MICROSOFT OFFICIAL COURSE

Module 9

Securing Windows 7 Desktops

Module Overview

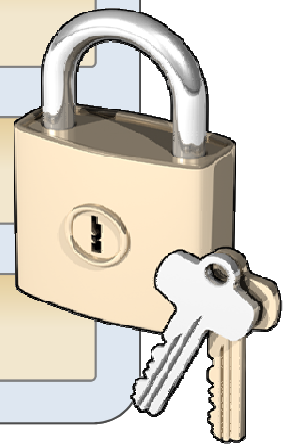
- Overview of Security Management in Windows 7
- Securing a Windows 7 Client Computer by Using Local Group Policy Settings
- Securing Data by Using EFS and BitLocker
- Configuring Application Restrictions
- Configuring User Account Control
- Configuring Windows Firewall
- Configuring Security Settings in Internet Explorer 8
- Configuring Windows Defender

Lesson 1: Overview of Security Management in Windows 7

- Key Security Features in Windows 7
- What Is Action Center?
- Demonstration: Configuring Action Center Settings

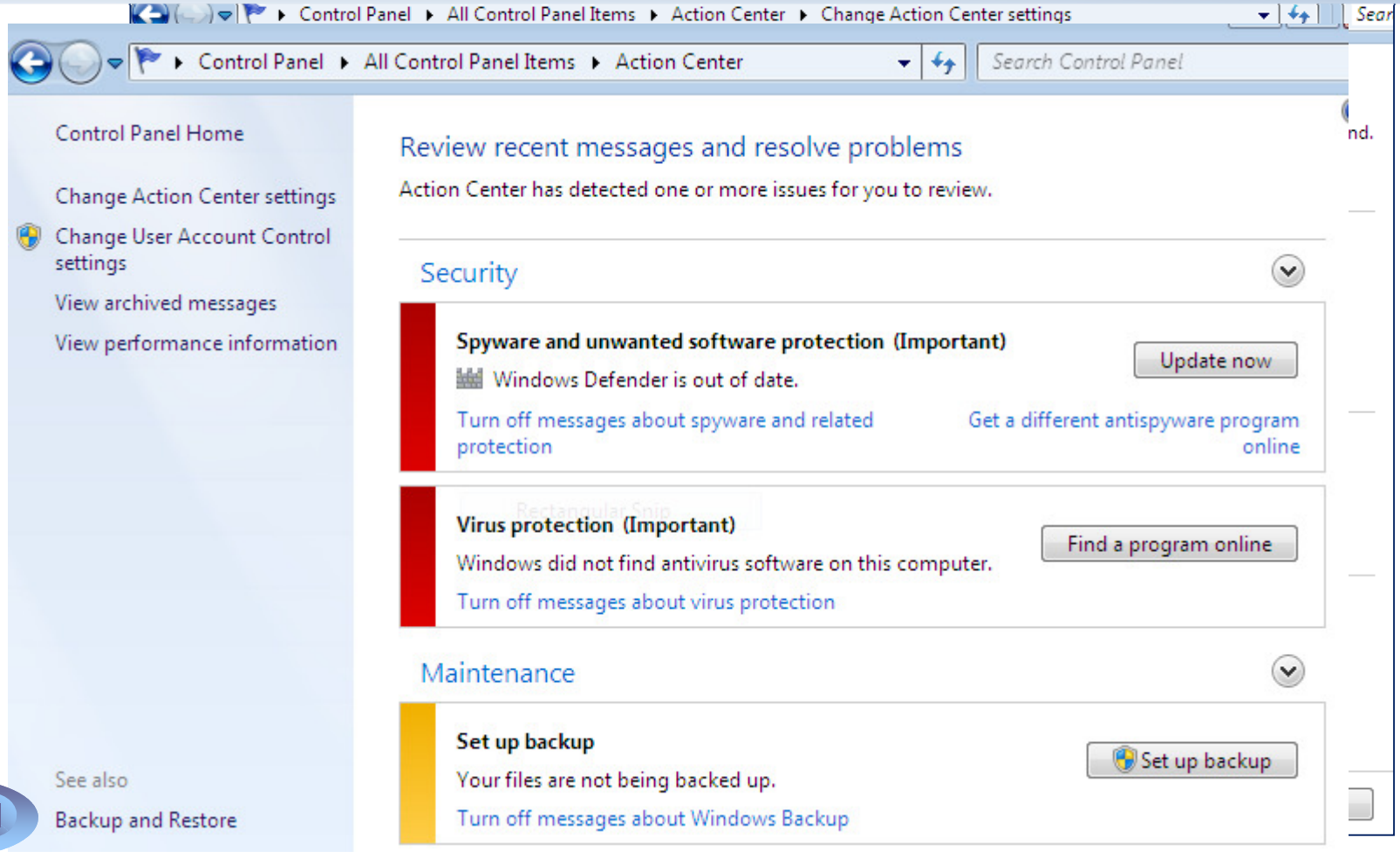
Key Security Features in Windows 7

- ✓ Windows 7 Action Center
- ✓ Encrypting File System (EFS)
- ✓ Windows BitLocker™ and BitLocker To Go™
- ✓ Windows AppLocker™
- ✓ User Account Control
- ✓ Windows Firewall with Advanced Security
- ✓ Windows Defender™



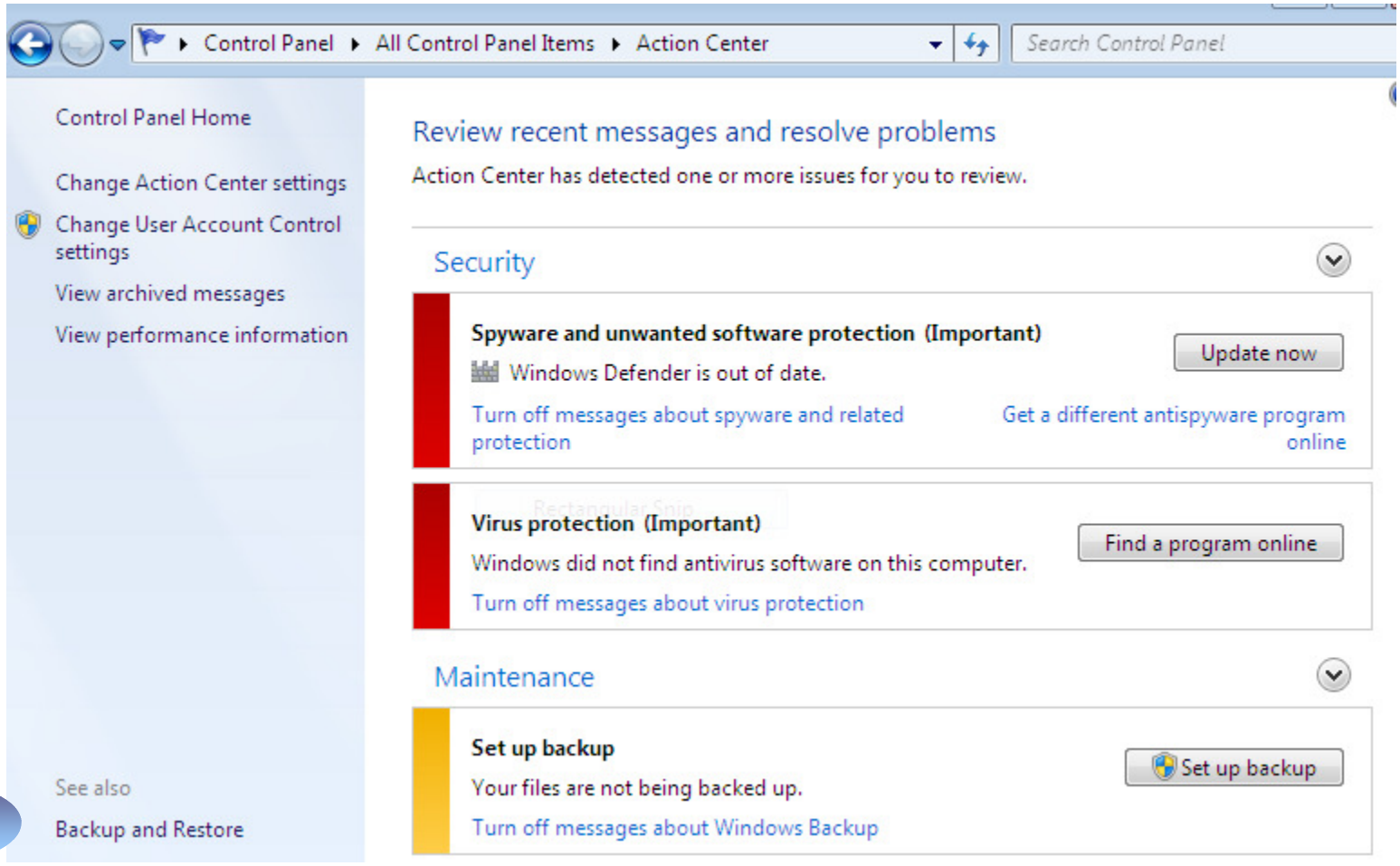
What Is Action Center?

Action Center is a central location for viewing messages about your system and the starting point for diagnosing and solving issues with your system



What Is Action Center?

Action Center is a central location for viewing messages about your system and the starting point for diagnosing and solving issues with your system



Notes Over-flow Slide

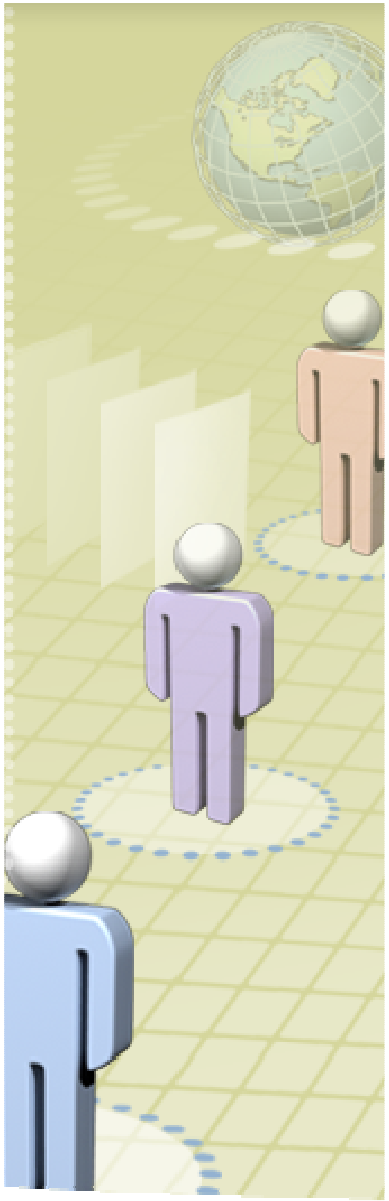
General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

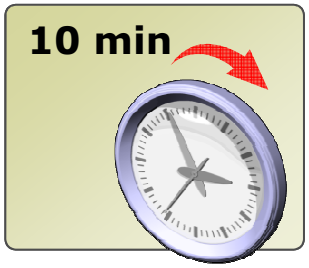
- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Demonstration: Configuring Action Center Settings



In this demonstration, you will see how to:

- Change Action Center Settings
- Change User Control Settings
- View Archived Messages



Lesson 2: Securing a Windows 7 Client Computer by Using Local Security Policy Settings

- What Is Group Policy?
- How Are Group Policy Objects Applied?
- How Multiple Local Group Policies Work
- Demonstration: Creating Multiple Local Group Policies
- Demonstration: Configuring Local Security Policy Settings

What Is Group Policy?

Group Policy enables IT administrators to automate one-to-several management of users and computers

Use Group Policy to:

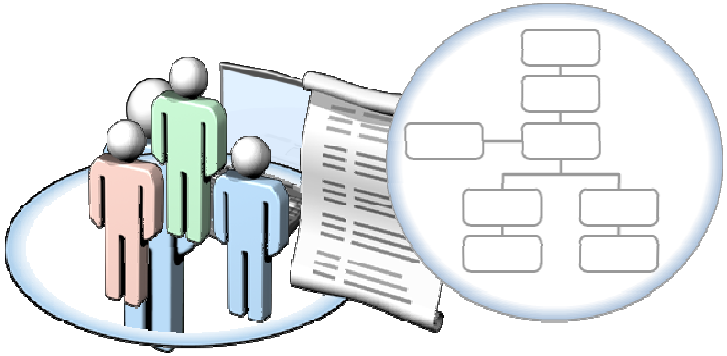
- Apply standard configurations
- Deploy software
- Enforce security settings
- Enforce a consistent desktop environment

Local Group Policy is always in effect for local and domain users, and local computer settings

How Are Group Policy Objects Applied?

Computer settings are applied at startup and then at regular intervals, while user settings are applied at logon and then at regular intervals.

Group Policy Processing Order:

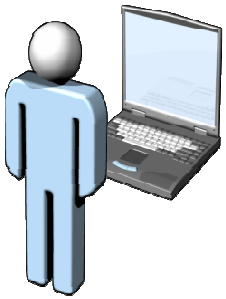


1. Local GPOs
2. Site-level GPOs
3. Domain GPOs
4. OU GPOs

How Are Group Policy Objects Applied?

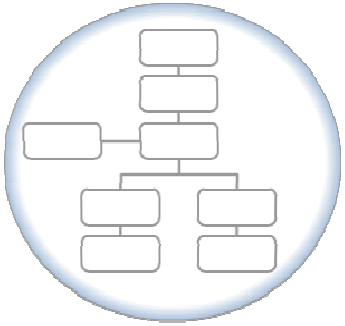
Computer settings are applied at startup and then at regular intervals, while user settings are applied at logon and then at regular intervals

Group Policy Processing Order:



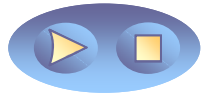
1. Local GPOs

2. Site-level GPOs



3. Domain GPOs

4. OU GPOs



How Multiple Local Group Policies Work

Multiple Local Group Policy allows an administrator to apply different levels of Local Group Policy to local users on a stand-alone computer.

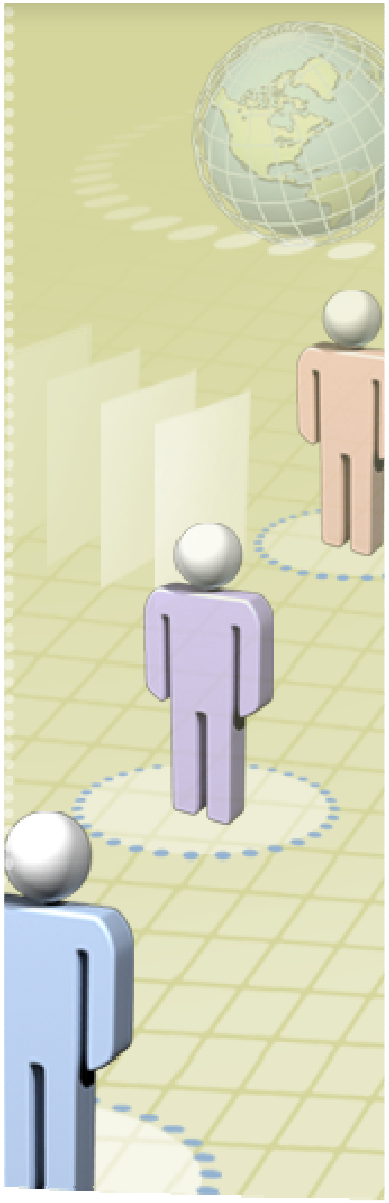
There are three layers of Local Group Policy Objects, which are applied in the following order:

1. Local Group Policy object that may contain both computer and user settings.

2. Administrators and Non-Administrators Local Group Policy objects are applied next and contain only user settings.

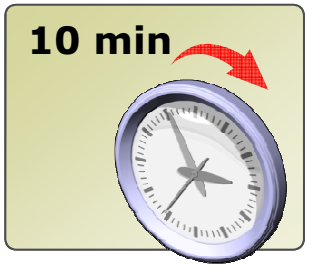
3. User-specific Local Group Policy is applied last, contains only user settings, and applies to one specific user on the local computer.

Demonstration: Creating Multiple Local Group Policies



In this demonstration, you will see how to:

- Create a custom management console
- Configure the Local Computer Policy
- Configure the Local Computer Administrators Policy
- Configure the Local Computer Non-Administrators Policy
- Test multiple local group policies



Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

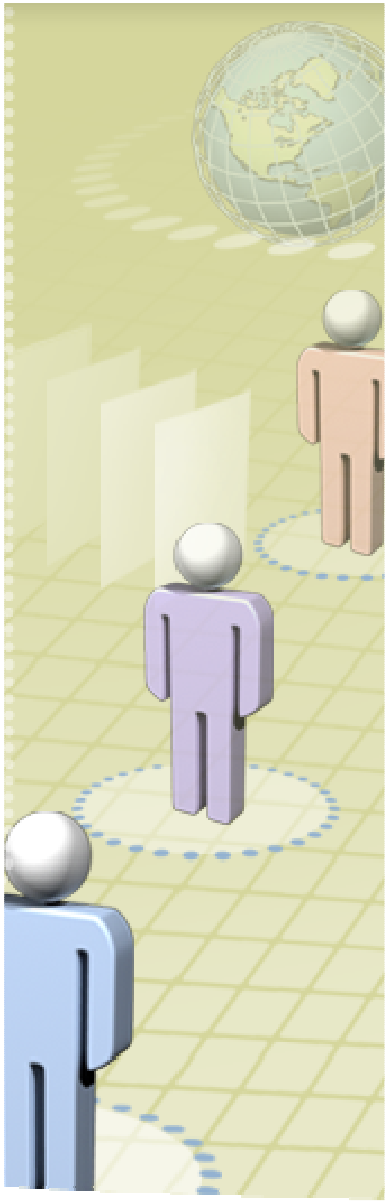
General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

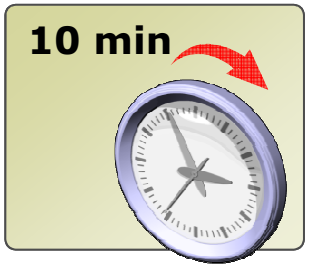
Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Demonstration: Configuring Local Security Policy Settings



In this demonstration, you will see how to review the local security group policy settings



Lesson 3: Securing Data by Using EFS and BitLocker

- What Is EFS?
- Demonstration: Encrypting and Decrypting Files and Folders by Using EFS
- What Is BitLocker?
- BitLocker Requirements
- BitLocker Modes
- Group Policy Settings for BitLocker
- Configuring BitLocker
- Configuring BitLocker to Go
- Recovering BitLocker Encrypted Drives

What Is EFS?

New EFS Features in Windows 7

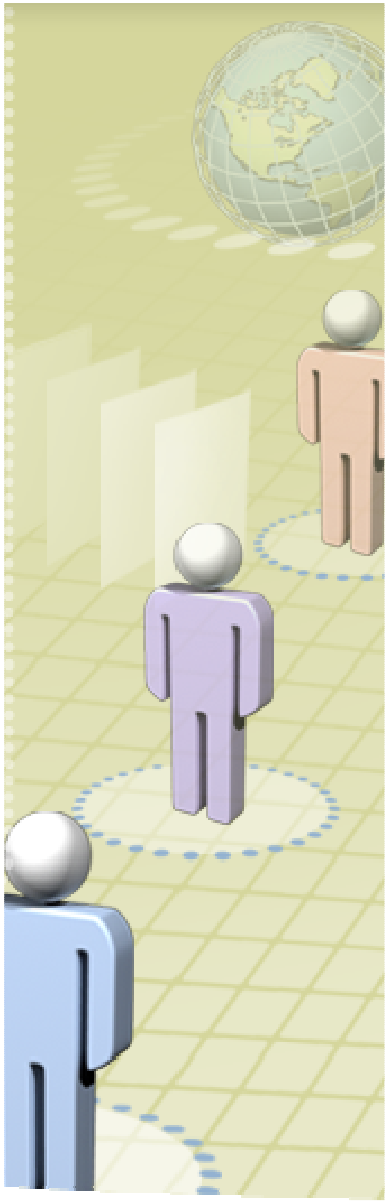
- ✓ Support for storing private keys on Smart Cards
- ✓ Encrypting File System Rekeying wizard
- ✓ New EFS Group Policy settings
- ✓ Encryption of the system page file
- ✓ Per-user encryption of offline files
- ✓ Support for AIS 256-bit encryption

What Is EFS?

Encrypting File System (EFS) is the built-in file encryption tool for Windows file systems.

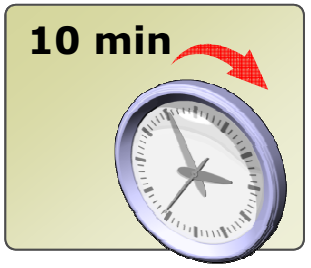
- Enables transparent file encryption and decryption
- Requires the appropriate cryptographic (symmetric) key to read the encrypted data
- Each user must have a public and private key pair that is used to protect the symmetric key
- A user's public and private keys:
  - Can either be self-generated or issued from a Certificate Authority
  - Are protected by the user's password
- Allows files to be shared with other user certificates

Demonstration: Encrypting and Decrypting Files and Folders by Using EFS



In this demonstration, you will see how to:

- Encrypt files and folders
- Confirm the files and folders have been encrypted
- Decrypt files and folders
- Confirm the files and folders have been decrypted



Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

What Is BitLocker?

- Windows BitLocker Drive Encryption encrypts the computer operating system and data stored on the operating system volume
- Provides offline data protection
- Protects all other applications installed on the encrypted volume
- Includes system integrity verification
- Verifies integrity of early boot components and boot configuration data
- Ensures the integrity of the startup process

BitLocker Requirements

Encryption and decryption key:

BitLocker encryption requires either:

- A computer with Trusted Platform Module (TPM) v1.2 or later
- A removable USB memory device

Hardware Requirements:

- Have enough available hard drive space for BitLocker to create two partitions
- Have a BIOS that is compatible with TPM and supports USB devices during computer startup

BitLocker Modes

Windows 7 supports two modes of operation:

- TPM mode
- Non-TPM mode

Non-TPM mode

- Uses Group Policy to allow BitLocker to work without a TPM
- Locks the boot process similar to TPM mode, but the BitLocker startup key must be stored on a USB drive
  - The computer's BIOS must be able to read from a USB drive
    - Provides limited authentication
  - Unable to perform BitLocker's system integrity checks to verify that boot components did not change

BitLocker Modes

Windows 7 supports two modes of BitLocker operation: TPM mode and Non-TPM mode

TPM mode

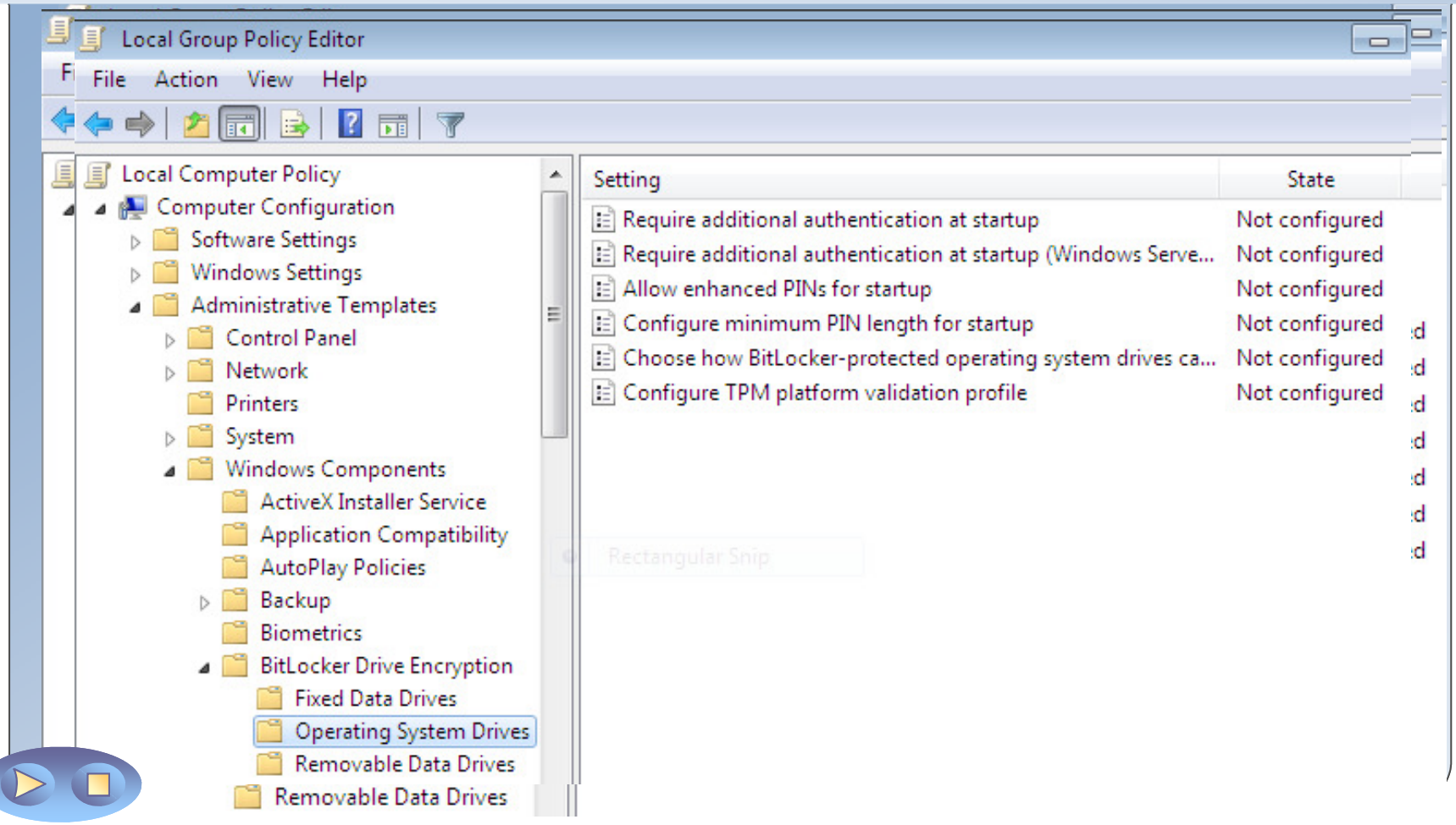
- Locks the normal boot process until the user optionally supplies a personal PIN and/or inserts a USB drive containing a BitLocker startup key
- Performs system integrity verification on boot components

Non-TPM mode

- Uses Group Policy to allow BitLocker to work without a TPM
- Locks the boot process similar to TPM mode, but the BitLocker startup key must be stored on a USB drive
- Provides limited authentication

Group Policy Settings for BitLocker

Settings for Operating System Drives



Group Policy Settings for BitLocker

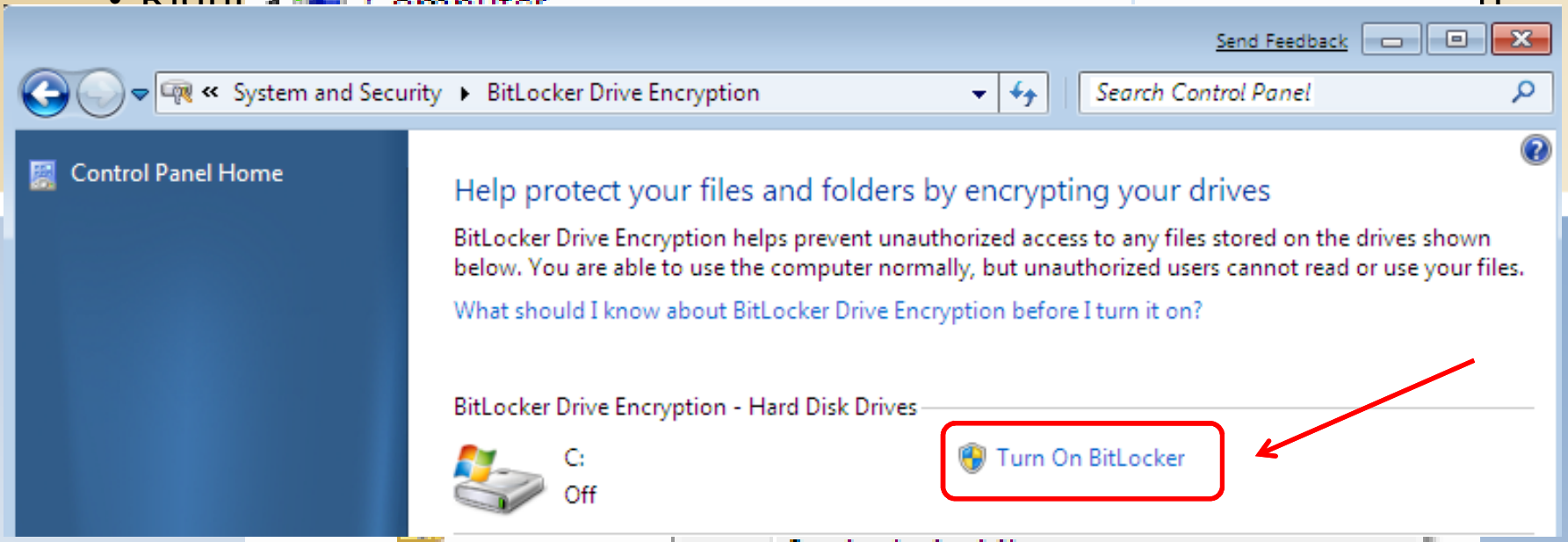
Group Policy provides the following settings for BitLocker:

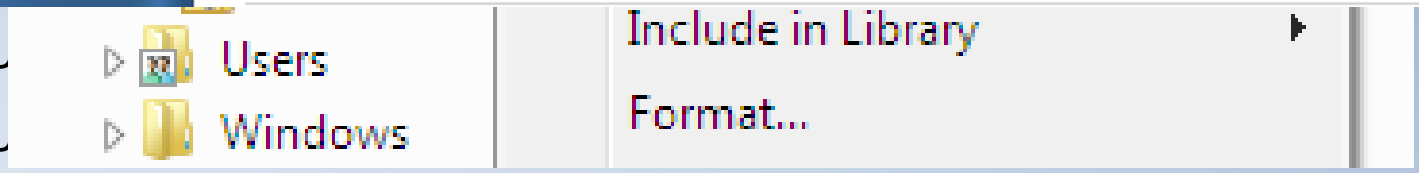
- Turn on BitLocker backup to Active Directory Domain Services
- Configure the recovery folder on Control Panel Setup
- Enable advanced startup options on Control Panel Setup
- Configure the encryption method
- Prevent memory overwrite on restart
- Configure TPM validation method used to seal BitLocker keys

Configuring BitLocker

Initiating BitLocker through the Control Panel

- Right
- U
- U
- No key





Configuring BitLocker

Three methods to enable BitLocker:

- From **System and Settings** in Control Panel
- Right-click the volume to be encrypted in Windows Explorer and select the **Turn on BitLocker** menu option
- Use the command-line tool titled **manage-bde.wsf**

Enabling BitLocker initiates a start-up wizard:

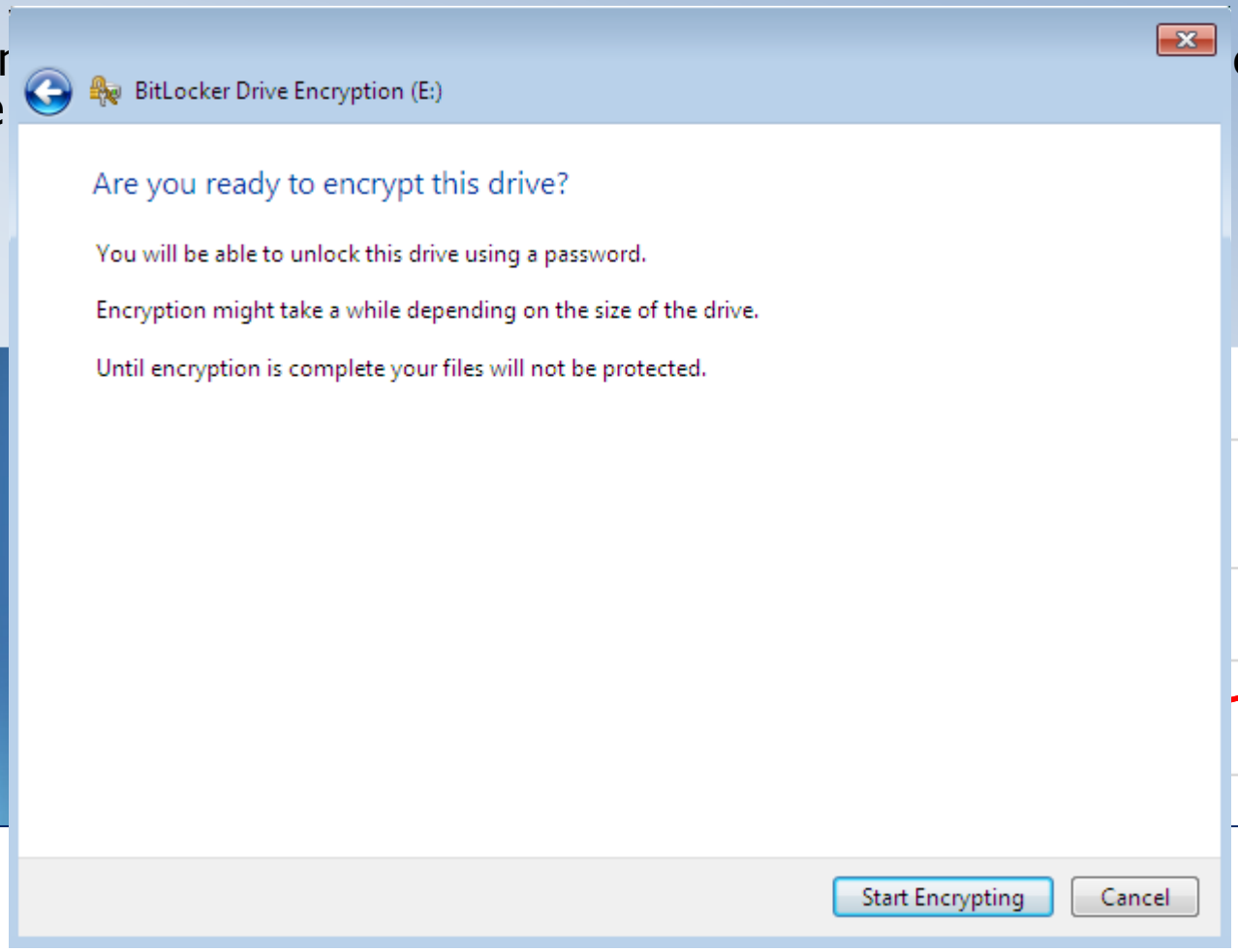
- Validates system requirements
- Creates the second partition if it does not already exist
- Allows you to configure how to access an encrypted drive:
  - USB
  - User function keys to enter the Passphrase
  - No key

Configuring BitLocker To Go

Encrypt the Drive

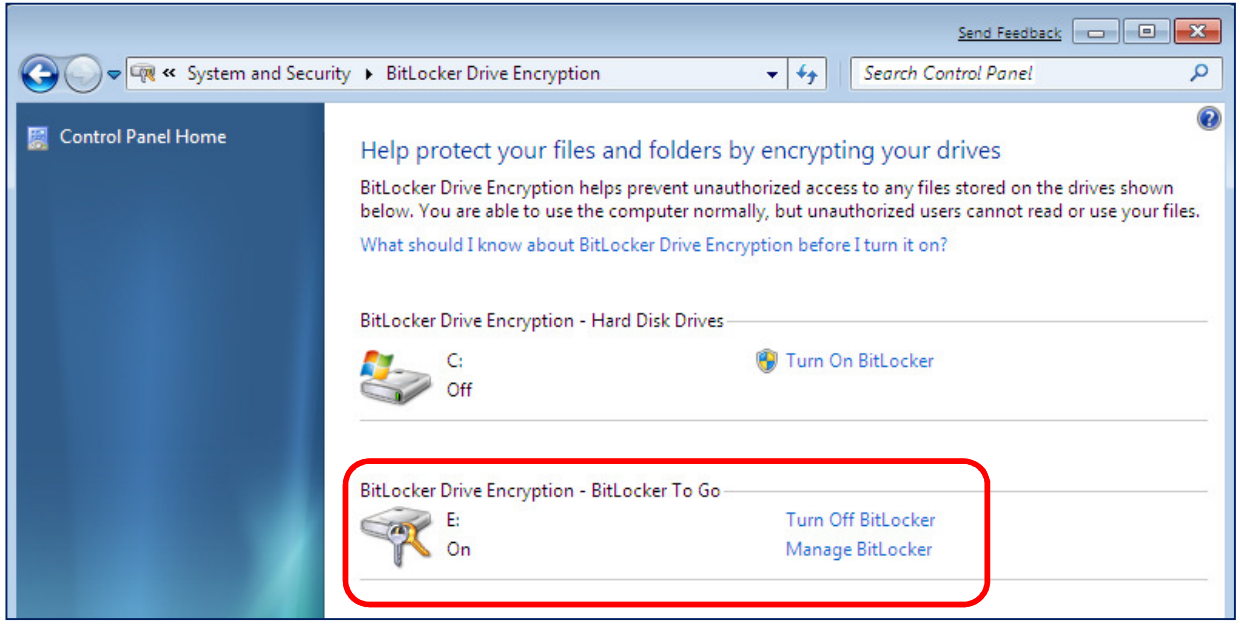
- Select or
  BitLocke
  - Unlock
  - Unlock
  - Always

ed with



Configuring BitLocker To Go

- Enable BitLocker To Go Drive Encryption by right-clicking the portable device (such as a USB drive) and then clicking **Turn On BitLocker**
- Select one of the following settings to unlock a drive encrypted with BitLocker To Go:
  - Unlock with a Recovery Password or passphrase
  - Unlock with a Smart Card
  - Always auto-unlock this device on this PC



Recovering BitLocker Encrypted Drives

When a BitLocker-enabled computer starts:

- BitLocker checks the operating system for conditions indicating a security risk
- If a condition is detected:
  - BitLocker enters recovery mode and keeps the system drive locked
  - The user must enter the correct Recovery Password to continue

The BitLocker Recovery Password is:

- A 48-digit password used to unlock a system in recovery mode
- Unique to a particular BitLocker encryption
- Can be stored in Active Directory
- If stored in Active Directory, search for it by using either the drive label or the computer's password

Lesson 4: Configuring Application Restrictions

- What Is AppLocker?
- AppLocker Rules
- Demonstration: Configuring AppLocker Rules
- Demonstration: Enforcing AppLocker Rules
- What Are Software Restriction Policies?

What Is AppLocker?

AppLocker is a new Windows 7 security feature that enables IT professionals to specify exactly what is allowed to run on user desktops

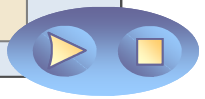
Benefits of AppLocker

- Controls how users can access and run all types of applications
- Ensures that user desktops are running only approved, licensed software

AppLocker Rules

Creating Custom Rules

- Use an AppLocker wizard found in the Local Security Policy Console to automatically generate rules
- You can configure Executable rules, Windows Installer rules, and Script rules
- You can specify a folder that contains the .exe files for the applications that apply to the rule
- You can create exceptions for .exe files
- You can create rules based on the digital signature of an application
- You can manually create a custom rule for a given executable



AppLocker Rules

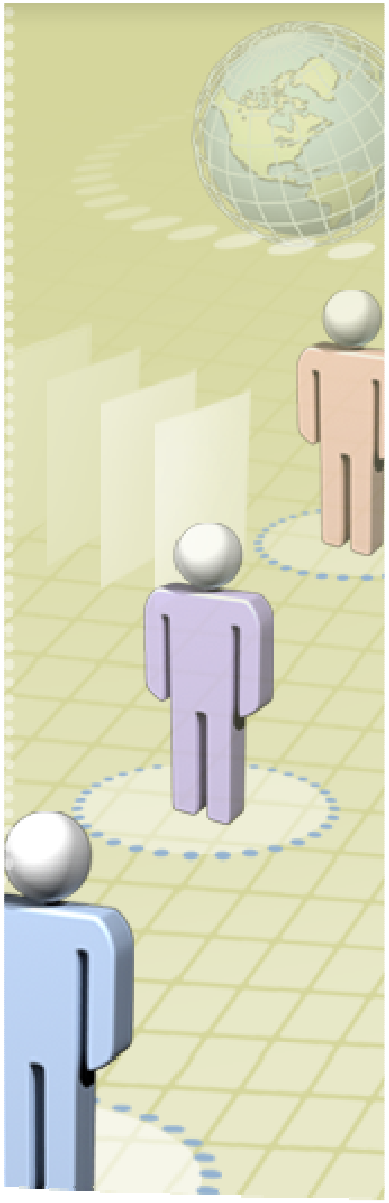
Create default AppLocker rules first, before manually creating new rules or automatically generating rules for a specific folder

Default rules enable the following:

- All users to run files in the default Program Files directory
- All users to run all files signed by the Windows operating system
- Members of the built-in Administrators group to run all files

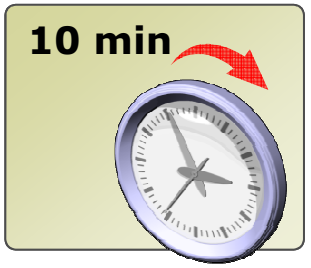
Create custom rules and automatically generate rules using an AppLocker wizard found in the Local Security Policy Console

Demonstration: Configuring AppLocker Rules



In this demonstration, you will see how to:

- Create new executable rule
- Create new Windows Installer rule
- Automatically generate Script rules



Notes Over-flow Slide

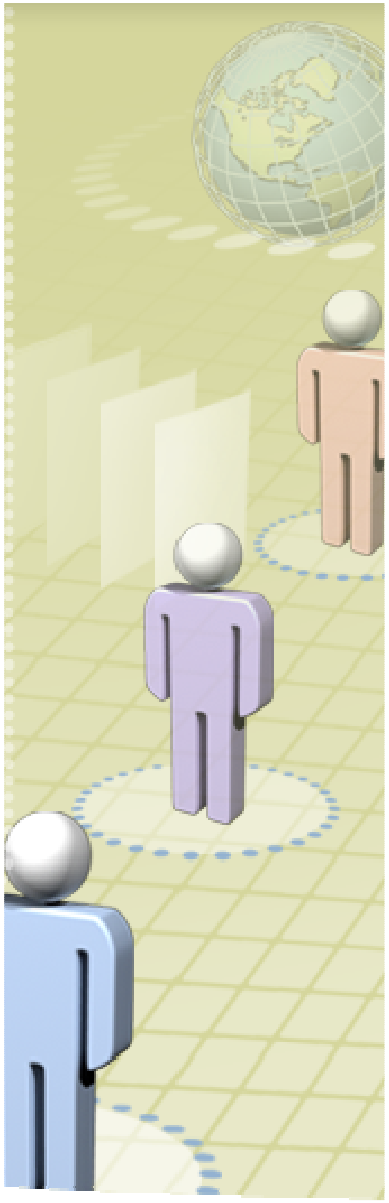
General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

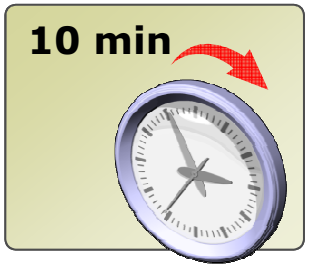
- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Demonstration: Enforcing AppLocker Rules



In this demonstration, you will see how to:

- Enforce AppLocker Rules
- Confirm the executable rule enforcement
- Confirm the Windows Installer rule enforcement



Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

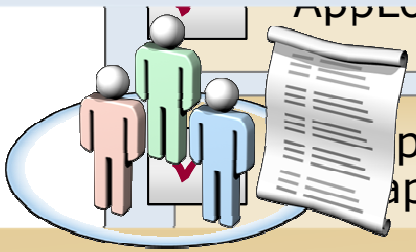
Printing Hidden Slides

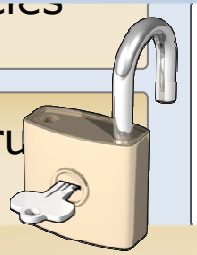
- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

What Are Software Restriction Policies?

Software Restriction Policies (SRP) allow administrators to identify which software is allowed to run

- SRP was added in Windows XP and Windows Server 2003
- SRP was designed to help organizations control not just hostile code, but any unknown code - malicious or otherwise
- SRP consists of a default security level and all the rules that apply to a Group Policy Object (GPO)





Comparing SRP and AppLocker

How does SRP compare to Windows AppLocker?

What Are Software Restriction Policies?

Software Restriction Policies (SRP) allow administrators to identify which software is allowed to run

- SRP was added in Windows XP and Windows Server 2003
- SRP was designed to help organizations control not just hostile code, but any unknown code - malicious or otherwise
- SRP consists of a default security level and all the rules that apply to a Group Policy Object (GPO)

Comparing SRP and AppLocker

- AppLocker replaces the SRP feature from prior Windows versions
- SRP snap-in and SRP rules are included in Windows 7 for compatibility purposes
- AppLocker rules and GPOs are completely separate from SRP
- If AppLocker rules are defined, only those rules are applied and any existing SRP rules are ignored

Lesson 5: Configuring User Account Control

- What Is UAC?
- How UAC Works
- Demonstration: Configuring Group Policy Settings for UAC
- Configuring UAC Notification Settings

What Is UAC?

User Account Control (UAC) is a security feature that simplifies the ability of users to run as standard users and perform all necessary daily tasks

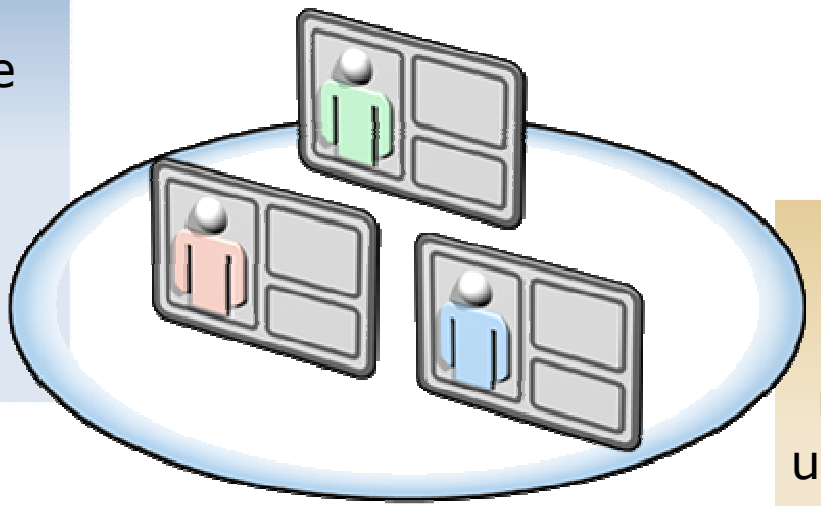
- UAC prompts the user for an administrative user's credentials if the task requires administrative permissions
- Windows 7 increases user control of the prompting experience

How UAC Works

In Windows 7, what happens when a user performs a task requiring administrative privileges?

Standard Users

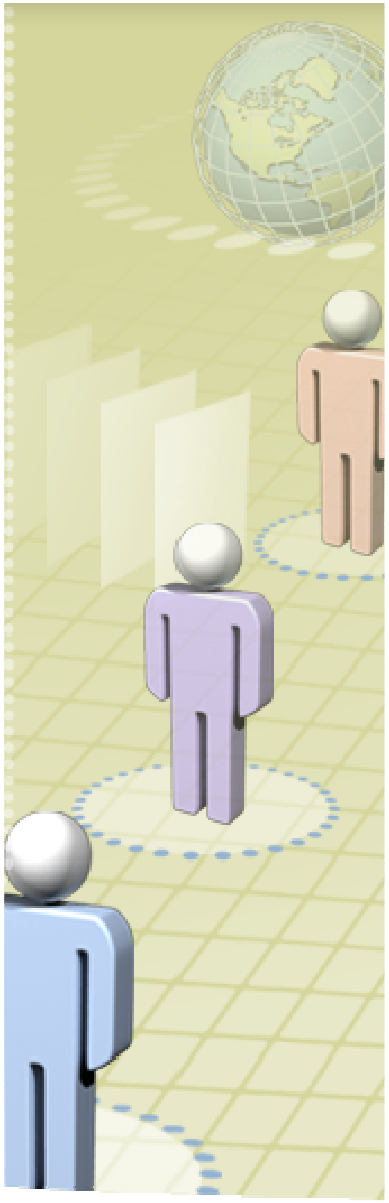
UAC prompts the user for the credentials of a user with administrative privileges



Administrative Users

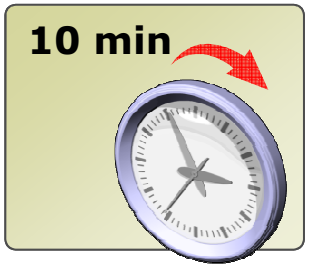
UAC prompts the user for permission to complete the task

Demonstration: Configuring Group Policy Settings for UAC



In this demonstration, you will see how to:

- Open the User Accounts window
- Review user groups
- View the Credential Prompt
- Change User Account Settings and View the Consent Prompt



Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

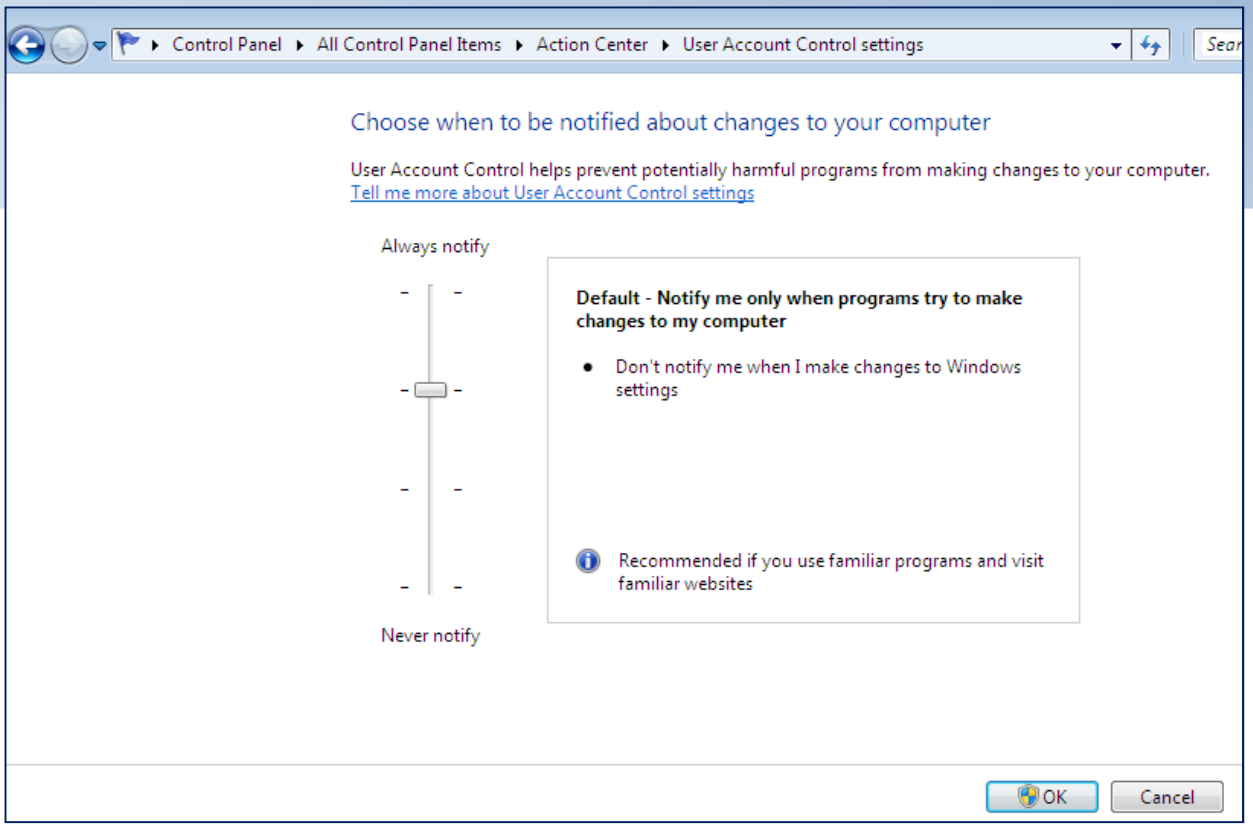
Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Configuring UAC Notification Settings

UAC elevation prompt settings include the following:

- Always notify me
- Notify me only when programs try to make changes to my computer
- Notify me only when programs try to make changes to my computer (do not dim my desktop)
- Never notify

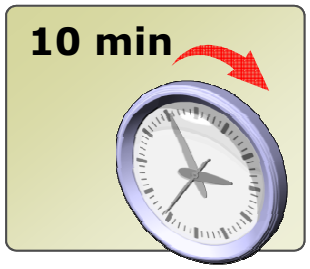


Lesson 6: Configuring Windows Firewall

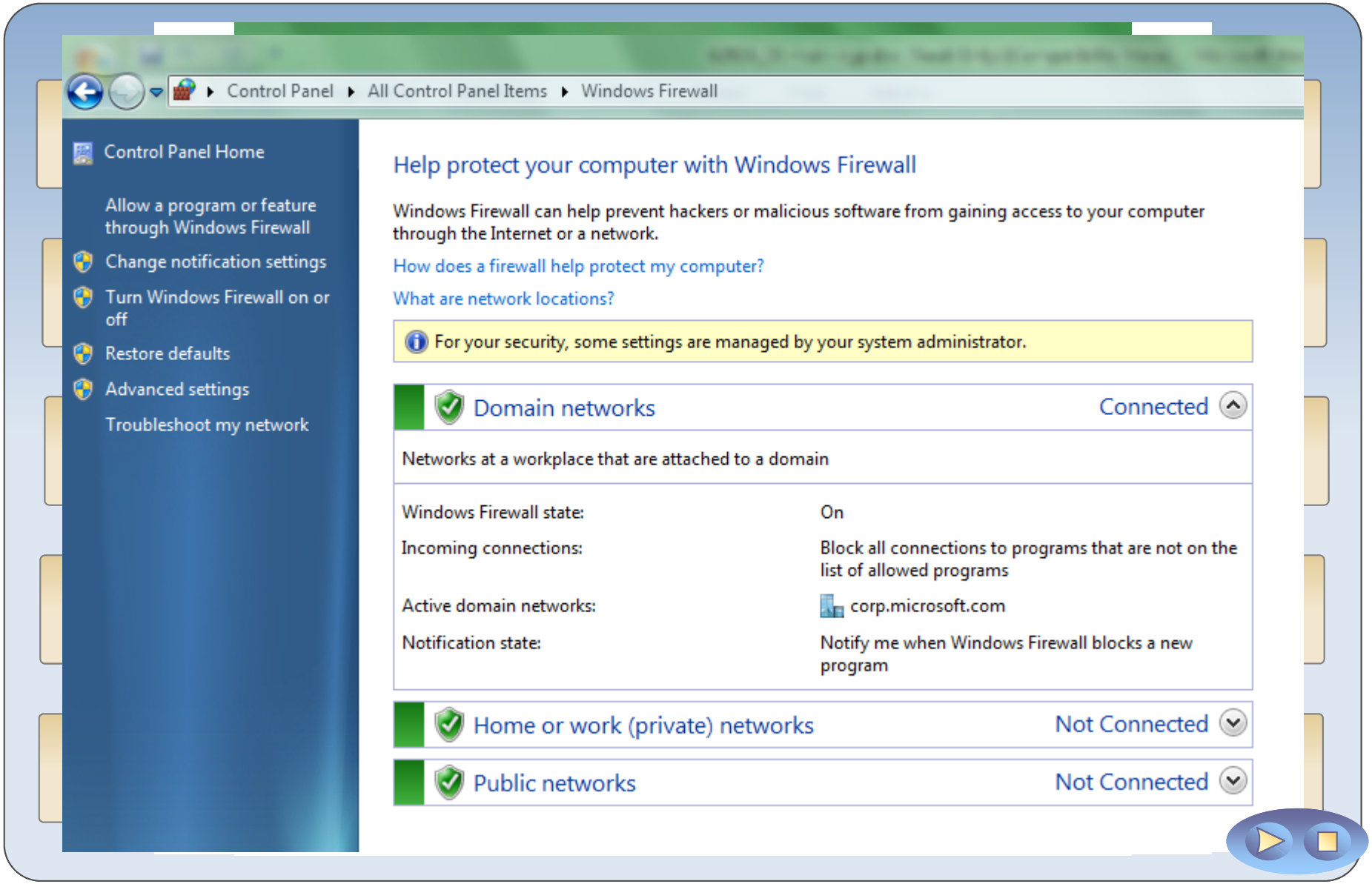
- Discussion: What Is a Firewall?
- Configuring the Basic Firewall Settings
- Windows Firewall with Advanced Security Settings
- Well-Known Ports Used by Applications
- Demonstration: Configuring Inbound, Outbound, and Connection Security Rules

Discussion: What Is a Firewall?

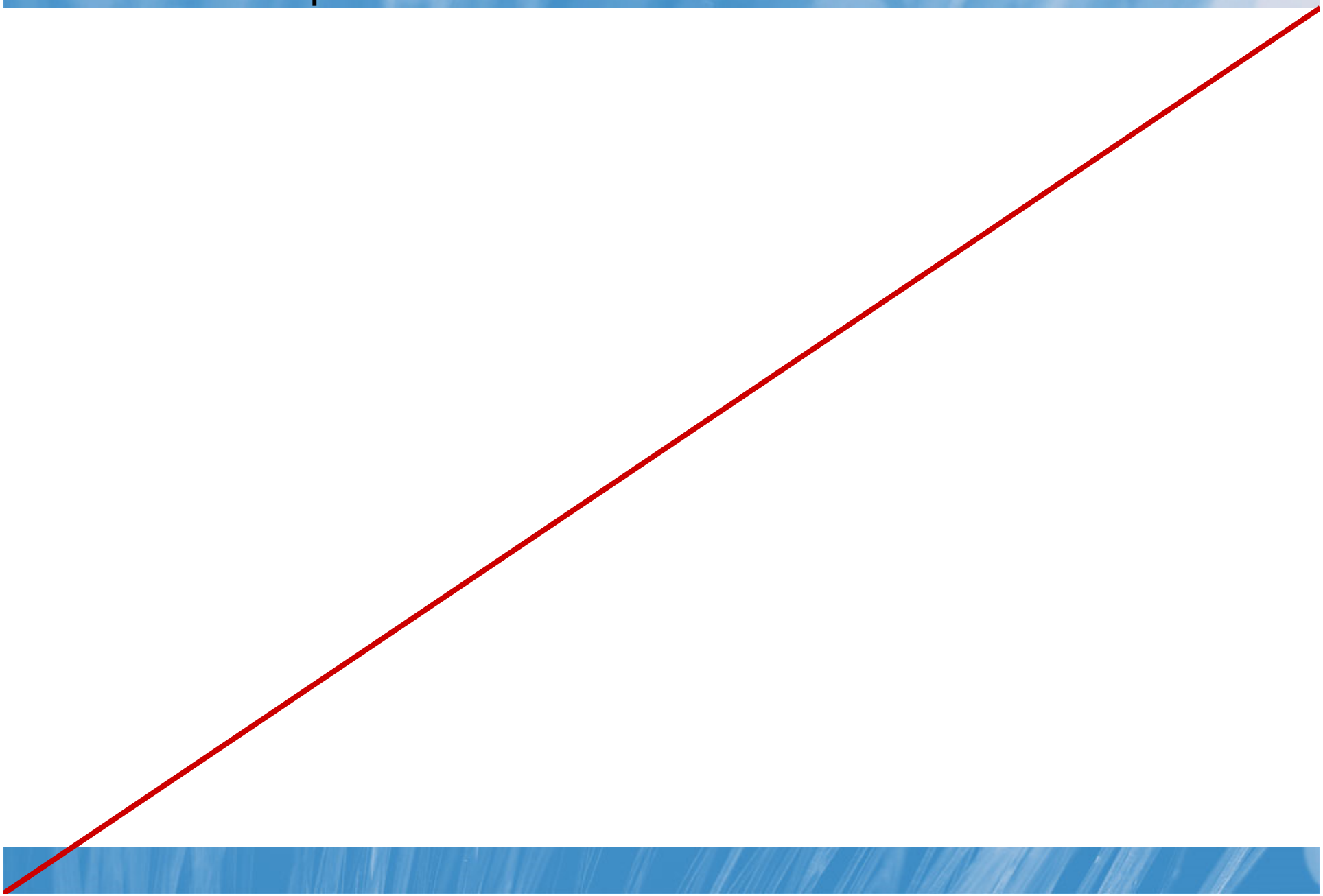
1. **What type of firewall does your organization currently use?**
2. **What are the reasons that it was selected?**



Configuring the Basic Firewall Settings



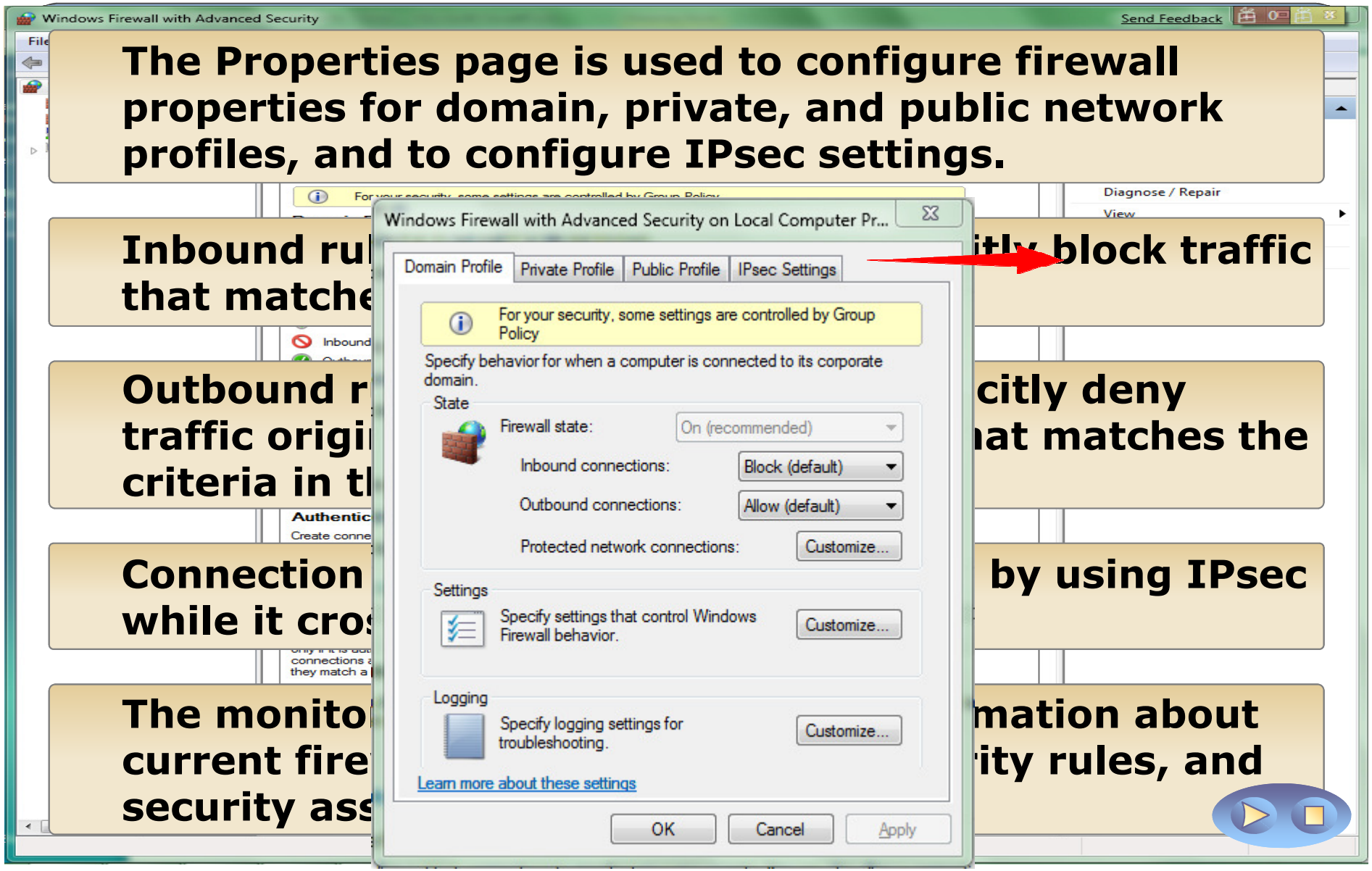
Notes Page Over-flow Slide. Do Not Print Slide. See Notes pane.



Configuring the Basic Firewall Settings

- **Configure network locations**
- **Turn Windows Firewall on or off and customize network location settings**
- **Add, change, or remove allowed programs and ports**
- **Set up or modify multiple active profile settings**
- **Configure Windows Firewall notifications**

Windows Firewall with Advanced Security Settings



Windows Firewall with Advanced Security Settings

The Properties page is used to configure firewall properties for domain, private, and public network profiles, and to configure IPsec settings.

Inbound rules explicitly allow or explicitly block traffic that matches criteria in the rule.

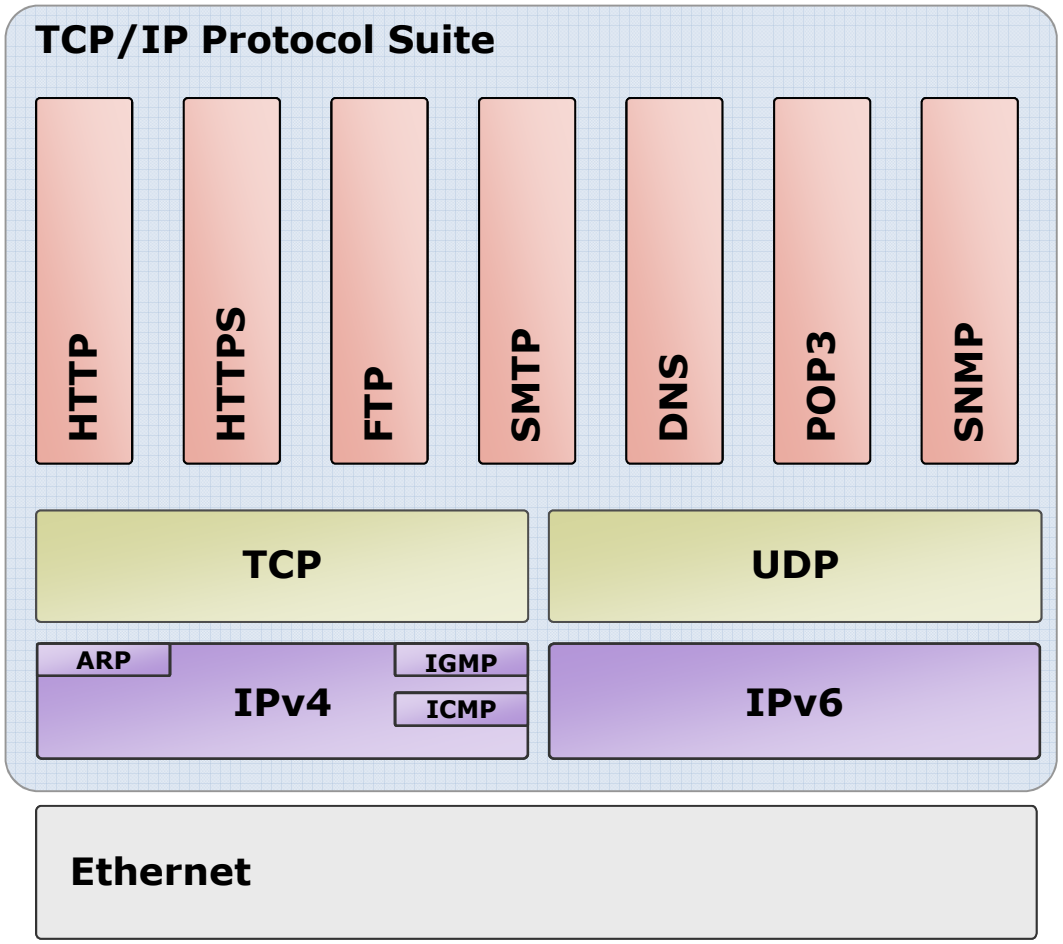
Outbound rules explicitly allow or explicitly deny traffic originating from the computer that matches the criteria in the rule.

Connection security rules secure traffic by using IPsec while it crosses the network.

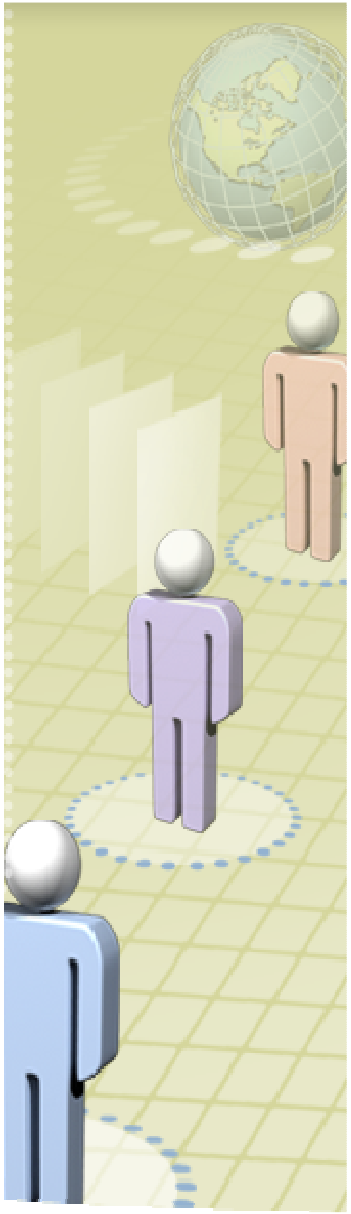
The monitoring interface displays information about current firewall rules, connection security rules, and security associations.

Well-Known Ports Used by Applications

When an application wants to establish communications with an application on a remote host, it creates a TCP or UDP socket.

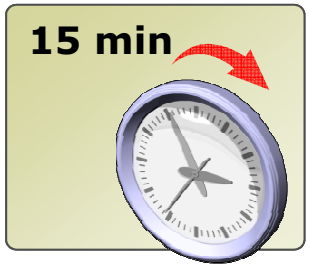


Demonstration: Configuring Inbound, Outbound, and Connection Security Rules

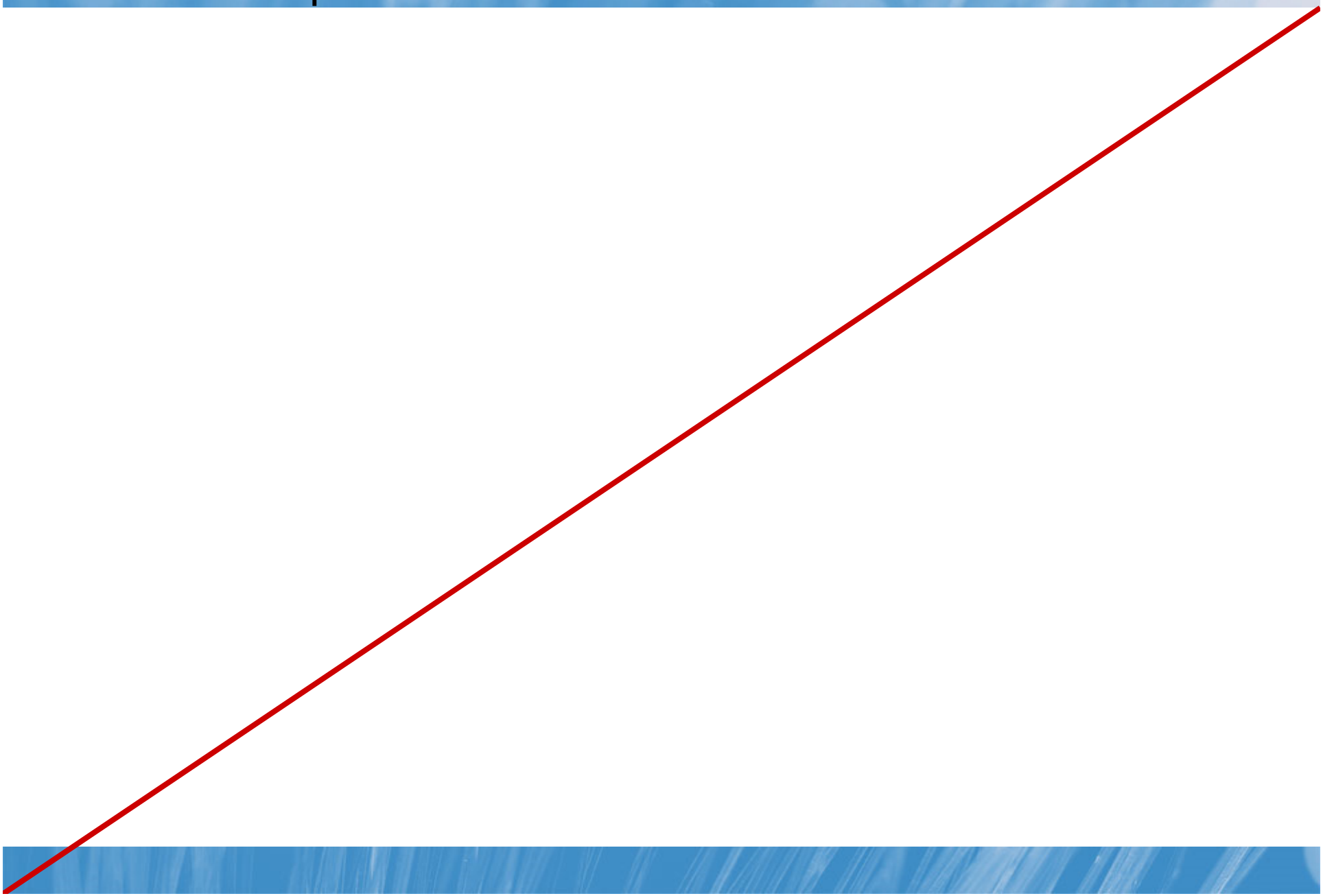


In this demonstration, you will see how to:

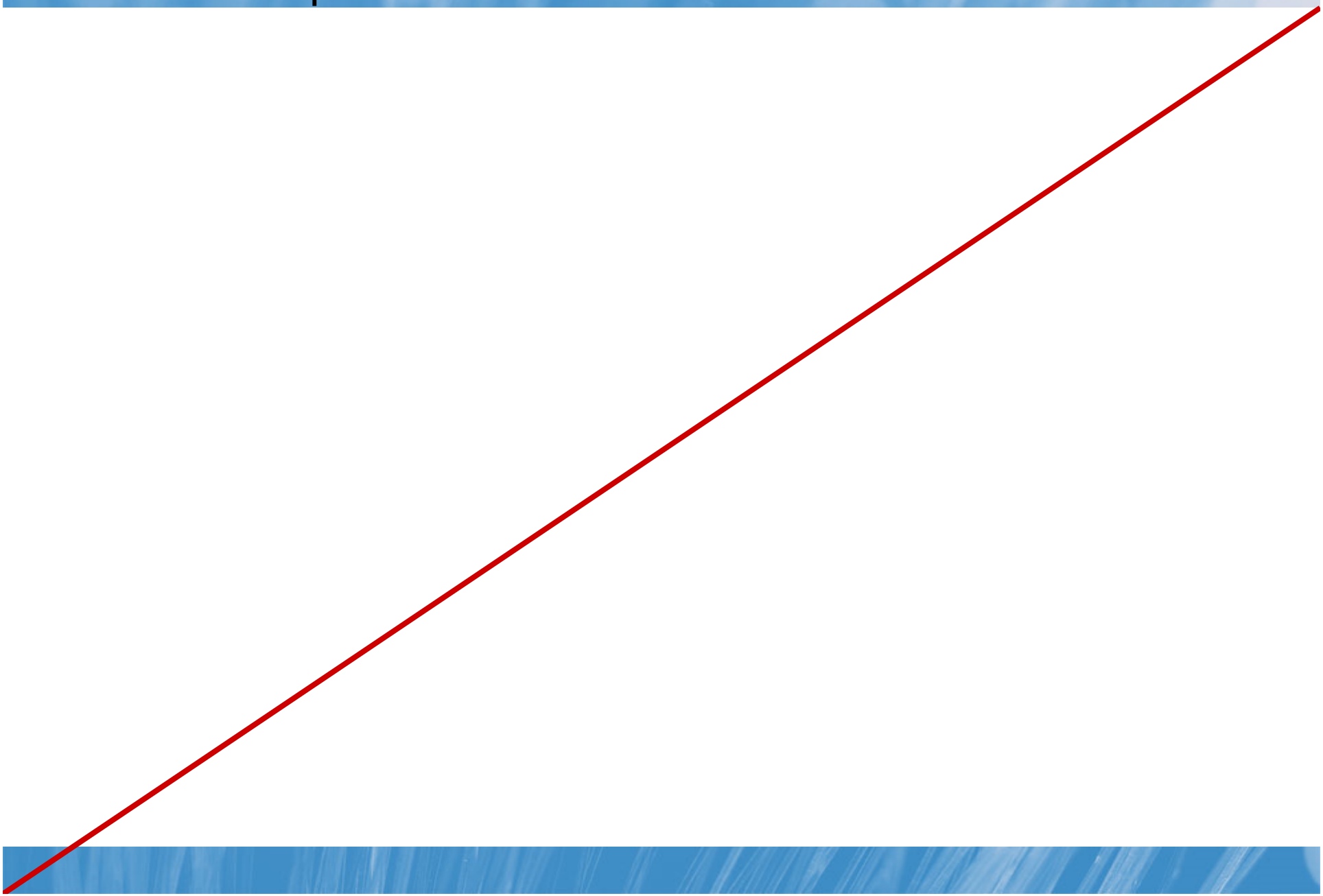
- Configure an Inbound Rule
- Configure an Outbound Rule
- Test the Outbound Rule
- Create a Connection Security Rule
- Review Monitoring Settings in Windows Firewall



Notes Page Over-flow Slide. Do Not Print Slide. See Notes pane.



Notes Page Over-flow Slide. Do Not Print Slide. See Notes pane.

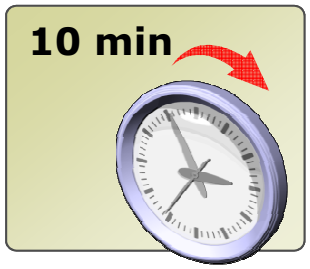


Lesson 7: Configuring Security Settings in Internet Explorer 8

- Discussion: Compatibility Feature in Internet Explorer 8
- Enhanced Privacy Features in Internet Explorer 8
- The SmartScreen Feature in Internet Explorer 8
- Other Security Features in Internet Explorer 8
- Demonstration: Configuring Security in Internet Explorer 8

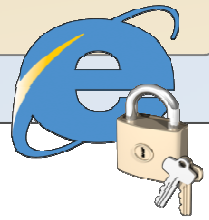
Discussion: Compatibility Features in Internet Explorer 8

What compatibility issues do you think you may encounter when updating Internet Explorer?



Enhanced Privacy Features in Internet Explorer 8

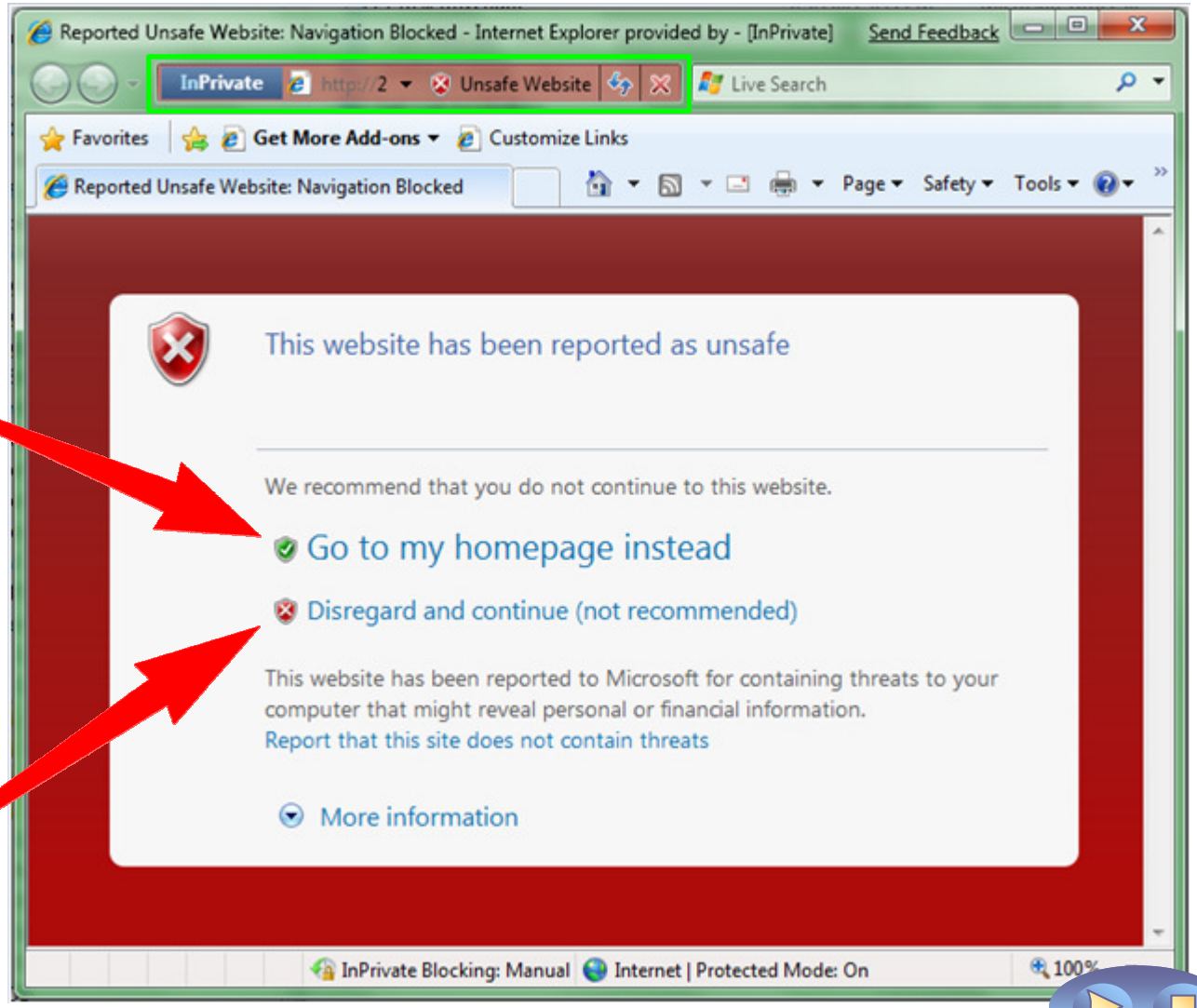
- **InPrivate Browsing** - inherently more secure than using Delete Browsing History to maintain privacy because there are no logs kept or tracks made during browsing
- **InPrivate Filtering** - helps monitor the frequency of all third-party content as it appears across all Web sites visited by the user
- **Enhanced Delete Browsing History** - enables users and organizations to selectively delete browsing history



The SmartScreen Feature in Internet Explorer 8

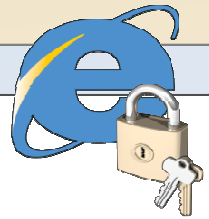
Use this link to navigate away from an unsafe Web site and start browsing from a trusted location

Use this link to ignore the warning; the address bar remains red as a persistent warning that the site is unsafe

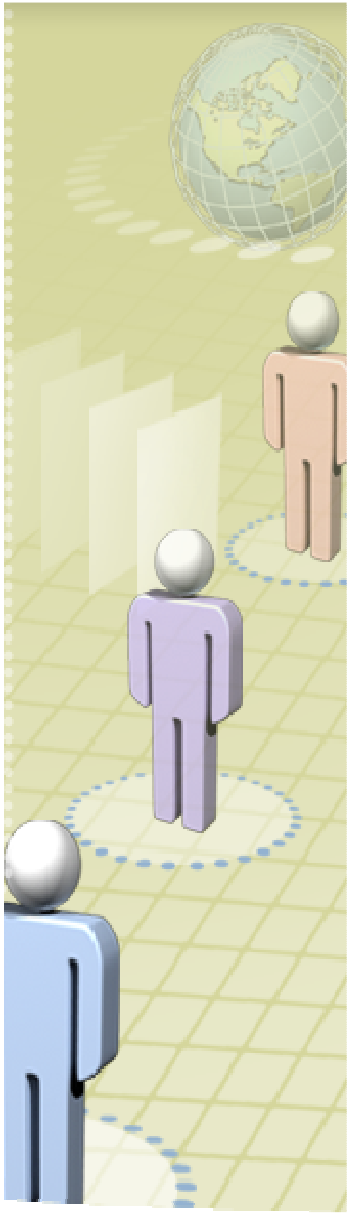


Other Security Features in Internet Explorer 8

- **Per-user ActiveX** - makes it possible for standard users to install ActiveX controls in their own user profile, without requiring administrative privileges
- **Per-site ActiveX** - IT professionals use Group Policy to preset allowed controls and their related domains
- **XSS Filter** - identifies and neutralizes a cross-site scripting attack if it is replayed in the server's response
- **DEP/NX protection** - helps thwart attacks by preventing code from running in memory that is marked non-executable

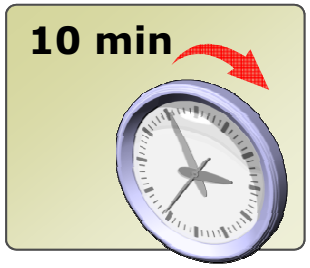


Demonstration: Configuring Security in Internet Explorer 8

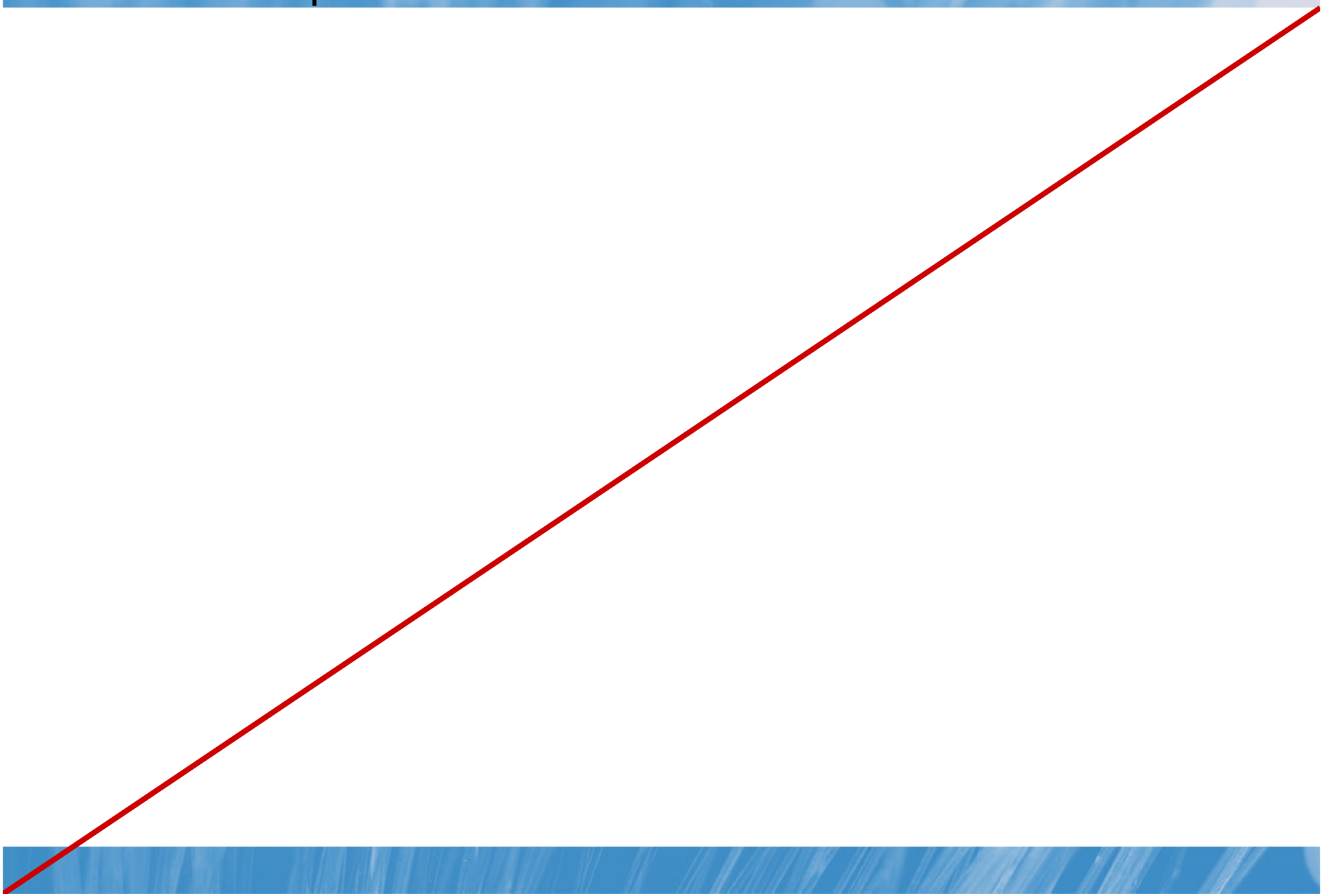


In this demonstration, you will see how to:

- Enable Compatibility View for All Web Sites
- Delete Browsing History
- Configure InPrivate Browsing
- Configure InPrivate Filtering
- View Add-on Management Interface



Notes Page Over-flow Slide. Do Not Print Slide. See Notes pane.



Lesson 8: Configuring Windows Defender

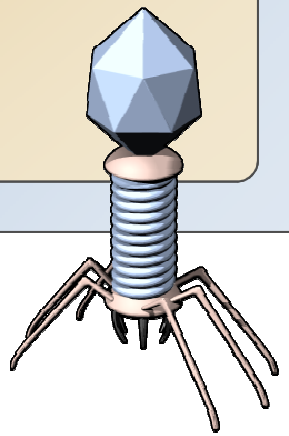
- What Is Malicious Software?
- What Is Windows Defender?
- Scanning Options in Windows Defender
- Demonstration: Configuring Windows Defender Settings

What Is Malicious Software?

Malicious software is software that is designed to deliberately harm a computer.

Malicious software includes:

- Viruses
- Worms
- Trojan horses
- Spyware
- Adware

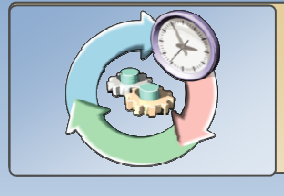


Malicious software leads to:

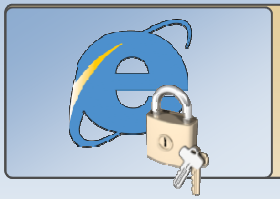
- Poor performance
- Loss of data
- Compromise of private information
- Reduction in end user efficiency
- Unapproved computer configuration changes

What Is Windows Defender?

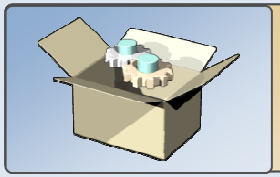
Windows Defender is software that helps protect the computer against security threats by detecting and removing known spyware from the computer.



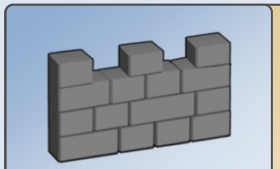
Schedules scans to occur on a regular basis



Provides configurable responses to severe, high, medium, and low alert levels



Works with Windows Update to automatically install new spyware definitions



Provides customizable options to exclude files, folders, and file types

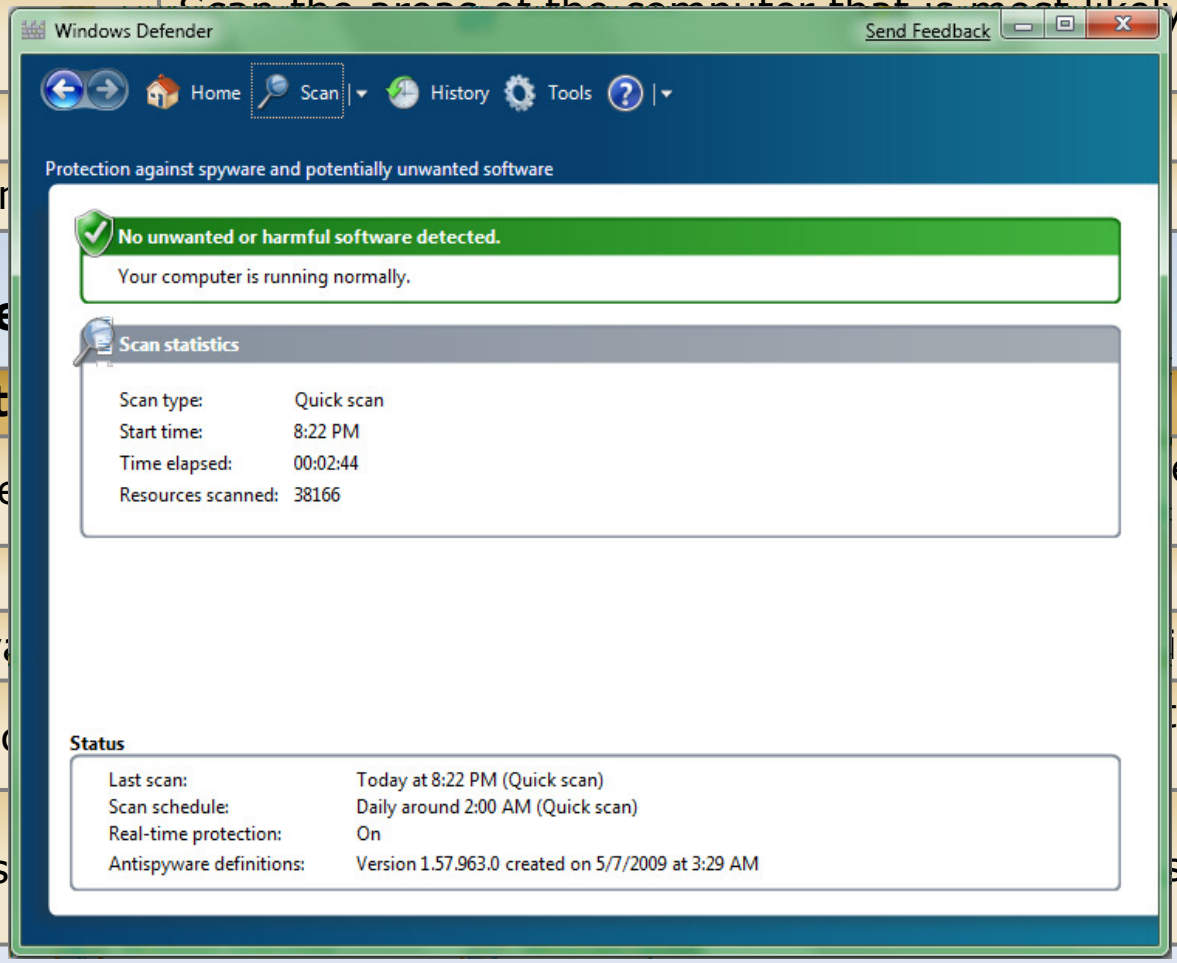
Scanning Options in Windows Defender

When a scan is complete, results display on the Home page.

Quick scan
Full scan
Custom scan

You define

Opt
Scan archive
Scan e-mail
Scan remova
Use heuristi
Create a res



Scanning Options in Windows Defender

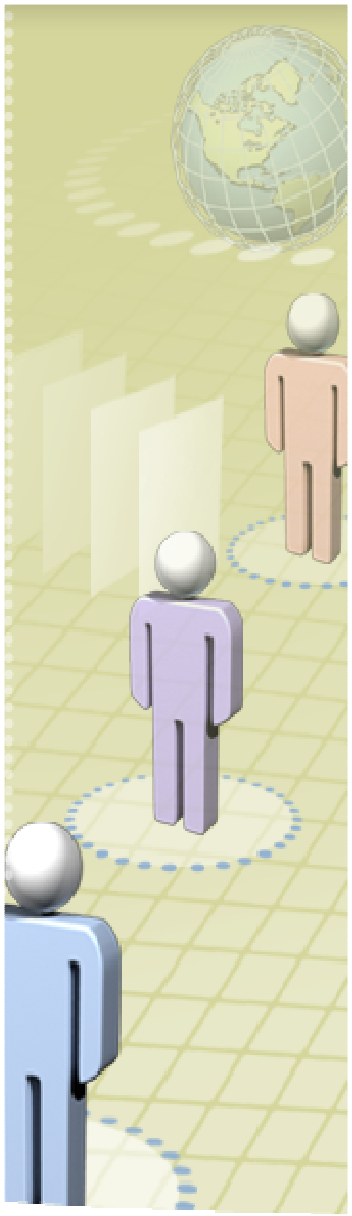
You define when to scan

Scan Type	Description
Quick scan	Scan the areas of the computer that is most likely to infect be infected
Full scan	Scan all areas of the computer
Custom scan	Scan specific areas of the computer only

You define what to scan

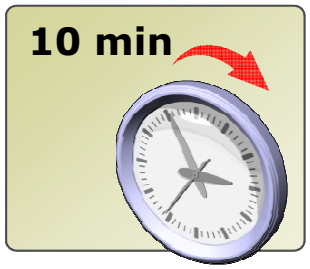
Option	Description
Scan archive files	May increase scanning time, but spyware likes to hide in these locations
Scan e-mail	Scan e-mail messages and attachments
Scan removable drives	Scan removable drives such as USB flash drives
Use heuristics	Alert you to potentially harmful behavior if it is not included in a definition file
Create a restore point	If detected items are automatically removed, this restores system settings if you want to use software you did not intend to remove

Demonstration: Configuring Windows Defender Settings

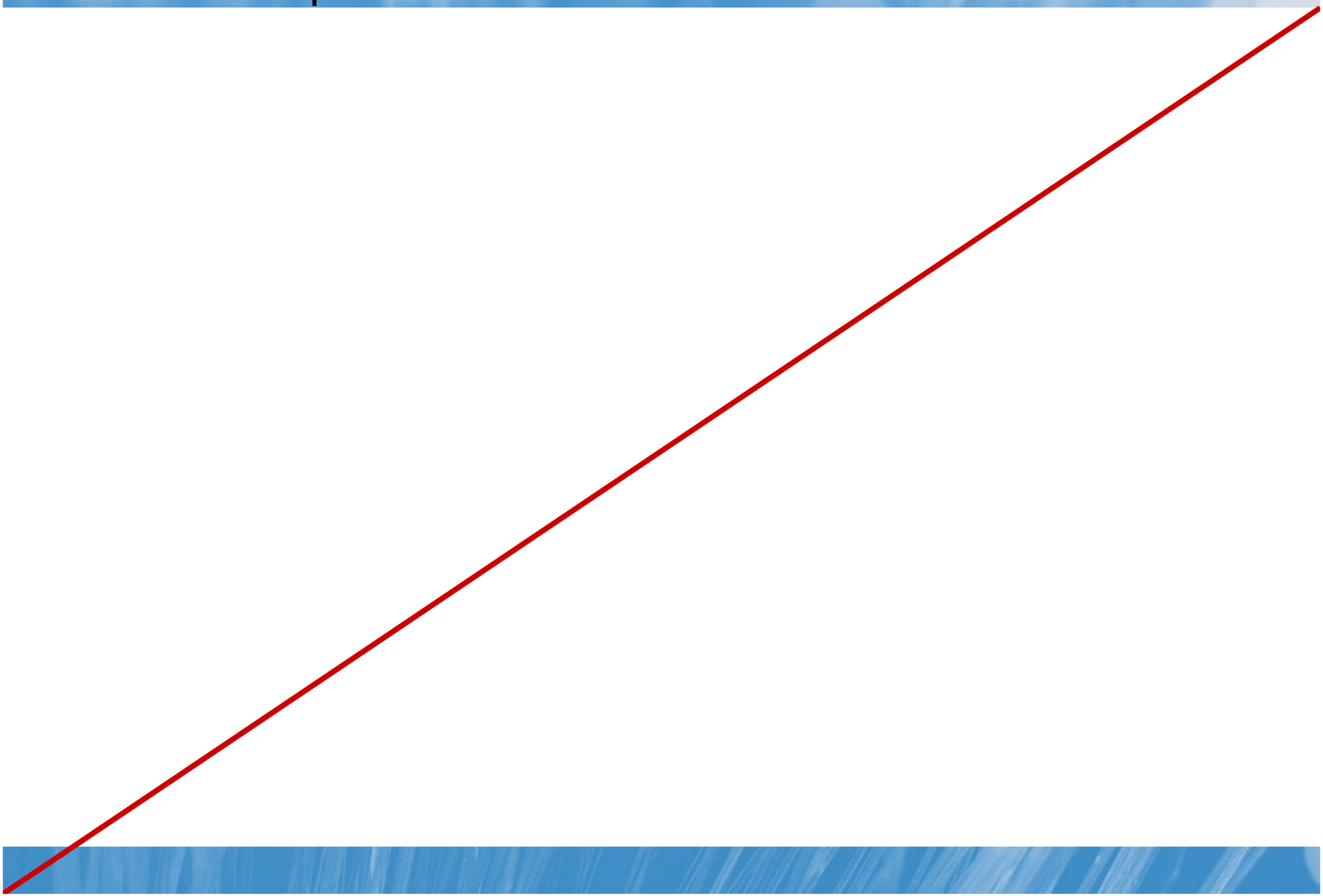


In this demonstration, you will see how to:

- Set Windows Defender Options
- View Quarantine Items
- View Allowed Items
- Microsoft SpyNet
- Windows Defender Website



Notes Page Over-flow Slide. Do Not Print Slide. See Notes pane.



Module Review and Takeaways

- Review questions
- Real-World Issues and Scenarios
- Common Issues
- Best Practices

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”

Notes Over-flow Slide

General information

- If you have too much Notes text associated with one slide to fit in one Notes Page, use the hidden Notes Over-flow Slide as page two of the Notes Page.
- The red line indicates that this slide must not be printed. In an actual module, do not add content to this slide or modify it in any other way. Only add content to the Notes Page.

Printing Hidden Slides

- Ensure that you print hidden slides when / if printing the Notes Pages. In the print dialog box, select “Print hidden slides”
- Ensure that you do ***not*** print hidden slides when / if printing the actual Slides. In the print dialog box, de-select “Print hidden slides”