Windows Security Checklist

This document is a checklist of the security options for a Windows server implementation. The options are based on Windows 2003 functionality, but many of the checks are also valid for Windows 2000.

Table of Contents

Password Policy

Password Policy	Default	Member Server	High Security	Domain Controller
Enforce password history	24	≥ 10	≥ 10	≥ 10
Maximum password age	42 days	• ≤ 30 days for administrator accounts • ≤ 90 days for Faculty and staff accounts • ≤ 180 days for student accounts	• ≤ 30 days for administrator accounts	• ≤ 30 days for administrator accounts • ≤ 90 days for Faculty and staff accounts • ≤ 180 days for student accounts
Minimum password age	1 day	≥ 1 day	≥ 1 day	≥ 1 day
Minimum password length	7 characters	≥ 8 characters	≥ 8 characters	≥ 8 characters
Password must meet complexity requirements	Disabled	Enabled, but use custom passfilt.dll to require alpha & numeric	Enabled, but use custom passfilt.dll to require alpha & numeric	Enabled, but use custom passfilt.dll to require alpha & numeric

Account lockout policy

Account Lockout Policy	Default	Member Server	High Security	Domain Controller
Account lockout duration	Not Defined	≥ 1 hour	≥ 1 hour	≥ 1 hour
Account lockout threshold	0 invalid login attempts	Between 5 and 10 invalid login attempts	Between 5 and 10 invalid login attempts	Between 5 and 10 invalid login attempts
Reset account lockout counter after	Not Defined	Between 15 minutes and 1 hour	Between 15 minutes and 1 hour	Between 15 minutes and 1 hour

Kerberos Policy

In most environments, these settings should not need to be changed.

Audit Policy

Audit Policy	Default	Member Server	High Security	Domain Controller
Audit account logon events	Success	Success, Failure	Success, Failure	Success, Failure
Audit account management	No Auditing	Success, Failure	Success, Failure	Success, Failure
Audit directory service access	No Auditing	Success, Failure	Success, Failure	Success, Failure
Audit logon events	Success	Success, Failure	Success, Failure	Success, Failure
Audit object access	Success	Success, Failure	Success, Failure	Success, Failure
Audit policy change	No Auditing	Success	Success	Success
Audit privilege use	No Auditing	Failure	Success, Failure	Failure
Audit system events	No Auditing	Success	Success	Success

User Rights Assignments

User Rights Assignments	Default	Member Server	High Security	Domain Controller
Access this computer from the network	Administrators, Backup Operators, Everyone, Power Users, and Users	Depending on your requirements • Defaults settings (Not Defined) • Administrators, Backup Operators, Power Users, and Users	Administrators, Authenticated Users	Administrators, Backup Operators, Power Users, and Users
Act as part of the operating system	Not Defined	Not Defined	No One	Not Defined

User Rights Assignments	Default	Member Server	High Security	Domain Controller
Add workstations to domain	Not Defined	Not Defined	Administrators	Depending on your requirements: Administrators
Adjust memory quotas for a process	Administrators, NETWORK SERVICE, LOCAL SERVICE	Not Defined	Not Defined	Not Defined
Allow log on locally	Administrators, Backup Operators, Power Users, Users	Not Defined	Administrators	Not Defined
Allow log on through Terminal Services	Administrators and Remote Desktop Users	Not Defined	Administrators	Administrators
Change the system time	Administrators and Power Users	Not Defined	Administrators	Administrators
Debug programs	Administrators	Not Defined	No One	Not Defined
Deny access to this computer from the network	SUPPORT_388945a0	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts
Deny log on through Terminal Services	Not Defined	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts
Enable computer and user accounts to be trusted for delegation	Not defined	Not defined	No One	No One
Impersonate a client after authentication	SERVICE, Administrators	Not defined / Default	Local Service; Network Service	Not defined / Default
Lock pages in memory	Not defined	Not defined	Administrators	Not defined
Log on as a batch job	SUPPORT_388945a0, LOCAL SERVICE	Not defined	No One	Not defined
Profile single process	Administrators, Power Users	Not defined / Default	Administrators	Administrators
Remove computer from docking station	Administrators, Power Users	Not defined / Default	Administrators	Administrators

User Rights Assignments	Default	Member Server	High Security	Domain Controller
Restore files and directories	Administrators, Backup Operators	Not defined / Default	Administrators	Not defined / Default
Shut down the system	Backup Operators, Power Users, Administrators	Not defined / Default	Administrators	Not defined / Default
Synchronize directory service data	Not Defined	Not defined	No One	Not defined

Security Options

The Security Options section of Group Policy is used to configure security settings for computers, such as digital signing of data, administrator and guest account names, floppy disk drive and CD – ROM drive access, driver installation behavior, and logon prompts.

Security Options	Default	Member Server	High Security	Domain Controller
Devices: Allow undock without having to log on	Enabled	Disabled	Disabled	Disabled
Devices: Restrict CD – ROM access to locally logged – on user only	Disabled	Not Defined/ Default	Enabled	Enabled
Devices: Restrict floppy access to locally logged – on user only	Disabled	Not Defined/ Default	Enabled	Enabled
Domain controller: Allow server operators to schedule tasks	Not Defined	Disabled	Disabled	Disabled
Domain controller: LDAP server signing requirements	Not Defined	Not Defined	Require signing if possible	Require signing if possible
Domain controller: Refuse machine account password changes	Not Defined	Disabled	Disabled	Disabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Disabled	Enabled if possible	Enabled if possible
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Enabled	Enabled	Enabled
Interactive logon: Do not display last user name	Disabled	Enabled	Enabled	Enabled

Security Options	Default	Member Server	High Security	Domain Controller
Interactive logon: Message text for users attempting to log on	Not Defined	Define – MnSCU Standard, "A log-on banner informing users as to authorizations, recourse, and privacy shall be presented on each log-on attempt."	Define – MnSCU Standard, "A log-on banner informing users as to authorizations, recourse, and privacy shall be presented on each log-on attempt."	Define – MnSCU Standard, "A log-on banner informing users as to authorizations, recourse, and privacy shall be presented on each log-on attempt."
Interactive logon: Message title for users attempting to log on	Not Defined	Define – Text should be a warning	Define – Text should be a warning	Define – Text should be a warning
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10	1	0	0
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Disabled	Enabled	Enabled
Interactive logon: Smart card removal behavior	No Action	Not Defined (Unless smart cards are being used)	Not Defined (Unless smart cards are being used)	Not Defined (Unless smart cards are being used)
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled if possible	Enabled if possible	Enabled if possible
Microsoft network server: Digitally sign communications (always)	Disabled	Disabled	Enabled if possible	Enabled if possible
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Enabled	Enabled	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	Enabled	Enabled	Enabled
Network access: Named Pipes that can be accessed anonymously	Not Defined	None	None	None

Security Options	Default	Member Server	High Security	Domain Controller
Network access: Remotely accessible registry paths	System\ CurrentControlSet\ Control\ ProductOptions; System\ CurrentControlSet\ Control\ Server Applications; Software\ Microsoft\ Windows NT\ Current Version	Not Defined / Default	None	None
Network access: Remotely accessible registry paths and sub – paths	System\ CurrentControlSet\ Control\ Print\ Printers; System\ CurrentControlSet\ Services\ Eventlog; Software\ Microsoft\ OLAP Server; Software\ Microsoft\ Windows NT\ CurrentVersion\ Print; Software\ Microsoft\ Windows NT\ CurrentVersion\ Windows; System\ CurrentControlSet\ Control\ ContentIndex; System\ CurrentControlSet\ Control\ Terminal Server; System\ CurrentControlSet\ Control\ Terminal Server\ UserConfig; System\ CurrentControlSet\ Control\ Terminal Server\ DefaultUserConfiguration; Software\ Microsoft\ Windows NT\ CurrentVersion\ Perflib; System\ CurrentControlSet\ Services\ SysmonLog	Not Defined / Default	None	None
Network access: Shares that can be accessed anonymously	COMCFG,DFS$	None	None	None
Network access: Sharing and security model for local accounts	Classic – local users authenticate as themselves	Not Defined / Default	Not Defined / Default	Not Defined / Default
Network security: Do not store LAN Manager hash value on next password change	Disabled	Enabled	Enabled	Enabled

Security Options	Default	Member Server	High Security	Domain Controller
Network Security: Force Logoff when Logon Hours expire	Disabled	Enabled	Enabled	Enabled
Network security: LAN Manager authentication level	Send NTLM response only	Send NTLMv2 responses only	Send NTLMv2 response only\ refuse LM & NTLM	If possible: Send NTLMv2 response only\refuse LM & NTLM
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum	No minimum	Enabled all settings	Enabled all settings
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum	No minimum	Enabled all settings	Enabled all settings
Shutdown: Clear virtual memory page file	Disabled	Disabled	Enabled	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined	User is prompted when the key is first used	If feasible: User must enter a password each time they use a key	User is prompted when the key is first used
System objects: Default owner for objects created by members of the Administrators group	Administrators group	Object creator	Object creator	Object creator
System settings: Optional subsystems	POSIX	None	None	None

Event Log

Log File Setting	Default	Member Server	High Security	Domain Controller
Maximum security log size	16,384 KB	≥100,000 KB	≥100,000 KB	≥100,000 KB

System Services

Service	Default	Member Server	High Security	Domain Controller
Application Layer Gateway Service (ALG)	Manual	Disabled	Disabled	Disabled
Application Management (AppMgmt)	Manual	Disabled	Disabled	Disabled
Automatic Updates (wuauserv)	Automatic	Automatic – Depending on your configuration	Automatic – Depending on your configuration	Automatic – Depending on your configuration
COM+ System Application (EventSystem)	Manual	Disabled	Disabled	Disabled

Service	Default	Member Server	High Security	Domain Controller
Distributed File System (Dfs)	Automatic	Disabled	Disabled	Automatic
Distributed Link Tracking Client (TrkWks)	Automatic	Disabled	Disabled	Disabled
Distributed Link Tracking Server (TrkSvr)	Manual	Disabled	Disabled	Automatic
Distributed Transaction Coordinator (MSDTC)	Automatic	Disabled	Disabled	Disabled
DNS Server (DNS)	Not Installed	Not Installed	Not Installed	Automatic
Error Reporting Service (ERSvc)	Automatic	Disabled	Disabled	Automatic
File Replication Service (NtFrs)	Manual	Disabled	Disabled	Automatic
FTP Publishing Service (MSFtpsvc)	Not Installed	Not Installed unless server is a FTP server	Not Installed unless server is a FTP server	Not Installed
Help and Support (helpsvc)	Automatic	Disabled	Disabled	Disabled
HTTP SSL (HTTPFilter)	Manual	Disabled	Disabled	Disabled
IIS Admin Service (IISADMIN)	Not Installed	Not Installed unless server is an IIS web server	Not Installed unless server is an IIS web server	Not Installed
Intersite Messaging (IsmServ)	Disabled	Disabled	Disabled	Automatic
Logical Disk Manager (dmserver)	Automatic	Manual	Manual	Manual
NT LM Security Support Provider (NtLmSsp)	Not Installed	Automatic	Automatic	Automatic
Portable Media Serial Number Service (WmdmPmSN)	Manual	Disabled unless the server is a print server	Disabled	Disabled
Print Spooler (Spooler)	Automatic	Disabled unless the server is a print server	Disabled	Disabled
Remote Access Auto Connection Manager (RasAuto)	Manual	Disabled	Disabled	Disabled
Remote Access Connection Manager (RasMan)	Manual	Disabled	Disabled	Disabled
Remote Administration Service (SrvcSurg)	Not installed	Manual	Manual	Manual
Remote Desktop Help Session Manager (RDSessMgr)	Manual	Disabled	Disabled	Disabled
Remote Procedure Call Locator (RPCLocator)	Manual	Disabled	Disabled	Automatic
Resultant Set of Policy Provider (RsoPProv)	Manual	Disabled	Disabled	Disabled
Secondary Logon (seclogon)	Automatic	Disabled	Disabled	Disabled
Shell Hardware Detection (ShellHWDetection)	Automatic	Disabled	Disabled	Disabled
Smart Card (ScardSvr)	Manual	Disabled	Disabled	Disabled
Special Administration Console Helper (Sacsvr)	Manual	Disabled	Disabled	Disabled
Task Scheduler (Schedule)	Automatic	Disabled	Disabled	Disabled

Service	Default	Member Server	High Security	Domain Controller
Telephony (TapiSrv)	Manual	Disabled	Disabled	Disabled
Terminal Services (TermService)	Manual	Automatic	Consider either Manual or Disabled if you do not use this management protocol.	Consider either Manual or Disabled if you do not use this management protocol.
Uninterruptible Power Supply (UPS)	Manual	Disabled – Depending on your configuration	Disabled – Depending on your configuration	Disabled – Depending on your configuration
Upload Manager (Uploadmgr)	Manual	Disabled	Disabled	Disabled
Virtual Disk Service (VDS)	Manual	Disabled	Disabled	Disabled
Volume Shadow Copy (VSS)	Manual	Disabled	Disabled	Disabled
Windows Internet Name Service (WINS)	Not Installed	Not Installed	Not Installed	Automatic – Depending on your Configuration
WinHTTP Web Proxy Auto-Discovery Service (WinHttpAutoProxySvc)	Manual	Disabled	Disabled	Disabled
Wireless Configuration (WZCSVC)	Automatic on Standard, Enterprise, and Datacenter Server. Manual on Web Server	Disabled	Disabled	Disabled
World Wide Web Publishing Service (W3SVC)	Not Installed	Not Installed unless server is an IIS web server	Not Installed unless server is an IIS web server	Not Installed

Administrative Templates

Disable Automatic Install of Internet Explorer components

Group Policy Value	Default	Setting
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\ Disable Automatic Install of Internet Explorer components	Not Configured	Enabled

Terminal Services: Always prompt client for a password on connection

Group Policy Value	Default	Setting

Group Policy Value	Default	Setting
Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\ Always prompt client for a password on connection	Not Configured	Enabled

Terminal Services: Encryption Levels

Group Policy Value	Default	Setting	Encryption Level
Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\ Encryption Levels	Not Configured	Enabled	High (128 Bit)

System: Turn off Autoplay

Group Policy Value	Default	Setting
Computer Configuration\Administrative Templates\System\Turn off Autoplay	Not Configured	Enabled

Screen Saver: Password protect the screen saver

Group Policy Value	Default	Setting
User Configuration\Administrative Templates\Control Panel\Display\Password protect the screen saver	Not Configured	Enabled

Registry Settings

Security Considerations for Network Attacks

The following registry value entries should be taken into consideration when hardening your server: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters**

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
EnableICMPRedirect	DWORD	1	0
SynAttackProtect	DWORD	0	1
EnablePMTUDiscovery	DWORD	1	0
KeepAliveTime	DWORD	7,200,000	300,000
DisableIPSourceRouting	DWORD	0	2
TcpMaxDataRetransmissions	DWORD	5	3

AFD.SYS settings

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
DynamicBacklogGrowthDelta	DWORD	0	10
EnableDynamicBacklog	DWORD	0	1
MinimumDynamicBacklog	DWORD	0	20
MaximumDynamicBacklog	DWORD	0	20000

Disable Auto Generation of 8.3 File Names: Enable the computer to stop generating 8.3 style filenames

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
NtfsDisable8dot3NameCreation	DWORD	0	1

Disable Autorun: Disable Autorun for all drives

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ Explorer

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
NoDriveTypeAutoRun	DWORD	0	0xFF

Make Screensaver Password Protection Immediate: The time in seconds before the screen saver grace period expires

HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
ScreenSaverGracePeriod	String	5	0

NTFS

NTFS partitions support ACLs at the file and folder levels. This support is not available with the file allocation table (FAT), FAT32, or file systems. FAT32 is a version of the FAT file system that has been updated to permit significantly smaller default cluster sizes and to support hard disks up to two terabytes in size. FAT32 is included in Windows 2000 and Windows 2003

Format all partitions on every server using NTFS. Use the **convert utility** to carefully convert FAT partitions to NTFS, but keep in mind that the convert utility will set the ACLs for the converted drive to **Everyone: Full Control**.

Configure SNMP Community Name

The Simple Network Management Protocol (SNMP) is a network management standard widely used with Transmission Control Protocol/Internet Protocol (TCP/IP) networks. SNMP provides a method of managing network nodes — servers, workstations, routers, bridges, and hubs — from a centrally located host. SNMP performs its management services by using a distributed architecture of management systems and agents. Systems running network management software are referred to as SNMP management systems or SNMP managers. Managed network nodes are referred to as SNMP agents.

The SNMP service provides a rudimentary form of security using community names and authentication traps. You can restrict SNMP communications for the agent and allow it to communicate with only a set list of SNMP management systems. Community names can be used

to authenticate SNMP messages, and thus provide a rudimentary security scheme for the SNMP service. Although a host can belong to several communities at the same time, an SNMP agent does not accept requests from a management system in a community that is not on its list of acceptable community names. There is no relationship between community names and domain names or workgroup names. A community name can be thought of as a password shared by SNMP management consoles and managed computers. It is your responsibility as a system administrator to set hard – to – guess community names when you install the SNMP service.

IIS Configuration

URLScan

UrlScan is a free security tool from Microsoft that restricts the types of HTTP requests that Internet Information Services (IIS) will process. By blocking specific HTTP requests, the UrlScan security tool helps prevent potentially harmful requests from reaching the server.

URLScan can be downloaded from:
http://www.microsoft.com/downloads/details.aspx?familyid=23d18937-dd7e-4613-9928-7f94ef1c902a&displaylang=en

The following table details the capabiliities of URLScan version 2.5 and native IIS6.0 capabilities.

UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
DenyExtensions: This feature was implemented in UrlScan to limit the attack surface of the server by preventing, based on file name extensions, specific requests from running ISAPI or CGI code on the server.	IIS 6.0 limits the attack surface of the server by allowing administrators to specify the ISAPI and CGI code that can run on the server. Because IIS 6.0 specifies the code directly, it is not necessary to know which file extensions in the URL are capable of invoking the code.	Consider deny the following extensions: .cer, .cdx,.asa, .exe, .bat, .cmd, .com, .htw, .ida,.idq, .htr, .idc, .stm, .printer, .ini, .log, .pol, .dat
DenyVerbs: WebDAV code can be invoked on a Web server based on the use of particular HTTP verbs. This feature was implemented in UrlScan to limit the attack surface of the server by preventing requests that would invoke WebDAV.	IIS 6.0 allows administrators to explicitly enable or disable WebDAV. Since this action affects the WebDAV executable code directly, it is not necessary to inspect the HTTP verb that is associated with each request.	At a minimum, deny the following verbs: TRACE/TRACK, DELETE, OPTIONS, PROPFIND
DenyHeaders: WebDAV code can be invoked on a Web server based on the presence of particular HTTP headers. This feature was implemented in UrlScan to limit the attack surface of the server by preventing requests that would invoke WebDAV.	IIS 6.0 allows administrators to explicitly enable or disable WebDAV. Since this action affects the WebDAV executable code directly, it is not necessary to inspect the HTTP header that is associated with each request.	If WebDAV is not required it should be disabled.

UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
NormalizeUrlBeforeScan: This feature allows administrators to specify whether IIS will process the raw URL that is sent by the client or the canonicalized URL that is processed on the server. **Note:** It is not practical to set this value to 0 on a production server. When this value is set to 0, all file name extensions and other URL checks in the UrlScan.ini file must specify all possible encodings of each character. The number of resulting permutations would be virtually impossible to manage on a production server.	The lockdown mechanism that is built into IIS 6.0 is based on the executable code that is permitted to run ? it is not based on the URL that the client requested. For this reason, **NormalizeUrlBeforeScan** is not necessary on IIS 6.0.	
VerifyNormalization: UrlScan was designed to run on many versions of IIS. The code that handles URL canonicalization has been improved with later releases and service packs of IIS. This feature allows UrlScan to detect potential issues with URL canonicalization on unpatched systems.	The HTTP.SYS component used by IIS 6.0 has improved canonicalization code that has been specifically written to help protect against URL canonicalization attacks.	
DenyUrlSequences: This feature was implemented in UrlScan to allow UrlScan to detect sequences that are used in URL?based attacks on a Web server.	It is not necessary for IIS 6.0 to deny URL sequences. By design, IIS 6.0 is not susceptible to URLbased attacks that use any of the character sequences listed in the default **DenyUrlSequences** section of the UrlScan.ini file provided by Microsoft.	Consider disabling the following Url Sequences: .., :, ./, \, %,&
AllowDotInPath: The UrlScan lockdown me ism depends on a filter notification that occurs very early in the processing of a request. At this time, UrlScan cannot know for sure how IIS will parse the URL for PATH_INFO. It is possible that PATH_INFO will affect the file name extension on the URL. Setting **AllowDotInPath** to 0 will cause UrlScan to reject any request where the file extension is ambiguous due to a dot-in-path condition.	The **AllowDotInPath** feature is not necessary in IIS 6.0 because IIS 6.0 does not depend on filter notifications for its lockdown mechanism.	

UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
RemoveServerHeader: This feature allows UrlScan to remove or alter the identity of the server from the "Server" response header in the response to the client.	IIS 6.0 does not include the **RemoveServerHeader** feature because this feature offers no real security benefit. Most server attacks are not operating system?specific. Also, it is possible to detect the identity of a server and information about the operating system by mechanisms that do not depend on the server header.	
EnableLogging, **PerProcessLogging**, and **PerDayLogging:** UrlScan is not part of the core IIS server. Rather, UrlScan is an add-on utility that produces its own log files. These settings control aspects of how UrlScan produces and names its log files.	IIS 6.0 logs all of its lockdown activity in the W3SVC logs. Requests that are rejected due to lockdown or executable code are identified by 404 errors with sub-error 2 (404.2) in the logs. Requests for static files that are rejected due to an unknown type are identified by 404 with sub-error 3 (404.3) in the logs.	
AllowLateScanning: This feature allows administrators to specify whether UrlScan examines URLs before or after other filters. There are a number of filters that modify URLs, and it might be desirable for UrlScan to examine the URL after it has been modified. The FrontPage Server Extensions filter is an example of such a filter.	The **AllowLateScanning** feature is not necessary in IIS 6.0 because IIS 6.0 does not depend on filter notifications for its lockdown mechanism. The lockdown mechanism built into IIS 6.0 is based on the executable code that is allowed to run ? not on the URL that the client requested.	
RejectResponseUrl: This feature works in conjunction with **UseFastPathReject**. If **UseFastPathReject** is set to 0, then any rejected requests will be remapped to the URL specified by **RejectResponseUrl**. If the specified URL does not exist, the client will receive a normal 404 response just as if the client had requested a non-existent page. If the specified URL does exist, the server can customize the response that is sent to the client.	In IIS 6.0, a request that is rejected due to a lockdown of executable code will generate a 404.2 custom error. A static file that is rejected due to an unknown MIME type will generate a 404.3 custom error. Administrators can use the IIS custom error mechanism to control these responses.	

UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
UseFastPathReject: The UrlScan lockdown mechanism depends on a filter notification that that occurs very early in the processing of a request. As a result, if UrlScan rejects the request directly from this notification, the normal 404 response cannot be generated. Rather, the client will receive a terse 404 response instead of the rich custom error that normally occurs. If **UseFastPathReject** is set to 0, UrlScan will remap the request to the URL specified by **RejectResponseUrl**.	IIS 6.0 does not depend on filter notifications for its lockdown mechanism. In IIS 6.0, a request that is rejected due to lockdown of executable code will generate a 404.2 custom error. A static file that is rejected due to an unknown file type will generate a 404.3 custom error. Administrators can use the IIS custom error mechanism to control these responses.	
AllowHighBitCharacters: This feature allows UrlScan to detect non-ASCII characters in URLs.	The character range that is allowed is handled by HTTP.SYS. This value can be changed by modifying the following registry key: HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ EnableNonUTF8 **Caution:** Incorrectly editing the registry could severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.	
MaxAllowedContentLength: This feature allows UrlScan to place limits on the size of requests that are posted to the server.	IIS 6.0 has the built-in capability to limit the size of requests, which is configurable by the **MaxRequestEntityAllowed** and **ASPMaxRequestEntityAllowed** metabase properties.	

UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
MaxUrl, **MaxQueryString**, and **MaxHeader:** These settings allow UrlScan to place limits on the sizes of URLs, query strings, and specific headers that are sent to the server.	The HTTP.SYS component used by IIS 6.0 allows size limits to be set on various parts of the request. The values can be changed by modifying **AllowRestrictedChars**, **MaxFieldLength**, **UrlSegmentMaxLength**, and **UrlSegmentMaxCount** in the registry under the following registry keys: • `HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ AllowRestrictedChars` • `HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ MaxFieldLength` • `HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ UrlSegmentMaxLength` • `HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ UrlSegmentMaxCount` **Caution:** Incorrectly editing the registry could severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.	

IISLockdown utility

The freely available IIS Lockdown Wizard functions by turning off unnecessary features, thereby reducing attack surface available to attackers. Running this tool implements several best practices:

- Removes IISHelp, IISAdmin, Scripts and other virtual directories installed by default
- Secures unused script mappings
- Disables anonymous Web users' write capability to Web content
- Disables execute permissions on administrative tools
- Backs up the metabase

This tool can be downloaded from: http://www.microsoft.com/technet/security/tools/locktool.mspx