

Security Overview for Windows Vista

**Bob McCoy, MCSE, CISSP/ISSAP
Technical Account Manager
Microsoft Corporation**

Agenda

User and group changes

Encryption changes

Audit changes

User rights

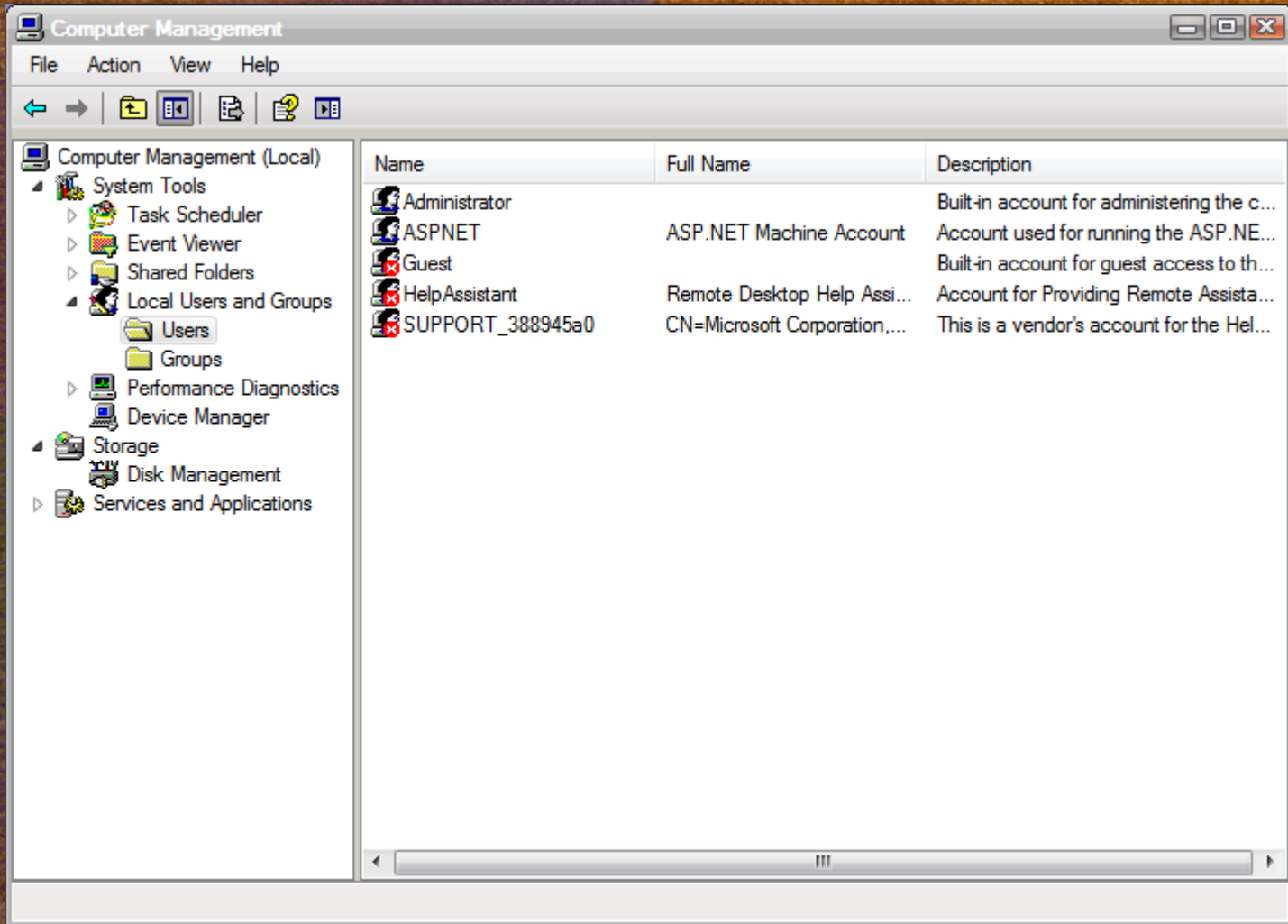
New and modified security options

Firewall changes

SMB v2

BitLocker

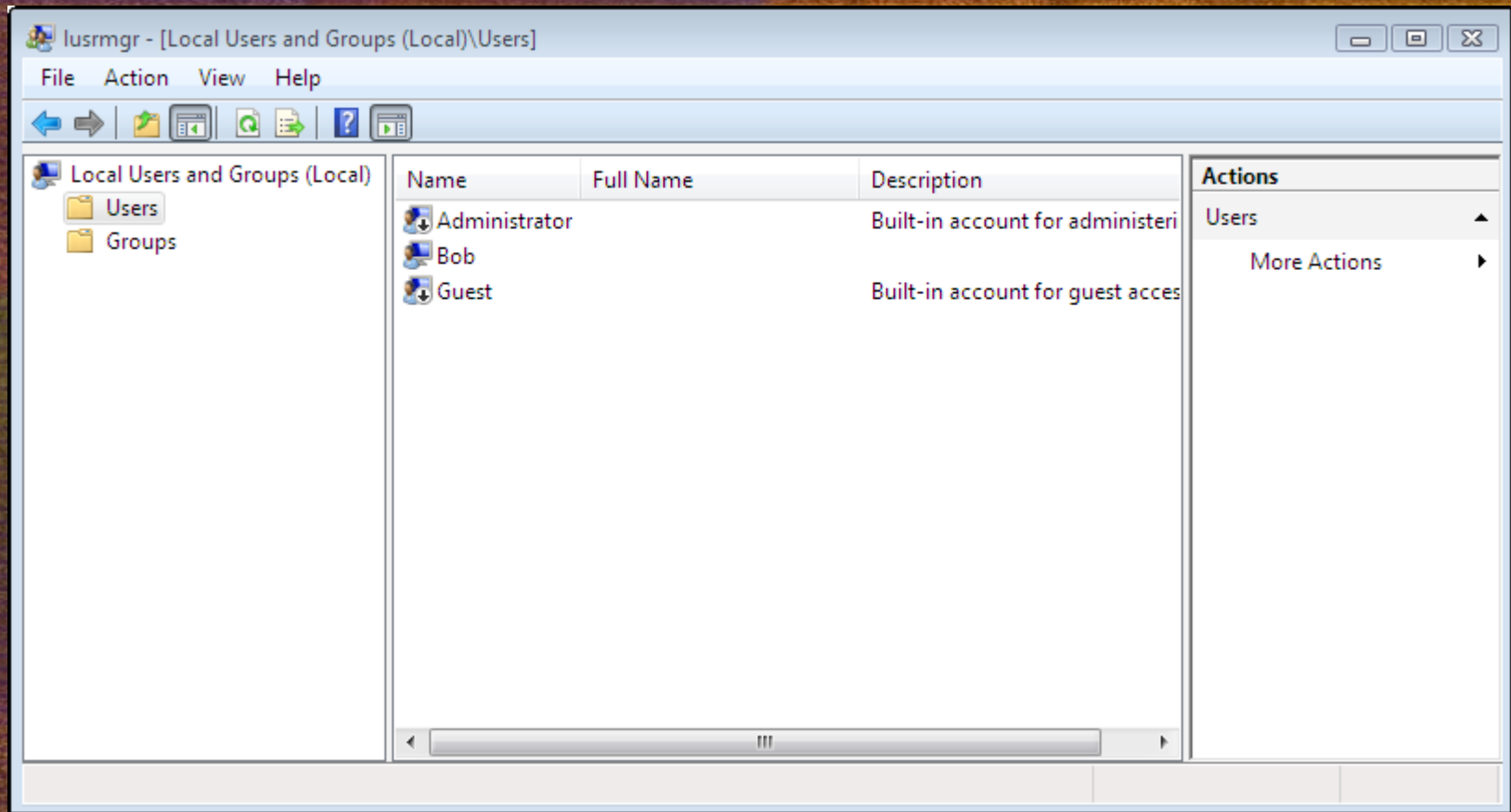
Administrator Account



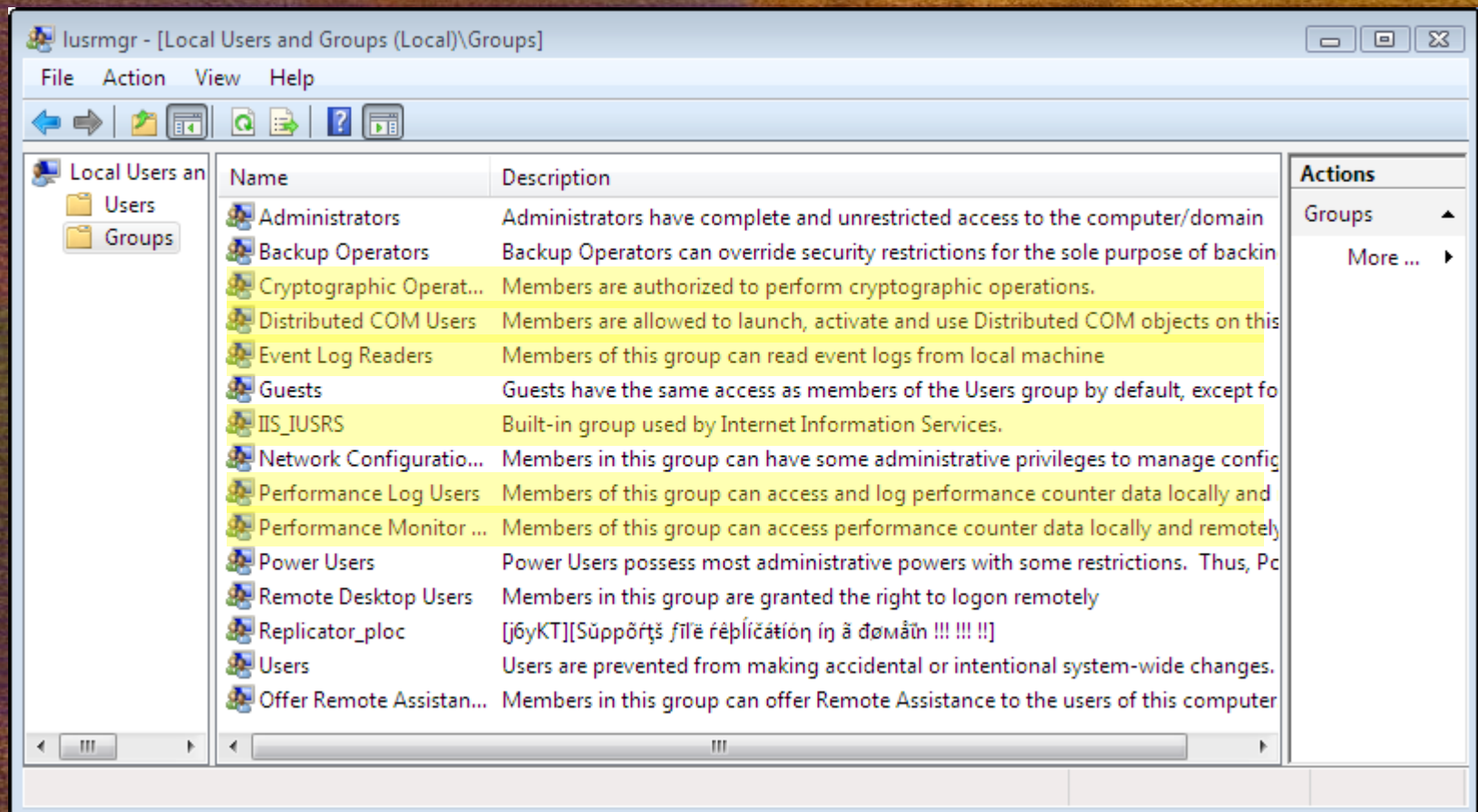
The screenshot shows the Windows Computer Management console. The left-hand navigation pane is expanded to 'Local Users and Groups' > 'Users'. The main pane displays a table of user accounts.

Name	Full Name	Description
Administrator		Built-in account for administering the c...
ASPNET	ASP.NET Machine Account	Account used for running the ASP.NE...
Guest		Built-in account for guest access to th...
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Remote Assista...
SUPPORT_388945a0	CN=Microsoft Corporation,...	This is a vendor's account for the Hel...

Administrator Account



New Groups



Suite-B Crypto

Software and Smart Card Key Storage Providers

Cryptographic configuration

NIST ECC Prime Curves support (smart cards too)

AES

SHA-2

IPSec support for AES and ECDH

ECC cipher suites in SSL

EFS with smart cards

New Auditing

Registry value change audit events

AD change audit events

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)

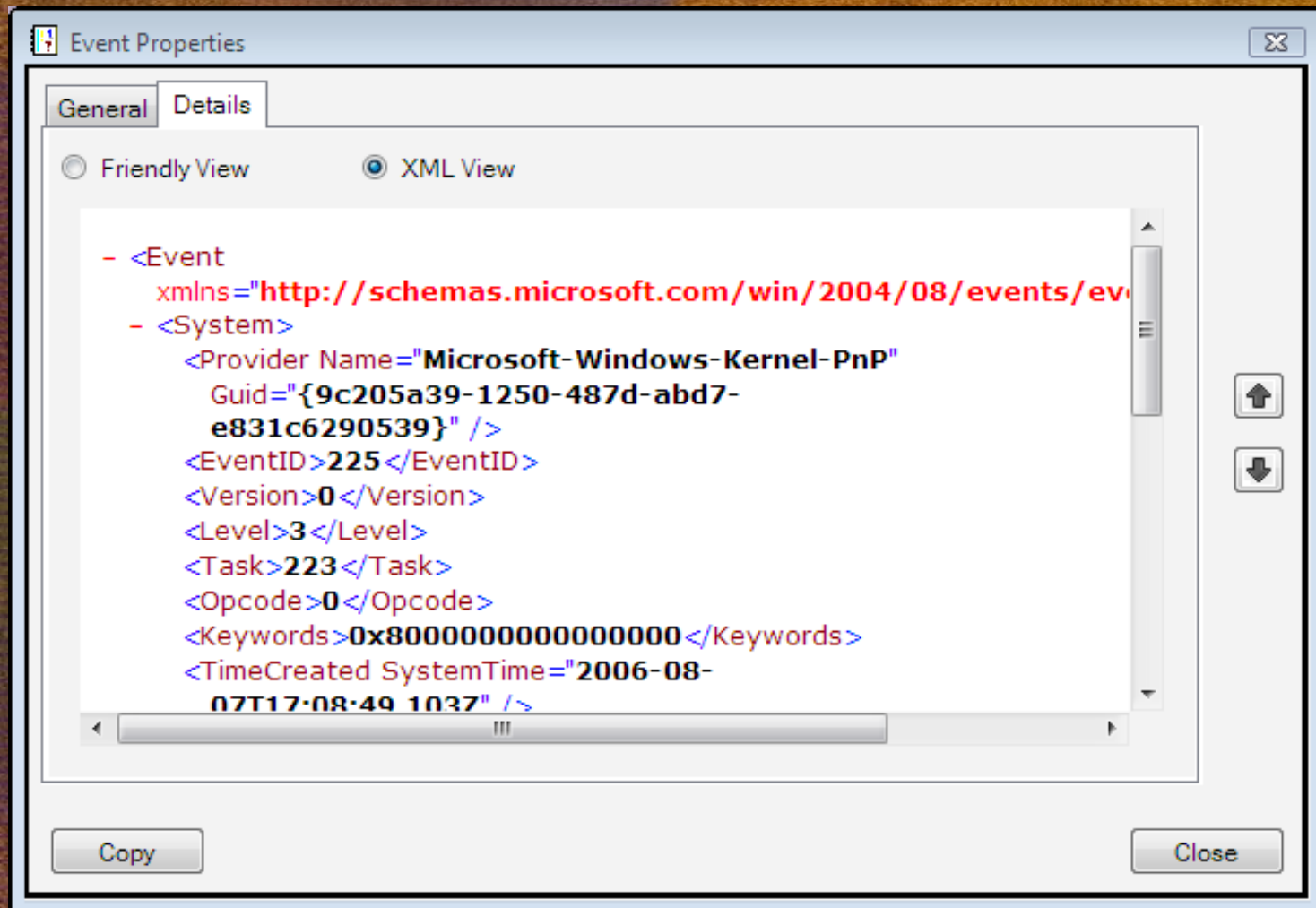
IAS (RADIUS) audit events (server only)

Event Log Changes

The screenshot shows the 'Event Properties' dialog box with the 'Details' tab selected. The main text area contains the following message: 'The process \\Device\\HarddiskVolume12\\off\\FILES\\SETUP\\OSE.EXE with process id 5824 vetoed the removal or ejection of the device USB\\VID_0DBF&PID_0300\\2B04010B04844913.' Below this, a metadata table provides details about the event. On the right side of the dialog, there are two arrow buttons (up and down) and a 'Close' button at the bottom right. A 'Copy' button is located at the bottom left.

Log Name:	System	Logged:	8/7/2006 12:08:49 PM
Source:	Kernel-PnP	Task Category:	(223)
Event ID:	225	Keywords:	
Level:	Warning	Computer:	BOBMCCOY02.northameric
User:	SYSTEM		
OpCode:	Info		
More Information:	Event Log Online Help		

Event Log Changes



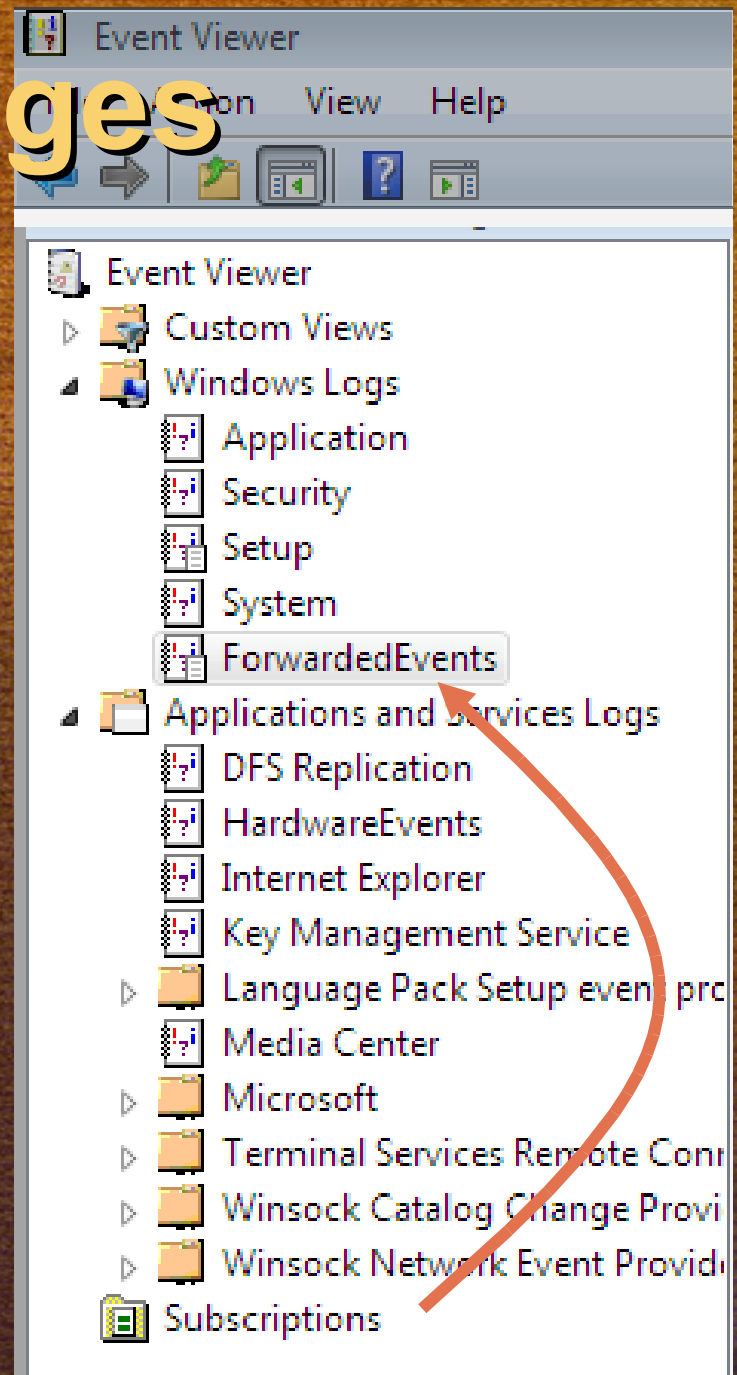
Event Log Changes

Event Forwarding

Set up the service and firewall (Quick Config) on sender

Add receiver to sender's Local Admins

Set up subscriptions on receiver



User Rights & Privileges

All rights for Power Users removed

Create global objects does not have
INTERACTIVE

SE_IMPERSONATE has added
IIS_IUSRS and removed ASPNET

Logon as a service is now empty by
default

New Privileges

Access credential manager as a trusted caller

Change time zone

Create symbolic links

Modify an object label

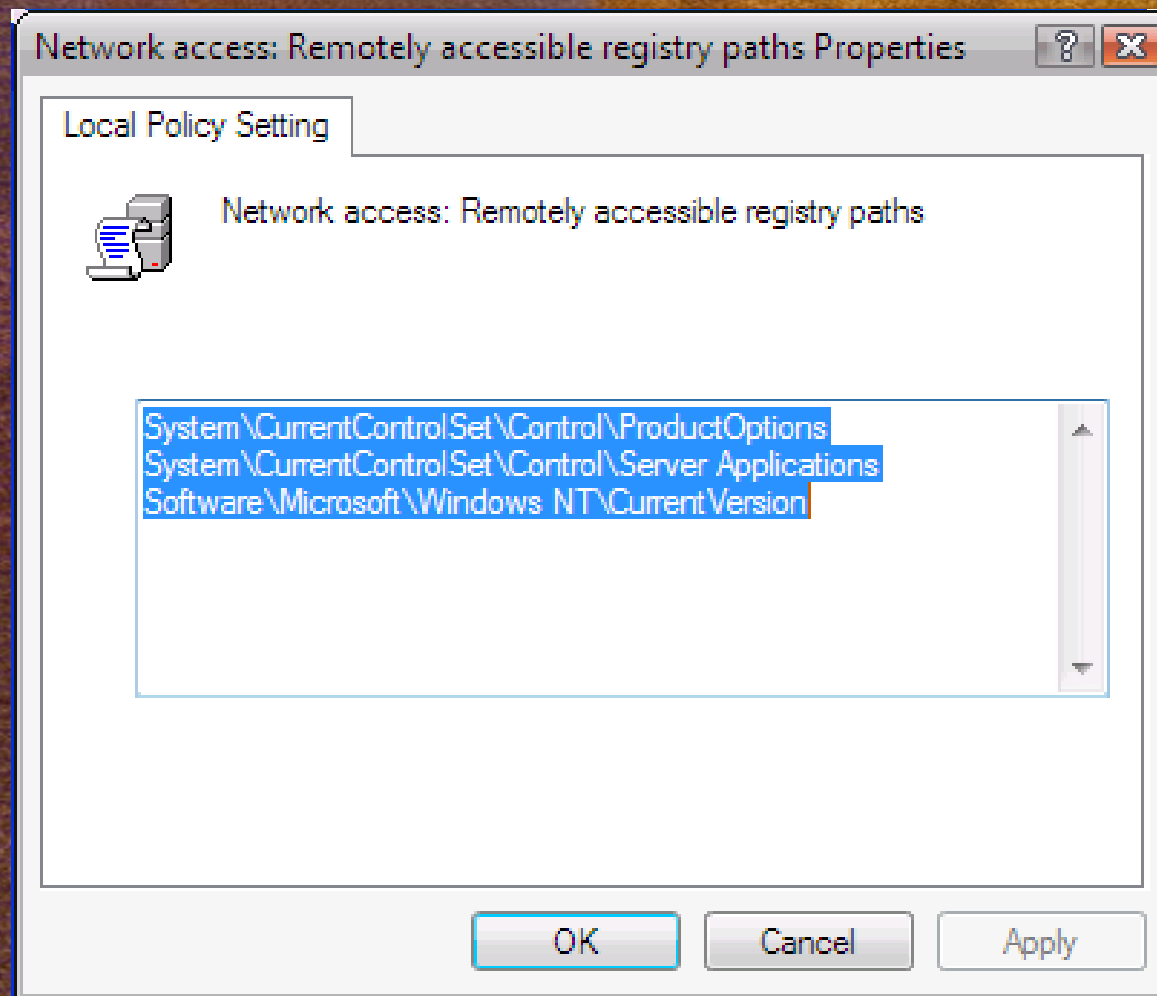
Synchronize directory service data

Increase a process working set

Security Options with Modified Defaults

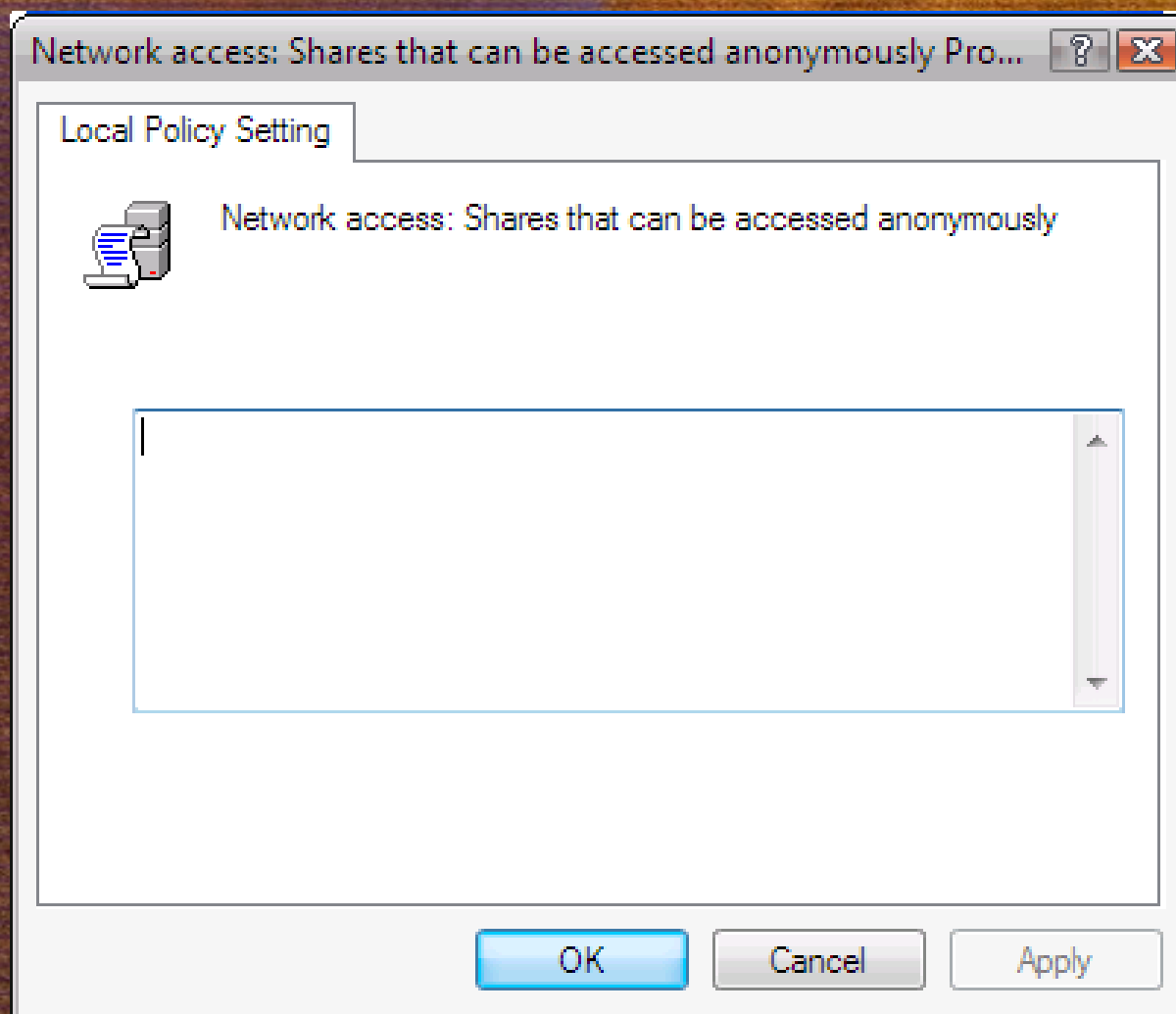
Network Access

Remotely Accessible Registry Paths



Network Access

Shares That Can Be Accessed Anonymously



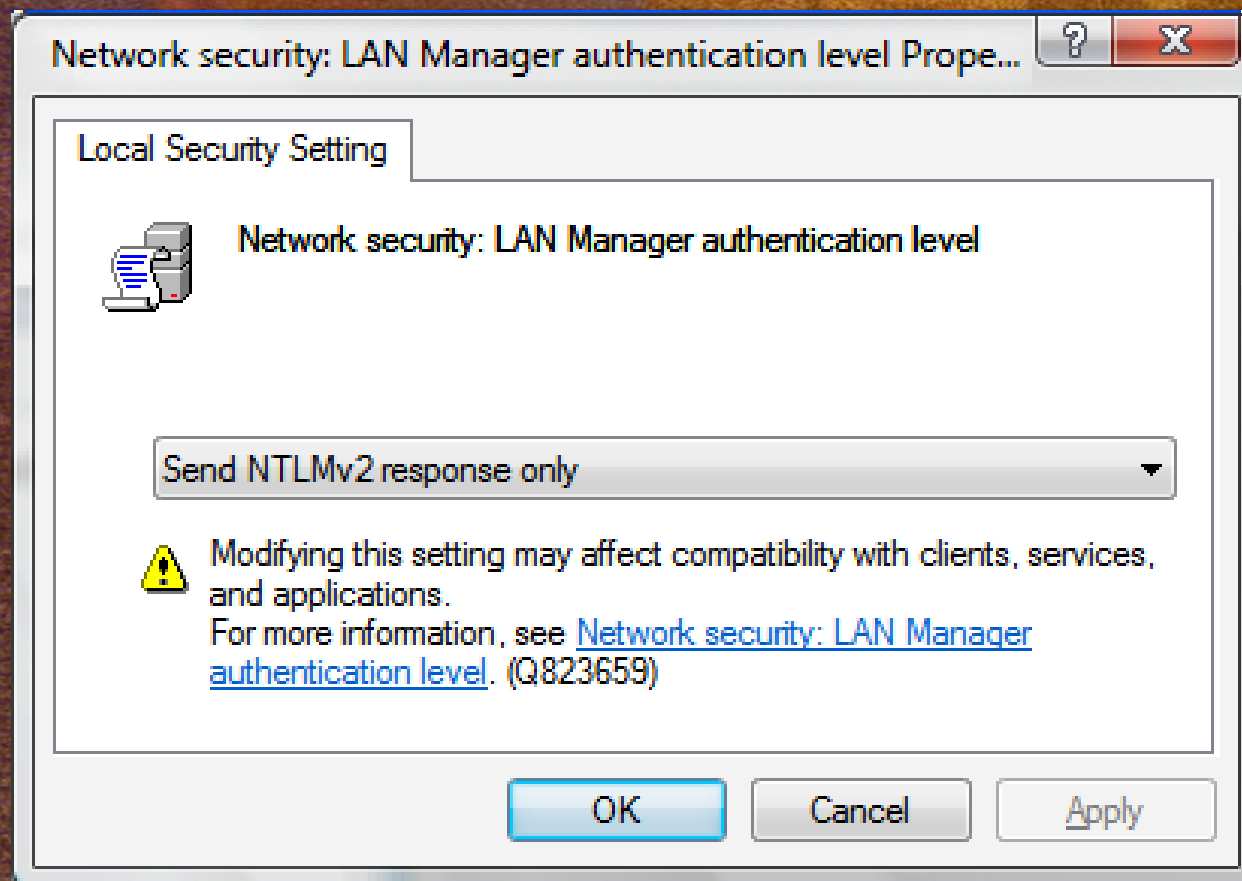
Network Security

Do Not Store LAN Manager Hash Value on Next Password Change



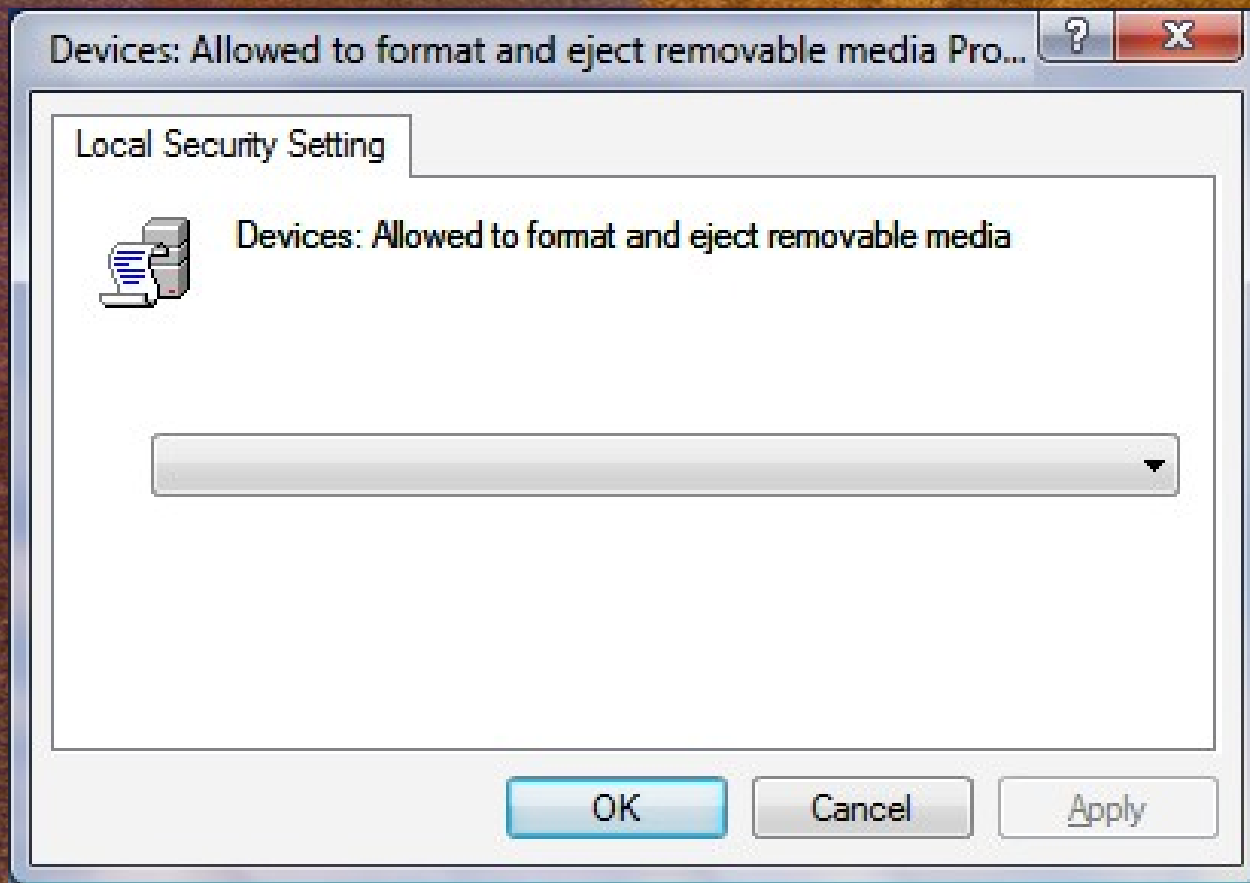
Network Security

LAN Manager Authentication Level



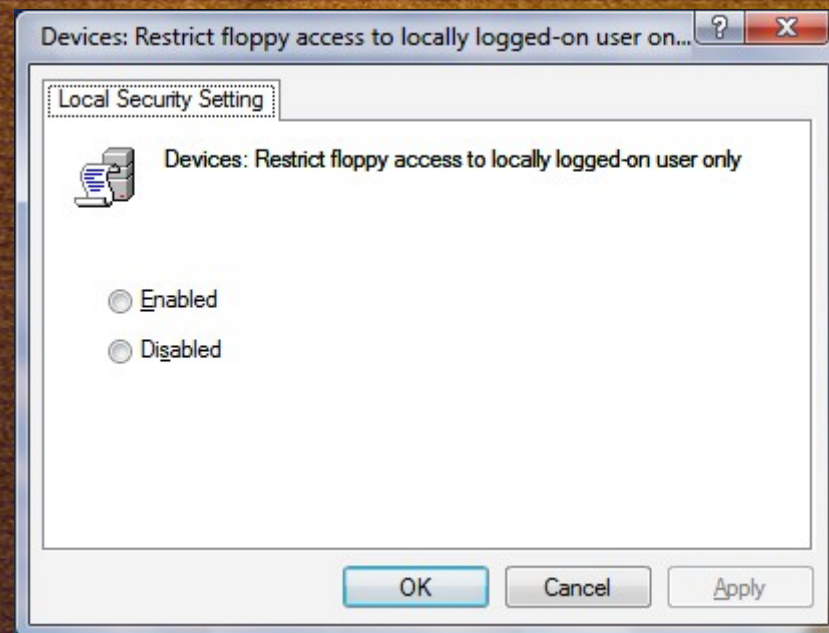
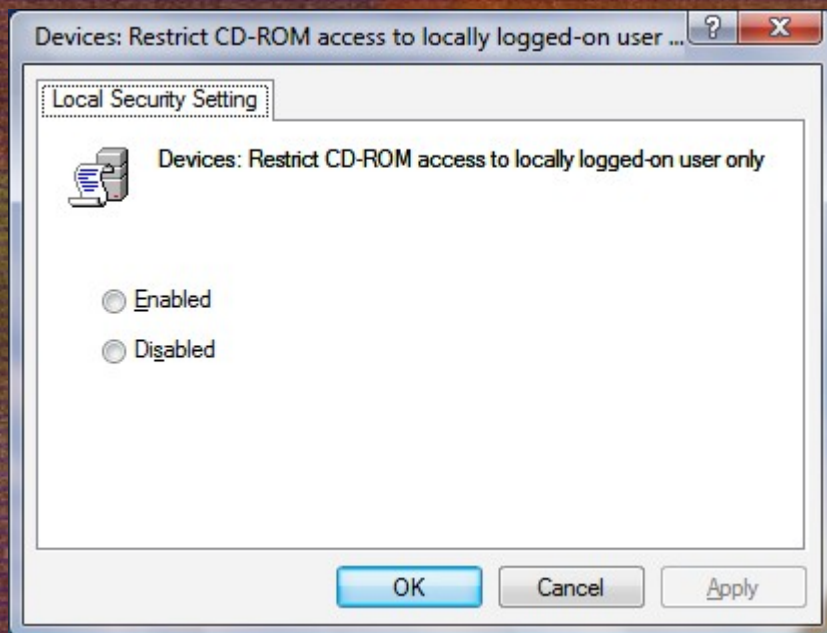
Devices

Allowed to format and eject removable media

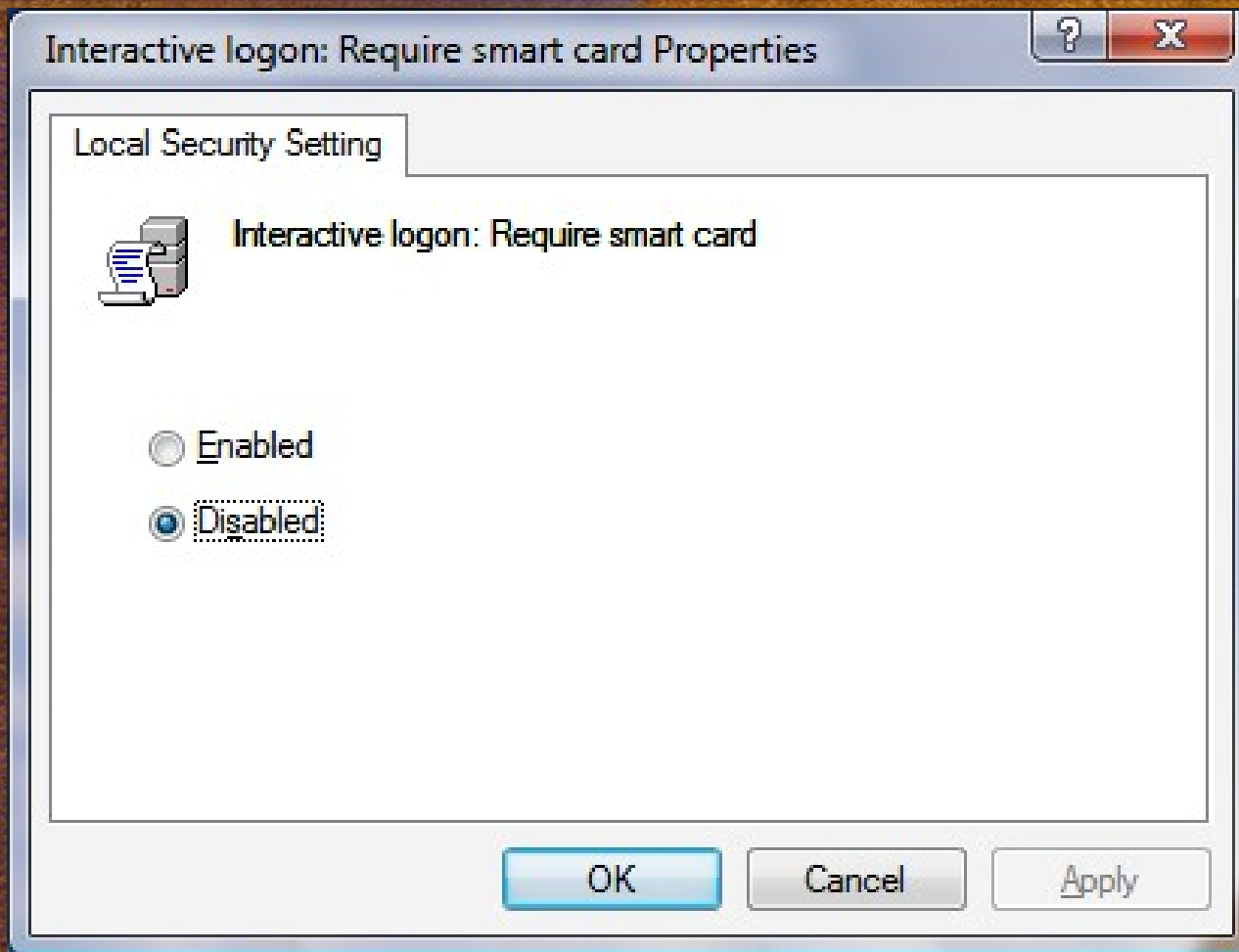


Devices

Restrict CD-ROM/Floppy Access to Locally Logged On User Only



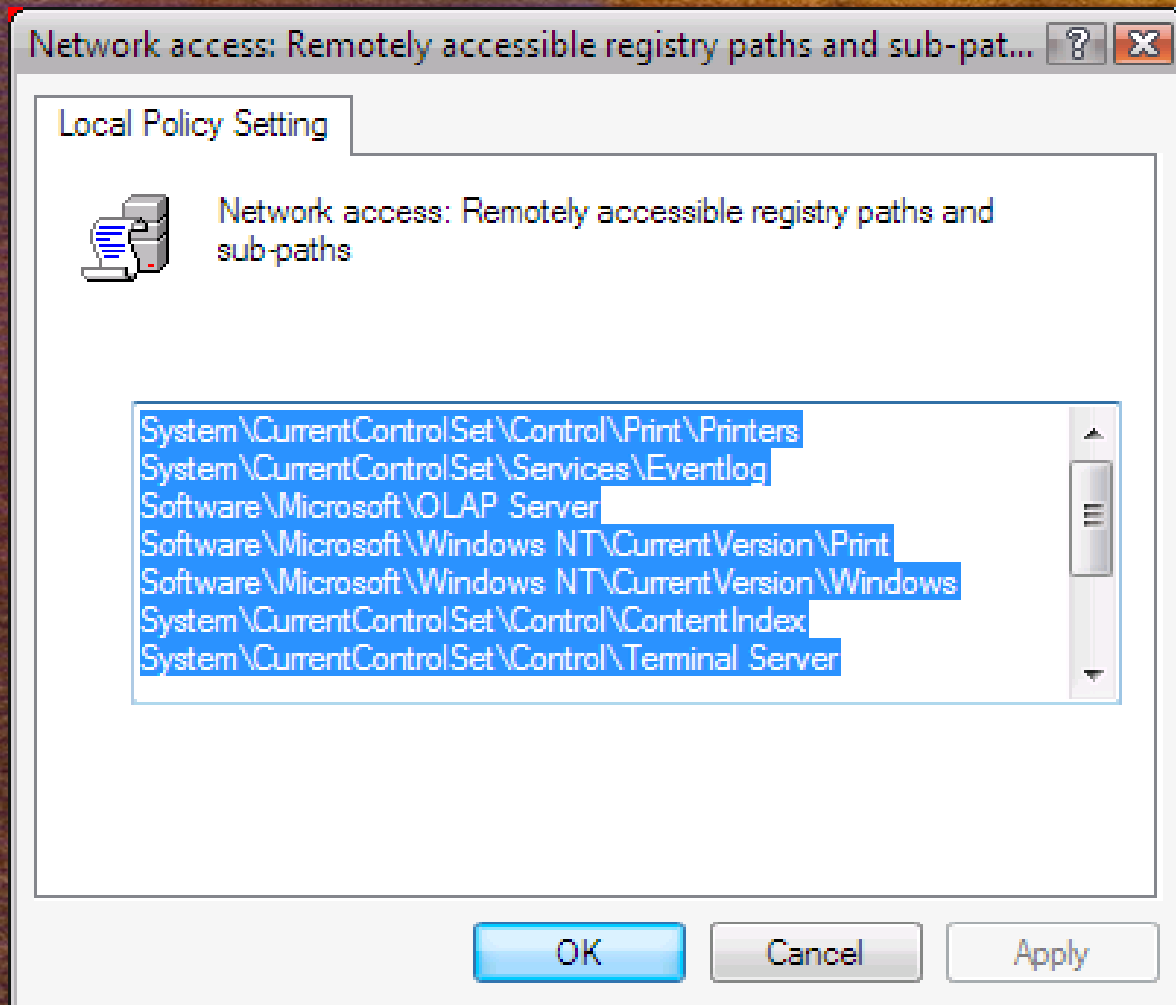
Interactive Logon Require Smart Card



New Security Options

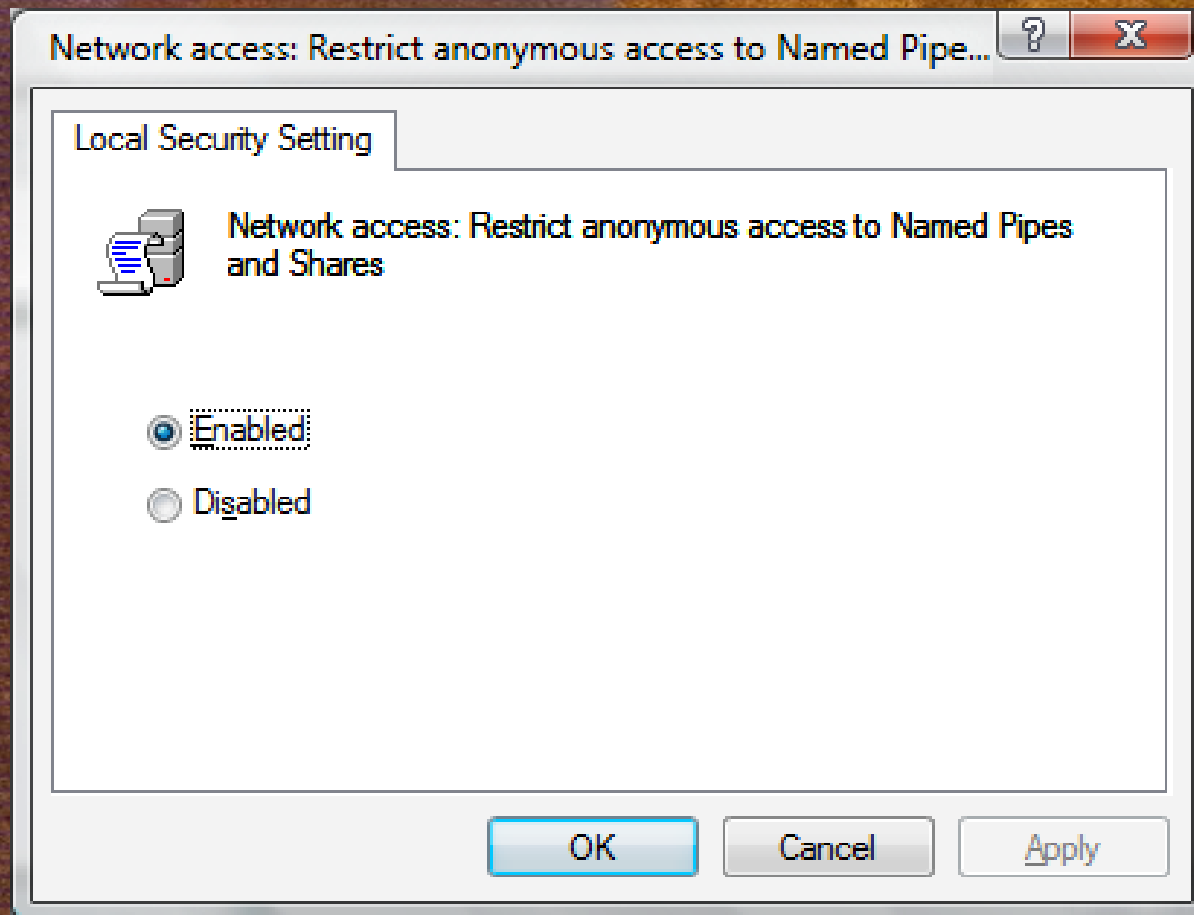
Network Access

Remotely Accessible Registry Paths and Sub-Paths



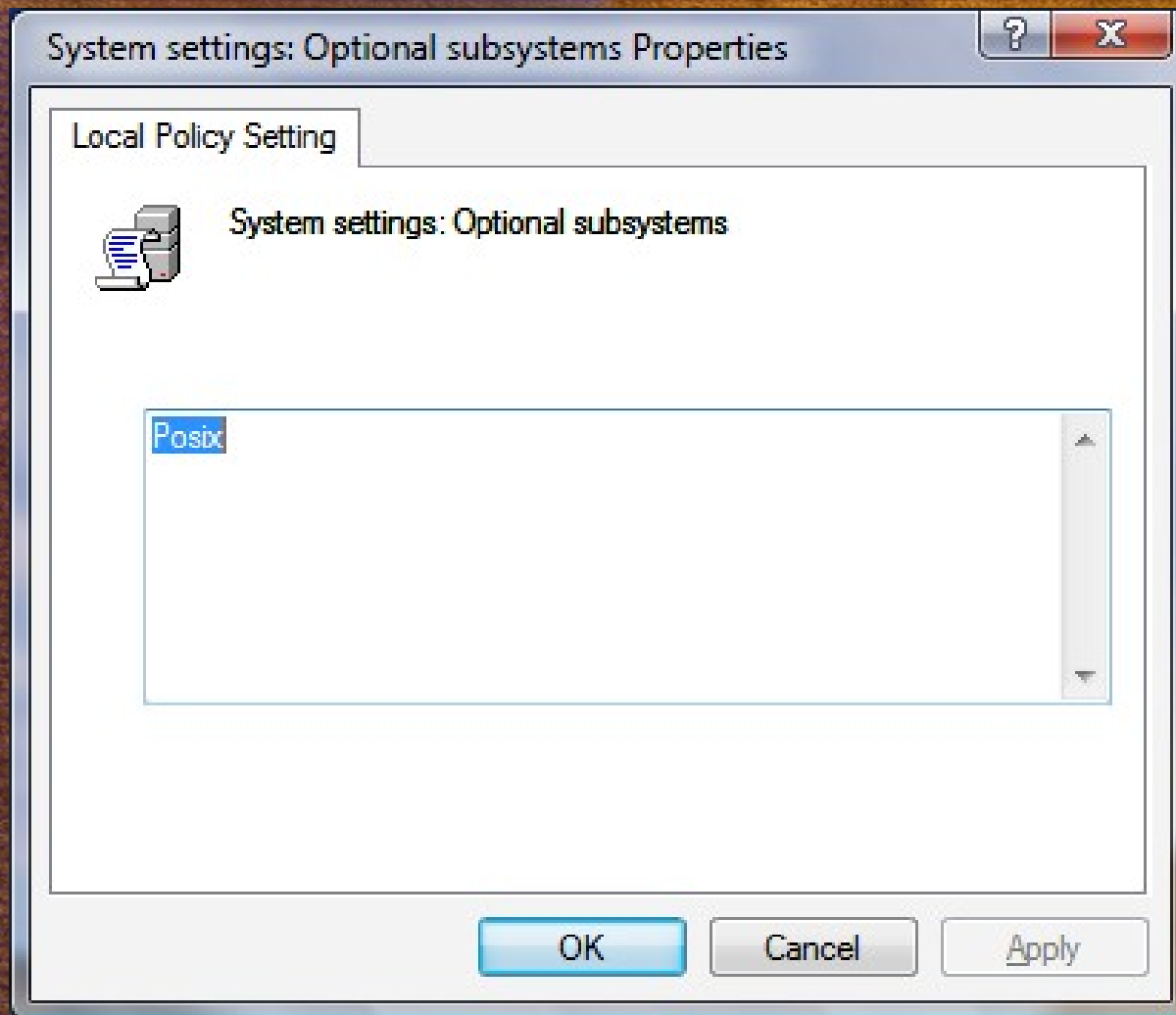
Network Access

Restrict Anonymous Access to Named Pipes and Shares



System Settings

Optional subsystems



Firewall Changes Overview

Outbound filtering

Filtering based on SIDs

Better management UI

5-tuple configuration

Local address, remote address, local port,
remote port, protocol

Integration with IPSec

Three profiles

Domain, now authenticates to the DCs

Private

Public

Interface type support

Per-user rules

Overview



For your security, some settings are controlled by Group Policy

Domain Profile

- ✓ Windows Firewall is on.
- ✓ Inbound connections that do not match a rule are allowed.
- ✓ Outbound connections that do not match a rule are allowed.

Private Profile

- ✓ Windows Firewall is on.
- ✗ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Public Profile

- ✓ Windows Firewall is on.
- ✗ All inbound connections are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

[Windows Firewall Properties](#)

Getting Started

Authenticate communications between computers

Specify how and when connections between computers are authenticated using Internet Protocol Security (IPsec). After specifying how to protect connections you wish to allow.

[Connection Security Rules](#)

View and create firewall rules

Create rules to allow or block connections to specify criteria such as whether the connection is authorized. If a connection does not match a specified rule, the default behavior applies.

[Inbound Rules](#)

[Outbound Rules](#)

Domain Profile

- ✓ Windows Firewall is on.
- ✓ Inbound connections that do not match a rule are allowed.
- ✓ Outbound connections that do not match a rule are allowed.

Private Profile

- ✓ Windows Firewall is on.
- ✗ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Public Profile

- ✓ Windows Firewall is on.
- ✗ All inbound connections are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

SMB v2

Only 16 commands (80 in SMB v1)

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

BitLocker

The Threats

Computer is lost or stolen

Theft or compromise of data

Attack against corporate network

Damage to OS if attacker installs alternate OS

Difficult and time-consuming to truly erase decommissioned disks

Existing ways to mitigate these threats are too easy for user to circumvent

Secure Startup

<i>Ensure boot integrity</i>	Resilient against attack	Protect system from offline software-based attacks
	Lock tampered systems	Prevent boot if monitored files have been altered
<i>Protect data when offline</i>	Encrypt user data and system files	All data on the volume is encrypted: user, system, page, hibernation, temp, crash dump
	Umbrella protection	Third-party apps benefit when installed on encrypted volume
<i>Ease equipment recycling</i>	Simplify recycling	Render data useless by deleting TPM key store
	Speed data deletion	Erasing takes seconds, not hours

Requires TPM 1.2 Chip

Microcontroller affixed to motherboard

Stores keys, passwords, digital certificates

For BitLocker, TPM stores volume encryption key

Key released only when system boots normally; compares each boot process against previously stored measurements

Any changes made to encrypted volume renders key irretrievable

No user interaction or visibility

Keys can be archived in Active Directory for the inevitable “Oh shoot!” moment

Prohibits use of software debuggers during boot

Won't EFS Protect Me?

Not quite – it's good for those who know what they're doing

Users often store data on the desktop – is it EFSed?

EFS doesn't protect the operating system

EFS is very strong against attacks

Four levels of key protection

Properly configured, EFS is computationally infeasible to crack

Continuum of Protection

	BitLocker	EFS	RMS
Laptops			
Branch office servers			
Local single user file protection (Windows partition only)			
Local multi-user file protection			
Remote file protection			
Untrusted administrator			
Remote document policy enforcement			

OS Co-Existence

BitLocker encrypts Windows *partition* only

You won't be able to dual-boot another OS on the same partition

OSes on other partitions will work fine

Attempts to modify the protected Windows partition will render it unbootable

Replacing MBR

Modifying even a single bit

Enabling BitLocker

Create a 1.5GB active partition

This becomes your “system” partition – where OS boots

The TPM boot manager uses only 50MB

Windows runs from on your “boot” partition—where the system lives

Enable TPM chip – usually in system BIOS

Enable BitLocker in Security Center

Update hard disk MBR

Encrypt Windows “boot” partition

Generate symmetric encryption key

Store key in TPM

Encryption begins after reboot

Doesn't Stop Everything

Hardware debuggers

Online attacks – BitLocker is concerned only with the system's startup process

Post logon attacks

Sabotage by administrators

Poor security maintenance

BitLocker Deployment

Requires hardware and software upgrades

Phase in, start with high priority computers

Mostly a feature for laptops

Also consider for desktop computers in insecure environments (factory floor, kiosk, ...)

Enterprise key management

Hardware lifecycle management

Microsoft®

© 2002 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.