Study Guide

Microsoft 70-686

PRO: Windows 7 Enterprise Desktop Administrator

ExamForce

About the Exam

Six major topic areas make up the Microsoft Windows 7 Enterprise PRO 70-686 certification exam.

- Planning and Managing a Client Life Cycle Strategy
- Designing a Standard Image
- Designing Client Configurations
- Designing a Windows 7 Client Deployment
- Designing Application Packages for Deployment
- Identifying and Resolving Deployment and Client Configuration Issues

This guide will walk you through all the skills measured by the exam, as published by Microsoft.

Objectives

Chapter 1: Planning and Managing a Client Life Cycle Strategy.

Plan and manage client licensing and activation.
Plan and manage software updates.
Plan and manage a physical hardware and virtualization strategy.

Chapter 2: Designing a Standard Image.

Design an image creation strategy.
Design a custom image.
Define an image update strategy.

Chapter 3: Designing Client Configurations.

Design standard system settings.
Define client security standards.
Define Windows Internet Explorer settings.

Chapter 4: Designing a Windows 7 Client Deployment.

Analyze the environment and choose appropriate deployment methods.
Design a lite-touch deployment strategy.
Design a zero-touch deployment strategy.
Design a user state migration strategy.

Chapter 5: Designing Application Packages for Deployment.

Design a delivery or deployment strategy.
Manage application compatibility.

Chapter 6: Identifying and Resolving Deployment and Client Configuration Issues.

Identify and resolve Internet Explorer issues.
Identify and resolve Group Policy issues.
Identify and resolve networking issues.
Identify and resolve authentication and authorization issues.

Chapter 1 – Planning and Managing a Client Life Cycle Strategy.

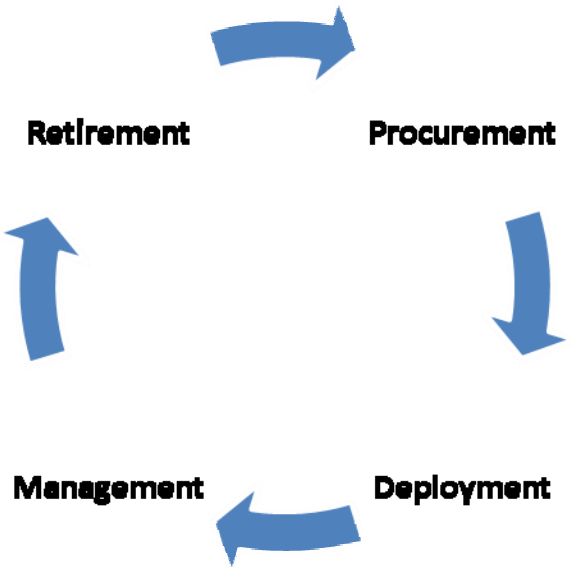
Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

There are 3 life cycles that are involved when considering the Pro: Windows 7, Desktop Administrator certification.

The first is the **Client Lifecycle**. It is made up of 4 areas listed as follows –

1. Procurement: Acquiring needed items from a vendor in an authorized way.
2. Deployment: Activates that make the system ready for use.
3. Management: Updating and supporting the system and the user community.
4. Retirement; The removal of old systems/software for production.



The second focuses on the **Hardware Lifecycle**. It is made up of 7 areas listed as follows –

1. Plan: The ability to understand where you are at and where you need to go. Includes demand forecasting, hardware selection, design configuration.
2. Buy: Acquiring the needed items from a vendor… See Client Lifecycle step 1.
3. Deployment: The rolling out of configuration items including but not limited to software, hardware, data migration. See Client Lifecycle step two.

4. Operate: This is all the tasks that go into making sure the configuration item is available. This would include facilities management, security management for the machines as well as the data, and IT administration.
5. Support: The day to day tasks that go along with managing user interaction with a system.
6. Upgrade: Rolling out a new version of the configuration item to the user population, be it software or hardware.
7. Retire: The removal of old configuration items, getting them picked up, data cleaned off of them, shipping and packaging.

The third and last lifecycle talked about is the **Desktop Deployment Lifecycle**. This life cycle looks at the task involved with a successful software or OS rollout.

The three items looked at are –

Planning – This looks at the business needs and determines if there is a good ROI.
Tasks include –
Organization readiness for desktop deployment
Verifying that you have the proper tools for the build and deploy phases
Listing expected deliverables

Building – This phase looks at getting the base image together and streamlining the installation process. Testing of the image before deployment.

Deployment - The rolling out of the solution to the user community.

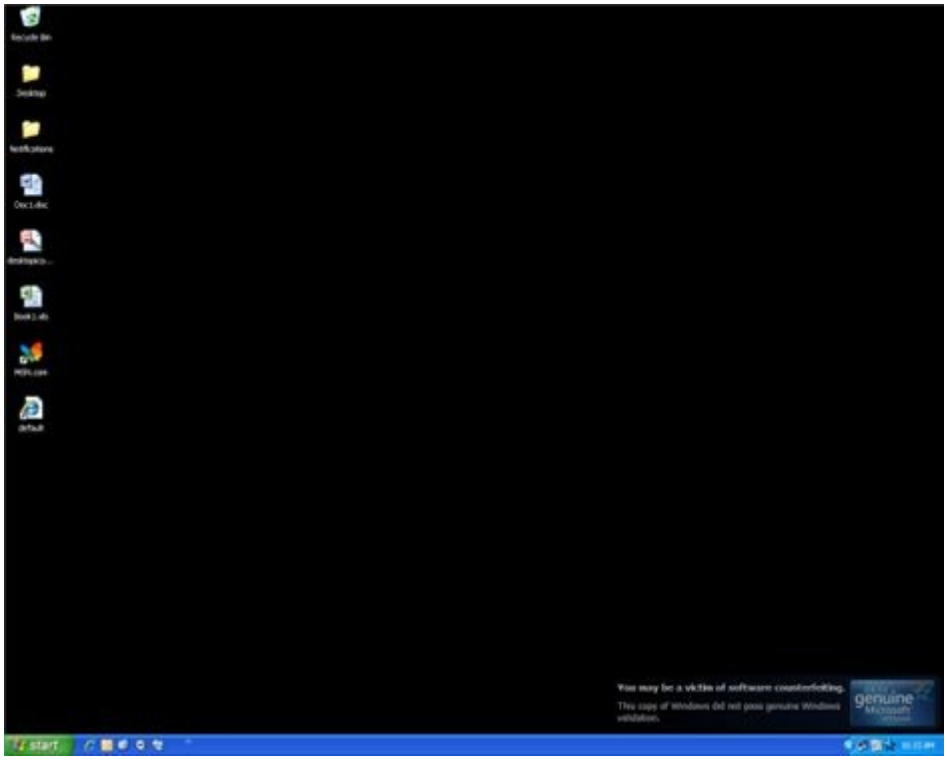
Plan and manage client licensing and activation.

All versions of Windows 7 and Server 2008 require activation. This is part of Microsoft's Windows Genuine Advantage.

There is a 30 grace period for Windows 7. After that the machine goes into *Persistent Notification* mode.

3 things happen in persistent notification mode –

Desktop background is black
Nag notifications
Only critical updates are installed



There are 3 methods for activation –

- Retail – you buy it at a retail store and it comes with one unique product key.
- OEM – resellers of machines that include a custom build OS. i.e. Dell, HP

- Volume Licensing – usually found in the Enterprise arena, these keys allow for multiple activations.
  VL uses 2 activations models –
  Multiple Activation Key – (MAK)
  Key Management System – (KMS)

MAK Model –

Company buys a pool of licenses, as machines activate against the pool the quantity of remaining activations goes down.

There are two ways to check the number of remaining activations –

- Microsoft Licensing Website - http://www.microsoft.com/licensing/

- Volume Activation Management Tool (VMAT)

There are two ways to activate machines using MAK

- MAK Independent Activation – Each machine activates its own license either by telephone or by the connection to the Internet. The way this works is that the MAK key is embedded in the system image on the MAK clients or is pushed from Microsoft out to the MAK clients. The clients connect directly to Microsoft and provide their hardware information and the product key. Microsoft and the clients exchange certificates and then Microsoft delivers the Conformation ID (CID) to active the MAK clients.

- MAK proxy – This allows for one connection to Microsoft to activate multiple machines. This method is configured through the use of VMAT. Do not use it in networks that have no connectivity to the Internet. The MAK Proxy gathers the Installation ID (IID) send this information to Microsoft. Microsoft then sends out the Conformation ID (CID) which is managed to the individual machines by the MAK Proxy.

http://technet.microsoft.com/en-us/dd936200.aspx
http://technet.microsoft.com/en-us/library/dd979805.aspx

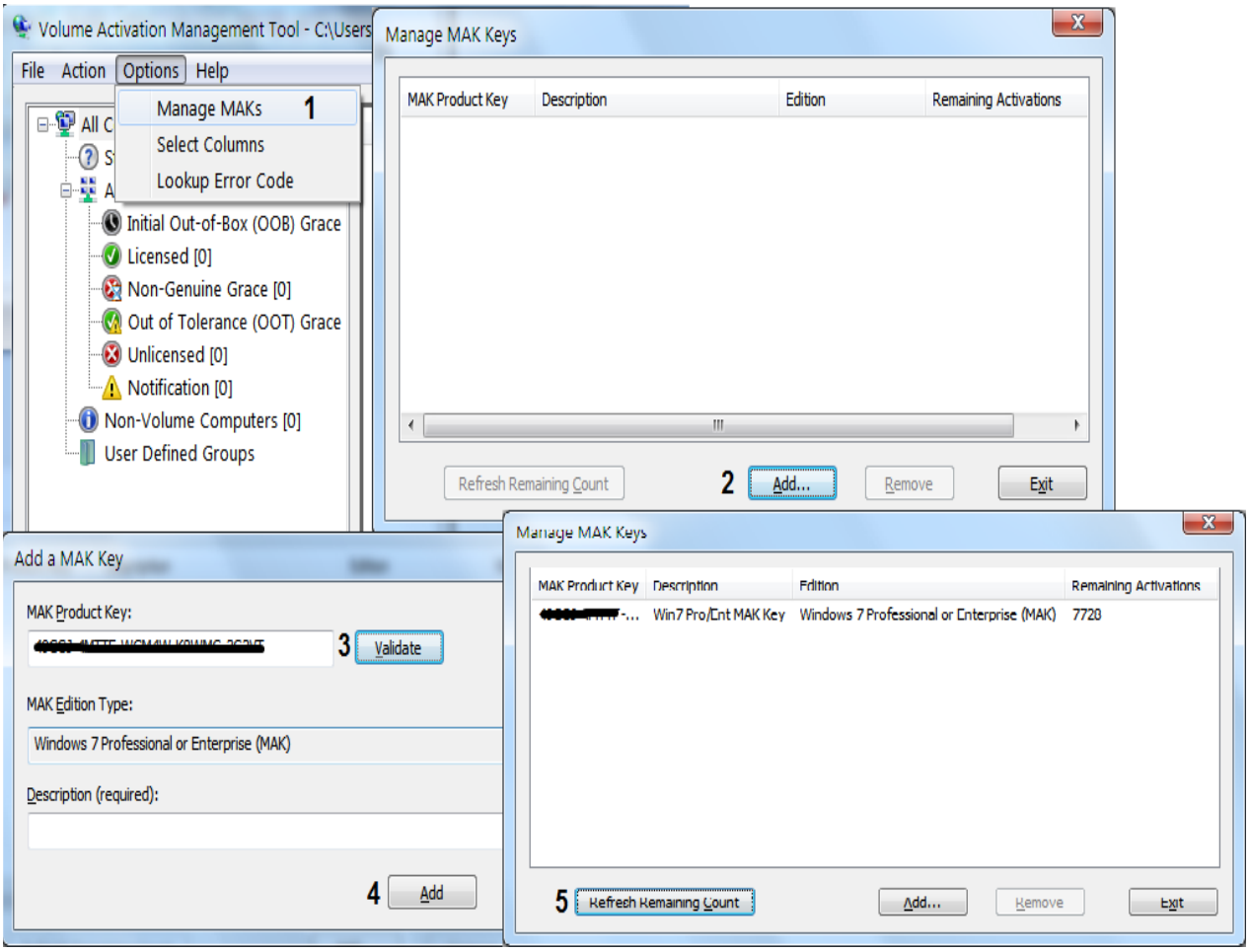
Main advantage of MAK is that it is “one time activation”. It does not require any further administrative effort unless there are “significant hardware changes”.

NOTE: The following website has information as to what are significant hardware changes. The site documents XP, however it should still be good for Windows 7.

http://aumha.org/win5/a/wpa.php

VMAT is a downloadable tool that comes in the Windows Automated Installation Kit. It allows for that allows multiple machines to activate through one connection. Management of specific groups of machines can be done based on the following specifications -

Active Directory Directory Services (AD DS)
Workgroup names
IP addresses
Computer Host name



Functionality delivered by VAMT is –

MAK Independent Activation management –This is when machines are sending their own IID and importing CID from Microsoft.

MAK Proxy Activation management –The machines are using a proxy to gather and manage their IID's and the CID's coming back from Microsoft.

Activation Status – To see what the activation status of managed machines on the network.

Reaming MAK Activations – How many activations there are left in the pool.

XML Imports/Exports – Allowing for management of machines in a disconnected network to manage.

Local Reactivation – Reactivation based on machine information saved in XML format so that machines do not need to send IID out to Microsoft again.

Configuration for KMS activation – The ability to convert MAK activations to KMS activations.

Common MAK Activation Issues –

Verify the activations status of the machine by looking for the "Windows is activated" message in the Windows 7 welcome center. You can also run the *Slmgr.vbs –dli* command at the command prompt.

Verify connectivity with the internet, or activate by phone.

If both the internet and phone activation fail contact Microsoft Activation Call Center.

If *slmgr.vbs –ato* returns an error, resolve the error message by running *slui.exe 0x2a 0x<error code>*

http://technet.microsoft.com/en-us/library/dd772270.aspx

KMS Model -

If all the machines in the organization connect to the company network then the Key Management Service can be used.

http://technet.microsoft.com/en-us/library/dd936199.aspx

In order for KMS to work the following need to be in place.

A machine will need to have a KMS key installed so that it can run the KMS host service. The key can be installed online or over the phone. This can be a machine that is running other services. Most organization will be able to function with only 2 KMS host machines, one primary and one backup. (Each KMS host machine can support hundreds of thousands of KMS clients.)

To enable the KMS functionality input the following at a command prompt with elevated privileges.

Cscript C:\windows\system32\slmgr.vbs –ipk <KMSKey>

The KMS Host machine then registers its service with the DNS server and publishes its existence in the SRV resource records.

The KMS clients will then query DNS to locate the KMS host service. The clients then send activation requests to the KMS host.

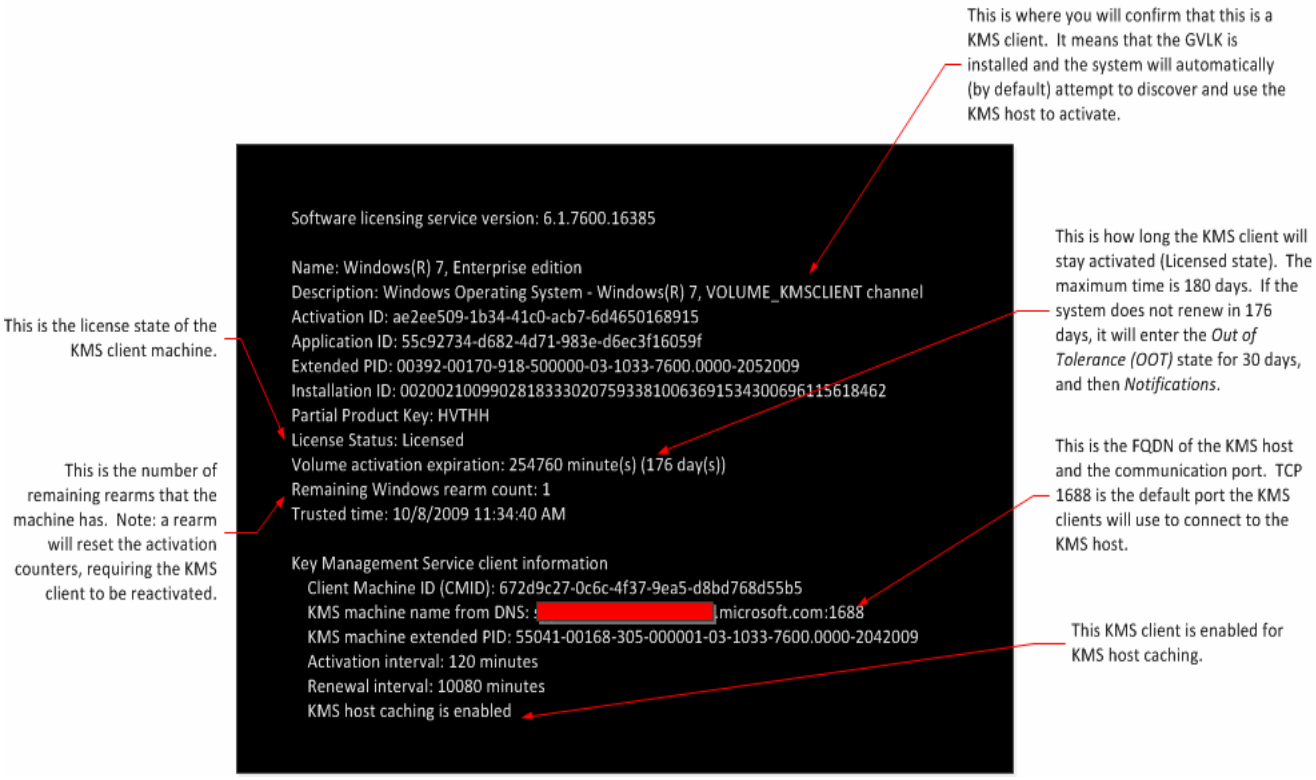
The KMS host keeps a count threshold per OS, and returns this information to the clients. If the count threshold is met then the clients activate.

Count threshold per OS -

Windows Vista – 25 physical machines
Windows Server 2008 – 5 physical machines
Windows 7 – 25 physical and virtual machines
Windows Server 2008 R2 – 5 physical and virtual machines

Activation issues –

- Clients that do not activate with the KMS host will try to connect every 2 hours until they activate.
- Clients must renew activation by connecting to the KMS host every 180 days.
- After activation clients will try to renew their activation every 7 days.



http://technet.microsoft.com/en-us/library/ee939272.aspx

Clients will connect using anonymous RPC over TCP/IP using the default port of 1688. KMS host and clients need to use VL media.

Common MKS Activation Issues –

- Verify the activations status of the machine by looking for the "Windows is activated" message in the Windows 7 welcome center. You can also run the *Slmgr.vbs –dli* command at the command prompt.
- Verify DNS is working properly and that the SRV resource records are updated to reflect the KMS Host location.
- Verify that the minimum number of clients are trying to activate
- Verify that TCP port 1688 is open
- Look for events in Windows Application even log.
    - Event ID 12288
    - Event ID 12289
    - Event ID 12290

If *slmgr.vbs –ato* returns an error, resolve the error message by running *slui.exe 0x2a 0x<error code>*

http://technet.microsoft.com/en-us/library/dd772270.aspx

Plan and manage software updates.

Understand the different tools that are available for application deployment. Specifically the following 4 -

- Configuration Manager
  - Create a package
  - Create a program for the package
  - Move the package to distribution points
  - Advertise the package

- Dependencies for Configuration Manager

Dependency	Consideration
Software distribution component configuration	The software distribution component settings must be configured
Advertise Programs Client Agent	The software distribution feature's client connection must be enabled
Distribution Points	At least one distribution point must be configured. By the default the site server has a distribution point site role enabled
Collections	This is the clients that the software distribution packages will be installed on
Package Access Accounts	This allows for the clients and administrators to access packages

- Group Policy Deployment
  - Create software distribution point
  - Create GPO for software distribution
  - Assign a package in the GPMC
  - Publish a package so that users can access it from Active Directory

- Dependencies needed for GPO Deployment

  - GPMC
  - AD
  - Clients that support Group Policy
  - Software that can be packages into MSI files
  - Proper permissions for access to the distribution point

- App-V (application virtualization)

  App-V allows for applications to be executed from the network, storage or a machine to provide dynamic allocation of recourses in real-time.

- TS RemoteApp

  RemoteApp allows access to applications through Terminal Services. Users have access to RemoteApp programs along with applications loaded on their desktop.

Plan and manage a physical hardware and virtualization strategy.

- Hardware Requirements for Windows 7
  - 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
  - 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
  - 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
  - DirectX 9 graphics device with WDDM 1.0 or higher driver

- All Windows 7 editions will support multiple core processors. Windows7 Pro, Ultimate, and Enterprise will support duel physical processers.
- BitLocker requires an USB or a TPM (Trusted Platform Module chip)
- Windows XP mode requires Windows 7 Pro, Ultimate, or Enterprise.

- Tools for doing a inventory of the IT infrastructure include
  - MAP, which does Hardware inventory, compatibility analysis, and readiness reporting
  - Configuration Manager 2007
  - Microsoft Desktop Optimization Pack

- Required Infrastructure for deploying desktops include

- Images that will range in size
- Gigabit switch network
- 100 MB ether connect minimum for one installation
- Windows Deployment Servers and storage servers

- Microsoft Virtual Desktop Infrastructure (VDI)

VDI allows for centralized desktop solutions that store and execute users desktop environments inside virtual machines. Users access the VDI with RDP. This allows the users to have the same interactions with the client desktops as they would if they had the desktop top loaded fat. The main consideration when deciding to deploy either physical or VDI is the bandwidth of the network.

http://blogs.technet.com/windowsserverexperts/archive/2010/01/12/microsoft-virtual-desktop-infrastructure-vdi-explained.aspx

Chapter 2 – Designing a Standard Image.

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Design an image creation strategy.

Image creation starts with the overall imaging process. This is defined as

- Envisioning phase where we look at what we want to accomplish putting together a project plan.
- Planning phase, where build our imaging lab and select an image strategy.
- Development phase where make the images and configure the builds to meet our strategy, configure the distribution points and capture our OS
- Stabilizing phase where we do our pilots and get ready for deployment
- Deployment phase, where we push the images that are accepted from pilot out to the user's desktops.

While the goal is to have a standard desktop that can be deployed to any machine we have in the environment, the reality for most organizations is that they maintain several desktop images.

Keep in mind that each image created will incur cost that will be associated with maintaining the image, storage of the image, testing and development of the image.

There are 3 basic kinds of images that we have to deal with.

- Thick images have everything that the users need. They are deployed in a single step. Some issues with this type of image is that they are not flexible. Take considerable amount of time to push to the client and may have applications that are not need by all users in the company.
- Thin images are images that contain OS and nothing else. They are cheaper to build and maintain then Thick images but they also require more steps to deploy as they do not contain core applications.

- Hybrid Image is where the OS gets pushed down to the desktop and then the applications are installed from a network location. Because the hybrid uses a thin image to drop the OS costs stay down and they are not as complex to build. However they do take longer to deploy then a thin image.

When designing an image strategy, give consideration to the following

- Geographic location can cause issues when trying to download across a slow wan link. Consider putting a image server at the remote location.
- Function-specific client requirements can also cause problems if there are areas in the organization that require special application loads. This can move you away from a monolithic image to more of a thin or hybrid image.
- Dual boot options will also cause issues for images, consider using a virtual environment if you need to run more than one OS on a machine.
- For the administrative side of the image, consider using group policy to manage OS setting, this will reduce the amount of images that you need to retain.

Design a custom image.

Creating a custom image will allow for the administrator to imbed required language packs, specific hardware drivers and requisite business unit applications.

All Windows 7 installs have a minimum of one language pack and language neutral binaries. Depending on the deployment of the desktop multilingual deployment needs may arise.

There are two multilingual deployment circumstances:

1. Deploying an image that contains multiple language packs but only one language pack can be activated as the default language. This is true of all Windows 7 versions except Ultimate and Enterprise. The other versions are known as single language editions.
2. Deploying a Multilingual image that lets the user move between on language and another. Only Ultimate and Enterprise will all more than one language pack to be active at a time.

WARNING: Things to watch out for on language packs.

1. Size of the image increases with each language added.
2. Cross-language upgrades are not supported. No upgrading from one default language to a different one.
3. The default language once chosen cannot be removed. SIDs are generated from the default language.

Installing device drivers for the devices that are supported in the enterprise such as printers and cameras are required. Having the correct network adapter device drivers for the chipset that the image is being pushed to is paramount.

Driver signing is required for 64-bit OS. It is still recommended for 32-bit.

Some best practice when managing device drivers are to

Mange multiple drivers by placing them in separate folders by category.

Do not over populate the diver folders with driver packages you don't need.

Think about using DPInst to selectively install non-critical drivers boot drivers from the network. That way only the drivers that needed for the hardware present is installed.

NOTE: DPInst can be downloaded in the Windows Driver Kit. This the version that this link points to is 7.1.0 and is only good as when Microsoft decides to change it.

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=36a2630f-5d56-43b5-b996-7633f2ec14ff

Applications can also be included in images, however applications can make the image bloat also causing the image to be unmanageable. Think about using a network share and a unattended answer file to in applications after the OS has been loaded.

If working with a non-networked environment use a configuration set that will copy all applications and drivers to removable media.

Create an application inventory that lists every application the organization has, then prioritize applications by need, use, age.

Creating categories for the application is also a benefit, knowing what applications that are core applications such as Microsoft Office and what is a supplemental applications like Spider Solitaire will help in building efficient images.

Define an image update strategy.

Servicing an image allows for the image to have the latest updates and fixes. There are three types of servicing methods.

- Offline servicing – changing the image without starting up the image.
- Windows Startup – uses a unattended answer file (UAF)
- Online servicing – Starting the system in audit mode and adding the needed drivers and fixes.

With offline servicing, using the Deployment Image Servicing and Management tool (DSIM) will allow for the administrator add needed files. There are two scenarios where offline servicing is useful.

Mount scenario – the administrator maintains master images for the environment.
Apply scenario – done when the image is being deployed.

```
Administrator: Command Prompt

C:\>dism /?

Deployment Image Servicing and Management tool
Version: 6.1.7105.0


DISM.exe [dism_options] {WIM_command} [<WIM_arguments>]
DISM.exe {/Image:<path_to_offline_image> | /Online} [dism_options]
         {servicing_command} [<servicing_arguments>]

DESCRIPTION:

  DISM enumerates, installs, uninstalls, configures, and updates features
  and packages in Windows images. The commands that are available depend
  on the image being serviced and whether the image is offline or running.

WIM COMMANDS:

  /Get-MountedWimInfo      - Displays information about mounted WIM images.
  /Get-WimInfo             - Displays information about images in a WIM file.
  /Commit-Wim              - Saves changes to a mounted WIM image.
  /Unmount-Wim             - Unmounts a mounted WIM image.
  /Mount-Wim               - Mounts an image from a WIM file.
  /Remount-Wim             - Recovers an orphaned WIM mount directory.
  /Cleanup-Wim             - Deletes resources associated with mounted WIM
                             images that are corrupt.

IMAGE SPECIFICATIONS:

  /Online                  - Targets the running operating system.
  /Image                   - Specifies the path to the root directory of an
                             offline Windows image.

DISM OPTIONS:

  /English                 - Displays command line output in English.
  /Format                  - Specifies the report output format.
  /WinDir                  - Specifies the path to the Windows directory.
  /SysDriveDir             - Specifies the path to the system-loader file named
                             BootMgr.
  /LogPath                 - Specifies the logfile path.
  /LogLevel                - Specifies the output level shown in the log (1-4).
  /NoRestart               - Suppresses automatic reboots and reboot prompts.
  /Quiet                   - Suppresses all output except for error messages.
  /ScratchDir              - Specifies the path to a scratch directory.

For more information about these DISM options and their arguments, specify an
option immediately before /?.

  Examples:
    DISM.exe /Mount-Wim /?
    DISM.exe /ScratchDir /?
    DISM.exe /Image:C:\test\offline /?
    DISM.exe /Online /?


C:\>
```

NOTE: DISM can be downloaded from here.

http://www.microsoft.com/downloads/details.aspx?FamilyID=886cd1dd-91aa-4bf4-8557-decedef7fa5d&displaylang=en

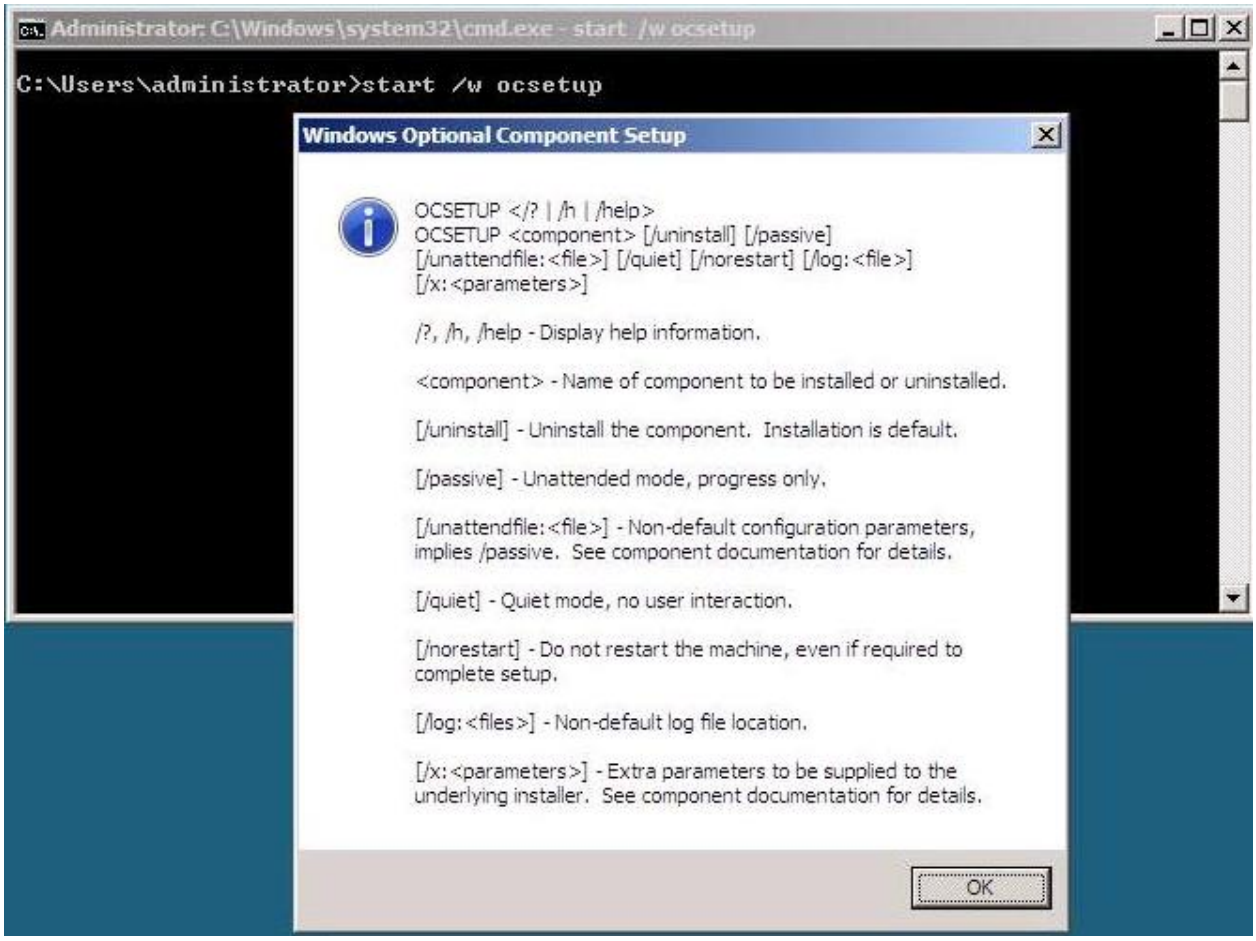
With online servicing the administrator starts the machine in audit mode. This will skip the welcome screen and allow for changes to the machine before it gets to its finale objective.

Servicing of the image in audit mode makes use of the following tools –

DSIM

```
Administrator: Command Prompt

C:\>dism /?

Deployment Image Servicing and Management tool
Version: 6.1.7105.0


DISM.exe [dism_options] {WIM_command} [<WIM_arguments>]
DISM.exe {/Image:<path_to_offline_image> | /Online} [dism_options]
         {servicing_command} [<servicing_arguments>]

DESCRIPTION:

  DISM enumerates, installs, uninstalls, configures, and updates features
  and packages in Windows images. The commands that are available depend
  on the image being serviced and whether the image is offline or running.

WIM COMMANDS:

  /Get-MountedWimInfo      - Displays information about mounted WIM images.
  /Get-WimInfo             - Displays information about images in a WIM file.
  /Commit-Wim              - Saves changes to a mounted WIM image.
  /Unmount-Wim             - Unmounts a mounted WIM image.
  /Mount-Wim               - Mounts an image from a WIM file.
  /Remount-Wim             - Recovers an orphaned WIM mount directory.
  /Cleanup-Wim             - Deletes resources associated with mounted WIM
                             images that are corrupt.

IMAGE SPECIFICATIONS:

  /Online                  - Targets the running operating system.
  /Image                   - Specifies the path to the root directory of an
                             offline Windows image.

DISM OPTIONS:

  /English                 - Displays command line output in English.
  /Format                  - Specifies the report output format.
  /WinDir                  - Specifies the path to the Windows directory.
  /SysDriveDir             - Specifies the path to the system-loader file named
                             BootMgr.
  /LogPath                 - Specifies the logfile path.
  /LogLevel                - Specifies the output level shown in the log (1-4).
  /NoRestart               - Suppresses automatic reboots and reboot prompts.
  /Quiet                   - Suppresses all output except for error messages.
  /ScratchDir              - Specifies the path to a scratch directory.

For more information about these DISM options and their arguments, specify an
option immediately before /?.

  Examples:
    DISM.exe /Mount-Wim /?
    DISM.exe /ScratchDir /?
    DISM.exe /Image:C:\test\offline /?
    DISM.exe /Online /?


C:\>
```

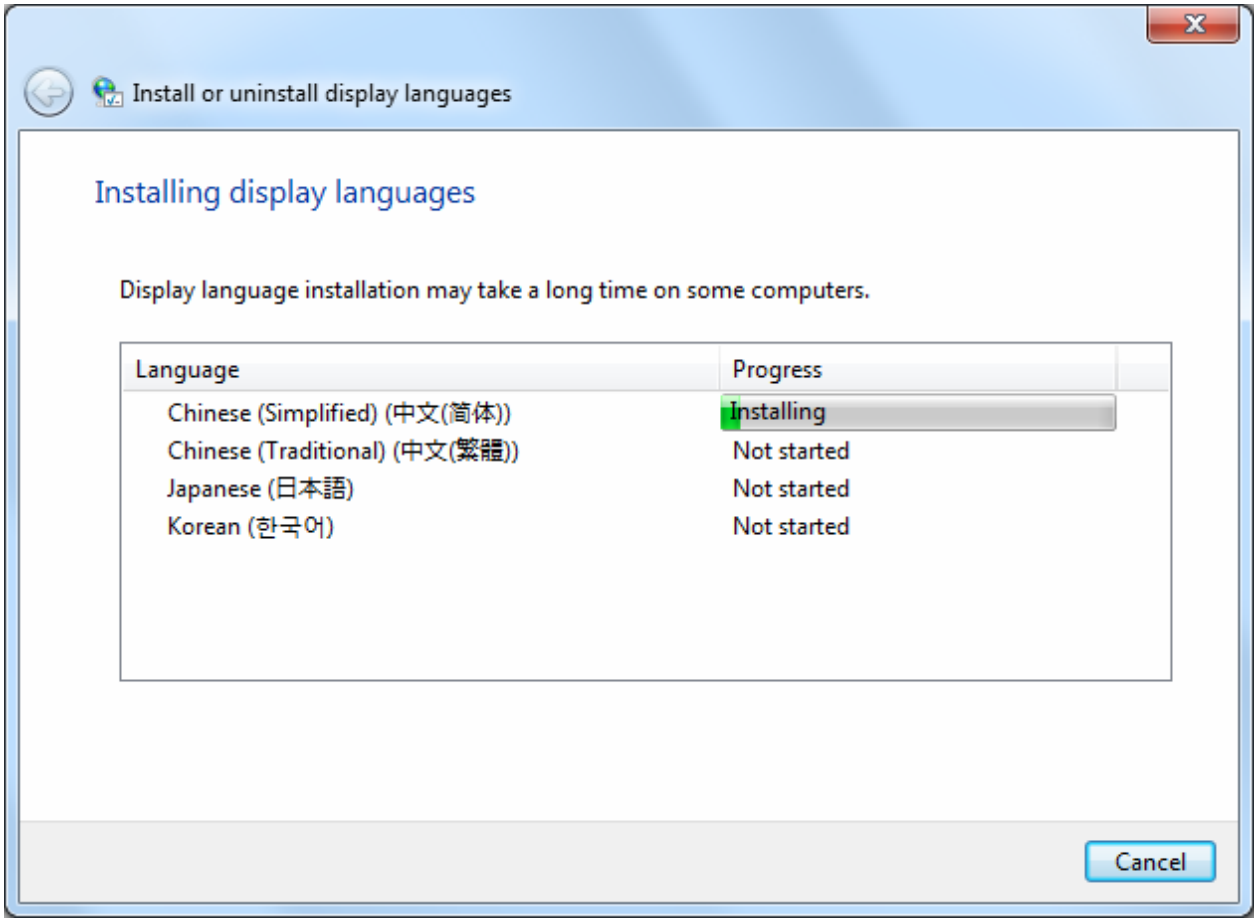
OCSetup


Administrator: C:\Windows\system32\cmd.exe - start /w ocsetup
C:\Users\administrator>start /w ocsetup
Windows Optional Component Setup
OCSETUP </? | /h | /help>
OCSETUP <component> [/uninstall] [/passive]
[/unattendfile:<file>] [/quiet] [/norestart] [/log:<file>]
[/x:<parameters>]
/?, /h, /help - Display help information.
<component> - Name of component to be installed or uninstalled.
[/uninstall] - Uninstall the component. Installation is default.
[/passive] - Unattended mode, progress only.
[/unattendfile:<file>] - Non-default configuration parameters, implies /passive. See component documentation for details.
[/quiet] - Quiet mode, no user interaction.
[/norestart] - Do not restart the machine, even if required to complete setup.
[/log:<files>] - Non-default log file location.
[/x:<parameters>] - Extra parameters to be supplied to the underlying installer. See component documentation for details.
OK

PNPUtil

```
Administrator: C:\Windows\system32\cmd.exe

Total attempted:              14
Number successfully imported: 14

C:\>pnputil -e
Microsoft PnP Utility

Published name :            oem0.inf
Driver package provider :   Microsoft
Class :                     Printers
Driver date and version :   06/21/2006 6.1.7600.16385
Signer name :               Microsoft Windows

Published name :            oem1.inf
Driver package provider :   Intel
Class :                     IDE ATA/ATAPI controllers
Driver date and version :   06/04/2009 7.0.0.1013
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem2.inf
Driver package provider :   Intel
Class :                     System devices
Driver date and version :   06/04/2009 9.1.1.1013
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem3.inf
Driver package provider :   Intel
Class :                     IDE ATA/ATAPI controllers
Driver date and version :   06/04/2009 9.1.1.1013
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem4.inf
Driver package provider :   Intel
Class :                     IDE ATA/ATAPI controllers
Driver date and version :   06/04/2009 9.1.1.1013
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem5.inf
Driver package provider :   Intel
Class :                     System devices
Driver date and version :   06/04/2009 1.0.0.0002
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem6.inf
Driver package provider :   Intel
Class :                     System devices
Driver date and version :   06/04/2009 1.0.0.0002
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem7.inf
Driver package provider :   Intel
Class :                     Universal Serial Bus controllers
Driver date and version :   08/20/2009 9.1.1.1020
```

LPKSetup


Install or uninstall display languages
Installing display languages
Display language installation may take a long time on some computers.
Language
Progress
Chinese (Simplified) (中文(简体))
Installing
Chinese (Traditional) (中文(繁體))
Not started
Japanese (日本語)
Not started
Korean (한국어)
Not started
Cancel

Chapter 3 – Designing Client Configurations.

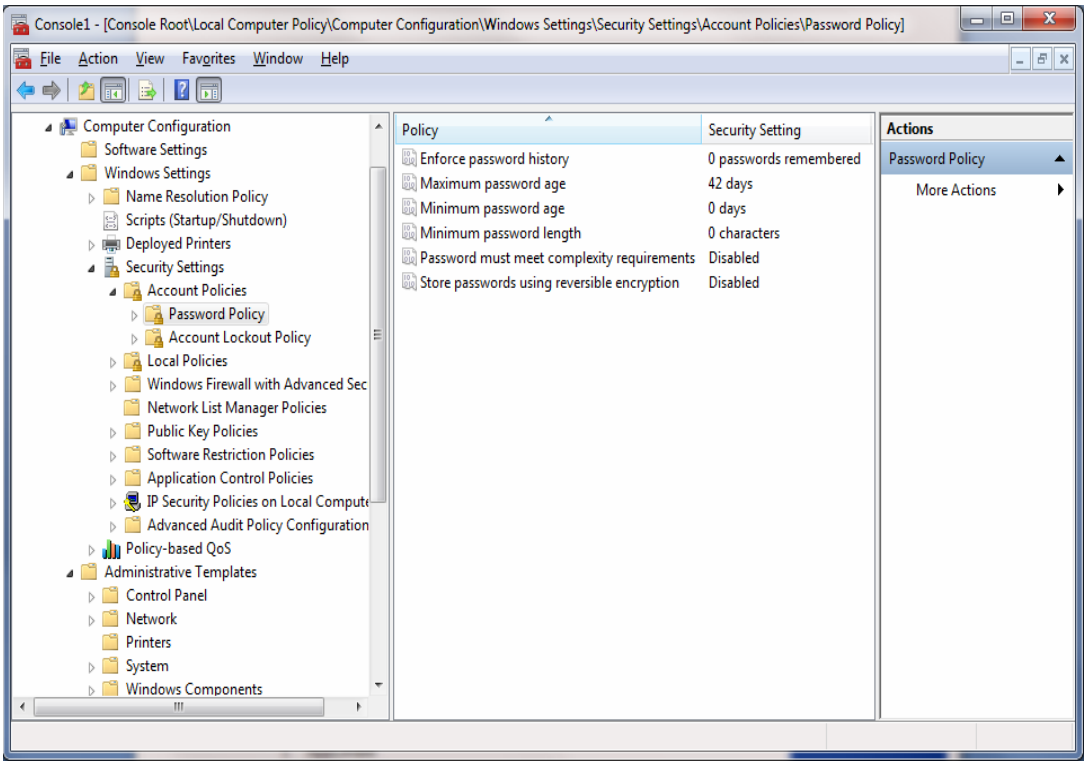
Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

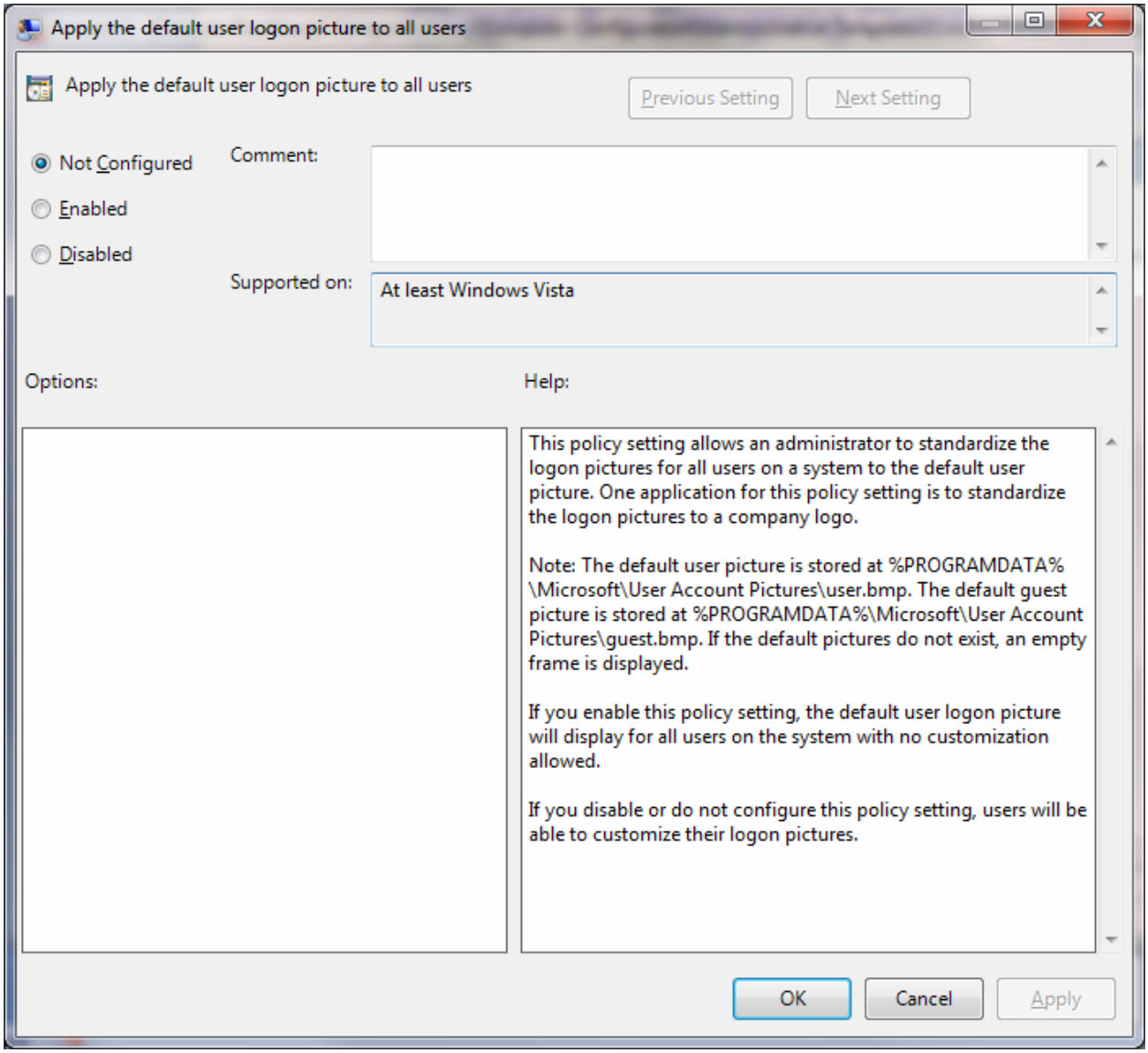
Design standard system settings.

Standard system settings are defined in the local group policy snap-in. Once the snap-in is added to the mmc there are settings for local machine and local user.

These setting can configure the control panel, printers,, windows explorer, desktop configuration, start menu settings, logon and security settings.



Settings can have configuration options and can also be enabled, disabled, or not configured.



Depending on how the machine will be used will determine the need to control the local machine.

NOTE: Most organizations will not waste their time controlling the local machine. They will apply GPO's to the Domain and OU structure.

Places that may have a local policy assigned are below.

Different manages scenarios are –

- Lightly Managed – this would be a machine where the user has a lot of control over the machine. An example would be a power user.
- Mobile - this would take in consideration users that have a laptop and need to synchronize documents with the production environment.
- Multi-User – Machines that are located in areas such as a library. Limited control is given to the system for things like wallpaper.
- AppStation – Specific business units applications would be loaded and the machine would be tightly controlled.
- TaskStation and Kiosk – Both machines would be tightly controlled and may not standard users to change anything.

Define client security standards.

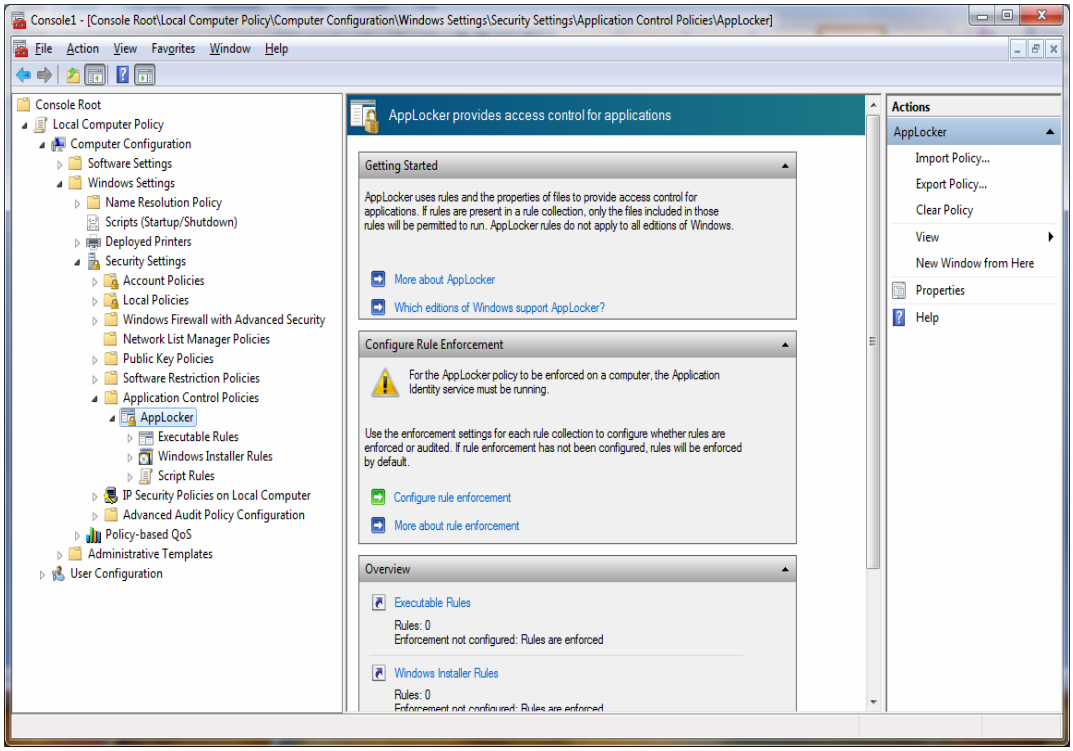
Microsoft has provided security benefits for Windows 7 –

1. AppLocker
2. UAC
3. BitLocker
4. Windows Firewall

AppLocker –

Because more applications are being built that do not need administrator privileges, users are able to get around desktop control. AppLocker makes applications control simple to use and manage.

AppLocker allows for multiple, and independently configurable rules for executables, installers, scripts and Dlls.

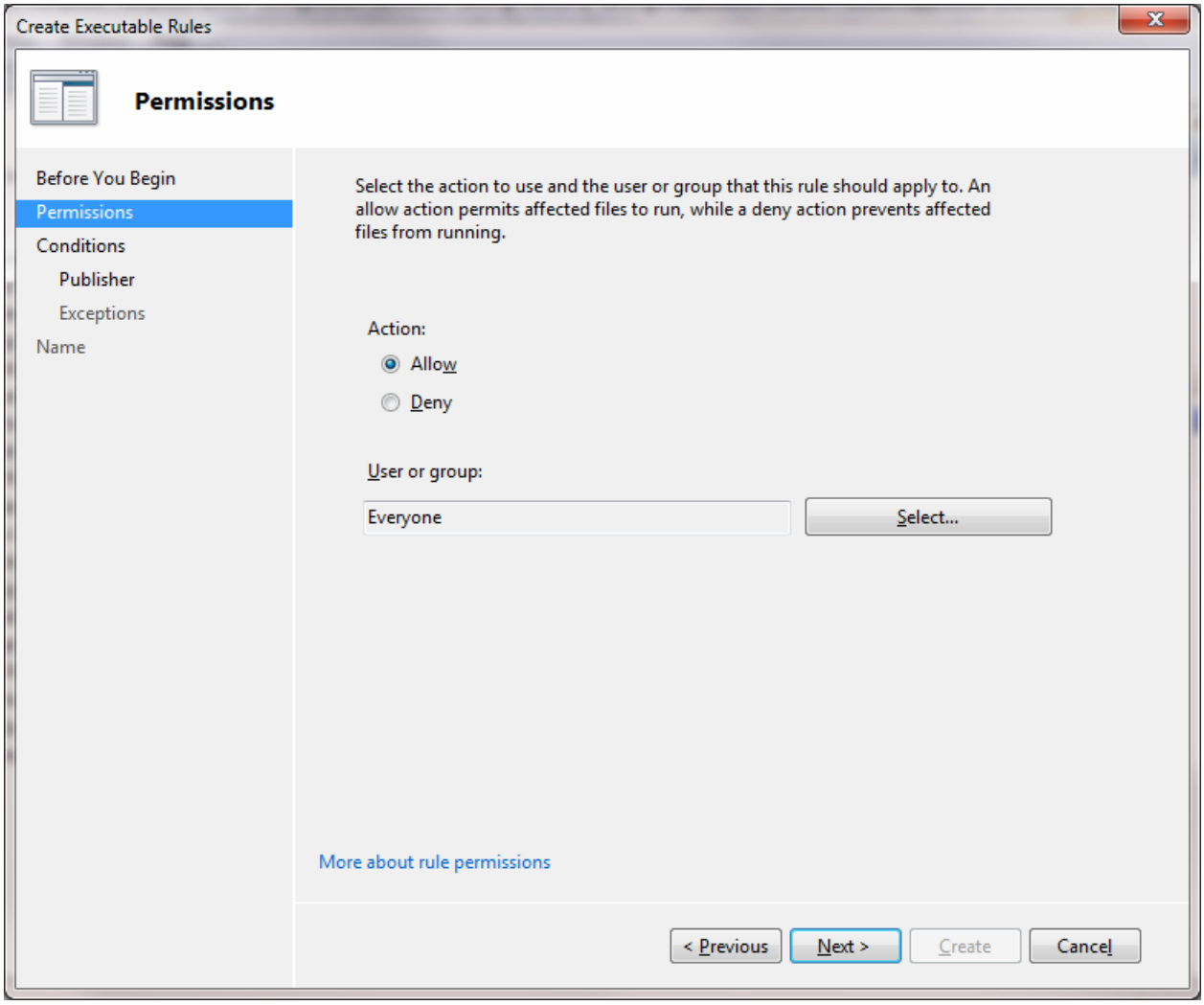


AppLocker has 3 rule types –

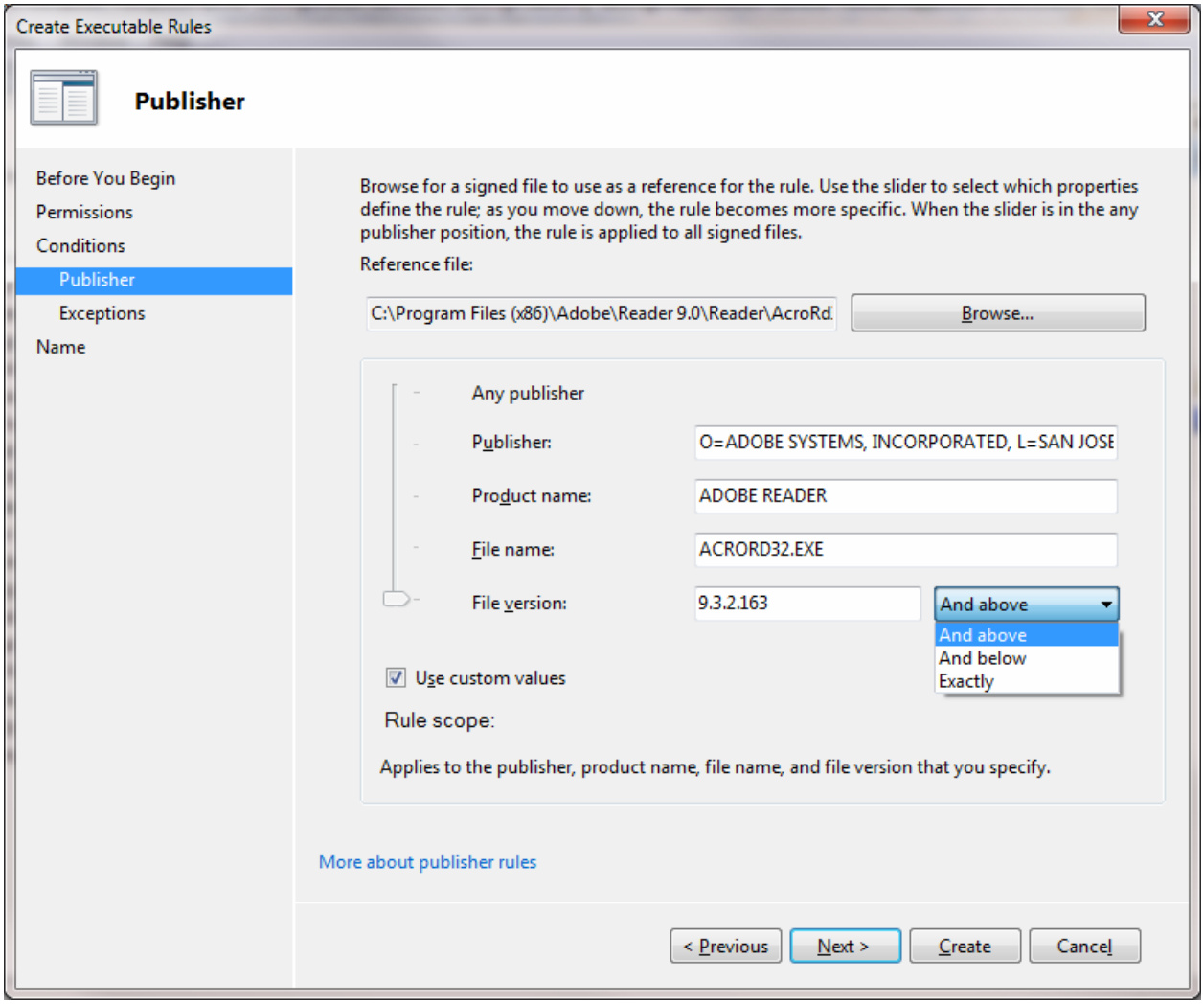
Allow – allow rules match applications to a known good list and allow execution of the applications on the list and block everything else.

Deny – deny rules allow the execution of all applications that are not on the deny list.

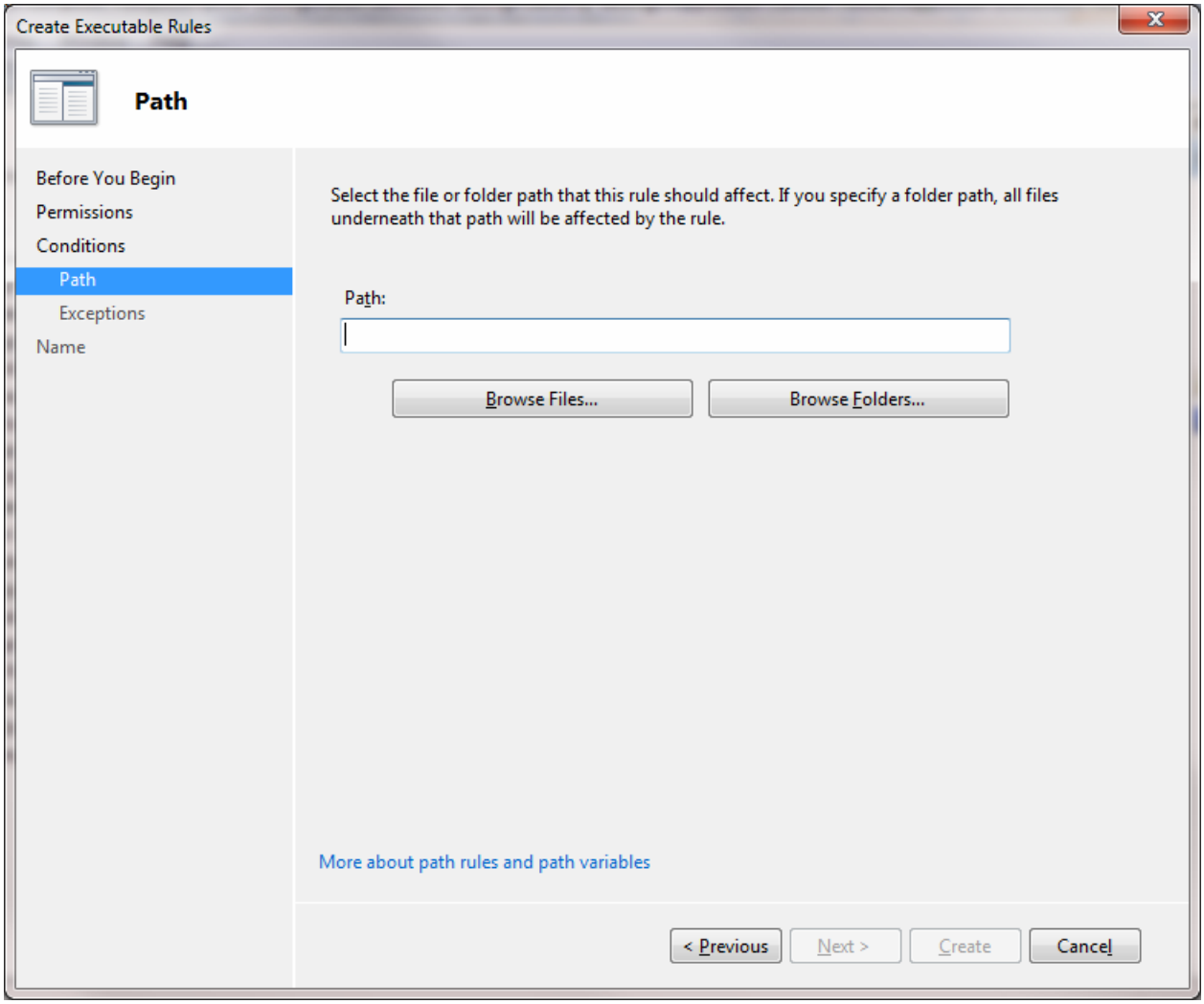
Exceptions – exception rules allow for the exclusion of files from a allow or a deny rule that would be included in that rule. Using exceptions allow rules can be created and specific applications can be removed from individual users or groups.



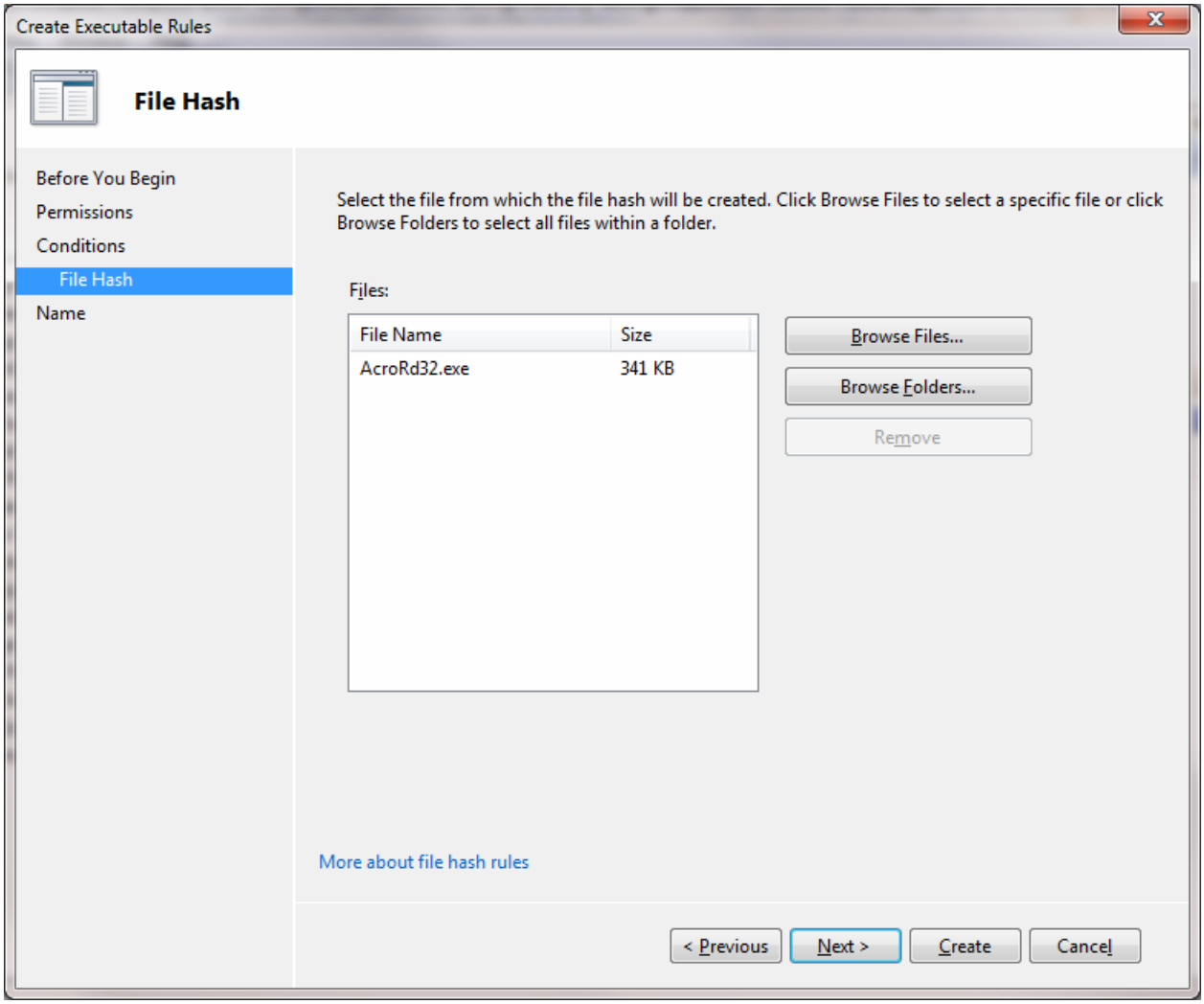
Publisher rules are based on digital signature of an applications. This lets the administrator to create rules for applications that will endure updates made by the vendor. This is done based on applications attributes.


Create Executable Rules
Publisher
Before You Begin
Permissions
Conditions
Publisher
Exceptions
Name
Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.
Reference file:
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd
Browse...
Any publisher
Publisher:
O=ADOBE SYSTEMS, INCORPORATED, L=SAN JOSE
Product name:
ADOBE READER
File name:
ACRORD32.EXE
File version:
9.3.2.163
And above
And above
And below
Exactly
Use custom values
Rule scope:
Applies to the publisher, product name, file name, and file version that you specify.
More about publisher rules
< Previous
Next >
Create
Cancel

Path rules will apply to all files under the path given.



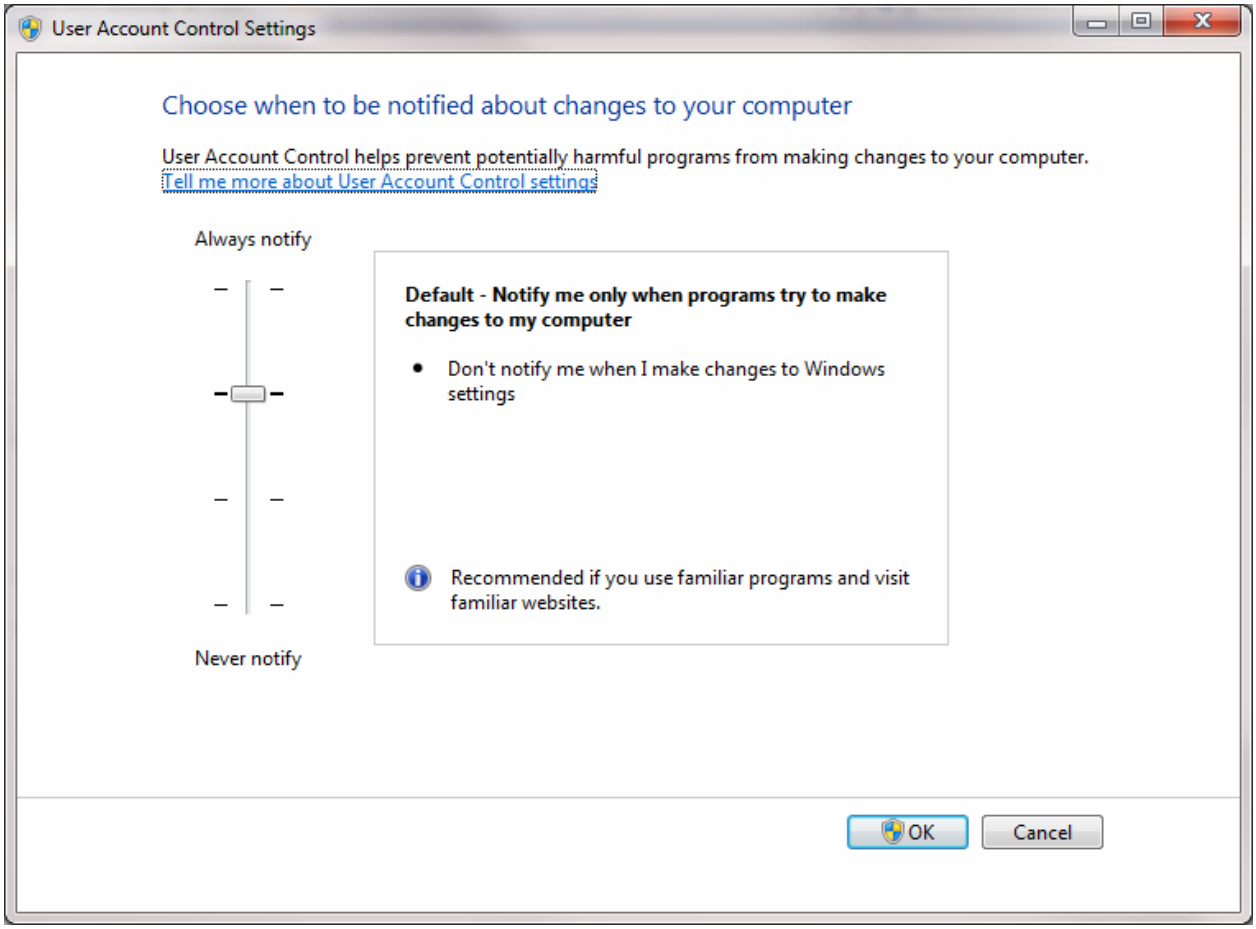
File hash will make a hash of any file added to the list, if the file changes then it will not run because the hash will change.



User Account Control –

UAC was introduced in windows Vista. It allows for the standard user to be controlled in how they access the system.

The change in Vista to Windows was the amount of notifications and what a standard user can do to the machine environment without getting a notification.



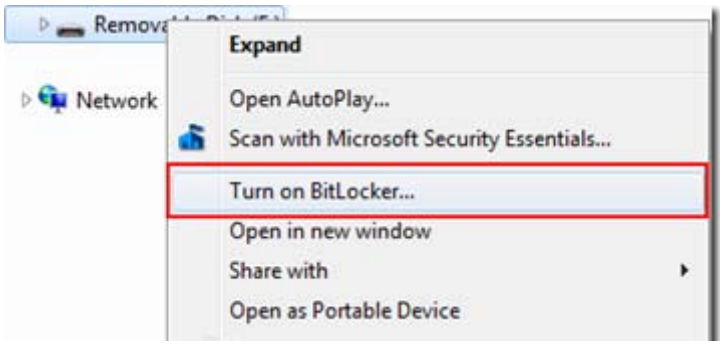
BitLocker Drive encryption

BitLocker is full disk encryption for a system. This helps protect data stored on a drive from being lost, stolen or tampered with.

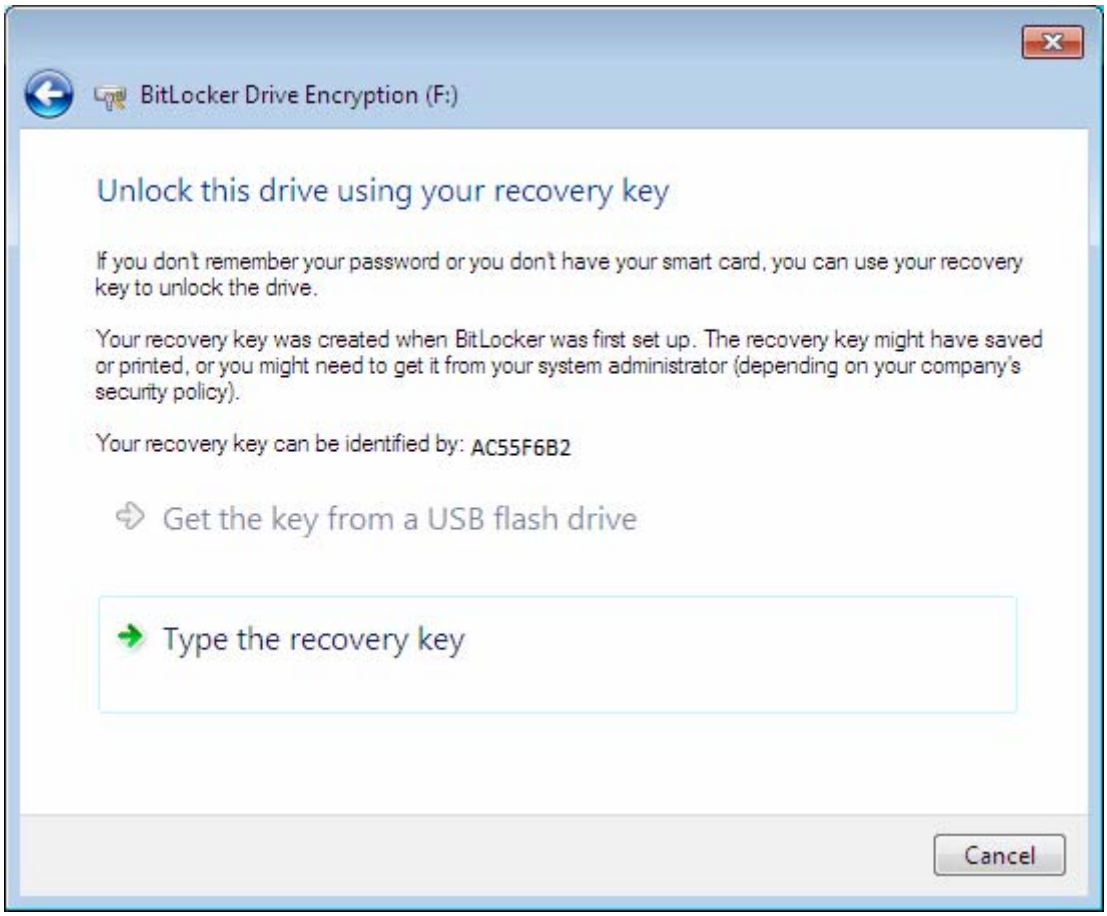
Bitlocker runs in two modes

1. Machines running a Trusted Platform Module chip (TPM) chip. This is used by windows to validate the boot components and BIOS have not been modified from the time the drive was locked using BitLocker
2. The other way is with a USB flash device. The encryption key is not stored in the TPM chip but on the flash drive. The USB device must be present every time the drive is unlocked for use.

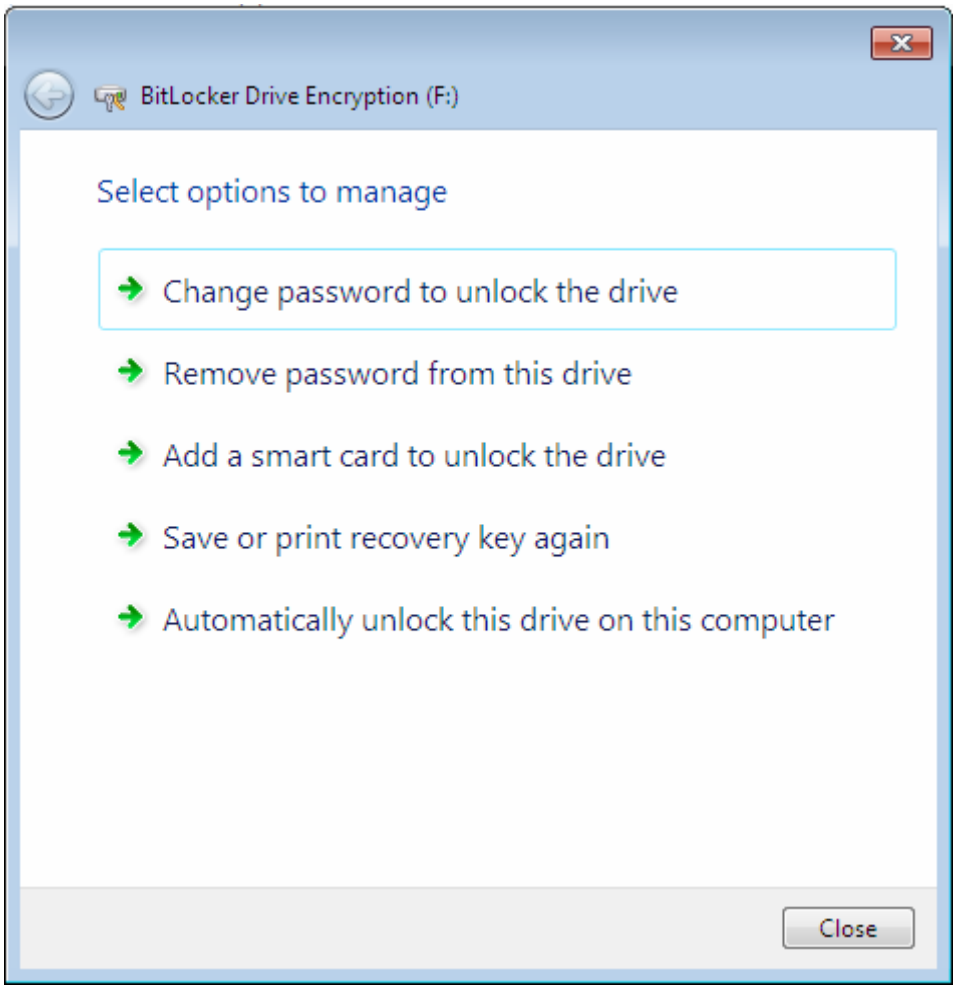
BitLocker also extends its capability with BitLocker to Go. This ability allows a user to encrypt USB flash drives with a right click on the drive.



Access to the flash drive is done with the key that was typed in.



Management of the drive is done from then context menu. There the password can be changed or removed, or enable auto unlocking of the USB device.

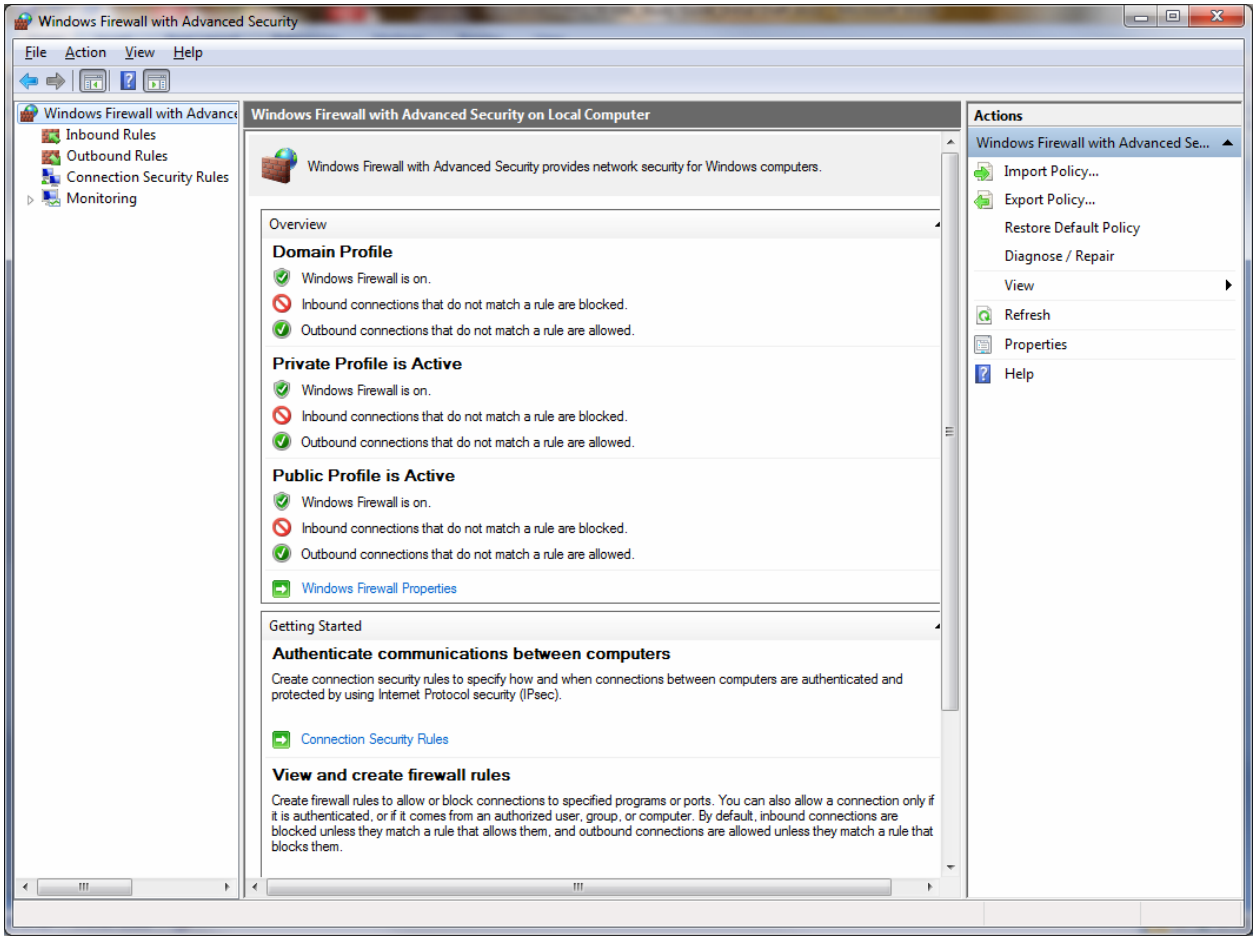


Windows Firewall

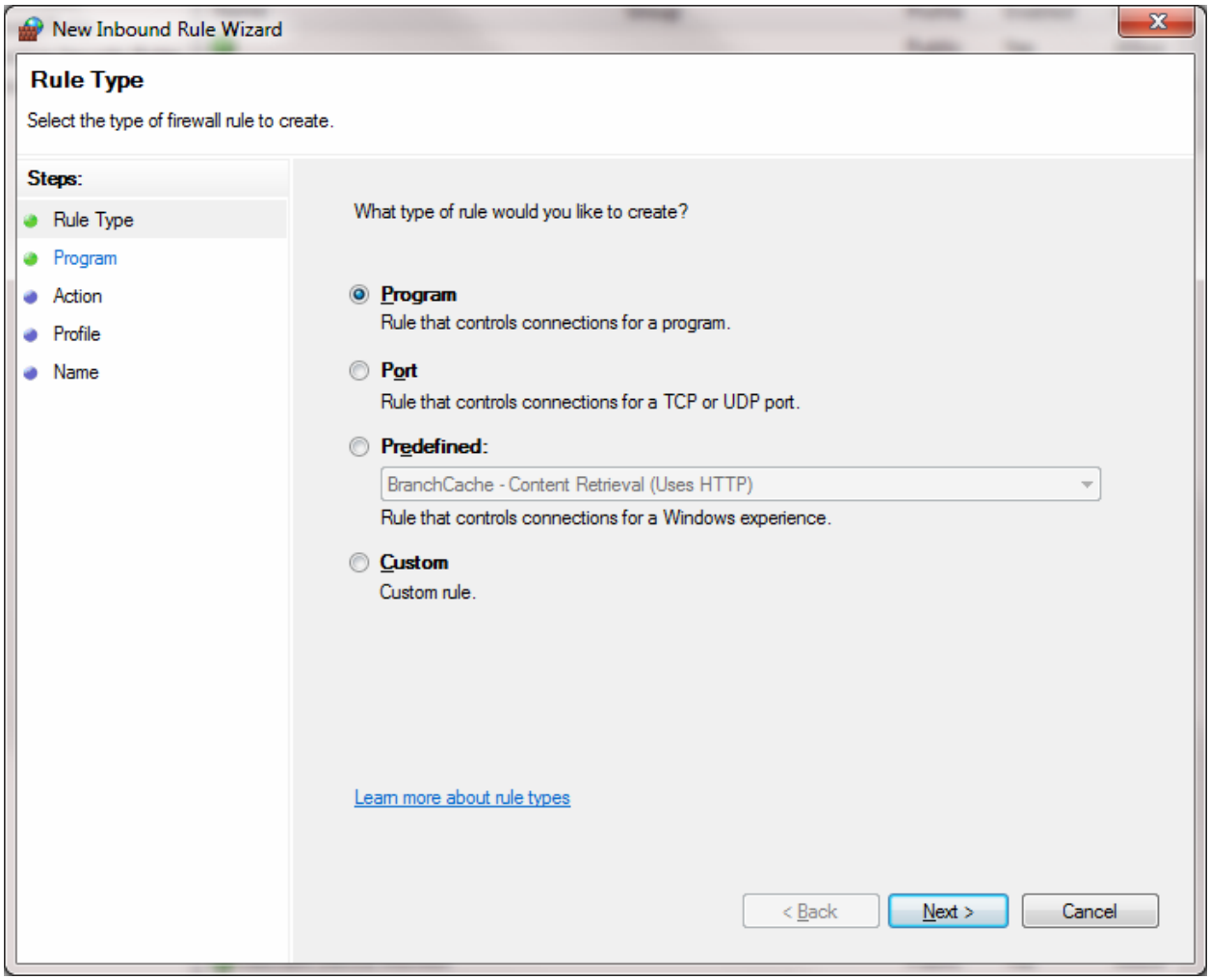
Microsoft Windows Firewall is a host based firewall that is configurable for connections on the specific machine it is running on.

Connection are based on firewall rule priority.

1. Authenticated bypass – these are rules that override any current blocking rules
2. Block connection – these rules block matched inbound traffic
3. Allow connection – these rules allow matched inbound traffic
4. Default profile – set to block unsolicited inbound traffic, but will allow out bound traffic.



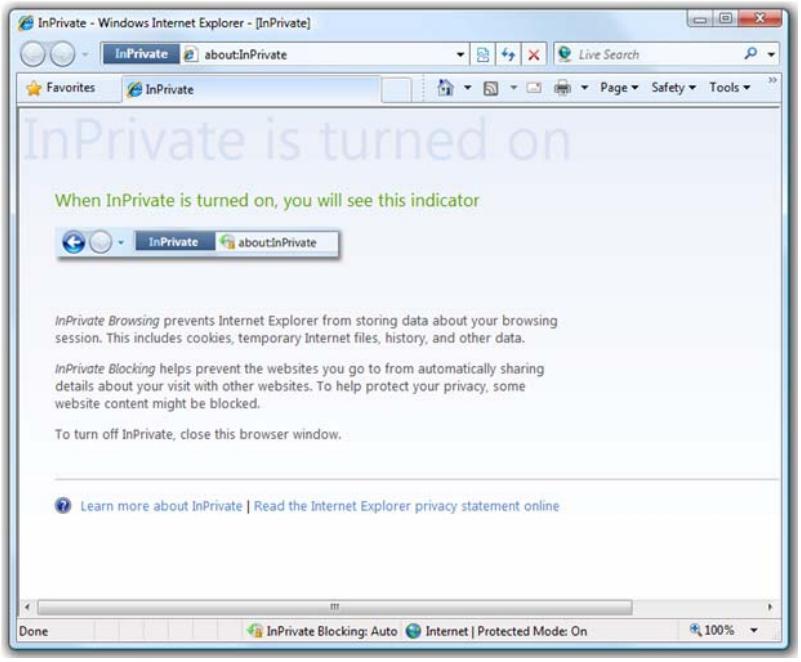
Four areas of manageability are inbound rules, outbound rules, connections and monitoring.


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.
Custom
Custom rule.
Learn more about rule types
< Back
Next >
Cancel

Define Windows Internet Explorer settings.

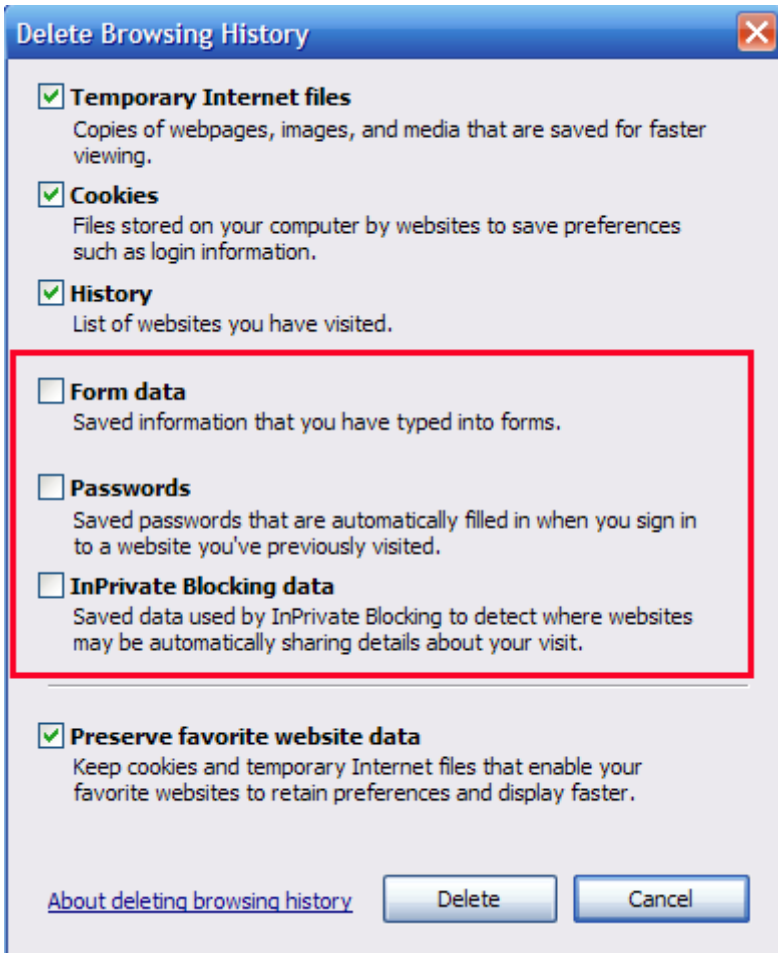
IE 8 provides for some new privacy features when browsing the Internet.

> InPrivate Browsing when selected prevents user information from being stored locally on the machine.

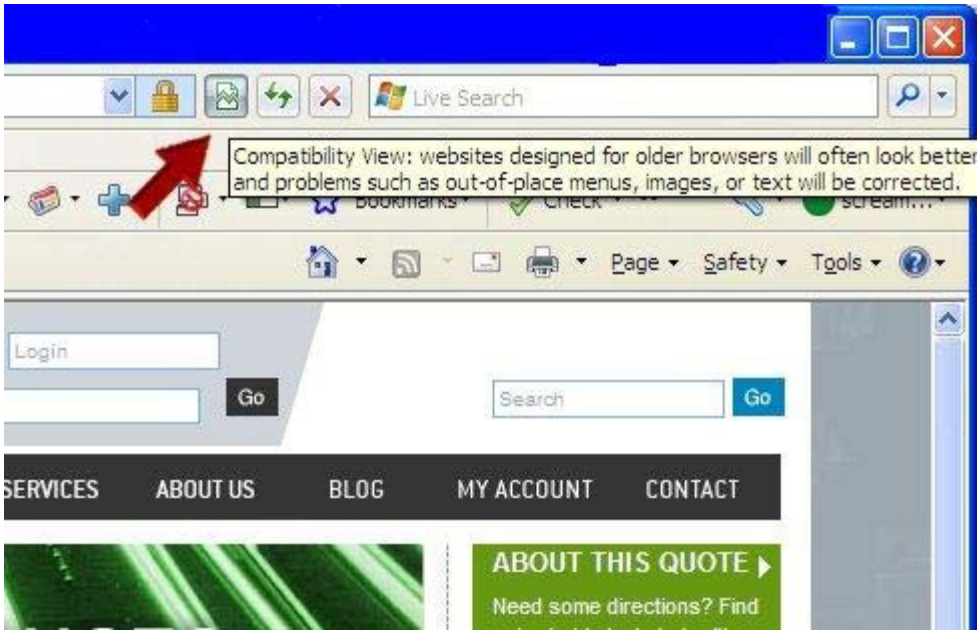


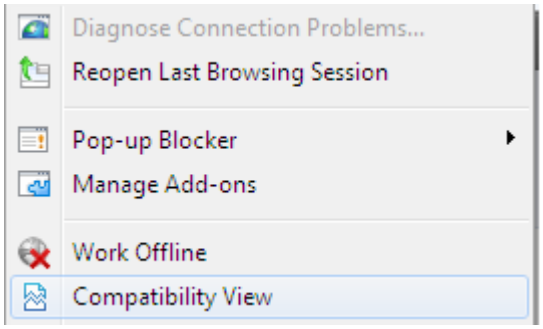
InPrivate Filtering monitors all 3rd party content and you visit different websites. 3rd party content that appears with a high level of frequency is blocked.

Enhanced Delete Browsing History allows for the user to selectively delete browsing history.



Compatibility View allows IE 8 to display the webpage as it was meant to be displayed. The compatibility view button only displays if the site does not state how it is to be rendered.





Chapter 4 – Designing a Windows 7 Client Deployment.

Analyze the environment and choose appropriate deployment methods.

There are 4 types of deployment that can be used in the environment.

- In-Place Deployment
- Side-by-Side Deployment
- Lite-Touch Deployment
- Zero-Touch Deployment

In-Place Deployment method

- 2 types –
  - **In-Place upgrade method** – upgrade the current OS to the new OS.

Supported Upgrade Scenarios

From Windows Vista (SP1, SP2)	Upgrade to Windows 7
Business	Professional, Enterprise, Ultimate
Enterprise	Enterprise
Home Basic	Home Basic, Home Premium, Ultimate
Home Premium	Home Premium, Ultimate
Ultimate	Ultimate

From Windows 7	Repair-In-Place Upgrade to Windows 7
Enterprise	Enterprise
Home Basic	Home Basic
Home Premium	Home Premium
Professional	Professional
Starter (x86 only)	Starter (x86)
Ultimate	Ultimate

Supported Upgrade Scenarios

From Windows 7	Anytime Upgrade to Windows 7
Home Basic	Home Premium, Professional, Ultimate
Home Premium	Professional, Ultimate
Professional	Ultimate
Starter	Home Premium, Professional, Ultimate

http://technet.microsoft.com/en-us/library/dd772579(WS.10).aspx

WARNING: !	The **Upgrade** option is available in Windows 7 Setup for some computers running Windows Vista®, but it is not available for Windows XP. http://technet.microsoft.com/en-us/library/dd446674(WS.10).aspx

- **Wipe-and-Load method -** This is a clean install of Windows 7. This would also include using USMT to migrate the users setting to a storage location to be restored when the load is completed.
    - Standard 5 step process –
        1. Backup the machines whole HD
        2. Save the user settings and data for migration
        3. Install clean version of OS
        4. Reinstall all applications
        5. Restore user settings and data

- Advantages of In-Place Deployment
    - In-place upgrade –
        - No investment on new machine
        - No storage for migration
        - No reinstall of applications
        - No reinstall of user settings
        - Down time is minimal
        - Windows 7 setup runs unattended

- Wipe-and-Load -
    - Reduced cost
    - Cleans up existing machines
    - New stable desktop
    - Standard desktop configuration

- Disadvantages include –
    - In-place upgrade –
        - Does not allow for a fresh image
        - Does not allow for edition changes
        - Applications may not work
    - Wipe-and-Load -
        - Requires migration tools
        - Requires reinstallation of applications
        - Requires storage space for user data
        - Reduced productivity as applications and settings are tweaked

Side-by Side method

- Used when replacing with old/broken machines with new/spare machines.
- New machine has clean image on it and user settings and data are transferred to the new machine.
- Standard steps include –
    1. Save user settings
    2. Install clean version of OS
    3. Install applications
    4. Restore user settings and data
- Advantages of Side-by-Side –
    - Limited environment disruption
    - Clean desktop environment
- Disadvantages include –

- Additional hardware
- Reinstall of applications
- If user settings not migrated can cause loss of productivity

Lite-Touch method

- Using the Microsoft Deployment Toolkit (MDT) Lite-Touch Installation (LTI) method, administrators have limited interaction with the install. They provide customized information for the installation. After that the install is usually automated.

- LTI is primarily designed for medium sized company installs.

- Advantages of LTI –
  - Limited interaction
  - Standard configuration
  - Fast deployment
  - Minimal infrastructure requirement
- Disadvantages include –
  - Manual Start
  - Requires interaction

Zero-Touch method

Complete automation, no interaction by the administrator. ZTI requires SCCM 2007 SP2 for fully-automated deployment of the OS.

Advantages of ZTI –

- Full automation with SCCM 2007 SP2
- Standard configuration
- Fast deployment

Disadvantages include –

- Significant infrastructure needs to be in place to support ZTI
- Requires experts in deployment

Design a lite-touch deployment strategy.

- Deploying LTI has 7 standard steps –

    1. Design the LTI environment
        a. Make sure the infrastructure is built so that the LTI tools can be used.
        b. Must have a managed network and a file server.
        c. Large amount of storage for images.
    2. Implement the LTI infrastructure
        a. Build the deployment server also known as the build server, to hold the images.
        b. Build the data server to hold the backups and user state data.
        c. Build the Application installation server to store the application source files.
        d. Build the Windows Deployment Services (WDS) server for PXE booting.
        e. Build the Database server as an optional centralized repository for configuration settings.
    3. Install MDT 2010
        a. MDT 2010 allows for the Deployment Workbench to be installed. This is the administration console for MDT 2010 that is used for daily tasks.
        b. Prerequisite software for MDT 2010 are –
            i. MMC 3.0
            ii. .NET Framework 2.0
            iii. Windows PowerShell 2.0
            iv. AIK 2.0
    4. Create and populate the deployment share
        a. This is a share that is created usually created on the build server but can be on the data server.
        b. The share is created using the MDT 2010 Deployment Workbench
    5. Create and customize a task sequence
        a. Tasks are steps preformed during deployment.
            i. Region
            ii. Language setting
            iii. Location
            iv. Product key
    6. Create the Win PE and Windows 7 image
        a. Use Deployment Workbench to manage the Windows PE boot images
        b. Update the deployment share to use the Windows PE boot images
    7. Deploy the OS images to the client machines
        a. Run the deployment wizard with elevated rights

Design a zero-touch deployment strategy.

- ZTI deployments are done by using SCCM 2007 SP2 and MDT 2010
  - Deploying ZTI has 9 standard steps –

    1. Design the LTI environment
       a. Make sure the infrastructure is built so that the ZTI tools can be used.
       b. Must have a managed network and a file server.
       c. Large amount of storage for images.
    2. Implement the ZTI infrastructure
       a. Build the deployment server also known as the build server, to hold the images.
       b. Build the data server to hold the backups and user state data.
       c. Build the Application installation server to store the application source files.
       d. Build the Windows Deployment Services (WDS) server for PXE booting.
       e. Build the Database server as an optional centralized repository for configuration settings.
    3. Install and Configure Configuration Manager 2007
    4. Install MDT 2010
       a. MDT 2010 allows for the Deployment Workbench to be installed. This is the administration console for MDT 2010 that is used for daily tasks.
       b. Prerequisite software for MDT 2010 are –
          i. MMC 3.0
          ii. .NET Framework 2.0
          iii. Windows PowerShell 2.0
          iv. AIK 2.0
    5. Integrate Configuration Manager 2007 and MDT 2010
    6. Configure PXE service
       a. This is a Configuration Manager 2007 site role
       b. The service point must accept PXE boot requests by CM2007 clients
       c. You must configure the WDS server role
          i. WDS need to be configured to not respond to clients
    7. Create and distribute images and packages
       a. Images will contain the OS
       b. Images will contain OS related files
       c. Other applications can also be installed
       d. Boot images are stored with the .WMI extension
       e. CM 2007 has two boot images, one for x86 and one for x64
       f. Images use distribution points for access to packages
    8. Configure and advertise task sequences
       a. Task sequence allows for
          i. Installation of existing image
          ii. Capture of a reference OS

iii. Make customized task using variables
b. Advertisement is done with the New Advertisement Wizard
c. Read access to the task sequence is required

9. Create collections
   a. Collections are logical organized structure of tasks
   b. CM 2007 has 16 default collections
   c. To make a new collection you must have Create permission
   d. To advertise a collection you must have the Advertise permission

Packages and Images that are required are as follows –

Package or Image	**Contains**
Boot image package	Boot image used to initiate the ZTI deployment process.
Microsoft Deployment Files package	Contents of the Microsoft Deployment distribution share directory. The files used from the distribution share directory are the scripts and control files.
OS image	Image of the operating system to be deployed to the target computer.
Client package	Configuration Manager client installation files.
USMT package	USMT files used to capture and restore user state.
Custom Settings package	Unattended files and customsettings.ini.
Sysprep files package	Specific Sysprep files defined for a package.

Optional packages -

- Application packages
- Windows package file packages
- Device Driver packages

Image types –

- Capture image: a boot image that is used to capture an OS as a .wim file
- Discover image: a boot image that allows non-PXE machines to have an OS image installed on them.
- Thin image: OS files only
- Thick image: OS and application files

Distribution points –

- Can be either a server or a server share
- This is the only system role that can be created as a server share

Option	Advantage	Disadvantage
Server	Configuration Manager automatically creates a common package share when the first package is copied to the distribution point. There is less chance of failing to copy a package because Configuration Manager 2007 creates a new SMSPKG*x*$ share when more space is needed. The server can be configured as a branch distribution point. The server can be configured to support Internet-based clients.	Every time Configuration Manager copies a package to the distribution point, it chooses the NTFS drive with the most free disk space, making it difficult to determine which drive letter will hold the new package. Configuration Manager 2007 can take over all available NTFS disk space on the server.
Server share	Configuration Manager does not use space reserved for other functions on other partitions.	Administrators must manually create a shared folder before creating the new site system server share. Configuration Manager might fail to create a package if there is no free space on the partition where the shared folder was created. Configuration Manager does not create a data discovery record (DDR) to monitor the health of the site system. The server share cannot be configured as a branch distribution point. The server share cannot be configured to support Internet-based clients.

- Branch Distribution points are designed for supporting branch offices
- Enable BITS if you help control bandwidth utilization
- Protect the Distribution point if it is on a slow network link or at a branch office

Design a user state migration strategy.

There are 2 user state migration tools to use –

- Windows Easy Transfer (WET)
  - Used where there is a limited number of users to migrate

- Cannot be used to transfer program files or applications
- Will transfer application settings if the application is already installed
- Windows 7 WET had a file explorer to allow for customized selection of data to be moved.

➢ To move files and settings with WET use the following –
- A WET cable
- A Network connection
- Removable media

➢ User State Migration Tool (USMT)
- 2 tools used my USMT
  - ScanState – to collect all the files and settings
  - LoadState – to push settings on the new machine

3 steps to migrate a user with USMT
Collect files and settings with ScanState
Install OS and applications on new machine
Restore Files with LoadState

- USMT is for large scale migrations not for one offs
  - Do not use USMT if end user interactions are required, or there is customization that needs to be done.
- Configurations files included with USMT are
  MigApp.xml – settings for migrating application settings
  MigDocs.xml – helps find user documents on the old machine
  MigUser.xml – rules for migrating user profiles and data
  Config.xml – lets you exclude files to be transferred

Items that USMT does not migrate –

Application Settings from earlier versions of an application, applications settings and OS settings when a local account is made, or when you migrate from Project 2003 to 2007

Existing Applications, all applications have to be reinstalled

OS settings that are not migrated include the following, Mapped drives, Shared folders, Files and settings migrated between OS's with different languages, Custom icons for shortcuts, Taksbar settings for XP, or network printers and firewall settings when the destination machine is XP

Run Scanstate.exe in the USMT with the /p switch to see the estimated size of the user state migration data.

To migrate local account the do not exist on the destination machine use LoadState with the /lac switch.

http://technet.microsoft.com/en-us/library/dd560755(WS.10).aspx

Migrations store is done one of three ways,

Uncompressed (UNC) way is exactly as it sounds, stores the image in a uncompressed state.

Compressed, a single file that is usually encrypted

Hard-link, this allows the store to be maintained on the local computer as the old OS is being removed and the new one is being installed. This store will only work with a computer refresh.

http://technet.microsoft.com/en-us/library/dd940011(WS.10).aspx

The following Best Practices are suggested in using USMT

1. Install applications before running LoadState, USMT does not migrate applications.
2. Do not use MigUser.xml and MigDocs.xml together, these files can have conflicting instructions.
3. Close all applications before running ScanState or LoadState
4. Log off after running LoadState, some settings need the user to log on
5. Create a managed environment
6. Run Chkdsk to verify that the disk is good
7. Migrate users in groups of similar user type

Security Best Practices

1. Use caution when migrating files encrypted with EFS, this could cause the USMT to fail
2. Do encrypt the migration store whit the /encrypt switch, this will protect the data while waiting for LoadState to run
3. Run an anti-virus
4. Secure the file server and the deployment server
5. USMT does not migrate passwords
6. Watch local account migration

Chapter 5 – Designing Application Packages for Deployment.

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Design a delivery or deployment strategy.

When designing a delivery strategy 7 things need to be looked at –

1. Determine the number of WDS instances require.
    a. Look at the locations that need access to a WDS instance. For every location that requires image deployment one instance is required.
    b. Multiple instances may be needed in a isolated network or sites with low bandwidth.
2. Look to see if there is an existing RIS infrastructure or if there is already a new WDS infrastructure in place.
3. Decided what Role will be needed.
    a. Full WDS requires AD DS, DHCP, DNS
    b. Transport server role is a subset and as will contain only the main parts of WDS. The transport role is good for a standalone server using multicast.
4. Look at the resource requirements.
    a. Is the WDS going to be virtualized or physical
    b. Boot files are stored locally on the WDS server.
    c. Scaling up the servers
    d. WDS is heavy on I/O and reading to and from the disk.
    e. WDS tries to cache the image in memory, RAM is vital
    f. Network speeds of a 1 Gbps or more is optimal
5. Define share fault tolerance.
    a. DFS
    b. Clustering
6. Image Consistency.
    a. Manual copy of the image.
    b. DFS Replication
    c. Some third party replication like Ghost.
7. Client discovery
    a. Network Boot referrals use DHCP options 66 and 67
    b. IP helper configured on the router and switches of the network.

Manage application compatibility.

When it comes to application compatibility, testing is a must. Common guidelines for testing commercial applications are –

- Installation of the application on the new desktop image
- Logging on to the application to test the features available
- Trying to install different options
- Applying GPO
- Running multiple applications at the same time
- Testing the backup features
- Working with large files, especially graphic files
- Testing OLE
- Testing the hardware
- Testing the application on Terminal Server Services
- Testing database usage

For custom applications you will need to test all the above features along with the following

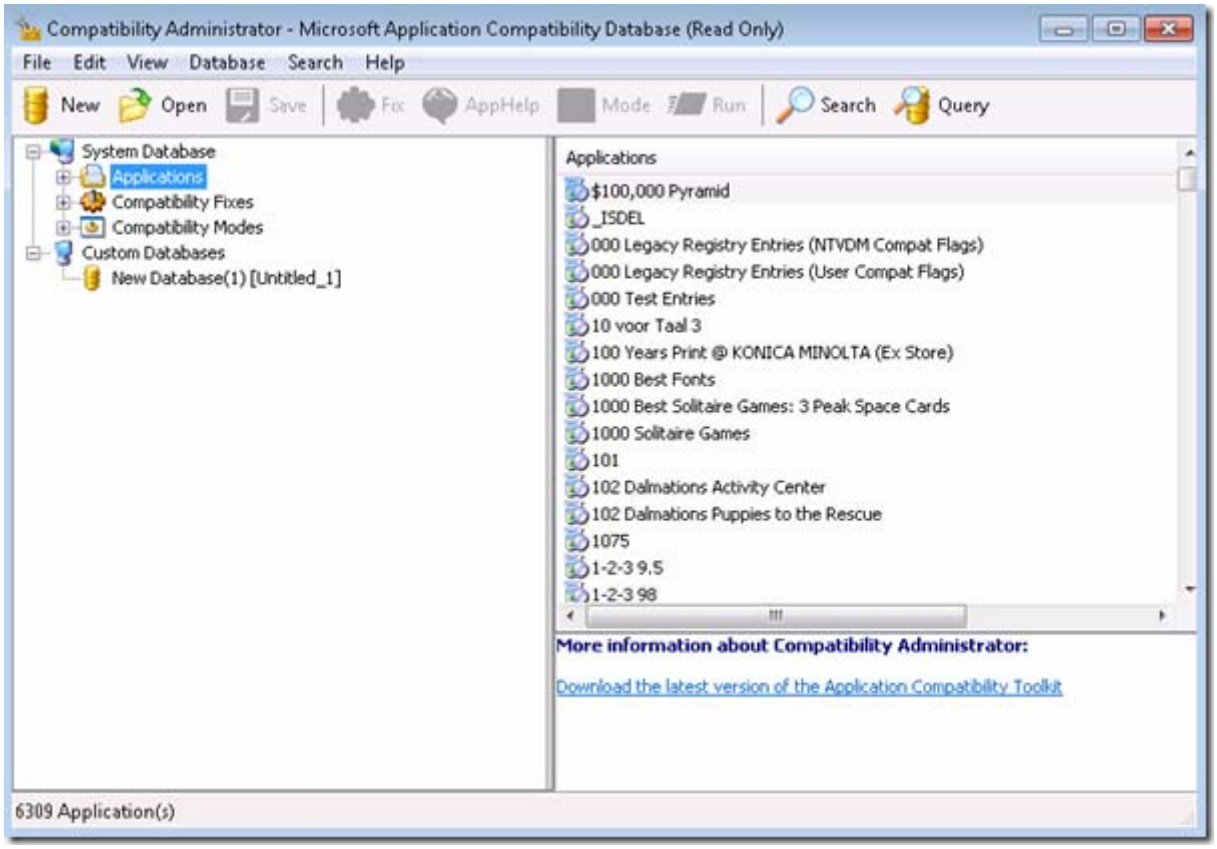
Testing the custom application on a clean installation of Windows 7
Testing all features and known issues from previous installs on older OS
Testing the custom application on an upgrade to Windows 7 from an older OS

Some of the common issues the applications face from a OS migration are

Setup and installation issues
User Account Control or permission issues
Kernel-mode driver
Windows Resource Protection
IE 7 and 8 Protected mode
IE 8 User Agent String
64-bit architecture
Windows Filtering API
Deprecated components

To help with application compatibility issues Microsoft has provided the Application Compatibility Toolkit (ACT)

http://technet.microsoft.com/en-us/windows/aa905066.aspx



Requirements for ACT are the following –

Operating Systems
ACT supports the following operating systems:

- Windows® 7
- Windows Vista®
- Windows Vista with Service Pack 1 (SP1)
- Windows XP with Service Pack 2 (SP2)
- Windows XP with Service Pack 3 (SP3)
- Windows® Server® 2003 with Service Pack 2 (SP2)
- Windows® Server 2008 R2

Database Components
After ACT has been installed, it requires one of the following database components:

- Microsoft® SQL Server® 2008

- SQL Server 2005
- SQL Server 2008 Express
- SQL Server 2005 Express Edition

.NET Framework
ACT requires the .NET Framework 2.0 or newer.

ACT components	Minimum requirements	Recommended requirements
Application Compatibility Manager client and ACT Log Processing Service servers	550-megahertz (MHz) processor with 256 megabytes (MB) of RAM	2.8-gigahertz (GHz) processor with 2 gigabytes (GB) of RAM
ACT client databases	1-GHz processor with 512 MB of RAM	2.8-GHz processor with 2 GB of RAM

ACT 5.5 uses 3 different compatibility evaluators to test current applications –

Inventory Collector – this looks at all the applications that are installed on each machine that have a Data Collection Package installed.

User Account Control Compatibility Evaluator (UACCE) – this looks at issues when the application is running under Protected Administrator or Standard User accounts

Update Compatibility Evaluator (UCE) – this looks at what might happen when a new Windows update is released

The Standard User Analyzer is a tool that allows you to test User Account Controls problems that are related to Windows 7 UAC. This is done with a API that monitors things like registry keys, files, tokens, privileges…

The Compatibility Administrator Tool is used to fix issues found using SUA and apply the fix to a new image.

Chapter 6 – Identifying and Resolving Deployment and Client Configuration Issues.

Identify and resolve Internet Explorer issues.

Issues related to IE can be numerous some of the more common ones are –

1. Antivirus or antispyware can cause IE to respond slowly or not at all. To fix this, test them in the lab before moving to production.
2. Add-ons like Flash or Adobe Reader can cause IE to freeze. Try running without Add-ons and see if this fixes the problem
3. There could be a process that is conflicting with IE. To test this try running different applications in the lab with IE and see it you can recreate the issue.
4. If nothing else works try Resetting IE. This puts it back to the state when it was installed. If it still freezes then try reinstalling IE.

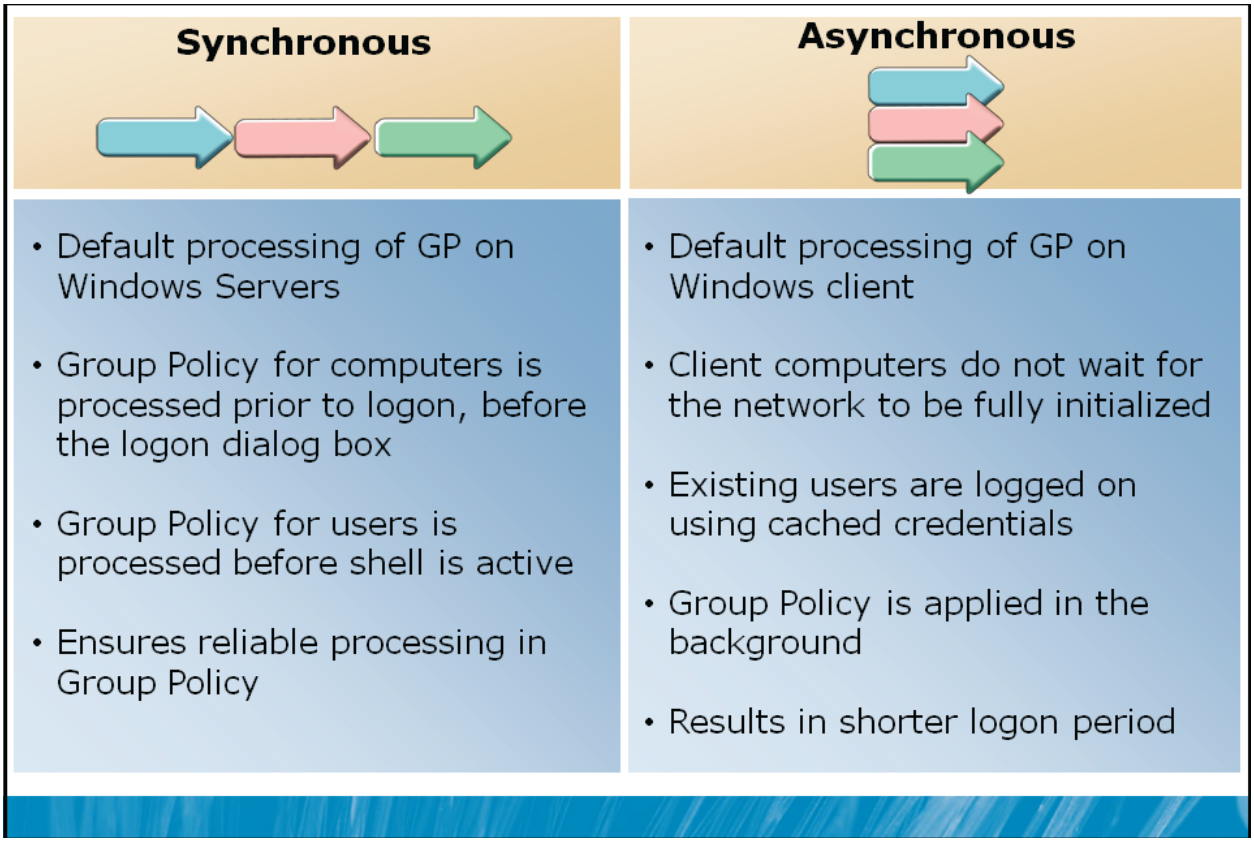
Identify and resolve Group Policy issues.

Group Policies are processed in a specific order with the previous policy being over written if there is a conflict. If there is no conflict then the machine has all the GPOs applied.

The order of application is as follows –

Local GPOs
Site-Level GPOs
Domain-Level GPOs
Organizational Unite (OU) GPOs

GPOs are either Synchronous or Asynchronous –



GPOs are inherited from the parent container by default. There are GPO options that can be set to change that default setting.

Link order is the precedence order that GPOs are linked, the GPO that has the link order of 1 takes precedence over other GPOs that are linked to that container

Enforce allows the administrator to force a GPO setting even if the child container has a different setting in the linked GPOs

Block Inheritance allows the administrator to block GPOs from being inherited, however this does not apply to enforced GPOs, they will always be processed.

Link Enabled, GPOs by default are not linked to a container until the administrator links them. This allows the administrator to have multiple GPOs attached to the container but not be processed.

Loopback processing of a GPO allows the administrator to apply GPO setting to a user no matter what machine they log on to. This setting means that we can apply alternate user settings based on the machine. There are two modes for Loopback processing, Merge mode where the computer applied GPOs are added to the end of the user applied GPOs. The other mode is Replace mode, where only the computer GPOs are applied.

When planning a GPO structure some of the things that need to be addressed are

Delegating administrative authority to individuals in specific OUs

Applying the GPO at the lowest level of the organization, this will allow that administrator not to have to block inheritance on containers that do not need the policy or that may cause a conflict.

Making sure that you comply with SLA when changing GPOs

Knowing what the objectives and reasons are for making the GPO

Making guidelines for creating and implementing GPOs in the Enterprise.

Knowing where the GPO will be linked and the scope needed

Determining the number of GPOs for the Enterprise

When working with GPOs the following are considered Best Practices –

Editing GPOs on the PDC Emulator- By editing the GPO on the PDC Emulator there is a reduced possibility for conflict if two administrators are editing the same GPO on different DCs.

Editing the GPO offline will allow changes to be made to the GPO but will not affect the production environment until that GPO is deployed.

Testing of the GPO should always be done in a Test lab. GPOs should be tested in a lab that closely simulates your production environment.

Back up and Archive the GPO before you edit it, that way if you modify more than one setting and don’t remember which ones you have modified then you can go back.

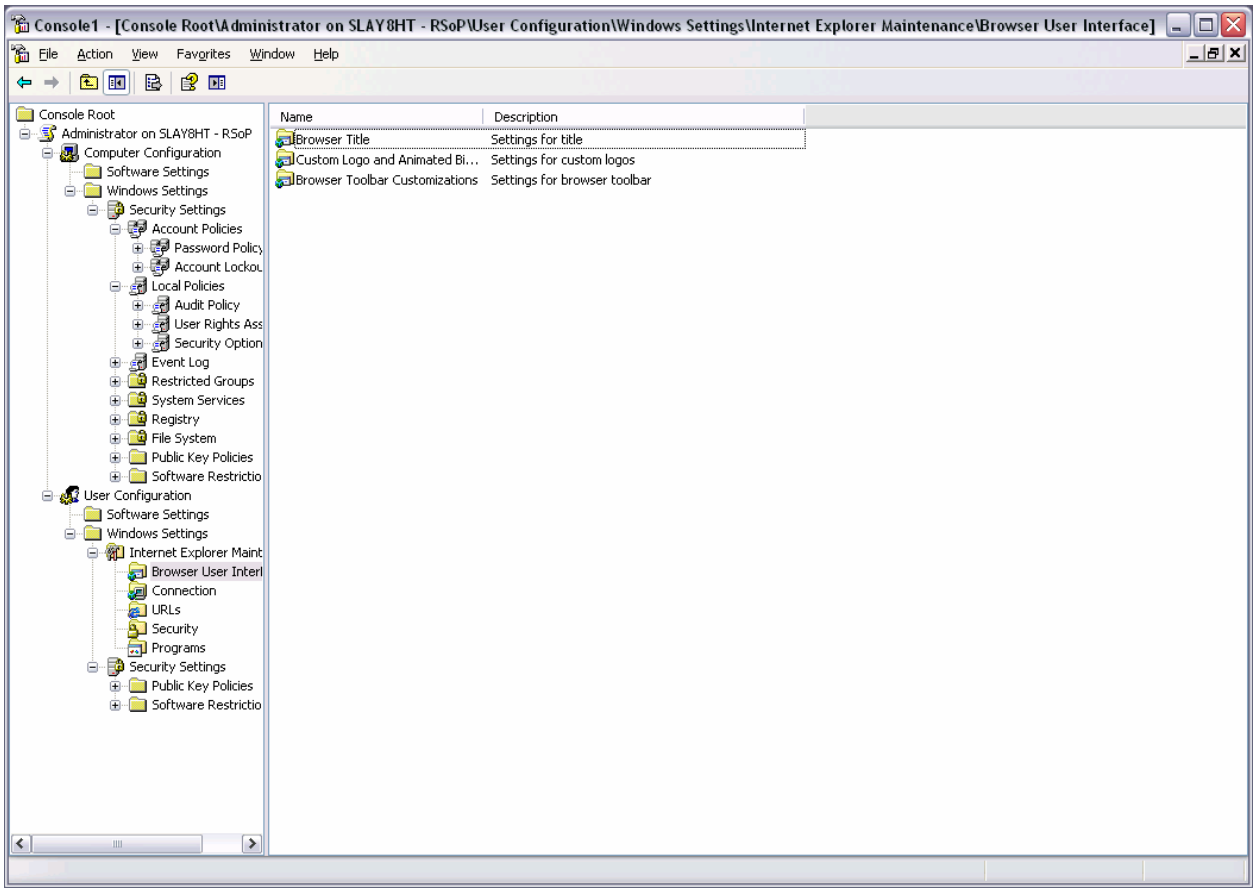
Importing your tested GPOs into the production domain will allow the transfer of the import settings to an existing GPO.

Use the GPO accelerator to create GPOs needed to deploy the recommended security settings to the enterprise.

GPOs problems can cause users to be able to gain access to network resources or can cause the users individual machine to not respond in a predictable manner.

To troubleshoot GPOs, Microsoft has provided the following tools –

Resultant Set of Policy (RSoP) in the Management Console. This allows you to predict the policies that will get applied to a specific machine.



GPResult is a command line tool that will show what policies are in effect.

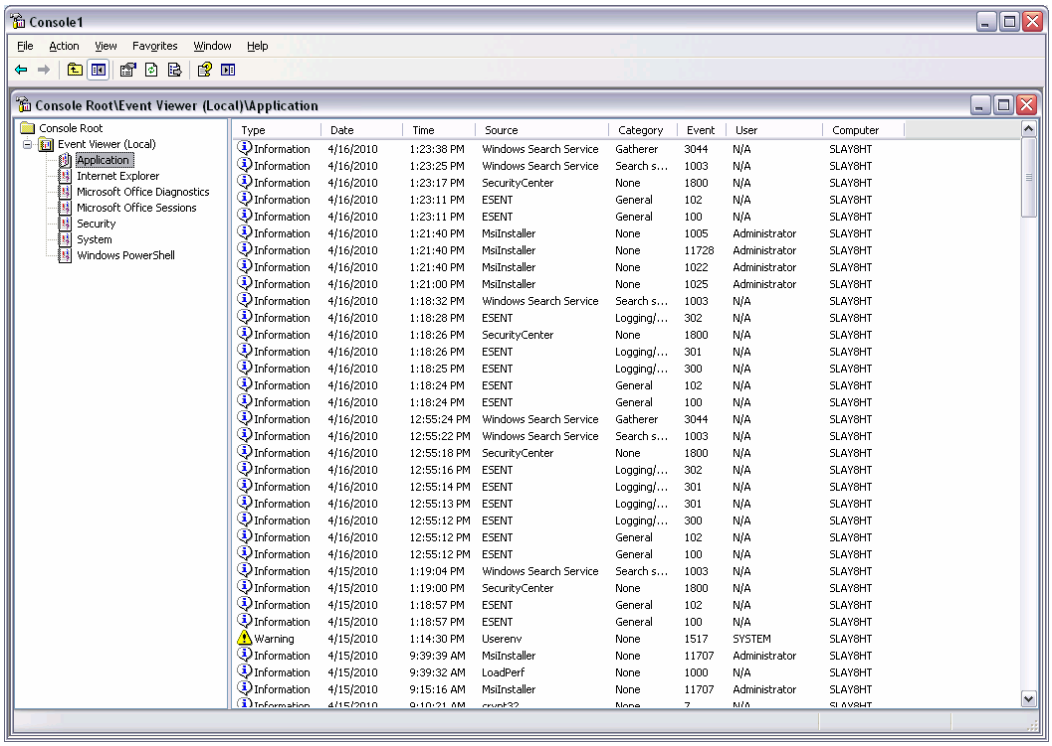
C:\WINDOWS\system32\cmd.exe

```
C:\>gpresult

Microsoft (R) Windows (R) XP Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 4/16/2010 at 2:50:31 PM


RSOP results for SLAY8HT\Administrator on SLAY8HT : Logging Mode
-----------------------------------------------------------------

OS Type:                      Microsoft Windows XP Professional
OS Configuration:             Standalone Workstation
OS Version:                   5.1.2600
Domain Name:                  SLAY8HT
Domain Type:                  N/A<Local Computer>
Site Name:                    N/A
Roaming Profile:
Local Profile:                C:\Documents and Settings\Administrator
Connected over a slow link?: Yes


COMPUTER SETTINGS
-----------------

    Last time Group Policy was applied: 4/16/2010 at 1:22:52 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps

    Applied Group Policy Objects
    ----------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The computer is a part of the following security groups:
    --------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        NT AUTHORITY\Authenticated Users


USER SETTINGS
-------------

    Last time Group Policy was applied: 4/16/2010 at 1:23:02 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps

    Applied Group Policy Objects
    ----------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups:
    ----------------------------------------------------
        None
        Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        NT AUTHORITY\Authenticated Users
        LOCAL
```

GPOTool is another command line tools that will check each domain controller and GPO and provide summery information on each object found.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\allpowerfull>gpotool server1 /verbose
Domain: fabrikan.com
Validating DCs...
Available DCs:
Server1.fabrikan.com
Searching for policies...
Found 9 policies
========================================================
Policy {2E25F0ED-2396-4BDF-8D24-F5D4E8AC71C1}
Friendly name: asdfasdf
Policy OK
Details:
--------------------------------------------------------
DC: Server1.fabrikan.com
Friendly name: asdfasdf
Created: 10/5/2007 1:27:01 PM
Changed: 10/5/2007 1:27:01 PM
DS version:     0(user) 0(machine)
Sysvol version: 0(user) 0(machine)
Flags: 0 (user side enabled; machine side enabled)
User extensions: not found
Machine extensions: not found
Functionality version: 2
--------------------------------------------------------
========================================================
Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Policy
Policy OK
Details:
--------------------------------------------------------
DC: Server1.fabrikan.com
Friendly name: Default Domain Policy
Created: 8/23/2007 5:50:27 PM
Changed: 5/1/2008 2:23:58 PM
DS version:     3(user) 3(machine)
```

Event Viewer lets you see all event that relate to the machine that your quering, you can then filter the logs for events that pertain to Group Policy.



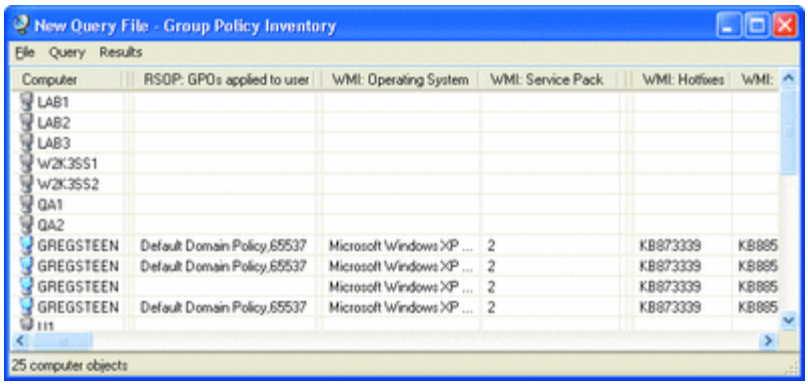
Type	Date	Time	Source	Category	Event	User	Computer
Information	4/16/2010	1:23:38 PM	Windows Search Service	Gatherer	3044	N/A	SLAY8HT
Information	4/16/2010	1:23:25 PM	Windows Search Service	Search s...	1003	N/A	SLAY8HT
Information	4/16/2010	1:23:17 PM	SecurityCenter	None	1800	N/A	SLAY8HT
Information	4/16/2010	1:23:11 PM	ESENT	General	102	N/A	SLAY8HT
Information	4/16/2010	1:23:11 PM	ESENT	General	100	N/A	SLAY8HT
Information	4/16/2010	1:21:40 PM	MsiInstaller	None	1005	Administrator	SLAY8HT
Information	4/16/2010	1:21:40 PM	MsiInstaller	None	11728	Administrator	SLAY8HT
Information	4/16/2010	1:21:40 PM	MsiInstaller	None	1022	Administrator	SLAY8HT
Information	4/16/2010	1:21:00 PM	MsiInstaller	None	1025	Administrator	SLAY8HT
Information	4/16/2010	1:18:32 PM	Windows Search Service	Search s...	1003	N/A	SLAY8HT
Information	4/16/2010	1:18:28 PM	ESENT	Logging/...	302	N/A	SLAY8HT
Information	4/16/2010	1:18:26 PM	SecurityCenter	None	1800	N/A	SLAY8HT
Information	4/16/2010	1:18:26 PM	ESENT	Logging/...	301	N/A	SLAY8HT
Information	4/16/2010	1:18:25 PM	ESENT	Logging/...	300	N/A	SLAY8HT
Information	4/16/2010	1:18:24 PM	ESENT	General	102	N/A	SLAY8HT
Information	4/16/2010	1:18:24 PM	ESENT	General	100	N/A	SLAY8HT
Information	4/16/2010	12:55:24 PM	Windows Search Service	Gatherer	3044	N/A	SLAY8HT
Information	4/16/2010	12:55:22 PM	Windows Search Service	Search s...	1003	N/A	SLAY8HT
Information	4/16/2010	12:55:18 PM	SecurityCenter	None	1800	N/A	SLAY8HT
Information	4/16/2010	12:55:16 PM	ESENT	Logging/...	302	N/A	SLAY8HT
Information	4/16/2010	12:55:14 PM	ESENT	Logging/...	301	N/A	SLAY8HT
Information	4/16/2010	12:55:13 PM	ESENT	Logging/...	301	N/A	SLAY8HT
Information	4/16/2010	12:55:12 PM	ESENT	Logging/...	300	N/A	SLAY8HT
Information	4/16/2010	12:55:12 PM	ESENT	General	102	N/A	SLAY8HT
Information	4/16/2010	12:55:12 PM	ESENT	General	100	N/A	SLAY8HT
Information	4/15/2010	1:19:04 PM	Windows Search Service	Search s...	1003	N/A	SLAY8HT
Information	4/15/2010	1:19:00 PM	SecurityCenter	None	1800	N/A	SLAY8HT
Information	4/15/2010	1:18:57 PM	ESENT	General	102	N/A	SLAY8HT
Information	4/15/2010	1:18:57 PM	ESENT	General	100	N/A	SLAY8HT
Warning	4/15/2010	1:14:30 PM	Userenv	None	1517	SYSTEM	SLAY8HT
Information	4/15/2010	9:39:39 AM	MsiInstaller	None	11707	Administrator	SLAY8HT
Information	4/15/2010	9:39:32 AM	LoadPerf	None	1000	N/A	SLAY8HT
Information	4/15/2010	9:15:16 AM	MsiInstaller	None	11707	Administrator	SLAY8HT

Software Installation Diagnostice Tool (Addig.exe) looks at the software instaltion policys that have been applied. It display applications visible in Windows and installations for the current user.

For an expamle of addiag.exe go here.

http://technet.microsoft.com/en-us/library/cc739206(WS.10).aspx

Group Policy Inventory (GPInventory.exe) lets administrators see what they have in their enterprise by running multiple RSoP and presenting it as output.



Steps in resloving GPO issuses –

1. Enable verbose debug logging
2. Verify connectivity and DNS
3. Verify that GP settings and where they are suppost to be applied
4. Run GPResult
5. Run GPOTool
6. View the Userenv.log file
7. Determine weather loopback processing is in effect

Identify and resolve networking issues.

The process that Windows 7 goes through to resolve Networking issues is a follows. –

1. Application or system component reports a problem with the TCP connection
2. Windows Network Diagnostics passes the problem to the Network Diagnostics Engine. The NDE displays a list of possible causes and repair options
3. The user gets to select the a repair option, Windows then tries to automatically repair the issue, then rechecks the TCP connection.
4. If the problem is resolved the user is notified that it has been fixed, if not then the user can choose another repair option.

Considerations when trying to resolve network issues

1. Make sure you have an up-to-date physical and logical diagram of the network.
2. Verify if a VPN is in use, determine if L2TP or PPTP is being uses as the VPN tunnel
3. Look to see if IPv6 is being used
4. Verify that the protocols that are being used are supported
5. Look to see that there are no legacy devices that are causing issues.
6. Verify your firewall settings. For internal machine Firewalls are usually turned off.
7. Look to see if there are any security filters turned on.
8. Determine if the network is wired or wireless.

Considerations for Wireless networks –

1. Verify 802.11 support
2. Verify adapter compatibility. Look to see if the device has an B adapter you only support G.
3. Look at the signal strength. This could cause intermittent problems
4. Verify that the device is connection to the correct SSID
5. Look at the authentication and encryption setting. Determine if the user should be using WPA, WPA2, WEP, or WPA Enterprise with a RADIUS server.
6. Verify that there is enough address in you DHCP scope for your wireless clients

Consideration for Remote Network connection problems are as follows –

1. SLIP is no longer supported
2. BAP is no longer supported
3. IPv6 over PPP or PPPoE is supported for access to the internet through DSL or Cable
4. PPTP no longer supports MS-CHAP v1.
5. RC4 is no longer supported
6. L2TP no longer supports DES with MD5
7. IKE has been improved to support Deffie-Hellman 256 and 384
8. AES 128,192 and 256 bit keys are supported

When troubleshooting IPv6 remember that you cannot uninstall IPv6, however you can disable it. The easiest way is to go into the Local area connection and uncheck the IPv6 protocol box. You can also disable IPv6 in the registry at the following location.

HLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponets.

Identify and resolve authentication and authorization issues.

Authentication is the process of identifying yourself to the network or local machine. Proving you are who you say you are. The most common form of authentication is user name and password.

Example would be the user name of Bob and the password of Pa$$w0rD.

Issues that come up on authentication is where am I logging on to? There are two places in the Windows world that we log on to, the first being the local machine and the more familiar being a domain of some sort.

If the user is logging on to the local machine then the user must have an account on the local machine to authenticate to. These accounts are found in Computer Management console.

The only access that these accounts allow for is access to the local machine. So if a user can not access say an Excel spreadsheet on another users machine then the most likely problem is that user1 does not have an account on the machine where the Excel spreadsheet is.

The second type of authentication is done to a domain, and specifically to a domain controller. The DC is a centralized repository for user accounts, machine accounts, along with other items used to manage the enterprise environment.

Again the most common form of authentication in this environment is the user name and password. However you can also find multi-factor authentication which would be combination of something you have, something you know or something you are. For example a swipe card and a pin number or it could also be something you are, which is biometrics.

The main thing to remember for authentication is that there has to be an account somewhere.

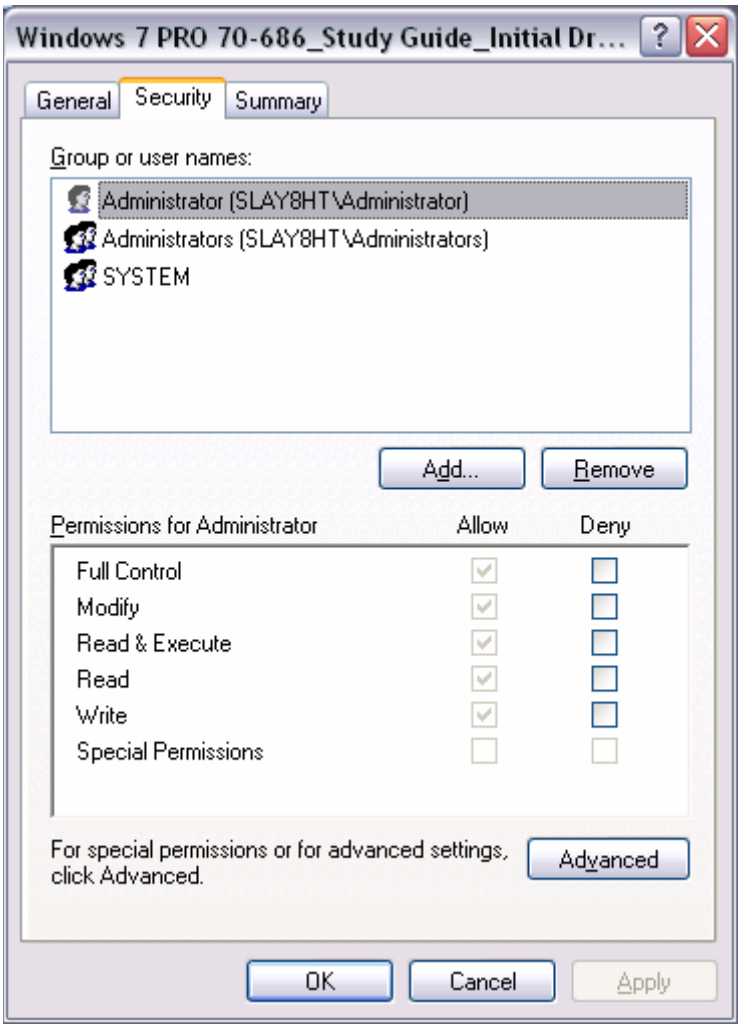
Authorization is NOT the same thing as authentication. While authentication will allow a user to have access to the network or machine, it does not define what that user can do.

This is where authorization comes in to play. In Windows networking we get authorized by the permissions that we have to an object. These permission allow the user to access the object and do something with it.

NTFS permissions control what access a user gets. They are as follows –

- Full control – the account has access to do anything
- Modify – allows the account to do almost anything, one of the big differences is that Modify does not have the take ownership permission.
- List Folder Contents – this permission is only found on folders and allows the account to see what is in that folder
- Read – only read access to a file or a folder
- Write – only write access to a file or a folder
- Special permissions – when you want a custom configuration and the above permissions will not do it.
- Deny – denies access to a permission on an object

NTFS permission are viewed by looking at the Access Control List of an object.



Share Permission allows the user to access a resource from across the network. Share permission do not come into effect if the account is logging on locally to the machine.

Share permission are as follows –

Full control – the account has access to do anything
Change - the account has read and write permission
Read - read only to the share
Deny – denies access to the share.

Common issues when looking at permissions are that user does not have access to the share, the user does not have the correct NTFS permissions to the object.

Authentication and Authorization in a Windows Active Directory Directory Services relies on Kerberos. Kerberos uses time stamps for generating ticket granting tickets and session tickets. Issues can arise if a machines time or the time that the server is using is not correct.