Windows Vista Security

Security Enhancements for Windows Vista

ISACA
Serving IT Governance Professionals
San Francisco Chapter

MAZE & ASSOCIATES

Introductions

Donald E. Hester
CISSP, CISA, CAP, MCT, MCSE Security, MCSA Security, MCDST, Security+, CTT+, MV
Maze & Associates / San Diego City College
Email: DonaldH@MazeAssociates.com
LinkedIn https://www.linkedin.com/in/donaldehester

Introduce yourself:
What's your name?
What experience with Vista?
What have you heard about Vista?

Windows Vista Security

INTRODUCTION

Windows Vista Products

Windows Vista
Ultimate

Consumer Line up

Professional Line up

Emerging Markets

Windows
Starter

Windows Vista
Home Premium

Windows Vista
Enterprise

Windows Vista
Home Basic

Windows Vista
Business

Priority Shift

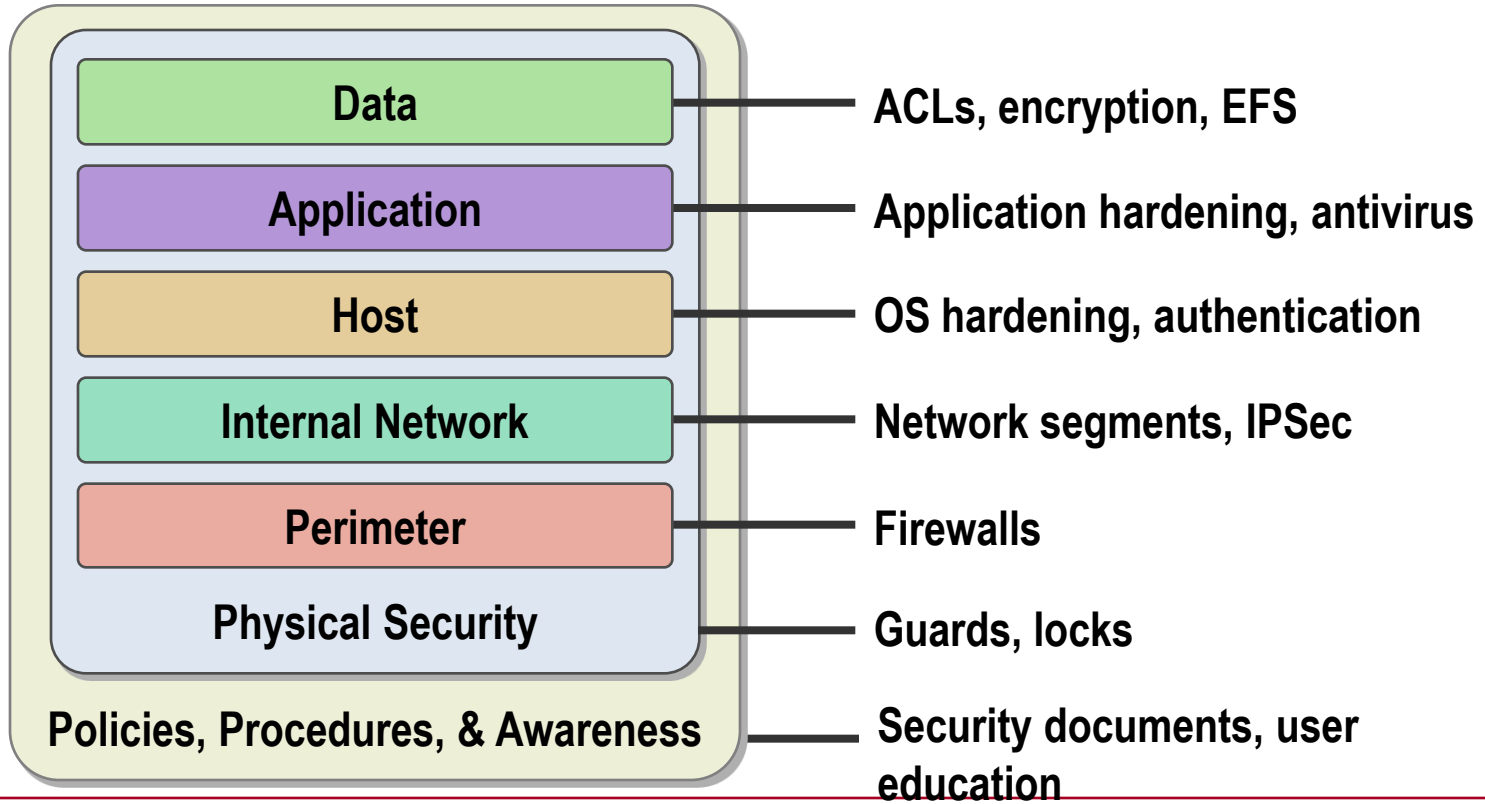
- In the past access was a top priority
  - Open-by-default
  - Start with everything open and then start locking down as needed
- Control is now a top priority
  - Closed-by-default
  - Start with everything closed and open only what is needed

Top to Bottom

- Security was a top priority at the very beginning.
- A paradigm shift in technology
- SDLC incorporated security at every level
- One goal was TCSEC (Orange Book) compliance (Level B)
- Many of the features designed to meet FISMA (NIST SP 800-53 rev1) requirements

What Is the Defense-in-Depth Model?

- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



Security and Compliance

Fundamentals

- Security Development Lifecycle
- Threat Modeling and Code Reviews
- Windows Service Hardening

Threat & Vulnerability Mitigation

- IE Protected Mode
- Windows Defender
- Network Access Protection

Identity & Access Control

- User Account Control
- Plug and Play Smartcards
- Granular Auditing

Information Protection

- BitLocker™ Drive Encryption
- EFS Smartcards
- RMS Client

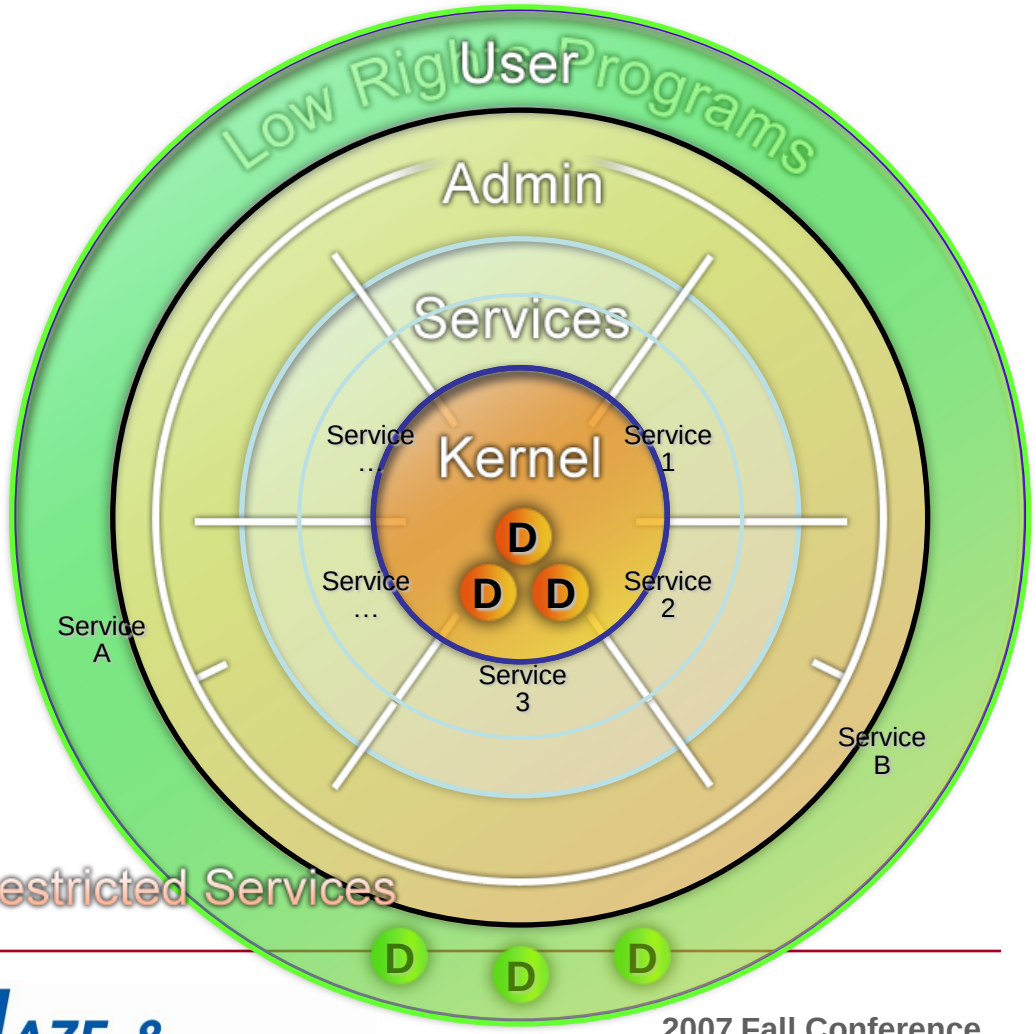
Windows Service Hardening

Defense-in-Depth: Factoring and Profiling of Windows Kernel

- Reduce size of high risk layers
- Segment the services
- Increase number of layers

D Kernel Drivers

D User-mode Drivers



Windows Vista Security Guide

- Released December 2006 / OS released January 2007 (a first for Microsoft)
- NSA and NIST had input
- Guide comes with two configurations
  - Enterprise Client (EC)
  - Specialized Security Limited Functionality (SSLF)
- OMB will require applications that will run on Federal government systems to meet SSLF standards (March 2007)

Identity & Access Management

Windows Rights Management Services

Microsoft Identity Integration Server 2003

Windows Active Directory

Security Fundamentals

Threat & Vulnerability Mitigation

Microsoft Internet Security & Acceleration Server

Sybari A Microsoft Subsidiary

Windows OneCare

Microsoft Internet Explorer 7.0

System Integrity

Microsoft Windows xp

Microsoft Windows Code Name Longhorn

Microsoft Windows Server 2003

Windows Vista™

Windows OneCare

Note:

- Network administrators are holding off on deployments for the wrong reasons
- It isn't that Vista isn't ready for the enterprise, it is the applications and administrators who are not ready
- Hopefully you will understand the security benefits and deploy it sooner and have a more secure enterprise
- Irrespective of the applications the OS has been designed with security in mind

The New Security Features

- User Account Control (UAC)
- Windows Defender
- Windows Firewall
- Windows Security Center
- Malicious Software Removal Tool (MSRT)
- Software Restriction Policies
- Internet Explorer 7
- Data Execution Protection (DEP)
- Windows Integrity Controls
- Windows Resource Protection (WRP)
- Code Integrity Checking
- BitLocker™ Drive Encryption
- Encrypting File System (EFS) Improvements
- Rights Management Services (RMS)
- Parental Controls
- Reliability and Performance Monitor
- Device Installation Restriction
- ACL Improvements
- Volume Shadow Copy
- Increased GPOs
- Secure Design SDLC
- Network Access Protection
- TCP/IP Next Generation
- Restart Manager
- Increased Audit Abilities
- RDP Improvements
- SMB v2
- User Account Changes
- Vista Security Guide & SSLF
- Event Viewer Improvements
- Problem Reports and Solutions

Windows Vista Security

Section 1: Malware Protection

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Malware protection

- Windows Vista includes several new and enhanced technologies that provide enhanced defense against malware. These technologies include:
  - User Account Control (UAC)
  - Windows Defender
  - Windows Firewall
  - Windows Security Center
  - Malicious Software Removal Tool (MSRT)
  - Software Restriction Policies
  - Internet Explorer 7
  - Data Execution Protection (DEP)
  - Integrity Controls
  - Windows Resource Protection (WRP)

Windows Vista Security

USER ACCOUNT CONTROL (UAC)

Intro

- User Account Control (UAC), a new set of features in Windows Vista, helps strike a balance between the flexibility and power of an administrator account and the security of a standard user account.
- UAC will help users run Vista without requiring administrator privileges to be productive. Administrators can also run most applications with a limited privilege, but have "elevation potential" for specific administrative tasks and application functions.

User Account Control (UAC)

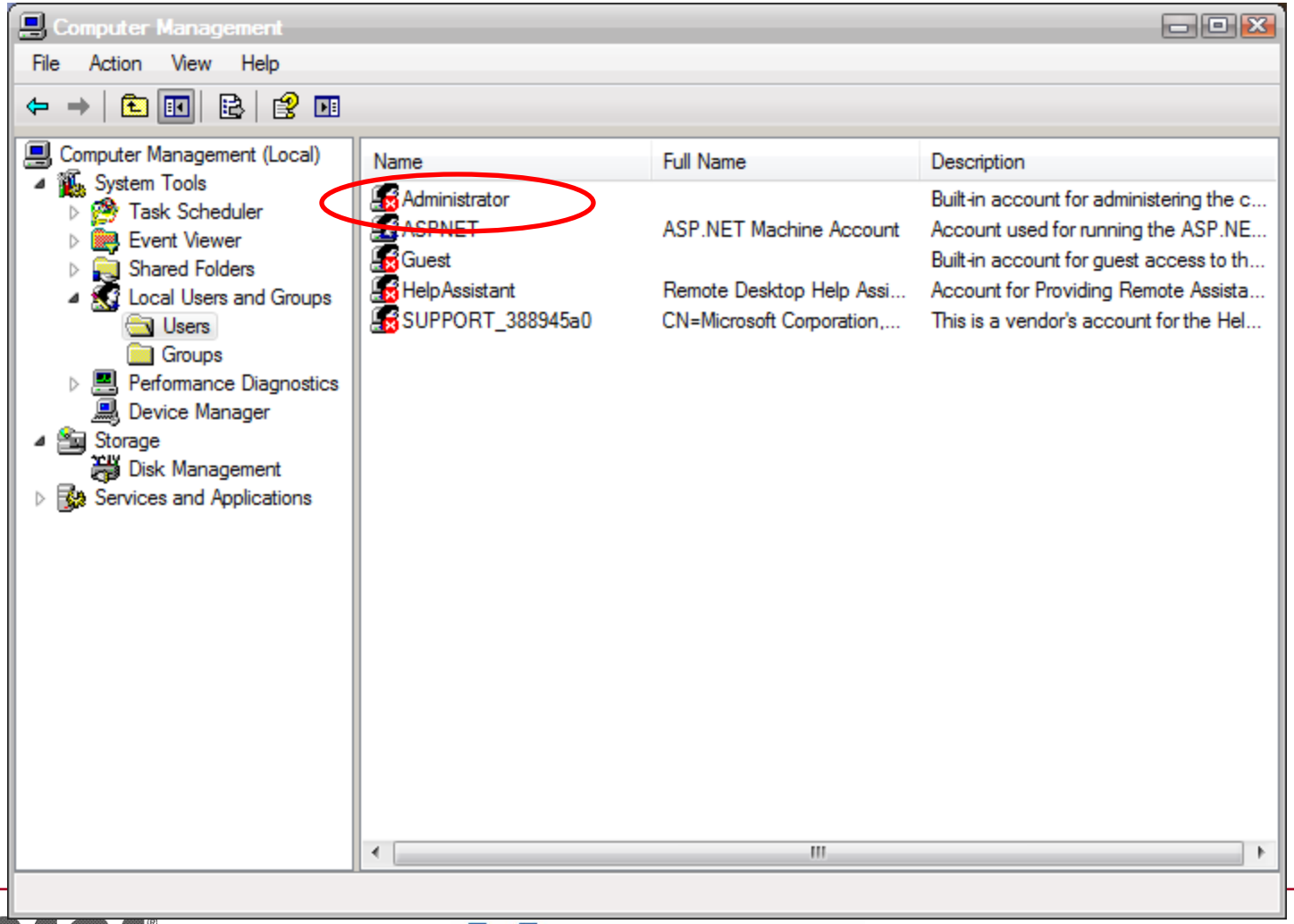
1. Businesses: Manage desktops better
2. Consumers: Use parental controls
   - Make the system work well for standard users
     - Change time zone and power settings, add printers, and connect to secure wireless networks
     - Make it clear when elevation to admin is required and allow without logging off
     - High application compatibility with file/registry virtualization
   - Administrators use full privilege only for admin tasks or applications
   - User provides explicit consent before using elevated privilege

User Type Changes

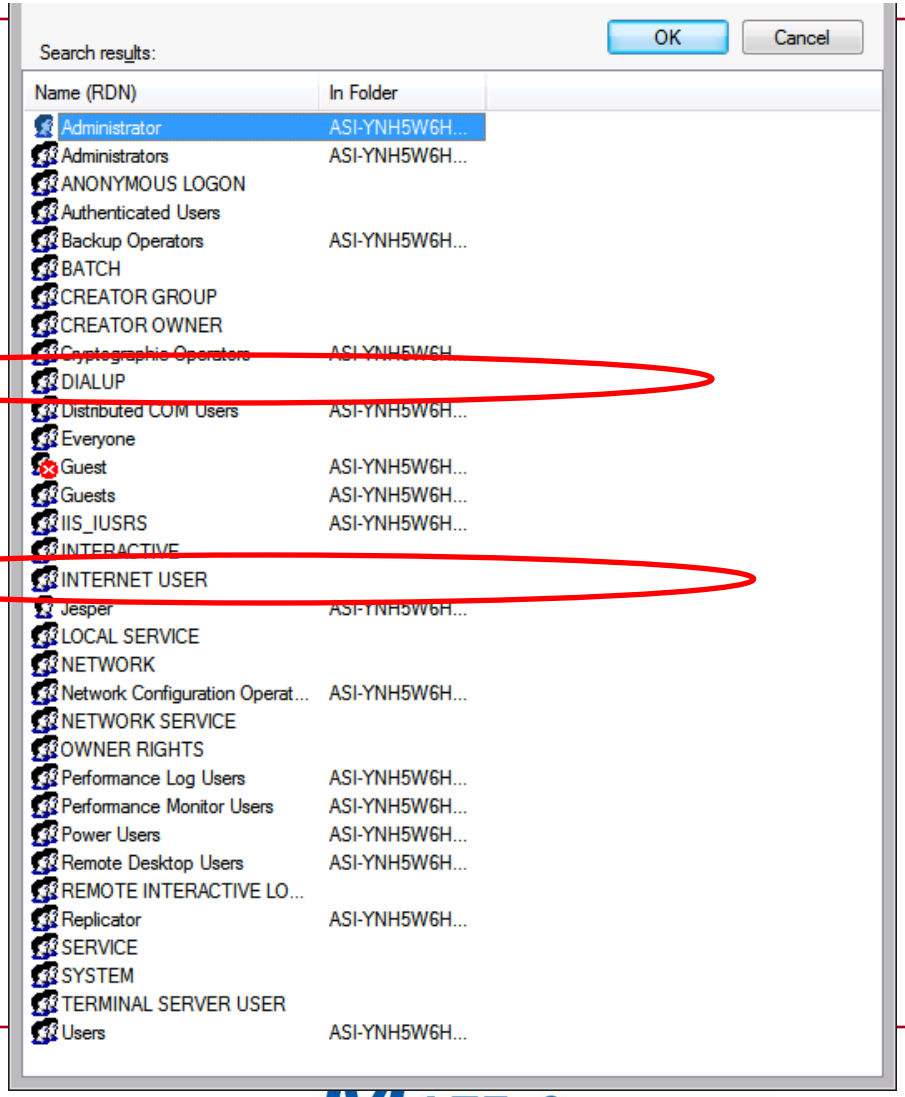
- Standard User
- Administrator
- No more “Power User”

“In response to the challenges customers encounter when attempting to run as a standard user, Microsoft began researching how to make running as a standard user easier for everyone.” Microsoft

Administrator Account Disabled by Default

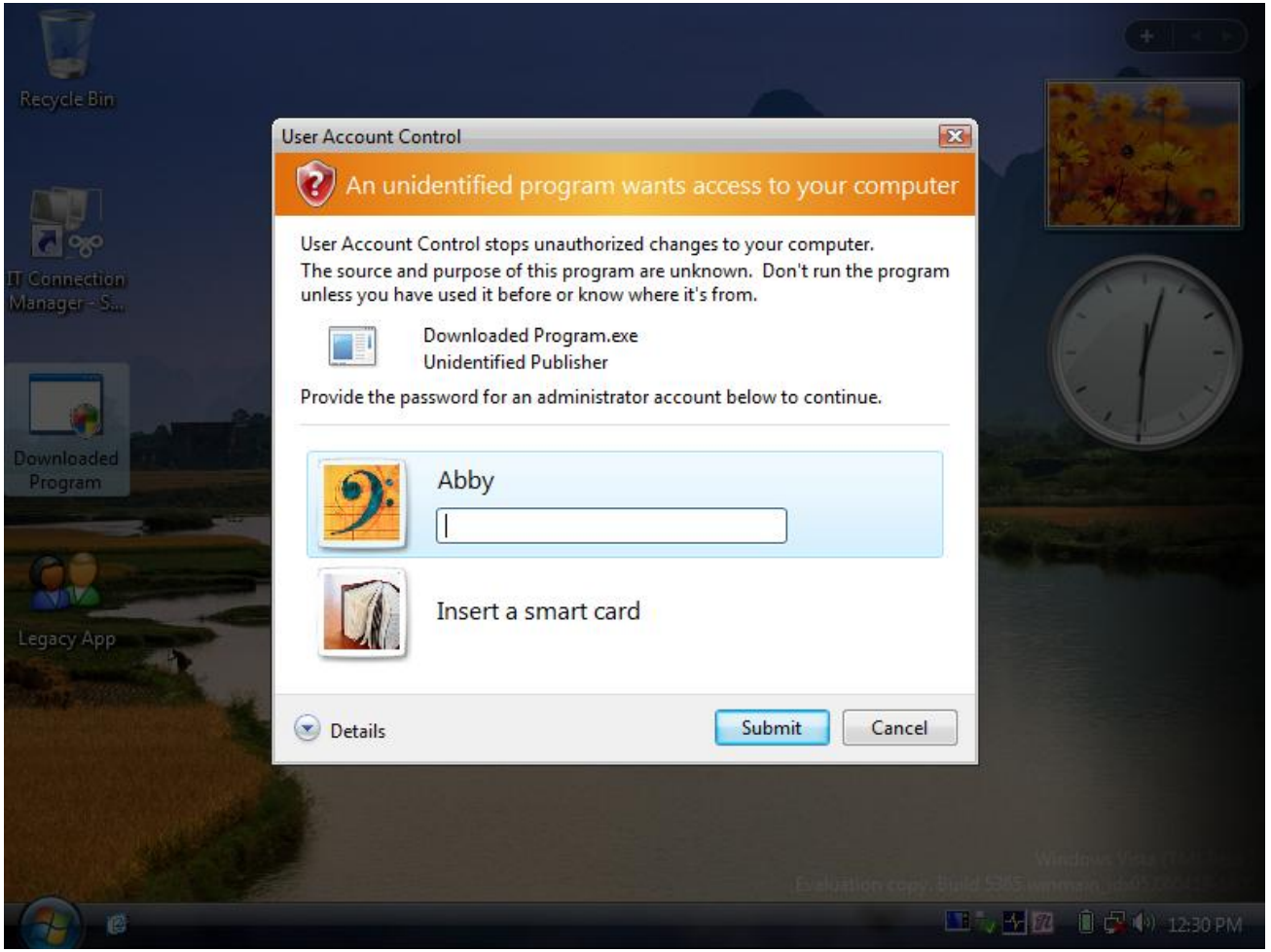


Some Additional User Groups



Credential Prompt

Replacement for “Run As”



Administrator

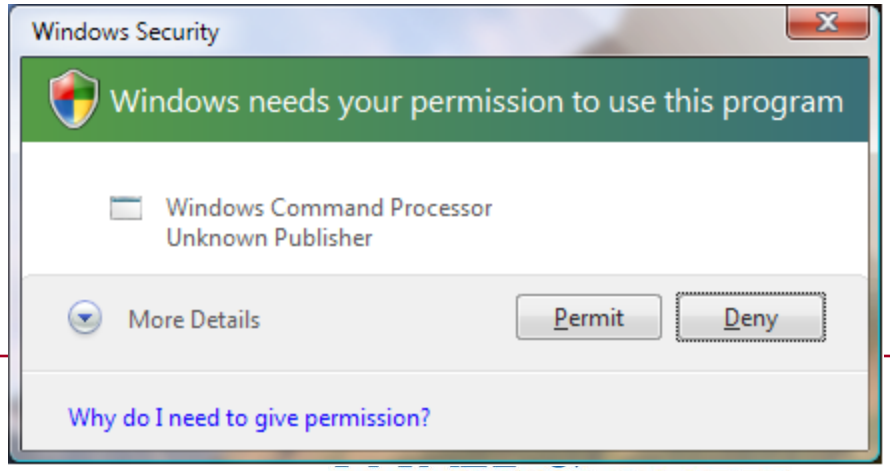
- When someone logs on as an administrator they will be given two tokens at the during the log on process. (AKA “split token” or “filtered token”)
  - One Standard user token
  - One Administrator token
- Administrators run in “Administrator Approved Mode” sometimes called “Protected Administrators”

Tokens

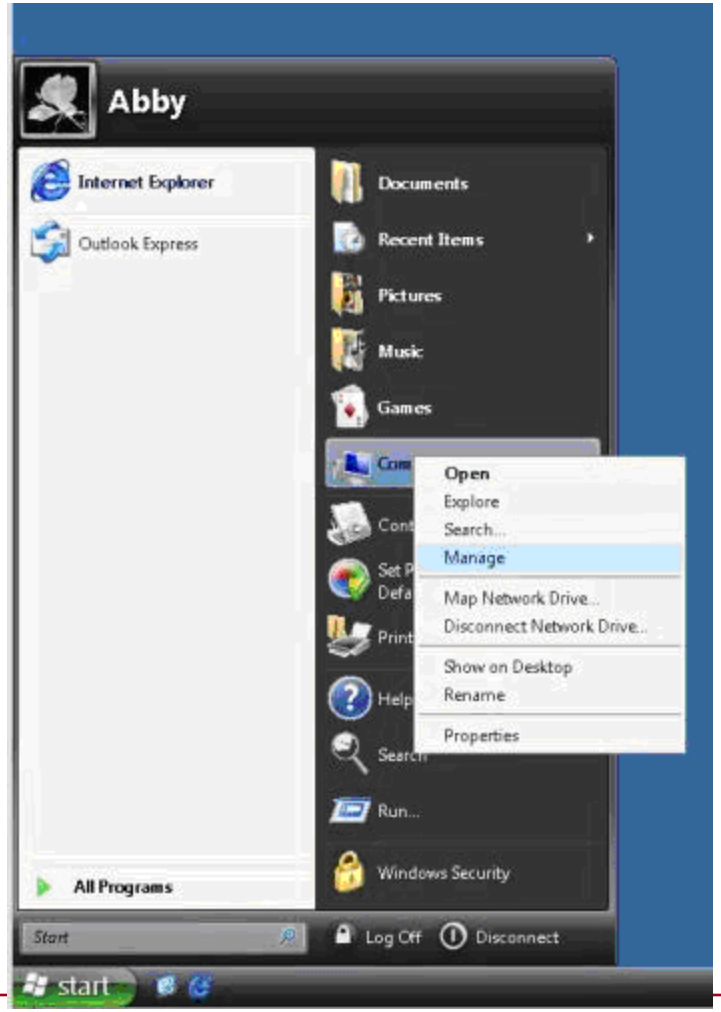
- Token contains a list of group memberships and privileges
- Token loaded into RAM
- When a program is launched a copy of the token is copied to the program. (You can not switch tokens unless you close and restart program)

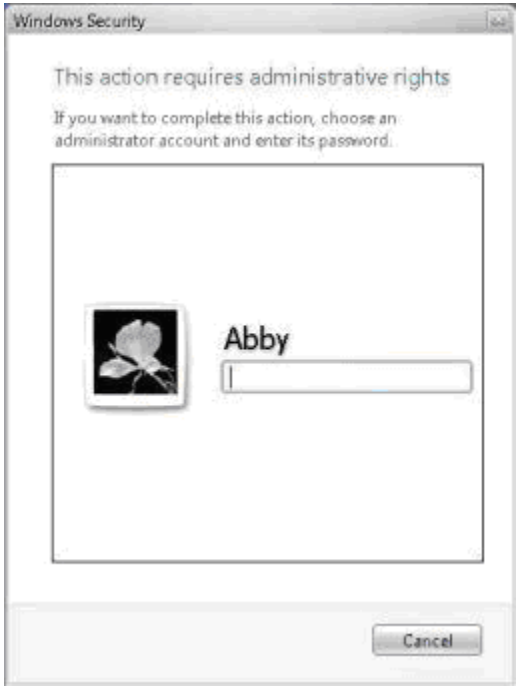
Administrator's Token

- Is not generally used when you launch a program. Vista will use the Standard User token.
- If Vista knows you need to use administrator token it will ask you if it can use it. (Consent UI or Consent Prompt)



Credential Prompting





Rights, Privileges & Permissions

- Rights – not on your token (10 different types a user can have)
- Permissions – not in your token (located on the object in DCAL & ACL)
- Privileges – on your token (34 different types a user can have)

Standard Users Privileges

- Shut the system down
- Manipulate a file
- Undock/dock laptop
- Increase the amount of memory a program uses
- Change time zone

Denied Privileges

- Create a token object
- Act as part of the operating system
- Take ownership
- Load and unload device drivers
- Back up and Restore
- Impersonate a client
- Modify Object label
- Debug programs

In Windows XP

- When a user is added to the local administrators group, that user is automatically granted every Windows privilege.

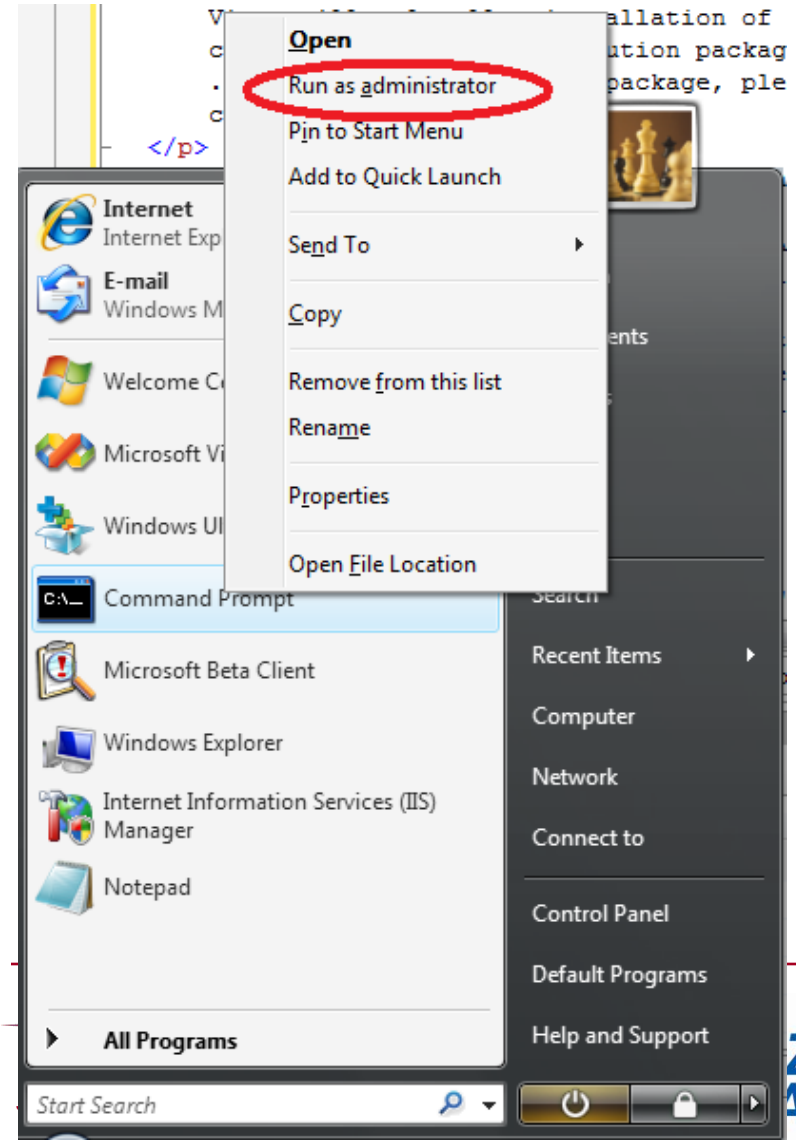
In Windows Vista

- When you log on as an Administrator you are running as a standard user (using standard user token)
- Have to elevate to Administrator Approved Mode (use administrator token) “Elevated”
- So you are prompted if you are about to use a restricted privilege. (Consent UI)

Standard User Token for Administrators

- Copy of the administrators token
  - Same SID
  - Membership in Domain Admins would remain
- Remove the following groups
  - BUILTIN\Administrators
  - BUILTIN\Backup Operators
  - BUILTIN\Power Users
  - BUILTIN\Network Configuration Operators
- Remove Denied Privileges
- Integrity Level goes from High to Medium

How to change or modify UAC



Run As Method

- Right Click
- “Run As” replaced with “Run as Administrator”
- Displays Consent UI
- Uses Administrator token

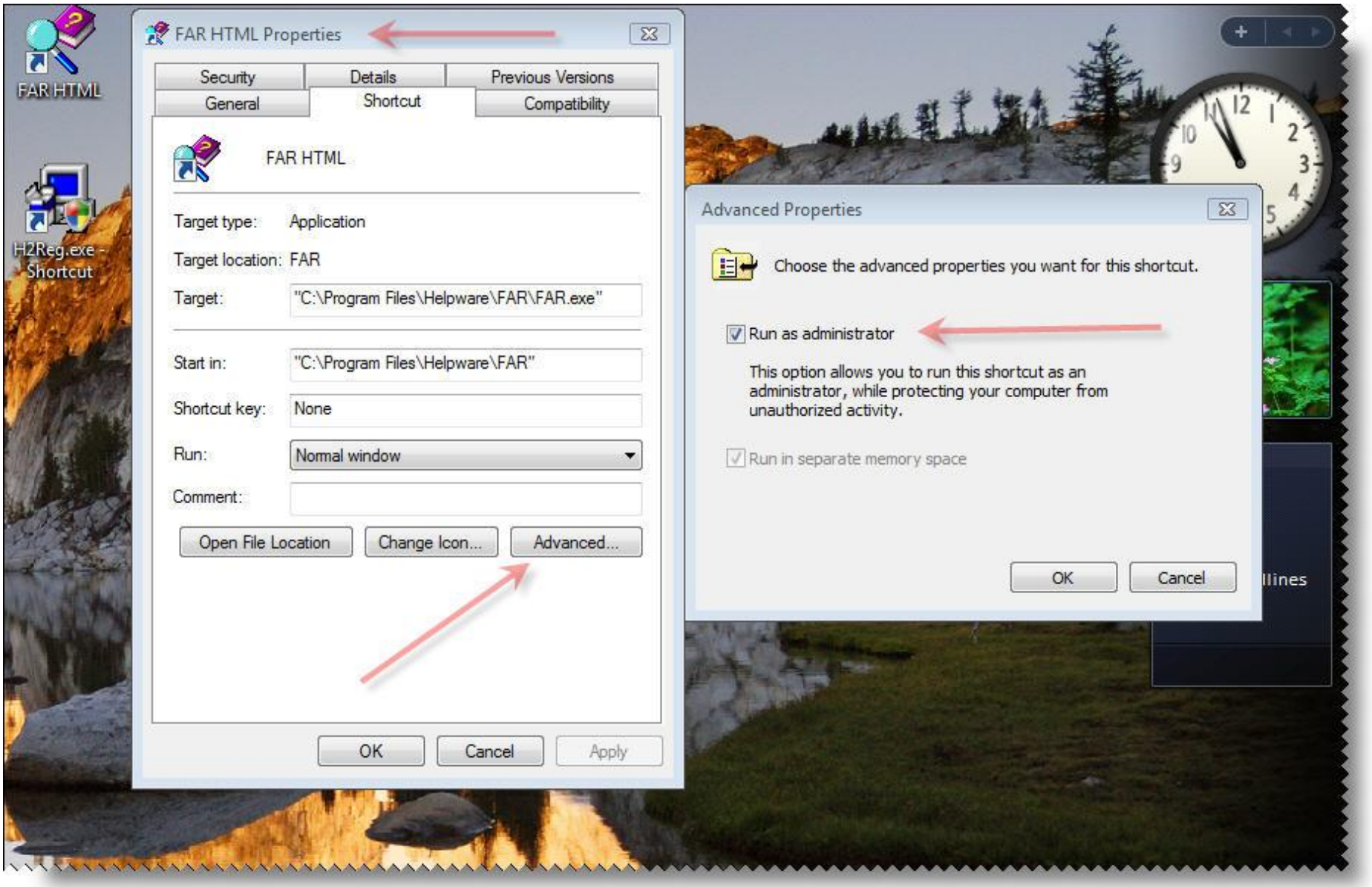
Run As Administrator

- If you are a member of a low power administrator groups
- Example “Backup Operators”
- You will get a prompt to run as your account or input other credentials

How to change or modify UAC

Shortcut method

- Create a shortcut
- Select “Advanced” on “Shortcut” tab
- Check the box next to “Run as Administrator”
- Uses Administrator token


FAR HTML
H2Reg.exe - Shortcut
FAR HTML Properties
Security
Details
Previous Versions
General
Shortcut
Compatibility
FAR HTML
Target type: Application
Target location: FAR
Target: "C:\Program Files\Helpware\FAR\FAR.exe"
Start in: "C:\Program Files\Helpware\FAR"
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply
Advanced Properties
Choose the advanced properties you want for this shortcut.
Run as administrator
This option allows you to run this shortcut as an administrator, while protecting your computer from unauthorized activity.
Run in separate memory space
OK
Cancel

How to change or modify UAC

For an EXE file

- Right click an executable and select “Properties”
- On the “Compatibility” tab
- Select “Run this program as an Administrator” under “Privilege Level”
- Or, select “Show settings for all Users” and select “Run this program as an Administrator” for all users.

Change the prompt

User Account Control in Security template

- Behavior of the elevation prompt for administrators or User Account Control
- Behavior of the elevation prompt for standard users
  - No prompt
  - Prompt for credentials
  - Prompt for consent

How to change or modify UAC

- Add or change the *manifest* in the executable file (Issue if the exe was digitally signed)
- Add an external *manifest* file
- Manifests are also used for Side by Side DLL

How to turn off UAC, if you must

How Vista Displays Icons for UAC

- Vista guesses that it'll need elevation, then Vista adds a shield icon automatically
- Seems to only add to EXE

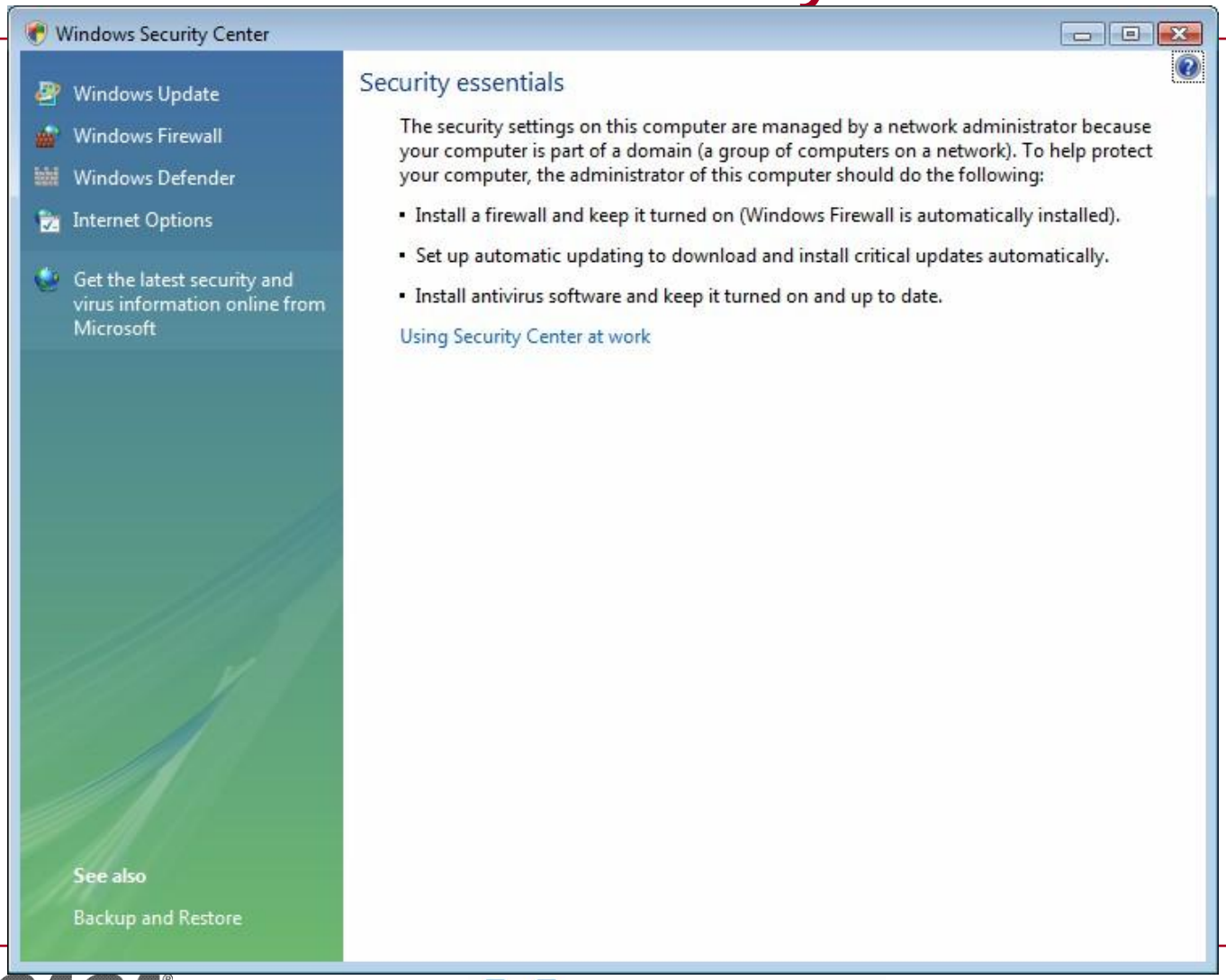
GPO for UAC

- You can configure the UAC settings in the following location in the Group Policy Object Editor:
- **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**
- You can configure the UAC Credentials user interface (UI) in the following location in the Group Policy Object Editor:
- **Computer Configuration\Administrative Templates\Windows Components\Credential User Interface**
- You can configure the ActiveX Installer Service in the following location in the Group Policy Object Editor:
- **Computer Configuration\Administrative Templates\Windows Components\ActiveX Installer Service**

Windows Vista Security

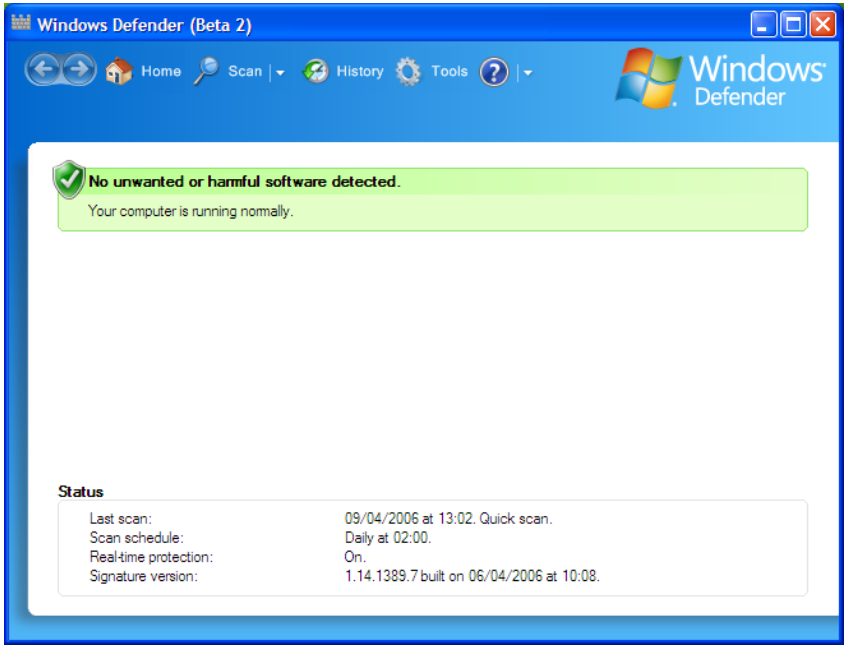
WINDOWS DEFENDER

Located in New Security Center



Integrated Windows Defender

- Integrated detection, cleaning, and real-time blocking of malware:
  - Malware, rootkits, and spyware
  - Targeted at consumers – enterprise manageability will be available as a separate product
- Integrated Microsoft Malicious Software Removal Tool (MSRT) will remove worst worms, bots, and trojans during an upgrade and on a monthly basis



Defender: GPO

- You can review and configure the available Windows Defender settings in the following location in the Group Policy Object Editor:
- **Computer Configuration\Administrative Templates\Windows Components\Windows Defender**

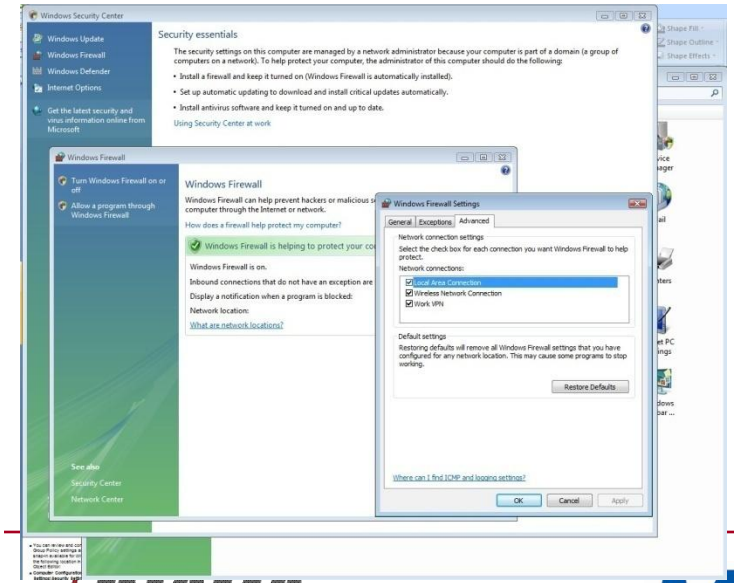
Windows Vista Security

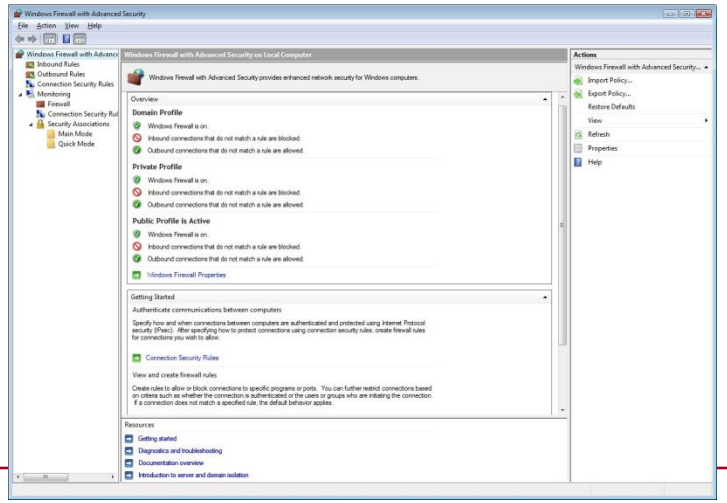
WINDOWS FIREWALL

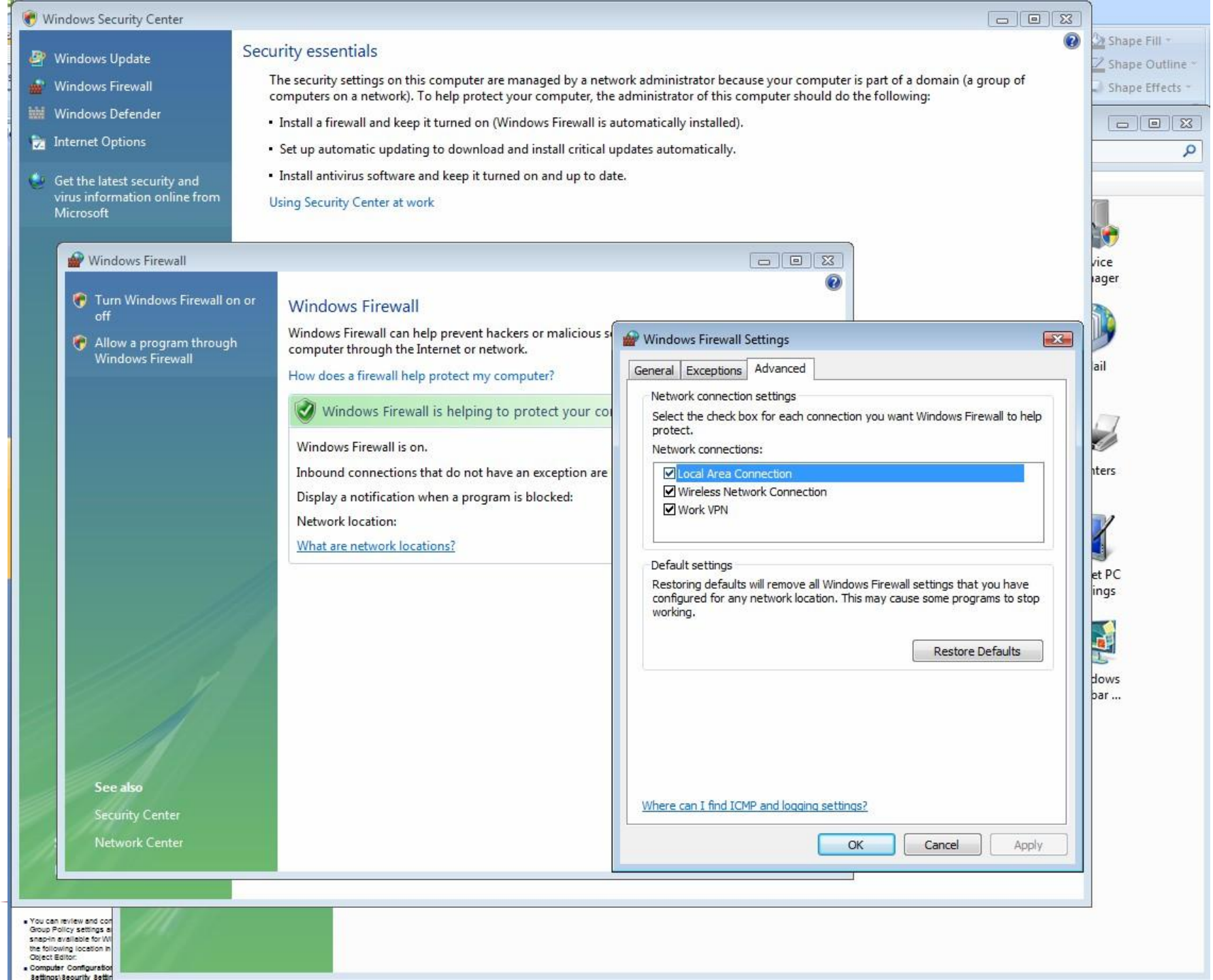
Two locations for Windows Firewall

- Security Center
- Has basic options

- Administrative tools
- Under control panel
- Advanced controls

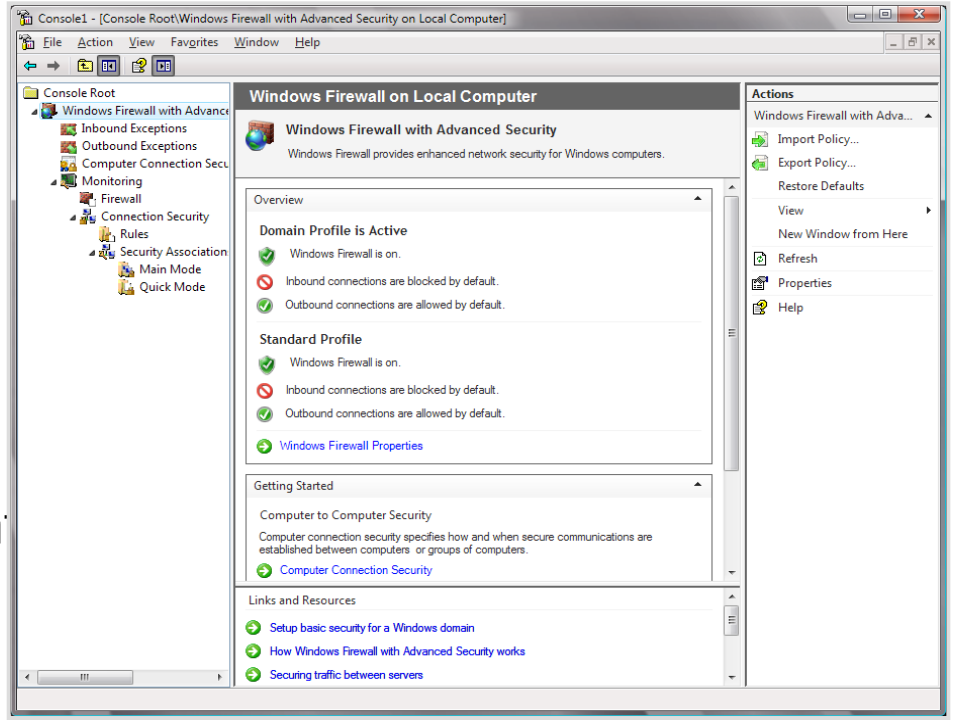





Windows Security Center
Windows Update
Windows Firewall
Windows Defender
Internet Options
Get the latest security and virus information online from Microsoft
Security essentials
The security settings on this computer are managed by a network administrator because your computer is part of a domain (a group of computers on a network). To help protect your computer, the administrator of this computer should do the following:
Install a firewall and keep it turned on (Windows Firewall is automatically installed).
Set up automatic updating to download and install critical updates automatically.
Install antivirus software and keep it turned on and up to date.
Using Security Center at work
Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall
Windows Firewall
Windows Firewall can help prevent hackers or malicious s
computer through the Internet or network.
How does a firewall help protect my computer?
Windows Firewall is helping to protect your co
Windows Firewall is on.
Inbound connections that do not have an exception are
Display a notification when a program is blocked:
Network location:
What are network locations?
See also
Security Center
Network Center
Windows Firewall Settings
General
Exceptions
Advanced
Network connection settings
Select the check box for each connection you want Windows Firewall to help protect.
Network connections:
Local Area Connection
Wireless Network Connection
Work VPN
Default settings
Restoring defaults will remove all Windows Firewall settings that you have configured for any network location. This may cause some programs to stop working.
Restore Defaults
Where can I find ICMP and logging settings?
OK
Cancel
Apply
Shape Fill
Shape Outline
Shape Effects

Windows Vista Firewall

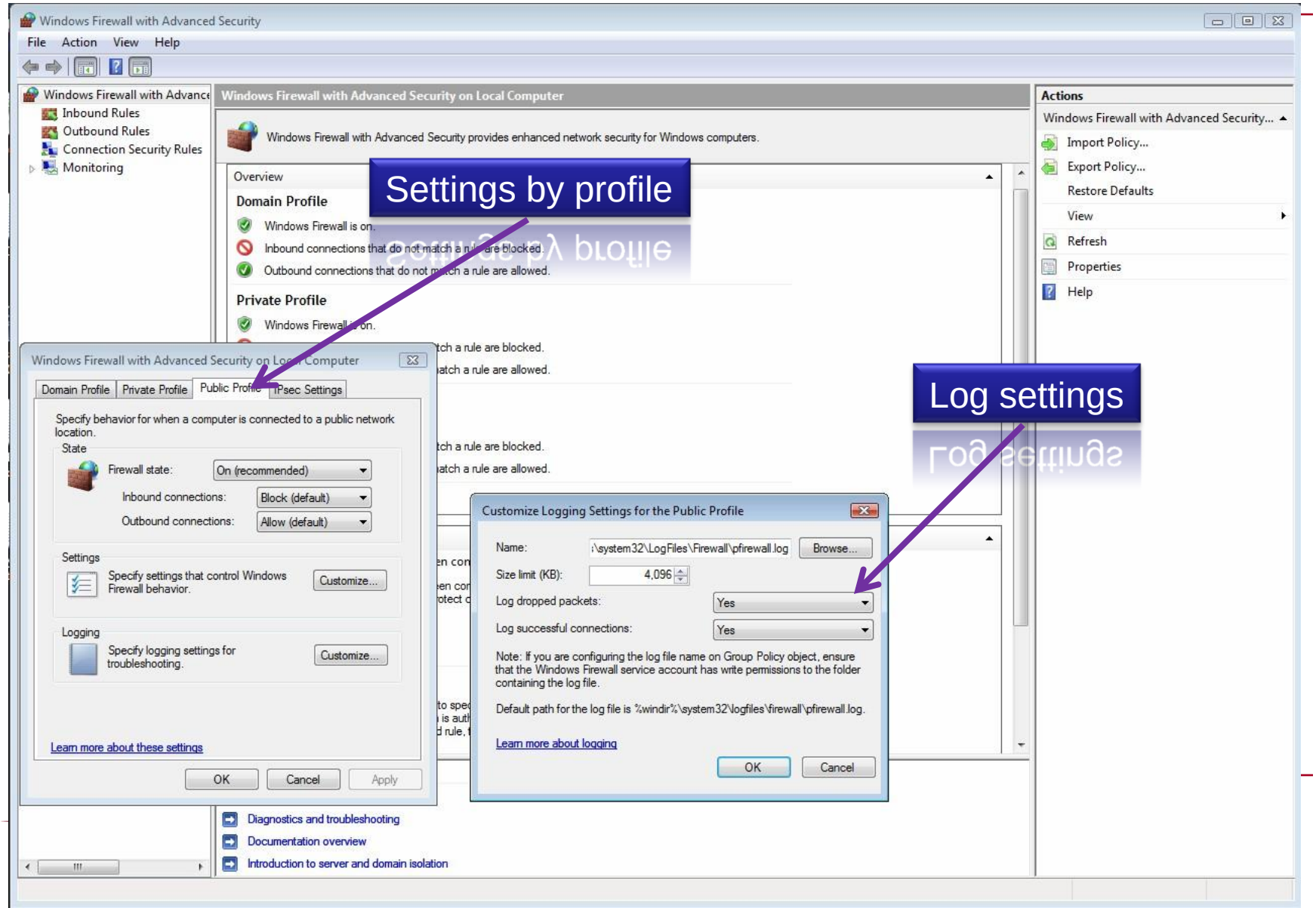
- Both inbound and *outbound*
- Authentication and authorization aware
- Outbound application-aware filtering is now possible
  - Includes IPSec managemen
  - Of course, policy-based administration
  - Great for Peer-to-Peer control



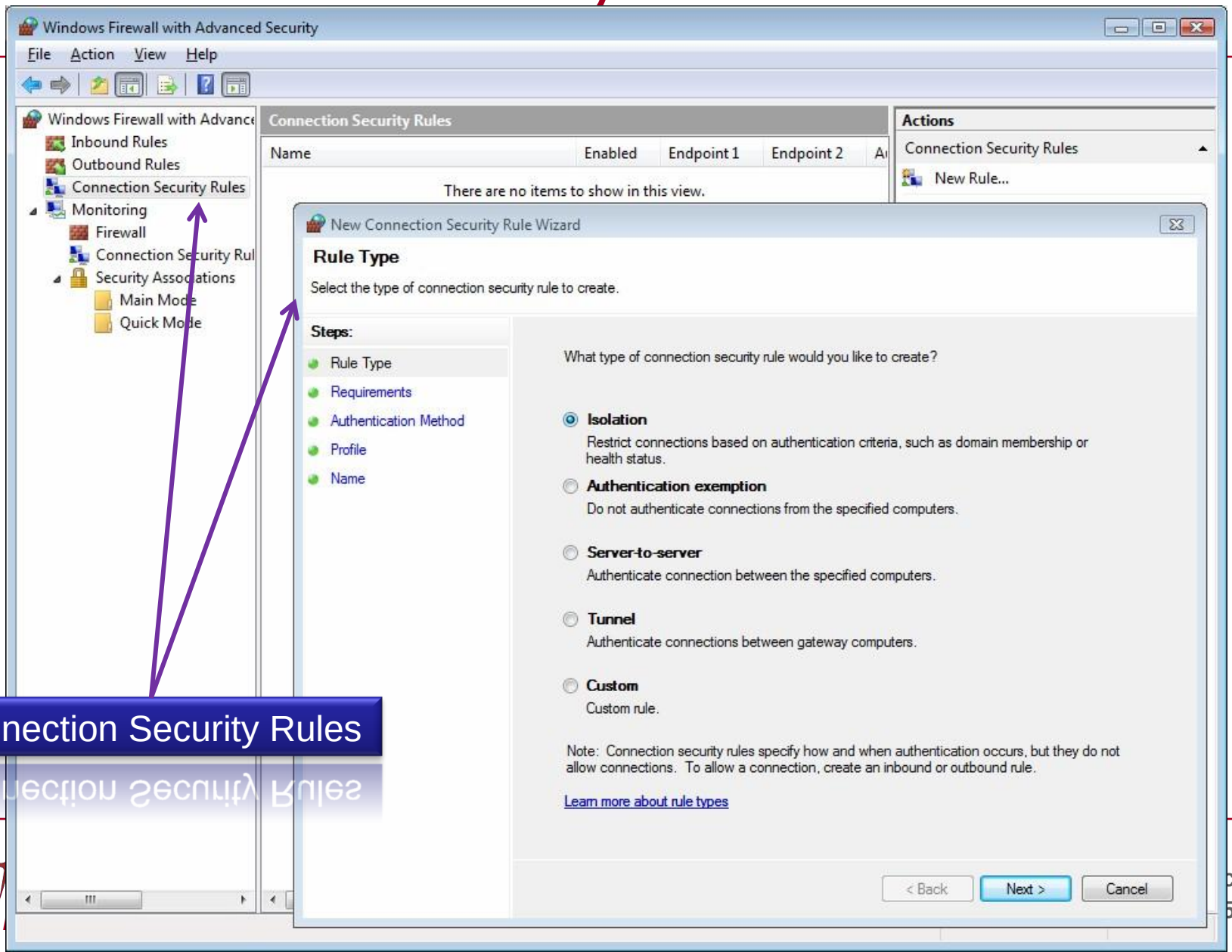
Firewall: Advanced Security

- Windows Firewall with Advanced Security supports the following environment profiles:
  - **Domain Profile**. This profile applies when a computer is connected to a network and authenticates to a domain controller in the domain to which the computer belongs.
  - **Public Profile**. This profile is the default network location type when the computer is not connected to a domain. Public profile settings should be the most restrictive because the computer is connected to a public network where security cannot be as tightly controlled as within an IT environment.
  - **Private Profile**. This profile only applies if a user with local administrator privileges assigns it to a network that was previously set to Public. Microsoft recommends only doing this for a trusted network.

Firewall Logging

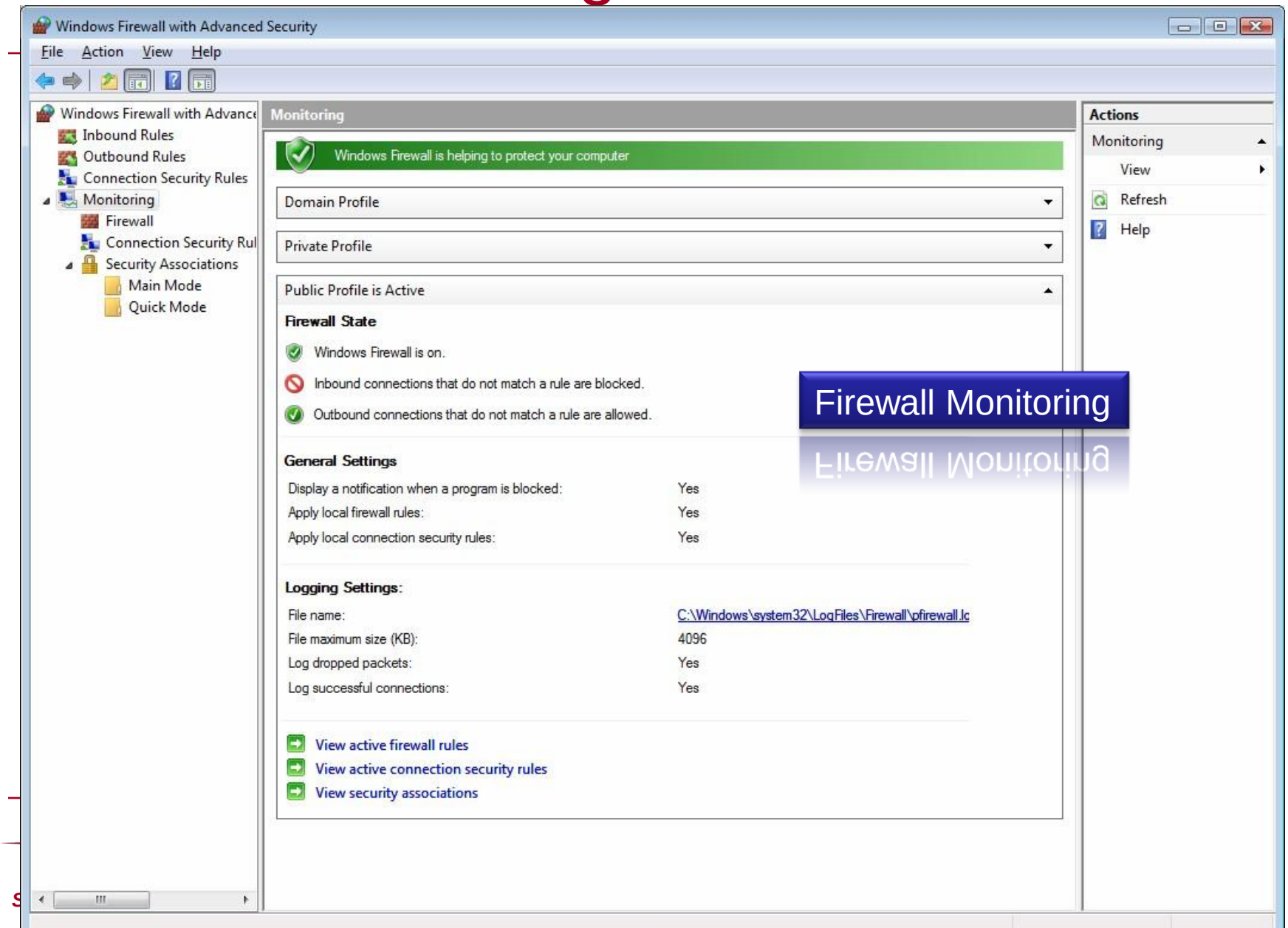


Connection Security Rules

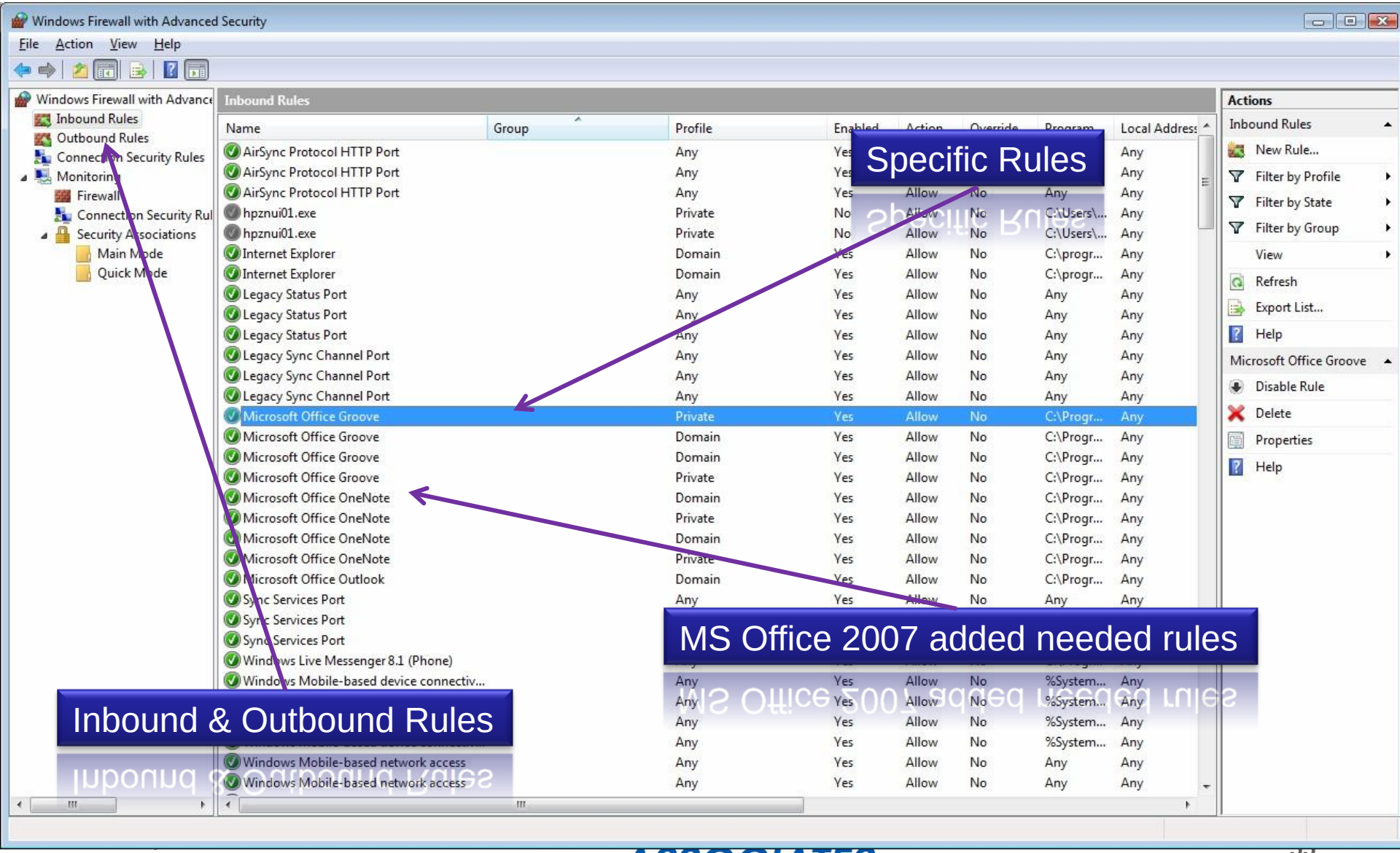


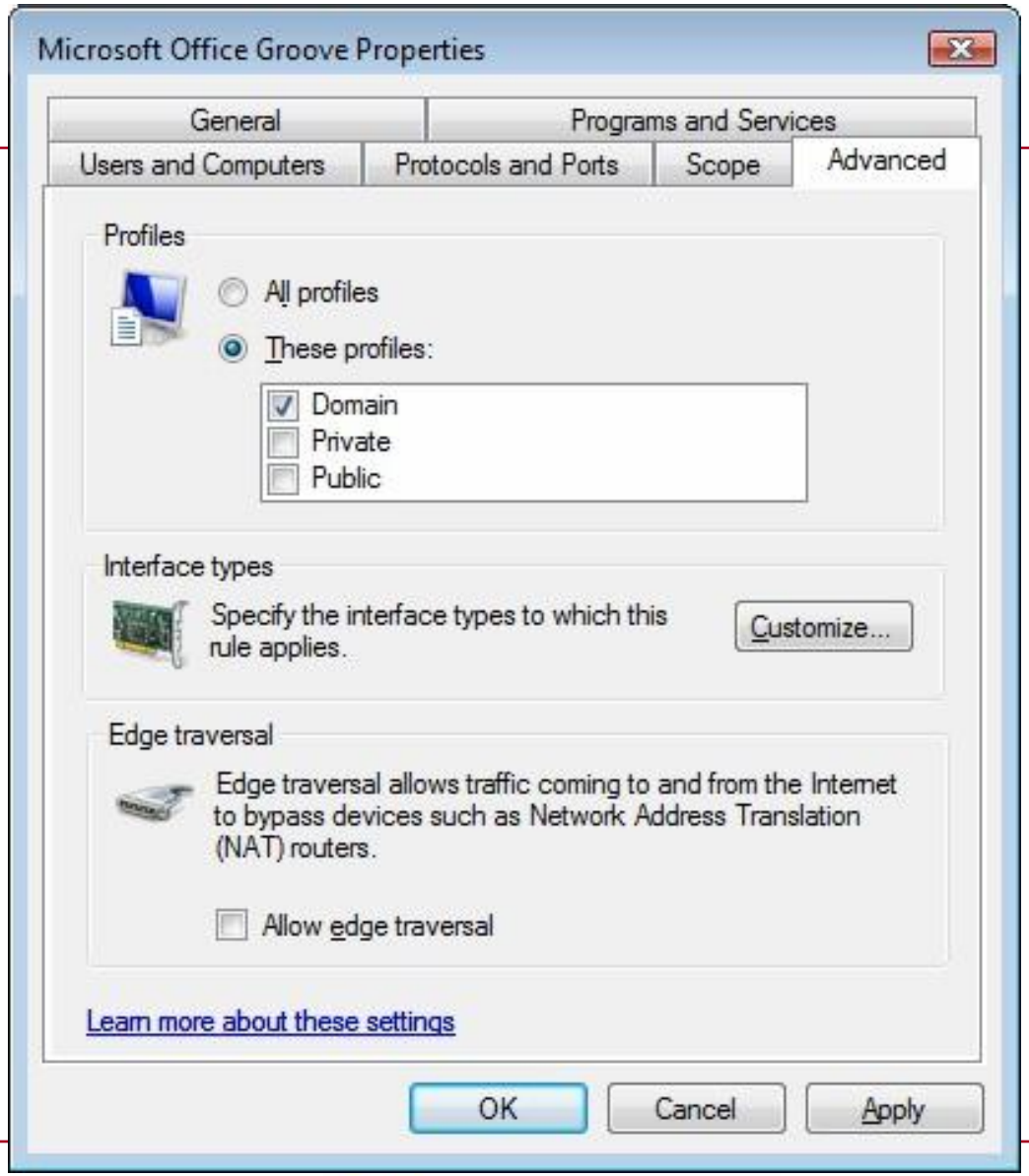
Connection Security Rules

Firewall Monitoring



Inbound & Outbound Rules




Microsoft Office Groove Properties
General
Programs and Services
Users and Computers
Protocols and Ports
Scope
Advanced
Profiles
All profiles
These profiles:
Domain
Private
Public
Interface types
Specify the interface types to which this rule applies.
Customize...
Edge traversal
Edge traversal allows traffic coming to and from the Internet to bypass devices such as Network Address Translation (NAT) routers.
Allow edge traversal
Learn more about these settings
OK
Cancel
Apply

Firewall: GPO

- You can review and configure the new Group Policy settings and management snap-in available for Windows Firewall in the following location in the Group Policy Object Editor:
- **Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security**

Windows Vista Security

INTERNET EXPLORER 7

Internet Explorer 7: Security Features

- Internet Explorer Protected Mode
- ActiveX Opt-in
- Cross-domain scripting attack protection
- Security Status Bar
- Phishing Filter
- Additional security features

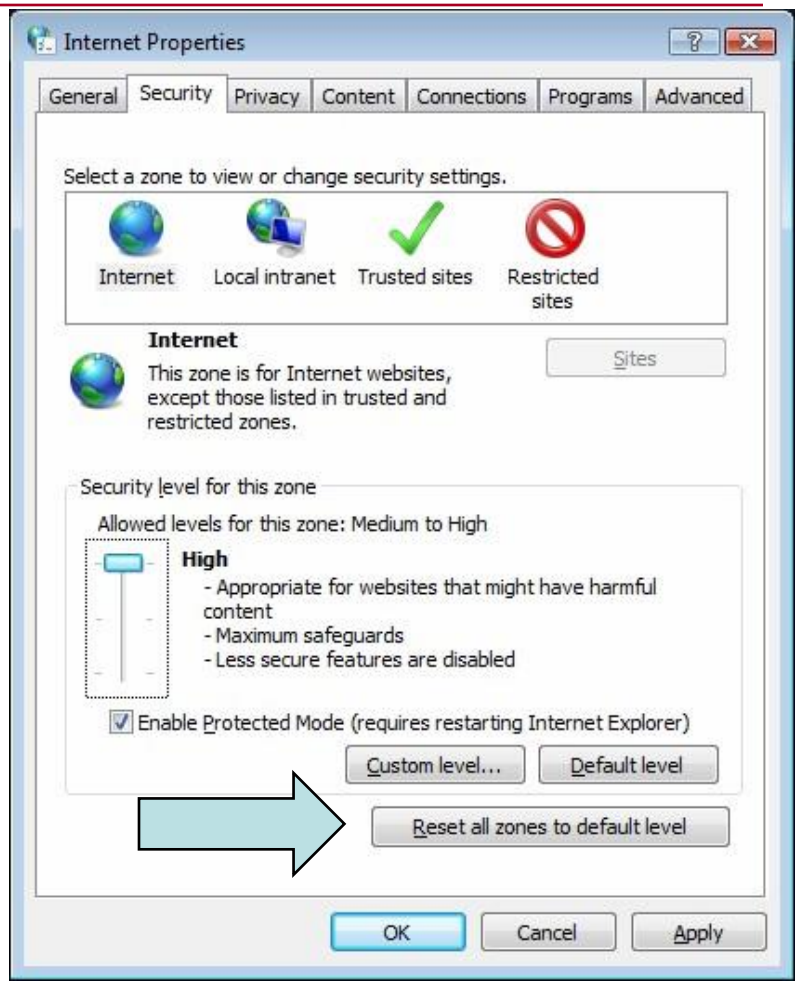
Information Security Magazine (Jan 2006) Rated #1 browser for security

User Privacy

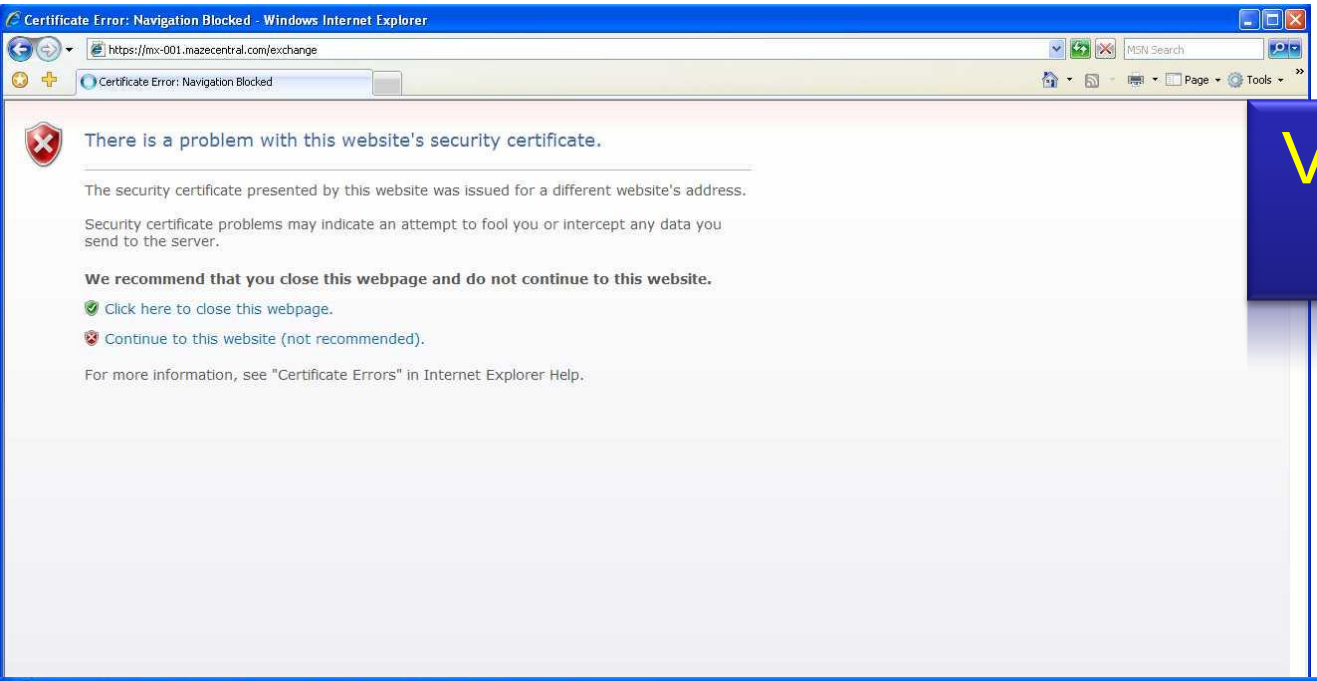
- Delete browsing history
- Single button deletion
- Delete only selected groups of information

Fix My Settings

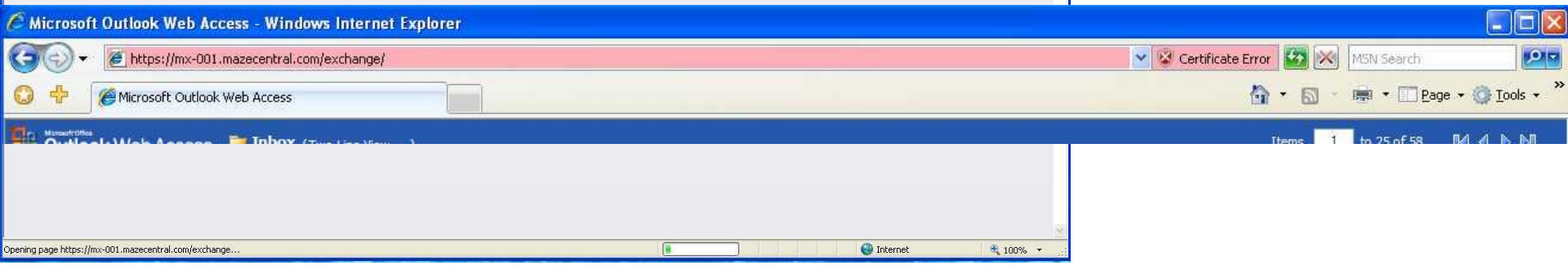
- Helps to protect you from browsing with unsafe settings
- Warning in status bar if settings are changed
- One click to fix and reset to the "Medium-High" default



Security Status Bar



Visual prompts for security

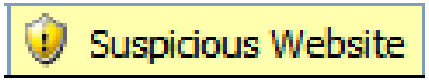


Phishing Filter in IE

Dynamic Protection Against Fraudulent Websites

- 3 checks to protect users from phishing scams:
  1. Compares web site with local list of known legitimate sites
  2. Scans the web site for characteristics common to phishing sites
  3. Double checks site with online Microsoft service of reported phishing sites updated several times every hour
- Two Levels of Warning and Protection in IE7 Security Status Bar

Level 1: Warn
Suspicious Website
Signaled

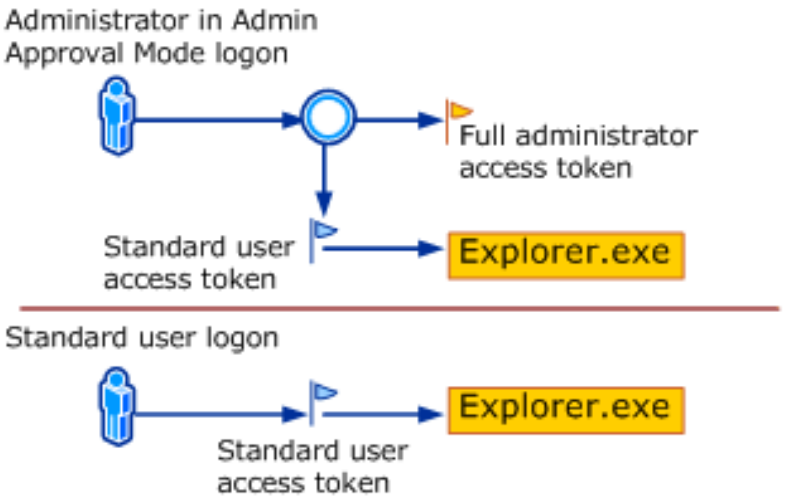


Level 2: Block
Confirmed Phishing Site
Signaled and Blocked

Internet Explorer 7

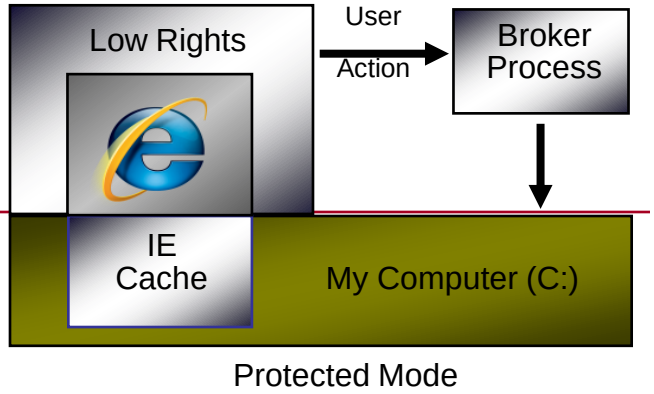
- In addition to building on UAC, IE includes:
  - Protected Mode that only allows IE to browse with no other rights, even if the user has them, such as to install software
    - "Read-only" mode, except for Temporary Internet Files when browser is in the Internet Zone of security

Internet Explorer 7 Protected Mode



- During the logon process IE is loaded
- An application that is running cannot change it token
- Starting a new window of IE does not give you a new token

Broker Process



- Allow elevated privilege in a secure way
- Mediates between IE and OS
- Requires User input
- Eliminated unknown or unwanted installations
- Protected Mode API uses UIPI & MIC

CDB

- Cross-Domain barriers
- Stops scripts from working across domains or websites
- Limit malware from malicious sites that might exploit flaws in other sites
- Used for drive-by installations and pop-up ads

IEAK 7

- Internet Explorer Administration Kit 7
  - Establish version control across your organization
  - Central distribution
  - Configure automatic connection profiles for users
  - Customize features, security, communications settings and other elements

Internet Explorer 7: GPO

- Add-on Management
- Binary Behavior Security Restriction
- Consistent MIME Handling
- Information Bar
- Local Machine Zone Lockdown Security
- MIME Sniffing Safety Feature
- MK Protocol Security Restriction
- Network Protocol Lockdown
- Object Caching Protection
- Protection From Zone Elevation
- Restrict ActiveX Install
- Restrict File Download
- Scripted Windows Security Restrictions

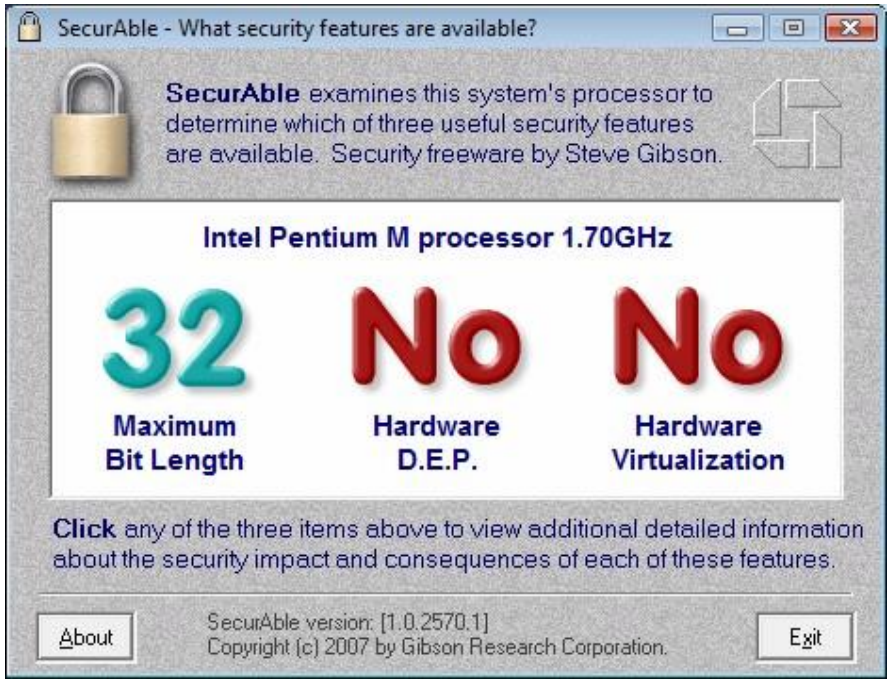
Windows Vista Security

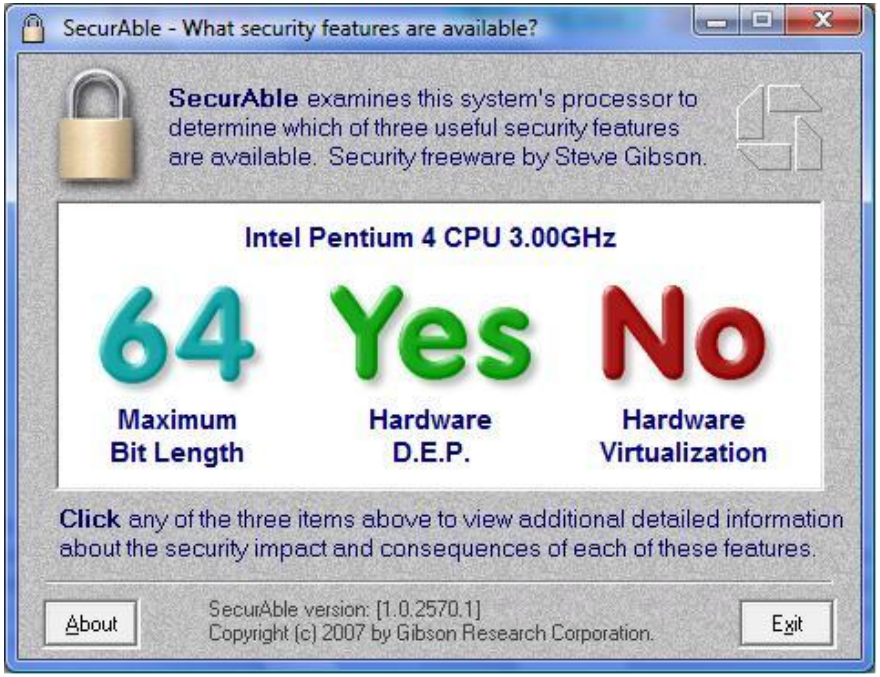
DATA EXECUTION PREVENTION (DEP)

Data Execution Prevention (DEP)

- Prevent malicious software rather than error out and potentially crashing the system
- Hardware-enforced DEP
  - Protects memory locations
  - The no-execute page-protection (NX) processor feature as defined by AMD.
  - The Execute Disable Bit (XD) feature as defined by Intel.
- Software-enforced DEP (Not the same thing)
  - Protects system binaries and exception-handling
  - Software built with SafeSEH

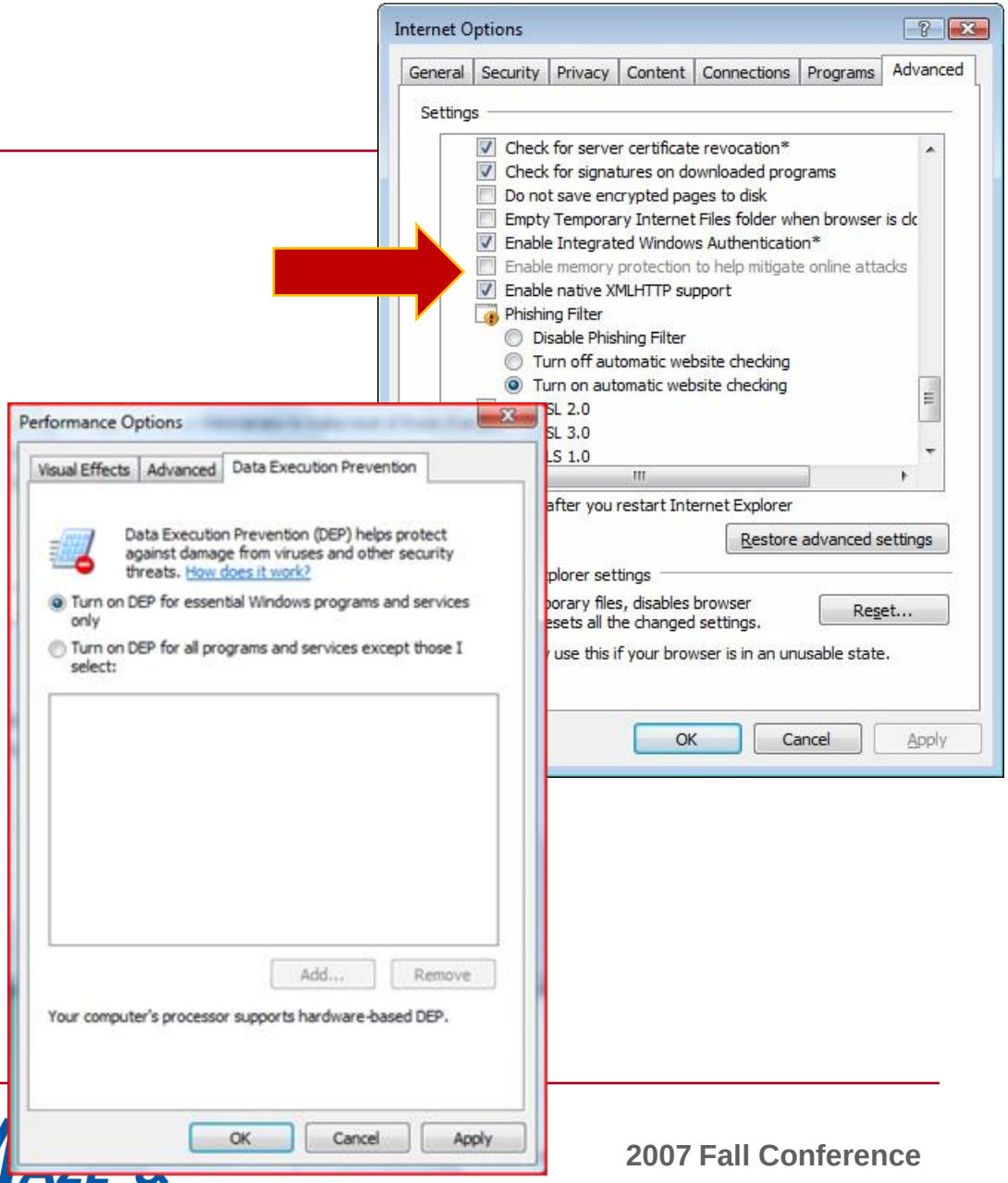
Does your Hardware support DEP?





Vista DEP

- DEP Modes
  - Kernel Only
  - User Mode
  - Internet Explorer



Windows Vista Security

INTEGRITY PROTECTION

Windows Integrity Controls

- One goal was CC (Common Criteria) compliance (TCSEC Level B)
- MIC (Mandatory Integrity Control) later named WIC (Windows Integrity Control)
- Has been available for decades but only in military computers
- That means there may be files that not even the administrator can delete

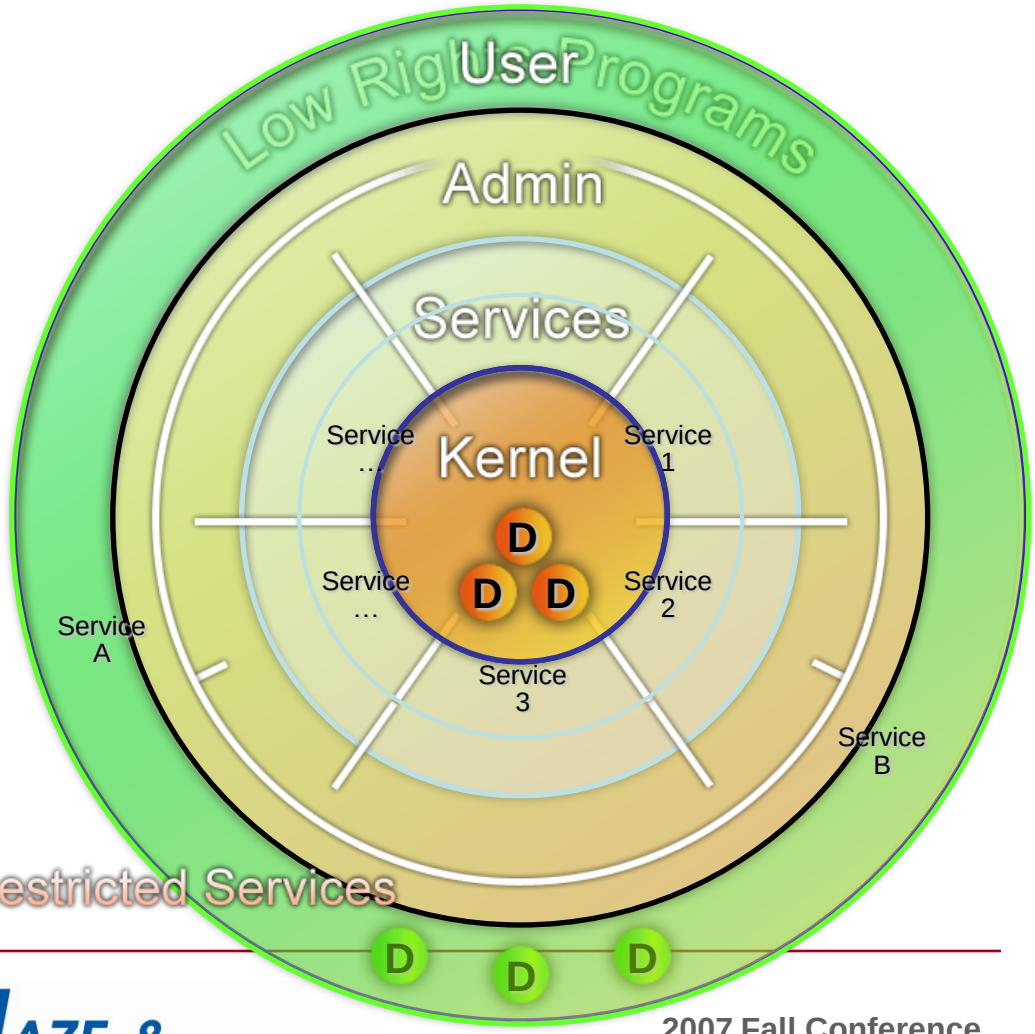
MIC

- *Mandatory Integrity Control* (MIC), a model in which data can be configured to prevent lower-integrity applications from accessing it.
- The primary integrity levels are Low, Medium, High, and System.
- Processes are assigned an integrity level in their access token.
- Securable objects such as files and registry keys have a new mandatory access control entry (ACE) in the System Access Control List (ACL).

Integrity Levels

Defense-in-Depth: Factoring and Profiling of Windows Kernel

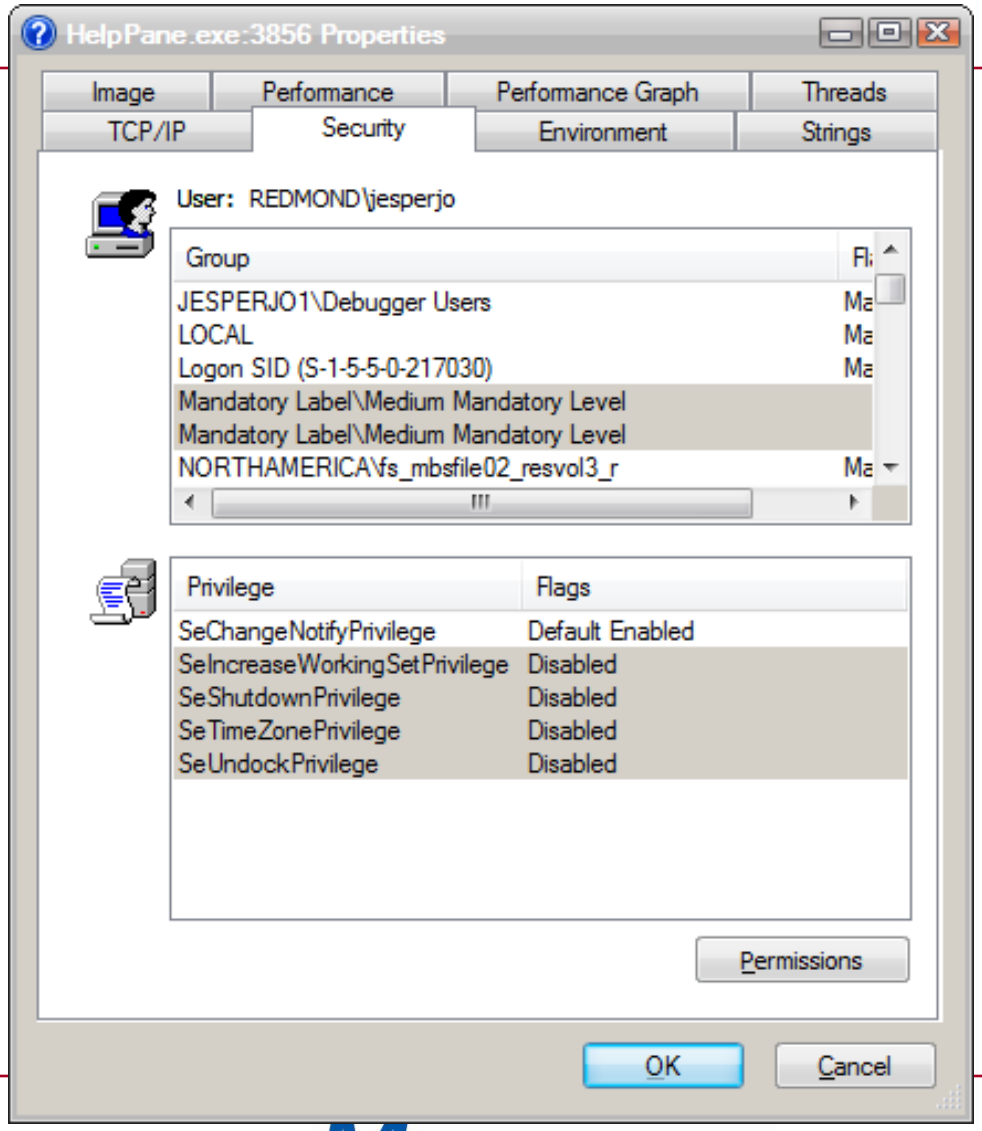
- Reduce size of high risk layers
- Segment the services
- Increase number of layers



D Kernel Drivers

D User-mode Drivers

Integrity Levels in Token



Windows Resource Protection

- This new feature in Windows Vista helps safeguard system files and protected registry locations to help improve the overall security and stability of the operating system.
- Most applications that previously accessed or modified these locations are automatically redirected to temporary locations, which they can then use to continue to operate without issues.

Code Integrity

- All DLLs and other OS executables have been digitally signed
- Signatures verified when components load into memory (64 bit)

Windows Resource Protection (WRP)

- Protects protected system files and registry keys
- Creates a temporary work area & redirects
- Temporary work area is not persistent from one session to another
- Protects %systemroot% files and folders
- Only accessed by System Service
- Administrators can read system files and folders but cannot write to them

Fundamental Change to Windows Operation

- Registry and file virtualization to provide compatibility
  - Per-machine registry writes are redirected to per-user locations if the user does not have administrative privileges
  - Effectively: standard accounts can run “admin-required” legacy applications safely!
  - You can redirect the virtualization store

UIPI

- *User Interface Privilege Isolation* (UIPI) blocks lower-integrity from accessing higher-integrity processes. Isolate applications
- For example, a lower-integrity process cannot send window messages or hook or attach to higher priority processes
- Internet browsers are a prime target “jump from application to application”
- This helps protect against "shatter attacks."
  - A shatter attack is when one process tries to elevate privileges by injecting code into another process using windows messages.

Windows Vista Security

Section 2: Data Protection

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Data Protection

- BitLocker™ Drive Encryption
- Encrypting File System (EFS)
- Rights Management Services (RMS)
- Device control
- ACL Improvements
- Volume Shadow Copy

Windows Vista Security

BITLOCKER™ DRIVE ENCRYPTION

BitLocker ™

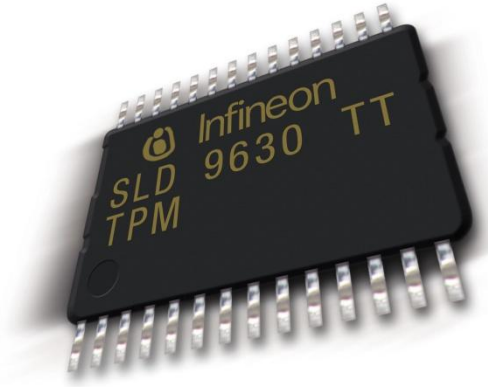
- Over 600,000 laptops are stolen a year
- BitLocker ensures that data stored on a computer running Windows Vista remains encrypted even if the computer is tampered with when the operating system is not running
- BitLocker is designed to offer a seamless user experience

BitLocker ™

- Preventing off-line modifications
- Entire drive encryption
- TPM (Trusted Platform Module) to store key
- Can use additional protection factors such as a USB dongle, PIN or password
- Data recovery strategy must be planned carefully!
- Single digit performance hit (overhead)

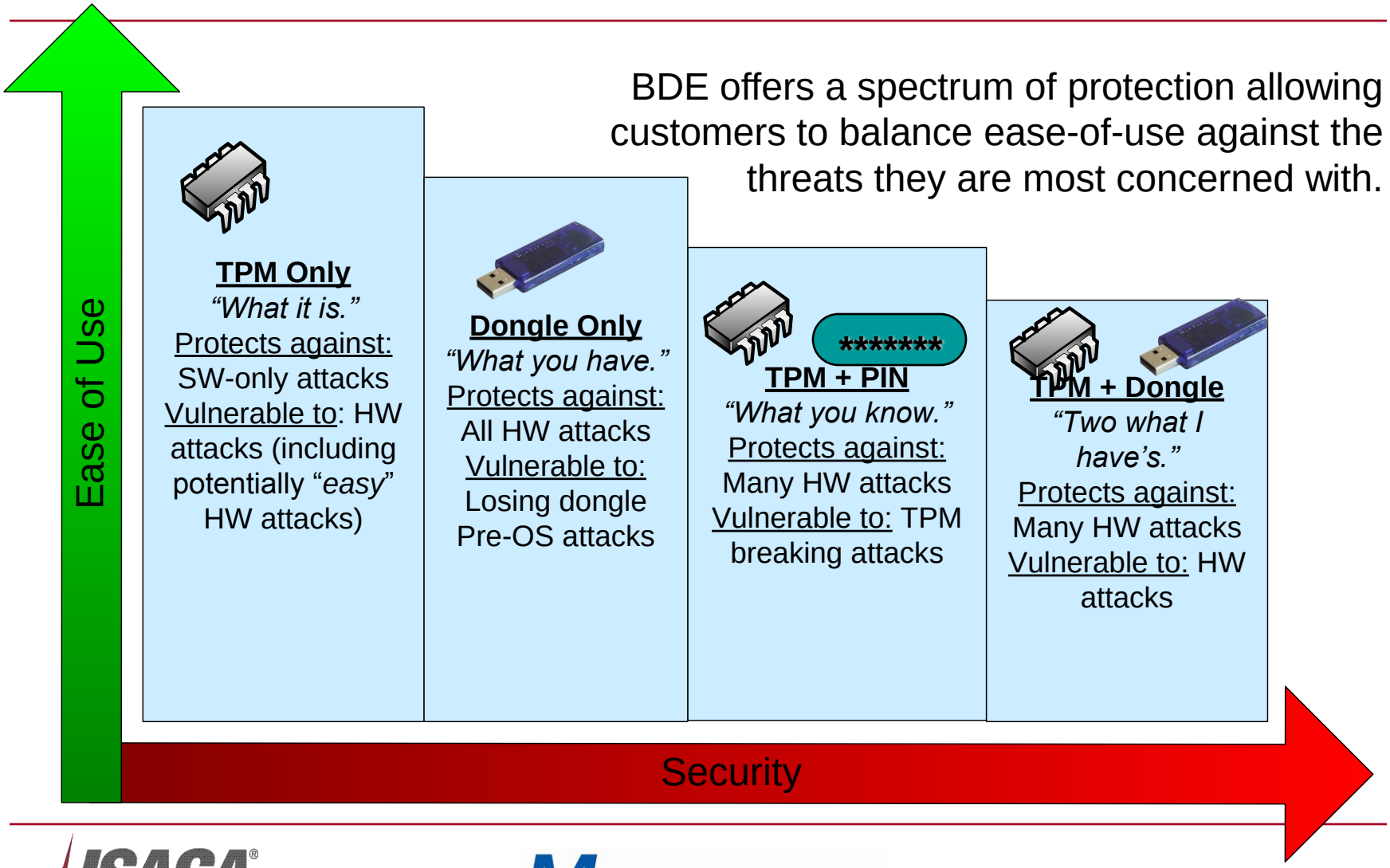
Trusted Platform Module
TPM Chip Version 1.2

- Hardware present in the computer, usually a chip on the motherboard
- Securely stores credentials, such as a private key of a machine certificate and is crypto-enabled
  - Effectively, the essence of a smart smartcard
- TPM can be used to request encryption and digital signing of code and files and for mutual authentication of devices
- See www.trustedcomputinggroup.org



Spectrum Of Protection

BDE offers a spectrum of protection allowing customers to balance ease-of-use against the threats they are most concerned with.



Deployment Options

- Dongle Only: If you don’t have TPM you can deploy BitLocker with the key on a USB device
- TPM only: You can use BitLocker with TPM
- TPM & PIN: you can use a PIN number in addition for added security
- TPM & Dongle: For the greatest protection

Hardware and Software requirements

- A computer that meets the minimum requirements for Windows Vista.
- A TPM microchip, version 1.2, turned on.
- A Trusted Computing Group (TCG)-compliant BIOS
- Two NTFS drive partitions, one for the system volume and one for the operating system volume. The system volume partition must be at least 1.5 gigabytes (GB) and set as the active partition
- A BIOS setting to start up first from the hard drive, not the USB or CD drives.

Partitioning a Hard Disk for BitLocker

- 1st partition, system volume, (label “S” for example) contains unencrypted boot information
- 2nd partition, operating system volume (label “C” for example) contains encrypted user data and operating system

BitLocker Disk Layout and Key Storage

Recovery Password

- During the setup process you can save the recovery password in the following ways.
  - Save the password on a USB drive.
  - Save the password in a folder.
  - Print the password.
- The password is so important that it is recommended that you make additional copies of the password stored in safe places to assure you access to your data

Tampering & Recovery

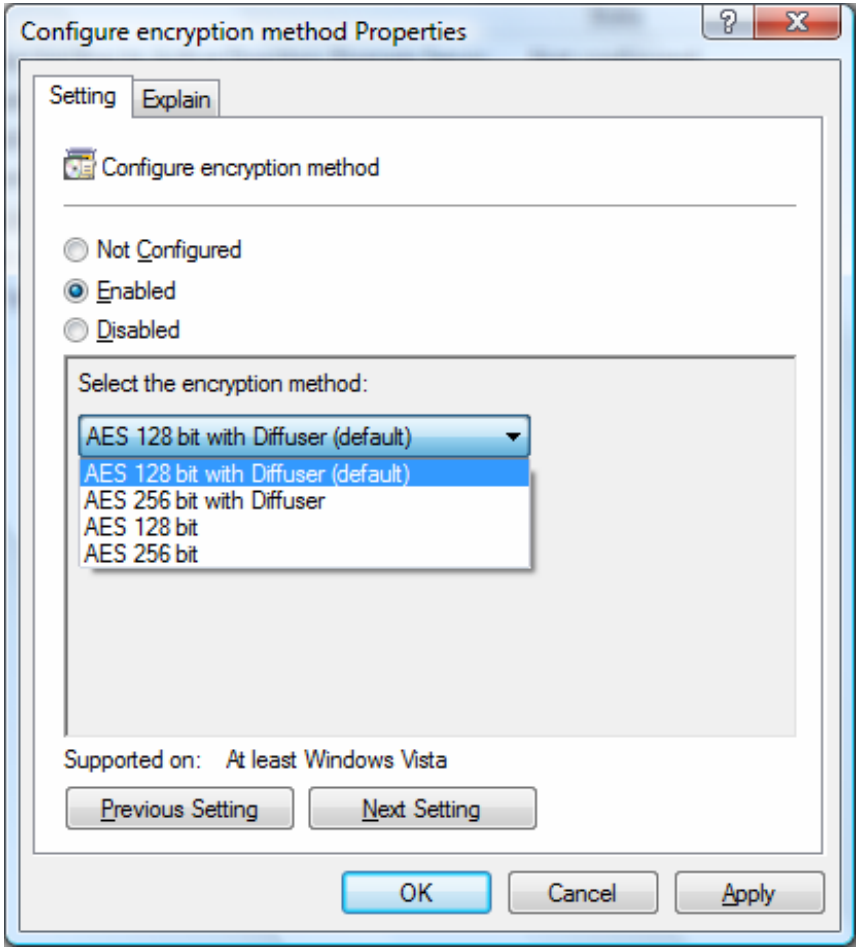
- You BitLocker will enter recovery mode, and you will need a recovery password to regain access to the data if,
  - The TPM is missing or changed
  - Or if the startup information has changed
- Recovery happens so early in the startup process, the accessibility features of Windows are not available.
- BitLocker Drive Encryption Recovery Console

BitLocker & TPM: GPO

- You can configure these settings in the following location within the Group Policy Object Editor:
  - **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption**
- You can configure these settings in the following location in the Group Policy Object Editor:
  - **Computer Configuration\Administrative Templates\System\Trusted Platform Module Services**

Performance & Security

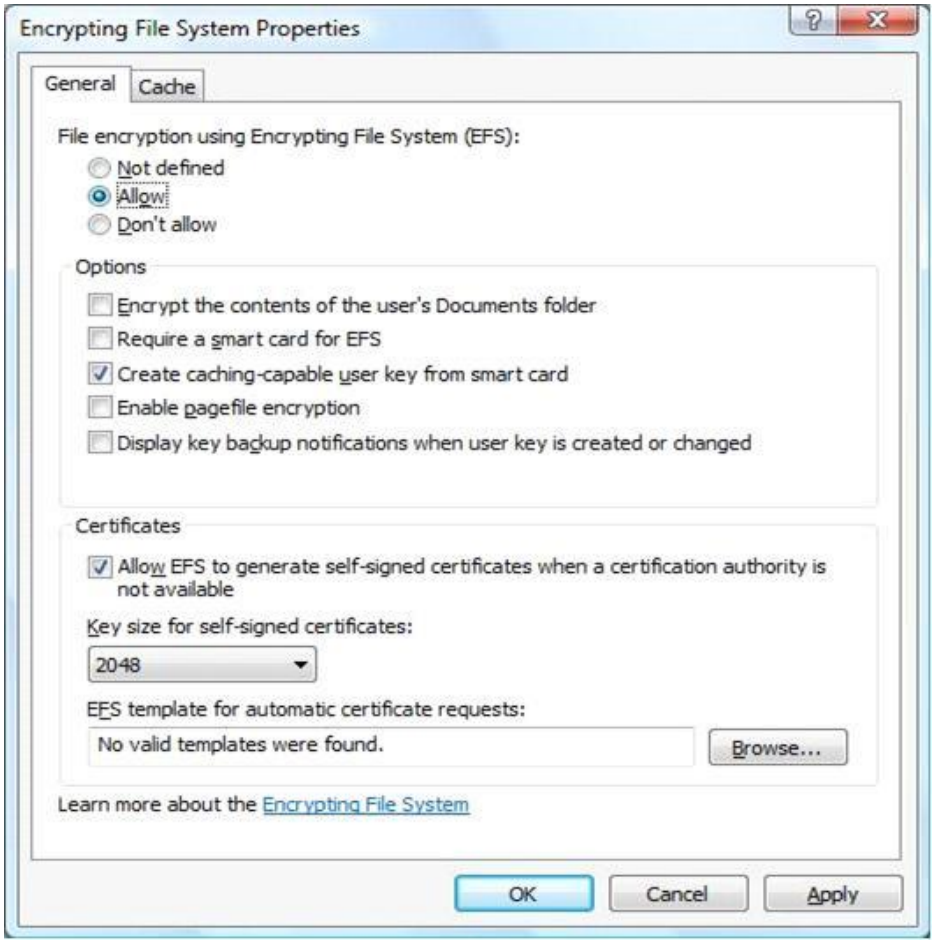
- 4 levels of AES encryption
- 128 & 256 bit
- the diffuser is a new unproven algorithm
- diffuser runs in about 10 clock cycles/byte
- Combination with AES-CBC for performance & security



Windows Vista Security

EFS

Encrypting File System



New Features for EFS

- User keys on smart cards
- Recovery keys can be stored on smart cards
- Can encrypt Windows paging file
- Encrypt offline files cache
- Support wider range of user certificates
- More GPO support (e.g. stipulate minimum key length)

Windows Vista Security

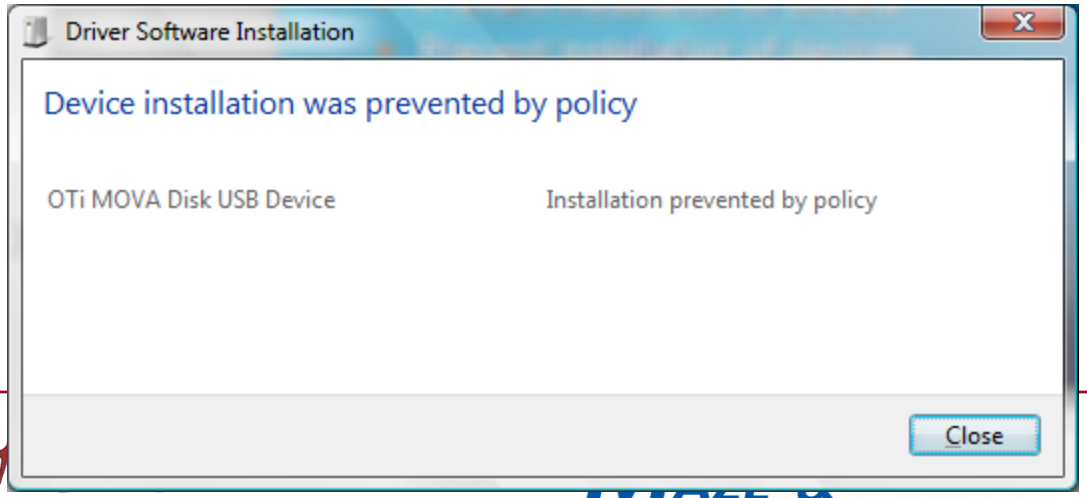
DEVICE INSTALLATION RESTRICTION

Control Over Device Installation

- Control over removable device installation via a policy
  - Mainly to disable USB-device installation
  - You can control them by device class or driver
- Approved drivers can be pre-populated into trusted Driver Store
- Driver Store Policies (group policies) govern driver packages that are not in the Driver Store:
  - Non-corporate standard drivers
  - Unsigned drivers

Device Restrictions

- Device installation restrictions
- Determine what devices can be installed on computers.
  - Prevent installation of drivers
  - Prevent installation of devices



Device GPO

- Using Group Policy to Control AutoPlay and AutoRun
  - Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies
- Using Group Policy to Control Device Usage
  - Computer Configuration\Administrative Templates\System\Removable Storage Access
- Using Group Policy to Control Device Installation
  - Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions

Windows Vista Security

RIGHTS MANAGEMENT

Rights Management Service (RMS)

- Rights Management Services (RMS) is designed to provide security and usage policy enforcement for sensitive e-mail, documents, Web content, and other types of information. RMS provides information security by encrypting information persistently so that as a file or e-mail message is transmitted through the enterprise or the Internet, only those who are authenticated and explicitly authorized to access it can do so.

RMS Components

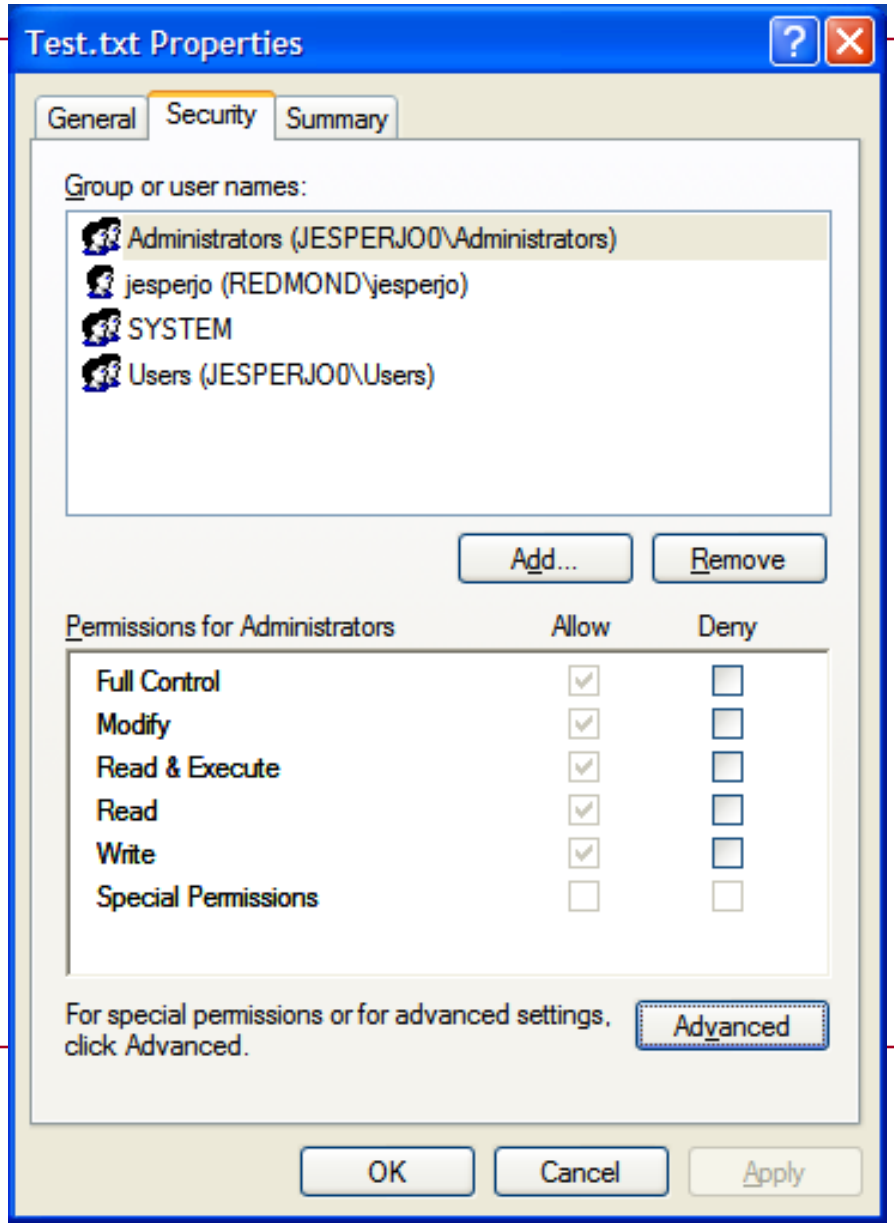
- **RMS server**. Windows Vista requires Windows Rights Management Services for Windows Server 2003 or later.
- **RMS client**. This is included with Windows Vista.
- **RMS platform or application**. This is a platform or application that is designed to encrypt and control usage of the information it manages.

RMS is primarily a server-based solution, Windows Vista supports RMS

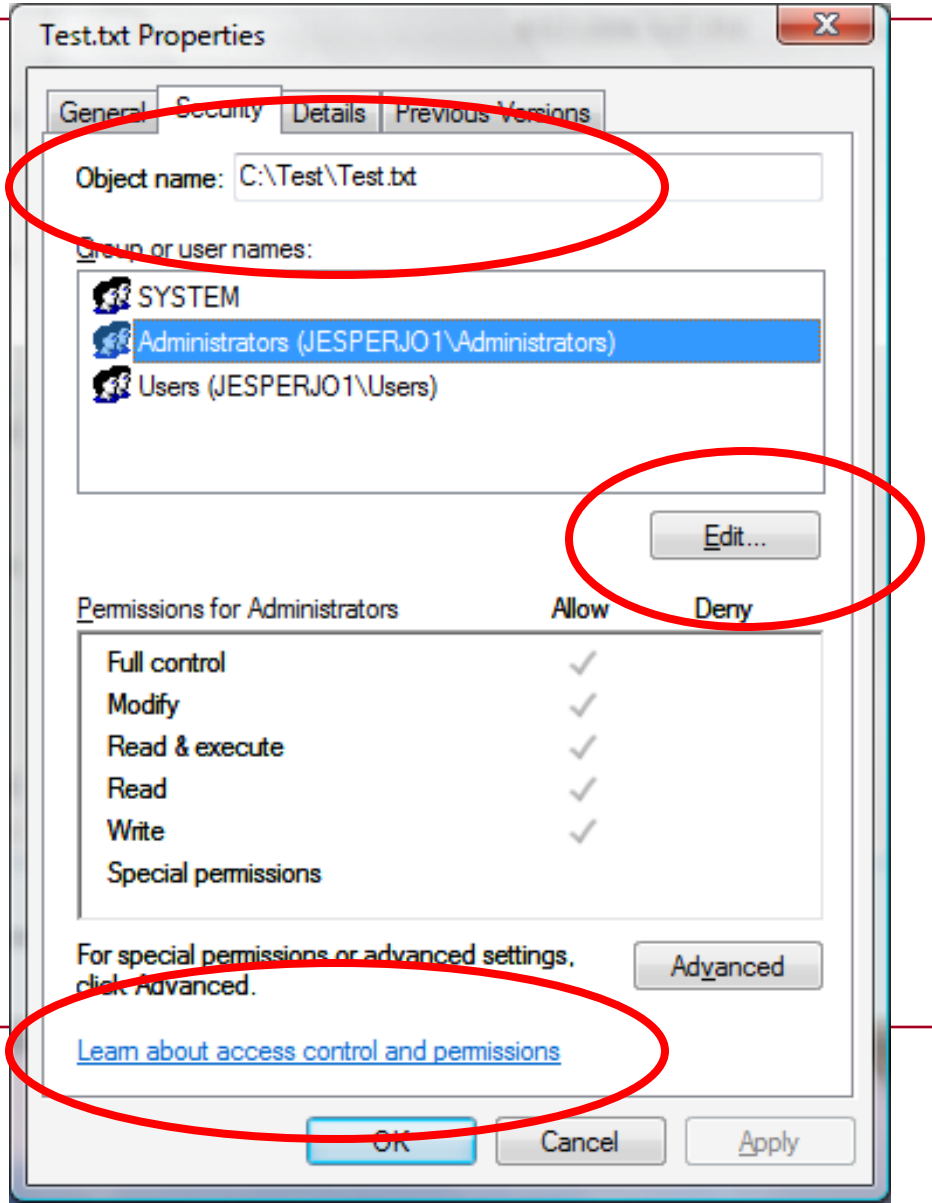
Windows Vista Security

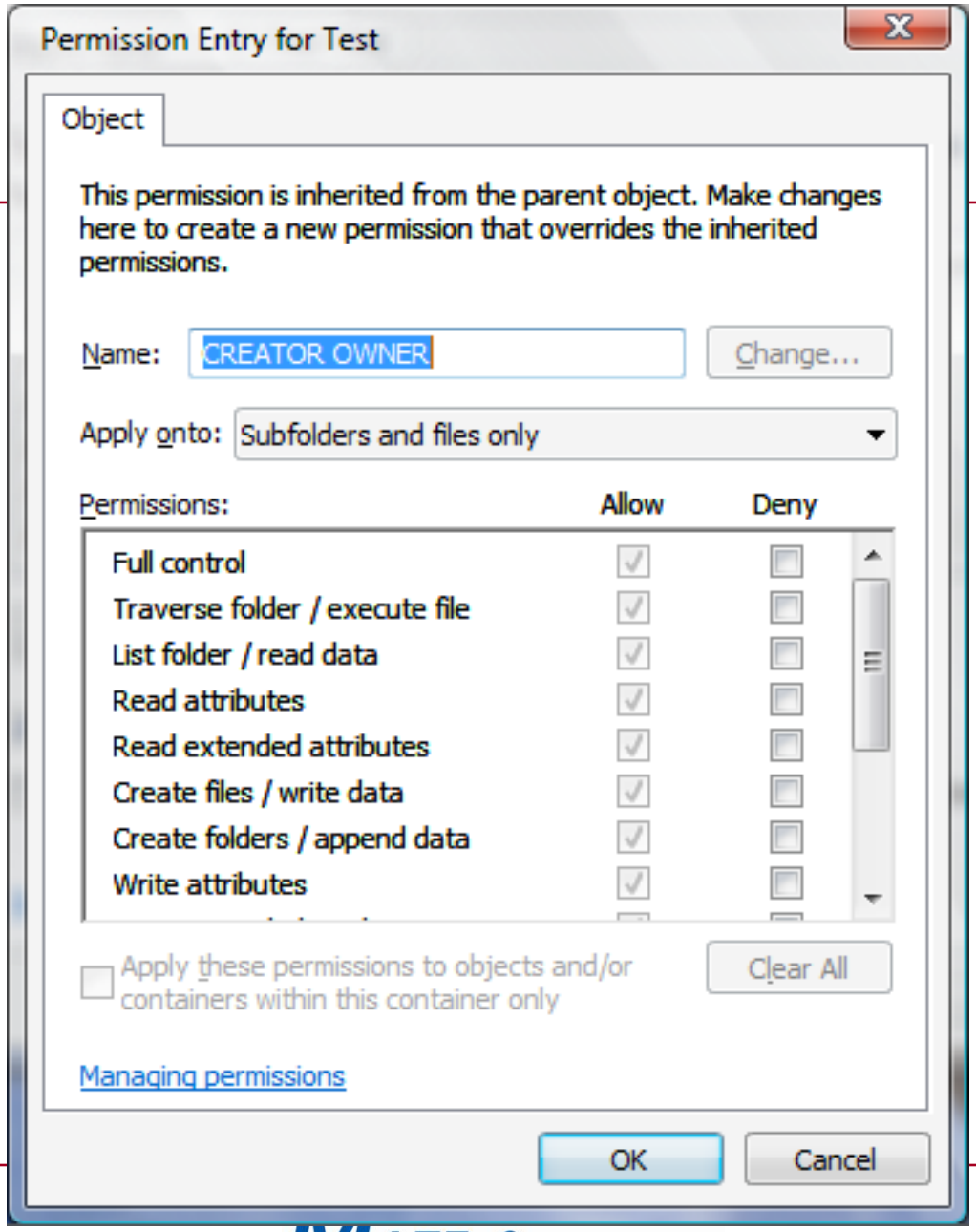
ACL IMPROVEMENTS

Old ACL UI


Test.txt Properties
General
Security
Summary
Group or user names:
Administrators (JESPERJO0\Administrators)
jesperjo (REDMOND\jesperjo)
SYSTEM
Users (JESPERJO0\Users)
Add...
Remove
Permissions for Administrators
Allow
Deny
Full Control
Modify
Read & Execute
Read
Write
Special Permissions
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

New ACL UI


Test.txt Properties
General
Security
Details
Previous Versions
Object name: C:\Test\Test.txt
Group or user names:
SYSTEM
Administrators (JESPERJO1\Administrators)
Users (JESPERJO1\Users)
Edit...
Permissions for Administrators
Allow
Deny
Full control
Modify
Read & execute
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply


Permission Entry for Test
Object
This permission is inherited from the parent object. Make changes here to create a new permission that overrides the inherited permissions.
Name:
CREATOR OWNER
Change...
Apply onto:
Subfolders and files only
Permissions:
Allow
Deny
Full control
Traverse folder / execute file
List folder / read data
Read attributes
Read extended attributes
Create files / write data
Create folders / append data
Write attributes
Apply these permissions to objects and/or containers within this container only
Clear All
Managing permissions
OK
Cancel

Windows Vista Security

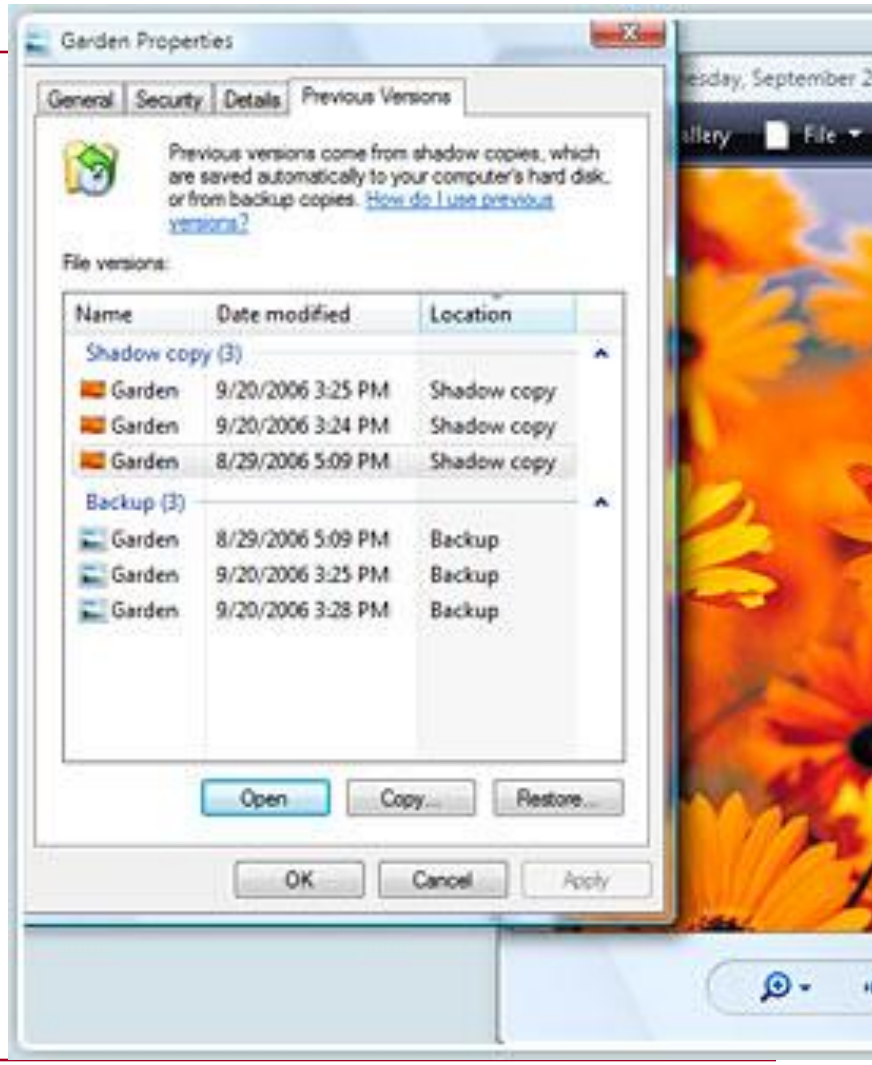
VOLUME SHADOW COPY

Features

- Available in the Ultimate, Business, and Enterprise editions
- Creates point-in-time copies of files as you work
- Creates incremental copies on a scheduled basis of files that have changed
- Easily access to this feature (end user)
- Single files as well as whole folders

Easy Access

- To access
- Right click on a folder
- Select “Properties”
- In the properties dialog box select the “Previous Versions” tab.
- So easy a caveman can do it.



System Protection

- If System Protection is turned on, Windows automatically creates shadow copies of files that have been modified since the last restore point was made.

Windows Vista Security

Section 3: Improvements

ISACA
Serving IT Governance Professionals
San Francisco Chapter

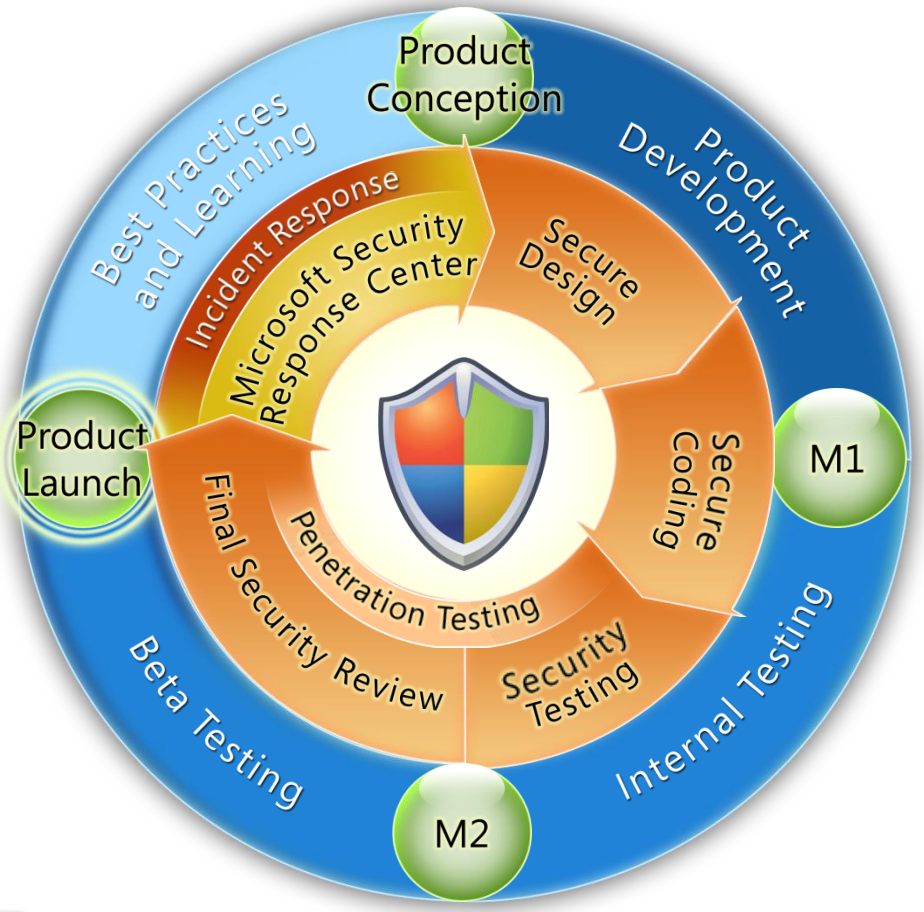
Windows Vista Security

IMPROVEMENT INTRODUCTION

Windows Vista

- Secure Design SDLC
- Network Access Protection
- TCP/IP Next Generation
- Restart Manager
- Increased Audit Abilities
- Code Integrity
- RDP
- SMB v2
- Stricter Policies

Security Development Lifecycle



Process

- Defines security requirements and milestones
- MANDATORY if exposed to meaningful security risks
- Requires response and service planning
- Includes Final Security Review (FSR) and Sign-off

Education

- Mandatory annual training – internal trainers
- BlueHat – external speakers on current trends
- Publish guidance on writing secure code, threat modeling and SDL; as well as courses

Accountability

- In-process metrics to provide early warning
- Post-release metrics assess final payoff (# of vulns)
- Training compliance for team and individuals

Microsoft Product Development Lifecycle

Microsoft Security Development Lifecycle

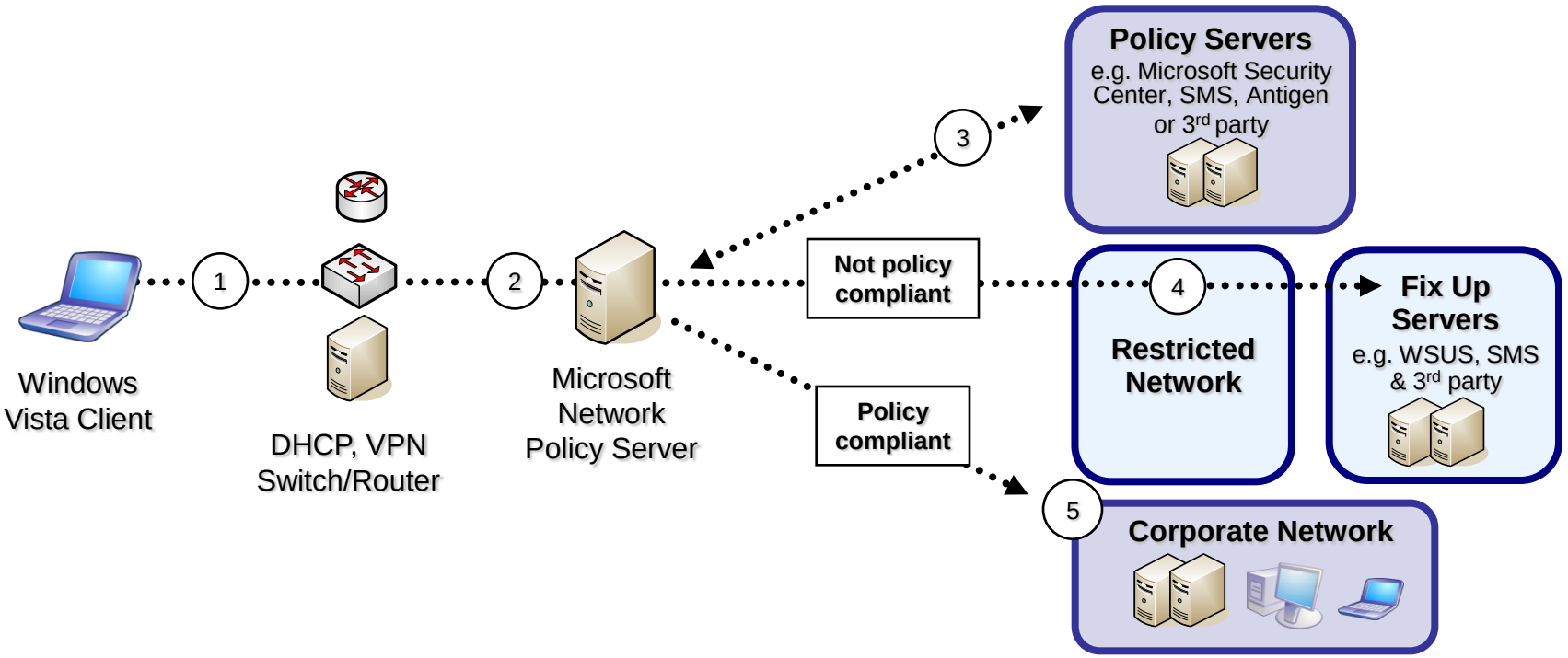
Windows Vista Security

NETWORK ACCESS PROTECTION

NAP - Network Access Protection

- NAP is a new technology that has roots in VPN quarantine, but now extends to all network clients, not just remote access
- Relies on NAP-aware servers
- Ensures computer adheres to your policy
- If PC is non-compliant, it will be given a chance to update

Network Access Protection



What Is Network Access Protection?

A policy enforcement system to ensure network clients meet health requirements such as:

- Software update levels
- Antivirus signatures
- Specific configuration settings
- Open and closed ports
- Firewall settings

What Are the NAP Components?

The components used by NAP are:

- Network Policy Server
- Enforcement client

The NAP enforcement options are:

- IPsec
- 802.1X
- VPN
- DHCP

What Are the NAP Implementation Scenarios?

NAP scenarios are:

- Monitor the health of roaming laptops
- Ensure the health of desktop computers
- Determine the health of visiting portable computers
- Verify the health of unmanaged home computers

Windows Vista Security

TCP/IP IMPROVEMENTS

NG TCP/IP

Next Generation TCP/IP in Vista and "Longhorn"

- A new, fully re-worked replacement of the old TCP/IP stack
- Dual-stack IPv6 implementation, with now obligatory IPSec
  - IPv6 is more secure than IPv4 by design, esp.:
    - Privacy, tracking, network port scanning, confidentiality and integrity
- Other network-level security enhancements for both IPv4 and IPv6
  - Strong Host model
  - Windows Filtering Platform
  - Improved stack-level resistance to **all known** TCP/IP-based denial of service and other types of network attacks
  - Routing Compartments
  - Auto-configuration and no-restart reconfiguration

- Read: www.microsoft.com/technet/community/columns/cableguy/cg0905.mspx

TCP/IP protection

- Enhancements:
  - Smart TCP port allocation
  - SYN attack protection is enabled by default
  - New SYN attack notification IP Helper APIs
  - Winsock self-healing

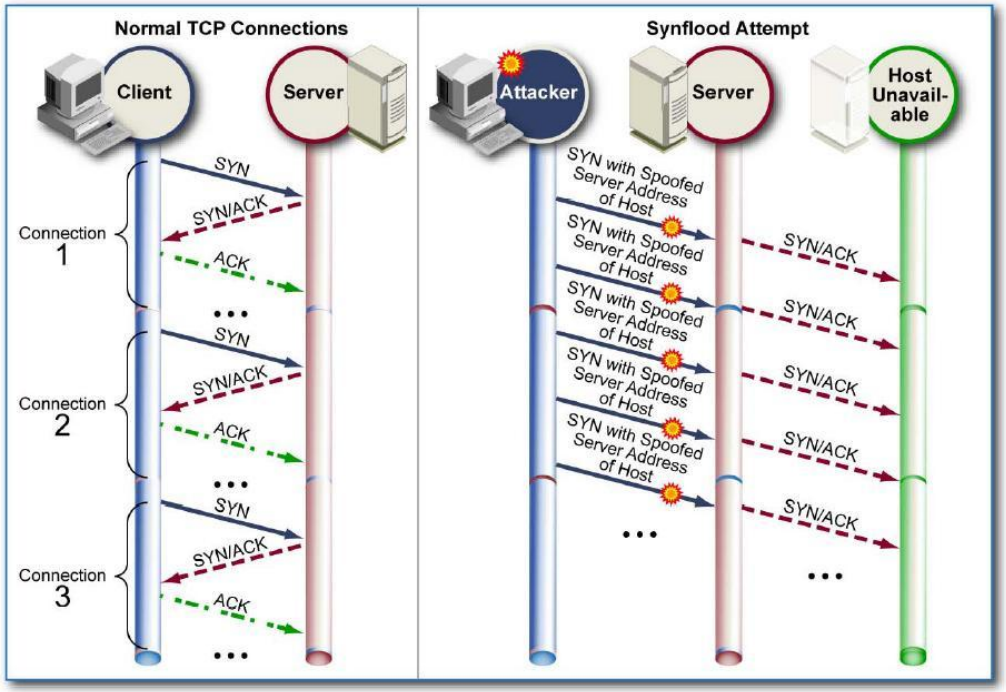


Figure 4-4. Synflood Attack

Windows Vista Security

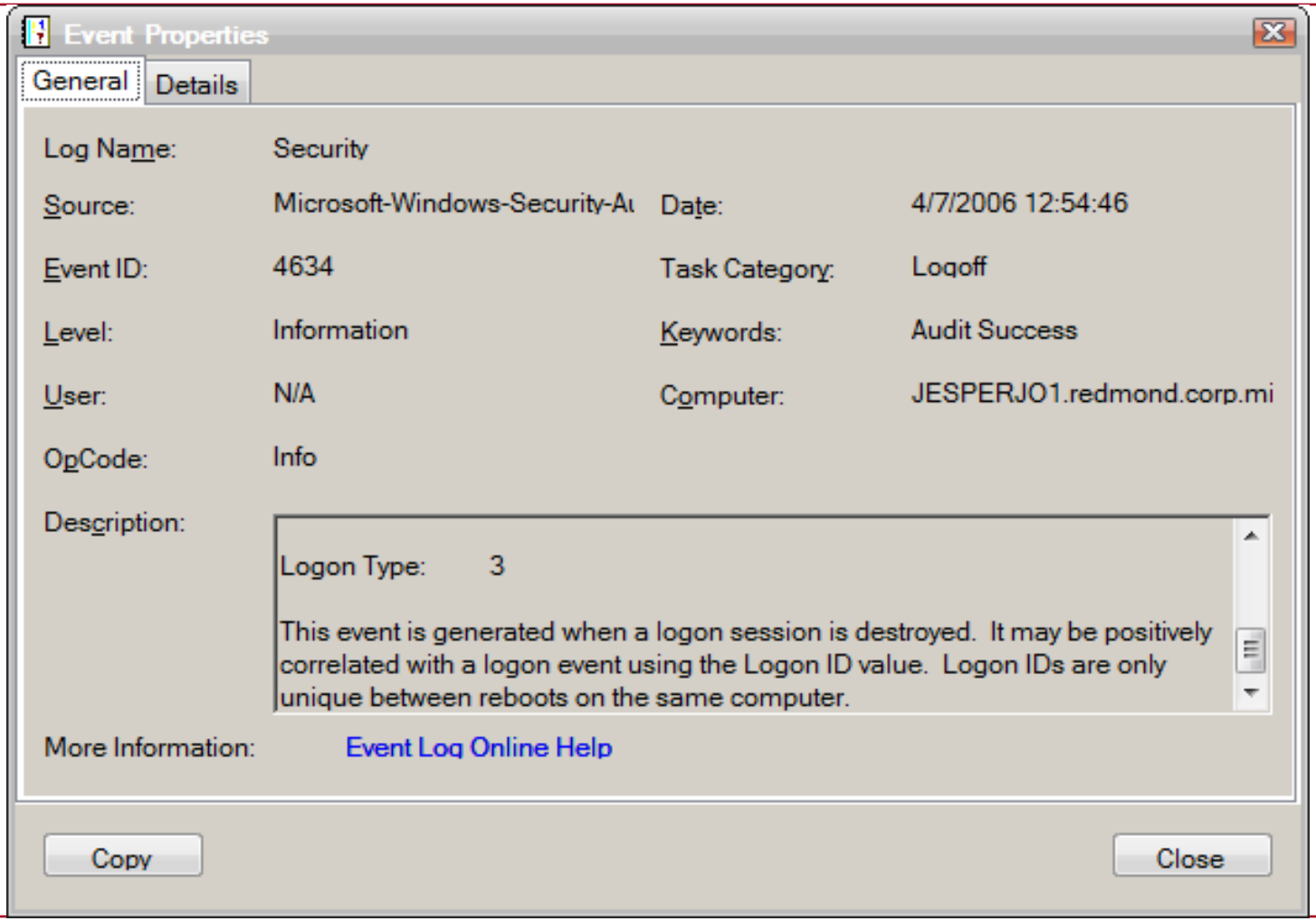
AUDIT IMPROVEMENTS

Granular Audit Policy

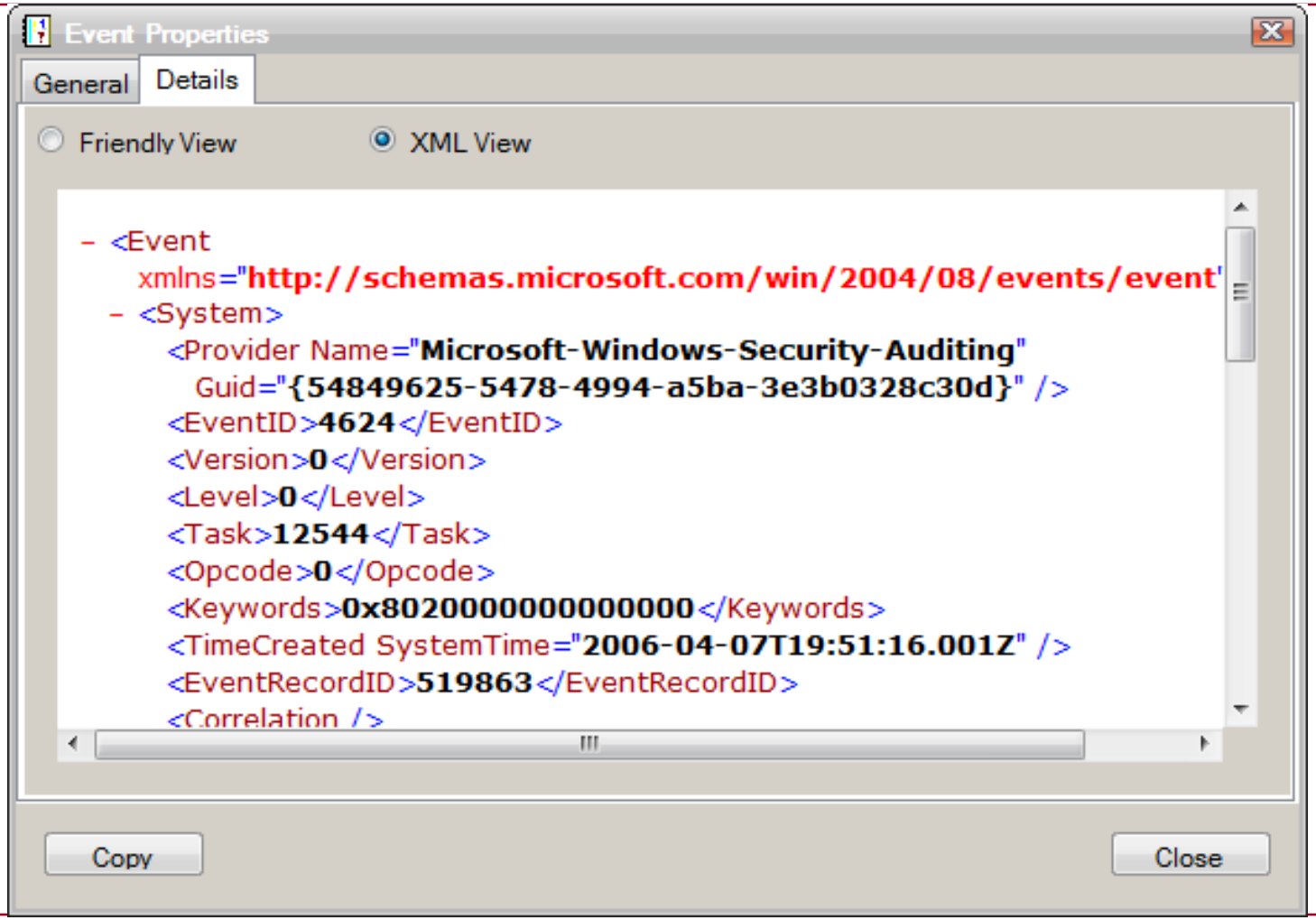
Added Auditing For

- Registry value change audit events (old+new values)
- AD change audit events (old+new values)
- Improved operation-based audit
- Audit events for UAC
- Improved IPSec audit events including support for AuthIP
- RPC Call audit events
- Share Access audit events
- Share Management events
- Cryptographic function audit events
- NAP audit events (server only)
- IAS (RADIUS) audit events (server only)

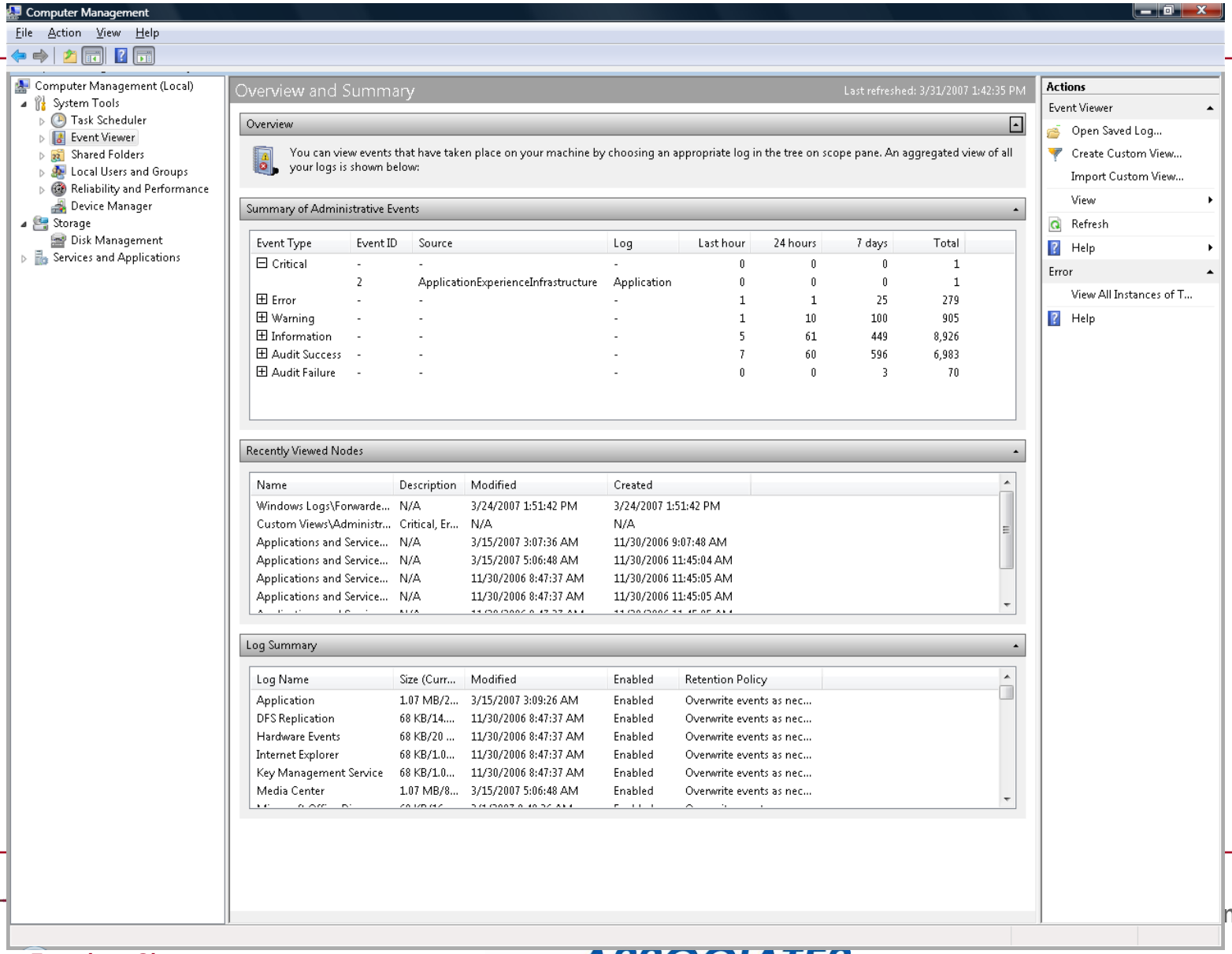
More Info In Event Log UI



Events Stored in XML



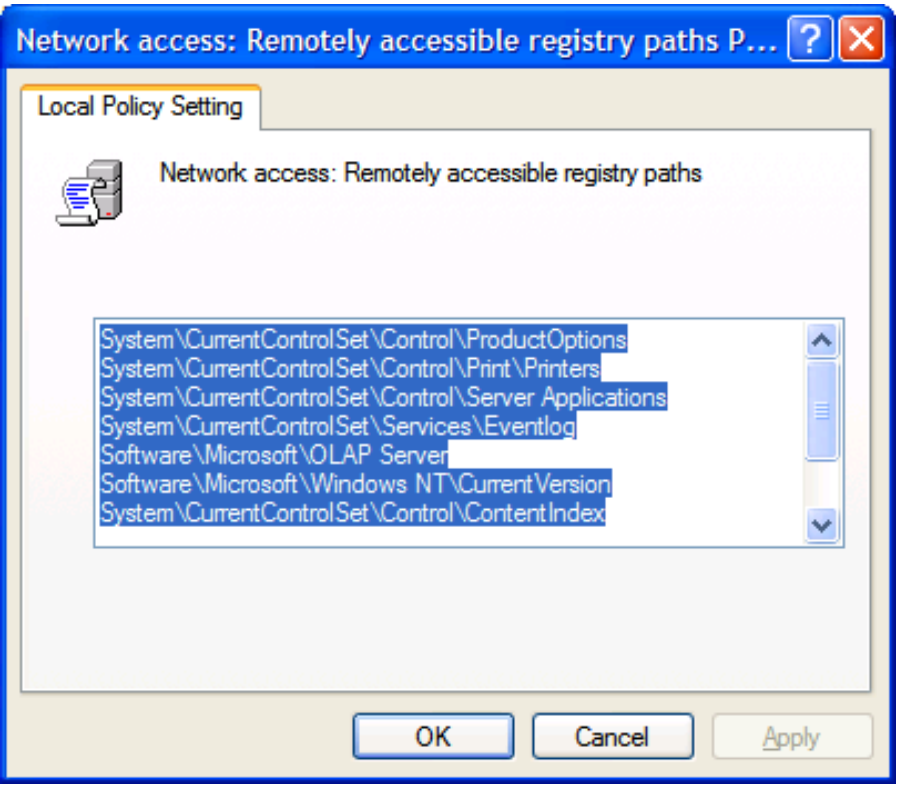
New Event Viewer

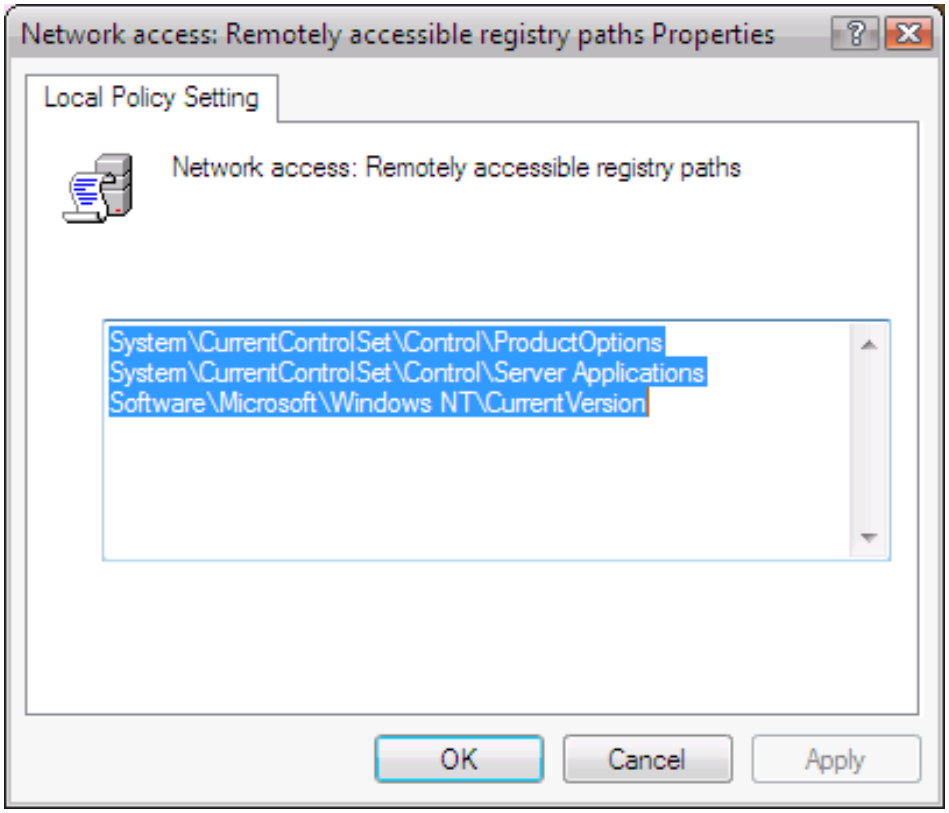


Windows Vista Security

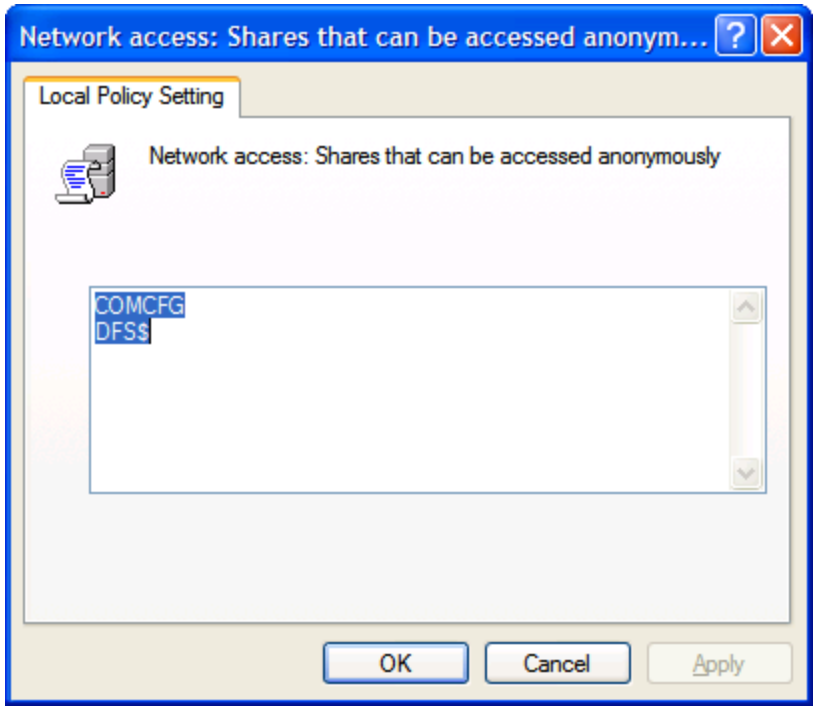
STRICTER POLICIES

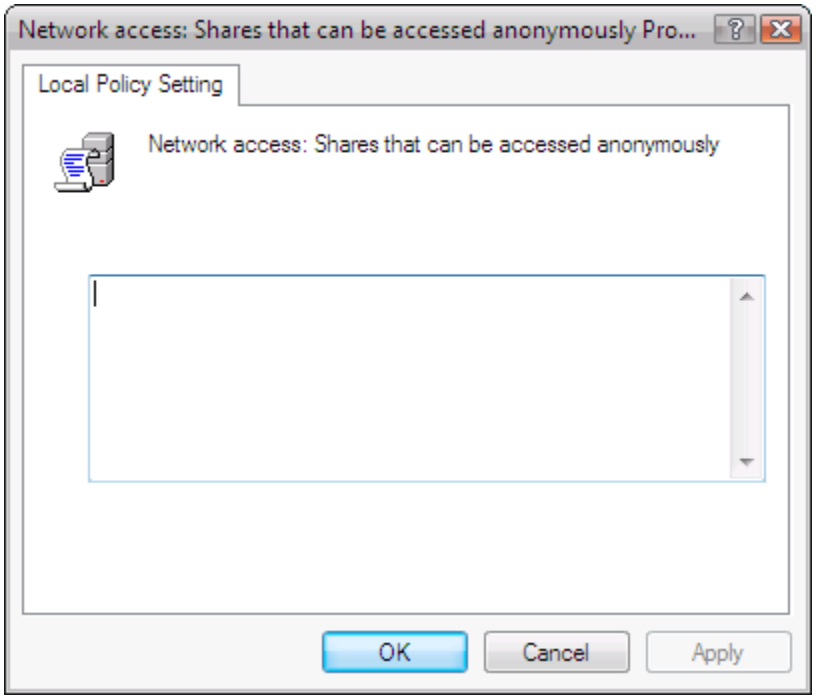
Stricter Policies

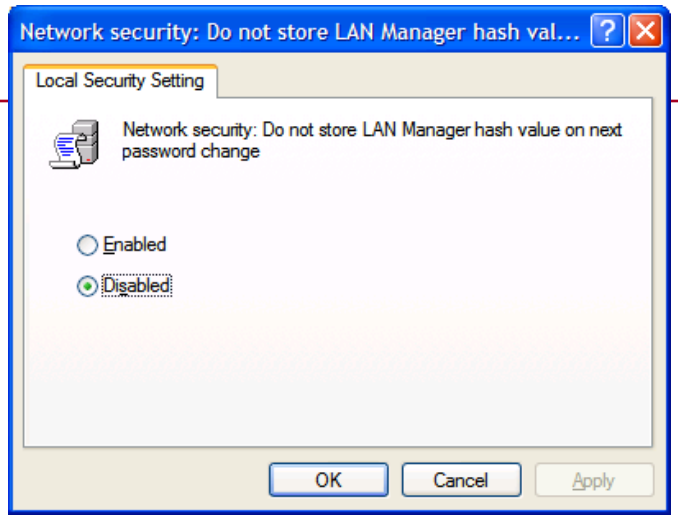


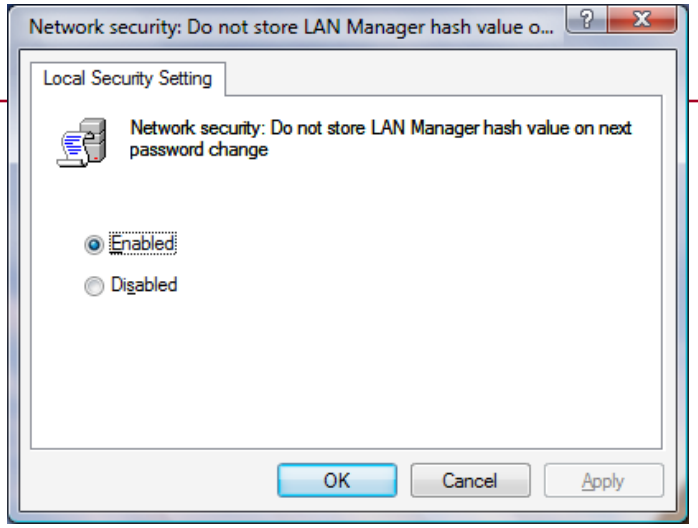


Stricter Policies

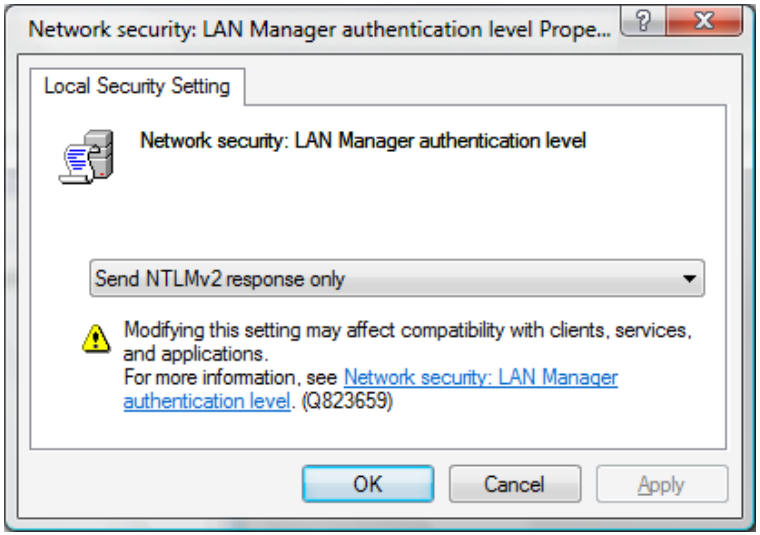





Network security: Do not store LAN Manager hash val...
Local Security Setting
Network security: Do not store LAN Manager hash value on next password change
Enabled
Disabled
OK
Cancel
Apply


Network security: Do not store LAN Manager hash value o...
Local Security Setting
Network security: Do not store LAN Manager hash value on next password change
Enabled
Disabled
OK
Cancel
Apply


Network security: LAN Manager authentication level ...
Local Security Setting
Network security: LAN Manager authentication level
Send LM & NTLM responses
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)
OK
Cancel
Apply


Network security: LAN Manager authentication level Prope...
Local Security Setting
Network security: LAN Manager authentication level
Send NTLMv2 response only
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)
OK
Cancel
Apply

Windows Vista Security

OTHER IMPROVEMENTS

What's New In SMBv2

- Only 16 commands (80 in SMBv1)
- Implicit sequence number speeds up hashing
- SHA-256 signatures (MD-5 in SMBv1)
- Handles reconnections more reliably
- Client-side file encryption
- Symbolic links across shares (disabled by default)
- Better load balancing mitigates DOS attacks

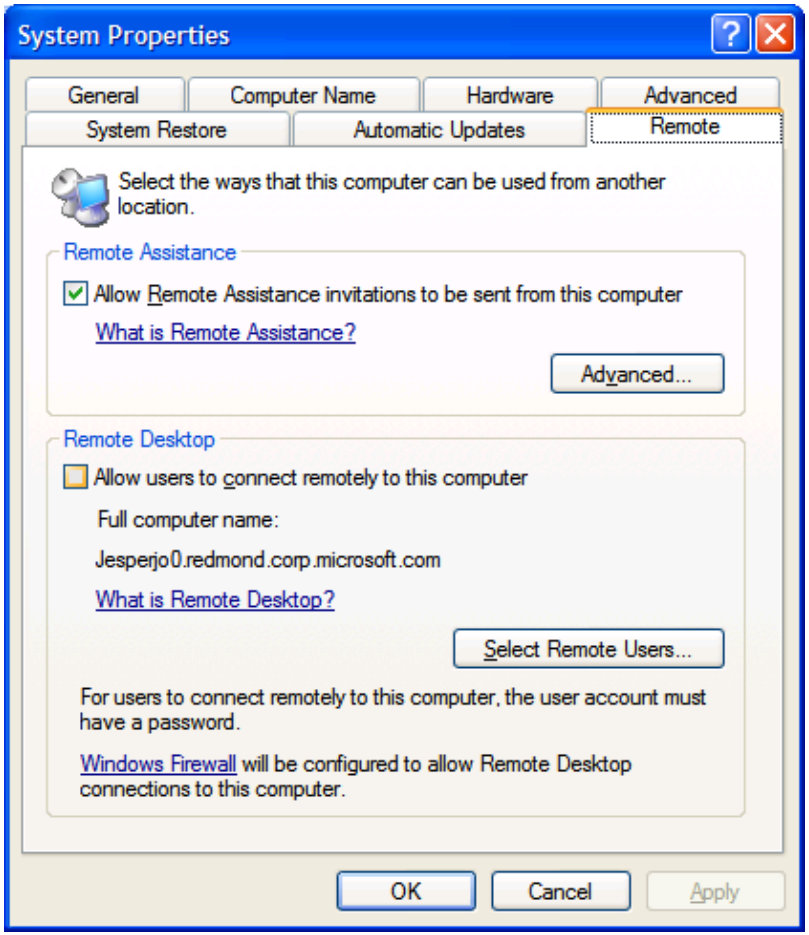
Restart Manager

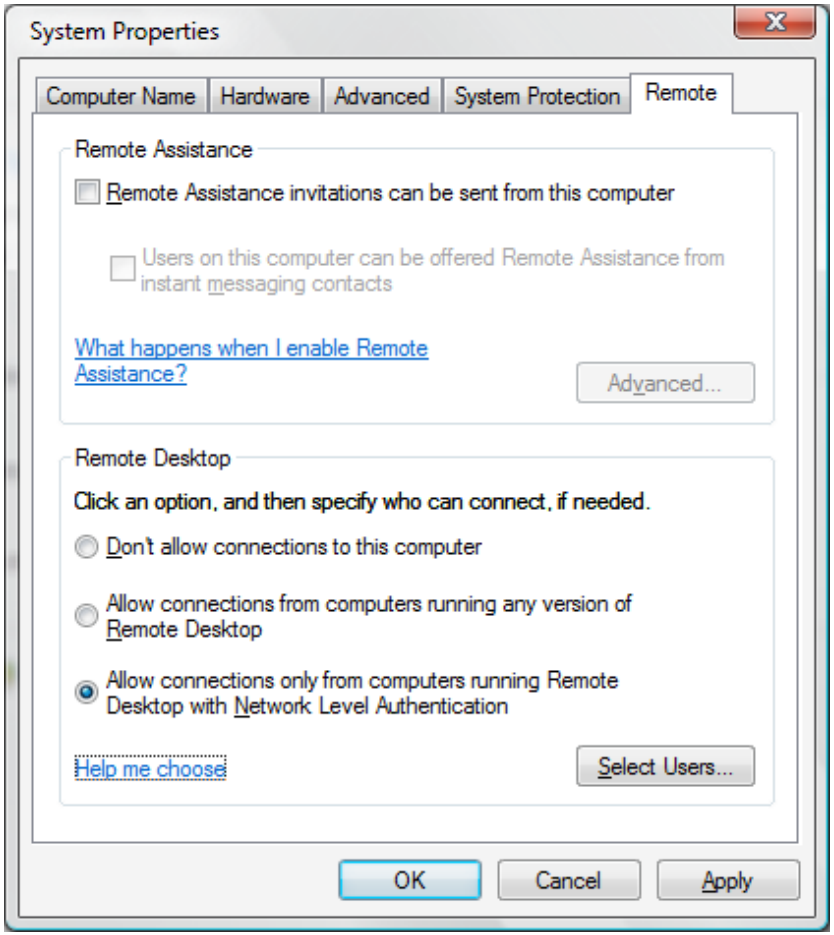
- Some updates require a restart
- Restart Manager will:
  - Minimise the number of needed restarts by pooling updates
  - Deal with restarts of computers that may be left locked by a user with applications running
    - E.g. after restart, Microsoft Word will re-open a document on page 42, as it was before the restart
    - This function of most importance to centralised desktop management in corporations, not home users, of course

Better Buffer Overflow Protection

- Second cookie protects exception handlers
- Safer CRT exception handlers
- No more executable pages outside images
- /NXCOMPAT linker flag in build tools
- Heap protection
- Signed kernel code (x64 only)

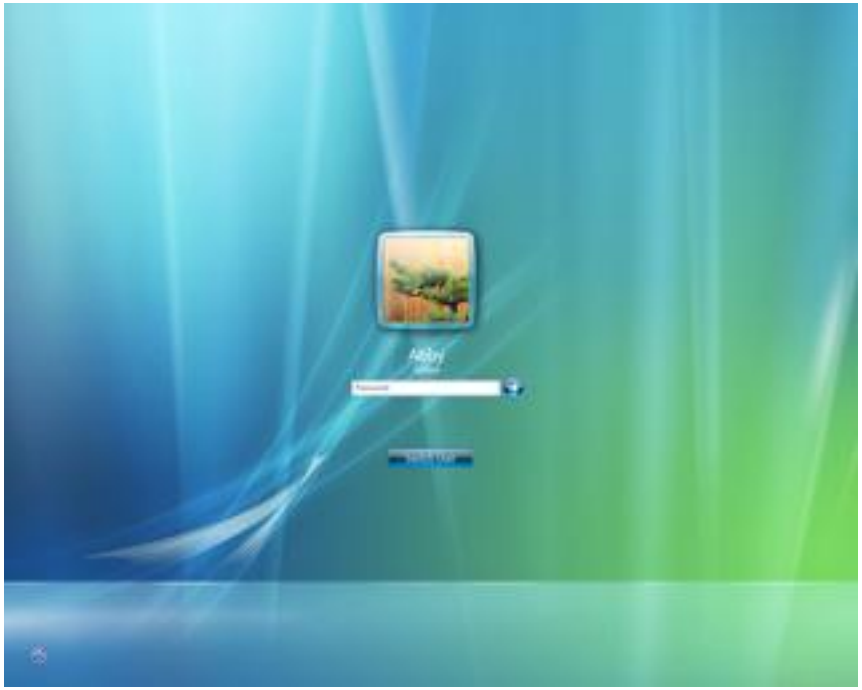
New RDP Controls





Bye, bye GINA

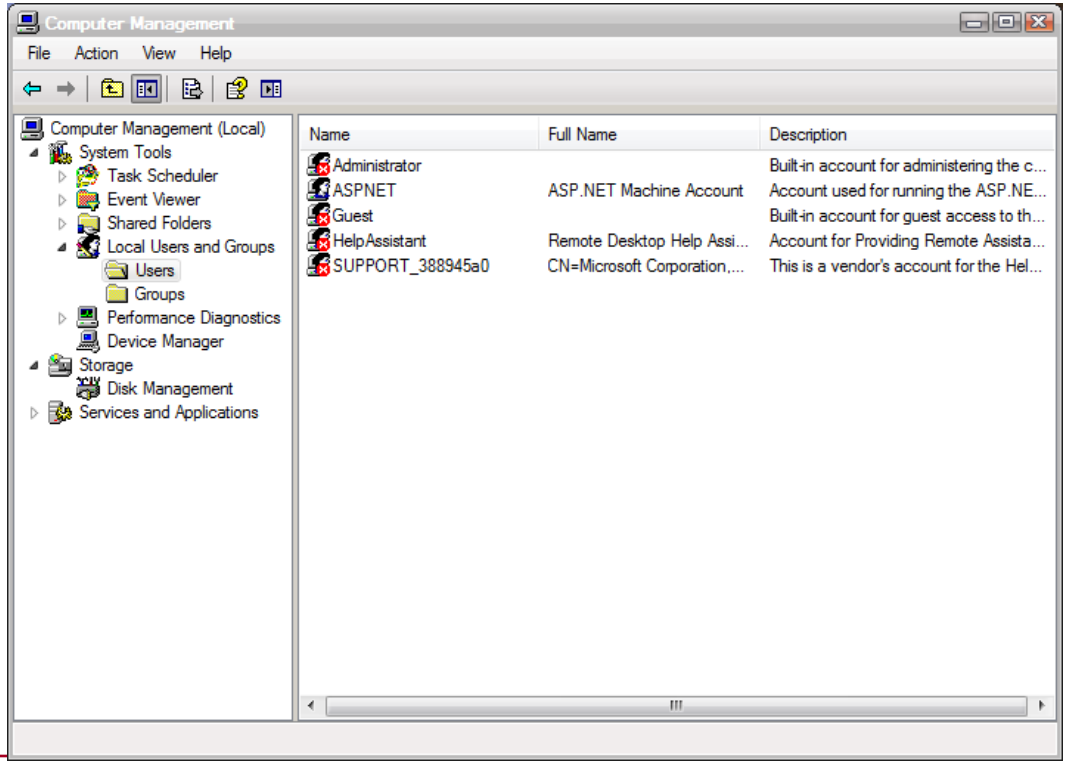
- GINA has been replaced with Credential Service Provider interfaces



Graphical Identification and Authentication (**GINA**)

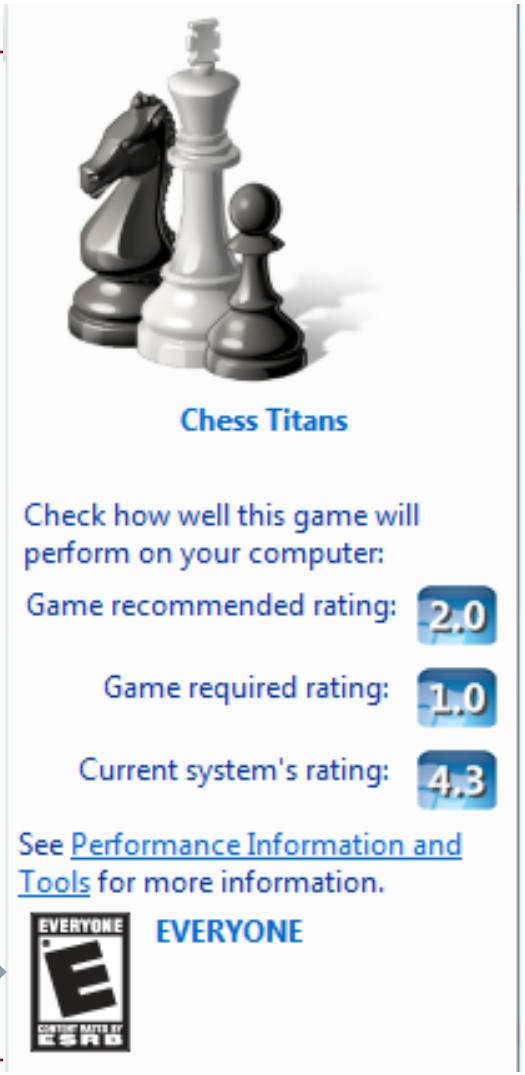
User Accounts

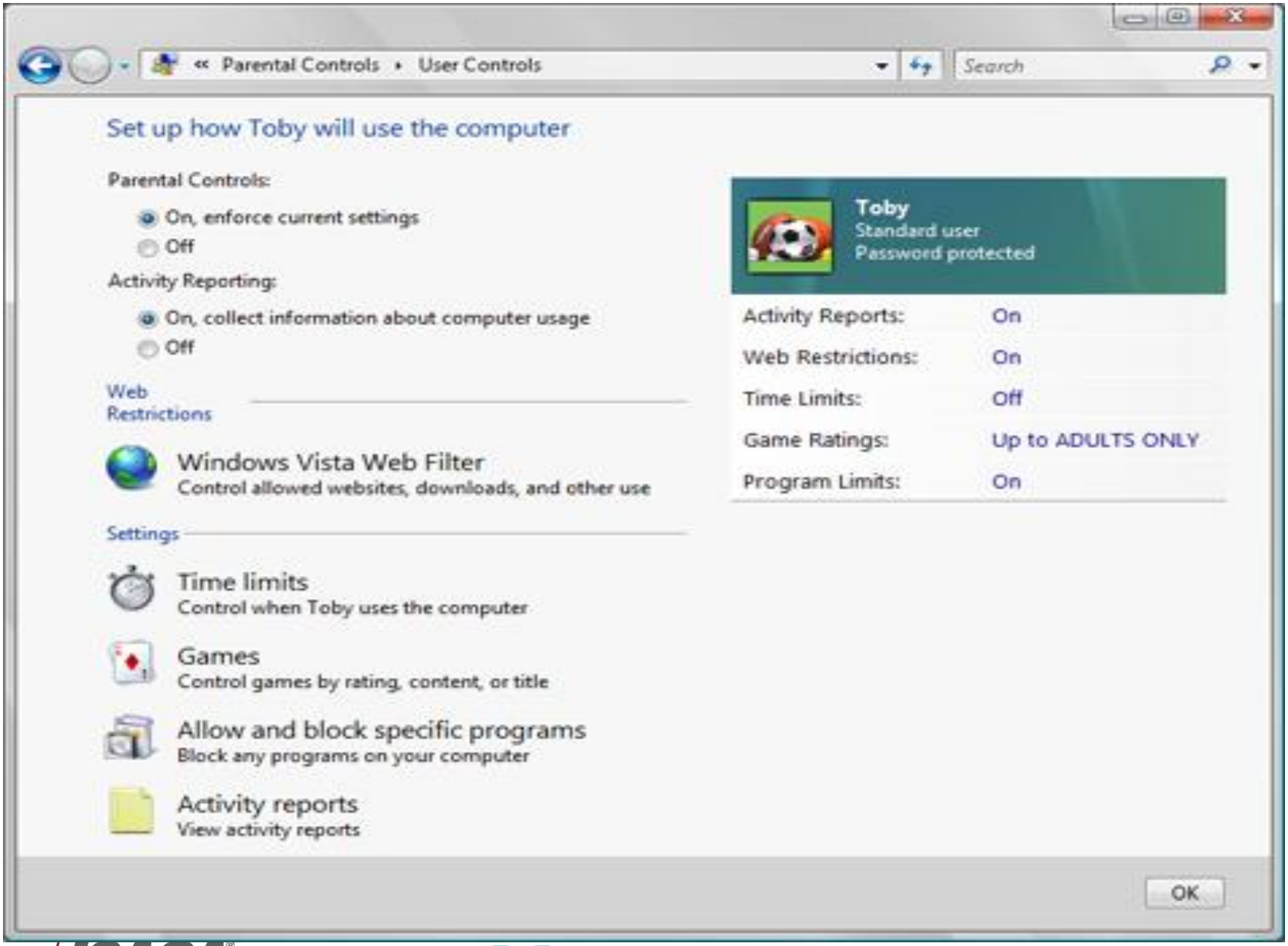
- Administrator Account disabled
- Power users gone

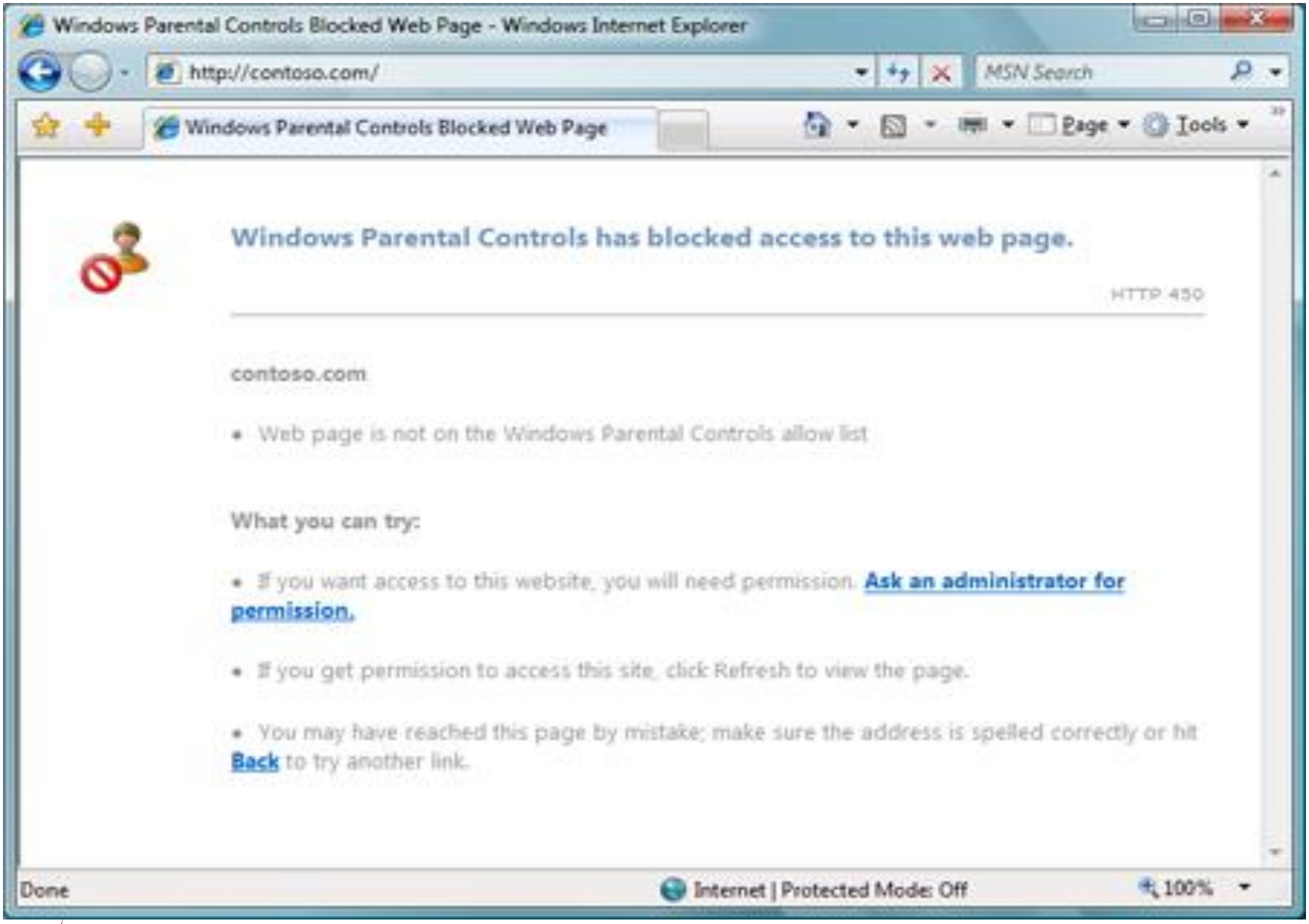


A Word about Parental Controls

- Web Restrictions
- Time Limits
- Program that can be run.
  - Games can be limited by rating
- Display activity reports

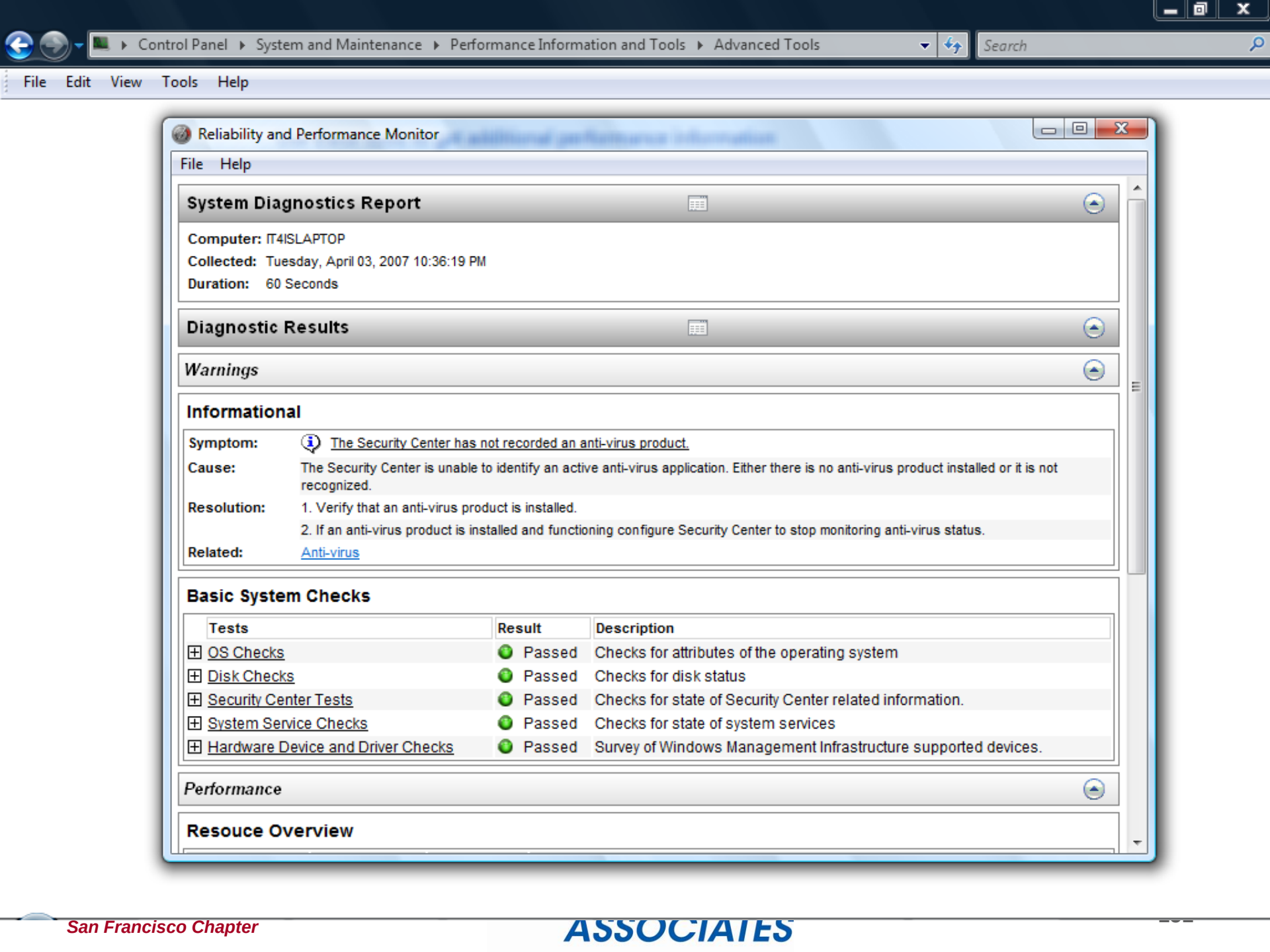



« Parental Controls ▸ User Controls
Search
Set up how Toby will use the computer
Parental Controls:
On, enforce current settings
Off
Activity Reporting:
On, collect information about computer usage
Off
Web Restrictions
Windows Vista Web Filter
Control allowed websites, downloads, and other use
Settings
Time limits
Control when Toby uses the computer
Games
Control games by rating, content, or title
Allow and block specific programs
Block any programs on your computer
Activity reports
View activity reports
Toby
Standard user
Password protected
Activity Reports: On
Web Restrictions: On
Time Limits: Off
Game Ratings: Up to ADULTS ONLY
Program Limits: On
OK


Windows Parental Controls Blocked Web Page - Windows Internet Explorer
http://contoso.com/
MSN Search
Windows Parental Controls Blocked Web Page
Page
Tools
Windows Parental Controls has blocked access to this web page.
HTTP 450
contoso.com
• Web page is not on the Windows Parental Controls allow list
What you can try:
• If you want access to this website, you will need permission. Ask an administrator for permission.
• If you get permission to access this site, click Refresh to view the page.
• You may have reached this page by mistake; make sure the address is spelled correctly or hit Back to try another link.
Done
Internet | Protected Mode: Off
100%

For more information use System Diagnostic Reports

- Open System and Maintenance
  - Performance Information and Tools
  - Advanced Tools
  - Generate a System Health Report


Control Panel ▸ System and Maintenance ▸ Performance Information and Tools ▸ Advanced Tools
Search
File Edit View Tools Help
Reliability and Performance Monitor
File Help
System Diagnostics Report
Computer: IT4ISLAPTOP
Collected: Tuesday, April 03, 2007 10:36:19 PM
Duration: 60 Seconds
Diagnostic Results
Warnings
Informational
Symptom: The Security Center has not recorded an anti-virus product.
Cause: The Security Center is unable to identify an active anti-virus application. Either there is no anti-virus product installed or it is not recognized.
Resolution: 1. Verify that an anti-virus product is installed.
2. If an anti-virus product is installed and functioning configure Security Center to stop monitoring anti-virus status.
Related: Anti-virus
Basic System Checks
Tests Result Description
OS Checks Passed Checks for attributes of the operating system
Disk Checks Passed Checks for disk status
Security Center Tests Passed Checks for state of Security Center related information.
System Service Checks Passed Checks for state of system services
Hardware Device and Driver Checks Passed Survey of Windows Management Infrastructure supported devices.
Performance
Resouce Overview

Reliability and Performance Monitor

File Help

Basic System Checks

Tests	Result	Description
OS Checks	Passed	Checks for attributes of the operating system

Test Groups	Tests	Failed	Description
OS Version Check	1	0	Passed

Disk Checks	Passed	Checks for disk status

Test Groups	Tests	Failed	Description
SMART Predict Failure Check	1	0	Passed
Logical Disk Dirty Bit Check	1	0	Passed
Free Disk Space Available C:	1	0	Drive C: has 30% free disk space [22372 MB]

Security Center Tests	Passed	Checks for state of Security Center related information.

Test Groups	Tests	Failed	Description
Check that Anti-Spyware Product is up-to-date.	1	0	Passed
Check for Anti-Spyware Product that is enabled.	1	0	Passed
User Account Control Enabled Check	1	0	Passed
Windows Update Enabled Check	1	0	Passed

System Service Checks	Passed	Checks for state of system services

Test Groups	Tests	Failed	Description
Abnormally Terminated Services Check	1	0	Passed
Workstation Service Check	1	0	Passed

Hardware Device and Driver Checks	Passed	Survey of Windows Management Infrastructure supported devices.

Test Groups	Tests	Failed	Description
Controller Device Configured Fail Count	14	0	Controller devices.
Controller Device Status Fail Count	14	0	Controller devices.
Cooling Configured Fail Count	2	0	Cooling devices.
Cooling Status Fail Count	2	0	Cooling devices.

Reliability and Performance Monitor

File Help

Storage Device Status Fail Count	2	0 Storage devices.
Video Device Configured Fail Count	2	0 Video devices.
Video Device Status Fail Count	2	0 Video devices.
PlugAndPlay Device Configured Fail Count	128	0 PlugAndPlay devices.
PlugAndPlay Device Status Fail Count	128	0 PlugAndPlay devices.

Performance

Resouce Overview

Component	Status	Utilization	Details
CPU	Idle	15 %	Low CPU load.
Network	Idle	0 %	Busiest network adapter is less than 15%.
Disk	Idle	11 /sec	Disk I/O is less than 100 (read/write) per second on disk 0.
Memory	Normal	45 %	1132 MB Available.

Software Configuration

Hardware Configuration

CPU

Network

Disk

Memory

Report Statistics

Reliability and Performance Monitor

File Help

Query	Result
root\cimv2:SELECT * FROM Win32_OperatingSystem	0x0
root\cimv2:SELECT * FROM Win32_ComputerSystem	0x0

Security Center Information

Anti-Spyware Information

Top: 1 of 1

Query	Query Result
root\SecurityCenter:SELECT * FROM AntiSpywareProduct	0x0

Anti-Virus Information

Top: 1 of 1

Query	Query Result
root\SecurityCenter:SELECT * FROM AntiVirusProduct	0x0

Firewall Information

Top: 1 of 1

Query	Query Result
root\SecurityCenter:SELECT * FROM FirewallProduct	0x0

User Account Control Settings

Top: 1 of 1

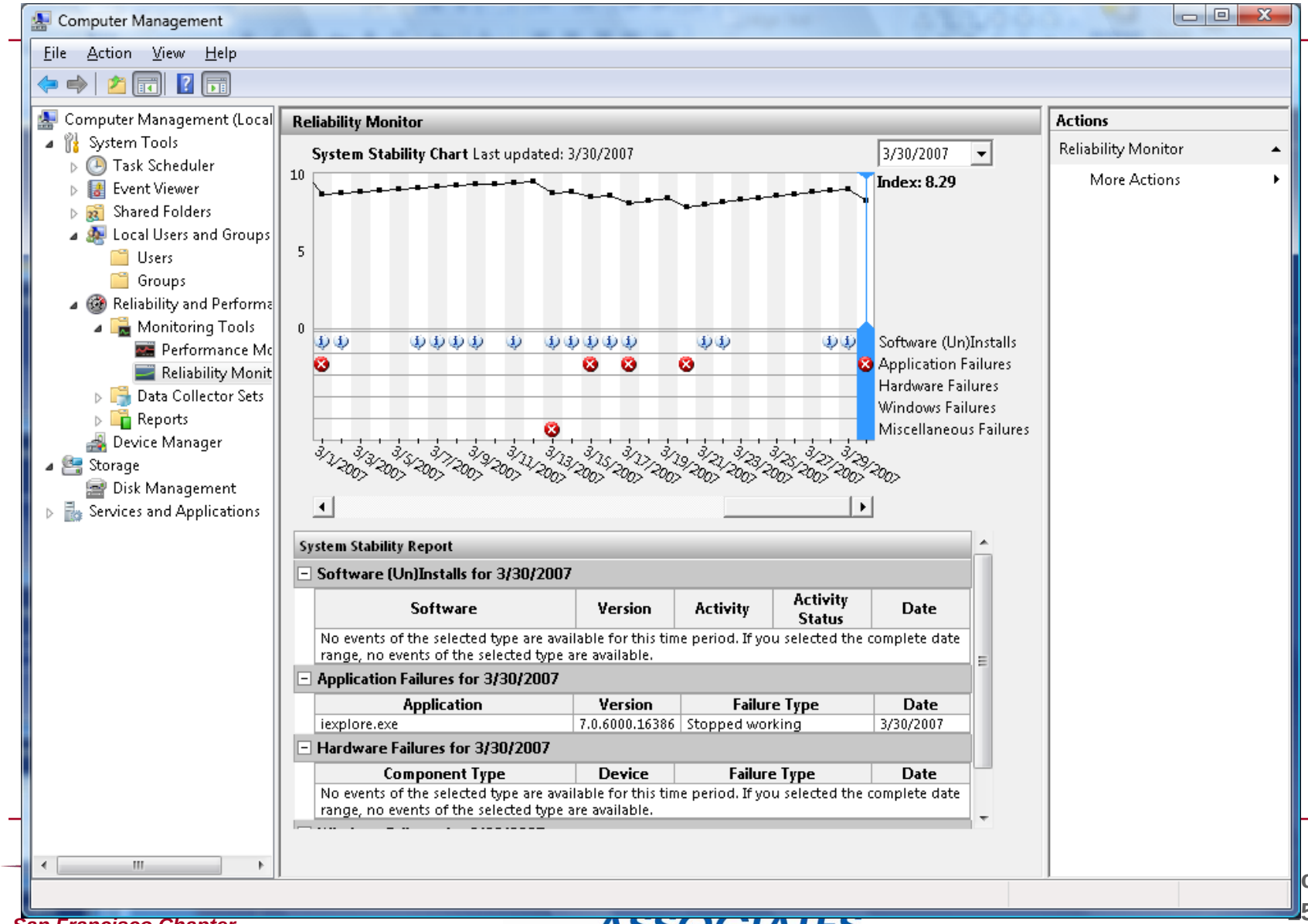
Query	Result
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	0x0

Windows Update Settings

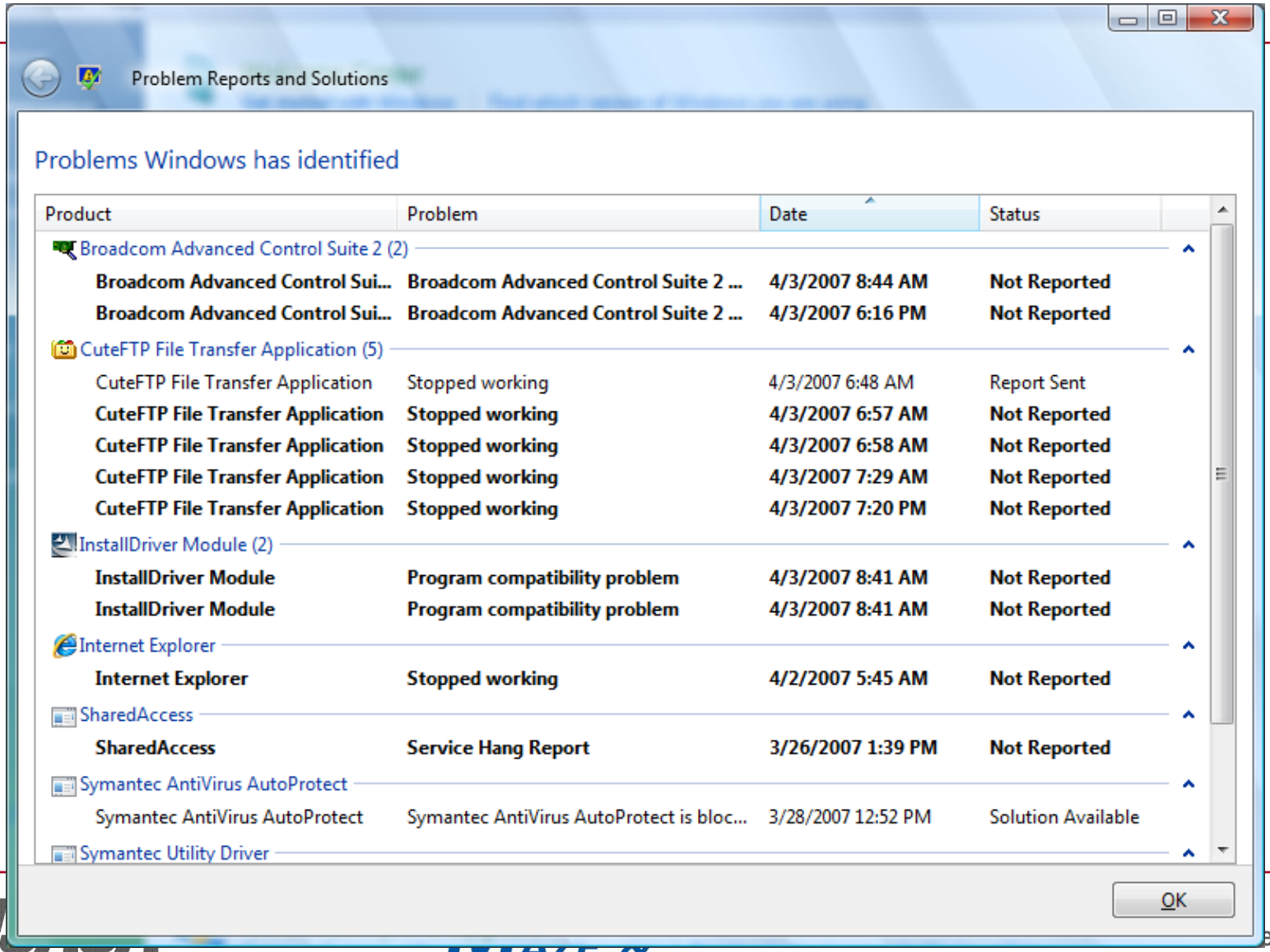
Top: 2 of 2

Query	Result
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\\	0x0

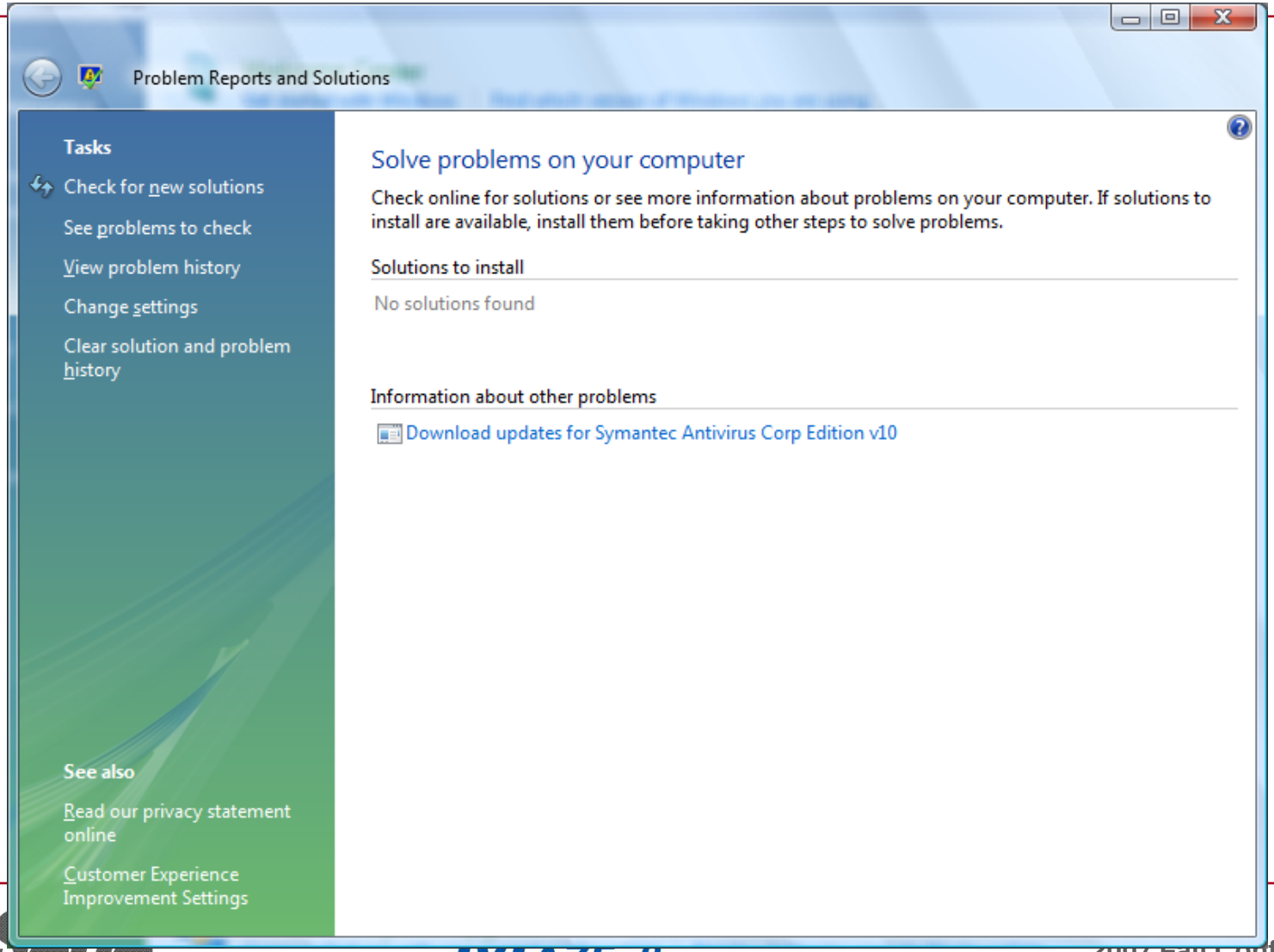
Reliability Monitor

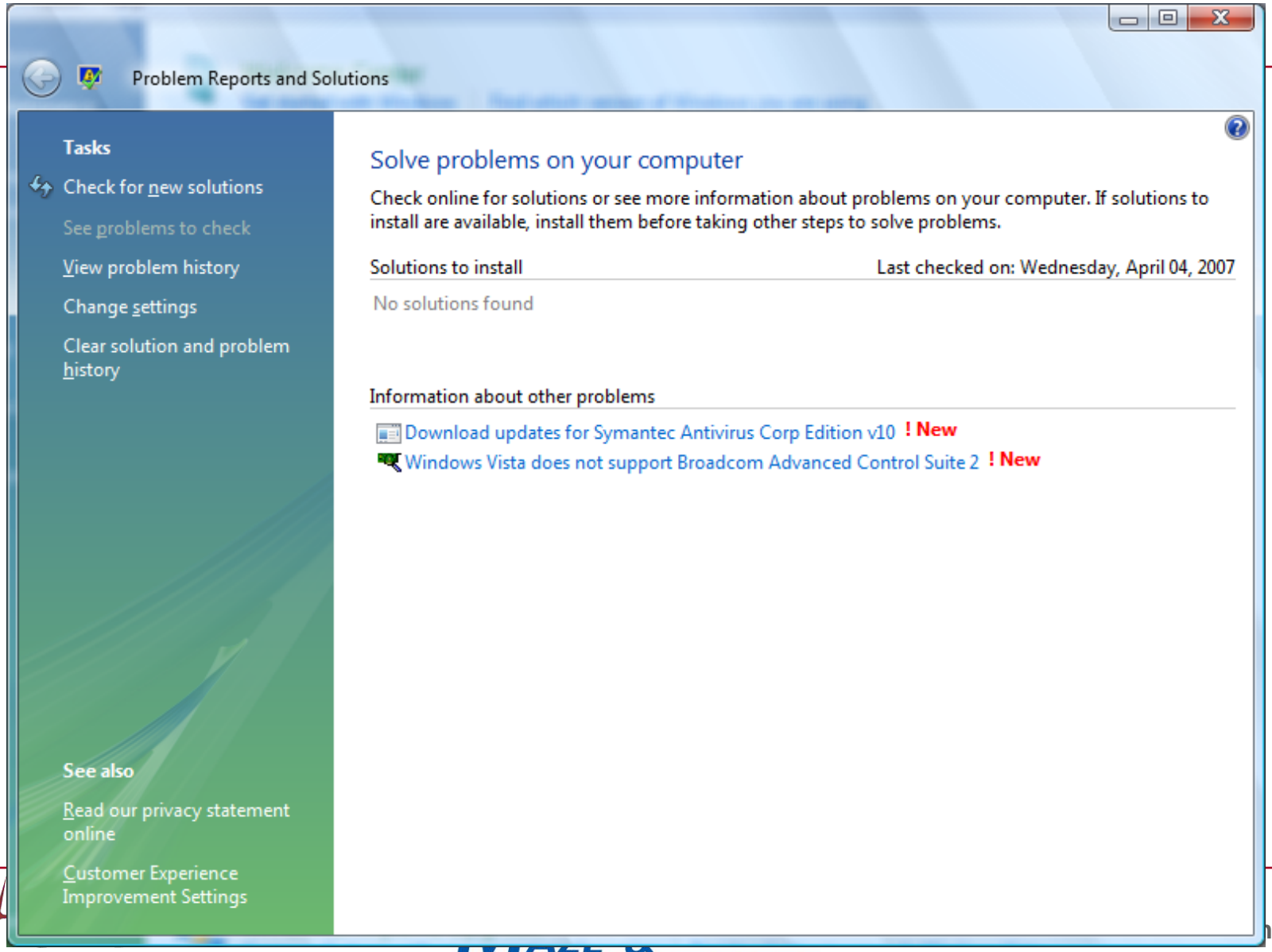


Problems Windows Identified

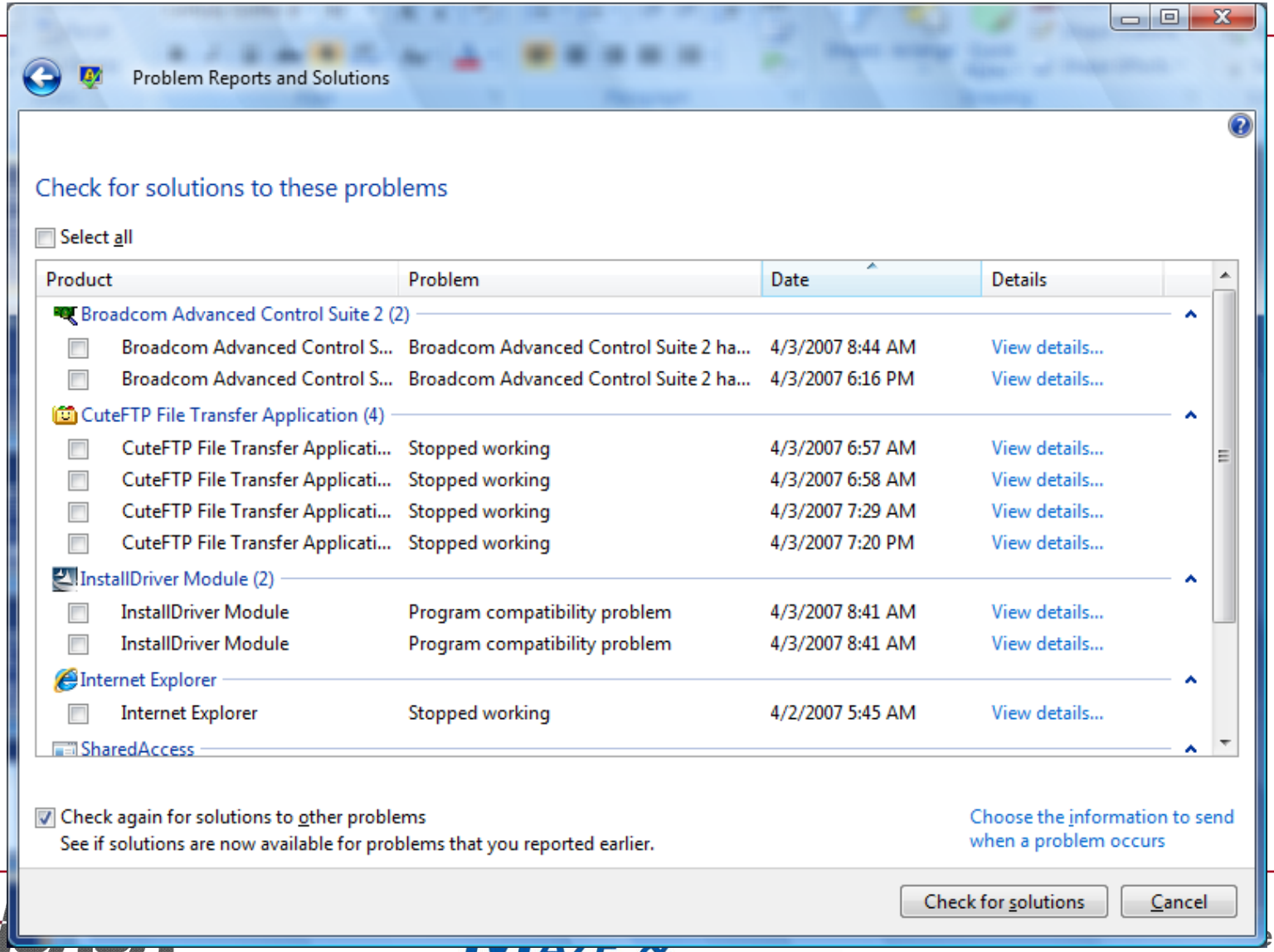


Problems and Solutions




Problem Reports and Solutions
Tasks
Check for new solutions
See problems to check
View problem history
Change settings
Clear solution and problem history
See also
Read our privacy statement online
Customer Experience Improvement Settings
Solve problems on your computer
Check online for solutions or see more information about problems on your computer. If solutions to install are available, install them before taking other steps to solve problems.
Solutions to install
Last checked on: Wednesday, April 04, 2007
No solutions found
Information about other problems
Download updates for Symantec Antivirus Corp Edition v10 ! New
Windows Vista does not support Broadcom Advanced Control Suite 2 ! New

Check for Solutions



Windows Vista Security

Section 4: Secure Deployment

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows Vista

SECURE DEPLOYMENT

Deployment baselines

- Available from Windows Vista Security Guide
- For high security
  - Specialized Security – Limited Functionality (SSLF) baseline
- For balanced security
  - Enterprise Client (EC) baseline

Warning!

- SSLF is not for most environments
- SSLF is appropriate for environments:
  - Where security is most important
  - Where loss of manageability and functionality is acceptable
- Expect more helpdesk calls
- Be prepared to exhaustively test the computers before deployment

SSLF Areas of Higher Security & Limited Functionality

- Restricted services and data access
- Restricted network access
- Strong network protection

Services & Data Access

- Disable administrator accounts.
- Enforce stronger password requirements.
- Require more strict account lockout policy.
- Require more strict policy for the following **User Rights Assignments** settings: **Log on as a Service** and **Log on as a Batch Job**.

Example GPO Settings

Setting	Windows default	Domain controller default	VSG EC Domain GPO	VSG SSLF Domain GPO
Enforce password history	0 passwords remembered	24 passwords remembered	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	42 days	90 days	90 days
Minimum password age	0 days	1 day	1 day	1 day
Minimum password length	0 characters	7 characters	8 characters	12 characters
Password must meet complexity requirements	Disabled	Enabled	Enabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled	Disabled	Disabled

Restrict Network Access

- Limit access to client systems across the network.
- Hide systems from browse lists.
- Control Windows Firewall exceptions.
- Implement connection security, such as packet signing.

Strong Network Protection

- Control process memory quota assignments.
- Control object creation.
- Control the ability to debug programs.
- Control process profiling.

Windows Vista

FINAL COMMENTS & RESOURCES

The Most Secure Windows Yet

Windows Vista™

Threat and Vulnerability Mitigation

- IE –protected mode/anti-phishing
- Windows Defender
- Bi-directional Firewall
- IPSEC improvements
- Network Access Protection (NAP)

Identity and Access Control

- User Account Control
- Plug and Play Smartcards
- Simplified Logon architecture
- Bitlocker
- RMS Client

Fundamentals

- SDL
- Service Hardening
- Code Scanning
- Default configuration
- Code Integrity

Special Thanks

Russ Humphries, Sr. Product Manager, Windows Vista Security, Microsoft

Jeff Sigman, Program Manager Windows Networking, Microsoft

Rob Labbe, Security Consultant, Microsoft

Resources

- Windows Vista Security Guide
  - http://www.microsoft.com/technet/windowsvista/security/guide.mspx
- Scott Riley Presentation
  - http://www.microsoft.com/emea/itsshowtime/sessionh.aspx?videoid=223
- http://technet.microsoft.com/en-us/windowsvista/aa905117.aspx

Resources

- Windows Server 2003 Security Guide
  - http://go.microsoft.com/fwlink/?LinkId=14846
- WindowSecurity.com
- SecWish@microsoft.com (Feedback email)
- Microsoft Windows Security Resource Kit (2nd Ed.) ISBN 0-7356-2174-8
- Service Pack 1 Overview
  - http://www.microsoft.com/technet/prodtechnol/windowsserver2003/servicepack/overview.mspx

Resources

- Microsoft Security Assessment Tool (MSAT)
- https://www.securityguidance.com/
- Microsoft Security
- http://www.microsoft.com/security/default.mspx
- Microsoft Baseline Security Analyzer (MBSA)
- http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- Microsoft Anti-Spyware (beta) Defender
- http://www.microsoft.com/athome/security/spyware/software/default.mspx

Resources

- RootKit Revealer
- http://www.sysinternals.com/Utilities/RootkitRevealer.html
- Strider GhostBuster Project (Rootkit detector)
- http://research.microsoft.com/rootkit/
- Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP
- http://go.microsoft.com/fwlink/?LinkId=15160

Contact Info

- Donald E. Hester
  - DonaldH@MazeAssociates.com

  - https://www.linkedin.com/in/donaldehester