Windows Security Tips

Produced by the CyberNEXS Team

Siobhan Moran

August 2009

Windows Overview

- Knowledge is security
  - Older Windows were built for ease of use, not security
  - This has changed with Windows Server 2003/2008 and Windows Vista
    - Most options OFF by default
    - Security mechanisms “built in” like Windows Firewall, Windows Defender, etc.
    - Security Center is included

The trick is to make sure your security is on and functioning properly

Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries.

Defending your Windows Box

- Patching
  - Keep up to date with latest service packs and hot fixes
- Disable unnecessary services
  - If a service is not needed, shut it off – especially those services that enable any kind of "sharing"
- Secure configuration
  - Strong passwords
  - File permissions
  - Proper configuration of services (IIS, DNS, MSSQL, etc.)
  - Use Security Configuration Tools (Security Configuration Wizard, GUI based policy tools, Compliance Tools)
- Logging
  - Configuring and monitoring Event Viewer
  - Set up auditing of security events like "Logon attempts"
- SANS Top Ten Vulnerabilities
  - Mitigate most common vulnerabilities

Patching Options

Patching

- Tools to determine missing patches
  - Shavlik NetChk Protect Limited
    - Free GUI utility checks registry, file versions and checksums for missing patches
    - Checks missing patches for:
      - Operating system (2000 / XP / 2003/ Vista/Win7/Server 2008)
      - Internet Information Server 5.0/6.0/7.0/8.0
      - SQL Server 2003 and later
      - Internet Explorer
    - Can be performed on local machine or remote machine
      - Administrator privileges required
    - Will NOT download or install patches for you
  - Belarc Advisor
    - Graphical User Interface (GUI)
    - Checks for ANY missing Microsoft patches applications in their database
    - Checks antivirus or spyware status
    - Checks Oracle or other database status
    - Analyzes and reports on your hardware components
    - Checks patch status of many vendor applications installed

Patching

- Tools to determine missing patches (continued)
  - Microsoft Baseline Security Analyzer (MBSA)
    - Free GUI-based tool from Microsoft
    - Scans (remote and local) for ALL missing Microsoft patches
      - Administrator privileges required
    - Also scans for common misconfigurations in:
      - IIS
      - MSSQL Server
      - Office
      - Internet Explorer
      - Checks for weak passwords and account status
  - Windows Update
    - Website (http://windowsupdate.microsoft.com)
    - Checks for missing patches via ActiveX control
      - Critical, recommended, and driver updates
      - Must use Internet Explorer

Verify Patch Installation

- Run applicable patch tool again
  - Check if any patches were missed

- Run MBSA (Microsoft Baseline Security Analyzer)
  - Checks to see which hotfixes are installed
  - Determines if there are any patch anomalies

Manual Process Pros/Cons

Pros:

- Greatest amount of control over process
- Best information on patch status
- Command line utilities are flexible and can be scripted

Cons:

- Time consuming
- Does not scale well to multiple systems (unless you're good at scripting!)

Automatic Patching Pros/Cons

Pros:

- Easy to visit site
- Can update without technical knowledge
- Can also update drivers
- Significantly simplifies patching process
- Can use automated patching from centralized servers using WSUS
- Can be incorporated with Server 2008 NAC policies

Cons:

- Must have Administrator rights to install
- Only updates Windows OS
- Must remember to check periodically for patches
- May break other applications

Disabling Unnecessary Services

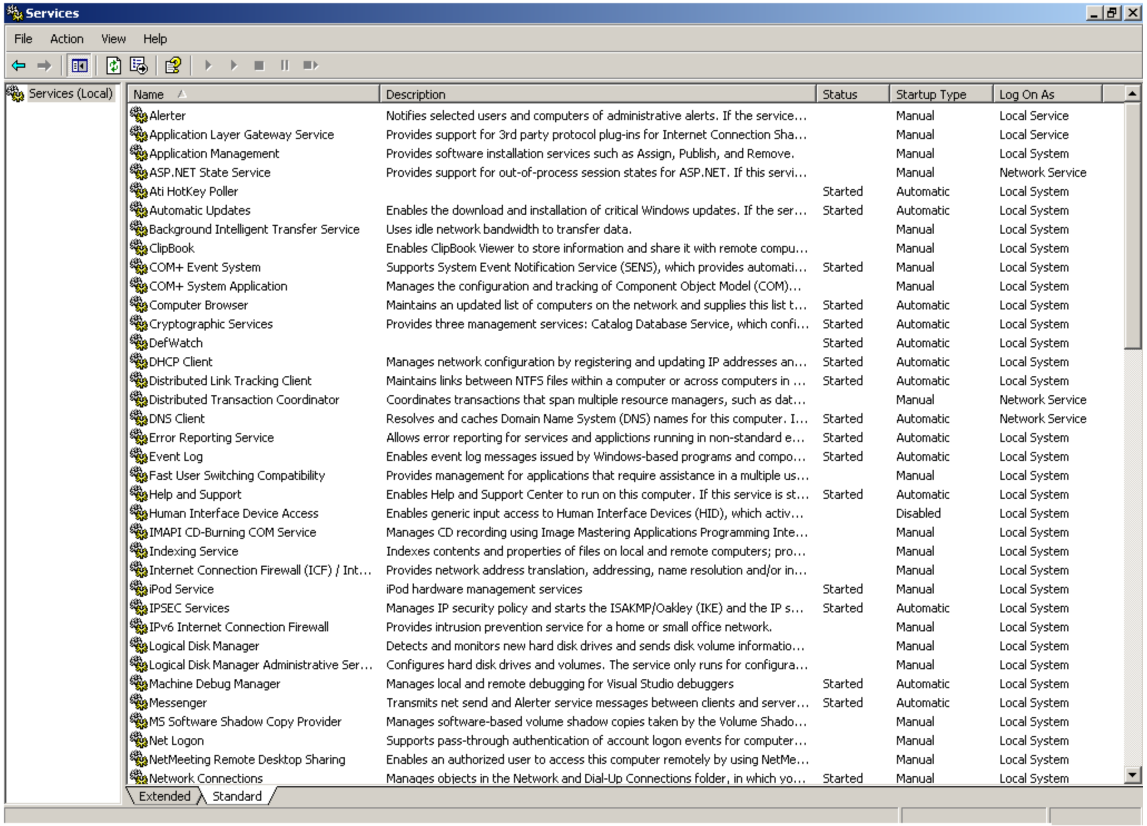
System Services Tab

- In Control Panel under “Administrative Tools”
  - Enable Services based on “Role” and disable what is not needed
- For services that need to run
  - Service startup parameters
    - Automatic
      - Starts automatically when system is booted
    - Manual
      - Not started automatically, but can be started manually by a user or program
    - Disabled
      - Not started, cannot be started manually unless an Administrator changes this value
  - Service permissions
    - Use lowest permissions needed by service

System Services

Some services are particularly vulnerable and should be disabled (only the IP Helper service is installed by default)

- Fax (fax)
- IP Helper (iphlpsvc)
- FTP Publishing Service (msftpsvc)
- Peer Networking
- Identity Manager (p2pimsvc)
- Simple TCP/IP Services (simptcp)
- Telnet (tlntsvr)

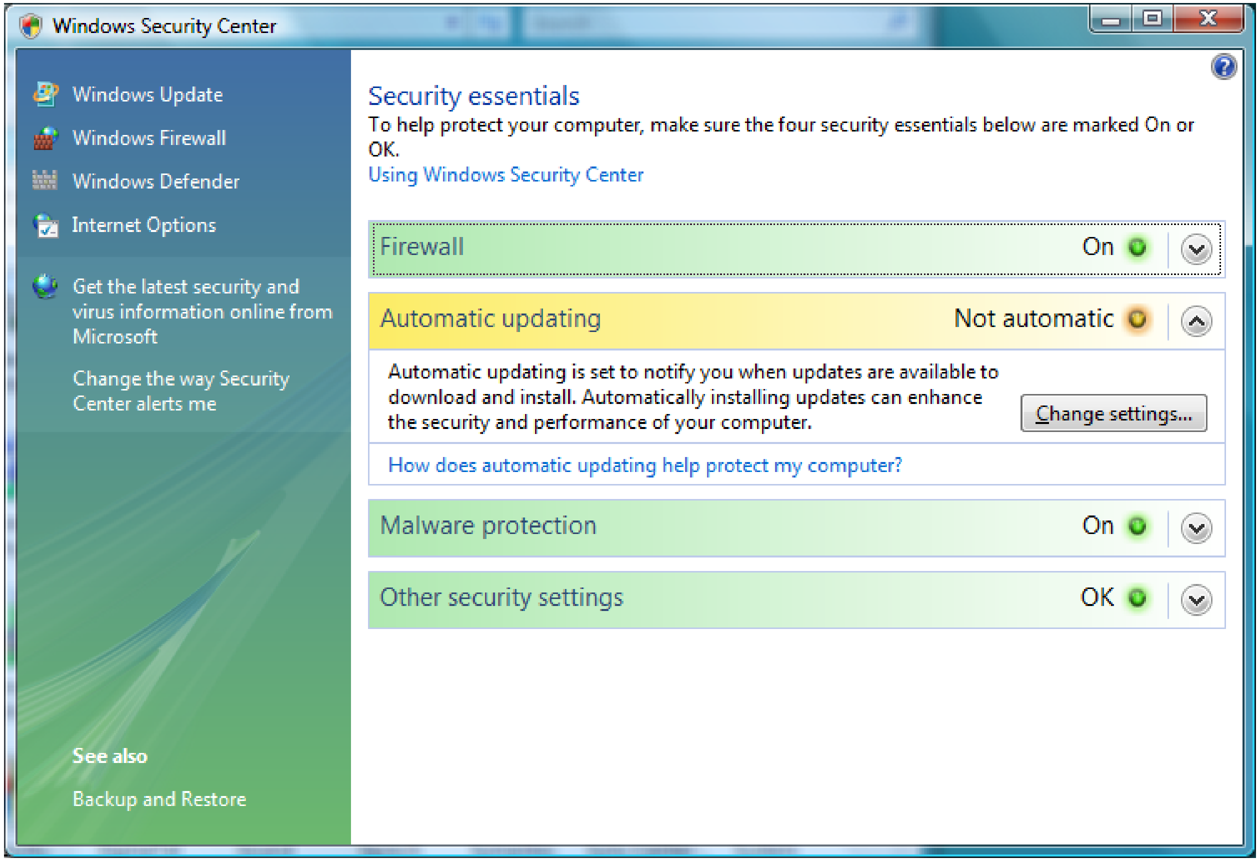


Name	Description	Status	Startup Type	Log On As
Alerter	Notifies selected users and computers of administrative alerts. If the service...		Manual	Local Service
Application Layer Gateway Service	Provides support for 3rd party protocol plug-ins for Internet Connection Sha...		Manual	Local Service
Application Management	Provides software installation services such as Assign, Publish, and Remove.		Manual	Local System
ASP.NET State Service	Provides support for out-of-process session states for ASP.NET. If this servi...		Manual	Network Service
Ati HotKey Poller		Started	Automatic	Local System
Automatic Updates	Enables the download and installation of critical Windows updates. If the ser...	Started	Automatic	Local System
Background Intelligent Transfer Service	Uses idle network bandwidth to transfer data.		Manual	Local System
ClipBook	Enables ClipBook Viewer to store information and share it with remote compu...		Manual	Local System
COM+ Event System	Supports System Event Notification Service (SENS), which provides automati...	Started	Manual	Local System
COM+ System Application	Manages the configuration and tracking of Component Object Model (COM)...		Manual	Local System
Computer Browser	Maintains an updated list of computers on the network and supplies this list t...	Started	Automatic	Local System
Cryptographic Services	Provides three management services: Catalog Database Service, which confi...	Started	Automatic	Local System
DefWatch		Started	Automatic	Local System
DHCP Client	Manages network configuration by registering and updating IP addresses an...	Started	Automatic	Local System
Distributed Link Tracking Client	Maintains links between NTFS files within a computer or across computers in ...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinates transactions that span multiple resource managers, such as dat...		Manual	Network Service
DNS Client	Resolves and caches Domain Name System (DNS) names for this computer. I...	Started	Automatic	Network Service
Error Reporting Service	Allows error reporting for services and applictions running in non-standard e...	Started	Automatic	Local System
Event Log	Enables event log messages issued by Windows-based programs and compo...	Started	Automatic	Local System
Fast User Switching Compatibility	Provides management for applications that require assistance in a multiple us...		Manual	Local System
Help and Support	Enables Help and Support Center to run on this computer. If this service is st...	Started	Automatic	Local System
Human Interface Device Access	Enables generic input access to Human Interface Devices (HID), which activ...		Disabled	Local System
IMAPI CD-Burning COM Service	Manages CD recording using Image Mastering Applications Programming Inte...		Manual	Local System
Indexing Service	Indexes contents and properties of files on local and remote computers; pro...		Manual	Local System
Internet Connection Firewall (ICF) / Int...	Provides network address translation, addressing, name resolution and/or in...		Manual	Local System
iPod Service	iPod hardware management services	Started	Manual	Local System
IPSEC Services	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP s...	Started	Automatic	Local System
IPv6 Internet Connection Firewall	Provides intrusion prevention service for a home or small office network.		Manual	Local System
Logical Disk Manager	Detects and monitors new hard disk drives and sends disk volume informatio...		Manual	Local System
Logical Disk Manager Administrative Ser...	Configures hard disk drives and volumes. The service only runs for configura...		Manual	Local System
Machine Debug Manager	Manages local and remote debugging for Visual Studio debuggers	Started	Automatic	Local System
Messenger	Transmits net send and Alerter service messages between clients and server...	Started	Automatic	Local System
MS Software Shadow Copy Provider	Manages software-based volume shadow copies taken by the Volume Shado...		Manual	Local System
Net Logon	Supports pass-through authentication of account logon events for computer...		Manual	Local System
NetMeeting Remote Desktop Sharing	Enables an authorized user to access this computer remotely by using NetMe...		Manual	Local System
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which yo...	Started	Manual	Local System

Secure Configuration

Windows Security Center

Use the Security Center in Windows (Vista, Windows7 and Server 2008) to check or change security options.



Security essentials

To help protect your computer, make sure the four security essentials below are marked On or OK.

Using Windows Security Center

Firewall: On ●

Automatic updating: Not automatic ●

Automatic updating is set to notify you when updates are available to download and install. Automatically installing updates can enhance the security and performance of your computer.

Change settings...

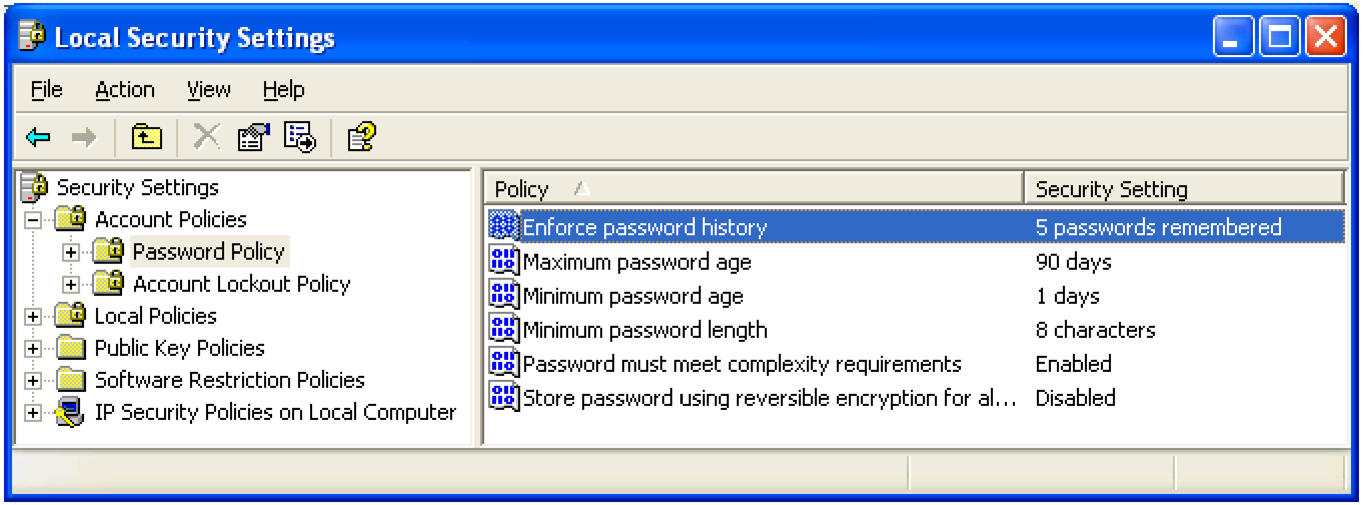
How does automatic updating help protect my computer?

Malware protection: On ●

Other security settings: OK ●

Windows Password Policy

- Configured in:
  - Local Security Policy (individual host)
  - Local Group Policy Object (individual host – alternate method)
  - Group Policy (domain-wide)



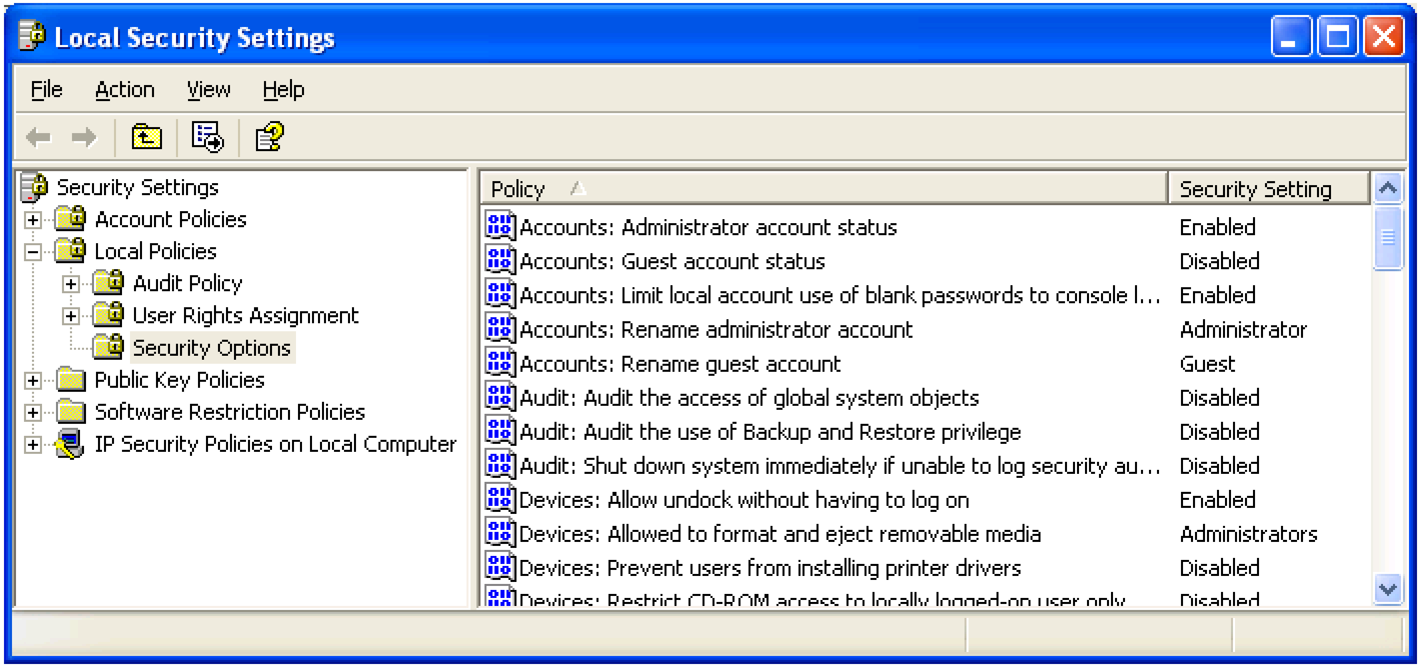
Policy	Security Setting
Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for al...	Disabled

Password Policy

- Enforce password history (at least 5)
  - Prevent reuse of same password
- Maximum password age (90 days max)
  - Limits ability to compromise password
- Minimum password age (1 day)
  - Prevent cycling back to favorite password
- Minimum password length (8 characters)
  - Limits guessing/cracking
- Store password using reversible encryption
  - Disabled – forces use of one-way hash for storage
- Passwords must meet complexity requirements
  - Enabled – forces use of “strong” passwords

Use Security Configuration Tools

- GUI tools to allow **direct** configuration of local security settings, including many registry settings



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Public Key Policies
  - Software Restriction Policies
  - IP Security Policies on Local Computer

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console l...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security au...	Disabled
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled

Security Configuration Tool Set

- Two components:
  - **Security Templates:** policy files used to define a wide range of security settings
  - **Security Configuration and Analysis:** database and related tools allow you to automatically:
    - **Compare (audit)** security settings
    - **Configure (apply)** security settings
- Built-in to Windows 2000 and later
- Can be downloaded for NT

Local Security Policy Pros/Cons

Pros:

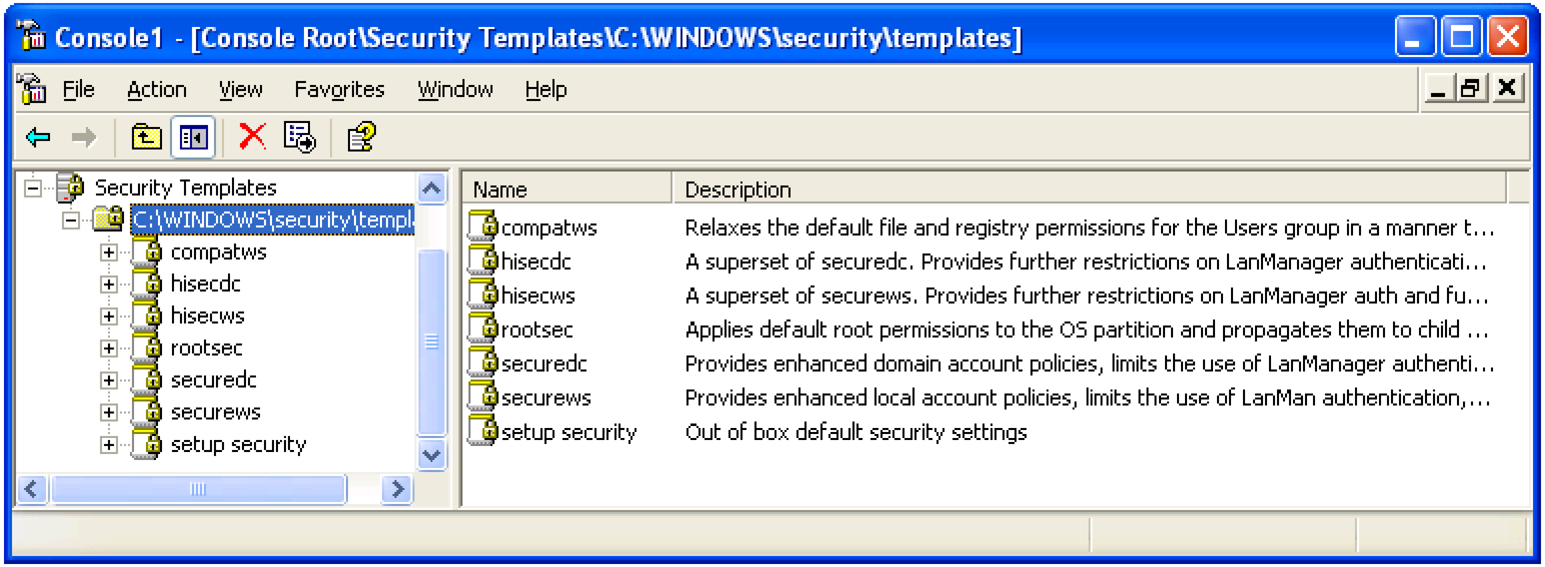
- Simplifies configuration of key security options
- Direct changes to system (reboot may be needed)
- Works best for manual configuration of a small number of hosts

Cons:

- Cannot be used on remote hosts
- No way to automate
- Does not scale well for large number of hosts
- No way to ensure settings remain as configured

Security Templates

- Numerous built-in templates: basic, compatible, secure, high security…
- Third-party templates: NSA, Center for Internet Security…



Console1 - [Console Root\Security Templates\C:\WINDOWS\security\templates]
File
Action
View
Favorites
Window
Help

Security Templates
- C:\WINDOWS\security\templ
  - compatws
  - hisecdc
  - hisecws
  - rootsec
  - securedc
  - securews
  - setup security

Name	Description
compatws	Relaxes the default file and registry permissions for the Users group in a manner t...
hisecdc	A superset of securedc. Provides further restrictions on LanManager authenticati...
hisecws	A superset of securews. Provides further restrictions on LanManager auth and fu...
rootsec	Applies default root permissions to the OS partition and propagates them to child ...
securedc	Provides enhanced domain account policies, limits the use of LanManager authenti...
securews	Provides enhanced local account policies, limits the use of LanMan authentication,...
setup security	Out of box default security settings

What Can I Configure?

- Almost everything related to security!
  - Miscellaneous registry-based security settings
  - Account Policies
  - Local Policies
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System

Group Policies

- Group Policy Objects stored in:
  - Active Directory (Group Policy Container – GPC)
    - Replicated by Active Directory so you need a DOMAIN environment
- GPO linked to container applies to all computers and users in that container
  - Does not apply to groups
- With GPOs you can control what functions the computers in your network have access to, and what the users will be able to do once they log in
- For example, if you want to restrict users from running software on their machines – use Group Policy

Group Policy Computer Administrative Templates

- Use group policy administrative templates to control
- Windows Components
  - NetMeeting, Internet Explorer, Task Scheduler, Windows Installer
- System
  - Logon, Disk Quotas, DNS Client, Group Policy, Windows File Protection
- Network
  - Offline Files, Network and Dial Up Connections
- Printers

User Administrative Templates

- Windows Components
  - NetMeeting, Internet Explorer, Windows Explorer, MMC, Task Scheduler, Windows Installer
- Start Menu and Taskbar
- Desktop
  - Active Desktop, Active Directory
- Control Panel
  - Add/remove programs, display, printers, regional options
- Network
  - Offline files, network and dial-up connections
- System
  - Logon/logoff, Group Policy

Group Policy Recommended Practices

- Plan your Active Directory structure carefully
- Set **least** restrictive policy at higher levels
  - Get more restrictive as you move down the hierarchy
- Group computers and users in separate containers
  - Improves performance
- **Document** your settings!

Delegation of Control

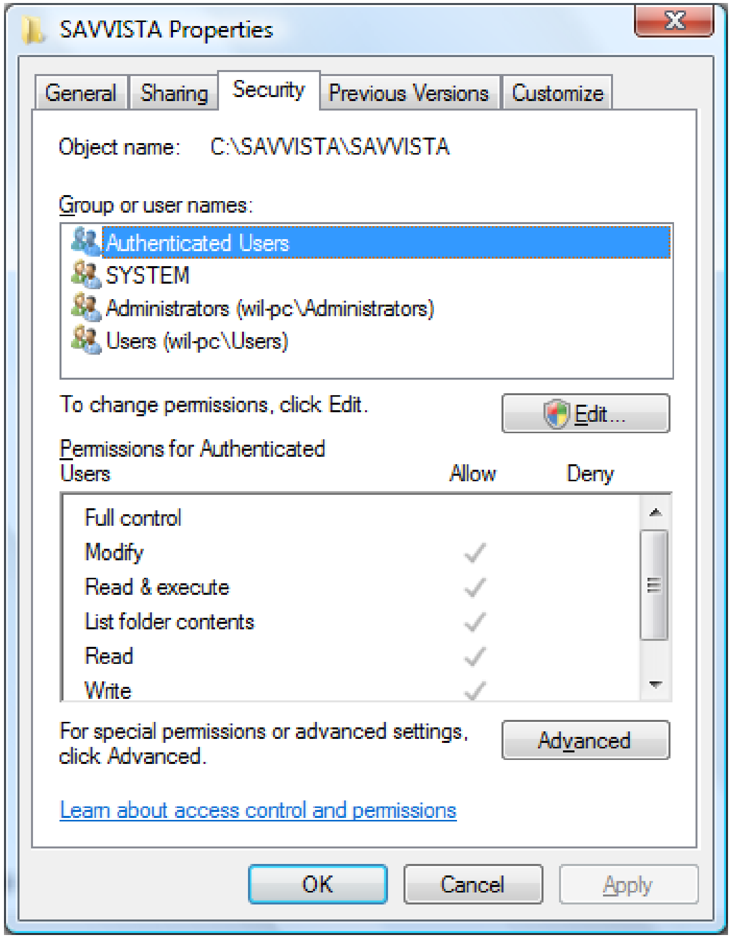
- One of Active Directory’s strengths is the ability to delegate administrative tasks
- Delegation of Control Wizard is used to:
  - Simplify modification of permissions on a given container
  - Assign responsibility for some/all container objects to users or groups

NTFS Permissions

- Strictly speaking, applies to file and directory permissions
  - Only available on NTFS-formatted drives
- Permissions also apply to other resources
  - Printers
  - Services
  - Active Directory objects and individual object properties
  - Registry keys
- Permissions options vary depending on nature of object

Basic File and Directory Permissions

- List folder contents (directories only)
- Read & execute
- Write
- Modify
- Full control
- **Deny Permissions always overrides Allow Permissions**



SAVVISTA Properties

Object name: C:\SAVVISTA\SAVVISTA

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (wil-pc\Administrators)
- Users (wil-pc\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

NTFS Permissions versus Share Permissions

NTFS Permissions

- Apply to **all** users (local and network)
- Very granular control over permissions
- NTFS permissions are **cumulative** – total of all permissions for user/groups

Share Permissions

- Apply to **network** users **only**
- No granular control (Read/Modify/Full)
- Share permissions are **cumulative** – total of all permissions for user/groups

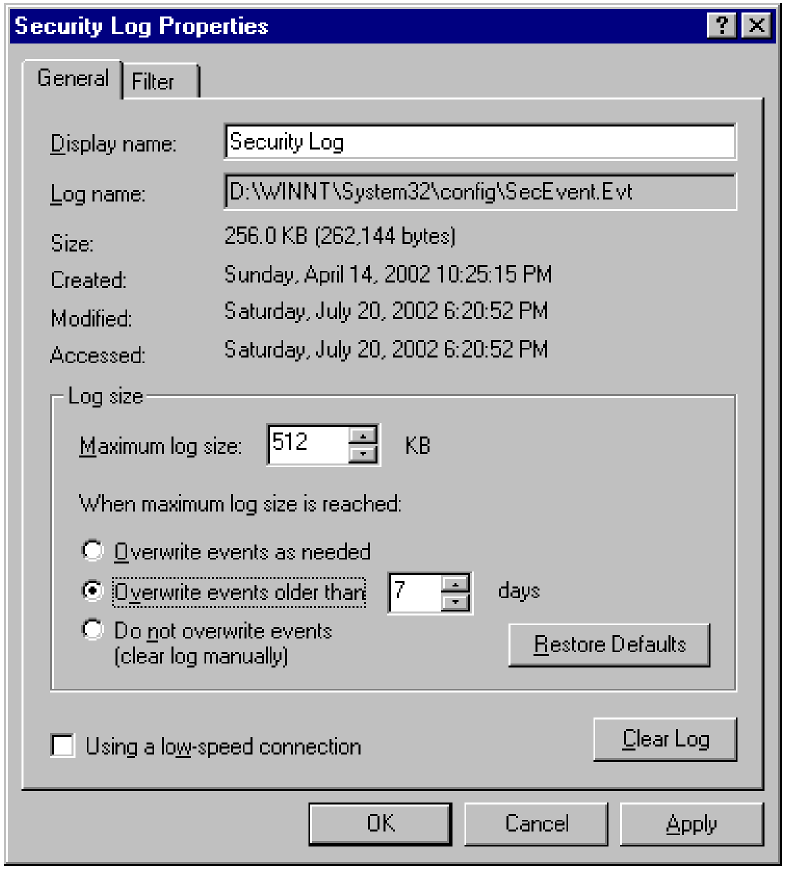
Logging/Event Viewer

Event Viewer

- Primary logging and auditing tool is Event Viewer
  - Binary log format (.evt)
  - %systemroot%\system32\config
- Manages the following logs:
  - System
  - Application
  - Security
  - Directory Services (DC only)
  - File Replication (DC only)
  - DNS (DNS server only)

Configuring Event Viewer

- Log file location
  - %systemroot%\system32\config by default
- Log file size
  - 512KB default
  - Too small for most needs
- Log file wrapping options
  - Overwrite after 7 days by default
- Restrict Guest Access



Security Log Properties

General | Filter

Display name: Security Log

Log name: D:\WINNT\System32\config\SecEvent.Evt

Size: 256.0 KB (262,144 bytes)

Created: Sunday, April 14, 2002 10:25:15 PM

Modified: Saturday, July 20, 2002 6:20:52 PM

Accessed: Saturday, July 20, 2002 6:20:52 PM

Log size

Maximum log size: 512 KB

When maximum log size is reached:

○ Overwrite events as needed

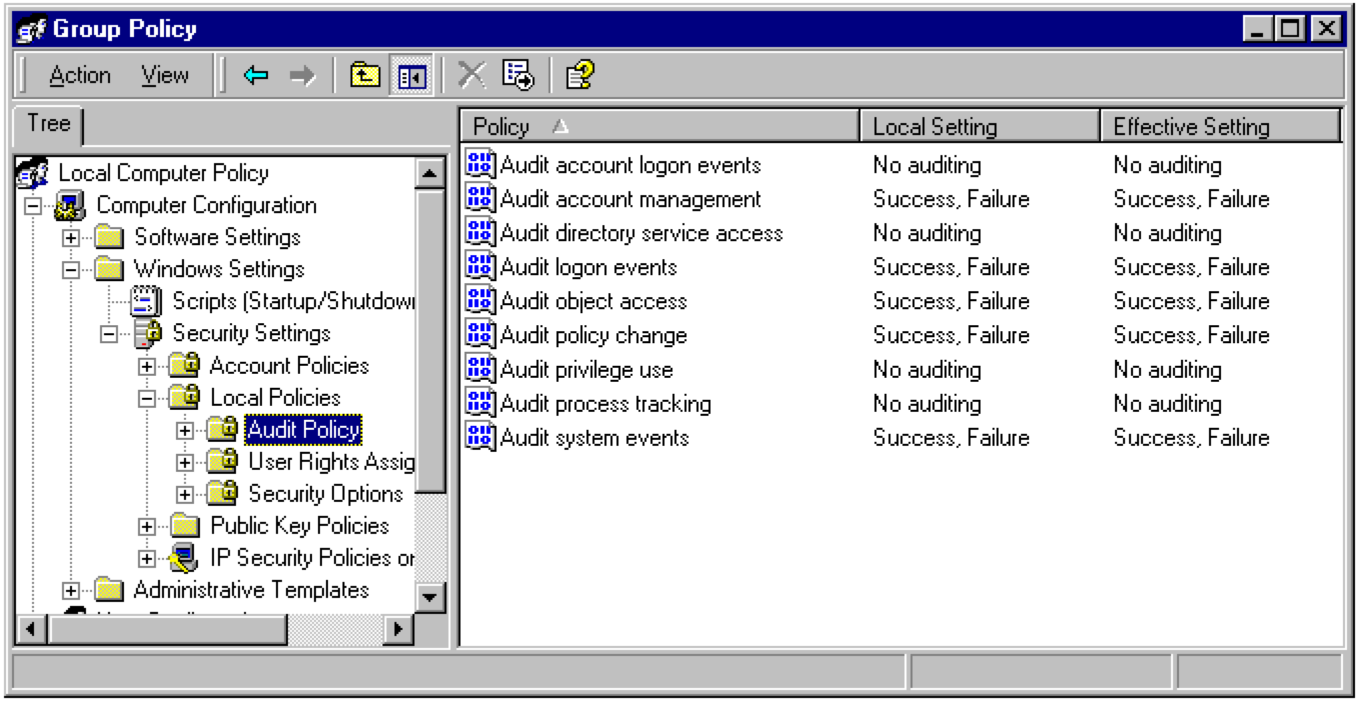
● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

Configuring Auditing

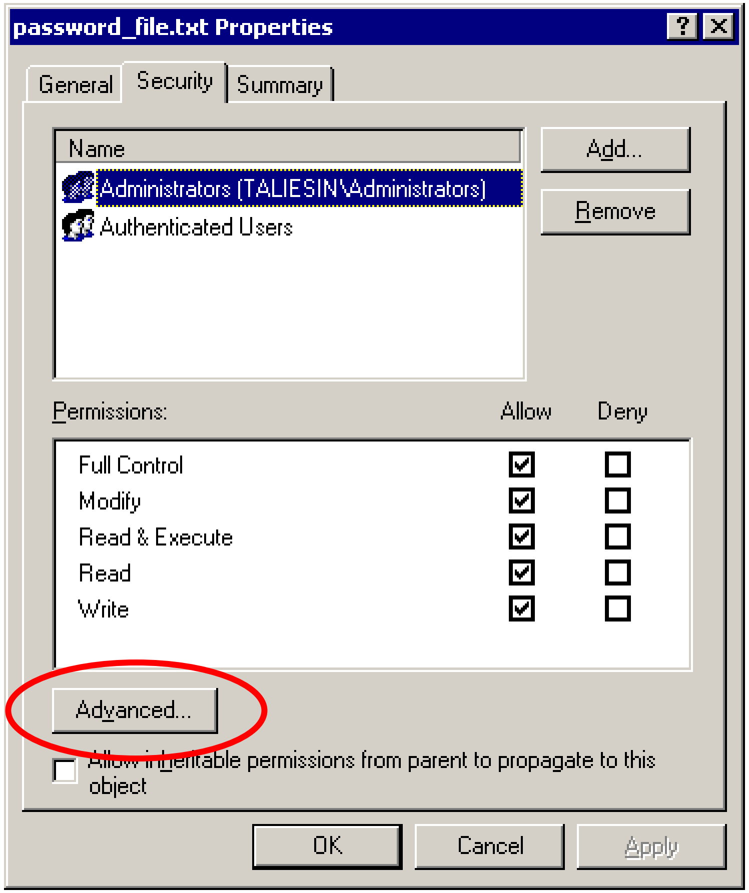
- Via Group Policy or security templates



Policy	Local Setting	Effective Setting
Audit account logon events	No auditing	No auditing
Audit account management	Success, Failure	Success, Failure
Audit directory service access	No auditing	No auditing
Audit logon events	Success, Failure	Success, Failure
Audit object access	Success, Failure	Success, Failure
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	Success, Failure	Success, Failure

Configuring Object Auditing

- Simply enabling object auditing will not audit any objects
- Must specify objects
  - Files/directories
  - Printers
  - Registry keys
- Must set audit parameters
- System Access Control List (SACL) = list of audit entries associated with object



password_file.txt Properties

Name

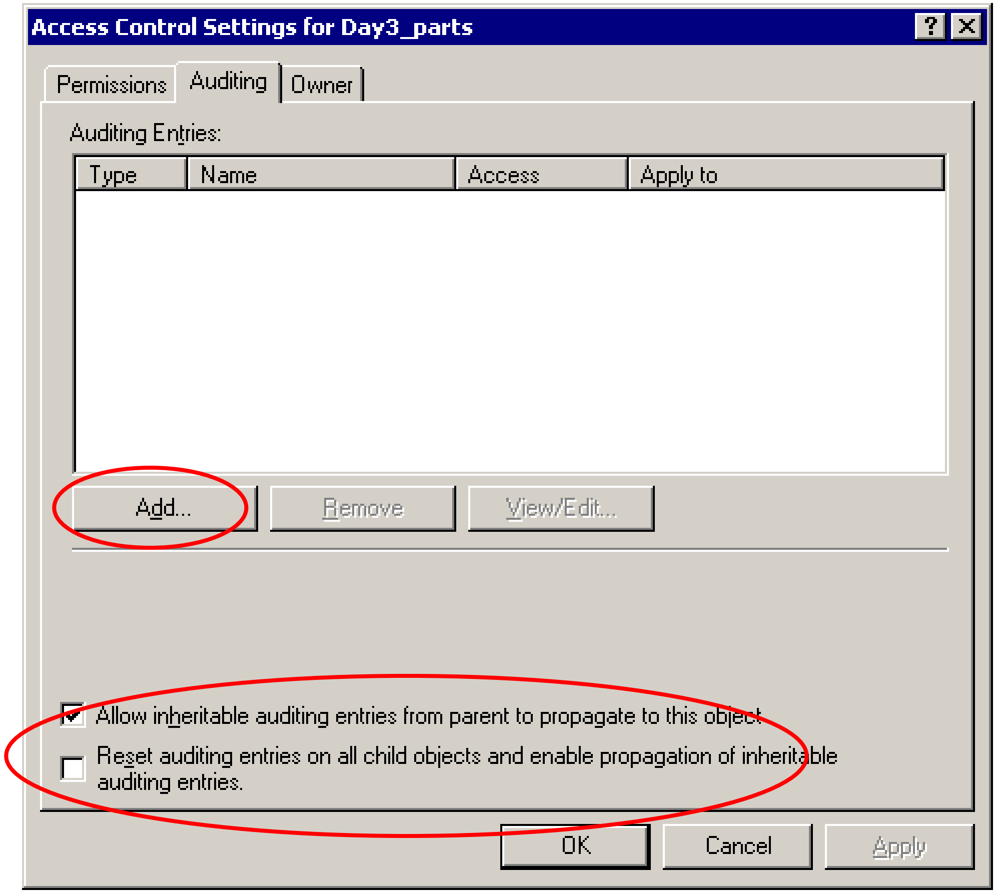
- Administrators (TALIESIN\Administrators)
- Authenticated Users

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

Adding Users/Groups

- SACL is blank by default
  - Click Add to select users/groups
- Objects will inherit SACL entries by default

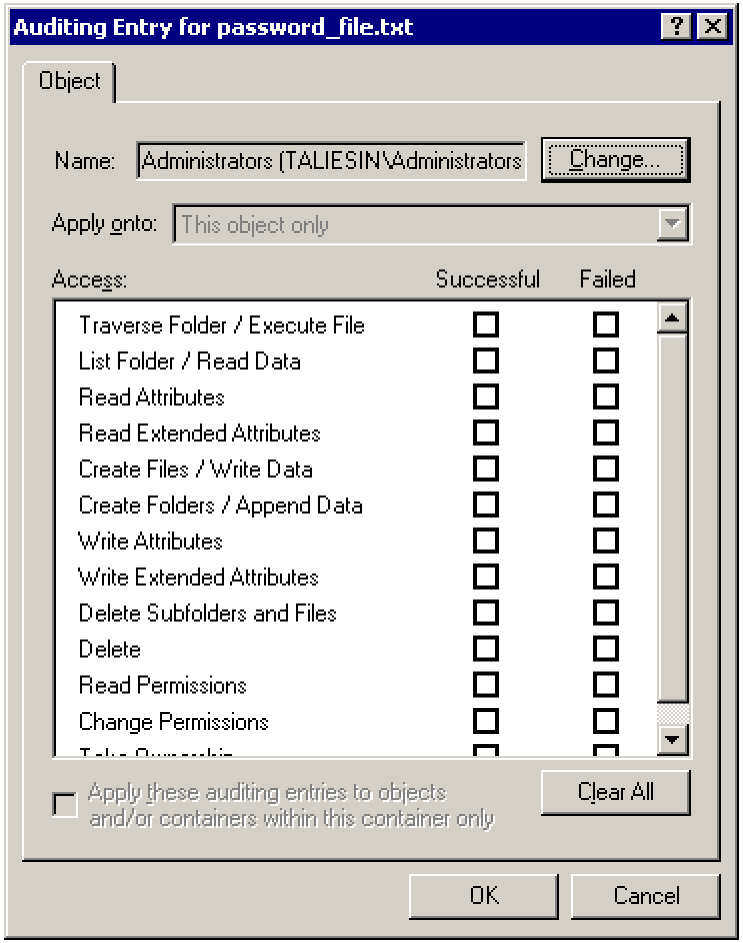


☑ Allow inheritable auditing entries from parent to propagate to this object

□ Reset auditing entries on all child objects and enable propagation of inheritable auditing entries.

Setting SACLs

- Specify users and/or groups to audit
- Specify types of access to audit for each user/group
- Specify successful/failed or both
- Specify based on advanced permissions



Auditing Entry for password_file.txt

Name: Administrators (TALIESIN\Administrators

Apply onto: This object only

Access:	Successful	Failed
Traverse Folder / Execute File	□	□
List Folder / Read Data	□	□
Read Attributes	□	□
Read Extended Attributes	□	□
Create Files / Write Data	□	□
Create Folders / Append Data	□	□
Write Attributes	□	□
Write Extended Attributes	□	□
Delete Subfolders and Files	□	□
Delete	□	□
Read Permissions	□	□
Change Permissions	□	□
Take Ownership	□	□

□ Apply these auditing entries to objects and/or containers within this container only

Recommended Logging Practices

- Enable auditing/logging
- Review logs (manually or via scripts) regularly
- Copy logs to a remote, secure server on a regular basis
  - Write to secure server in real time if possible
- Backup logs regularly
- Archive and retain logs

Guides for Hardening Windows

- Microsoft
  - General guidance, common criteria…
- National Security Agency (NSA)
  - Numerous guides and templates
- Center for Internet Security (minimum security)
  - Minimum templates and scanning auditing tools
- Defense Information Systems Agency (DISA)
  - Security Technical Implementation Guides (STIGs)
- If your systems must be certified/accredited (C&A), using an industry standard may help the process!

Bottom Line

Follow these simple security tips to secure Windows

You never can be totally secure,
but you can come pretty close…

Attribution and Trademark Statements

Belarc and Belarc Advisor are registered trademarks of Belarc, Inc.

Microsoft, Windows, and Microsoft Baseline Security Analyzer are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

Shavlik NetChk Protect, Shavlik HFNetChkPro Plus, Shavlik NetChk Limited, Shavlik NetChk Agent, Shavlik NetChk Tracker, and Shavlik NetChk Configure are registered trademarks of Shavlik Technologies.

UNIX is a registered trademark of The Open Group in the U.S. and other countries.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.