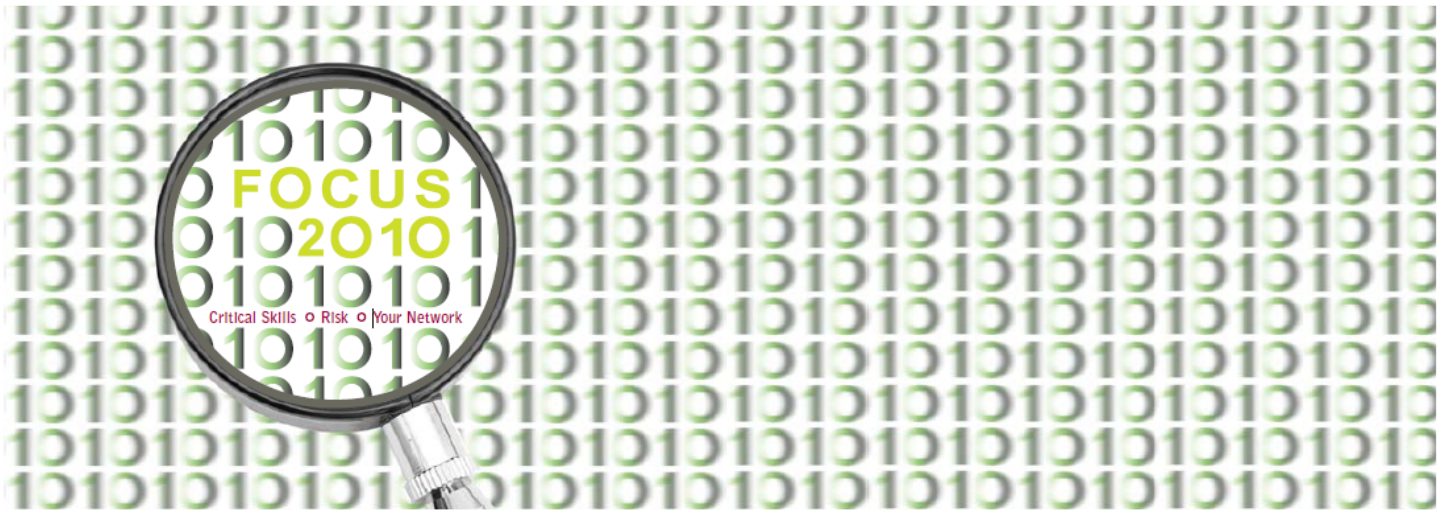


10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



# T21: Microsoft Windows Server and Client Security

Donald E. Hester, Maze Associates

# Microsoft Windows Server and Client Security

Windows 7, Vista and Server 2008 R2



Donald E. Hester

CISSP, CISA, CAP, MCT, MCITP, MCTS, MCSE Security, Security+, CTT+  
Maze & Associates

University of San Francisco / San Diego City College



[www.LearnSecurity.org](http://www.LearnSecurity.org)



<http://www.linkedin.com/in/donaldehester>



<http://www.facebook.com/group.php?gid=245570977486>



[LearnSecurity.org](http://www.LearnSecurity.org)



**Updates** Manageability  
It manages, implements, updates and never takes a sick day.

Meet IT 24-7  
Watch more videos of the ultimate server unleashed.

Web  
Serving up better, faster, more secure experiences.

Copy Box  
Let's get enough robots? thought so.

- For updates to this slide deck and other slide decks please see:
- <http://www.learnsecurity.org/>

San Francisco Chapter

**Windows 7**

**ISACA**  
Trust in, and value from, information systems  
San Francisco Chapter

**FOCUS**  
Critical Skills • Risk • Your Network

## Windows 7

- AppLocker
- BitLocker
- Direct Access
- User Account Control
- Windows Filtering Platform (WFP)
- Biometrics Support
- SmartCard Support
- System Restore
- Windows Defender
- DNSSEC Support
- Action Center



## Windows 7 Goals

- Fundamentally Secure Platform
  - Windows Vista Foundation
  - Streamlined UAC
  - Enhanced Auditing
- Protect Users & Infrastructure
- Secure Anywhere access
- Protect Data for Unauthorized Viewing



## Windows 7 Goals

- Fundamentally Secure Platform
- Protect Users & Infrastructure
  - AppLocker
  - Internet Explorer 8
  - Data Recovery
- Secure Anywhere access
- Protect Data for Unauthorized Viewing



## Windows 7 Goals

- Fundamentally Secure Platform
- Protect Users & Infrastructure
- Secure Anywhere access
  - Network Security
    - DNSSEC
    - Multi-home Firewall Profiles
    - Policy based network segmentation
  - Network Access Protection
  - DirectAccess
- Protect Data for Unauthorized Viewing



## Windows 7 Goals

- Fundamentally Secure Platform
- Protect Users & Infrastructure
- Secure Anywhere access
- Protect Data for Unauthorized Viewing
  - RMS
  - EFS
  - BitLocker
  - BitLocker to Go



## Windows 7 UAC

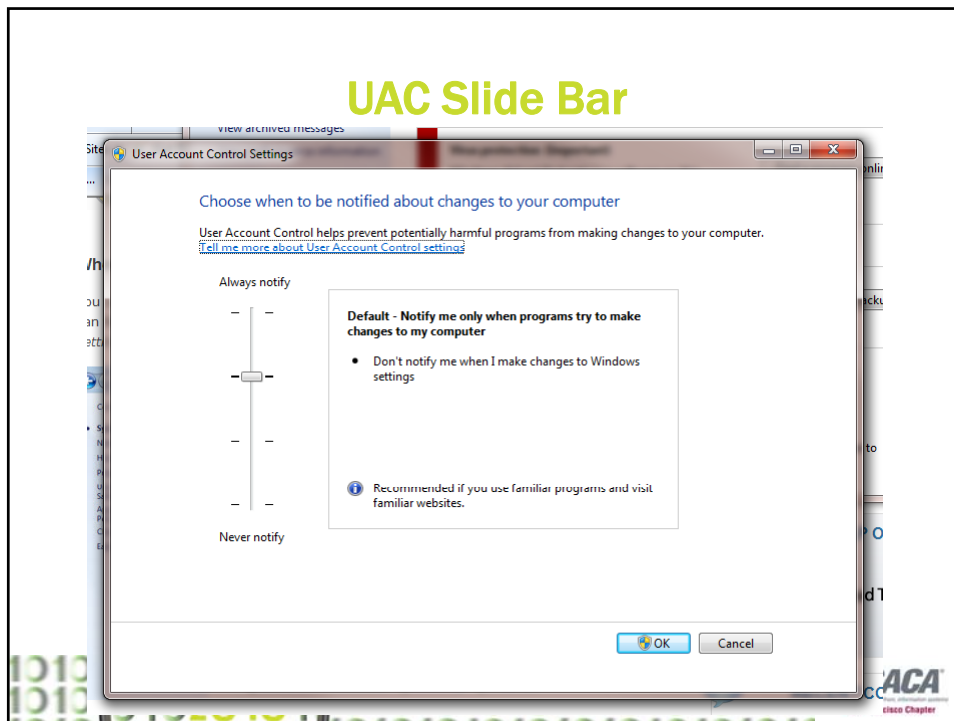
- 29% fewer user account control (UAC) prompts than Windows Vista has, and
- fewer prompts in general
- "We've put users in control and allowed them the ability to tune the level of prompting" using a slider bar
  - Paul Cooke, director of Windows Client Enterprise Security



## User Account Control Levels

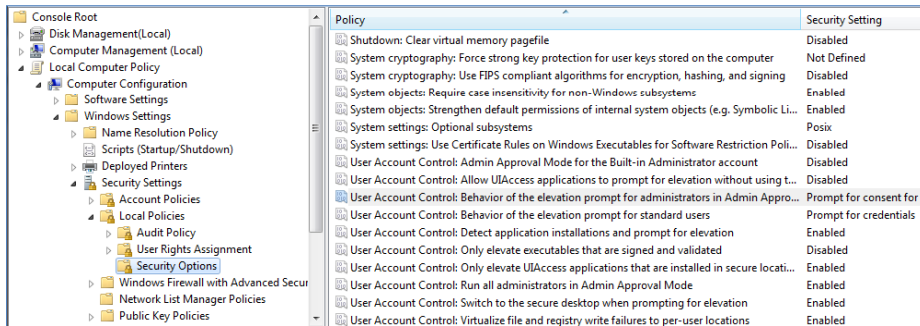
- High: Vista equivalent
  - Prompts for: all elevations
  - Prompts on: secure desktop
- Medium: default
  - Prompts for: non-Windows elevations
    - Windows means:
      - Signed by Windows certificate
      - In secure location
      - Doesn't accept control command-line (e.g. cmd.exe)
  - Prompts on: secure desktop
- Low:
  - Prompts for: non-Windows elevations
  - Prompts on: standard desktop
    - Avoids black flash and user can interact with desktop
    - Possible appcompat issues with 3rd-party accessibility applications
- Off: UAC off
  - No Protected Mode IE
  - No file system or registry virtualization

## UAC Slide Bar





## UAC in GPO



The screenshot shows the Windows Group Policy Editor interface. The left pane displays the tree structure, with 'Local Computer Policy' expanded to 'Security Settings' > 'Security Options'. The right pane shows a list of policies with their corresponding security settings.

Policy	Security Setting
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Li...	Enabled
System settings: Optional subsystems	Posix
System settings: Use Certificate Rules on Windows Executables for Software Restriction Poli...	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using t...	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Appro...	Prompt for consent for...
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locati...	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled



## DirectAccess

- DirectAccess offers remote workers the same level of seamless and secure connectivity as they have in the office.
- The system automatically creates a secure tunnel to the corporate network and workers don't have to manually connect
- DirectAccess also allows IT administrators to patch systems whenever a remote worker is on the network





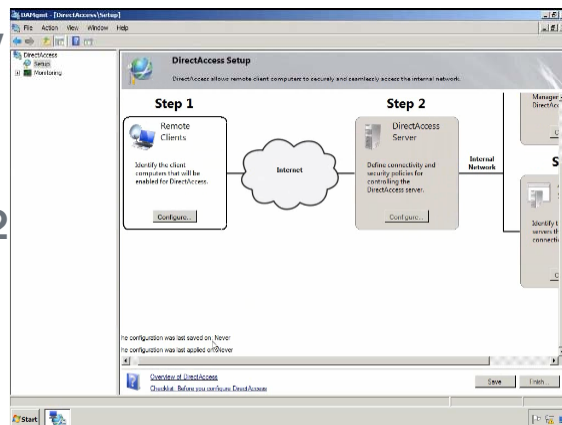
## DirectAccess

- DirectAccess also uses IPsec to authenticate the computer and user, encrypt the data crossing over the Internet
- Can even be used to require employees to authenticate with a smart card



## DirectAccess Requirements

- Active Directory
- PKI Certificates
- IPv6
- Server 2008 R2
- Windows 7





## BitLocker

- Windows Vista users have to repartition their hard drive to create the required hidden boot partition, but Windows 7 creates that partition automatically when BitLocker is enabled
- Windows 7 extends the Data Recovery Agent (DRA) to include all encrypted volumes; as a result, only one encryption key is needed on any BitLocker-encrypted Windows machine



## BitLocker-to-Go

- BitLocker To Go extends the data encryption features to removable storage devices like USB thumb drives and flash drives
- A password or a smart card with a digital certificate stored on it can be used to unlock the data
- The devices can be used on any other Windows 7 machine (password needed)
- XP and Vista machines, the data read but not modified





## BitLocker w/ SmartCard

- BitLocker to Go SmartCard access
- A user can insert a card into a smart-card reader built into a laptop and either enter a personal identification number or use a fingerprint to access the data
- Not for use with System Volume

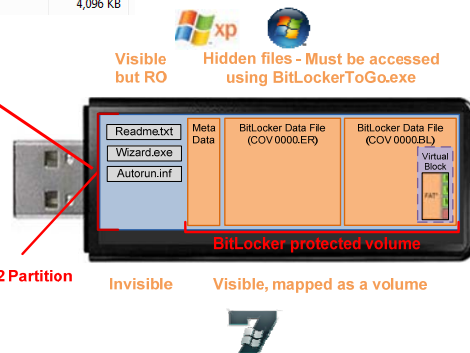


## BitLocker-to-Go Format

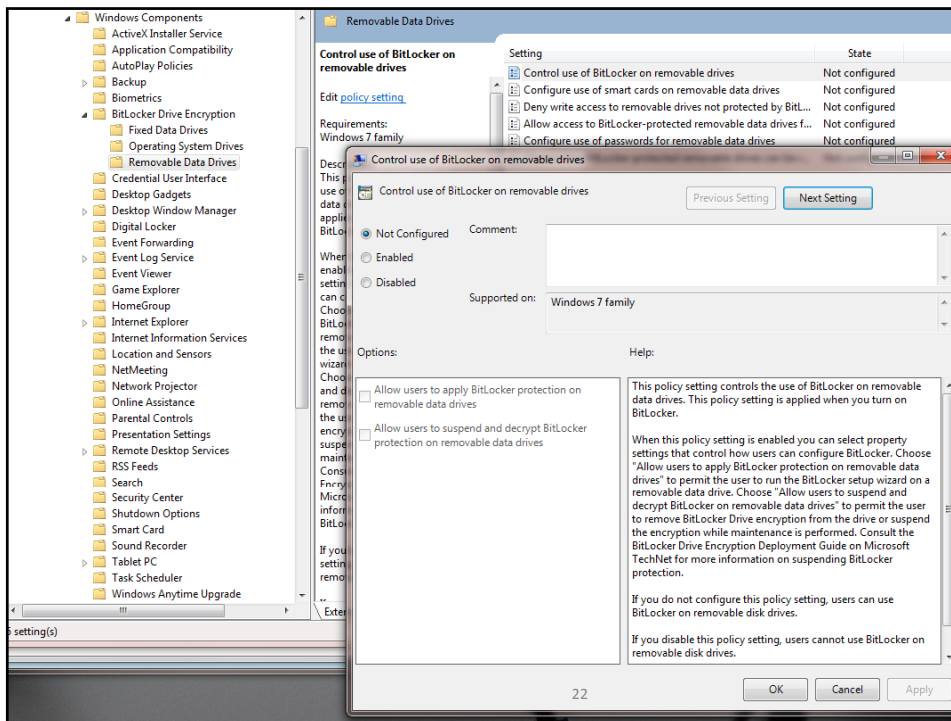


Name	Date modified	Type	Size
autorun.inf	10/15/2008 8:12 AM	Setup Information	1 KB
BitLockerToGo.exe	12/12/2008 8:59 PM	Application	167 KB
COV 0000.BL	1/24/2009 12:14 PM	System File	32 KB
COV 0000.ER	1/24/2009 12:14 PM	System File	4,001,952 KB
en-US_BitLockerToGo.exe.mui	12/13/2008 7:32 AM	MUI File	8 KB
PAD 0000.NG	1/24/2009 12:14 PM	System File	0 KB
PAD 0000.PD	1/24/2009 12:14 PM	System File	4,096 KB

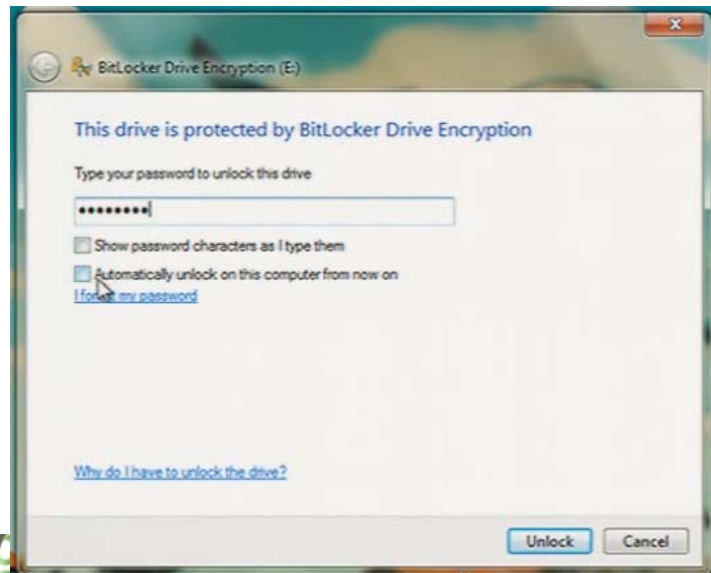
View on Down-Level System



## Prevent unencrypted use



## BitLocker to Go



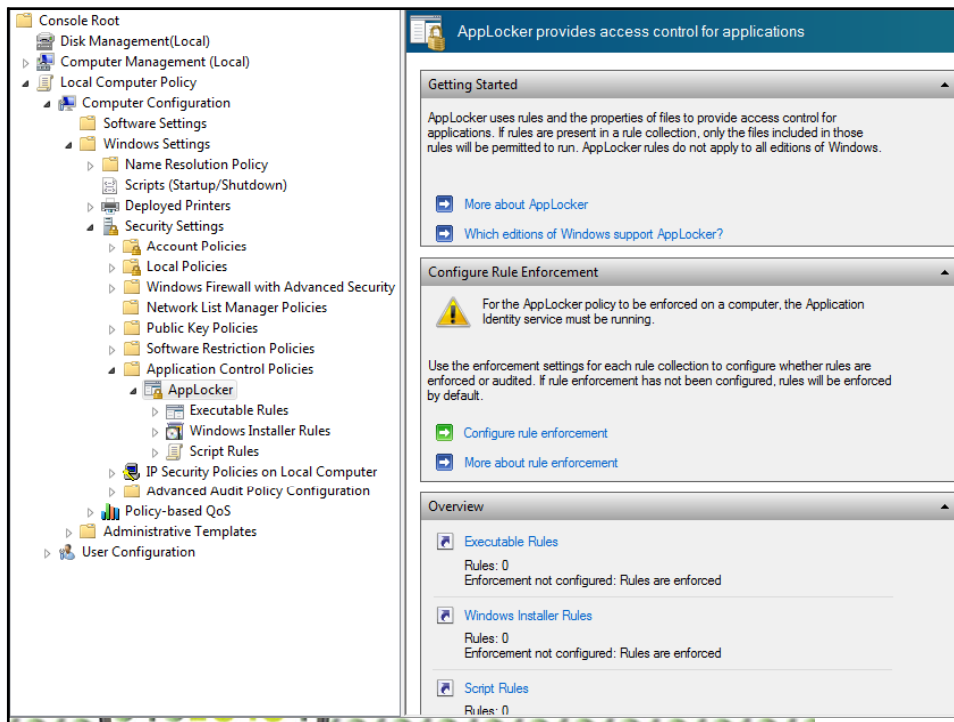
**ISACA**  
San Francisco Chapter

## AppLocker

- AppLocker technology that allows administrators to control the software that runs on Windows 7 machines
- This ensures that only authorized scripts, installers, and dynamic load libraries are accessed
- It can also be used to keep unlicensed software off machines

**FOCUS**

**ISACA**  
San Francisco Chapter



## Windows Filtering Platform (WFP)

- group of APIs and system services that allow third party vendors to tap further into Windows' native firewall resources
- The idea is that third parties can take advantage of aspects of the Microsoft Windows Firewall in their own products. Microsoft says "third-party products also can selectively turn parts of the Windows Firewall on or off, enabling you to choose which software firewall you want to use and have it coexist with Windows Firewall



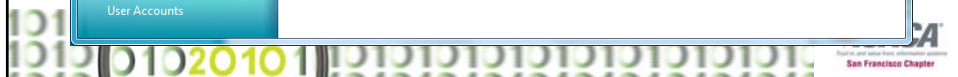
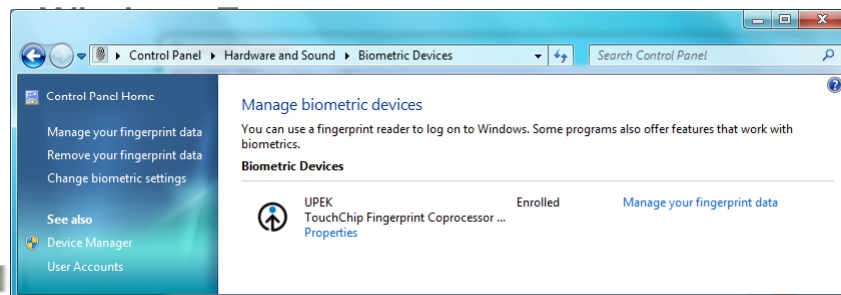
## Multiple Active Firewall Policies

- Windows 7 and WFP in particular permit multiple firewall policies, so IT professionals can maintain a single set of rules for remote clients and for clients that are physically connected to their networks
- Only one profile at a time with Vista
- Multiple profiles, each connection has its own profile
  - Connect to home network then start a VPN which policy is applied?

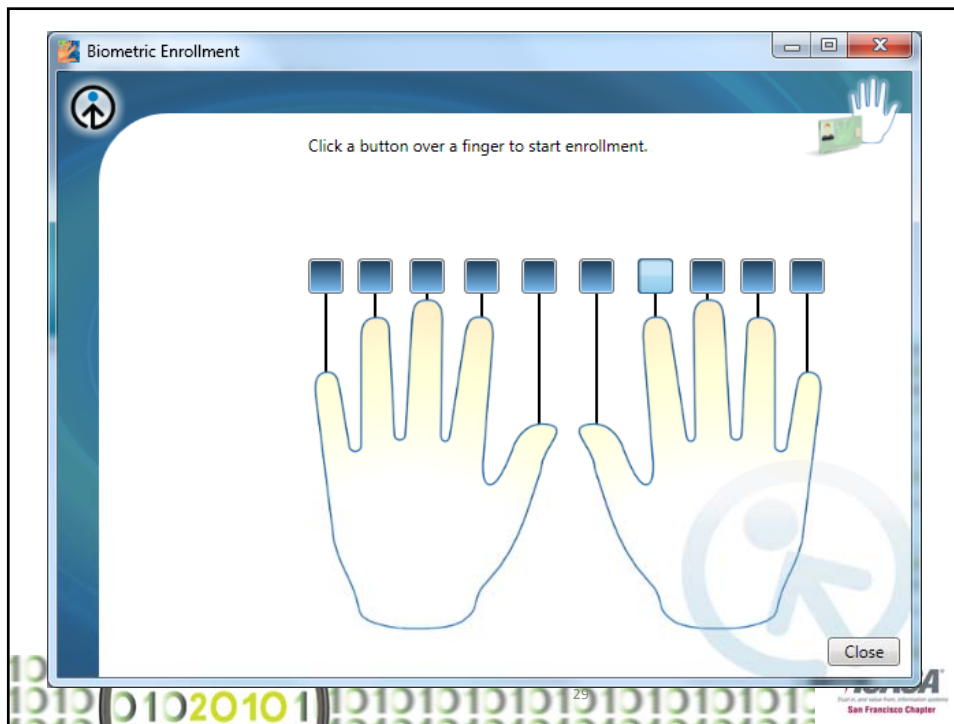


## Biometrics Support

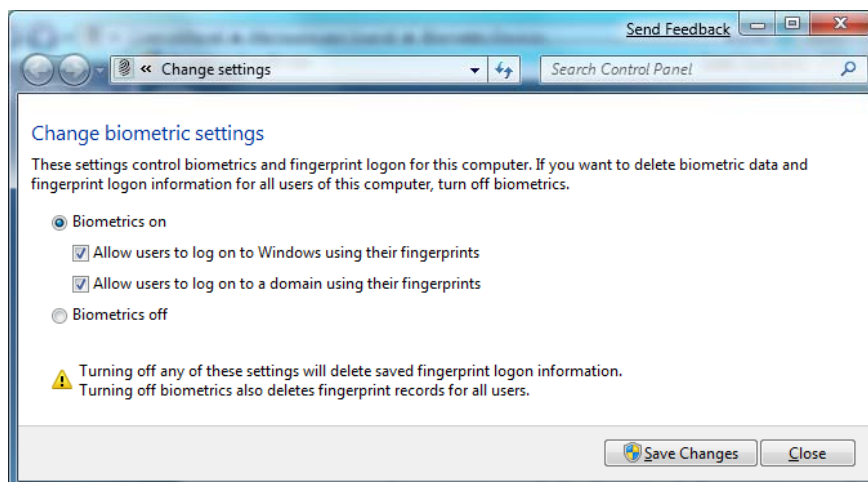
- Biometrics enhancements include easier reader configurations, allowing users to manage the fingerprint data stored on the computer and control how they log on to







## Biometric Settings



## Smart Card Support

- Windows 7 extends the smart card support offered in Windows Vista by automatically installing the drivers required to support smart cards and smart card readers, without administrative permission.



## System Restore

- System Restore includes a list of programs that will be removed or added, providing users with more information before they choose which restore point to use
- Restore points are also available in backups, providing a larger list to choose from, over a longer period of time



## System Restore

- First, System Restore displays a list of specific files that will be removed or added at each restore point.
- Second, restore points are now available in backups, giving IT professionals and others a greater list of options over a longer period of time



## BranchCache

- Microsoft recommends that users run Windows 7 clients in conjunction with Windows 2008 R2 servers in order to get the benefit of BranchCache, a caching application that makes networked applications faster and more responsive

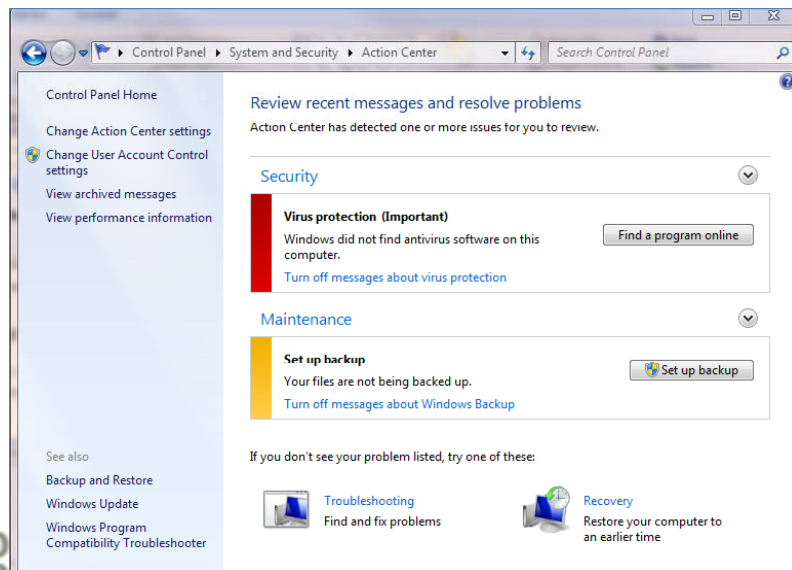


## Action Center

- Action Center includes alerts and configuration settings for several existing features, including:
  - Security Center
  - Problem, Reports, and Solutions
  - Windows Defender
  - Windows Update
  - Diagnostics
  - Network Access Protection
  - Backup and Restore
  - Recovery
  - User Account Control

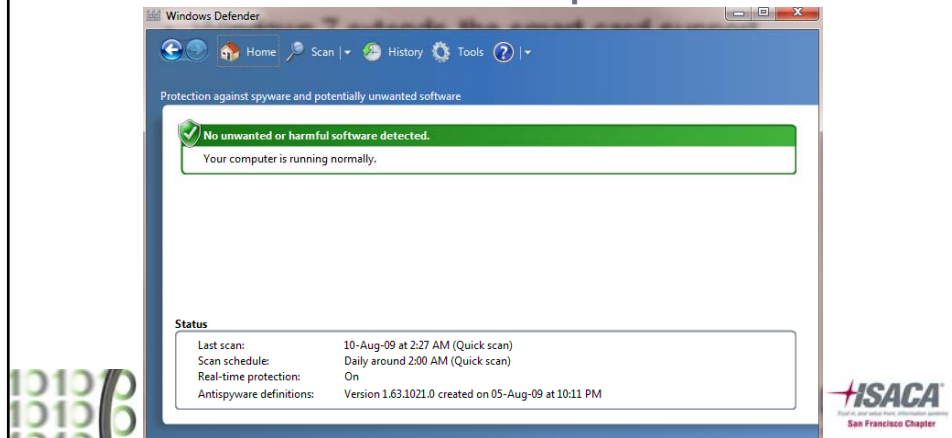


## Action Center



## Windows Defender

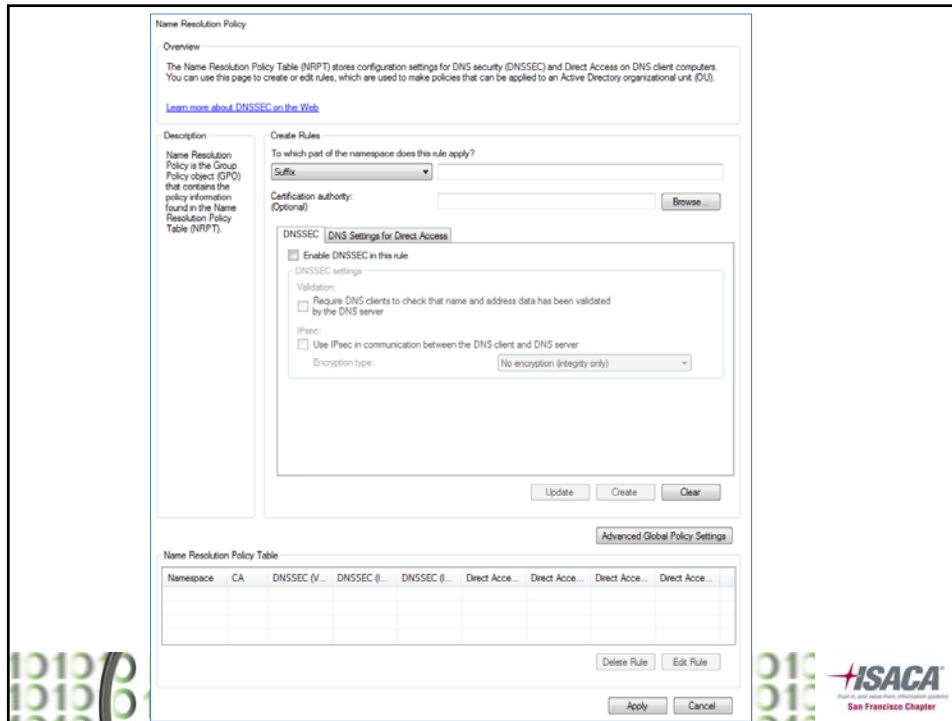
- Performance enhancement
- Removed the Software Explorer tool



## DNSSEC

- Windows 7 also supports Domain Name System Security Extensions (DNSSEC), newly established protocols that give organizations greater confidence that DNS records are not being spoofed





## Event Auditing

- Windows 7 also makes enhancements to event auditing
- Regulatory and business requirements are easier to fulfill through management of audit configurations, monitoring of changes made by specific people or groups, and more-granular reporting.
- For example, Windows 7 reports why someone was granted or denied access to specific information.



# Advanced Audit Policy Configuration

The screenshot shows the Windows Security console with the 'Advanced Audit Policy Configuration' window open. The left pane shows the navigation tree with 'Advanced Audit Policy Configuration' selected. The right pane displays the 'Getting Started' information and a table of audit categories.

**Getting Started**

Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.

[More about Advanced Audit Configuration](#)

[Which editions of windows support Advanced Audit Configuration?](#)

A summary of the settings is provided below:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured



## Vista / Windows 7

- Kernel Patch Protection
- Service Hardening
- Data Execution Prevention
- Address Space Layout Randomization
- Mandatory Integrity Levels





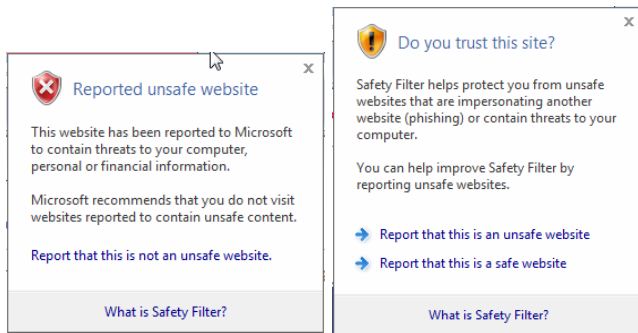
# IE 8



Internet Explorer 8 security features target three major sources of security exploits: social engineering, Web server, and browser-based vulnerabilities

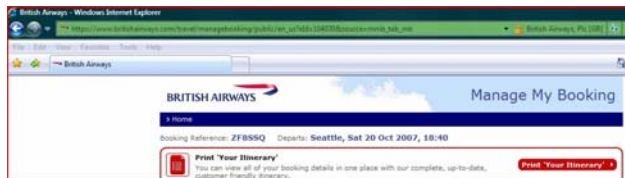


## Internet Explorer 7 Contribution to Building Trust



### Phishing Filter

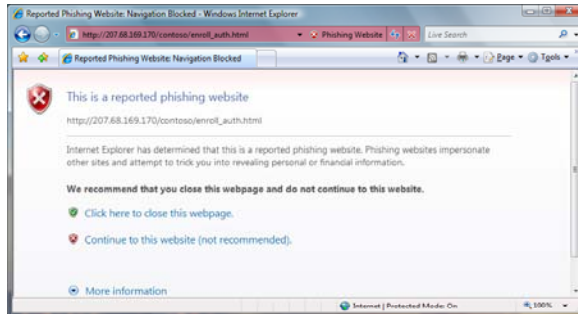
Over 1M phishing attempts blocked per week



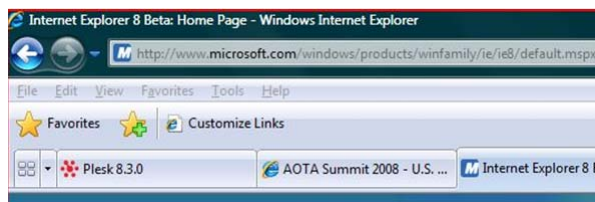
### Extended Validation Certificates

Over 5000 issued to date

## What's New in Trust in Internet Explorer 8?



**SmartScreen™**  
Expanding scope to incorporate new threats



**Domain Name Highlighting**  
Helps the user identify real domain name

## Internet Explorer 8 Management



### Group Policy (over 1300 in IE8)

- Control browser features, ex : Turn on/off Phishing Filter
- Configure browser features, ex : home page, favorites
- Enforce security settings, ex: trusted sites
- New features exposed through group policy



### Support Infrastructure

- Pay per incident support available to everyone
- Support agreements for Windows OS include support for Internet Explorer
- Professional support organization provides issue resolution

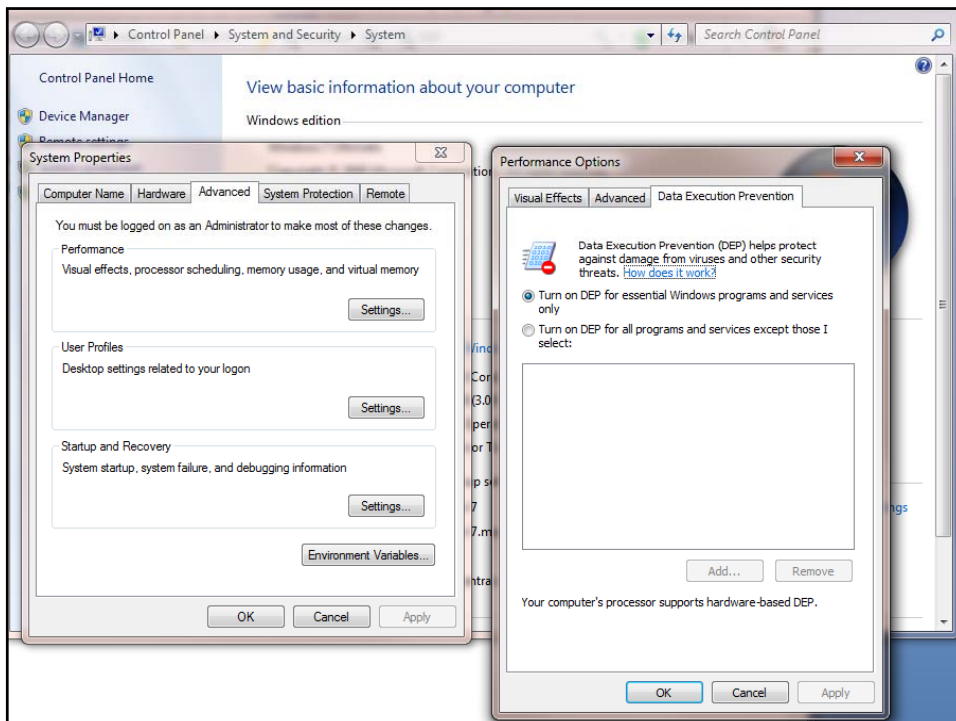
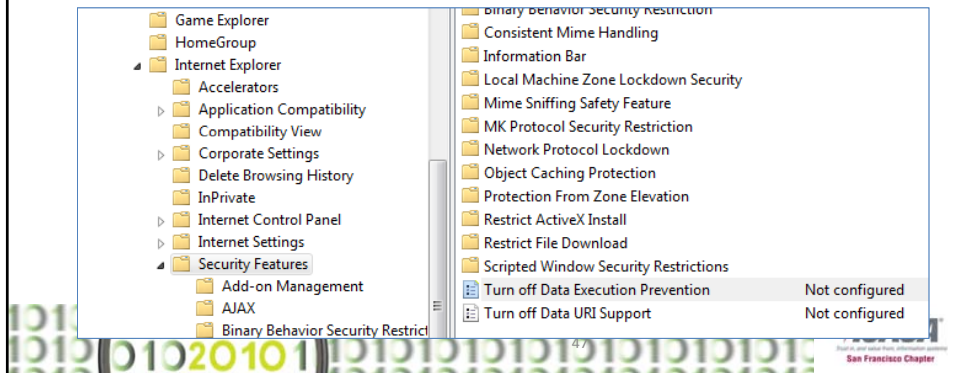


### New in IE8 – Crash Recovery

- Tabs isolated into separate processes – one tab crashing does not bring down the browser
- Crash recovery reloads tabs when they crash

## IE 8 DEP

- Internet Explorer 7 on Windows Vista introduced an DEP off-by-default
- DEP enabled by default for IE 8 on Windows Server 2008 and Windows Vista SP1 and later



## 6 Reasons You (Should) Care About the Browser

### Customer Connection

- Your company has a website and does business on the web

### Customer Trust

- Your business on the web relies on customer trust that the web is a safe place to do business

### Security

- You care about the integrity of your business data, infrastructure and PCs

### Compatibility & Standards

- Your company uses internal web apps and is building or buying more

### Supportability

- Your users probably spend 2 hours or more in the browser every day

### Manageability

- Keeping up to date with browser patches and updates is hard



Windows Server<sup>®</sup> 2008 R2



## Windows Server 2008 R2

- BitLocker
- Virtual Accounts
- Managed Service Accounts
- Hyper-V R2
- Cluster Failover
- Live Migration



## Managed Service Accounts

- Services sometimes require network identity e.g. SQL, IIS
- Before, domain account was only option
  - Required administrator to manage password and Service Principal Names (SPN)
  - Management could cause outage while clients updated to use new password
- Windows Server 2008 R2 Active Directory introduces Managed Service Accounts (MSA)
  - New AD class
  - Password and SPN automatically managed by AD like computer accounts
  - Configured via PowerShell scripts
  - Limitation: can be assigned to one system only



## Virtual Accounts

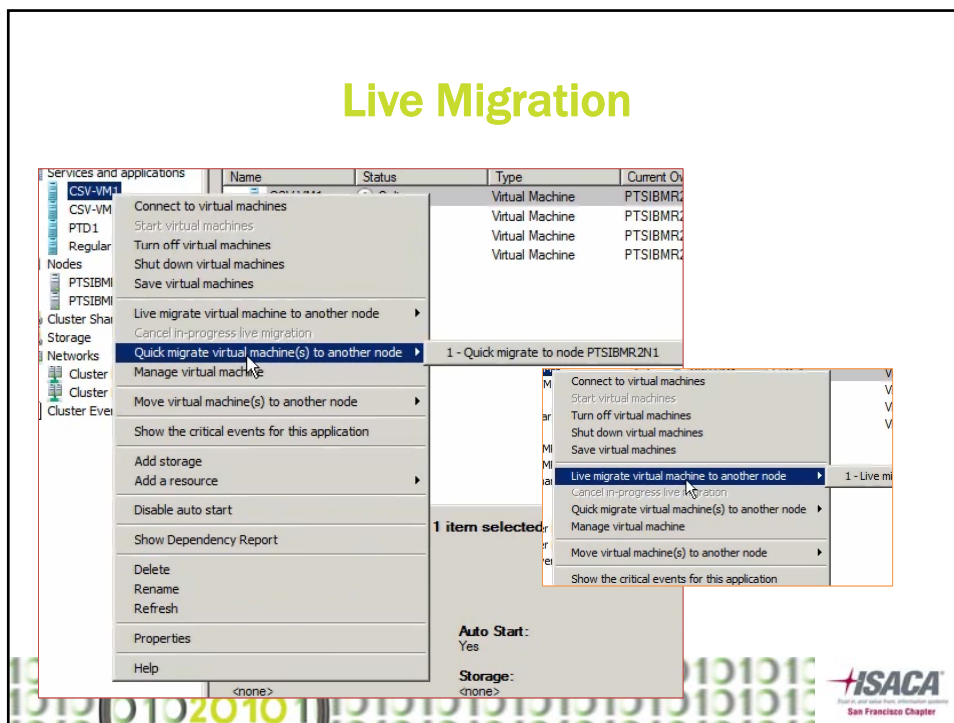
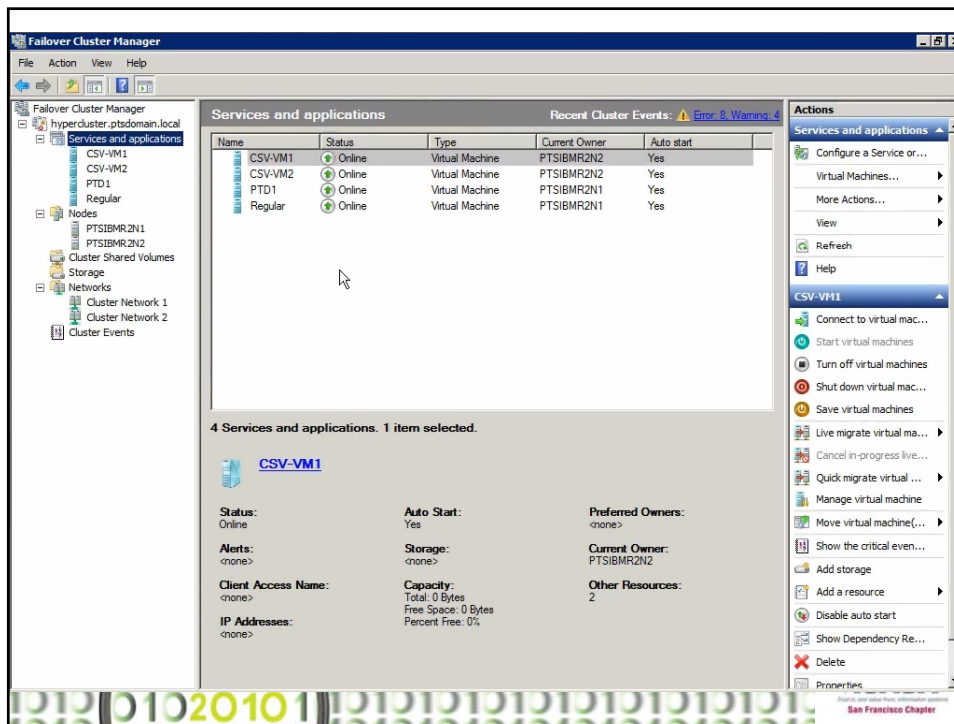
- Want better isolation than existing service accounts
  - Don't want to manage passwords
- Virtual accounts are like service accounts:
  - Process runs with virtual SID as principal
    - Can ACL objects to that SID
  - System-managed password
  - Show up as computer account when accessing network
- Services can specify a virtual account
  - Account name must be "NT SERVICE\<>service>"
    - Service control manager verifies that service name matches account name
  - Service control manager creates a user profile for the account
- Also used by IIS app pool and SQL Server



## Migration

- Quick Migration
  - Pauses the virtual machine
  - Moves the virtual machine
  - Resume the virtual machine
- Live Migration
  - Move virtual machine without stopping
- Cluster Fail Over
  - Automatic failover for virtual machines









## Cluster Fail Over

Name	Status
CSV-VM1	Pending (Starting VM)
CSV-VM2	Pending (Starting VM)
PTD1	Pending
Regular	Pending

Name	Status	Type
CSV-VM1	Online	Virtual
CSV-VM2	Online	Virtual
PTD1	Pending (Starting VM)	Virtual
Regular	Pending (Starting VM)	Virtual



## Conclusion

Windows 7

Internet Explorer 8

Windows Server 2008 R2



## Notes

- <http://blogs.techrepublic.com.com/10things/?p=488>
- <http://www.microsoft.com/windows/internet-explorer/default.aspx>
- <http://technet.microsoft.com/en-us/library/dd367859.aspx>
- <http://blogs.msdn.com/vijaysk/archive/2009/02/13/goodbye-network-service.aspx>
- <http://www.neowin.net/news/main/09/01/11/windows-7-problem-steps-recorder-overview>
- 



## Resources

Microsoft  
**tech.ed**  
Online

[www.microsoft.com/teched](http://www.microsoft.com/teched)  
Sessions On-Demand & Community

Microsoft | **Learning**

[www.microsoft.com/learning](http://www.microsoft.com/learning)  
Microsoft Certification & Training  
Resources

Microsoft **TechNet**

<http://microsoft.com/technet>  
Resources for IT Professionals

**msdn**

<http://microsoft.com/msdn>  
Resources for Developers

[www.microsoftlearning.com](http://www.microsoftlearning.com)  
Microsoft E Learning Resources

# Questions

Donald E. Hester  
CISSP, CISA, CAP, MCT, MCITP, MCTS, MCSE Security,  
MCSA Security, MCDST, Security+, CTT+

Blog

[www.LearnSecurity.org](http://www.LearnSecurity.org)

LinkedIn

<http://www.linkedin.com/in/donaldehester>



**MAZE &  
ASSOCIATES**