



Security Enhancements for Windows Vista





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 Linked in 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







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







Fundamentals

Threat & Vulnerability Mitigation

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

- IE Protected Mode
- Windows Defender
- Network Access
 Protection

Security and Compliance

Έ&

Identity & Access Control

User Account Control
 Plug and Play
 Smartcards

Serving IT Governance Professionals San Francisco Chapter Information Protection

- BitLocker™ Drive
 Encryption
- EFS Smartcards

RMS Client 7 Fall Conference

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
 - **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)







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



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)









- 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

100

-			
Search res <u>u</u> lts:		ОК	Cancel
Name (RDN)	In Folder		
Administrator	ASI-YNH5W6H		
Administrators	ASI-YNH5W6H		
ANONYMOUS LOGON			
Authenticated Users			
Backup Operators	ASI-YNH5W6H		
BATCH			
CREATOR GROUP			
CREATOR OWNER			
Cryptographic Operatore	ASI YNIHEW/CH		
DIALUP			
Distributed COM Users	ASI-YNH5W6H		
Everyone			
Guest	ASI-YNH5W6H		
Guests	ASI-YNH5W6H		
	ASI-YNH5W6H		
22 INTERNET USER			>
2 Jesper	ASI-TINH5W6H		
ALOCAL SERVICE			
RNETWORK			
Network Configuration Operat	ASI-YNH5W6H		
METWORK SERVICE			
WOWNER RIGHTS			
Performance Log Users	ASI-YNH5W6H		
💀 Performance Monitor Users	ASI-YNH5W6H		
Power Users	ASI-YNH5W6H		
Remote Desktop Users	ASI-YNH5W6H		
REMOTE INTERACTIVE LO			
Replicator	ASI-YNH5W6H		
SERVICE			
SYSTEM			
TERMINAL SERVER USER			
 🕵 Users	ASI-YNH5W6H		



IVIAZE & ASSOCIATES

Credential Prompt

Replacement for "Run As"









- 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







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







- 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





Shortcut method

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





Security	Details Previous Versions	
General	Compatibility	and the state of the state of the
FA	AR HTML	9
Target type:	Application	Advanced Properties
Target location:	FAR	Choose the advanced properties you want for this shortcut.
Target:	"C:\Program Files\Helpware\FAR\FAR.exe"	
8 1 8488		Run as administrator
Start in:	"C:\Program Files\Helpware\FAR"	This option allows you to run this shortcut as an administrator, while protecting your computer from
Shortcut key:	None	unauthorized activity.
Run:	Normal window 💌	Run in separate memory space
Comment:		
Open File Lo	ocation Change Icon Advanced	
	X	OK Cancel
	OK Cancel Apply	
and the second		



G

H


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



BitLocker Drive Encryption





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

🕐 Windows Security Center



- 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

See also

Backup and Restore





2007 Fall Conference

- C X

?

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 becancy center			
 Windows Update Windows Firewall Windows Defender Internet Options Get the latest security and virus information online from Microsoft 	ecurity essentials The security settings on this computer are managed by a networ computers on a network). To help protect your computer, the a • Install a firewall and keep it turned on (Windows Firewall is au • Set up automatic updating to download and install critical up • Install antivirus software and keep it turned on and up to date Using Security Center at work	Prk administrator because your computer is part of a domain (a group of idministrator of this computer should do the following: tomatically installed). Indates automatically.	Shape Fill Shape Outlin Shape Effect
 Windows Firewall Turn Windows Firewall on or off Allow a program through Windows Firewall See also Security Center Network Center 	<section-header><section-header><section-header><text><text><text><text><text><text></text></text></text></text></text></text></section-header></section-header></section-header>	Image: Content of the second section of the second section sect	vice ager ail nters et PC ings dows par

Windows Vista Firewall

- Both inbound and outbound
- Authentication and authorization aware
- Outbound applicationaware filtering is now possible
 - Includes <u>IPSec</u> managemen⁻
 - Of course, policy-based administration
 - Great for Peer-to-Peer control



Console1 - [Console Root\Windows Firewall with Advanced Security on Local Computer]





- O -X

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

C

🔗 Windows Firewall with Advance	Connection Security Rules		Actions
Inbound Rules	Name	Enabled Endpoint 1 Endpoint 2 A	Connection Security Rules
Connection Security Rules	There a	are no items to show in this view.	😤 New Rule
Monitoring	Mew Connection Securit	iy Rule Wizard	Σ
 Connection Security Rul Security Associations Main Mode 	Rule Type Select the type of connection	security rule to create.	
🛃 Quick Mode	Steps: Rule Type	What type of connection security rule would you like to	create?
	 Requirements Authentication Method Profile 	 Isolation Restrict connections based on authentication criteri health status. 	a, such as domain membership or
	 Name 	Authentication exemption Do not authenticate connections from the specified	computers.
		Server-to-server Authenticate connection between the specified con	nputers.
		Tunnel Authenticate connections between gateway computed	ters.
		Custom Custom rule.	
ection Security	Rules	Note: Connection security rules specify how and when allow connections. To allow a connection, create an ir	authentication occurs, but they do not bound or outbound rule.
action Security	Rilles	Learn more about rule types	

Firewall Monitoring

Windows Firewall with Advanced	Security			• 🔀
<u>File Action View Help</u>				
🗢 🔿 🔽 🔽 🗊				
Pindows Firewall with Advance	Monitoring		Actions	
Inbound Rules	Windows Firewall is beloing to protect your computer		Monitoring	
Connection Security Rules	Windows Thewains helping to protect your compate		View	۲
Monitoring	Domain Profile		Refresh	
Firewall			- Relp	
Security Associations	Private Profile	•		
Main Mode	Public Profile is Active	*	1	
Quick Mode	Firewall State			
	🧭 Windows Firewall is on.			
	S Inbound connections that do not match a rule are blocked			
	Outbound connections that do not match a rule are allowe	ring		
	General Settings	Firewall Monito	ring	
	Display a notification when a program is blocked:	Yes		
	Apply local tirewall rules:	Yes		
	Apply local connection security fules.	Tes		
	Logging Settings:			
	File name:	C:\Windows\system32\LogFiles\Firewall\pfirewall.lc		
	File maximum size (KB):	4096		
	Log dropped packets:	Yes		
	Log successful connections:	Yes		
	View active firewall rules			
	View active rinewan rules			
	View security associations			
•				

Inbound & Outbound Rules

= 🔿 🔰 🖬 🔂 🖬									
P Windows Firewall with Advance	Inbound Rules								Actions
K Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Drogram	Local Address	Inbound Rules
Connection Rules	AirSync Protocol HTTP Port		Any	Yes C	naaif		ulaa	Any	🐹 New Rule
Monitorinu	AirSync Protocol HTTP Port		Any	Yes O	pecii	IC RU	lies	Any _	Filter by Profile
Firewall	AirSync Protocol HTTP Port		Any	Yes	Allow	No	Any	Any	
🚡 Connection Security Rul	Mpznui01.exe		Private	No O	Allow		C:\Users\	Any	Y Filter by State
Security Associations	Mpznui01.exe		Private	No	Allow	No D	C:\Users\	Any	Filter by Group
🔡 Main Mode	🞯 Internet Explorer		Domain	Ves	Allow	No	C:\progr	Any	View
🔡 Quick Myde	🕑 Internet Explorer		Domain	Yes	Allow	No	C:\progr	Any	Refresh
1	🕑 Legacy Status Port		Any	Yes	Allow	No	Any	Any	
	🕑 Legacy Status Port		Any	Yes	Allow	No	Any	Any	Export List
	🖉 Legacy Status Port		Any	Yes	Allow	No	Any	Any	🛛 🛛 🖓 Help
	🖉 Legacy Sync Channel Port		Any	Yes	Allow	No	Any	Any	Microsoft Office Groove
	Legacy Sync Channel Port		Any	Yes	Allow	No	Any	Any	Disable Rule
	Legacy Sync Channel Port	K	Any	Yes	Allow	No	Any	Any	
	Microsoft Office Groove		Private	Yes	Allow	No	C:\Progr	Any	X Delete
	Microsoft Office Groove		Domain	Yes	Allow	No	C:\Progr	Any	Properties
	Microsoft Office Groove		Domain	Yes	Allow	No	C:\Progr	Any	Help
	Microsoft Office Groove		Private	Yes	Allow	No	C:\Progr	Any	
	Microsoft Office OneNote		Domain	Yes	Allow	No	C:\Progr	Any	
	Whicrosoft Office OneNote		Private	Yes	Allow	No	C:\Progr	Any	
	Microsoft Office OneNote		Domain	Yes	Allow	No	C:\Progr	Any	
	Wicrosoft Office OneNote		Private	Yes	Allow	No	C:\Progr	Any	
	Microsoft Office Outlook		Domain	Ves	Allow	No	C:\Progr	Any	
	Sync Services Port		Any	Yes	ALL DIA/	No	Any	Any	
	Sync Services Port							ماريس ام ما	
	Synd Services Port			ice Zul) ac	laea	need	iea ruie	es
	Windows Live Messenger 8.1 (Phone)								
	Windows Mobile-based device connectiv.		Any	Yes	Allow	No	%System	Any	
Jun hou un d			Pux S Off	C G Yes () (Allow	No	%System	Any LITE	C
inpound a	s Outbound Rule	S	Any	Yes	Allow	No	%System	Any	
-	ă.		Any	Yes	Allow	No	%System	Any	
	Windows Mobile-based network access	2	Any	Yes	Allow	No	Any	Any	
	Windows Mobile-based network access	6	Any	Yes	Allow	No	Any	Any +	

ASSOCIATES

San Francisco Chapter

General	Progra	ms and Servi	ices	
Users and Computers	Protocols and Ports	Scope	Advanced	
Profiles	s ofiles: ain ite			
Interface types Specify the in rule applies.	ic terface types to which th	is <u>C</u> us	tomize	
Edge traversal Edge traversa to bypass de (NAT) routers Allow <u>edg</u>	al allows traffic coming to vices such as Network A s. ge traversal	and from the ddress Trans	e Internet slation	
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

elete Browsing History	6		
Temporary Internet Files			
Copies of webpages, images, and media that are saved for faster viewing.	Delete <u>fi</u> les		
Cookies	-		
Files stored on your computer by websites to save preferences such as login information.	Delete cookies		
History	ſ		
List of websites you have visited.	Delete <u>h</u> istory		
Form data			
Saved information that you have typed into forms.	Delete forms		
Passwords			
Passwords that are automatically filled in when you log on to a website you've previously visited.	Delete passwords		
	Close		





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

Certific	ate Error: Navigation Blocked - Windows Internet Explorer		
00-	https://mx-001.mazecentral.com/exchange	MSN Search	
0 4	O Certificate Error: Navigation Blocked	🚰 🔹 🔂 🔹 📾 🔹 🛄 Page 🔹 🎯 Tools 👻	
8	There is a problem with this website's security certificate.		lisual promote
	The security certificate presented by this website was issued for a different website's address.	· · · · · · · · · · · · · · · · · · ·	isual prompts
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.		for security
	We recommend that you close this webpage and do not continue to this website.		Tor bootinty
	Click here to close this webpage.		
	😵 Continue to this website (not recommended).		
	For more information, see "Certificate Errors" in Internet Explorer Help.		
			\sim \sim
C Mici	rosoft Outlook Web Access - Windows Internet Explorer		
()	🕽 👻 🖉 https://mx-001.mazecentral.com/exchange/		🔽 😨 Certificate Error 🚱 🔀 MSN Search
01			🔊 - 🖸 - 🗖 - 🗖 Daga - 🖉 Tarle - 🎽
6 7	Microsoft Outlook web Access		📶 · 🕅 🖓 🖓 runs +
Ele 🛪			Items 1 to 25 of 58 Bd at Is Isl
pening page	https://mx-001.mazecentral.com/exchange	🗳 Internet 🛞 100%, 🔸 .	
etocological and a constant			





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



🕖 Suspicious Website

Level 2: Block Confirmed Phishing Site Signaled and Blocked

🕲 Phishing Website





- 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







- 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

San Francisco Chapter

- Kernel Only
- User Mode
- Internet Explorer





Windows Vista Security

INTEGRITY PROTECTION





2007 Fall Conference

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







- 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
 - **Kernel Drivers**

D User-mode Drivers





Integrity Levels in Token

Image	Pe	erformance	Performance Graph	Threads	
TCP/I	P	Security	Environment	Strings	
6	User: RE	DMOND\jesperj	þ		
	Group			Fi 🔦	
	JESPERJ	01\Debugger U	lsers	Ma	
	LOCAL			Ma	
	Logon SIE) (S-1-5-5-0-217	030)	Ma	
	Mandatory	y Label\Medium	Mandatory Level		
	Mandatory	y Label\Medium	Mandatory Level		
	NORTHA	MERICA\fs_mb	sfile02_resvol3_r	Ma 🔻	
	<				
	Privilege		Flags		
ED	SoChonor	NotifuPrivilego	Default Epobled		
	Selacreas	e Working Set Pri	vilege Disabled		
	SeShutdo	wnPrivilege	Disabled		
	SeTimeZo	nePrivilege	Disabled		
	SeUndock	kPrivilege	Disabled		
				Permissions	
			<u>O</u> K	<u>C</u> ancel	
		• • •			
		IVIA	ZE &		2007 Fall Conferer
			ACCOCIATI	22	



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 "adminrequired" 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.









Section 2: Data Protection



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





2007 Fall Conference 86



- 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









- 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

San Francisco Chapter



ASSOCIATES

- 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

Disk Layout & Key Storage

Windows Partition Contains

- Encrypted OS
- Encrypted Page File
- Encrypted Temp Files
- Encrypted Data
- Encrypted Hibernation File

Where's the Encryption Key?

- SRK (Storage Root Key) contained in TPM
- SRK encrypts VEK (Volume Encryption Key) protected by TPM/PIN/Dongle
- VEK stored (encrypted by SRK) on hard drive in Boot Partition



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





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

Configure encryption method Properties
Setting Explain
Configure encryption method
○ Not <u>C</u> onfigured
<u>E</u> nabled
© <u>D</u> isabled
Select the encryption method:
AES 128 bit with Diffuser (default)
AES 128 bit with Diffuser (default) AES 256 bit with Diffuser
AES 128 bit
AES 256 Dit
Supported on: At least Windows Vista
Previous Setting <u>N</u> ext Setting
OK Cancel Apply







Windows Vista Security







2007 Fall Conference 99

Encrypting File System

1000000	Cache				
File end	cryption usin	g Encrypting F	ile System (EFS):	
O	Not defined				
0	Allow				
0	<u>D</u> on't allow				
Optio	ons				
E 8	Encrypt the o	ontents of th	e user's Docume	nts folder	
E #	Require a <u>s</u> m	art card for E	FS		
1	Create cachir	ng-capable <u>u</u> s	er key from sma	rt card	
	Enable gagef	ile encryption			
	Display key b	ackup notifica	tions when user	key is created or ch	nanged
Certi	ficates Allow EFS to	generate self	-signed certificat	tes when a certificat	ion authority is
Kev	not available size for self	-sianed certific	ates:		
Key	not available size for self	signed certific	cates:		
Key 20-	not available size for self 48	signed certific	cates:		
Key 20- EES	not available size for self 48 template for	signed certific	rtificate request	s:	
Key 204 EES No	not available size for self- 48 template for valid templa	signed certific automatic ce tes were four	cates: rtificate request nd.	s:	Browse
EES No	not available size for self- 48 template for valid templa nore about t	-signed certific - automatic ce tes were four he Encrypting	cates: rtificate request nd. File System	s:	Browse





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





2007 Fall Conference 102

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







Windows Vista Security

RIGHTS MANAGEMENT





2007 Fall Conference 106

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 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

Serving IT Governance Professionals San Francisco Chapter


ACL IMPROVEMENTS





Old ACL UI

Test tyt Droperties		2 1	
General Security Summary			
Group or user names:			
Administrators (JESPEBJO0) Adminis	strators)		
g iesperio (REDMOND\iesperio)	And to roy		
SYSTEM			
Users (JESPERJO0\Users)			
Ac	<u>d</u> d <u>R</u> er	nove	
Permissions for Administrators	Allow De	ny	
Full Control			
Modify			
Read & Execute	¥		
Read			
Write			
Special Permissions			
For special permissions or for advanced s	ettings, Adva	nced	
click Advanced.			
			2007 Fall Confere
ОК	Cancel	Apply	
		CPP7	



New ACL UI





This permission is inherited from the p here to create a new permission that	arent object. overrides the	Make chang inherited	es	
permissions.				
Name: CREATOR OWNER		Change		
Apply onto: Subfolders and files only	1		-	
Permissions:	Allow	Deny		
Full control	1		<u> </u>	
Traverse folder / execute file	1			
List folder / read data	1		=	
Read attributes	1			
Read extended attributes	1			
Create files / write data	1			
Create folders / append data	1			
Write attributes	~		-	
Apply these permissions to object containers within this container or	s and/or Ily	Clear All		
Managing permissions				
	ОК	Cano	el	

Serving IT Governance Professionals



VOLUME SHADOW COPY







- 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.

ame	Date modified	Location		
adow cos	vy (3)	Procession in the second	*	
Garden	9/20/2006 3:25 PM	Shadow copy		
Garden	9/20/2006 3:24 PM	Shadow copy		
Garden	8/29/2006 5:09 PM	Shadow copy		
lackup (3)				
Garden	8/29/2006 5:09 PM	Backup		
Garden	9/20/2006 3:25 PM	Backup		
Garden	9/20/2006 3:28 PM	Backup		
	Open Coj	oy Restor	•	k







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









Section 3: Improvements





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



San Feater San Chapter 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



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







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







AUDIT IMPROVEMENTS





Granular Audit Policy



C:\Windows\system32\cmd.exe Microsoft Windows [Version 6.0.5359] (C) Copyright 1985-2005 Microsoft Corp. C:\Users\Jesper>auditpol /list /subcategory:* Category/Subcategory System Security State Change Security System Extension System Integrity IPsec Driver Other System Events ⊿oqon∕Loqoff Logon Logoff Account Lockout IPsec Main Mode **IPsec Quick Mode IPsec** Extended Mode Special Logon Other Logon/Logoff Events Object Access File System Registry Kernel Óbject SAM Certification Services Application Generated Handle Manipulation File Share Filtering Platform Packet Drop Filtering Platform Connection Other Object Access Events Privilege Üse Sensitive Privilege Use Non Sensitive Privilege Use Other Privilege Use Events Detailed Tracking **Process Creation** Process Termination DPAPI Activity Other Detailed Tracking Events Policy Change Audit Policy Change Authentication Policy Change Authorization Policy Change MPSSUC Rule-Level Policy Change Filtering Platform Policy Change Other Policy Change Events Account Management User Account Management Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events DS Access Directory Service Access Directory Service Changes Directory Service Replication Detailed Directory Service Replication Account Logon **Credential Validation** Kerberos Ticket Events **Other Account Logon Events** C:\Users\Jesper>_

AJJUCIAIEJ

_ 🗆 🗙

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

Event Properties	5		×
Log Name:	Security		
Source:	Microsoft-Windows-Security-Au	Da <u>t</u> e:	4/7/2006 12:54:46
Event ID:	4634	Task Category:	Logoff
Level:	Information	Keywords:	Audit Success
<u>U</u> ser:	N/A	Computer:	JESPERJO1.redmond.corp.mi
O <u>p</u> Code:	Info		
Des <u>c</u> ription:	Logon Type: 3 This event is generated when a correlated with a logon event us unique between reboots on the	a logon session is des sing the Logon ID val e same computer.	stroyed. It may be positively ue. Logon IDs are only
More Information:	Event Log Online Help		
Сору			Close





Events Stored in XML

Event Properties	
General Details	
Friendly View SXML View	
<pre>- <event -="" <system="" xmlns="http://schemas.microsoft.com/win/2004/08/events/event"></event></pre>	
Copy	3





New Event Viewer

Computer Management (Local)	Overview and Summ	nary				Last refreshed	I: 3/31/2007 1:42:35 PM	Actions		
18 System Loois								Event Viewer	· •	
Event Viewer	Overview						<u> </u>	👩 Open Sa	aved Log	
Shared Folders	👔 You can view events that have taken place on your machine by choosing an appropriate log in the tree on scope pane. An aggregated view of all						🛛 🔻 Create (Custom View		
Local Users and Groups	your logs is shown	below:						Import	Custom View	
Reliability and Performance								View	`	
🚔 Device Manager	Summary of Administrative	Events					•		· · · · ·	
Storage		ID C			241	7.1	TIL	Refresh		
Services and Applications	Event Type Event	ID Source	Log	Last hour	24 hours	/ days	lotal	[Help	•	
	E Critical -	- Ann Kanton Consta	- 	U .	U	U	1	Error	•	
	E Error	ApplicationExperie	nceintrastructure Appii	cation U	1	25	270	View All	Instances of T	
	E Critor -	-	-	1	10	100	279	2 Help		
	H Information -			5	10 61	449	8 976	Inelp		
	E Audit Success -	-	-	7	60	596	6 983			
	⊞ Audit Failure -	-	-	0	0	3	70			
				-	-	-				
	Custom Views\Administr Applications and Service Applications and Service Applications and Service Applications and Service	 Critical, Er N/A N/A 3/15/200 N/A 3/15/200 N/A 11/30/20 N/A 11/30/20 N/A 11/30/20 	N/A 17 3:07:36 AM 11/30 17 5:06:48 AM 11/30 006 8:47:37 AM 11/30 06 8:47:37 AM 11/30 06 8:47:37 AM 11/30	/2006 9:07:48 AM /2006 11:45:04 AM /2006 11:45:05 AM /2006 11:45:05 AM			Ŧ			
	Log summary						•			
	Log Name	Size (Curr Modifie	t Enabl	ed Retention Pol	cy		^			
	Application	1.07 MB/2 3/15/20	17 3:09:26 AM Enabl	ed Overwrite eve	nts as nec					I
	DFS Replication	68 KB/14 11/30/20	106 8:47:37 AM Enabl	ed Overwrite eve	nts as nec					I
	Hardware Events	68 KB/20 11/30/20	106 8:47:37 AM Enabl	ed Overwrite eve	nts as nec					I
	Internet Explorer	68 KB/1.0 11/30/20	106 8:47:37 AM Enabl	ed Overwrite eve	nts as nec					
	Key Management Service	68 KB/1.0 11/30/20	106 8:47:37 AM Enabl	ed Overwrite eve	nts as nec					
	Media Center	1.07 MB/8 3/15/200	1/5:06:48 AM Enabl	ed Overwrite eve	nts as nec		-			



STRICTER POLICIES





Stricter Policies

Network access: Remotely accessible registry paths P ? 🔀	Network access: Remotely accessible registry paths Properties 🛛 😰 📧
Local Policy Setting Network access: Remotely accessible registry paths	Local Policy Setting Network access: Remotely accessible registry paths
System \CurrentControl Set \Control \ProductOptions System \CurrentControl Set \Control \Print \Printers System \CurrentControl Set \Control \Server Applications System \CurrentControl Set \Services \Eventlog Software \Microsoft \OLAP Server Software \Microsoft \Windows NT\Current Version System \CurrentControl Set \Control \Content Index	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion
OK Cancel Apply	OK Cancel Apply





Stricter Policies

Network access: Shares that can be accessed anonym ? 🔀	Network access: Shares that can be accessed anonymously Pro 👔 🔀
Local Policy Setting	Local Policy Setting
Network access: Shares that can be accessed anonymously	Network access: Shares that can be accessed anonymously
COMCFG DFS\$	
OK Cancel Apply	OK Cancel Apply





Network security: Do not store LAN Manager hash val ? 🔀	Network security: Do not store LAN Manager hash value o
Local Security Setting	Local Security Setting
Network security: Do not store LAN Manager hash value on next password change	Network security: Do not store LAN Manager hash value on next password change
 ○ Enabled ○ Disabled 	Enabled Disabled
OK Cancel Apply	OK Cancel Apply
Network security: LAN Manager authentication level ?X	Network security: LAN Manager authentication level Prope
Local Security Setting	Local Security Setting
Network security: LAN Manager authentication level	Network security: LAN Manager authentication level
Send LM & NTLM responses	Send NTLMv2 response only
Modifying this setting may affect compatibility with clients, services, and applications. For more information, see <u>Network security: LAN Manager</u> <u>authentication level</u> . (Q823659)	Modifying this setting may affect compatibility with clients, services, and applications. For more information, see <u>Network security: LAN Manager</u> <u>authentication level</u> . (Q823659)
OK Cancel Apply	OK Cancel Apply







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

ystem Properti	ies		? 🛛	System Proper
General	Computer Name	Hardware	Advanced	Computer Nam
System Rest Select the location. Remote Assista Allow <u>R</u> emote <u>What is Remote</u>	e ways that this compute ince te Assistance invitations mote Assistance?	tic Updates	Remote another computer	Remote Ass
Remote Desktor	p to <u>c</u> onnect remotely to th er name: edmond.corp.microsoft.co <u>mote Desktop?</u>	is computer		Remote Des Click an opt © Don't alk © Allow co Remote
For users to c have a passw <u>Windows Fire</u> connections t	connect remotely to this c vord. wall will be configured to to this computer.	Select Remo omputer, the user a allow Remote Desk	te Users ccount must ttop	Allow co Desktop
	ОК	Cancel	Apply	








 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



Chess Titans

Check how well this game will perform on your computer:

Game recommended rating:



Game required rating:



Current system's rating:



See <u>Performance Information and</u> <u>Tools</u> for more information.



EVERYONE





Parental Controls: ● On, enforce current settings ● Off On, collect information about computer usage ● Off Off Web Restrictions On Windows Vista Web Filter Control allowed websites, downloads, and other use Off Settings On Time limits Control when Toby uses the computer On	Set up how Toby will use the computer		
Games	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 Control allowed websites, downloads, and other use Settings Control when Toby uses the computer Cames	Toby Standard & Password Activity Reports: Web Restrictions: Time Limits: Game Ratings: Program Limits:	user protected On Off Up to ADULTS (On







San Francisco Chapter

For more information use System Diagnostic Reports

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





Q

🗢 🍫 Search



Reliability and	d Performance Monitor	different per	Rettourse information		×		
File Help							
System Diag	gnostics Report			۲	Â		
Computer: IT4	SLAPTOP						
Collected: Tue	sday, April 03, 2007 10:36:19 PM	1					
Duration: 60	Seconds						
Diagnostic I	Results			۲			
Warnings				۲			
Information	al						
Symptom:	ptom: (1) 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 Syste	m Checks						
Tests		Result	Description				
OS Checks		Passed	Checks for attributes of the operating system				
E Disk Check	<u>s</u>	Passed	Checks for disk status				
Security Center Tests Passed Checks for state of Security Center related information.							
<u>System Ser</u>	System Service Checks Passed Checks for state of system services						
⊞ <u>Hardware D</u>	evice and Driver Checks	Passed	Survey of Windows Management Infrastructure supported devices.				
Performance				۲			
Resouce Ov	verview				-		

ASSOCIATES

пер						
Basic System Checks						
Tests	Result	Description				
OS Checks	Passed	Checks for attributes	ofthe	operating	syste	em
Test Groups		Tests	Fa	iled Desc	riptio	n
OS Version Check		1		0 Pass	ed	
Disk Checks	Passed	Checks for disk stat	JS			
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	s 30% f	free disk s	pace	[22372 MB]
Security Center Tests	Passed	Checks for state of S	ecurity	Center re	lated	information.
Test Groups				Те	sts	Failed Description
Check that Anti-Spyware Product is up-to-	date.				1	0 Passed
Check for Anti-Spyware Product that is en	abled.				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 s	ystem	services		
Test Groups				Tests	•	Failed Description
Abnormally Terminated Services Check				1	1	0 Passed
Workstation Service Check				1	1	0 Passed
Hardware Device and Driver Checks	Passed	Survey of Windows N	lanage	ement Infra	struc	cture supported devices.
Test Groups			Tests	Failed	Des	cription
Controller Device Configured Fail Count			14	0	Con	troller devices.
Controller Device Status Fail Count			14	0	Con	troller devices.
Cooling Configured Fail Count			2	0	Coo	ling devices.
Cooling Status Fail Count			2	0	Coo	ling devices.

J

Reliability and	Performance Mo	nitor					x	
File Help								
Storage Device Status Fail Count 2 0 Storage devices.							*	
Video Device	Configured Fail	Count		2	0 Video devices.			
Video Device	e Status Fail Coun	ıt		2	0 Video devices.			
PlugAndPlay Device Configured Fail Count 128				0 PlugAndPlay devices.				
PlugAndPlay	PlugAndPlay Device Status Fail Count 128 0 PlugAndPlay devices.							
Performance						۲		
Resouce Ov	verview]	
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 Co	nfiguration		E			\odot		
Hardware Co	onfiguration		E			\odot		
CPU			Ē			\odot		
Network			Ē	=		\odot		
Disk						€	=	
Memory	Memory 📰 💽							
Report Stati	stics		E			\odot		
							-	

Reliability and Performance Monitor	
File Help	III INCOMI
root\cimv2:SELECT * FROM Win32_OperatingSystem	0x0
root\cimv2:SELECT * FROM Win32_ComputerSystem	0x0
Security Center Information	۲
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
	0-00070000

Reliability Monitor



Problems Windows Identified

1		
	2.1	
15.	$ \rightarrow $	
11	11	

Problem Reports and Solutions

Problems Windows has identified

Product	Problem	Date	Status
🔫 Broadcom Advanced Control Suite 2 (.	2)		
Broadcom Advanced Control Sui	Broadcom Advanced Control Suite 2	4/3/2007 8:44 AM	Not Reported
Broadcom Advanced Control Sui	Broadcom Advanced Control Suite 2	4/3/2007 6:16 PM	Not Reported
🔟 CuteFTP File Transfer Application (5) -			
CuteFTP File Transfer Application	Stopped working	4/3/2007 6:48 AM	Report Sent
CuteFTP File Transfer Application	Stopped working	4/3/2007 6:57 AM	Not Reported
CuteFTP File Transfer Application	Stopped working	4/3/2007 6:58 AM	Not Reported
CuteFTP File Transfer Application	Stopped working	4/3/2007 7:29 AM	Not Reported
CuteFTP File Transfer Application	Stopped working	4/3/2007 7:20 PM	Not Reported
InstallDriver Module (2)			
InstallDriver Module	Program compatibility problem	4/3/2007 8:41 AM	Not Reported
InstallDriver Module	Program compatibility problem	4/3/2007 8:41 AM	Not Reported
<i>(</i> Internet Explorer			
Internet Explorer	Stopped working	4/2/2007 5:45 AM	Not Reported
SharedAccess			
SharedAccess	Service Hang Report	3/26/2007 1:39 PM	Not Reported
📰 Symantec AntiVirus AutoProtect ——			
Symantec AntiVirus AutoProtect	Symantec AntiVirus AutoProtect is bloc	3/28/2007 12:52 PM	Solution Available
Symantec Utility Driver			

ASSOCIATES



<u>0</u>K

- O X

Problems and Solutions



Problem Reports and Solutions

Tasks

Scheck for <u>new</u> solutions

See problems to check

View problem history

Change settings

Clear solution and problem <u>h</u>istory

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

- O X

2

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

See also

<u>Read our privacy statement</u> online

<u>Customer Experience</u> Improvement Settings

Serving IT Governance Professionals

ASSOCIATES

Check for Solutions

Problem Reports and Solutions <u>.</u>

Check for solutions to these problems

Select <u>all</u>

G

Product		Problem	Date	Details	
🔍 Broadcom Advan	ced Control Suite 2 (2	2)			- ^
Broadcom A	dvanced Control S	Broadcom Advanced Control Suite 2 ha	4/3/2007 8:44 AM	View details	
Broadcom A	dvanced Control S	Broadcom Advanced Control Suite 2 ha	4/3/2007 6:16 PM	View details	
🔟 CuteFTP File Trar	sfer Application (4) -				- ^
CuteFTP File	Transfer Applicati	Stopped working	4/3/2007 6:57 AM	View details	E
CuteFTP File	Transfer Applicati	Stopped working	4/3/2007 6:58 AM	View details	
CuteFTP File	Transfer Applicati	Stopped working	4/3/2007 7:29 AM	View details	
CuteFTP File	Transfer Applicati	Stopped working	4/3/2007 7:20 PM	View details	
InstallDriver Mod	ule (2)				- ^
InstallDriver	Module	Program compatibility problem	4/3/2007 8:41 AM	View details	
InstallDriver	Module	Program compatibility problem	4/3/2007 8:41 AM	View details	
Internet Explorer					~
Internet Expl	orer	Stopped working	4/2/2007 5:45 AM	View details	
SharedAccess					- ^ -
Check again for sole See if solutions are r	utions to <u>o</u> ther proble now available for prol	ms plems that you reported earlier.		Choose the <u>i</u> nformati when a problem occu	on to send Irs
			Ch	eck for <u>s</u> olutions	<u>C</u> ancel
Governance Professionals		TTALE O			

X

2





Section 4: Secure Deployment





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







- 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

Threat and Windows Vista Vulnerability Mitigation Identity and

- IE –protected mode/antiphishing
- Windows Defender
- Bi-directional Firewall
- IPSEC improvements
- Network Access Protection (NAP)
 Fundamentals
 - SDL
 - Service Hardening
 - o Code Scanning
 - Default configuration
 - Code Integrity

Serving IT Governance Professionals San Francisco Chapter



Control User Account Control

Access

- Plug and Play Smartcards
- Simplified Logon architecture
- Bitlocker
- RMS Client

Special Thanks

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

Jeff Sigman, Program Manager Windows Networking, Microsoft

Rob Labbe, Security Consultant, Microsoft





- Windows Vista Security Guide
 - <u>http://www.microsoft.com/technet/windowsvist</u> <u>a/security/guide.mspx</u>
- Scott Riley Presentation
 - <u>http://www.microsoft.com/emea/itsshowtime/s</u> essionh.aspx?videoid=223
- <u>http://technet.microsoft.com/en-us/windowsvista/aa905117.aspx</u>





- Windows Server 2003 Security Guide

 <u>http://go.microsoft.com/fwlink/?LinkId=14846</u>
- WindowSecurity.com
- <u>SecWish@microsoft.com</u> (Feedback email)
- Microsoft Windows Security Resource Kit (2nd Ed.) ISBN 0-7356-2174-8
- Service Pack 1 Overview
 - <u>http://www.microsoft.com/technet/prodtechnol/window</u>
 <u>sserver2003/servicepack/overview.mspx</u>





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





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





Contact Info

- Donald E. Hester
 - DonaldH@MazeAssociates.com

Linked in.

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



