To DVMs

Manually Assign Pano Zero Client in Device-Based Collections

Deploy Resources

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

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

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

vCenter Server 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 Controller chooses the largest datastore in the cluster. If that datastore is local to a single host, then Pano Controller 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 Controller keeps at least 512MB of memory free in a resource pool. This avoids problems with vCenter Server 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 Controller 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 Controller log, indicating the resources that should be checked for each resource pool. To retrieve these log messages, go to Work with Log Files.

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 System Endpoints; 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 System Endpoints.

The result is that a nurse who uses a Pano System Endpoint 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 third-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 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 System Endpoint using the credentials of the specified user. If you have set up 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

You aren’t required to use device restrictions. Device restrictions can be used to control how devices are associated with collections. For example you can set up collections, even of the same collection type, with different access properties for the same network and then control which devices associate with each collection. There are many use cases for device restrictions.

To implement device restrictions:

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

1. Rename your Pano devices so that they use a naming convention that represents how you intend to apply device restrictions.

   Example:

   If you want to restrict access to a specific set of Pano System Endpoints, type a string that matches the names of those Pano System Endpoints. For example, if you’re a hospital and you want to restrict access to all Pano System Endpoints on the 1st floor rename all such Pano System Endpoints that are physically installed on the 1st floor to something like `PanoFirstFloor01`, `PanoFirstFloor02`, `PanoFirstFloor03`, etc.

2. As you create the collection or update the collection, specify your naming convention as a search string in the **Device Restrictions** field. Continuing the same example, Type `PanoFirstFloor*` as the search string.

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

Update DVM Collections

To update a DVM Collection:

Before You Begin: Determine the DVM types that you want. Go to DVM Collections.

1. Log on to the Pano Controller.
2. Click the **DVM Collections** tab.
3. In the table, select the DVM Collection that you want to update, then click **Edit....**. The Update DVM Collection wizard launches.
4. In the **General** tab, define collection type, then click **Next** or **Update DVM Collection**.
5. In the **Access** tab, provide access to DVM collection, then click **Next** or **Update DVM Collection**.
6. In the **Deployment** tab, configure for DVM deployment, then click **Next** or **Update DVM Collection**.
7. In the **Capacity** tab, configure extra desktops and power state, then click **Next** or **Update DVM Collection**.
8. In the **User Control** tab, configure for user control of desktops, then click **Next** or **Update DVM Collection**.
9. In the **Pano Remote** tab, set options for Pano Remote users, then click **Next**.
10. In the **Overview** tab, verify your selection, then click **Update DVM Collection**.

Related Topics

Update DVM Collections–XenDesktop

Delete DVM Collections

Occasionally, you need to delete collections. Deleting a DVM Collection does not disturb users' sessions or delete the virtual machines from the virtualization platform. However, a best practice is to disable the logins for the collection, perform the desired operations on the desktops (for example, logout users or delete the desktops, then delete the collection.

To remove a DVM Collection:

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

Related Topics

Delete DVM Collections–XenDesktop

Create Virtualization Hierarchy–VMware

vCenter Server provides the Virtual Machines & Templates view to help you organize and manage virtual machines using folders.

DVM Collections rely on this folder organization. Pano System requires a separate folder for each collection type that you intend to use. The Pano Controller prevents collections from sharing the same folder. When you configure a DVM Collection, you specify a folder that contains the virtual machines. The Pano Controller manages all virtual machines that reside in the specified folder.

If you are using ESX host *without* vCenter Server you cannot create folders, as outlined in Choose Your VMware Virtualization Infrastructure. All DVMs are saved at the root level. Therefore, you can only create one DVM Collection, and the Pano Controller manages all the virtual machines at the root level and that you specify for that single DVM Collection.

To create a virtualization hierarchy folder using the Pano Controller:

Although you can create the folders through the vSphere Client, you can also do so from the Pano Controller. However, if you want to rearrange your folders, you must do so from the vSphere Client.

1. Log on to the Pano Controller.
2. Click the **Setup** tab.
3. Expand the Virtualization Configuration section, then click **Browse**. The Browse Virtualization dialog launches.
4. In the Browse tab, click **edit** > **New Folder...**.
5. Type a folder name, then click **Create Folder**.

What to do next: Assign Pano Zero Clients and Users To DVMs

To organize DVMs and templates:

The following example illustrates a best practice.

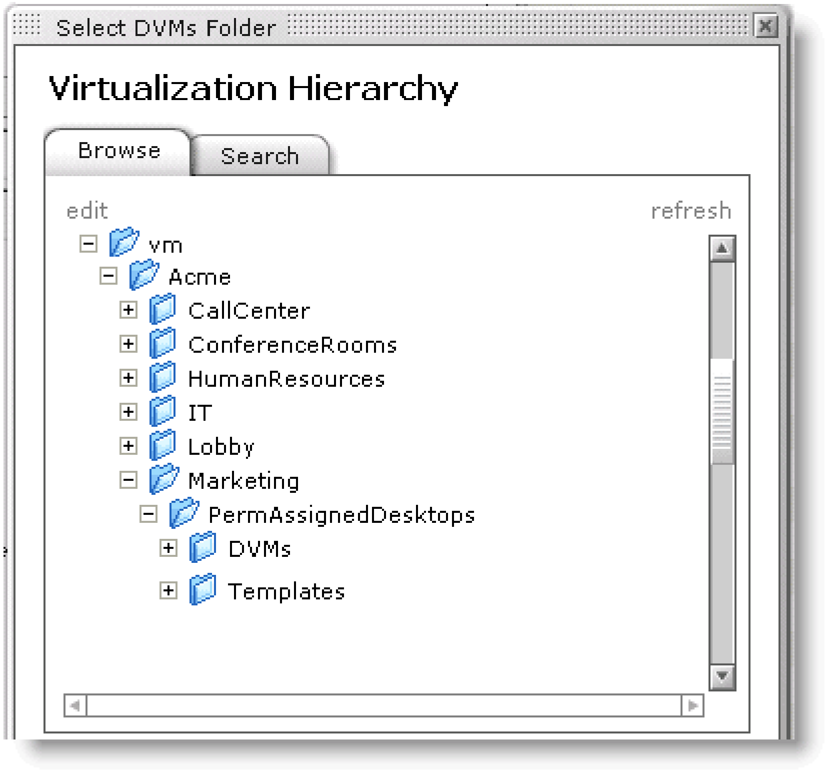
1. Launch your vSphere Client and connect to your ESX/ESXi host.
2. From the Virtual Machines & Templates view, right-click on the data center where you want to create your folder hierarchy or alternately select the data center and type Ctrl+F to create the base folder for your folder structure.

1. Log on to the Pano Controller.
2. Click the **DVM Collections** tab.
3. Click **Add**. The **Add DVM Collection** wizard launches.

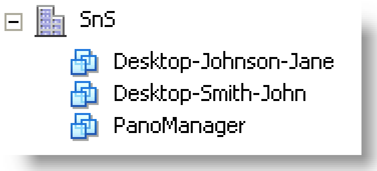
- Create a base folder. You can name the first of these folders Pano Logic or whatever name is logical for your company. Sometimes there is a preference to name them by department, for instance Accounting, Engineering, and so on. In addition, if you want DVMs in your conference rooms or lobby, you can create folders to contains these DVMs.
- Create a top level folder with the same name as the DVM Collection.

- 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.
- 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.

Folder structure in ESX/ESXi with vCenter Server



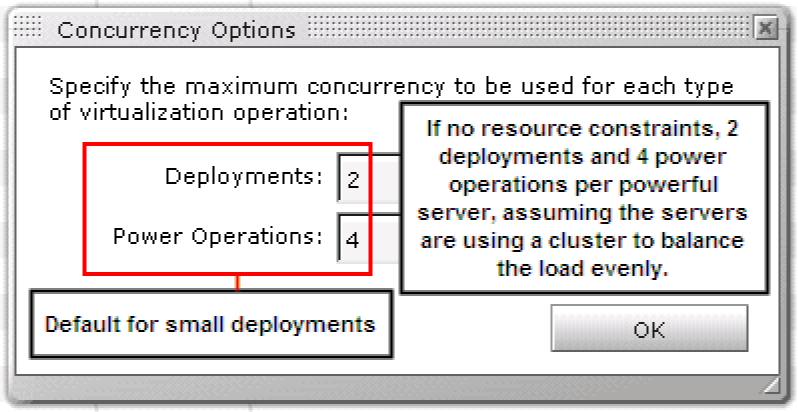
Folder structure in ESX host without vCenter Server



Configure for Concurrent Deployment and Power Operations

If you have a large deployment with surplus computing resources (cpu, memory, disk, network bandwidth, etc), you can improve how quickly DVMs deploy and power on by increasing the number of concurrent deployment and power operations that are allowed simultaneously.

By default, the Pano Controller assumes that you have a small deployment and so the Pano Controller is configured to push a modest number of concurrent operations to vCenter Server:



Specify the maximum concurrency to be used for each type of virtualization operation:

Deployments: 2

Power Operations: 4

If no resource constraints, 2 deployments and 4 power operations per powerful server, assuming the servers are using a cluster to balance the load evenly.

Default for small deployments

However, you can increase the number of operations to match your resource capacity thereby improving automatic deployment performance. Do not change the default values unless you have a large number of fast servers with desktops being deployed or powered on/off. If you increase concurrent operations to the point of stressing your computing resources, you will actually increase the time it takes to deploy and power on/off virtual desktops.

If you do not have resource constraints, consider increasing concurrent operations (a rule of thumb is 2 deployments and 4 power operations per powerful server, assuming the servers are using a cluster to balance the load evenly) under the following conditions:

- Increase concurrent deployments when deploying a large number of desktops. After deployment, return to default settings.
- Increase concurrent power operations if you have many virtual desktops that might power on/off simultaneously. For example, you have a Pooled Desktops collection type with power off enabled for workers that tend to log on/off around the same time.

To modify maximum number of concurrent operations:

1. Log on to the Pano Controller.
2. Click the **DVM Collections** tab.
3. In the Setting drop-down list, choose **Concurrency Operations**, then click **OK**.

   Specify the maximum number of concurrent operations for the following operations:
   - **Deployments** - maximum number of VMs that can deploy simultaneously.
   - **Power Operations** - maximum number of DVMs that can power on, power off, shut down, reset, and restart simultaneously.

45 Create and Manage DVM Collections–Xen

This section provides information on creating collections of DVM for users of Xen. Additional administrative functions can be found in:

- Pano Controller Administration
- Setting Up DHCP
- DVM Administration
- Optimize DVM Performance
- Endpoint Administration
- Define USB Peripheral Support
- Create and Manage DVM Collections–VMware & Hyper-V

Xen offers two ways to create and manage DVM Collections, using either XenServer or XenDesktop.

- Create DVM Collections–XenServer explains how to create DVM collections when you are using XenServer hypervisor
- Create DVM Collections–XenDesktop lets you create collections under XenDesktop for any supported virtualization platform.
- Assign Pano Zero Clients and Users To DVMs–XenDesktop
- User Membership Rules–XenDesktop
- Manually Assign Users To DVMs in User Based Collections–XenDesktop
- Use Cases for Device Restrictions–XenDesktop
- Update DVM Collections–XenDesktop
- Delete DVM Collections–XenDesktop
- Set Up Collections with Device Restrictions–XenDesktop

Create DVM Collections–XenServer

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

Task	Go to...
Create Security groups in AD that represent the set of users of the desktop virtual machines. You specify these Security groups when you create the DVM Collections.	Create a New Group
Determine if you need device restrictions. You can add these restrictions after you create the DVM Collection.	Use Cases for Device Restrictions–XenDesktop
Create the DVM Collection	Create DVM Collections–XenDesktop
Assign Pano System Endpoints to DVMs	Assign Pano Zero Clients and Users To DVMs–XenDesktop
Set up the DVM Collection with device restrictions, if you didn't do so when you created the DVM Collection.	Set Up Collections with Device Restrictions–XenDesktop

Create DVM Collections–XenDesktop

Before You Begin: Do the following:

Create a security group in Active Directory that represents the set of users of the desktop virtual machines for the collection that you intend to create. You will specify this security group when you create the DVM collection.

1. Log on to the Pano Controller.
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 wizard launches.
4. In the **General** tab, define collection type, then click **Next**.
5. In the **Access** tab, provide access to DVM collection, then click **Next**.
6. In the **Pano Remote** tab, set options for Pano Remote users, then click **Next**.
7. In the **Overview** tab, verify your selection, then click **Add DVM Collection**.
   - The Pano Controller starts cloning a DVM that belongs to this collection.:
   - After a few minutes, the new DVM appears in the table.

What to do next: Assign Pano Zero Clients and Users To DVMs–XenDesktop

Define Collection Type–XenDesktop

From the **General** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, provide the following:

- **Type:**

  For XenDesktop, the wizard chooses the Citrix XenDesktop collection by default. Via this collection, the following three types of Desktop Groups (which are equivalent to Collections in the Pano Controller) are supported:

  - Pre-Assigned Desktop Group
  - First-Use Assigned Desktop Group
  - Pool Desktop Group

- **Name:**

  Choose a short collection name that represents how you are going to use this collection. For example, if the DVMs in this collection will be used by the Marketing Department, name the folder `MarketingDept`. A user can have more than one DVM, but each must reside in a separate collection. If you intend to enable multi-DVM support, consider naming the collections `MarketingDeptXP`, `MarketingDeptWin7`, etc.

Related Topics

Create DVM Collections–XenDesktop

Provide Access To DVM Collection–XenDesktop

You can control who can access the collection’s desktops and, optionally, configure auto-assignment to associate users to DVMs.

Specify the accounts which are to have access to the DVMs. The simplest approach is to specify a security group that includes all domain users. Even though all users would be entitled within the Pano Controller, the user entitlements defined in XenDesktop will still be used to implement more specific user-to-desktop mappings. Thus, if an account is entitled in Pano Controller but not in XenDesktop, the user will be prevented from connecting.

From the **Access** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, enable Auto-assignment of users or Pano devices to DVMs:

- **Accounts**

  If applicable, click the browse button (…) to find the directory objects to which you want to give access to the DVM Collection. Select the **enable multiple selection** checkbox to choose more than one object.

- **Device Restrictions**

  If you want to restrict access to a specific set of Pano System Endpoints, type a string that matches the names of those Pano System Endpoints. For example, if you're working in a hospital and you want to restrict access to all Pano System Endpoints on the 1st floor, type `PanoFirstFloor*` as the string, and then rename all such Pano System Endpoints that are physically installed on the 1st floor to something like `PanoFirstFloor01`, `PanoFirstFloor02`, `PanoFirstFloor03`, etc.

- **Login Enabled**

  When login is disabled, users will not be allowed to log on from any Pano managed client. This option does not restrict users from logging on from the console or Remote Desktop Connection client.

Related Topics

Create DVM Collections–XenDesktop

Log On To DVMs as End User

Set Access Options for Pano Remote Users–XenDesktop

The use of Pano Remote™ is supported when using XenDesktop with the same functionality as on other virtualization platforms (except as noted under Limitations of XenDesktop). From the **Pano Remote** tab of the Add DVM Collection wizard or the Update DVM Collection wizard, provide the following:

- **Allow external access.** External access refers to a connection via the WAN.
- **Allow internal access.** Internal access refers to a connection via the LAN.
- **Redirect clipboard**. It's a best practice to enable users to copy and paste between the local desktop and the DVM by enabling a shared clipboard between the local Windows system and the remote DVM. For this reason, this option is enabled by default.
- **Redirect printer.** Your users might want to print to their local printer. If you enable printer redirection, the users' local printer appears in the list of printers attached to the DVM. However, the DVM must have the printer driver for the local printer installed on the DVM.
- **Redirect drives.** For security reasons, you might not want local drives accessible from the DVM. For this reason, this option is disabled by default.
- **Color quality.** 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. From the Pano Control Panel, your users can override the default setting that you set as outlined in Configure DVMs for 24-bit Color.

Make sure to add users to the “Direct RDP Access Administrators” group for each DVM. See http://support.citrix.com/article/CTX121657

Assign Pano Zero Clients and Users To DVMs–XenDesktop

With the Citrix XenDesktop collection type, which is a User Based Collection, DVMs must be assigned to users – after you create the collection. After assignment, a lock icon appears in the **DVMs** tab next to the username. Assignments to DVMs managed by XenDesktop cannot be made through the Pano Controller. Such DVMs should be assigned to users through the XenDesktop product.

Related Topics

View Users’ DVM Login Status and DVM Assignment

Manually Assign Users To DVMs in User Based Collections–XenDesktop

User Membership Rules–XenDesktop

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 User Based Collection. The Pano Controller provides the DVM from the 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 View

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

Manually Assign Users To DVMs in User Based Collections–XenDesktop

Manual assignment is an alternative to Auto-Assignment. Auto-Assignment overrides manual assignment.

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 customizations for that user ahead of time.

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

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

Troubleshooting: If you receive a `not entitled to access the desktop collection` error message, you attempted to assign the DVM to a user that is not a member of the group that is defined in the collection.

Related Topics

User Membership Rules–XenDesktop

Determine Pano Direct Service Version

Unassign Users from DVMs

Use Cases for Device Restrictions–XenDesktop

Device restrictions can be used with User Based Collections. Device restrictions for Device-Based Collections are not supported with the Citrix XenDesktop collection type. For more information, go to Limitations of XenDesktop.

- **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 a 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 System Endpoints; 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 System Endpoints.

The result is that a nurse who uses a Pano System Endpoint 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 third-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–XenDesktop outlines the steps to follow when setting up a User Based Collection with the device restrictions feature.

Update DVM Collections–XenDesktop

Before You Begin: Determine the DVM types that you want. Go to DVM Collections.

1. Log on to the Pano Controller.

2. Click the **DVM Collections** tab.
3. In the table, select the DVM Collection that you want to update, and then click **Edit....**. The Update DVM Collection wizard launches.
4. In the **General** tab, define collection type, and then click **Next** or **Update DVM Collection**.
5. In the **Access** tab, provide access to DVM collection, and then click **Next** or **Update DVM Collection**.
6. In the **Pano Remote** tab, set options for Pano Remote users, and then click **Next**.
7. In the **Overview** tab, verify your selection, and then click **Update DVM Collection**.

Delete DVM Collections–XenDesktop

Occasionally, you need to delete collections. Deleting a DVM Collection does not disturb users' sessions or delete the virtual machines from the virtualization platform. However, a best practice is to disable the logins for the collection, perform the desired operations on the desktops (for example, log out users or delete the desktops, and then delete the collection).

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

Set Up Collections with Device Restrictions–XenDesktop

You aren't required to use device restrictions. Device restrictions can be used to control how devices are associated with collections. For example you can set up collections, even of the same collection type, with different access properties for the same network and then control which devices associate with each collection. There are many use cases for device restrictions.

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

1. Rename your Pano devices so that they use a naming convention that represents how you intend to apply device restrictions.

   Example:

   If you want to restrict access to a specific set of Pano System Endpoints, type a string that matches the names of those Pano System Endpoints. For example, if you're working in a hospital and you want to restrict access to all Pano System Endpoints on the 1st floor, rename all the Pano System Endpoints that are physically installed on the 1st floor to something like `PanoFirstFloor01`, `PanoFirstFloor02`, `PanoFirstFloor03`, etc.
2. As you create the collection or update the collection, specify your naming convention as a search string in the **Device Restrictions** field. Continuing the same example, Type `PanoFirstFloor*` as the search string.

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

46
Troubleshooting

If your symptoms might be related to DVM performance, go to Optimize DVM Performance.

Troubleshoot Networking Problems

If the Pano Button is not turn blue (go to Pano Zero Client Light Indicators), the Pano user login screen will not display. Troubleshooting starts from the color of the Pano Button:

Symptom	What's it mean?	What do I do?
Solid red	Something is wrong with the Power connection on the Pano System Endpoint.	Connect another compatible power adapter to the Pano Zero Client. Verify that your USB devices are not drawing excess power: see What's the maximum power that a Pano System Endpoint can draw?. If these solutions fail, the Pano Zero Client may be defective. Call Pano Logic Technical Support.
Blinking red	There is no network plugged into a Pano System Endpoint, or the network cable is damaged or disconnected on the other end.	Try using another network cable to connect the Pano System Endpoint to the network.
Blinking orange	If the Pano Button does not turn Solid Orange after a minute, the Pano System Endpoint 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 that the server didn't have any more IP address in its range to assign. 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 System Endpoint to DHCP server. If that isn't the case, try another Pano System Endpoint—using the same network cable.
Solid orange	If the Pano Button does not turn solid blue after a minute, the Pano System Endpoint could not connect to Pano Controller or its Desktop Virtual Machine. The DHCP Server is not configured with the Vendor class to allow communication with Pano Controller.	Set up the Vendor Option in DHCP Server. Go to Set Up Pano Client Discovery Using DHCP.

Troubleshoot DVM Login Problems

- Normal Login Process
- DVM Login Error Messages

Normal Login Process

Once a Pano System Endpoint is connected to a Pano Controller, the Pano user login screen is displayed to the user. After the user enters the username and password and hits the Login button, the Pano Controller 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 Controller transfers the connection of the Pano System Endpoint to the Pano Direct Service running on the DVM.

There is a small interval of time between which the connection of the Pano System Endpoint to Pano software (Pano software refers to Pano Controller or Pano Direct Service) 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 Controller and the virtualization platform (for example, vCenter Server). If you're like many IT organizations, where one group manages the administration of virtualization platform and another group performs desktop management, you might not have access to the virtualization platform management tools to troubleshoot DVM login issues. That's okay! You can use the error messages that Pano Controller displays–without accessing the virtualization platform.

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

- **The desktop to which you are attempting to connect is running an incompatible version of Pano Direct Service. Please contact your system administrator.**

This message means that your end user logged in to the DVM from a Pano G2 Zero Client and the DVM is not running a supported version of Pano Direct Service for that model. Make sure that you're running Pano Direct Service v4.0 at minimum.

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

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

Note: In XenDesktop, this error might be due to a Citrix NetScaler misconfiguration. Go to Configure NetScaler to Monitor XenDesktop Controllers).

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 Controller by modifying the settings of the DVM collection, or in vCenter Server. 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) in the DVMs in the collection using a 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 System Endpoint 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 the Pano user 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 Controller` 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 Controller is in the process of contacting the user's DVM. This can take some time. After a few seconds the Pano Controller 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 the Active Directory server is lost. Refresh the configuration. Log on to Pano Controller. Then, in the Directory Configuration area, click the Setup tab, then click **Configure**. If it does not connect, there is a problem with connectivity between Pano Controller and Active Directory.

Troubleshoot Monitor, Mouse, and Keyboard Problems

Generally, we support and have certified most USB device classes (go to Support for USB Devices) with the Pano System Endpoint. Here are some troubleshooting steps related to computer peripherals:

Symptom	What do I do?
• The screen is black or 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	The monitor 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 System Endpoint. • Hook up monitor to another PC or laptop. • Do one of the following: • For global change, Go to Pano Controller 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 DVM Log Files.
• 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 the color quality is an odd number (for example, `15`) 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?
• 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. To install tools, refer to Install Windows. • Verify that the Pano Direct Service is installed. If the Pano Logic icon appears in your task bar (**Start** > **Programs** > **PanoDirect** > **Pano Control Panel**), then the Pano Direct Service is installed. The Pano Control Panel works in coordination with the VMware Tools and the Pano Direct Service on your DVM to further configure and accelerate your keyboard input response. If not installed, go to VMware Disposable Desktops. • Change the Repeat rate keyboard setting. Go to Set Keyboard Settings for Specific DVMs. • If those solutions don't work, then collect the log files. Go to Download DVM Log Files.

Troubleshoot USB Device 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.
- 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 System Endpoint will not allow the connection. The user should try to connect the USB device to the Pano System Endpoint via a powered USB hub.
- Sometimes the Pano System Endpoint 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 System Endpoint.

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.

- **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 System Endpoint from communicating with the Pano Direct Service running on every DVM. Go to Configure DVM Firewall. 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 3389.

- **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.

- **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 Service 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.

- **Host cannot be found**

If the URL that you specified in the Pano Controller is the hostname, trying using the IP address instead. If you can ping the IP address, but not the hostname, then you have a DNS problem. This might seem obvious to you, but it's easy to overlook the simple stuff.

- **No Global Catalog**

If the dialog box is empty (you cannot browse), but a red error message does not appear, the Pano Controller 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.yourdomain.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 Controller 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 Controller 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. Type 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 Controller 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 System Endpoint 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 Controller via the log file (go to Work with Log Files):

- supportedLDAPVersion
- namingContexts
- defaultNamingContext
- configurationNamingContext
- supportedCapabilities
- supportedControl

Troubleshoot Communication Problems with vCenter Server

- If you click **Configure** and get a Java exception error, then do the following:
  - Check that the URL of vCenter Server 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 vCenter Server as well as customization scripts and other objects. This user should be able to login to vCenter Server from the vSphere Client.
- If you are unable to connect to vCenter Server, try using the admin user of vCenter Server and check if Pano Controller can connect to vCenter Server. If Pano Controller can connect to vCenter Server 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 vCenter Server. Then, stop the vCenter Serverservices and restart. Log out of Pano Controller, then log on again and try to connect again.

Troubleshoot GINA Install and Uninstall Problems

To troubleshoot issues during installation, you can enable MSI logging. All GINA chaining steps are logged to an MSI log file during an install/uninstall.

To enable MSI logging during install, run the following command:

```
msiexec /i PanoDirect.msi /l*vx Test1.log
```

To enable MSI logging during uninstall, run the following command:

```
msiexec /x PanoDirect.msi /l*vx Test2.log
```

GINA Agent	GINA DLL Name	Registry Location (Chained)	GINA Chain Name	Registry Location (Prior GINA)	GINA Chain Name (Prior GINA)
VMware View Agent	wsgina.dll	`Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon`	NextGinaDLL	n/a	n/a
SplitView	SVGina.dll	`Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon`	SVNextGina	n/a	n/a
Imprivata	SGLaunch.dll	`Software\\SSOProvider\\SuperGina\\TargetGina`	GinaDllPath	`Software\\SSOProvider\\ISXAgent`	PriorGINA
Ensure Technologies XyLoc	EtGina01.dll	`Software\\Ensure Technologies\\Gina`	GinaDLL	n/a	n/a

Troubleshoot Backup Problems

If your Backup Configuration doesn't indicate `Connected`, click on the **Log** tab.

- If you see messages related to access, make sure that the user account has `Full Control`.
- If you see log messages related to the directory, make sure that the directory is a Windows share and that the directory exists.

```
...
BackupManager.DirectoryDoesNotExist=The backup share cannot be accessed: The
directory does not exist.
BackupManager.ShareIsNotDirectory=The backup share cannot be accessed: The share is
not a directory.
...
```

- If you see a log message related to an invalid backup, you might have a non-backup file (for example, a text file) in the directory. Don't save any other files to the backup directory. The Pano Controller reads all files in the backup directory.

```
...
BackupManager.InvalidBackupFile=Invalid backup file detected: {0}
...
```

- If you see a log message related to space, verify that the backup directory has enough disk space. Refer to About Backup Manager.

```
...
BackupManager.NotEnoughSpace=Not enough space available for backup. {0} bytes
needed.
...
```

- Other Messages:

```
BackupManager.DeleteLocalFailed=Cannot delete local copy of backup: {0}. Please
contact support.
```

```
BackupManager.ListLocalFilesFailed=Cannot list local backups. Please contact
support.
BackupManager.TransferFailed=Backup could not be transfered. Please check your
backup configuration and share location: {0}
BackupManager.InvalidCredentials=Invalid backup credentials. Please check your
backup configuration.
BackupManager.RemoveFailure=Backup could not be removed: {1}: {0}
BackupManager.InvalidChecksum=Backup could not be restored: invalid checksum: {0}
BackupManager.RestoreFailure=Backup could not be restored: {1}: {0}
```

Troubleshoot Pano Remote Problems

Any error code that begins with `0x03` is a Pano Gateway error. Otherwise, it’s a terminal services error.

The connection to your virtual desktop failed while communicating with the Terminal Services Gateway server. Please contact your administrator.

This error means that the `.exe` file was configured with the incorrect gateway. Reconfigure the file as outlined in Recommended: Add Server String to Executable.

A connection cannot be made because you are already connected to the computer.

This error means that the user is already logged on to the desktop. This usually occurs when a user inserts the Pano Remote USB into a Pano System Endpoint after having already logged on to the desktop from the Pano user login screen.

Pano Remote error code 0x1f4

This error occurs if the ASP .NET role service is not installed on IIS or if the application pool settings are configured for something other than the NETWORKSERVICE account. If you install and configure the TS gateway using the local machine administrator account, this error occur does not appear, assuming that ASP.NET role service is installed.

Pano Remote error code 0x204

An RDP connection to the DVM cannot be established. This usually occurs when RDP is disabled on the DVM.

Pano Remote error code 0x300006

The common name that you specified when you generated the certificate does not match the gateway server name.

Pano Remote error code 0x3000005

The common name that you specified when you generated the certificate does not match the gateway server name, or the SSL certificate is not installed on the machine that is using Pano Remote.

Pano Remote error code 0x3000016

Typically this message appears if a user tries to connect to a DVM that has remote desktop disabled (My Computer > Remote Tab > Allow users to connect remotely to this computer).

error code 0x300001c and 0x300000d

This error indicates that your `TS_CAP` and `TS_RAP` policies are not defined correctly in the Terminal Services Gateway. If an end user attempts to log on with account credentials that are not part of a user group that is defined in the `TS_CAP` and `TS_RAP` policies, the user receives this error.

For example:

Assuming `user2` is a user account defined in `panodemo\domain` users group on Win2K3 DC, this group must be included in the **TS_CAP Requirements** tab under **User Group Membership**. This group must also be defined in the **TS_RAP User Groups** tab.

If `panodemo\domain` users are not included in both `TS_CAP` and `TS_RAP` policies, when attempting to authenticate with `user2` credentials, the end user receives the error and cannot access the DVM, even if all other Pano Gateway configurations are correct.

For more information about how to configure `TS_CAP` and `TS_RAP` policies, refer to Microsoft's TS Gateway Step-by-Step Guide, choosing the scenario that represents your configuration:

- (Most Common) "Configuring the TS Gateway Core Scenario"
- "Configuring the TS Gateway NAP Scenario"
- "Configuring the TS Gateway ISA Server Scenario"

Troubleshooting Group Membership Problems

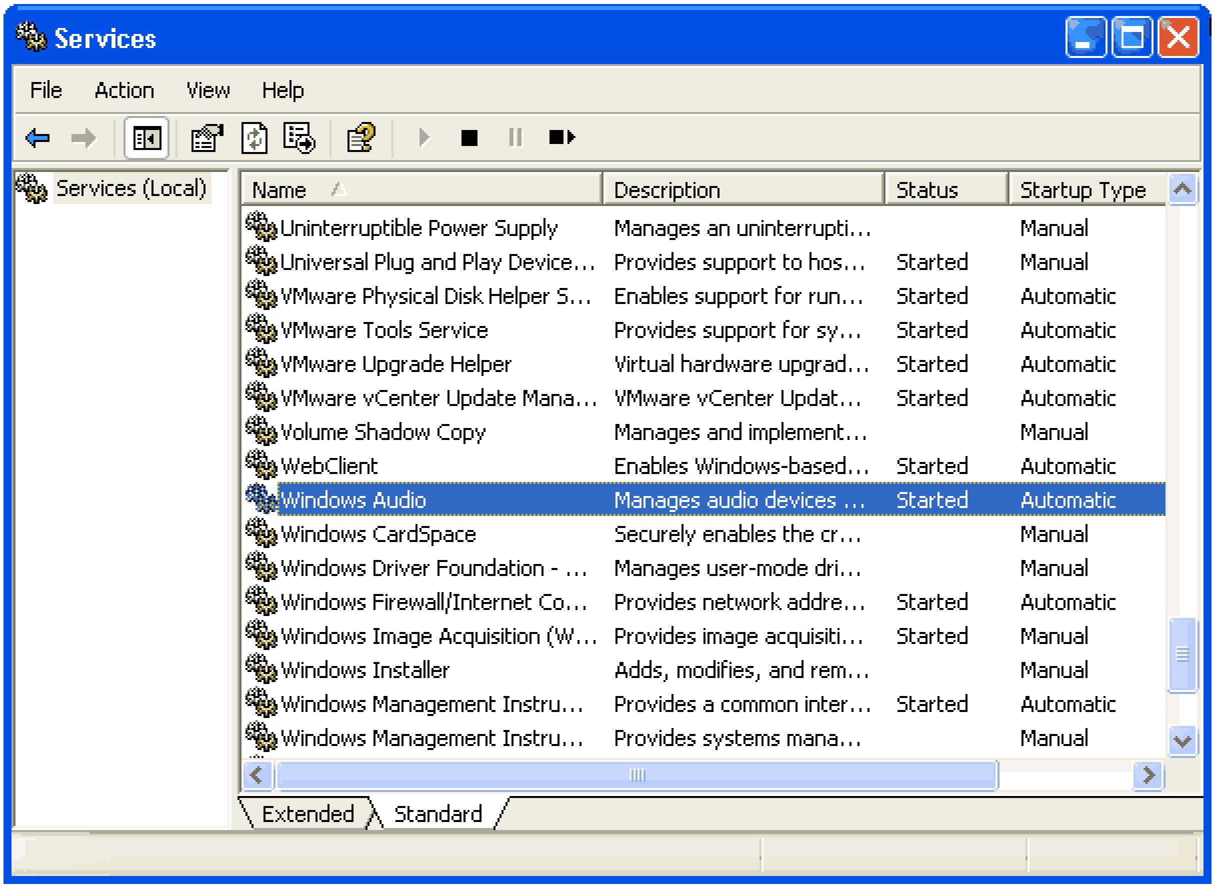
If one of the members does not appear in the list, ensure that:

- The Pano Controller is powered on.
- The Pano Controller is configured as part of the group.
- The members are configured with the same group name.
- The members are running the same Pano Controller version.

Windows XP Audio Problems

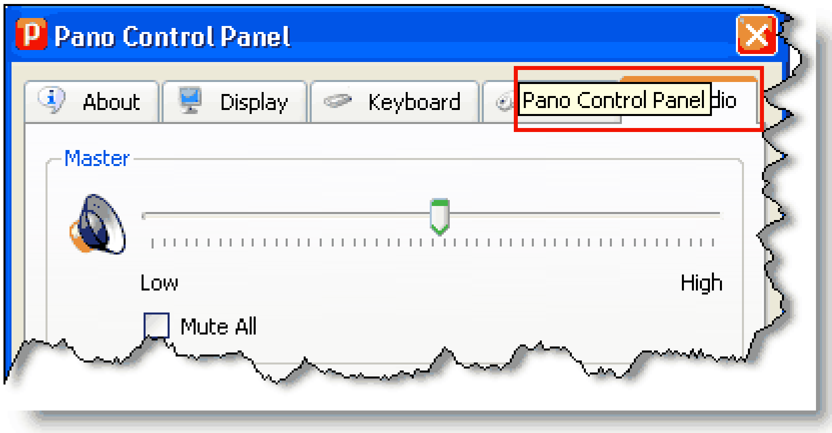
If there is no audio coming from the DVM, do the following:

- Ensure that the Windows Audio service is running. Go to Windows Control Panel > Administrative Tools > Services:

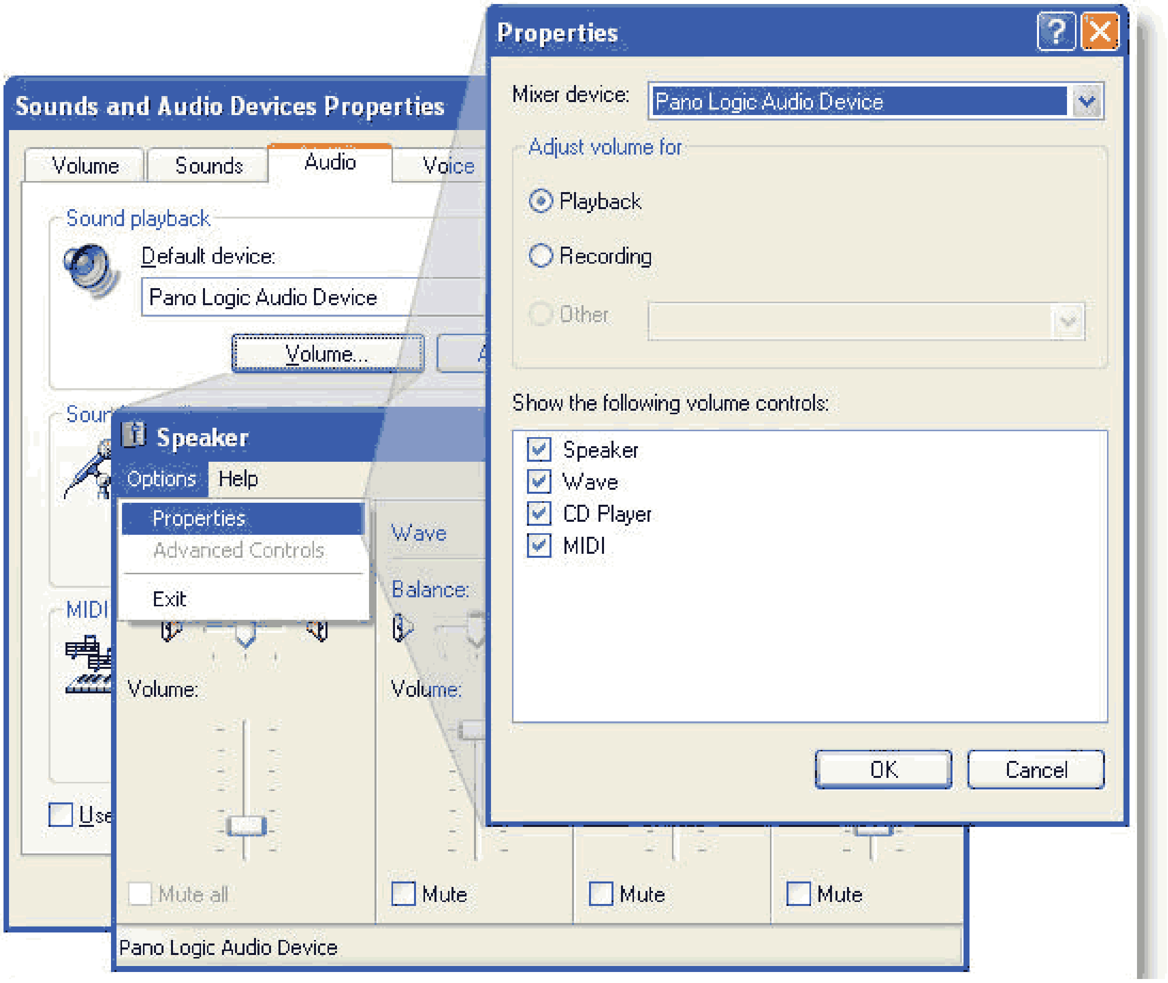


Name	Description	Status	Startup Type
Uninterruptible Power Supply	Manages an uninterrupti...		Manual
Universal Plug and Play Device...	Provides support to hos...	Started	Manual
VMware Physical Disk Helper S...	Enables support for run...	Started	Automatic
VMware Tools Service	Provides support for sy...	Started	Automatic
VMware Upgrade Helper	Virtual hardware upgrad...	Started	Automatic
VMware vCenter Update Mana...	VMware vCenter Updat...	Started	Automatic
Volume Shadow Copy	Manages and implement...		Manual
WebClient	Enables Windows-based...	Started	Automatic
Windows Audio	Manages audio devices ...	Started	Automatic
Windows CardSpace	Securely enables the cr...		Manual
Windows Driver Foundation - ...	Manages user-mode dri...		Manual
Windows Firewall/Internet Co...	Provides network addre...	Started	Automatic
Windows Image Acquisition (W...	Provides image acquisiti...	Started	Manual
Windows Installer	Adds, modifies, and rem...		Manual
Windows Management Instru...	Provides a common inter...	Started	Automatic
Windows Management Instru...	Provides systems mana...		Manual

- Verify that the Pano Control Panel indicates that the Pano Audio Device is configured:



- Ensure that the Pano Audio Device is the Mixer device (Control Panel > Audio tab > Options menu > Properties menu option). If the Pano Audio Device is your audio device, the volume control is grayed out.



Default device: Pano Logic Audio Device

Mixer device: Pano Logic Audio Device

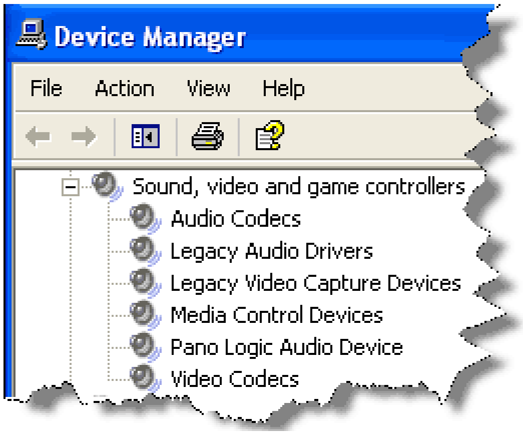
● Playback
○ Recording
○ Other

Show the following volume controls:

☑ Speaker
☑ Wave
☑ CD Player
☑ MIDI

Pano Logic Audio Device

- Verify that the Device Manager lists the Pano Audio Device:



Sound, video and game controllers
- Audio Codecs
- Legacy Audio Drivers
- Legacy Video Capture Devices
- Media Control Devices
- Pano Logic Audio Device
- Video Codecs

If Pano Controller group members are not able to see each other in the configured group, but respond to each other via ping and other direct communication, the issue may be related to jgroups and the Cisco Nexus 1000v switch. See Techstacks HOWTO: Troubleshoot JGroups and Multicast IP Issues for more information.

Work with Log Files

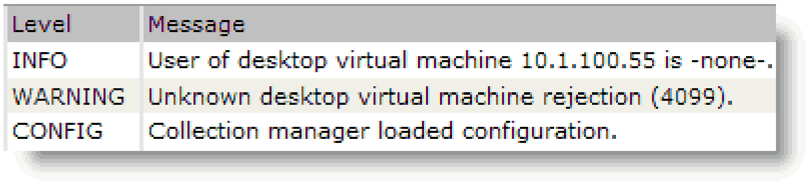
Pano Controller provides a list of system messages concerning the activity and performance of the Pano System. Pano Controller and Pano Direct Service both generate log files that can help you diagnose problems. Occasionally, when assisting you with a technical problem, Pano Logic Technical Support may ask that you send them these log files.

- Display and Filter Pano Controller’s System Messages
- Download Pano Controller Log Files
- Download DVM Log Files

Display and Filter Pano Controller’s System Messages

To display a Pano Controller’s system messages:

1. Log on to the Pano Controller.
2. Click on the **Log** tab.
3. Use the following information to determine the significance of the message.

<table>
<tr><th>Column Name</th><th>Contents</th></tr>
<tr><td>Time</td><td>Time the system message was issued. Time is derived from the Pano Controller’s local time.</td></tr>
<tr><td>Level</td><td>The security level of the incident

<table>
<tr><th>Level</th><th>Message</th></tr>
<tr><td>INFO</td><td>User of desktop virtual machine 10.1.100.55 is -none-.</td></tr>
<tr><td>WARNING</td><td>Unknown desktop virtual machine rejection (4099).</td></tr>
<tr><td>CONFIG</td><td>Collection manager loaded configuration.</td></tr>
</table></td></tr>
<tr><td>Message</td><td>Text of the system message</td></tr>
</table>

4. (Optional) Download these messages. Go to Download Pano Controller Log Files.

To filter the list of system messages:

1. Log on to the Pano Controller.
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 Controller.
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 Controller.
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 Controller Log Files

The log files download as a zip file. These log files contain archived messages.

To download the Pano Controller's log files:

1. Log on to the Pano Controller.
2. Click on the **Log** tab.
3. Click **Download**.
4. When prompted, save the`.zip` file to a specific location.

Download DVM Log Files

A DVM's log files are time stamped with the local time of the Pano Direct Service that is running on that DVM.

To download a DVM's log files:

1. Connect to the DVM using a Pano System Endpoint or RDP. Go to Log On To DVMs as End User.
2. Zip the contents of directory `C:\Program Files\Pano Logic\PanoDirect\LOG` and copy to your desktop.
3. Unzip the file.
4. Use Wordpad to open the `.log` file. Neither Notepad nor Excel will not format the text properly. The log files have the following naming conventions:
   - PanoDirect-*DVMComputerName*-*YearMonthDayTime*.log
   - PanoCP-*DVMComputerName*-*YearMonthDayTime*.log

48
FAQs

This chapter includes the following topics:

- Basics FAQs
- Requirements and Sizing Guidelines FAQs
- Installation and Deployment FAQs
- Upgrades and Maintenance FAQs
- Pano Controller and DVM Performance FAQs
- Pano Controller and Pano Controller VM FAQs
- DVM and Pano Device Administration FAQs
- USB Devices and Peripherals FAQs
- DVM Collections FAQs
- DVM Creation, Templates, and Cloning FAQs
- DVM Preferences and Settings FAQs
- DVM Connections FAQs
- VMware vCenter Server and ESX Server FAQs
- Firewalls FAQs
- Directory Services, DHCP, and DNS FAQs
- VMware View FAQs
- Windows 7 FAQs
- XenDesktop FAQs
- Licensing FAQs

Basics FAQs

- Does the Pano System support Vista?
- Does the Pano System support 64-bit Windows XP?
- What Pano software do I install on a DVM?
- Does Pano System have any hypervisor dependencies?
- Is Pano System dependent on HA or DRS?
- Does the Pano Controller have HA capability?
- Can Pano System work with third-party Windows login modules?
- What third-party hardware/software do I need to run Pano System?
- How many IP addresses do I need to run Pano System?
- What components comprise Pano System?
- What Operating Systems does Pano System support?
- Where does the Pano Controller fit into my environment?
- Does Pano System support non-standard color depths?

Does the Pano System support Vista?

No. For details, go to Supported Operating Systems for Pano Direct Service Service.

Does the Pano System support 64-bit Windows XP?

No, as Pano Logic has not seen a great deal of interest in this platform. If you have a need, let us know!

What Pano software do I install on a DVM?

The software that goes in the guest is called Pano Direct Service. It runs as a service and communicates with the Pano System Endpoints.

The Pano Direct Service sends screen updates to the Pano System Endpoints and retrieves peripheral events like keyboard, mouse, audio, USB from the Pano System Endpoint. Most of the Pano Direct Service code runs in user space. There is a small kernel mode driver used to support USB redirection, and this driver allows USB devices plugged into the Pano System Endpoint to appear to the Windows system as a local USB device, providing a plug-and-play solution. USB just works.

Does Pano System have any hypervisor dependencies?

The Pano System has been architected to be independent of the underlying hypervisor. Currently Pano System is supported on the platforms outlined in Supported Virtualization Platforms.

Is Pano System dependent on HA or DRS?

No. The Pano System can take advantage of VMware Distributed Resource Scheduler (VMware DRS) and VMware High Availability (VMware HA) if present, but these VMware features are not required.

Does the Pano Controller have HA capability?

Yes. You can configure the Pano Controller for high availability. To do so, go to Configure Pano Controller Groups.

Can Pano System work with third-party Windows login modules?

Yes. Refer to Supported Third-Party Login Screens.

What third-party hardware/software do I need to run Pano System?

There are a few products, especially infrastructure. Go to Supported Virtualization Platforms.

How many IP addresses do I need to run Pano System?

Your The Pano System is meant to be efficient and to merge easily into your existing network infrastructure. For the Pano Controller itself you'll only need one additional static IP in addition to the IP(s) that are already used by your VMware host. The Pano System Endpoints themselves get their IP addresses from your DHCP server, just as any other PC or network device would in most networks.

What components comprise Pano System?

There are several components. For an architecture overview, go to Pano System Overview.

What Operating Systems does Pano System support?

For a list, go to Supported Operating Systems for Pano Direct Service Service. If you don't see your operating system supported, let us know.

Where does the Pano Controller fit into my environment?

The Pano Controller resides on your VMware host system. Its functionality is to facilitate management of your Pano System Endpoints and relationships between them and DVMs that reside in your VMware environment. For more information about Pano Controller, go to Pano Controller Group Architecture.

Does Pano System support non-standard color depths?

Pano Logic supports standard 16/24/32-bit color depth so long as your operating system supports these color depths. However, Pano Logic does not support nonstandard such as 15-bit color depth.

Requirements and Sizing Guidelines FAQs

- How scalable is Pano System?
- How do I size the hardware requirements for my VMware deployment?

- How do I size the hardware requirements for my Microsoft deployment?
- How do I size the hardware requirements for my Microsoft deployment?
- What are the sizing guidelines for the Pano Controller?
- How do I size my the Pano Controller to support a specific number of DVMs?
- How many Pano System Endpoints can I manage per Pano Controller instance?
- How many Pano System Endpoints can I manage per Pano Controller instance?
- What are the bandwidth requirements for Pano System?
- What are the minimum system requirements for a Pano System deployment?
- What’s the maximum power that a Pano System Endpoint can draw?

How scalable is Pano System?

There are a number of factors that can influence scalability. Using ESX servers will improve scalability. For a basic estimate, go to Monitor Load Balancing Across a Group.

How do I size the hardware requirements for my VMware deployment?

There are a number of factors that can influence how to size your environment. For a basic estimate, go to Requirements for VMware vSphere.

How do I size the hardware requirements for my Microsoft deployment?

There are a number of factors that can influence how to size your environment. For a basic estimate, go to Requirements for Windows Server 2008 R2 Hyper-V.

How do I size the hardware requirements for my Microsoft deployment?

There are a number of factors that can influence how to size your environment. For a basic estimate, go to Requirements for XenServer.

What are the sizing guidelines for the Pano Controller?

The Pano Controller is pretty self-contained and can be simply “dropped” into an existing ESX server. The default size works for most installations. Because the Pano Controller does not store huge amounts of data and its role is to facilitate communication between Pano System Endpoints and DVMs, it is quite light weight and does not consume high CPU or memory resources. For a basic estimate, go to Hardware & Resource Requirements.

How do I size my the Pano Controller to support a specific number of DVMs?

There are a number of factors that can influence how to size your environment. For a basic estimate, go to Requirements for VMware vSphere.

How many Pano System Endpoints can I manage per Pano Controller instance?

Pano Logic continues to increase the scalability of the Pano Controller in each release. If you need to scale beyond the limit outlined in Supported Number of DVMs and Pano Zero Clients, contact Pano Logic Technical Support for further assistance and guidance.

What are the bandwidth requirements for Pano System?

Bandwidth consumption is always a variable just as with a normal PC depending on if you're running at idle or doing things that cause bursts of traffic. For overall bandwidth requirements, go to Hardware & Resource Requirements.

What are the minimum system requirements for a Pano System deployment?

The requirements depend on your environment. For basic sizing guidelines, go to Hardware & Resource Requirements.

What’s the maximum power that a Pano System Endpoint can draw?

For general information about the voltage requirement and the power consumption of a Pano Device, go to Pano Zero Client Technical Specification.

Installation and Deployment FAQs

- Where can I download the latest Pano software?
- How do I prevent the Pano Control Panel from launching after a silent install?
- Why is my automatic deployment failing with a `Customization Failed` error?
- Why do I need to create folders in vCenter Server for Pano Logic?
- What license for vCenter Server on VMware ESX do I need to deploy Pano System?
- Can I install Pano System with ESXi without vCenter Server?
- How do I install VMware Tools in the Pano Controller?
- I just installed VMware Tools. What does `VMware hgfs: HGFS is disabled in the host` mean?
- Why can't I import PanoMan.tar.gz to Pano Controller using WinSCP or FTP?

Where can I download the latest Pano software?

Go to http://download.panologic.com. When prompted type in the download site credentials that Pano Logic Technical Support provided you. When the Support Services page launches, click the **Latest** link.

How do I prevent the Pano Control Panel from launching after a silent install?

With a "silent" install, the Pano Control Panel launches by default after the installer finishes. To avoid confusing your users, set the `LAUNCH_PANOCP` property to `0`.

- If the value is `1` then the Pano Control Panel will be launched when the installer finishes.
- If the value is `0` then the Pano Control Panel will *not* be launched when the installer finishes.

```
C:> msiexec LAUNCH_PANOCP=0 /i panodirect.msi
```

Why is my automatic deployment failing with a `Customization Failed` error?

This failure might be the result of one of two main causes: (1) The correct Sysprep tools are not installed. Ensure the correct Sysprep tools for the template's OS and version (for example, Windows XP SP3) are installed as outlined in Install Windows. (2) The template's correct "Guest OS" was not chosen. In this case, you need to convert the template to a virtual machine, then edit the settings to specify the correct Guest OS.

Why do I need to create folders in vCenter Server for Pano Logic?

Folders help you manage DVMs. Pano Logic recommends that you create a few folders. For instructions, go to Create Virtualization Hierarchy–VMware.

What license for vCenter Server on VMware ESX do I need to deploy Pano System?

You must have individual licenses for both vCenter Server and ESX Sever, but they can be evaluation licenses. Pano System doesn't require any features licenses for VMware HA, VMotion, DRS, etc, unless you want to use these features.

Can I install Pano System with ESXi without vCenter Server?

Yes, but there is a limitation to this deployment/configuration. For more information, go to Install Pano System with ESXi without vCenter Server.

How do I install VMware Tools in the Pano Controller?

There are time synchronization and performance benefits with VMware Tools. For installation instructions, go to Install Windows.

I just installed VMware Tools. What does `VMware hgfs: HGFS is disabled in the host` mean?

During the bootup process and after VMware Tools has been installed, you might see a message that mounting HGFS (Host-Guest File System) shares failed. HGFS is used by VMware to share folders between the host and the guest. Installing VMware Tools adds an entry to `/etc/fstab` to specify the location of shared folders. To avoid the mounting HGFS shares failure message, comment out the line in /etc/fstab added by VMware Tools:

```
# .host:/ /mnt/hgfs vmhgfs defaults,ttl=5 0 0
```

Why can’t I import PanoMan.tar.gz to Pano Controller using WinSCP or FTP?

It’s highly likely that the file system is read only. This problem can occur if the DVM was created by an account without write permission to the ESX host. To fix this problem, reinstall the DVM with root account on ESX host.

Upgrades and Maintenance FAQs

- How do I upgrade Pano System?
- Does a Pano Controller upgrade interrupt my users?
- Why do I get unsigned driver error?
- How do I upgrade the firmware on my Pano System Endpoint?
- How do I upgrade the Pano Controller?
- How do I upgrade Pano Direct Service?
- Must I upgrade both Pano Direct Service and Pano Controller?
- What kind of ongoing maintenance does the Pano System require?
- Can I safely remove files in the Pano Controller Virtual Machine /tmp directory?

How do I upgrade Pano System?

There are a few components that you must upgrade in order to upgrade the entire solution. For instructions, go to Upgrading Your Pano System to 6.0.

Does a Pano Controller upgrade interrupt my users?

If your users are logged on to their DVMs, they will not be affected while Pano Controller is being upgraded. The only impact is to users that aren’t currently logged on as they can’t log on until you complete the upgrade.

Why do I get unsigned driver error?

You might be prompted a couple of times when you install or upgrade Pano Direct Service because of unsigned drivers. You might be also be asked to overwrite existing files if you upgrade to a released version from a beta version. These are normal situations, and there’s no reason to be concerned.

How do I upgrade the firmware on my Pano System Endpoint?

All updates to the Pano platform are performed on the Pano Direct Service and the Pano Controller. Pano System Endpoints do not require any updates, as the Pano has no software, no CPU, and requires no software maintenance.

How do I upgrade the Pano Controller?

The upgrade process begins with downloading the latest software from Pano Logic’s download site. For instructions, go to Upgrading Your Pano System to 6.0.

How do I upgrade Pano Direct Service?

The upgrade process begins with downloading the latest software from Pano Logic’s download site. For instructions, go to Upgrade Pano Direct Service.

Must I upgrade both Pano Direct Service and Pano Controller?

For compatibility and best performance, Pano Logic recommends that you upgrade both software components.

What kind of ongoing maintenance does the Pano System require?

When you upgrade, you only do so for Pano Controller and Pano Direct Service. Pano Logic releases updates regularly; however, you aren't required to upgrade. Pano Logic encourages upgrades because they include enhancements and fixes. For more information about upgrades, go to Upgrading Your Pano System to 6.0.

Because Pano System depends on third party products, you should periodically browse Pano Controller's log files to determine if any errors are being reported. Sometimes errors are caused by a change in vCenter Server or storage solution. For more information about log files, go to Work with Log Files.

Can I safely remove files in the Pano Controller Virtual Machine `/tmp` directory?

Yes. However, before you do so, stop the Pano Controller service, delete the files, then restart:

```
service atto stop
cd /tmp
del *
service atto start
```

Pano Controller and DVM Performance FAQs

- How do I improve the availability of DVMs?
- How do I limit the resource usage of the Pano Controller?
- How do I prevent CPU spikes?
- How do I increase service console memory?
- How do I use Session Timeouts for maximum resource efficiency and data security?
- How do I add a second virtual CPU? Will an additional CPU improve DVM performance?
- What happens to DVMs in case of an active path failure to my SAN?
- Can I improve the speed at which users can log on to their Pano System Endpoints?
- Why does keyboard input seem slow and "jumpy"?
- Can I improve the performance of mouse movement? Mouse movement seems slow or "jumpy".
- How does video perform on Pano System Endpoint over WAN?

How do I improve the availability of DVMs?

For Pooled Desktops collection type this is easy because all DVMs are the same. If a DVM crashes or gets corrupt, the Pano Controller can simply direct vCenter Server to create a new DVM.

However for Permanently Assigned Desktops collection type where each DVM belongs to a specific user, added measures have to be taken to improve availability. VMWare High Availability (VMWare HA) and VMotion functionality can be used. Regular backups and snapshots of the DVMs should also be added to the management of the DVMs. This way users will not be affected when underlying virtualization infrastructure is affected.

How do I limit the resource usage of the Pano Controller?

Create a dedicated resource pool for Pano management server. For instructions, go to Reserve Resources for the Pano Controller VM in vCenter Server.

How do I prevent CPU spikes?

You can disable `rdpclip.exe` to prevent CPU spike. For instructions, go to Increase VMware ESX Server Service Console Memory.

How do I increase service console memory?

By increasing service console memory, you can improve performance. For instructions, go to Increase VMware ESX Server Service Console Memory.

How do I use Session Timeouts for maximum resource efficiency and data security?

Session Timeout settings end both disconnected and idle sessions. For details, go to Control Session Timeouts.

How do I add a second virtual CPU? Will an additional CPU improve DVM performance?

Depending on the performance issues, an additional CPU might improve performance. To add a second virtual CPU:

1. Power off the DVM.
2. Edit the settings and change the number of CPUs to `2`.
3. Restart the DVM.

What happens to DVMs in case of an active path failure to my SAN?

Without disk timeouts, you don't have high availability against such failures. For instructions on how to set up a disk timeout, go to Protect Against Connection Failures To SAN Devices.

Can I improve the speed at which users can log on to their Pano System Endpoints?

One of the possible reasons for slow login is that it takes a long time to get LDAP information. If you have more than one LDAP server, configure the Pano Controller to use the closest LDAP (Connect Pano Controller To Directory Services). You can ping different LDAP servers to determine which one is closest to the Pano Controller.

Why does keyboard input seem slow and "jumpy"?

The problem might be related to VMware Tools, Pano Direct Service, or the Repeat rate. To troubleshoot, go to Mouse or keyboard is not working with Pano System Endpoints.

Can I improve the performance of mouse movement? Mouse movement seems slow or "jumpy".

Yes, you can do so through mouse scheme and hardware acceleration. For instructions, go to Ways To Optimize DVM Performance. If that doesn't work, verify that VMware Tools are installed on your DVM(s). VMware Tools improves performance. Go to Install Windows.

How does video perform on Pano System Endpoint over WAN?

Pano System Endpoints are optimized for LAN. They are not optimized for WAN, especially for video applications.

Pano Controller and Pano Controller VM FAQs

- Why can't I connect to the Pano Controller?
- How do I enable https and use a custom certificate with Pano Controller?
- Why can't I delete a row in the log file that has a future date?
- How do I configure the Pano Controller to connect to vCenter Server on VMware ESX?
- Why do I receive a java exception error when I connect to vCenter Server from the Pano Controller Web UI?
- What ports does the Pano Controller use?
- Why can't I see a DVM's information in the Pano Controller's DVMs tab?
- What is the default root password for the Pano Controller?
- What the Pano Controller's default admin username and password?
- Why can't I connect to the Pano Controller, despite having typed the correct username and password?

Why can't I connect to the Pano Controller?

There are two very common causes:

- The Pano Controller Virtual Machine is uncompressed on a Windows virtual machine, and results in a partially working virtual machine. The Pano Controller Virtual Machine must be uncompressed on the ESX host.
- There is no default network label, VM Network, on the ESX host. The Pano Controller uses this default network label to connect to physical network adapter and its virtual network adapter will not be connected if this label does not exist. The fix this problem, manually edit the Network Adapter settings for the Pano Controller VM and choose the correct network label.

How do I enable https and use a custom certificate with Pano Controller?

It's relatively easy to upload your own self-signed certificate. For instructions, go to Replace Pano Controller's Self-Signed Certificate.

How do I disable http port 80 for user web login?

To disable port 80, comment the lines that redirects port 80 and opens 8084 as shown in How do I disable http port 80 for user web login?.

Why can't I delete a row in the log file that has a future date?

The timestamp dates on your log files are based on the ESX server's time. If you didn't have VMware Tools installed and if at one time your ESX server was configured with a later times (e.g. year 2009), then it was updated with the correct time (e.g. year 2008), you'll see 2009 entries in the log file, and they'll appear at the top.

To delete rows from the log table where the timestamp of the rows is greater than now:

1. ssh to the Pano Controller. Go to Initiate Secure Connections.
2. Type **su postgres**.
3. Type **psql attodevices**.
4. Delete from ad_log_event where ad_timestamp > CURRENT_TIMESTAMP;
5. Type **commit;**.
6. Type **\q**.
7. Type **exit**.
8. Log off the Pano Controller.

How do I configure the Pano Controller to connect to vCenter Server on VMware ESX?

You must specify either the IP address or hostname. Also, the Pano Controller must have the correct DNS server configured.

- To configure the Pano Controller's connection with vCenter Server, go to Connect Pano Controller To vCenter Server.
- If you have problems connecting to vCenter Server, go to Troubleshoot Communication Problems with vCenter Server.

Why do I receive a java exception error when I connect to vCenter Server from the Pano Controller Web UI?

This problem is usually the result of a misconfiguration. No problem. Go to Troubleshoot Communication Problems with vCenter Server.

What ports does the Pano Controller use?

The Pano Controller communicates on specific inbound and outbound ports. For a list, go to Pano Controller Network Port Usage.

Why can't I see a DVM's information in the Pano Controller's DVMs tab?

Do the following:

- Verify the firewall is configured correctly. You can configure this locally on the machine (configure to allow port 8319 via TCP), or you can set a group policy as outlined in Configure DVM Firewall.
- Verify the Pano Direct Service is installed on the DVM and that the Pano Direct Service service is running. Go to Deploy Resources.
- Verify your Virtual Infrastructure license. If the license is expired, the DVM may behave in this manner.

What is the default root password for the Pano Controller?

It is `password`. Be sure to change it.

What the Pano Controller's default admin username and password?

The user name is `admin`. There is no default password: the password was set when the Pano Controller was configured as part of deployment.

You should use this credential to log in to the Pano Controller, not the root credentials.

Why can't I connect to the Pano Controller, despite having typed the correct username and password?

Make sure you are using a domain account.

DVM and Pano Device Administration FAQs

- How do my users access their DVMs remotely?
- Can I lock a Pano System Endpoint?
- How do I expand the size of a DVM's hard drive?
- Why does the Pano Controller show partial or incorrect information for a DVM?
- How do I set the date and time in the Pano Controller?
- How do I manage my Pano System Endpoints?
- Why can't I see the DVM and Template folders in the Pano Controller?
- How do I add an additional hard drive to a DVM?

How do my users access their DVMs remotely?

Use Pano Remote. With Pano Remote you do not need a VPN configuration. For more information, go to Deploy Pano Remote.

Can I lock a Pano System Endpoint?

Yes, absolutely! To learn how, go to Secure Pano Devices.

How do I expand the size of a DVM's hard drive?

The method depends on whether your drive is a system drive or a data drive. For step-by-step instructions, go to Expand DVM Hard Drives.

Why does the Pano Controller show partial or incorrect information for a DVM?

Often a restart of vCenter Server fixes the problem. An expired vCenter Server license can also cause this problem.

How do I set the date and time in the Pano Controller?

The Pano Controller automatically syncs its time with the ESX host. Make sure that your ESX host's date and time are correct.

How do I manage my Pano System Endpoints?

Pano System makes use of various third party components: Active Directory, VMware ESX Server, and vCenter Server. The Pano Controller speaks directly to these key components and helps you manage your Pano System Endpoints. For a complete product overview, go to Pano System Overview.

Using a web server running on your Pano Controller, the Pano Controller Web UI easily manages your Pano System Endpoints. The Pano Controller resides on a stand-alone virtual machine that you'll simply import to your VMware host; either ESX/ESXi will work. The Pano Controller consists of two virtual disks.

- The 1st disk is the primary disk that contains the Pano Controller's operating system and the web server. The web server is responsible for providing easy management of your Pano System Endpoints and the login screens to your Pano System Endpoints. Login screens enable your end-users to enter their standard domain credentials to get their DVMs.
- The second disk is for database storage of information about available DVMs for use via your Pano System Endpoints. The Pano Controller obtains this information by communicating with your Microsoft Active Directory and your vCenter Server.

To deploy Pano System, go to Deploying Your Pano System.

Why can't I see the DVM and Template folders in the Pano Controller?

These folders don't exist by default in vCenter Server. You must create them. For instructions, go to Create Virtualization Hierarchy–VMware.

How do I add an additional hard drive to a DVM?

To add a hard drive:

1. From the ESX server, go to Edit Settings.
2. Add the drive for the DVM.
3. Log in to the DVM, then using Disk Management, add the drive as you would for a physical desktop computer.

USB Devices and Peripherals FAQs

- Does Pano Logic support USB isochronous devices?
- Does Pano Logic support touchscreen monitors?
- How do I prevent users from using USB devices such as a flash drive?
- Why doesn't my USB hard drive work with my Pano System Endpoint?
- Why doesn't my mouse and keyboard work with my Pano System Endpoint?
- How do I install USB driver so that I can use generic USB devices?
- How do I limit access to generic USB devices?
- Can I still use my flash drive or external cd/dvd burner?
- Do I need special peripherals for my Pano System Endpoints?

Does Pano Logic support USB isochronous devices?

Yes. For more information, go to Supported Isochronous USB Devices for Pano G2.

Does Pano Logic support touchscreen monitors?

Yes, but not all touchscreen monitors are supported. For more information, go to Support for USB Devices.

How do I prevent users from using USB devices such as a flash drive?

You can restrict users from using specific USB device by specifying a USB filter string value. For instructions, go to Restrict or Allow Use of Specific USB Devices.

Why doesn't my USB hard drive work with my Pano System Endpoint?

As outlined in Support for USB Devices, Pano Logic supports many such devices. If the Pano System Endpoint does not recognize your particular device, send the model number of the device(s) to Pano Technical Support. We will test it internally and enhance the product if necessary.

Why doesn't my mouse and keyboard work with my Pano System Endpoint?

There are few causes for this problem. Go to Troubleshoot Monitor, Mouse, and Keyboard Problems.

How do I install USB driver so that I can use generic USB devices?

To do so you must install a USBD.SYS driver is on your Windows DVMs. For instructions, go to Install Pano Device USB Support.

How do I limit access to generic USB devices?

You can restrict users from using specific USB device by specifying a USB filter string value. For instructions, go to Restrict or Allow Use of Specific USB Devices.

Can I still use my flash drive or external cd/dvd burner?

Yes. To see a list of supported devices, go to Support for USB Devices.

Do I need special peripherals for my Pano System Endpoints?

No. The Pano System Endpoint works with standard USB devices (go to Support for USB Devices). If you have any concerns or questions about compatibility with certain devices you depend on for your business need please consult with Pano Logic Technical Support or your Pano Logic certified reseller.

DVM Collections FAQs

- Why does user get a different DVM, even though the collection type is custom?
- What is the typical use case for a pooled collection?
- What is the typical use case for a cloned collection?
- I tried to create a collection. What does `Users not found - please check the canonical names` mean?
- What is the typical use case for a custom collection

Why does user get a different DVM, even though the collection type is custom?

With a custom collection, only one DVM should be put in the DVMs folder (refer to Create Virtualization Hierarchy–VMware). If there are more than one then it is possible that the user will get a different DVM when the user logs in multiple times. For details about the collection types, go to DVM Collections and Provide Access To DVM Collection.

What is the typical use case for a pooled collection?

There are unique use cases for each collection type. For details, go to DVM Collections.

What is the typical use case for a cloned collection?

There are unique use cases for each collection type. For details, go to DVM Collections.

I tried to create a collection. What does `Users not found - please check the canonical names` mean?

For a definition, see wikipedia. Check the URL string. Make sure organization names or organization unit names are correct: the strings are case sensitive. For example "ldaps://172.16.202.22:636/o=OAG" is different from "ldaps://172.16.202.22:636/o=oag" Also "ldap:///DC=panodc,DC=com" is different from "ldap:///DC=Panodc,DC=com".

What is the typical use case for a custom collection

There are unique use cases for each collection type. For details, go to DVM Collections.

DVM Creation, Templates, and Cloning FAQs

- I just converted a physical machine to a virtual machine. Why am I having network issues?
- How do I create a Window XP virtual machine?
- I tried to create a virtual machine. What does `cannot copy vmscsi.sys file` mean?
- Why do I need to create new folders for DVMs and Templates in my VMware environment?
- Why and how should I organize my DVMs and templates?
- What does `the operation is not supported on the object` error message mean?
- Why can't I select a group as remote users to my template?
- How do I configure my Windows XP template for best performance?
- Why can't I clone any DVMs, despite having chosen the folder that contains my template in DVM Collection?
- What kind of DVM Collection is best for my users?
- How do I automate DVM creation?
- Can virus scanner software cause failure in cloning?
- How do I configure a DVM to join a specific OU after cloning?

I just converted a physical machine to a virtual machine. Why am I having network issues?

If you just converted a VMware Foundation virtual machine to an ESX virtual machine and everything seems normal:

- The machine powers on, and gets an IP address and DNS name.
- The firewall is disabled.
- You can ping the DVM from Pano Controller VM.

However, the status of the DVM in Pano Controller is `Unreachable`. To fix this problem, delete the network card and add it again.

How do I create a Window XP virtual machine?

It's quite easy. For instructions, go to Create Desktop Virtual Machines in vSphere Client.

I tried to create a virtual machine. What does `cannot copy vmscsi.sys file` mean?

The error message is setup cannot copy vmscsi.sys file. This error message comes even though the floppy drive is connected to the virtual machine. The error was due to the Windows XP image being used, and was created with NLite iso image.

When creating the image, you have to make sure that the OEM Preinstall (within the unattended screen of NLite) is set to disabled. If it is set to enabled it will look for the scsi drivers as referenced by the winnt.sif file. This is why it can't find the vmscsi.sys files as it is only looking in this directory on the CD and never references the floppy drive. Unless you have a number of custom drivers, you need to integrate; it's much simpler to just use the floppy image.

Why do I need to create new folders for DVMs and Templates in my VMware environment?

Folders help you manage your DVMs. For more information, go to Create Virtualization Hierarchy–VMware.

Why and how should I organize my DVMs and templates?

Using an example whereby you need to deploy DVMs for two departments, Helpdesk and Engineering, do one of the following:

Option #1

Create a folder hierarchy for each group of users. Create a folder called Helpdesk and two other folders, `DVMs and Template`, inside `HelpDesk`. Create another folder, `Engineering`, in the same level as `Helpdesk` and two other folders, `DVMs` and `Template`, inside `Engineering`.

Option #2

Create a master folder, `DVM Deployment`, that contains three folders, `Helpdesk`, `Engineering`, and `Templates`.

For more information, go to [Create Virtualization Hierarchy–VMware](#).

What does `the operation is not supported on the object` error message mean?

If you received this error when your collection failed to clone a virtual machine the most common cause is that you created the folder structure in the **Hosts and Clusters** view in VMware vCenter Server. Create the folder structure in the **Virtual Machines and Templates** view instead.

Why can't I select a group as remote users to my template?

Make sure this template is in a domain, and make sure the group's scope is global.

How do I configure my Windows XP template for best performance?

Follow the workflow outlined in Create Desktop Virtual Machines in vSphere Client and tips listed in Ways To Optimize DVM Performance.

Why can’t I clone any DVMs, despite having chosen the folder that contains my template in DVM Collection?

You must choose the specific template, not the folder that contains the template.

What kind of DVM Collection is best for my users?

Each collection type has its benefits. For detailed information, go to Provide Access To DVM Collection.

How do I automate DVM creation?

Pano System uses the Customization Specification (wizard and templates (Create Desktop Virtual Machines in vSphere Client).

Can virus scanner software cause failure in cloning?

Yes, and this is a known issue with VMware. Some virus scanner software can cause failure in cloning because such software can interfere with sysprep. For more information, see Virtual Machines Deployed From a Template Might Not be Customized Correctly, KB 1006848, and KB 1008281.

How do I configure a DVM to join a specific OU after cloning?

All DVMs will join the default OU after cloning by default. If you want them to be in a specific OU, you can run a script in customization stage. The sample script below will join all DVMs in a specific OU:

```
sleep 30

netdom join %computername% /domain XXX /userd:DOMAIN\
ACCOUNT /passwordd:XXXX
/OU:"ou=XXX,ou=YYY,dc=ZZZ,dc=WWW" /reboot:20

del c:\windows\temp\join.cmd
```

This script is called `join.cmd` and is executed as Run Once from Client Customization. In the Client Customization, you must select the login once as Administrator checkbox for this to work.

For Windows 2008 Server examples see dsmove or netdom for more Windows 2003 Server examples.

DVM Preferences and Settings FAQs

- Can I switch between user accounts from my Windows XP DVM?
- How do I specify a default input language for Pano System Endpoints?
- How do I specify a default input language for Pano System Endpoints?
- Are the screenbits encrypted between the Pano System Endpoint and its associated DVM?
- How do I set the power save option for a Pano System Endpoint?
- Why doesn’t my monitor work with my Pano System Endpoint?
- How do I change/define the screen resolution on my DVM?
- What does the color of the Pano Button mean?
- How do I set the power save option for a Pano System Endpoint?
- How do I enable 24-bit color for Pano System Endpoints?
- How do I display my company's logo on Pano user login screen?
- My audio is distorted. How do I adjust the output?
- How do I configure my audio settings?
- How do I configure display/video settings?
- Does Pano Logic support wireless bridges?

Can I switch between user accounts from my Windows XP DVM?

No. Pano System does not support fast user switching for Windows XP DVMs. For more information, see Limitations to Fast User Switching. See also Can I switch between user accounts from my Windows 7 DVM?.

How do I specify a default input language for Pano System Endpoints?

These are two different ways to customize the language that your end-users see:

- Enable Language Preference for Pano Client Login Screen
- Set Default Keyboard Layout and Input Language for Specific DVMs

Are the screenbits encrypted between the Pano System Endpoint and its associated DVM?

Keyboard and mouse traffic are encrypted between Pano System Endpoints and ESX server. Such encryption prevents anyone from being able to piggy back onto the network using packet sniffers. However the screen traffic is not encrypted, as the screen traffic is binary and represents just screen bits.

How do I set the power save option for a Pano System Endpoint?

There are two ways to set this option. You can either do so from the Pano Controller. For instructions, go to Set Power Save Option for All Pano Zero Clients. Optionally, you can do so from the Pano Control Panel. For instructions, go to Set Power Save Settings for Specific DVMs as End User.

Why doesn’t my monitor work with my Pano System Endpoint?

It’s possible that the monitor is out of range. To troubleshoot this problem, go to Troubleshoot Monitor, Mouse, and Keyboard Problems.

How do I change/define the screen resolution on my DVM?

You can do so from the Pano Control Panel. For instructions, go to Set Screen Resolution Settings for Specific DVMs.

What does the color of the Pano Button mean?

The meaning depends on the color. Compare the state of your Pano Button to the information in Pano Zero Client Light Indicators.

How do I set the power save option for a Pano System Endpoint?

You can do so from the Pano Control Panel. For instructions, go to Set Power Save Settings for Specific DVMs as End User.

How do I enable 24-bit color for Pano System Endpoints?

Graphics are much sharper with 24-bit color; however, consider that the benefit of 24-bit does not outweigh the significant performance hit that users experience with 24-bit. To enable 24-bit color, go to Configure DVMs for 24-bit Color.

How do I display my company's logo on Pano user login screen?

It's quite simple. You just need to upload a `.png` file of your logo. For instructions, go to Use a Custom Login Image.

My audio is distorted. How do I adjust the output?

You can adjust the audio setting from the Pano Control Panel. For instructions, go to Set Audio Settings for Specific DVMs.

How do I configure my audio settings?

You can configure the audio setting from the Pano Control Panel. For instructions, go to Set Audio Settings for Specific DVMs.

How do I configure display/video settings?

You can do so from the Pano Control Panel. For instructions, go to Set Screen Resolution Settings for Specific DVMs.

Does Pano Logic support wireless bridges?

Yes. To configure, go to Connect Pano Zero Clients To Your Wireless Network.

DVM Connections FAQs

How do Pano System Endpoints get sessions to my Windows desktop virtual machine?

Pano System uses DVM collections to enable connections between Pano System Endpoints and your Windows desktop virtual machine (DVM). The DVM collections define policies that determine which DVMs you can connect to. For more information, go to DVM Collections and Provide Access To DVM Collection.

Why is the light on my Pano System Endpoint blinking orange/amber?

Pano Button indicators have specific meanings, depending on if the state is a fault state or a normal (temporary) state. To identify the state of your Pano System Endpoint, go to Pano System Endpoint Login Status Indicators.

Why do I receive a `No UPN` error when I log in to a DVM from the Pano System Endpoint?

The problem might be because the user account lacks the correct permissions, or Active Directory is misconfigured. For more information, go to No Privileges or No UPN Format.

Why am I receiving a `Your Desktop Is Being Reset in login screen` error message?

If this message is shown, your desktop might be resetting; however, if you experience this error continually or for an extended period of time, restart vCenter Server to resolve the problem.

How do I troubleshoot session problems with my DVM?

How you troubleshoot depends:

- If the problem is related to networking, go to Troubleshoot Networking Problems.
- If the problem is related to login problems, go to Troubleshoot DVM Login Problems.

Why does the login screen go blank after I log on to the domain from Pano System Endpoint?

RDP might not be enabled. Go to Enable Remote Desktop & Set RDP Users.

Why do I receive a data encryption error when I try to connect to a DVM through RDP?

This is a known issue with Windows XP. To apply a fix, go to Data encryption error.

Why can't I log on to a DVM, even though RDP is enabled?

The problem might be the result of the Windows firewall on the DVM. For more information, go to Firewall prevents communication. If this solution doesn't fix the problem, refer to a complete list of solutions: go to Troubleshoot RDP Connection Problems.

What does `Cannot login because authentication is not available at this time` mean?

This can happen in an instance where the Pano Controller is not able to communicate properly with your Active Directory or other user authentication service. Proper configuration is outlined in Connect Pano Controller To Directory Services.

For user authentication service you can typically use any username that has the privileges or permissions to browse your AD/LDAP tree in order to authenticate users. Many Pano Logic customers simply use a regular account such as an account that is a member of an OU (for example, domain users).

What does `Cannot login because you do not have a UPN` mean?

Check to see if the user account that you specified has administrator privileges. The user name has to be in UPN format. For more information, go to No Privileges or No UPN Format.

What does `Login Failure - No DVM's are configured for you` mean?

The problem might be related to DVM collection itself. For more information, go to No desktops are available. Please contact your system administrator; No DVMs are configured for you; No DVMs are available for you..

What does `Cannot connect to DVM` mean?

The DVM was detected, but you cannot connect.

What does `No DVM's are available for you` mean?

The problem might be related to DVM collection itself. For more information, go to No desktops are available. Please contact your system administrator; No DVMs are configured for you; No DVMs are available for you..

VMware vCenter Server and ESX Server FAQs

- Why can't the Pano Controller communicate with vCenter Server anymore, after having created folders in vCenter Server?
- How and where do I install sysprep tools?
- I tried to connect to vCenter Server from the Pano Controller. What does `VMware vSphere:¶¶WARNING: VirtualizationManager.ConnectFailure` mean?

Why can't the Pano Controller communicate with vCenter Server anymore, after having created folders in vCenter Server?

Always be sure to create and edit folders in the **Virtual Machines and Templates** view, not in **Hosts and Clusters** view.

How and where do I install sysprep tools?

The Pano Controller can automatically provision desktops by utilizing a Customization Specification script that you can easily create through vCenter Server. However, in order to utilize this functionality the Microsoft Sysprep tools must be installed in the correct directory on your vCenter Server server. For example: In order to automatically provision an XP DVM you need place the Microsoft Sysprep tools for XP in `C:\Documents and Settings\All Users\Application Data\VMware\VMware vCenter\sysprep\xp`.

For in-depth OS-specific instructions, go to *Installing the Microsoft Sysprep Tools* in the VMware's ESX Server Basic Administration Guide.

I tried to connect to vCenter Server from the Pano Controller. What does `VMware vSphere:¶¶WARNING: VirtualizationManager.ConnectFailure` mean?

Usually, this means that vCenter Server has a different IP address or hostname than what's specified in the Pano Controller. If you have the correct IP address or hostname, ensure that you also specified `/sdk` at the end of the URL string. For more information, go to Troubleshoot Communication Problems with vCenter Server.

Firewalls FAQs

- How and where do I configure the GPO settings to open ports on a Windows firewall?
- Over what port(s) does the Pano Controller communicate with the DVMs?

How and where do I configure the GPO settings to open ports on a Windows firewall?

You can use a local policy or a domain policy. Pano Logic recommends that you use a domain level GPO as this kind of policy takes precedence over any local machine policy, ensuring proper functionality with less interaction and maintenance.

- For instructions on how to open the required ports, go to Configure DVM Firewall.

- For a list of all network port information, go to Pano Zero Client Technical Specification.

Over what port(s) does the Pano Controller communicate with the DVMs?

The Pano Controller uses specific inbound and outbound TCP and UDP ports to communicate with your Pano System Endpoints and DVMs. For a list, go to Pano Controller Network Port Usage.

Directory Services, DHCP, and DNS FAQs

- My DVM successfully joined the domain. Why don't I see a DNS entry for the DVM?
- How do I configure a Netware DHCP server?
- How do I configure a Cisco IOS DHCP server?

- How do I configure a Linux DHCP server?
- Why can't I find my Pano System Endpoints, even though I've defined a vendor class in my DHCP server?
- Should I create a new group or OU for my Pano users, or use an existing group or OU?
- I tried to connect to Active Directory. What does `javax.naming.CommunicationException: localhost:389 [Root exception is java.net.ConnectException: Connection refused]` mean?
- How do I configure the Pano Controller to connect to Active Directory?
- Why isn't the Enable Local Broadcast method option in the Pano Controller working in my environment?
- Can I use OpenLDAP instead of Active Directory?
- How do I configure the Pano Controller for OpenLDAP?
- Can I use Novell eDirectory instead of Active Directory?
- How do I configure the Pano Controller for Novell eDirectory?
- How do I configure the Pano Controller to discover my Pano System Endpoints on my network?
- How do Pano System Endpoints get IP addresses?
- What peripherals do I need to connect to a Pano System Endpoint?
- How do I authenticate users with Pano System?
- Why can't I see the Active Directory (AD) tree, users, groups, and Organization Units (OU) in the Pano Controller's Setup tab?
- Why can't my DVM join the Active Directory (AD) domain?
- Why can't I connect to Active Directory from my the Pano Controller?
- What credentials do I use to connect my the Pano Controller to Active Directory (AD)?
- Why can't I browse the hierarchy even though my the Pano Controller is connected to Active Directory (AD)?

My DVM successfully joined the domain. Why don't I see a DNS entry for the DVM?

If no DNS entry appears you might need to enable dynamic updating of PTR records. To do this, perform the following steps:

1. Log on to your DNS server.
2. Click the **DNS** tab, then **Properties**.
3. Select the **Always dynamically update DNS and PTR records**.

How do I configure a Netware DHCP server?

Pano Logic has a tech note that addresses an example configuration. Go to Add Pano Logic Vendor Class for Netware DHCP Server.

How do I configure a Cisco IOS DHCP server?

Pano Logic has a tech note that addresses an example configuration. Go to Add Pano Logic Vendor Class for Cisco IOS DHCP Server.

How do I configure a Linux DHCP server?

Pano Logic has a tech note that addresses an example configuration. Go to Add Pano Logic Vendor Class for Linux DHCP Server.

Why can't I find my Pano System Endpoints, even though I've defined a vendor class in my DHCP server?

Do the following:

- Verify that vendor class is properly configured, and that your DHCP service or daemon is running.

- Check your networking and firewall settings: verify that necessary communication ports aren't being blocked. For more information, go to Firewall prevents communication.

Should I create a new group or OU for my Pano users, or use an existing group or OU?

It is not necessary to create new Groups or OUs within Active Directory in order for the Pano System to function properly. However, it is sometimes desirable to use Groups and OUs because they enable you to organize your Pano users.

For instance, you can choose `Domain Users`, which would allow anyone in your domain/organization to use a DVM from a Pano System Endpoint, providing that there is a DVM available for that user. This is good for simple testing, or if you don't need in-depth categorization.

However if you create new Groups or OUs you can categorize your Pano users by a geographical location (North America, Asia, etc) or a specific department (Accounting, HR, Engineering, Support, etc).

I tried to connect to Active Directory. What does `javax.naming.CommunicationException: localhost:389 [Root exception is java.net.ConnectException: Connection refused]` mean?

You might not have a service location record in your DNS Server. To add a service location record, go to No service location record.

How do I configure the Pano Controller to connect to Active Directory?

You do so through the Pano Controller. Pano Logic has a step-by-step procedure. Go to Connect Pano Controller To Directory Services.

Why isn't the Enable Local Broadcast method option in the Pano Controller working in my environment?

The Enable Local Broadcast option will only work in instances where your Pano System Endpoints and your Pano Controller are within the same subnet.

If your Pano System Endpoints are on a subnet that is external to that of your Pano Controller, you'll need to choose a different Discovery Configuration such as Remote Broadcast Networks, or Probe Address Range; keep in mind that for these options to work you'll need to make sure that your network switches allow broadcast traffic across segmented subnets.

In production environments, Pano Logic recommends implementing a vendor class in your DHCP services. The benefit is quick and accurate discovery of your Pano System Endpoints.

For instructions on using each of these methods, go to Connect Pano Controller To Directory Services.

Can I use OpenLDAP instead of Active Directory?

Yes! Pano System should work with any LDAP directory server.

How do I configure the Pano Controller for OpenLDAP?

Pano System should work with any LDAP directory server. Each product might require unique configuration settings. Follow the step-by-step instructions in Connect Pano Controller To Directory Services; if you have any difficulties, contact Pano Logic Technical Support.

Can I use Novell eDirectory instead of Active Directory?

Yes! For a complete list of the directory services that Pano System supports, go to Supported Directory Services.

How do I configure the Pano Controller for Novell eDirectory?

This is a common configuration process that's usually performed as part of your deployment. For specific instructions, go to Connect Pano Controller To Directory Services.

How do I configure the Pano Controller to discover my Pano System Endpoints on my network?

You must choose a discovery method. For more information, go to Choosing a Pano Client Endpoint Discovery Method.

How do Pano System Endpoints get IP addresses?

Your Pano System Endpoints get their IP addresses from your DHCP server. There is no facility or need to configure an IP address directly on a Pano System Endpoint. Just plug it in!

If you need to assign a specific IP address, you can easily do so by reserving specific IP addresses within your DHCP IP address pool(s); however, each Pano System Endpoint must get its address from your DHCP server, and each IP address must be unique.

What peripherals do I need to connect to a Pano System Endpoint?

The Pano System Endpoint plugs into your keyboard, mouse, monitor, and network just as a PC would except that it consumes much less resources (for example, disk space and power). Once a Pano System Endpoint powers on and obtains an IP address, it communicates with the Pano Controller in order to connect to a DVM that has been made available.

How do I authenticate users with Pano System?

Your users are authenticated through the Pano Controller by leveraging technologies that you most likely already have in your environment. Such technologies include Microsoft Active Directory, Novell eDirectory, or OpenLDAP. For step-by-step instructions to configure user authentication, go to Connect Pano Controller To Directory Services.

Why can't I see the Active Directory (AD) tree, users, groups, and Organization Units (OU) in the Pano Controller's Setup tab?

If you’ve entered the correct domain controller and credentials, and the status says `Connected`, yet the AD hierarchy of objects does not show up, the user credentials do not have privileges to see the tree. The user account is not required to have write privileges, but it is required to have read privileges on the AD tree.

Also, if you receive a java exception, then make sure that the user id is provided in UPN format. For instructions, go to Connect Pano Controller To Directory Services.

Why can't my DVM join the Active Directory (AD) domain?

Joining a DVM to the AD Domain is no different than joining a physical machine to the domain. There are two possible reasons for this problem:

- You either don’t have right permissions. Check to make sure that the user has admin privileges and has privilege to join the computer to the domain.
- There is a limit to the number of the computers that can join using this account.

Why can’t I connect to Active Directory from my the Pano Controller?

The problem might be the result of a misconfiguration, lack of administrator privileges, domain controller, or something else. To walk through all these possibilities, go to Troubleshoot Authentication and Directory Service Problems.

What credentials do I use to connect my the Pano Controller to Active Directory (AD)?

You must use a username that has at least read access to the AD tree. The username must also have a complete UPN format (User Principal Name) specified in its user container. For instructions, go to Connect Pano Controller To Directory Services.

Why can’t I browse the hierarchy even though my the Pano Controller is connected to Active Directory (AD)?

Check the log by clicking the Log tab to see if there is a `PartialResultException` error or a `Referral` error. If there are errors present it might be necessary to specify the Global Catalog port at the end of the url string, e.g, ldap://ad.acme.com:3268. 3268 is for normal LDAP, 3269 is for secured LDAP.

If you are able to successfully connect and browse the AD hierarchy after specifying the Global Catalog port, the problem might be due to one of the following issues:

- **PartialResultException Errors**: The domain the Pano Controller is on cannot reach the domain configured in the setup page. You can resolve this by setting the domain servers to refer to each other.
- **Referral errors**: The AD host cannot communicate with another host it was referred to during the communication over LDAP because of the following possibilities. Either the referred to host does not exist, cannot be reached, is behind a firewall, or the user account provided in the setup page does not have access to read certain information. If you have a complex AD server configurations with multiple domains or sub-domains and shared groups (security or distribution) and you want to remove the Global Catalog port, you must identify the issue and fix it.

VMware View FAQs

- I'm using VMware View as my connection broker. What does `VMWare VDM: Cannot contact VDM server` mean?
- Why is there no indication that VMware View is connected?
- I'm using the VMware View as my connection broker. Why do I get a `time out` error message?

I'm using VMware View as my connection broker. What does `VMWare VDM: Cannot contact VDM server` mean?

You can use VMware View as your connection broker (Install and Configure Pano Controller on VMware vSphere). Sometimes a user can get a `VMWare VDM: Cannot contact VDM server` error, when a user tries he to log in. There are two possible reasons for this error.

- SSL not enabled.

To verify, go to https://***ip-address-of-vmview-server***. If you don't see a login page, it means that SSL is not enabled.

To enable SSL, go to http://***ip-address-of-vmview-server***/admin and log in as administrator. Click **Configuration** and edit the Global Settings. Select the **Require SSL for client connections** check box, click **OK**, then log out. Restart your VMware View server, go to https://***ip-address-of-vmview-server***/admin, then log in as administrator to verify the change.

- RDP not enabled. For instructions, go to Connect Pano Controller To VMware View.

Why is there no indication that VMware View is connected?

Currently there is no indication as to whether VMware View is connected or not when you configure VMware View via the Pano Controller. However, the virtual machines appear in DVMs tab once users log on from a Pano System Endpoint.

I'm using the VMware View as my connection broker. Why do I get a `time out` error message?

You'll receive such a VMware View server communication failure if you do not have VMware View enabled for direct connections. Go to Enable Desktop Connections from Pano Devices.

Windows 7 FAQs

- What versions of Windows 7 does the Pano System support?
- Can I use Windows XP with our Windows 7 DVMs?
- How long will Pano Logic support Windows XP on DVMs?

- Are there any Pano Logic pricing changes when using Windows 7?
- Can I switch between user accounts from my Windows 7 DVM?

What versions of Windows 7 does the Pano System support?

The Pano System supports specific editions. For a list, go to Windows 7 Support.

Can I use Windows XP with our Windows 7 DVMs?

Yes. Pano Logic will continue to support the Windows XP versions outlined in Windows XP Support as a DVM virtualized operating system in Pano System v5.0.

To help your migration from Window XP to Windows 7, take advantage of the multi-DVM capability as outlined in Define Collection Type–VMware and Hyper-V.

How long will Pano Logic support Windows XP on DVMs?

We haven't determined which Pano System release would no longer support Windows XP, but we recognize that it will take our customers some time to migrate off Windows XP. At this time, we do not have a planned date or version when we will drop support for Windows XP. We will continue to monitor use of Windows XP by our customers and provide adequate notice of a change in our support of Windows XP.

Are there any Pano Logic pricing changes when using Windows 7?

No there isn't any difference in Pano System pricing or licensing for DVMs used with Windows 7 vs. Windows XP.

Can I switch between user accounts from my Windows 7 DVM?

Yes. But, there are some limitations as outlined in Limitations to Fast User Switching.

XenDesktop FAQs

- Is Citrix NetScaler required?
- Can I use a non-Citrix load balancer?

Is Citrix NetScaler required?

Citrix NetScaler is not a required component. However, you might consider using Citrix NetScaler for redundancy and scalability:

- **Redundancy** – Pano Controller will only connect to one address. If that address resolves to only one XML service, then that XML service is a single point of failure. If you want redundancy, you can deploy multiple XML services and place a load balancer (like NetScaler) in front of them.
- **Scalability** – the XML Service will be able to service some maximum number of requests. If your deployment is very large, it might overload the XML service, or response times might become unacceptably long. In this scenario, multiple XML services can be deployed with a load balancer in front to distribute the queries. Thus, scale will increase.

Can I use a non-Citrix load balancer?

Yes. However, it must properly balance/route SOAP/XML calls. Moreover, it must be configured properly (see Configure NetScaler to Monitor XenDesktop Controllers).

Can I have multiple instances of Citrix NetScaler?

No. The Pano System does not support multiple instances of Citrix NetScaler.

Licensing FAQs

- What is the new licensing system?
- What Does it Control?

- How does it work?
- Why is broader licensing technology being added to Pano System 6.0?
- What activities/capabilities are controlled by licensing?
- What do licenses cover?
- If you buy a license for Pano Virtual Client and the license expires in a year do you end up with a license in a violation state?
- What starts the clock on the 60-day unlicensed period for Pano Virtual Client?
- When you are in the 60-day Pano Virtual Client grace period is there any restriction on the number of concurrent Pano Virtual Client sessions you can run?
- When a user is trying to use Pano Virtual Client and their session is the one that is in excess of the licensed number, what do they see?
- If the Pano Virtual Client session limit is exceeded, what notifies the admin?
- If a customer tries out Pano Virtual Client without licensing it, after 60 days pass are they then blocked from ever trying Pano Virtual Client again?
- What types of product licenses are available?
- What does Device-based and concurrent user mean?
- What types of maintenance rights are controlled by licenses?
- Are there any products or services that don't require license keys?
- Are licenses tied to a specific Pano Zero Client?
- Is there a grace period before you must load a license key?
- What happens when a license limitation is violated or expires?
- How are upgrades controlled by licenses?
- How do customers with multiple sites use the new licenses?
- When are license keys created?
- How do customers get license keys?
- How do customers load license keys?
- Who do licenses get emailed to?
- Will existing customers already have license keys?

What is the new licensing system?

New more comprehensive licensing rules, a new License Manager UI in Pano Controller/Maestro, and a new license key file format

What Does it Control?

Ability to apply upgrades to Pano Controller and time-limited subscription licenses for the new Pano Virtual Client.

How does it work?

It uses license key files, one per customer, which are downloaded from the Pano Logic Customer Center (customer.panologic.com). Customers have a 60-day grace period before they must load a license key file after Pano Controller installation or first use of Pano Virtual Clients.

Why is broader licensing technology being added to Pano System 6.0?

With the introduction of Pano Virtual Client we are starting to offer software-only solutions that don't include or require a specific hardware endpoint. In the future we are planning on offering additional Pano System capabilities. To control the use of these software-based capabilities as well as ensuring compliance with maintenance policies we've added stronger licensing starting with Pano System 6.0.

What activities/capabilities are controlled by licensing?

The following are controlled by licensing in Pano System 6.0: ? Upgrading the Pano Controller appliance. ? Backup and restore between different versions of the Pano Controller database. ? Running Pano Virtual Client software.

What do licenses cover?

Each customer will be issued a single license key file that covers all of the products and maintenance purchased from Pano Logic. Within the license key, two kinds of capabilities are listed: ? Enable entitlements that govern the use of a software or hardware endpoint or accessory. ? Upgrade entitlements that govern the ability to upgrade Pano Controller.

If you buy a license for Pano Virtual Client and the license expires in a year do you end up with a license in a violation state?

No.

What starts the clock on the 60-day unlicensed period for Pano Virtual Client?

The first time the Pano Controller discovers a Pano Virtual Client.

When you are in the 60-day Pano Virtual Client grace period is there any restriction on the number of concurrent Pano Virtual Client sessions you can run?

There is no limit.

When a user is trying to use Pano Virtual Client and their session is the one that is in excess of the licensed number, what do they see?

The client will see an error when they try to login. The message will read "No valid licenses are currently available for Pano Virtual Clients. Please contact your system administrator."

If the Pano Virtual Client session limit is exceeded, what notifies the admin?

If the limit is exceeded, the license state becomes violation. Emails will be sent and alerts will be displayed at login time. Messages will be logged and the License Manager UI will turn red in the corresponding fields.

If a customer tries out Pano Virtual Client without licensing it, after 60 days pass are they then blocked from ever trying Pano Virtual Client again?

Yes, they are blocked from ever trying Pano Virtual Client again, unless they deploy a new Pano Controller.

What types of product licenses are available?

Currently all Pano Logic products and support services are only licensed in one way for each SKU. These licenses cover the use of both the endpoint hardware or software and the centralized Pano System (Pano Controller and Pano Maestro) software and are of two types: ? Perpetual device-based licenses ? for Pano Zero Clients and Pano Remote USB Keys. ? Subscription-period concurrent user licenses ? for Pano Virtual Client, typically for one year periods although longer licenses are available on request

What does Device-based and concurrent user mean?

Device-based means the license is tied to the use of a device, such as a Zero Client. Concurrent user means the license is for one active concurrent use and is not tied to a specific endpoint installation, serialized hardware product, or named user.

What types of maintenance rights are controlled by licenses?

License keys can control upgrade entitlements, also referred to as Maintenance rights. Maintenance rights can be purchased multiple ways including: * Bundled with the initial product purchase (1 year of maintenance is included in the purchase of a Pano System seat) * From a subsequent Maintenance renewal or extension * As a component of the Premium Maintenance and Support subscription or renewal

Are there any products or services that don't require license keys?

Yes ? some products don't require license keys such as physical hardware like VESA monitor mounts. Some services, such as Advance Warranty Replacement or Per Incident Support, also don't require license keys as they don't impact maintenance and upgrade rights.

Are licenses tied to a specific Pano Zero Client?

No ? licenses, even when device-based, aren't locked to specific Pano hardware. Customers can freely swap out Zero Client hardware without needing to change their license keys.

Is there a grace period before you must load a license key?

Yes ? customers can run in an UNCONFIGURED state without loading a license key file for up to 60 days. During that period the product will be fully functional but warning messages will be displayed to the administrator in Pano Controller. Even with this grace period we recommend that existing customers obtain their new license key file (see Q-16 below) before upgrading to Pano System 6.0.

What happens when a license limitation is violated or expires?

When a licensed quantity is exceeded or a license is within 60 days of expiring the administrator will see warnings displayed in Pano Controller. Operation of Pano Zero Clients will never be blocked by the 6.0 licensing. Use of Pano Virtual Clients will be stopped when their licenses expire or for concurrent connections over the licensed number.

How are upgrades controlled by licenses?

Maintenance coverage must exist in the loaded license key for all deployed Zero Clients before upgrades to Pano Controller are allowed. To cover upgrade done by backup and restore of the Pano Controller database, those activities between different Pano Controller versions are also controlled by licensing.

How do customers with multiple sites use the new licenses?

License can cover multi-site deployments of Panos provided that the sites are linked by a common Pano Maestro instance. Currently we do not directly support sharing licenses across multiple unlinked sites. However as licenses aren't restricted to one-time use a customer with multiple unlinked sites could load their single license file at each site.

When are license keys created?

Generally an update license key file will be generated and emailed to a customer (or the designated licensing contact) each time an invoice is generated for a licensed product or service.

How do customers get license keys?

Customers can also go to the Pano Logic Customer Center (at customer.panologic.com) and manually download their most recent license key file.

How do customers load license keys?

The new License Manager console in Pano Controller 6.0 is used to load license key files or check the status of licenses. This UI shows both products and services they are licensed for along with the current usage.

Who do licenses get emailed to?

Licenses are mailed to the designated?End Customer Sys Admin? contact for the customer. This may be the IT staff member responsible for the Pano deployment or it may be a reseller contact if you provide that level of support services for your customers. If you wish to be designated as the licensing contact for your customers please contact Customer Support.

Will existing customers already have license keys?

License keys issued with Pano System 5.0 are no longer valid and need to be replaced by the new format license keys. Customers (or the reseller supporting them) will need to go to the Pano Logic Customer Center (at customer.panologic.com) and select the Get License option from the menu.

Appendix: Known Issues

ID 1799

Description: For Windows XP, Pano Direct does not interoperate with Windows Remote Assistance.

Workaround: Use SMS Remote Control or DameWare Mini Remote Control.

ID 2377

Description: When an end user is connected to a desktop virtual machine configured for Pano Direct, the first click of the mouse in the vSphere Client (vSphere Client) console causes the end user's mouse to jump to that position. Subsequent movements and clicks of the mouse in the console do not affect the end user's mouse.

Workaround: The administrator should not move the mouse into the console area of the vSphere Client when the Pano lockout screen is displayed. The Pano lockout screen is completely static, so there is no need to control the mouse when this screen is being displayed.

ID 2383

Description: When one user is connected to a desktop virtual machine (DVM) that is part of a User Based Collection using Remote Desktop Connection and another user connects to the same virtual machine, the second user will not be able to access the DVM.

Workaround: The first user should log off so that the second user can access the DVM.

ID 2425

Description: 3D screen savers might cause problems when used with Pano G1 Zero Clients.

Workaround: Use Group Policy to prevent use of 3D screen savers. The best screen saver for overall system performance is "Blank".

Workaround: Do not select the Full Screen option or press Alt+Enter when the command window is active.

ID 2487

Description: Copying directly between two USB mass storage devices results in an I/O error.

Workaround: Copy the files from the first USB device to the desktop or local drive and then to the second USB device.

ID 2590

Description: You might receive a "Stop 0x0000008E" error message when using Windows XP with security update 954211 installed. There is a known issue with the security update that is fixed by KB959252. If you encounter this problem, the Pano Direct Service (Pano Direct Service) will not start. The log file for the Pano Direct Service will indicate:

```
WARNING : AgentServer: Agent Server failed to start. Reason: win32k.sys hotfix
available at http://support.microsoft.com/kb/959252/ is required.:
AgentServer::startAgentServer: AgentServer
```

Workaround: Install the update KB959252 available at http://support.microsoft.com/kb/959252/.

ID 2650

Description: User settings made through the Pano Control Panel are not saved if the user does not have a User Principal Name (UPN) defined.

Workaround: Define a UPN for the user.

ID 2764

Description: Selecting ClearType font smoothing in Internet Explorer 7, Office 2007 or Windows Display Properties causes the color of characters to appear incorrectly when using Pano Direct.

Workaround: In the case of Internet Explorer 7 or Office 2007 applications, deselect this option. In Windows Display Properties, deselect font smoothing or set it to Standard.

ID 2820

Description: Transparent objects in PowerPoint 2003 appear as solid or striped objects when viewed in the main panel at 24-bit color depth when using Pano Direct.

Workaround: Configure your desktop virtual machine for 16-bit color. Transparent objects appear correctly in Slide Show and Slide Sorter views at any color depth setting.

ID 2656

Description: Occasionally the U3 Launchpad application used with some USB flash drives will not automatically start.

Workaround: Manually run the Launchpad application.

ID 2967

Description: The following dead keys do not work on UK Extended keyboard:

- grave + w, W, y, Y
- diaeresis + w, W, Y
- circumflex + w, W, y, Y
- acute + w, W

Workaround: There is no workaround.

ID 3147

Description: Import of OVF results in wrong virtual network adapter. If users of VMware Converter 4.0.0 or 4.0.1 upload OVF to ESX 3.5 the result is that users will import `pc32net` as the default network card for `eth0`. This is a bug in VMware Converter.

Workaround: Do one of the following:

- ssh to the Pano Controller VM and change the network configuration file from network adapter eth0 to E1000.
- Use vCenter Server instead of VMware Converter.

ID 3497

Description: If you insert more than one USB mass storage device (for example, a camera and USB key) into a Pano System Endpoint, the Pano System Endpoint detects them and you can use one device initially, but the USB connection drops. The time it takes for a device to lose the connection varies. The USB device, not the Pano System Endpoint, loses its connection to the USB subsystem.

Workaround: This behavior is the result of a USB Support limitation. For the workaround, go to the section Limitations to USB Device Support, and see bullet item: Inability to connect more than one mass storage device to a Pano System Endpoint or transfer data between such devices.

ID 3554

Description: When VMware View's **User must change password at next logon** option is enabled, DVMs in a VMware View collection type receive a `cannot login view: VMWare VDM {1}` error.

Workaround: There is no workaround. This is a valid option: users should receive a prompt to change the password.

ID 3831

Description: The combination of the following products produces a weird condition when viewing the Log tab within the Management User Interface (MUI):

- Pano Manager or Pano Controller (depending on version)
- Firefox 3.5.3
- FlashPlayer 10.0.32.18
- Adblock Plus 1.1.1 (http://adblockplus.org)

Adblock Plus is a Firefox Add-on that blocks ads from web pages. When viewing the Log tab with the above configuration, scroll bars for the window intermittently appear as you scroll around the screen. If you select a log item and highlight text in the Detail section, large portions of the window periodically black out.

Workaround: Disable Adblock Plus for the Management User Interface (MUI) URL and re-start the browser, or disable the **Show tabs on flash and java** in the Adblock Options menu.

ID 3961

Description: When you attempt to install Pano Dual Monitor over RDP returns the following error message:

```
Before installing DisplayLink Core software and drivers,
please install up-to-date OEM drivers for your PC's graphics
hardware. Please refer to the DisplayLink Core documentation
for further information.
```

Workaround: There is no workaround. Installing Pano Dual Monitor via RDP is not supported. To install Pano Dual Monitor, log on to the DVM directly, then follow the instructions in Configure & Manage Pano Zero Clients & Desktop Preferences.

ID 3972

Description: When Pano Dual Monitor USB adapter is connected through a powered hub (Belkin F4U016), the monitor displays lines/interference on the desktop.

Workaround: This is a third-party bug due to IP cores. There is no workaround.

ID 4335

Description: If VMware Tools service stops running on a DVM for any reason, the Pano Controller is unable to communicate with Pano Direct Service. Other symptoms include:

- DVM Tools State indicates `Not Running`.
- IP Address, DVM Name, Pano Direct Status, and Pano Direct Version columns are blank.

This issue is known, and Pano Logic is evaluating possible solutions.

Workaround: Restart VMware Tools. Go here.

ID 4359

Description: On Windows XP, the VMware network adapter (`vmxnet)` might appear as an ejectable device, causing users to mistakenly eject the network adapter when they actually intend to eject their flash drive. Ejecting the network adapter causes the DVM to be inaccessible and requires you to add the network adapter back to the DVM through the vSphere Client.

You can modify your virtual machines to remove the network adapter as an ejectable device by disabling the hotplug functionality. Disabling hot-plugability only affects virtual hardware.

Workaround: Diable hotplug functionality.

ID 4677

Description: There is no support for audio input (audio recording).

Workaround: This support is scheduled for an upcoming release. There is no workaround at this time.

ID 4932

Description: Disturbances are heard when playing audio, specifically mono files, on Windows Media Player with a Pano G2 Zero Client.

Workaround: Pano Logic is working with Microsoft to resolve this issue. There is no workaround at this time.

ID 4935

Description: Audio sometimes jumps ahead of video. In other words, audio and video are not in sync.

Workaround: There is no workaround at this time.

ID 5153

Description: A Pano G2 Zero Client does not recognize Olympus DS-4000 digital recorder.

Workaround: There is no workaround at this time.

ID 5241

Description: Pano Controller/Pano Manager Connector for Microsoft SCVMM does not work/connect if you use any port other than port 8100 to install SCVMM. In this case, you might see the following error:

```
2010-10-25 11:47:38 WARNING Failed to connect to the
virtualization manager at URL https://10.0.32.30 as user
"administrator@acme.local". Unable to connect to the
Virtual Machine Manager server SCVMMJO. The Virtual
Machine Manager service on that server did not respond.
(Error ID: 1602)
```

Workaround: Microsoft's default port for SCVMM is 811. Change the port to 8100.

ID 5329

Description: An end user’s mouse freezes during both Gmail/Gtalk and Skype audio calls when CPU is at 100%. This issue occurs with both wireless and wired mouses and using a variety of headphones and microphones.

Workaround: There is no workaround at this time.

ID 5344

Description: Turbo foot pedal (version.14) does not work on WIndows XP and Windows 7 DVMs with a Pano G2 Zero Client but does work with a Pano G1 Zero Client.

Workaround: There is no workaround at this time.

ID 5357

Description: Logitech illuminated keyboard lights up but none of the keys work when connected to either a Pano G2 Zero Client or a Pano G1 Zero Client.

Workaround: There is no workaround at this time.

ID 5404

Description: PDS disconnects randomly when an isochronous device is connected. This issue occurs with both WIndows XP and Windows 7 DVMs on either a Pano G2 Zero Client or a Pano G1 Zero Client.

Workaround: There is no workaround at this time.

ID 5442

Description: There are various issues with isochronous devices disconnecting when a Gtalk call is in progress. (To reproduce a disconnection, simply move the Gtalk window from the first window to the second window when a Gtalk call is active.)

- Mouse freezes when disconnecting the isochronous devices and reconnecting when a call is in progress. Typically this issue occurs in standalone mode.
- Microphone does not recover after disconnecting and reconnecting a USB headset.
- When a call is active, pressing the Pano button or removing the device and plugging it back in results in a headset recovery, but the quality of the audio is poor. If an end user removes and reconnects the device the audio recovers.
- When Gtalk call is active, sometimes the USB device does not recover completely after disconnecting and reconnecting and the call still shows active, resulting in the need to end the call.
- When a USB device is removed on the receiver's end, there is a noticeable humming sound. A reconnect returns the device to a normal state.
- When a call is active on both Pano System Endpoints, whenever there is a bad disconnection on the caller's end, two messages come up in the Gtalk window: first message on the receiver's end says “call ended” and second message on the caller's end says “incoming call”.
- Whenever there is a bad disconnection, the Pano System Endpoint takes a long time to recover and display the client UI.
- After a bad disconnection, a login takes longer than expected.

Workaround: Depending on the issue, a device reconnect might resolve the issue. Otherwise, there is no workaround at this time.

ID 5465

Description: Disconnecting and connecting a webcam when either IE and Windows Explorer are open causes the first monitor to hang. In this case, the second monitor is still functional and an end user can still drag applications across monitors. Mouse click operations work on second monitor, but not first. Also, the keyboard does not respond.

Workaround: Kill explorer.exe from the Task Manager or unplug the USB webcam.

ID 5467

Description: When an end user installs the Logitech API and driver on a Windows XP or Windows 7 DVM via either the Logitech CD or downloadable installer, the DVM status changes to unreachable.

Adobe ID FP-1068

Description: The `admin.jsp` page appears as a blank page when you try to access the Pano Controller via https. This problem does not occur with http. The problem is the result of a flash/browser incompatibility, specifically an expiration settings in combination with https. This is a known Adobe bug.

Workaround: Edit `/opt/atto/broker/web/WEB-INF/web.xml` and comment out the following section:

```
 <filter-mapping>
  <filter-name>NoCacheFilter</filter-name>
  <url-pattern>*.swf</url-pattern>
 </filter-mapping>

when commented out it should look like this:

<!--
 <filter-mapping>
  <filter-name>NoCacheFilter</filter-name>
  <url-pattern>*.swf</url-pattern>
 </filter-mapping>
-->
```