

# Windows Server 2003 Hardening Checklist

## Introduction:

This checklist contains server hardening procedures that balance industry best practices with the unique requirements of UCDHSC's environment. Since Windows Server 2003 does not come configured securely out of the box it is necessary to follow these steps to prevent attacks from exploiting known vulnerabilities. These steps should be followed to secure a typical UCDHSC Windows 2003 server, but may not be appropriate in all cases. In cases where an exception must be made, documentation should be retained on this worksheet describing the reason for the exception and any mitigating actions. In all cases, this worksheet should be retained for future reference.

## Procedure:

- ❑ Install the latest Service Pack from <http://windowsupdate.microsoft.com>.  
Each Service Pack for Windows includes all security fixes from previous Service Packs. Keep up to date on Service Pack releases and install the correct Service Pack for your servers as soon as operational circumstances allow.
- ❑ Install the appropriate post-Service Pack security hotfixes from <http://windowsupdate.microsoft.com>.  
Microsoft issues security bulletins through its Security Notification Service. When these bulletins recommend installation of a security hotfix, you should immediately download and test the hotfix, then install it on your member servers as soon as operational circumstances allow.
- ❑ Configure local accounts.
  - Make sure the local Guest account is disabled. This is the default in Windows Server 2003.
  - Enable account lockout on the local administrator account (this still needs to be done using passprop on Win Srvr 2003)
  - Rename the local Administrator account to something other than Administrator.
  - Ensure that the local Administrator password meets the following criteria:
    - It contains at least eight alphanumeric characters.
    - It contains both upper and lower case characters.
    - It has digits and punctuation characters as well as letters.
    - It is not a word in any language, slang, dialect, jargon, etc.
    - It isn't based on personal information.

Make sure that Domain Admins are members of the Local Administrators group.

- Disable or delete unnecessary accounts.
  - Review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, disabling any non-active accounts, and deleting accounts that are no longer required, including duplicate user accounts, test accounts, shared accounts, and general departmental accounts.
  - Use group policies to assign permissions as needed.
- ❑ Disable unnecessary services.
  - After installing Windows 2003 Server, disable any network services not required for the server role. In particular, consider whether the server should be running the Server service for file and print sharing.
  - Also avoid installing applications on the server unless they are absolutely necessary to the server's function. For example, don't install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.
  - If SNMP is enabled, there must be no R/W community string, and the RO community string must be set to something other than "public." When choosing an SNMP community string, follow the same guidelines as choosing a complex password.
- ❑ Set stronger password policies.
  - Use the Domain Security Policy (or Local Security Policy) snap-in to strengthen the system policies for password acceptance, including:
    - Set the minimum password length to at least eight characters.



- Set a minimum password age
- Set a maximum password age
- Set a password history maintenance
- Enable password complexity.
- Local Security Policy -> Security Settings -> Account Policies -> Password Policy:

<b>Password Setting</b>	<b>Recommended Settings</b>
Enforce password history	12
Maximum password age	< 90
Minimum password age	2
Minimum password length	8
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

**Note:** Increase the log size from the 16384k default to at least 81920k.

- ❑ Prevent the last logged-in user name from being displayed.

The login dialog box makes it easier to discover a user name that can later be employed in a password-guessing attack. Disable this feature using the security templates provided on the installation CD, or via Group Policy snap-in.

*Local Security Policy* → *Security Settings* → *Local Policies* → *Security Options* → *Domain Member: Do not display last username*

- ❑ Configure a strong audit policy. Successful and failed logins, as well as privilege use, should be logged and monitored to detect any unauthorized activity. Applied Trust suggests the following Auditing settings:

<b>Audit Policy</b>	<b>Recommended Settings</b>
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	No auditing

- ❑ Install antivirus software and updates. Make sure file scanning is enabled and automatic definition updates are configured.
- ❑ Configure appropriate settings for access control on file shares, given that permissions are set through NTFS security.
  - All folders and files should be secured with standard NTFS settings. Minimum access rules should apply such that groups are created that allow the minimum number of users to have write access.
  - Where possible, the “Everyone” setting should be removed and replaced with user groups.
  - Once NTFS settings have been applied, then the most efficient share setting is to give all Authenticated Users full control access.



- ❑ Disable the autorun feature on the CD-ROM drive
  - Run the Registry Editor (REGEDIT.EXE).
  - Navigate to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom**.
  - Double-click the **Autorun** value, and type **0** for its value. (If it's not there, create it by selecting Edit -> New -> DWORD Value, and typing "Autorun" for its name.)
  - You may have to log out and then log back in for this change to take effect.
  - *Note: With this solution, Windows will no longer be notified when you insert a new CD. To make sure the correct icon and title for the current CD are displayed in **My Computer** and **Explorer**, press F5 to refresh the window.*
  
- ❑ Protect the registry from anonymous access
  - In the registry subkey HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\RPC, select one of the following values:
    - 1 - This default setting permits access to interfaces only by using authenticated connections, unless those connections specifically request to be exempt from this requirement. (Note: This exemption is required for some DCOM scenarios.)
    - 2 - This setting permits remote access to interfaces only by using authenticated connections. This setting does not permit exceptions to the authentication requirement.
  
- ❑ Ensure users have the correct level of debugging access. This can be done through:
  - ❑ The control panel of each machine
  - ❑ The platform SDK (SeDebugPrivilege)
  
- ❑ Set up the event logs.
  - GPO\_name\Computer Configuration\Windows Settings\Security Settings\Event Log\
    - Maximum application log size: 16384 KB
    - Maximum security log size: 16384 KB
    - Maximum system log size: 16384 KB
    - Prevent local guests group from accessing application log: enabled
    - Prevent local guests group from accessing security log: enabled
    - Prevent local guests group from accessing system log: enabled
    - Retain application log: Not defined
    - Retain security log: Not defined
    - Retain system log: Not defined
    - Retention method for application log: Overwrite as needed
    - Retention method for security log: Overwrite as needed
    - Retention method for system log: Overwrite as needed
  
- ❑ Once the server has been built, create a Level 0/Full backup of all drives and the System State. This backup should be stored for the life of the machine as a forensic baseline in case of a security incident. Additional Level 0 backups should be created and stored for the machine's lifetime upon major system upgrades.

